



НИИ
Публичного права
Caspian University

**ҚР Тәуелсіздік күніне орай және
Адам құқықтарының жалпыға бірдей декларациясының
қабылданғанына 75 жыл толуына арналған
«Интернет және адам құқығы»
атты XVII халықаралық ғылыми-практикалық конференциясы
материалдарының жинағы
(Алматы қ., Каспий университеті, 12 желтоқсан 2023 ж.)**

**Материалы
XVII Международной научно–практической конференции
«Интернет и права человека»
посвященной 75-летию принятия Всеобщей
декларации прав человека
и приуроченной ко Дню Независимости РК
(г. Алматы, Каспийский университет, 12 декабря 2023 г.)**

Алматы, 2024

УДК 340
ББК 67
О-13

ОТВЕТСТВЕННЫЕ РЕДАКТОРЫ:

Караев А.А. – кандидат юридических наук, профессор ВШП «Әділет» Каспийского университета

Калимбаева А.Р. – кандидат юридических наук, ассоциированный профессор ВШП «Әділет» Каспийского университета

П68 « Интернет и права человека»: Сб. статей Межд. науч.-практ. конф. (г. Алматы, 12 декабря 2023 г.). – Алматы, 2024. – 391 с. – каз., рус., англ.

ISBN –

В настоящий сборник вошли Материалы XVII Международной научно–практической конференции «Интернет и права человека», посвященной 75-летию принятия Всеобщей декларации прав человека и приуроченной ко Дню Независимости РК.

Материалы предназначены для молодых ученых, исследователей, преподавателей, студентов, магистрантов, докторантов, интересующихся проблемами обеспечения прав человека в условиях современного общества.

**Высшая Школа Права «Әділет» Каспийского университета
Фонд Нурсултана Назарбаева**

«ИНТЕРНЕТ И ПРАВА ЧЕЛОВЕКА»

Материалы

XVII Международной научно–практической конференции

Оркомитет конференции:

Мороз С.П., Караев А.А., Калимбекова А.Р.

В сборник включены тезисы выступлений участников конференции в сфере отечественного и международного опыта обеспечения прав человека в процессе цифровизации жизни общества, вопросов осуществления цифровых прав человека, борьбы киберпреступности, равного доступа к информации, обеспечения защиты детей от противоправного контента, предотвращения киберпреступлений в сфере законодательного урегулирования вопросов обеспечения информационной безопасности в интернет пространстве, вопросы суверенного интернета, кибербуллинга и его возможные формы; защиты интеллектуальной собственности; цифрового судопроизводства и др.

**Каспийский университет
Фонд Нурсултана Назарбаева**

Предисловие

12 декабря 2023 года Высшая школа права «Эділет» и НИИ публичного права Каспийского университета под эгидой Фонда Нурсултана Назарбаева провела очередную XVII Международную научно – практическую конференцию на тему: «Интернет и права человека», посвященную 75-летию принятия Всеобщей декларации прав человека и приуроченную ко Дню Независимости РК.

В 2023 году прогрессивное человечество, в том числе и наша Республика отмечала 75 годовщину принятия Всеобщей Декларации прав человека, провозгласившей права человека в качестве высшей ценности. За годы независимости в Казахстане сформирована национальная система защиты прав граждан среди которых особое место институт Омбудсмана, Уполномоченного по правам ребенка, ювенальная и административная юстиция, Конституционный Суд, и иные правозащитные институты.

В последнее время, продолжаются научные мероприятия, направленные на поиск более эффективных механизмов защиты прав человека. Все эти вопросы нуждаются в серьезном научном анализе и законодательном обеспечении.

Соблюдение норм и принципов международного права, провозглашенных во Всемирной Декларации прав человека и других международных документах в области прав человека является первоочередной задачей современного государства, осуществляющего цель построения правового государства. Казахстан последовательно выполняет все взятые на себя международные обязательства, и последовательно внедряет их в национальное законодательство. В интернет пространстве возникает необходимость обеспечения и соблюдения прав человека - равный доступ к информации, защита детей от противоправного контента, предотвращение киберпреступлений и многое другое. Развитие цифровизации жизни общества актуализирует дискуссию по вопросам цифровых прав человека по всем возможным направлениям. С ростом цифровых технологий институт защиты прав человека нуждается в особом правовом регулировании, при этом

необходимо учитывать также объективные факторы, связанные с недостаточным уровнем цифровой грамотности населения, по-прежнему не теряют актуальности вопросы привлечения к юридической ответственности за кибербуллинг. В условиях стремительного развития интернета наблюдается количественный рост киберпреступности в интернет пространстве. В связи с этим, в обществе появляется необходимость критически осмыслить действующее законодательство и восполнить пробелы в этой сфере. Важно осуществление четкого законодательного урегулирования проблем в сфере цифровизации общества, а также вопросам обеспечения информационной безопасности в интернет пространстве.

В данном сборнике материалов конференции представлены доклады и тезисы докладов участников конференции, в которых затронуты проблемы отечественного и международного опыта защиты прав человека в области защиты прав человека в условиях пандемии, вопросы суверенного интернета, кибербуллинга и его возможные формы; защиты интеллектуальной собственности; цифрового судопроизводства и др.

Оргкомитет конференции

СОДЕРЖАНИЕ

Мукашев С.К. , магистр юридических наук, преподаватель Казахско-русского международного университета, Ильясова А.С. , студентка 3 курса Казахско-русского международного университета ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ВЕРХОВЕНСТВА ПРАВА В ИНТЕРНЕТ ПРОСТРАНСТВЕ	11
Чингисбаева А.Е. , сеньор-лектор Высшей школы права «Әділет» Каспийского общественного университета, м.ю.н. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЛАТФОРМЕННОЙ ЗАНЯТОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН	20
Әбдіқадыр Д.Ә. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің магистранты, Тлешалиев Н.Д. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебі деканы орынбасары, PhD. ЗОРЛЫҚ-ЗОМБЫЛЫҚ ҚЫЛМЫСТАРЫНЫҢ АЛДЫН АЛУДЫҢ КЕЙБІР МӘСЕЛЕЛЕРІ	27
Әбдіқадыр Д.Ә. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің магистранты, Тлешалиев Н.Д. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебі деканы орынбасары, PhD. ТҰРМЫСТЫҚ ЗОРЛЫҚ-ЗОМБЫЛЫҚТЫҢ ТҮСІНІГІ ЖӘНЕ ТҮРЛЕРІ	35
Лаврушко Е.А. , магистр юридических наук, преподаватель Казахско-русского международного университета. ЭФФЕКТИВНАЯ ДЕЯТЕЛЬНОСТЬ ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО, КАК ПОКАЗАТЕЛЬ ОБЕСПЕЧЕНИЯ НЕПРИКОСНОВЕННОСТИ ЛИЧНЫХ ПРАВ И ЧАСТНОЙ ЖИЗНИ ГРАЖДАН В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ ИХ ДЕЯТЕЛЬНОСТИ ...	42
Маджитов Ш. , магистрант 1 курса Университета Международного Бизнеса имени Кенжегали Сагадиева. ПРЕИМУЩЕСТВА И НЕДОСТАТКИ СОЗДАНИЯ ВСЕОБЪЕМЛЮЩЕЙ КОНВЕНЦИИ В РАМКАХ МЕЖДУНАРОДНО-ПРАВОВОЙ БОРЬБЫ С ТЕРРОРИЗМОМ	50
Мамыраим Улан , магистрант 2 курса Университет Международного Бизнеса. НОРМАТИВНО-ПРАВОВАЯ БАЗА ПОПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ В РЕСПУБЛИКЕ КАЗАХСТАН И ЕВРОПЕЙСКОМ СОЮЗЕ	59

Мекебаев А. А., магистрант 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ ЛИЧНОЙ ИНФОРМАЦИИ В СЕТИ ..	70
Нусубалиева М.Е., «Қайнар» академиясының магистранты ПРОЦЕСТІК КЕЛІСІМ ТҮСІНГІ, ЖАСАСУДЫҢ ШАРТТАРЫ	81
Нусубалиева М.Е., «Қайнар» академиясының магистранты. ҚЫЛМЫСТЫҚ ПРОЦЕСТЕГІ ІС ЖҮРГІЗУ КЕЛІСІМІ ИНСТИТУТЫНЫҢ КЕЙБІР АСПЕКТІЛЕРІ	98
Абишев А.Ш., студент 3 курса Юридического факультета Казахского национального университета имени аль-Фараби. ВЛИЯНИЕ ИНТЕРНЕТА И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРАВА ЧЕЛОВЕКА	108
Ақтан Әділет, студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ	116
Аламан А.А., студент 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ: ПОНЯТИЕ, ПРОБЛЕМЫ, РЕШЕНИЯ ПРОБЛЕМЫ И ПРИМЕНЕНИЕ В ТРУДОВОМ ПРАВЕ	121
Алиш З.Б., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. ӘЛЕУМЕТТІК ЖЕЛІНІҢ БАЛАНЫҢ ҚҰҚЫҚТЫҚ САНАСЫНА ӘСЕРІ	126
Аманбай Г., студентка 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. СТАЛКИНГ КАК ВИД КИБЕРБУЛЛИНГА	138
Аманжол Е.Е., студент 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПРАВОВЫЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ ГРАЖДАН В ЦИФРОВОМ ПРОСТРАНСТВЕ	143
Аскербекова А., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 2 курс студенті. САНДЫҚ КЕҢІСТІКТЕГІ ҚҰҚЫҚ БҰЗУШЫЛЫҚ ПРОФИЛІН ЖАСАУ ЖӘНЕ АЛДЫН АЛУ	150
Балтабаева Ж.Р., студентка 1 курса Высшей школы права «Әділет» Каспийского общественного университета. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	159

Батырхан Д.К. , студентка 1 курса Высшей школы права «Әділет» Каспийского общественного университета. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ДОСТУПА К ИНТЕРНЕТ РЕСУРСАМ, К ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ	168
Бер В. , студентка 3 курса Высшей школы права «Әділет» Каспийского Общественного Университета. НЕДОПУЩЕНИЕ МОНОПОЛИЗМА ГОСУДАРСТВОМ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ В СТРАНАХ СНГ	174
Березницкий К. , студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И КИБЕРВОЙН, ФИШИНГА, ХАКИНГА, КРАЖИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРОБЛЕМЫ БЕЗОПАСНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДР	177
Джумалиев Ж.К. , студент 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА РЫНОК ТРУДА РК: ПЕРСПЕКТИВЫ РАЗВИТИЯ	185
Жабаев А.Б. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті. АДАМ ҚҰҚЫҚТАРЫ МЕН БОСТАНДЫҚТАРЫН ҚОРҒАУ	191
Желдыбай Нурдаулет , студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И КИБЕРВОЙН, ФИШИНГА, ХАКИНГА, КРАЖИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРОБЛЕМЫ БЕЗОПАСНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ	200
Жүнісхан Ш.А. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. КИБЕРБУЛЛИНГПЕН КҮРЕСУ ҮШІН БИЛІКТІҢ ӘЛЕУМЕТТІК ЖЕЛІНІ БАҚЫЛАУДЫ КҮШЕЙТУІ АДАМ ҚҰҚЫҒЫН ШЕКТЕУ ЕМЕС ПЕ?	208
Ибрагим Н. И. , студентка 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. КАК ПАНДЕМИЯ ПОВЛИЯЛА НА ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО РК	216
Исабаева Ж. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. ӘЛЕУМЕТТІК ЖЕЛІДЕГІ БАЛА ҚҰҚЫҚТАРЫН ҚОРҒАУ	223

Кайып З.К. , студентка 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ЭЛЕКТРОННЫЕ ПОДПИСИ И ПОДТВЕРЖДЕНИЕ ЛЕГИТИМНОСТИ ТРУДОВЫХ ОТНОШЕНИЙ: ПЕРЕХОД ОТ БУМАЖНЫХ К ЦИФРОВЫМ ФОРМАТАМ	227
Кастоева Дали , студентка 3 курса Университета Международного Бизнеса. БОРЬБА С КИБЕРБУЛЛИНГОМ: КАК ИНТЕРНЕТ ВОЗДЕЙСТВУЕТ НА ПРАВА ДЕТЕЙ И ПОДРОСТКОВ	237
Кахарманова М.К. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің курс студенті. ИНТЕРНЕТ-ХАЛЫҚТЫ ЖҰМЫСПЕН ҚАМТУДЫҢ ЖАҢА НЫСАНЫ РЕТІНДЕ	242
Константинова А.Р. , студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ИНТЕРНЕТ В СФЕРЕ ЗДРАВООХРАНЕНИЯ	248
Кумарбек А. , студент 2 курса “Юриспруденция” Университета Нархоз. УРОВЕНЬ ИНФОРМИРОВАННОСТИ НАСЕЛЕНИЯ РК ОБ ЭЛЕКТРОННЫХ И МОБИЛЬНЫХ ПОРТАЛАХ ПО ОКАЗАНИЮ ГОСУДАРСТВЕННЫХ УСЛУГ	252
Қалжан К.Ө. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. ИНТЕРНЕТ: МЕМЛЕКЕТ БӘРІМІЗДІ БАҚЫЛАУЫ КЕРЕК ПЕ ?	261
Мусаева К. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. КИБЕРҚЫЛМЫС ЖӘНЕ КИБЕР СОҒЫС, ЖЕКЕ ЖӘНЕ КИБЕР СОҒЫС, ЖЕКЕ ДЕРЕКТЕРДІ ҰРЛАУ, ЖЕКЕ ДЕРЕКТЕРДІ ҚАУІПСІЗ САҚТАУ МӘСЕЛЕЛЕРІ	266
Новосёлов А.М. , студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПРОБЛЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ В ИНТЕРНЕТЕ	273
Нурбосун И.С. , Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті. ҚҰҚЫҚТЫҚ АСПЕКТІЛЕРДІҢ ЭВОЛЮЦИЯСЫ: ӘЛЕУМЕТТІК ЖЕЛІ МЕН ИНТЕРНЕТТІҢ АДАМНЫҢ АЗАМАТТЫҚ ІС ЖҮРГІЗУ ҚҰҚЫҒЫНА ӘСЕРІ	280
Өмірхан С. , студентка 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	290

Райымбекқызы А., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті. КИБЕРҚЫЛМЫС: ТҮСІНІГІ, ТҮРЛЕРІ ЖӘНЕ ҚОРҒАНУ ӘДІСТЕРІ	301
Рақым Ә.Б., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. МЕМЛЕКЕТТІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ	309
Рзыкпаева Д.Ж., студентка 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЕГО ВЛИЯНИЕ НА ТРУДОВЫЕ ОТНОШЕНИЯ: ПЕРСПЕКТИВЫ И РИСКИ	314
Сатимова Д.С., студентка 3 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО В СТРАНАХ СНГ	318
Сейткасымов А.Қ., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті. АУА ҮШІН МИЛЛИОНДАР: ИНФОШУЛЕРЛЕР ЖӘНЕ ОНЛАЙН-КУРСТАР	327
Серік М.Б., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 1 курс студенті. ЦИФРЛЫҚ КЕҢІСТІКТЕГІ ҚҰҚЫҚБҰЗУШЫЛЫҚ ЖӘНЕ ОНЫҢ АЛДЫН АЛУ ЖОЛДАРЫ	340
Soltangazy Diana, 2 year student of the Higher School of Law "Adilet", Caspian Public University. THE IMPACT OF ARTIFICIAL INTELLIGENCE ON EMPLOYMENT LAW	347
Сыдыкова П., Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті. ЖАСАНДЫ ИНТЕЛЛЕКТ	355
Таипова Д.Т., студентка 3 курса Юридического факультета Казахского национального университета имени аль Фараби. ПРАВОВОЕРЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КАЗАХСТАНЕ И ЗА РУБЕЖОМ	362
Турдалиев К., студент 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	369
Уксикбаева К., студентка 1 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПОНЯТИЕ КИБЕРПРЕСТУПНОСТИ И ПУТИ БОРЬБЫ С НЕЙ	378
Эльбрусжанұлы К., студент 2 курса Высшей школы права «Әділет» Каспийского Общественного Университета. ПРОБЛЕМА ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ИНТЕРНЕТЕ	382

УДК 340.12 (470)

Мукашев Саламат Кайратович,
преподаватель кафедры «Право» КРМУ, м.ю.н.

Ильясова Алия Сериковна,
студентка 3 курса кафедры «Право» КРМУ
Казахско-Русский Международный университет,
Республика Казахстан, г. Актобе

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ВЕРХОВЕНСТВА ПРАВА В ИНТЕРНЕТ ПРОСТРАНСТВЕ

Аннотация

В настоящее время актуальна проблема обеспечения верховенства права в интернет пространстве. Поскольку именно в интернет пространстве сложно определить, что именно является нарушением личной жизни. В современном обществе стало обычным делом выставлять подробности своей личной жизни в социальных сетях посредством выкладывания своих фото, видео, размещением сведений своего места жительства, работы, семейного положения. И каждый, кто имеет доступ к интернету, без особого труда может собрать интересующие его сведения о другом человеке, а потом использовать их в своих целях.

Ключевые слова: интернет, право, закон, человек, личная жизнь

Мұқашев Саламат Қайратұлы
ҚРМУ «құқық» кафедрасының оқытушысы, з.ф.м.
Қазақстан Республикасы, Ақтөбе қ.

Ильясова Әлия Серікқызы
ҚРМУ «құқық» кафедрасының 3 курс студенті
Қазақ-Орыс Халықаралық университеті
Қазақстан Республикасы, Ақтөбе қ.

**ИНТЕРНЕТ КЕҢІСТІГІНДЕ ЗАҢ ҮСТІМДІЛІГІН
ҚАМТАМАСЫЗ ЕТУДІҢ МӘСЕЛЕЛЕРІ**

Аңдатпа

Қазіргі уақытта интернет кеңістігінде құқықтың үстемдігін қамтамасыз ету мәселесі өзекті болып отыр. Интернет кеңістігінде жеке өмірдің бұзылуының нақты не екенін анықтау қиын. Қазіргі қоғамда өзінің жеке өмірінің егжей-тегжейін әлеуметтік желілерде фотосуреттерін, бейнелерін жариялау, тұрғылықты жері, жұмысы, отбасылық жағдайы туралы мәліметтерді орналастыру арқылы көрсету әдеттегідей болды. Интернетке қол жеткізе алатын кез-келген адам оны қызықтыратын басқа адам туралы ақпаратты оңай жинай алады, содан кейін оларды өз мақсаттары үшін қолдана алады.

Түйінді сөздер: ғаламтор, құқық, заң, адам, жеке өмір

Mukashev Salamat Kairatovich

lecturer of the Department of "Law" of KRMU, M.yu.n.
Republic of Kazakhstan, Aktobe

Ilyassova Aliya Serikovna

3rd year student of the Department of "Law" of KRMU
Kazakh-Russian International University
Republic of Kazakhstan, Aktobe

PROBLEMS OF ENSURING THE RULE OF LAW IN THE INTERNET SPACE

Annotation

Currently, the problem of ensuring the rule of law in the Internet space is urgent. Because it is in the Internet space that it is difficult to determine what exactly is a violation of personal life. In modern society, it has become commonplace to expose the details of your personal life on social networks by posting your photos, videos, posting information about your place of residence, work, marital status. And everyone who has access to the Internet can easily collect information about another person that interests him, and then use it for their own purposes.

Keywords: internet, law, person, personal life

В соответствии со статьей 12 Конституции Республики Казахстан, признаются и гарантируются права и свободы человека и гражданина. Права и свободы человека принадлежат каждому от рождения, признаются абсолютными и неотчуждаемыми. Высшими ценностями госу-

дарства является человек, его права и свободы. На основании статьи 14 Конституции все равны перед законом и судом.

Дискриминация запрещается независимо от социального, должностного, и имущественного положения. Также, какое либо ущемление, либо ограничение прав не допускается по мотивам пола, расы, национальности, языка, по религиозным взглядам или другим обстоятельствам. По поводу соблюдения прав в интернет пространстве и регламентации норм права на которых должна строиться законодательная база на просторах интернет пространства, помимо Конституции Республики Казахстан, таким законом регулирующим общественные отношения в сфере средств массовой информации является закон о СМИ принятый 23 июля 1999 года. Согласно статье 20 Конституции РК свобода слова гарантируется, цензура запрещается. Свобода слова также гарантируется согласно статье 2 закона о СМИ, согласно которой, выражение своих взглядов в печатной и любой другой форме допускается, если это не запрещено законом. Также передавать и распространять информацию любым доступным способом, если это не затрагивает государственные или общественные интересы. Также если данные действия не сопряжены с пропагандой насилия, порнографии, наркотических средств либо их аналогов. Не носят в себе цель изменения насильственным образом конституционного строя, смену власти, пропаганду терроризма.

Однако на просторах сети интернета довольно проблематично отследить соблюдение законодательства, так как ограничение права на доступ либо распространение информации будет являться прямым нарушением Конституции РК, а также ущемлением прав и свобод человека. Также существенным препятствием к привлечению к ответственности лиц злоупотребляющих правом на свободу слова является тот факт, что крайне проблематично привлечь к ответственности лиц нарушающих законодательство о СМИ на просторах интернета, так как в этой сфере не существует в должной мере налаженной судебной практики. Единственный способ защиты собственных прав и свобод является привлечение таких лиц к ответственности в гражданско-правовом порядке через обращение в суд, с целью защиты своей личной жизни, деловой и профессиональной репутации путём опровержения порочащих сведений, затрагивающих честь и достоинство человека. Существуют современные научно-правовые подходы к определению понятия «неприкосновенность частной жизни».

Несмотря на сложность и многоаспектность понятия частной жизни, законодателям, судьям и правоприменителям необходимы определён-

ные инструменты, критерии и классификации для регулирования вопросов защиты права на неприкосновенность частной жизни. Как определить, что те или иные действия нарушают право на частную жизнь? Каким образом регулировать такие действия в законах и на практике, чтобы обеспечить качественную защиту этого права? Некоторые современные ученые исходят из таких прикладных задач и предлагают классифицировать нарушения прав на частную жизнь. Другими словами, вместо того, чтобы фокусироваться на самом понятии частной жизни и раскладывать его на составные элементы, что до сих пор не привело ученых к единому пониманию, они считают, что необходимо определить круг «вредных» действий, которые создают проблемы для реализации права на частную жизнь. Это попытка концептуализировать право снизу-вверх, чем сверху вниз, т.е. через конкретные проблемы и ситуации. Так, например, профессор Даниэл Солове разработал классификацию действий, нарушающих сферу частной жизни, и разбил их на четыре группы:

- сбор информации
- обработка информации
- распространение информации
- вторжение.

Каждая группа включает в себя различные виды деятельности, которые могут создавать проблемы для реализации права на частную жизнь. Определение предложено Зайцевой Ю. П. в статье «Частная жизнь гражданина».

Первая группа действий, которые влияют на частную жизнь, это сбор информации. Наблюдение – это прослушивание или запись действий отдельных лиц. Это включает всевозможные ОРМ (оперативно-розыскные мероприятия) или действия частных компаний по сбору информации о своих клиентах. Опрос состоит из различных форм анкет или поиска информации. Например, вопросы о вероисповедании, политических взглядах или сексуальной ориентации могут рассматриваться как нарушение право личности на частную жизнь.

Вторая группа действий связана с тем, как информация хранится, обрабатывается и используется - то, что совокупности называется «обработка информации», включает в себя комбинацию различных фрагментов данных о человеке. Идентификация связывает информацию с конкретными людьми. В безопасности подразумевается небрежность в защите хранимой информации от утечек и неправильного доступа. Вторичное использование - это использование инфор-

мации, собранной для одной цели, для других целей без согласия субъекта данных.

В этой связи можно сделать выводы о том, что вмешательство в личную жизнь граждан является грубейшим нарушением прав человека и гражданина.

Если, в обычной жизни мы можем определить, что именно является нарушением личной жизни то, в интернет пространстве сделать это практически невозможно, так как в современном обществе стало обычным делом выставлять подробности своей личной жизни в социальных сетях посредством выкладывания своих фото и видео, а также размещением сведений своего места жительства, работы, уровня образования и т.д. Практически любой, имея доступ в интернет без особого труда может собрать интересующие его сведения о другом человеке, а потом использовать эти сведения в своих целях.

Проблема верховенства закона и права всегда волновала мыслителей древности, средневековья, современности и находились в поле зрения философов, юристов, историков, независимо от их взглядов и суждений, а также от того, как называлось это государство. Смысл идеи правового государства у мыслителей, политических и общественных деятелей отличался. Однако независимо от взглядов и суждений о верховенстве закона и права, существование последних неизменно ассоциировалось с торжеством гуманизма, законности, и справедливости. Зачатки теории правового государства прослеживаются в рассуждениях мыслителей Древней Греции, Рима, Индии и других стран. Выражая своё отношение к государственной власти, праву и закону, Аристотель считал, что властвование должно осуществляться только по закону и без всякого насильственного подчинения, которое противоречит идее права. Там, где отсутствует «власть закона», делал вывод Аристотель, там нет места и какой-либо формы государственного строя. Под «истинным законом» Цицерон понимал разумное положение, соответствующее природе, распространяющееся на всех людей, которое служит идеям добра и справедливости, одновременно запрещая любые противодействия против закона.

Теоретической основой правового государства, явился сформулированный Цицероном правовой принцип, согласно которому под действие закона должны попадать все, а не только определённая категория граждан. В Китае ещё в глубокой древности философами и юристами была заложена мысль о том, что в государстве должен царить порядок, основанный на законе. Все эти учения о государстве и праве, исследова-

ния стали основой всего последующего процесса развития гуманистических взглядов и идей, составивших впоследствии фундамент теории правового государства.

Значительный вклад в развитие учений о государстве и праве внёс итальянский политический мыслитель — Марсилий Падуанский. Народ, согласно его учению - это источник всякой власти, носитель суверенитета и верховный законодатель. Право издавать юридические законы имеет народ, а законодательствовать должны наиболее достойные, выбираемые народом люди. Идея правового государства нашла значительное освещение и дальнейшее развитие в произведениях юристов, философов, политологов и социологов нового времени. В этот период она начинает закрепляться в прямой или косвенной форме в законодательстве. Основное внимание в разработке теории правового государства уделяется не только его основным чертам и признакам, но и наиболее важным условиям их формирования. Концепция разделения властей получила разработку в творчестве французского юриста Шарля Луи Монтескье. Различая в каждом государстве три ветви власти - законодательную, исполнительную и судебную, он отмечает, что для предотвращения злоупотреблений властью, необходим такой порядок управления государством, при котором различные ветви власти могли бы взаимно контролировать друг друга.

У немецкого философа Гегеля правовое государство - это действительность. Действительность по Гегелю - разумна, а разумное - действительно. Такую разумную действительность он называет идеей права. Право по Гегелю - это действительность свободы или идея свободы. Государство согласно Гегелю - это тоже право, но развитое право, включающее в себя все остальные более абстрактные права (права личности, семьи, общества). Развитие элементов правового государства прослеживалось на протяжении тысячи лет, но не привело к формированию законченной и оформленной системы. Процесс создания правового и социального государства займет много времени. Движение к этой цели в значительной мере будет зависеть от решения ряда первоочередных проблем: укрепления государственной власти, развития гражданского общества, соблюдения, принципов социальной справедливости.

Верховенство закона является одним из основных элементов правового государства, который обозначает подчиненность всех актов правоприменения и подзаконных актов закону. Верховенство закона обеспечивает защиту, гарантированную основным законом страны, всех прав и свобод человека. Верховенство закона свидетельствует о наличии в

стране соответствующих ценностей и приоритета в развитии правового государства. Верховенство права - правовая доктрина, согласно которой никто не выше закона, все равны перед законом. Положение о верховенстве права и закона является одной из важнейших характеристик правового государства (наряду с разделением властей и связанностью государства и граждан взаимными правами и обязанностями).

Вместе с тем объективно существующее несовпадение права и закона заставляет рассматривать верховенство права и верховенство закона отдельно. В литературе даже отмечается, что идея верховенства права исторически значительно старше идеи верховенства закона. Верховенство закона означает: а) верховенство конституции; б) особую процедуру принятия и изменения закона; в) обязательное соответствие всех иных нормативных актов закону; г) наличие механизмов реализации и защиты закона; д) конституционный надзор, обеспечивающий непротиворечивость всей законодательной системы.

Верховенство (господство) права предполагает прежде всего наличие законов с правовым содержанием (правовых законов), а также связанность государственной власти с правовыми законами, то есть правом. Для формирования верховенства закона и права должны быть созданы соответствующие предпосылки, основы его существования. Экономической основой верховенства закона и права являются производственные отношения, базирующиеся на многоукладности, на равноправии всех форм собственности, которая здесь принадлежит непосредственно производителям и потребителям материальных благ. Только наличие самостоятельности и свободы собственности могут экономически обеспечить господство права, равенство всех участников производственных отношений, постоянный рост благосостояния общества и его саморазвития.

Социальная основа верховенства закона и права является одним из основных элементов правового государства, который обозначает подчиненность всех актов правоприменения и подзаконных актов закону. Социальной основой верховенства закона и права является саморегулирующееся гражданское общество, в центре которого находится человек с его разнообразными интересами и запросами. Через систему социальных институтов создаются необходимые условия для реализации каждым гражданином своих трудовых, творческих возможностей, обеспечиваются личные права и свободы, достойный уровень жизни для всех. Верховенство закона обеспечивает защиту, гарантированную основным законом страны, всех прав и свобод человека. Верховенство

закона свидетельствует о наличии в стране соответствующих ценностей и приоритета в развитии правового государства. Верховенство права - правовая доктрина, согласно которой никто не выше закона, все равны перед законом.

Таким образом следует вывод о том, что необходима государственная политика в сфере воспитания правового сознания нашего общества и установления верховенства закона посредством внедрения правовой культуры и нетерпимости к нарушению закона.

Нравственной основой верховенства закона и права являются общечеловеческие принципы гуманизма и справедливости, равенства и свободы личности, ее чести и достоинства, исключение произвола и насилия над человеком.

Важнейшими предпосылками формирования верховенства закона и права также являются:

- достижение высокого уровня политической культуры и правосознания у широких масс для компетентного участия в управлении государственными и общественными делами;
- утверждение принципа плюрализма мнений во всех сферах жизни общества и государства;
- развитие системы самоуправления народа в центре и на местах;
- последовательное расширение и углубление принципов реальной демократии во всех сферах жизни общества.

Существуют и определенные условия формирования и функционирования верховенства закона и права. К ним относятся:

- достижение высокого уровня политического и правового сознания людей
- создание внутренне единого, непротиворечивого законодательства
- строгое исполнение законов
- наличие в стране гражданского общества как условия и гаранта существования правового государства.

Представим такую ситуацию, что, хотя бы на законодательном уровне общественные отношения в обществе и государстве не регулируются на основе верховенства закона и права. Любой гражданин государства и член общества остается не защищенным от произвола и беззакония со стороны тех лиц, у кого больше власти и соответственно больше и прав. Каждый человек может быть подвергнут к несправедливому и незаконному государственному преследованию со стороны чиновников и бюрократов, которых не устроили твои политические взгляды и мысли,

и в этом случае государство не несет никакой ответственности за действие своих служащих. Работник предприятия, в котором по найму работает специалист, в любой момент может быть уволен только за то, что он не устроил вышестоящее начальство, соответственно он не может защитить свои трудовые права.

В случае наличия какого-либо конфликта или насилия со стороны других лиц, также отсутствует возможность обратиться за помощью закона и права и восстановить социальную справедливость. В таком обществе однозначно я бы не хотел жить. Да, многие права и свободы нам, конечно, достались от предшествующих поколений, которые выстрадали, иногда ценой своей жизни и боролись за них, вознесли их в рамки закона. Однако для формирования верховенства закона и права, мне кажется, нам придется пройти еще не простой путь, если каждый член общества будет обращаться за защитой своих прав и свобод к закону и Конституции, можно еще все изменить в лучшую сторону. В РК существует демократический режим и царит верховенство закона и права, к сожалению, в нашем государстве не все так обстоит благополучно, как нам хотелось бы. Для этого существуют объективные и субъективные факторы, которые необходимо преодолеть. Одно из важных условий, возможно, это крайне радикальное, необходимо наличие прецедентного права, только в этом случае, удастся добиться полного верховенства закона и права.

Список использованных источников:

1. Конституция Республики Казахстан от 30 августа 1995 года
2. Закон Республики Казахстан «О средствах массовой информации» от 23 июля 1999 года № 451-1
3. Статья Зайцевой Ю.П. «Частная жизнь гражданина»: www.gramota.net/materials/3/2015/4-1/15.html
4. Гегель Г.В.Ф. Философия права. Академия наук СССР. Институт философии. М., 1990 г.
5. Аристотель. Политика / пер. с греч. С.Жебелева. – М: Эксмо, 2018 – 384с
6. Политология / под ред. В.Ю.Бельского, А.И.Сацуты, А.Б.Шатилова. – 3-е изд., перераб. и доп. –М: ЮНИТИ-ДАНА, 2021 – 463с

УДК 349

Чингисбаева Анар Елемесовна,
сеньор-лектор Высшей школы права «Әділет»,
Каспийского общественного университета, м.ю.н,
Республика Казахстан, г. Алматы

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЛАТФОРМЕННОЙ ЗАНЯТОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

Данная статья посвящена цифровым технологиям в сфере труда. Какие нормы трудового законодательства регулируют новые формы занятости. Также в статье дается определение платформенной занятости, перечисляются стороны, их обязанности, какие преимущества дают платформы цифрового труда, а также какие проблемы возникают при внедрении новых форм занятости

Ключевые слова: платформенная занятость, цифровые технологии, интернет-платформы, электронная биржа труда, дистанционная работа

Чингисбаева Анар Елемесқызы,
«Әділет» жоғары заң мектебінің сеньор-лекторы,
Каспий қоғамдық университеті, з.ғ.м.
Қазақстан Республикасы, Алматы қ.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА ПЛАТФОРМАДАҒЫ ЖҰМЫСПЕН ҚАМТУДЫ ҚҰҚЫҚТЫҚ РЕТТЕУ

Аңдатпа

Бұл мақала жұмыс әлеміндегі цифрлық технологияларға арналған. Қандай еңбек заңнамасының нормалары жұмыспен қамтудың жаңа нысандарын реттейді. Мақалада сонымен қатар платформалық жұмысқа анықтама берілген, тараптар, олардың міндеттері, цифрлық еңбек платформалары қандай артықшылықтар беретіні, сондай-ақ жұмыспен қамтудың жаңа нысандарын енгізу кезінде қандай мәселелер туындайтыны көрсетілген.

Түйінді сөздер: жұмыс платформасы, цифрлық технологиялар, интернет-платформалар, электронды еңбек биржасы, қашықтан жұмыс

Chingisbaeva Anar,
Senior Lecturer at the Higher School of Law “Adilet”,
Caspian Public University, M.L.Sc.,
Republic of Kazakhstan, Almaty

LEGAL REGULATION OF PLATFORM EMPLOYMENT IN THE REPUBLIC OF KAZAKHSTAN

Annotation

This article is devoted to digital technologies in the world of work. What labor legislation norms regulate new forms of employment. The article also gives a definition of platform employment, lists the parties, their responsibilities, what advantages digital labor platforms provide, as well as what problems arise when introducing new forms of employment

Key words: platform employment, digital technologies, Internet platforms, electronic labor exchange, remote work

В последнее время казахстанцы стали отдавать предпочтение платформенной занятости. Пандемия, развитие цифровых технологий - все это ускорило данное явление. С повышением мобильности граждан все чаще предпочтение в выборе деятельности отдается свободному графику и работе через различные интернет-платформы, которые являются посредниками между услугодателями и клиентами. Платформенная занятость стала популярна среди казахстанцев относительно недавно.

Примерами подобных сервисов являются такие площадки как Яндекс, Uber, Wolt, Naimi, и другие. По экспертным данным, на сегодняшний день на различных интернет-платформах осуществляет свою деятельность порядка 500 тысяч казахстанцев, и их число растет с каждым днем. Совсем недавно целая армия казахстанцев в виде курьеров, доставщиков и таксистов, которые зарегистрировавшись на таких крупных платформах как Indrive, Glovo, Яндекс, Uber, Wolt и др. работали без заключения трудовых договоров и не имея при этом никаких социальных выплат в виде пенсионных отчислений, в ОСМС и т.д. Нередко, к примеру, такая «занятость» приводила к забастовкам курьеров и таксистов, выразивших недовольство таким положением, которые требовали официального трудоустройства и вытекающих из этого социальных

лифтов. Однако, 1 июля 2023 года вступил в законную силу Социальный кодекс Республики Казахстан от 20 апреля 2023 года, в котором впервые получил закрепление новый инструмент трудоустройства, такой как платформенная занятость,

Статья 102 Социального кодекса определяет, что платформенная занятость представляет собой вид деятельности по оказанию услуг или выполнению работ с использованием интернет-платформ и (или) мобильных приложений платформенной занятости.[1]

У платформенной занятости три стороны: оператор интернет-платформы, заказчик и исполнитель.

1) Оператор интернет-платформы – индивидуальный предприниматель или юридическое лицо, оказывающие с использованием интернет-платформы услуги по предоставлению технических, организационных (в том числе услуг с привлечением третьих лиц для оказания работ или услуг), информационных и иных возможностей с применением информационных технологий и систем для установления контактов и заключения сделок по оказанию услуг и выполнению работ между исполнителями и заказчиками, зарегистрированными на интернет-платформе;

2) Заказчик – физическое или юридическое лицо, зарегистрированное на интернет-платформе и размещающее на ней заказ на оказание услуг или выполнение работ;

3) Исполнитель – физическое лицо, индивидуальный предприниматель или юридическое лицо, зарегистрированные на интернет-платформе, оказывающие заказчикам услуги или выполняющие работы с использованием интернет-платформы на основании публичного договора.

Для осуществления платформенной занятости заказчик и исполнитель регистрируются на интернет-платформе и (или) в мобильном приложении платформенной занятости. Взаимоотношения между оператором и заказчиком, а также исполнителем регулируются в соответствии с Гражданским кодексом Республики Казахстан.[2]

В случае привлечения исполнителем – юридическим лицом работников для оказания услуг и выполнения работ с использованием интернет-платформ и (или) мобильных приложений платформенной занятости трудовые отношения с ними оформляются в соответствии с Трудовым кодексом Республики Казахстан.

После принятия Социального Кодекса работники платформ при стабильном отчислении социальных платежей будут получать соот-

ветствующие пенсионные выплаты при достижении пенсионного возраста, социальные выплаты на случай утраты трудоспособности, потери работы, потери дохода в связи с беременностью и родами, потери дохода в связи с уходом за ребенком по достижении им возраста одного года. Также самозанятые станут участниками медицинского страхования, что позволит им пользоваться медицинскими услугами.

Соответствующие поправки были внесены и в Трудовой кодекс. В частности, его дополнили статьей, в которой определены особенности регулирования труда работников, нанимаемых индивидуальным предпринимателем или юридическим лицом, осуществляющим деятельность с применением интернет-платформ или мобильного приложения платформенной занятости (ст.137-1 ТК) [3]

Так, установлено, что трудовой договор между работником и индивидуальным предпринимателем или юридическим лицом, осуществляющим деятельность с применением интернет-платформ или мобильного приложения платформенной занятости, должен заключаться на определенный срок, но без ограничения на срок не менее одного года.

При заключении трудового договора с таким работником должны соблюдаться все нормы трудового законодательства. При этом режим работы, продолжительность ежедневной работы, учет рабочего времени, система и условия труда определяются по согласованию сторон и устанавливаются в коллективном или трудовом договорах, а также актах работодателя. Приведем наглядный пример: если водитель такси или курьер доставки, оказывая услугу попал в ДТП и получил увечья, которые привели к его нетрудоспособности или инвалидности, то он вправе получать социальные выплаты из Государственного фонда социального страхования. В случае поломки автотранспортного средства, а соответственно и утраты источника заработка, водитель такси сможет получать пособие по безработице

В настоящее время Работодатели участвуют в реализации государственной политики в сфере занятости населения путем: предоставления текущих вакансий и данных о прогнозируемом создании рабочих мест в разрезе востребованных специальностей в карьерные центры (центр трудовой мобильности) и (или) Электронную биржу труда;

Работодатель обязан:

1) размещать на Электронной бирже труда сведения о наличии вакансий в течение пяти рабочих дней со дня их появления с указанием условий труда и оплаты, за исключением вакантных должностей госу-

дарственных служащих, выборных государственных должностей, депутатов Парламента и маслихатов, судей Республики Казахстан, лиц, состоящих на воинской службе, сотрудников специальных государственных, правоохранительных органов и государственной фельдъегерской службы, работников Национального Банка Республики Казахстан и его ведомств, уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций;

2) предоставлять карьерному центру (центру трудовой мобильности) письменно или через Электронную биржу труда в полном объеме информацию о предстоящем высвобождении работников в связи с прекращением деятельности работодателя - физического лица либо ликвидацией работодателя - юридического лица, сокращением численности или штата, снижением объема производств и выполняемых работ и услуг, повлекшим ухудшение экономического состояния работодателя, о количестве и категориях работников, которых оно может коснуться, с указанием должностей и профессий, специальностей, квалификации и размера оплаты труда высвобождаемых работников и сроков, в течение которых они будут высвобождаться, не менее чем за один месяц до начала высвобождения;

С развитием технологий растут и требования работодателей к кандидатам на вакансии. Современный работодатель ищет себе не только работников по определенной профессии, но и формирует требования по профессиональным навыкам.

Для него важны навыки быстрого и эффективного решения проблемы в процессе работы, способность работника функционировать в условиях высокого давления и неопределенности. Работник должен уметь адаптироваться к изменениям и быстро переключаться между задачами, постоянно обновлять свои знания и развиваться. Иными словами современный работник должен быть стрессоустойчивым, гибким, обладать навыками аналитического, критического и творческого мышления, обладать лидерскими качествами и эмоциональным интеллектом. Также будет расти, в зависимости от степени технологического влияния на сферы экономики, спрос на навыки в области информационных технологий. К примеру, уже сегодня в сфере обрабатывающей промышленности умение работников использовать технологии и компьютерные программы является одним из приоритетных навыков для работодателей.

Эти навыки не только повышают эффективность работы, но и делают сотрудника более ценным в долгосрочной перспективе. Они особенно

важны в условиях быстро меняющейся экономической и технологической среды. Сотрудники, обладающие этими качествами, могут успешно адаптироваться к новым условиям и приносить дополнительную ценность своим компаниям.

Платформенная занятость, как и любое новое явление имеет свои позитивные и негативные аспекты.

Гибкий график работы позволяет работникам более свободно распределять свое время, что может быть выгодным в современном обществе. Возможность получения дохода без официального трудоустройства. Многие люди предпочитают неформальную занятость из-за возможности быстрого заработка, минуя официальные процедуры. Низкий уровень заработной платы, отсутствие социальных гарантий, таких как медицинское страхование или пенсионные выплаты, нестабильность - это лишь некоторые минусы неформальной занятости.

В Казахстане разработана и утверждена Концепция развития рынка труда на 2024-2029 годы. [4]

Особое внимание в Концепции уделили новым подходам формализации платформенных работников, которых по итогам 2022 года в Казахстане насчитывается порядка одного миллиона человек. Главные плюсы платформенной занятости - гибкость рабочего времени, возможность совмещения с основной деятельностью, баланс карьеры и личной жизни. Поэтому спектр платформенной занятости будет расширяться с каждым годом, проникая в сферы услуг, туризма, IT, торговли, строительства, недвижимости и другие. Основная задача государства - обеспечить защиту трудовых прав и социальные гарантии для платформенных работников.

Таким образом, технический прогресс радикально меняет нашу повседневную жизнь. Цифровые платформы труда стали частью нашего ежедневного быта. В научный оборот вводятся результаты исследования неформальной занятости в Казахстане, как формирующиеся новые и важные аспекты рынка труда, которые нуждаются в регулировании и поддержке со стороны государства. Аргументируется необходимость создания более стабильной и защищенной среды для работников неформального сектора экономики, которые в перспективе могут стать основными формами занятости не только в республике. Этой разновидности нестандартной занятости посвящен доклад МОТ «Перспективы занятости и социальной защиты в мире 2021: Роль платформ цифрового труда в преобразовании сферы труда. [5]

Настоящий доклад – первая серьезная попытка со стороны МОТ осмыслить опыт взаимодействия работников и предприятий с платформами цифрового труда. В его основу были положены результаты опросов и собеседований с участием 12 000 работников из 100 стран мира, 70 предприятий, 16 операторов платформ, а также 14 объединений работников платформ, действующих в различных секторах и странах.

В заключении хочется отметить, что цифровые платформы дают большие возможности как предприятиям, так и работникам. Предприятия выходят на новые рынки труда, сокращают издержки, удаленный режим позволил им увеличить рост электронной торговли, электронных услуг. Вместе с тем необходимо изучить все проблемы, связанные с новыми формами занятости и очень важно при внедрении цифрового труда, не забывать о соблюдении базовых норм трудового права.

Список использованных источников:

1. Кодекс Республики Казахстан от 20 апреля 2023 года № 224-VII ЗРК (Социальный кодекс Республики Казахстан (с изменениями по состоянию на 5.12.2023 г) // Электронный ресурс: <https://adilet.zan.kz>

2. Гражданский кодекс Республики Казахстан от 27 декабря 1994 г. № 268 Гражданский кодекс Республики Казахстан (Особенная часть) от 1 июля 1999, № 409 // <https://online.zakon.kz>

3. Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V ЗРК. // Электронный ресурс: <https://adilet.zan.kz>

4. Издательство «Северный Казахстан» газета «Северный Казахстан», «Концепция будущего» 07.12.23. <https://izdatelstvo-sk.kz/news/v-kazahstane-razrabotana-i-utvergdena-koncepciya7294/>

5. «Перспективы занятости и социальной защиты в мире 2021: Роль платформ цифрового труда в преобразовании сферы труда» https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---sro-moscow/documents/publication/wcms_829515.pdf

ӘОЖ 343.24:343.8(345)

Әбдіқадыр Дәуренбек Әділбекұлы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің магистранты

Қазақстан Республикасы, Алматы қ.

Тлешалиев Нурлан Даулеткулович

Каспий қоғамдық университеті «Әділет»

Жоғары құқық мектебі деканы орынбасары, PhD

Қазақстан Республикасы, Алматы қ.

ЗОРЛЫҚ-ЗОМБЫЛЫҚ ҚЫЛМЫСТАРЫНЫҢ АЛДЫН АЛУДЫҢ КЕЙБІР МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада зорлық-зомбылық қылмыстарын алдын алудың кейбір мәселелері қарастырылған. Авторлар ҚР қылмыстық заңнамасында бекітілген қылмыс пен қылмыстық теріс-қылық түсініктеріне талдау жүргізеді. Талдау барысында статистикалық деректемелерін қаастыра отыра, қылмыстардың ішінде физикалық немесе психикалық зорлық-зомбылықты қолданумен байланысты бірнеше топты бөлек қарастырып етеді.

Түйінді сөздер: зорлық-зомбылық, қылмыстылық, экстремизм, терроризм, қылмыс, жауаптылық, радикализм, адам өлтіру.

Әбдіқадыр Дәуренбек Әділбекұлы

Магистрант Высшей школы права «Әділет»

Каспийского общественного университета

Республика Казахстан, г. Алматы

Тлешалиев Нурлан Даулеткулович

Заместитель декана Высшей школы права «Әділет»

Каспийского общественного университета, PhD

Республика Казахстан, г. Алматы

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРОФИЛАКТИКИ НАСИЛЬСТВЕННЫХ ПРЕСТУПЛЕНИЙ

Аннотация

В статье рассматриваются некоторые проблемы предотвращения насильственных преступлений. Авторы анализируют понятия преступления и уголовного проступка, установленные в уголовном законодательстве Республики Казахстан. В ходе анализа с учетом статистических данных отдельно рассматриваются среди преступлений несколько групп, связанных с применением физического или психического насилия.

Ключевые слова: насилие, преступность, экстремизм, терроризм, преступление, ответственность, радикализм, убийство.

Abdikadyr D.

Master's student of the «Adilet» Higher School of Law
Caspian Public University
Republic of Kazakhstan, Almaty

Tleshaliev N.

Deputy Dean of the “Adilet” Higher School of Law
Caspian Public University, PhD
Republic of Kazakhstan, Almaty

SOME ISSUES IN THE PREVENTION OF VIOLENT CRIMES

Annotation

The article deals with some of the problems of preventing violent crimes. The authors analyze the concepts of crime and criminal misbehavior established in the criminal legislation of the Republic of Kazakhstan. In the course of the analysis, taking into account the statistical data, among the crimes, several groups related to the use of physical or mental violence are separately considered.

Keywords: violence, criminality, extremism, terrorism, crime, responsibility, radicalism, murder.

Қазақстан Республикасының Конституциясының 1-бабында: Қазақстан Республикасы өзін демократиялық, зайырлы, құқықтық және әлеуметтік мемлекет ретінде орнықтырады, оның ең қымбат қазынасы - адам және адамның өмірі, құқықтары мен бостандықтары делінген [1].

Қазақстан Републикасының қылмыстық кодекстің міндеттер: адамның және азаматтың құқықтарын, бостандықтары мен заңды мүдделерін, меншікті, ұйымдардың құқықтары мен заңды мүдделерін, қоғамдық тәртіп пен қауіпсіздікті, қоршаған ортаны, Қазақстан Республикасының конституциялық құрылысы мен аумақтық тұтастығын, қоғам мен мемлекеттің заңмен қорғалатын мүдделерін қоғамға қауіпті қолсұғушылықтан қорғау, бейбітшілік пен адамзат қауіпсіздігін сақтау, сондай-ақ қылмыстық құқық бұзушылықтардың алдын алу болып табылады.

Қылмыстық құқық бұзушылықтар қоғамға қауіптілік және жазаланушылық дәрежесіне қарай қылмыстар және қылмыстық теріс қылықтар болып бөлінеді [2].

Қылмыстық кодексте айыппұл салу, түзеу жұмыстары, қоғамдық жұмыстарға тарту, бас бостандығын шектеу немесе бас бостандығынан айыру түріндегі жазалау қатерімен тыйым салынған айыпты жасалған, қоғамға қауіпті іс-әрекет (әрекет немесе әрекетсіздік) қылмыс деп танылады.

Қылмыстық теріс қылық деп қоғамға зор қауіп төндірмейтін, жеке адамға, ұйымға, қоғамға немесе мемлекетке болмашы зиян келтірген не зиян келтіру қатерін туғызған, оны жасағаны үшін айыппұл салу, түзеу жұмыстары, қоғамдық жұмыстарға тарту, қамаққа алу, шетелдікті немесе азаматтығы жоқ адамды Қазақстан Республикасының шегінен тысқары жерге шығарып жіберу түріндегі жаза көзделген, айыпты жасалған іс-әрекет (әрекет не әрекетсіздік) танылады [2].

«Тіркелген қылмыстық құқық бұзушылықтар туралы» №1-М есебінің нысанына сәйкес, 2021 жылы Қазақстан Республикасында тіркелген қылмыстық құқық бұзушылықтар саны 181979 қылмыстық құқық бұзушылық. Оның ішінде қылмыстық теріс қылықтар 29025. Онша ауыр емес қылмыстар 25550, ауырлығы орташа қылмыстар 78379, ауыр қылмыстар 46174, аса ауыр қылмыстар 2823 [3].

Адам өліміне әкеп соққан қасақана қылмыстардың саны туралы мәліметтерге келсек барлық қылмыстар 1213. Оның ішінде (99-бап. 1 б.) Адам өлтіру -586, (99-бап. 2б.) Адам өлтіру – 150, (100-б) Жаңа туған баланы анасының өлтіруі -8, (101-б)Аффект жағдайында жасалған адам өлтіру – 9, (102-б)Қажетті қорғаныс шегінен шығу кезінде жасалған адам өлтіру – 5, (106-бап. 3 б.) Денсаулыққа қасақана ауыр зиян келтіру – 444, (112-бап. 2 б.) Қажетті қорғаныс шегінен шығу кезінде денсаулыққа ауыр зиян келтіру – 11, (24-бап. 1 б., 24- бап. 3 б., ҚК 99 -бап) Адам өлтіруге дайындалу және қастандық жасау – 224, (104-б.) Абайсызда

қазаға ұшырату – 82, (105-б.) Өзін-өзі өлтіруге дейін жеткізу – 553, (120-бап 1т. 3б.) Зорлау – 1, (121- бап 1т. 3б.) Сексуалдық сипаттағы зорлық-зомбылық әрекеттері - 1, (126-бап 3т. 3б.) Бас бостандығынан заңсыз айыру – 3, (128-бап 2т. 4б.) Адам саудасы – 2, (135-бап 2т. 4б.) Кәмелетке толмағандар саудасы – 2, (192 -бап 1т. 3б.) Қарақшылық – 2 [3].

(Адамның жоғалуы) Қылмыстық жойылу фактісі анықталмаған – 496. (Адамның өлімі) криминалдық өлім фактісі анықталмаған - 2058.

«Тіркелген қылмыстық құқық бұзушылықтар туралы» №1-М есебінің нысанына сәйкес, 2022 жылы Қазақстан Республикасында тіркелген қылмыстық құқық бұзушылықтар саны 184244 қылмыстық құқық бұзушылық. Оның ішінде қылмыстық теріс қылықтар 28634. Онша ауыр емес қылмыстар 26372, ауырлығы орташа қылмыстар 74963, ауыр қылмыстар 51527, аса ауыр қылмыстар 2747 [3].

Адам өліміне әкеп соққан қасақана қылмыстардың саны туралы мәліметтерге келсек барлық қылмыстар 1165. Оның ішінде (99-бап. 1 б.) Адам өлтіру - 515, (99-бап. 2б.) Адам өлтіру – 147, (100-б) Жаңа туған баланы анасының өлтіруі - 9, (101-б) Аффект жағдайында жасалған адам өлтіру – 6, (102-б) Қажетті қорғаныс шегінен шығу кезінде жасалған адам өлтіру – 12, (106-бап. 3 б.) Денсаулыққа қасақана ауыр зиян келтіру – 469, (112-бап. 2 б.) Қажетті қорғаныс шегінен шығу кезінде денсаулыққа ауыр зиян келтіру – 7, (24-бап. 1 б., 24- бап. 3 б., ҚК 99 -бап) Адам өлтіруге дайындалу және қастандық жасау – 151, (104-б.) Абайсызда қазаға ұшырату – 85, (105-б.) Өзін-өзі өлтіруге дейін жеткізу – 420, (120-бап 1т. 3б.) Зорлау – 0, (121- бап 1т. 3б.) Сексуалдық сипаттағы зорлық-зомбылық әрекеттері - 1, (125 -бап 3т. 3б.) Адамды ұрлау – 2, (126-бап 3т. 3б.) Бас бостандығынан заңсыз айыру – 6, (128-бап 2т. 4б.) Адам саудасы – 2, (192 -бап 1т. 3б.) Қарақшылық – 4 [3].

(Адамның жоғалуы) Қылмыстық жойылу фактісі анықталмаған – 369. (Адамның өлімі) криминалдық өлім фактісі анықталмаған - 1704 [3].

Зорлық-зомбылық қылмысы ежелден кез-келген елдің, кез-келген аймақтың, кез-келген қаланың қылмысының ажырамас бөлігі болды. Қылмыстың бұл түрінің айрықша ерекшелігі - оны құрайтын қылмыстарда зорлық-зомбылық компоненті бар.

Қылмыстық кодекстің 1-тарауында қарастырылған қылмыстардың ішінде зорлық-зомбылыққа қатысты келесі топтарды бөліп көрсетуге болады:

- өмір мен денсаулыққа қарсы қылмыстар;
- адамның бостандығына, ар-намысы мен қадір-қасиетіне қарсы қылмыстар;

- жыныстық қол сұғылмаушылық пен жыныстық бостандыққа қарсы қылмыстар.

Сонымен қатар, зорлық-зомбылық қылмысының құрылымына зорлық-зомбылық белгілерінің болуымен сипатталатын басқа да қылмыстарды жатқызуға болады (террористік сипаттағы және экстремистік бағыттағы қылмыстар, сот төрелігі мен басқару тәртібіне қарсы қылмыстар және т.б.), алайда, қол сұғушылық объектісі мен қылмыстық-құқықтық қорғау субъектілерінің ерекшеліктерін ескере отырып, қылмыстың бұл түрлерін қылмыстың тәуелсіз түрлеріне жатқызған жөн.

Зорлық-зомбылық ұғымын анықтау мәселесі осы құбылыстың түсініксіздігі мен күрделілігінде жатыр. «Зорлық-зомбылық» термині Қылмыстық кодексінің Ерекше бөлігінің көптеген баптарында кездеседі, сондықтан бұл санаттың семантикалық мазмұнын нақтылау маңызды рөл атқарады. Осы мақсатта «зорлық-зомбылық» сөзінің лексикалық мағынасына жүгінейік.

В. Далдың түсіндірме сөздігіне сәйкес зорлық-зомбылық-мәжбүрлеу, тұтқындау, ұялшақ, ренжітетін, заңсыз және ерікті әрекет болып табылады [4, бз б].

С.И. Ожеговтың түсіндірме сөздігінде, зорлық-зомбылықты біреуге физикалық күш қолдану, біреуге мәжбүрлі әсер ету деп анықтайды. Осылайша, зорлық-зомбылықтың лексикалық мазмұнына сүйене отырып, оның негізгі белгілері-басқа адамның еркіне қарсы әрекет, күш қолдану деп көрсетеді [5, б. 390].

Қылмыстардың алдын алу-негізгі функциялардың бірі, ол қолданыстағы заңнамаға сәйкес субъектілердің белгілі бір шеңберімен жүзеге асырылуы керек, нәтижесінде қоғамда қалыптасқан криминогендік шиеленіс азаяды, бұл әлеуметтік, экономикалық және саяси сипаттағы көптеген жағымсыз факторларды анықтайды. Ең алдымен, қылмыстың алдын алу қызметі, егер ол қоғамда өзінің өмір сүруімен қылмыстық қол сұғушылықтың өсуіне ықпал ететін криминогендік факторларға тікелей бағытталған болса, қандай да бір нәтижеге ие болады.

Құқық бұзушылық профилактикасы туралы Қазақстан Республикасының 2010 жылғы 29 сәуірдегі № 271-IV Заңына сәйкес, құқық бұзушылық профилактикасы - құқық бұзушылық жасауға итермелейтін себептер мен жағдайларды анықтау, зерделеу, жою арқылы құқықтық тәртіпті сақтауға және күшейтуге бағытталған, құқық бұзушылық профилактикасының субъектілері жүзеге асыратын

құқықтық, экономикалық, әлеуметтік және ұйымдастырушылық шаралар кешені болып табылады [6].

Құқық бұзушылық профилактикасы шараларының жүйесі

Құқық бұзушылық профилактикасы жалпы, арнаулы және жеке шаралар арқылы жүзеге асырылады.

Құқық бұзушылық профилактикасының жалпы шаралары: халықтың әлеуметтік жағынан әлсіз топтарын қорғау жөніндегі шараларды; экономиканы, әлеуметтік саланы, құқық қорғау қызметін басқарудағы қателіктер мен кемшіліктерді жоюға, сондай-ақ құқық бұзушылық профилактикасын нормативтік, ақпараттық, әдістемелік және ресурстық қамтамасыз етуді жетілдіруге бағытталған ұйымдастырушылық-басқарушылық шараларын; азаматтардың жалпы, тұрмыстық және құқықтық мәдениетін арттыратын, жалпы адамзаттық құндылықтарға, заңға мойынсұнушылық мінез-құлыққа, құқыққа қарсы мінез-құлыққа төзбеушілікке бағдарланған адамгершілік қасиеттерін қалыптастыру арқылы криминогендік факторларды жоятын немесе шектейтін идеологиялық шараларды; құқық бұзушылық жасауға тосқауыл болатын ғылым мен техника жетістіктерін қолдану арқылы іске асырылады [6].

Құқық бұзушылықтың жеке профилактикасы шаралары адам не адамдардың шектеулі тобы тарапынан құқық бұзушылық жасаудың алдын алу, сондай-ақ оны жасауға итермелейтін себептер мен жағдайларды жою мақсатында олардың құқықтық санасына және мінез-құлқына жүйелі түрде мақсатты ықпал ету үшін қолданылады [6].

Құқық бұзушылықтың жеке профилактикасы шаралары: профилактикалық әңгімелесу; қорғау нұсқамасы; құқық бұзушылық жасауға итермелейтін себептер мен жағдайларды жою туралы ұсыныс; медициналық сипаттағы мәжбүрлеу шаралары; құқық бұзушының мінез-құлқына ерекше талаптар белгілеу; профилактикалық есепке алу және бақылау; әкімшілік жаза қолдану; ата-ана құқықтарынан айыру не оларды шектеу, бала (ұл, қыз) асырап алудың күшін жою, қамқоршыларды және қорғаншыларды өздерінің міндеттерін орындаудан босату және шеттету, баланы патронаттық тәрбиешінің тәрбиесіне беру туралы шартты мерзімінен бұрын бұзу; сот үкімі бойынша қабылданатын шаралар; әкімшілік қадағалау орнату; жүріп-тұру еркіндігін алдын ала шектеу болып табылады.

Құқық бұзушылықтың жеке профилактикасы шаралары оған қатысты қолданылатын адамның жеке ерекшеліктері, оның жасаған

құқық бұзушылығының қоғамға қауіптілігінің сипаты мен деңгейі ескеріле отырып айқындалады.

Мүдделі адамдар құқық бұзушылықтың жеке профилактикасы шараларын қолдану туралы шешімге Қазақстан Республикасының заңнамасында белгіленген тәртіппен шағым жасауы мүмкін.

Кәмелетке толмағандарға қатысты құқық бұзушылықтың жеке профилактикасы шаралары Қазақстан Республикасының кәмелетке толмағандар арасындағы құқық бұзушылықтың, қадағалаусыз және панасыз қалудың профилактикасы туралы заңнамасында белгіленген ерекшеліктер ескеріле отырып қолданылады.

Тұрмыстық зорлық-зомбылық жасаған адамдарға қатысты құқық бұзушылықтың жеке профилактикасы шаралары Қазақстан Республикасының тұрмыстық зорлық-зомбылық профилактикасы туралы заңнамасында белгіленген ерекшеліктер ескеріле отырып қолданылады [6].

Құқық бұзушылықтың жеке профилактикасы шараларын қолдану Қазақстан Республикасының осы Заңына және өзге де заңдарына сәйкес жүзеге асырылады. Құқық бұзушылықтың жеке профилактикасы шараларын есепке алу орталық атқарушы органдар айқындаған тәртіппен олардың құзыреті шегінде жүзеге асырылады.

Кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы мен балалардың қадағалаусыз және панасыз қалуының алдын алу туралы Қазақстан Республикасының 2004 жылғы 9 шілдедегі N 591 Заңына сәйкес, кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы мен балалардың қадағалаусыз және панасыз қалуының алдын алу - кәмелетке толмағандар арасындағы құқық бұзушылықтардың, қадағалаусыз, панасыз қалудың және қоғамға жат іс-әрекеттердің алдын алуға, оларға ықпал ететін себептер мен жағдайларды анықтауға және жоюға бағытталған, кәмелетке толмағандармен, кәмелетке толмағандардың оларды тәрбиелеу, оқыту немесе бағып-күту жөніндегі міндеттерін орындамайтын не олардың мінез-құлқына теріс әсер ететін ата-аналарымен немесе басқа да заңды өкілдерімен, сондай-ақ кәмелетке толмағандарды құқық бұзушылықтар немесе қоғамға жат іс-әрекеттер жасауға тартып жүрген өзге де адамдармен жеке профилактикасы шараларын қоса жүзеге асыратын құқықтық, педагогикалық және өзге де шаралар жүйесі болып табылады [7].

Қорытындылай келе, қылмысқа қарсы іс-қимыл: теория мен практика мәселелері оның әсер ету объектісінде тудыратын салдары, сондықтан

ол өзінің маңыздылығына байланысты физикалық зорлық-зомбылыққа бой алдыра алмайды. Психикалық зорлық-зомбылық-бұл адамның психикасына тікелей әсер ететін және психикалық жарақат алуға немесе оның ерік бостандығын шектеуге (басуға) қабілетті зорлық-зомбылық.

Зорлық-зомбылық қылмысын мотивация элементі ретінде әрекет ететін немесе қандай да бір мақсатқа жету тәсілі ретінде қызмет ететін физикалық немесе психикалық зорлық-зомбылықты қолданумен байланысты осындай қылмыстардың жиынтығы ретінде анықтауға болады деп санаймыз. Осылайша, зорлық-зомбылықтың екі түрі бар: зорлық-зомбылық-өзімшілдік және өзімшілдік-зорлық-зомбылық. Бірінші типке процедуралық қылмыстар жатады (оларды жасау процесінің өзі қанағаттандырады), екіншісіне - аспаптық (белгілі бір мәселелерді шешу тәсілі ретінде қызмет етеді).

Пайдаланылған қайнар көздерінің тізімі:

1. Қазақстан Республикасының Конституциясы 1995 жылғы 30 тамыз // <http://online.zakon.kz>.

Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. // Электронды ресурс: <https://adilet.zan.kz>

2. Қазақстан Республикасының бас прокуратурасы жанындағы құқықтық статистика және ақпарат комитетінің 2021-2022 жылдарға арналған есебі. // www.gamgor.kz

3. Даль, В. И. Толковый словарь живого великорусского языка: в 4 т. / В. И. Даль ; Совмещен. ред. изд. В. И. Даля и И. А. Бодуэна де Куртенэ. – М. : ОЛМА-ПРЕСС, 2001. – Т. 2 : И-О. – 669 с.

4. Ожегов, С. И. Словарь русского языка : 70 000 слов / С. И. Ожегов ; ред. Н. Ю. Шведова ; Ин-т рус. яз. Акад. наук СССР. - 21-е изд., перераб. и доп. – М. : Рус. яз., 1989.–924 с.

5. Құқық бұзушылық профилактикасы туралы Қазақстан Республикасының 2010 жылғы 29 сәуірдегі № 271-IV Заңы/ Электронды ресурс: <https://adilet.zan.kz>

6. Кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы мен балалардың қадағалаусыз және панасыз қалуының алдын алу туралы Қазақстан Республикасының 2004 жылғы 9 шілдедегі N 591 Заңы/ Электронды ресурс: <https://adilet.zan.kz>

ӘОЖ 343.24:343.8(346)

Әбдіқадыр Дәуренбек Әділбекұлы

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің магистранты
Қазақстан Республикасы, Алматы қ.

Тлешалиев Нурлан Даулеткулович

Каспий қоғамдық университеті «Әділет»
Жоғары құқық мектебі деканы орынбасары, PhD
Қазақстан Республикасы, Алматы қ.

ТҰРМЫСТЫҚ ЗОРЛЫҚ-ЗОМБЫЛЫҚТЫҢ ТҮСІНІГІ ЖӘНЕ ТҮРЛЕРІ

Аңдатпа

Мақалада тұрмыстық зорлық-зомбылықтың түсінігі және түрлері қарастырылған. Сталкинг және харрасмент терминдеріне бөлек назар дара салып, оған қоса авторлар тұрмыстық зорлық-зомбылықтан қорғау жөніндегі қызметінің халықаралық құқықтық актілерге және қолданыстағы қазақстандық заңнамасына талдау жүргізе отыра, құқықтық негізін сипаттайды. Қазақстандағы дағдарыс орталығының қызметін ұйымдастыру және реттеу мәселелеріне назар аударып, тұрмыстық зорлық – зомбылыққа қатысты заңды жауапкершілікті күшейту қажеттілігін атап көрсетеді.

Түйінді сөздер: зорлық-зомбылық, қылмыстылық, экстремизм, терроризм, қылмыс, жауаптылық, радикализм, адам өлтіру.

Әбдіқадыр Дәуренбек Әділбекұлы

магистрант Высшей школы права «Әділет»
Каспийского общественного университета
Республика Казахстан, г. Алматы

Тлешалиев Нурлан Даулеткулович

заместитель декана Высшей школы права «Әділет»
Каспийского общественного университета, PhD
Республика Казахстан, г. Алматы

ПОНЯТИЕ И ВИДЫ БЫТОВОГО НАСИЛИЯ

Аннотация:

В статье рассмотрены понятие и виды домашнего насилия. Уделяя особое внимание понятиям stalking и harassment, авторы, кроме того, описывают правовую основу служб по защите от домашнего насилия на основе анализа международно-правовых актов и действующего казахстанского законодательства. Они обращают внимание на вопросы организации и регулирования деятельности кризисных центров в Казахстане, а также подчеркивают необходимость усиления юридической ответственности за домашнее насилие.

Ключевые слова: бытовое насилие, преступность, экстремизм, терроризм, преступление, ответственность, радикализм, убийство.

Abdikadyr D.

Master's student of the «Adilet» Higher School of Law
Caspian Public University
Republic of Kazakhstan, Almaty

Tleshaliev N.

Deputy Dean of the “Adilet” Higher School of Law
Caspian Public University, PhD
Republic of Kazakhstan, Almaty

CONCEPT AND TYPES OF DOMESTIC VIOLENCE

Annotation

The article discusses the concept and types of domestic violence. Paying special attention to the concepts of stalking and harassment, the authors, in addition, describe the legal basis of services for protection from domestic violence based on an analysis of international legal acts and current Kazakh legislation. They draw attention to the issues of organizing and regulating the activities of crisis centers in Kazakhstan, and also emphasize the need to strengthen legal liability for domestic violence.

Key words: domestic violence, crime, extremism, terrorism, crime, responsibility, radicalism, murder.

Біздің заманауи дамыған қоғамда тұратынымызға қарамастан, отбасылардағы тұрмыстық зорлық-зомбылық жағдайлары өте жиі

кездеседі. Көбінесе адамдар бұл туралы ашық айтпайды – онысы бекер. Қазақстан Республикасының Конституциясында адамның қадір-қасиетіне қол сұғылмайды, әркімнің ар-намысы мен абыройлы атының қорғалуына құқығы бар деп анық жазылған [1].

Тұрмыстық зорлық-зомбылық үшін кінәлі тұлғалар Қазақстан Республикасы «Әкімшілік құқық бұзушылық туралы» кодексінің 73 бабы бойынша жауапкершілікке тартылуы мүмкін, ал олардың әрекеттерінде қылмыстық құқық бұзушылық құрамы бар болған жағдайда, олар Қазақстан Республикасы Қылмыстық кодексінің 109 (ұрып-соғу), 110 (қинау), 131 (қорлау) баптары бойынша қылмыстық жауапкершілікке тартылады [2], [3].

Тұрмыстық зорлық-зомбылықтан қорғау жөніндегі бөлімшелер қызметінің құқықтық негізін БҰҰ Бас Ассамблеясы қабылдаған Адам құқықтарының жалпыға бірдей декларациясы мен Әйелдерге қатысты кемсітудің барлық нысандарын жою туралы конвенция, Қазақстан Республикасының Конституциясы, Қазақстан Республикасының Қылмыстық Кодексі, Қазақстан Республикасының «Әкімшілік құқық бұзушылық туралы» кодексі, Қазақстан Республикасының «Тұрмыстық зорлық-зомбылық профилактикасы туралы» Заңы, Қазақстан Республикасының «Неке (ерлі-зайыптылық) және отбасы туралы» кодексі, Қазақстан Республикасының «Қазақстан Республикасының Ішкі Істер органдары туралы» Заңы және басқа нормативтік құқықтық актілер құрайды [4], [5].

Мемлекет басшысы Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауында отбасылық зорлық-зомбылықты қылмыс санатына жатқызу мәселесі қоғамда көптен бері талқыланып жүр. Құқық қорғау органдары бұл ұсыныстың дұрыс екеніне күмәнмен қарайды. Себебі, мұндай тұрмыстық жағдайларды анықтау оңай емес, яғни осындай оқиғаларды тергеп-тексеру қиынға соғады. Бұл сөздің де жаны бар. Бірақ, қалай десек те, отбасылық зорлық-зомбылыққа көз жұма қарауға болмайды [6].

Отбасында ойран салатындар жазаға тартылмаса, олар одан бетер басынып кетеді. Ал жапа шеккендер мүлдем қорғаусыз қалады. Мұндай әрекеттер үшін жазаны күшейтетін кез келді деп санаймыз. Зардап шеккен жандар елдің сөзінен немесе біреудің қысым жасауынан қорықпауы қажет. Сондықтан, полиция қызметкерлері олармен өте мұқият жұмыс жүргізіп, тиісті шаралар қолдануы керек [6].

Тұрмыстық зорлық-зомбылық күш көрсету, психологиялық, сексуалдық және (немесе) экономикалық зорлық-зомбылық түрінде болуы мүмкін.

Күш көрсету зорлық-зомбылығы - дене күшін қолданып, денені ауырттып денсаулыққа қасақана зиян келтіру.

Психологиялық зорлық-зомбылық - адамның психикасына қасақана әсер ету, оны қорқыту, қорлау, бопсалау немесе құқық бұзушылықтарды немесе өмірге немесе денсаулыққа қауіп төндіретін, сондай-ақ психикалық, дене және жеке басы дамуының бұзылуына әкелетін әрекеттерді жасауға мәжбүрлеу (еріксіз көндіру) арқылы ар-намысы мен абыройын кемсіту.

Сексуалдық зорлық-зомбылық - адамның жыныстың тиіспеушілігіне немесе жыныстық еркіндігіне қауіп төндіретін құқыққа қарсы қасақана іс-әрекет, сондай-ақ кәмелетке толмағандарға қатысты сексуалдық сипаттағы іс-әрекеттер.

Экономикалық зорлық-зомбылық - адамды заңмен көзделген құқығы бар тұрғын үйінен, тамағынан, киімінен, мүлкінен, қаражатынан қасақана айыру.

Қылмыстық құқық бұзушылықтар қоғамға қауіптілік және жазаланушылық дәрежесіне қарай қылмыстар және қылмыстық теріс қылықтар болып бөлінеді [7].

Жыл сайын Ішкі істер министрлігі тұрмыстық зорлық зомбылыққа қатысты 60 мыңнан астам қорғау нұсқамасын шығарады, 8 мыңнан астам адамға қатысты мінез-құлыққа ерекше талаптар белгіленеді.

Сонымен қатар, тұрмыстық зорлық-зомбылық өте жоғары кідіріске ие. Тирандық күйеулерден зардап шеккен әйелдердің 70-90% – ы ұзақ уақыт полицияға көмек сұрамайды. Зорлық-зомбылық құрбаны әртүрлі себептермен басқаларға отбасында не болып жатқандығы туралы хабарлағысы келмейді.

Сондай-ақ әкімдіктердің құрылымында отбасы, балалар және жастар істері жөніндегі үйлестіруші орган құру, азаматтарды тұрмыстық зорлық-зомбылықтың алдын алу жүйесіне тартуды жандандыру ұсынылды. Өңірлерде отбасылық жанжалдаушылар үшін психокоррекциялық бағдарламалар өткізуді ұйымдастыру.

Қазақстанда тұрмыстық зорлық-зомбылық болған жағдайда қайда жүгіну керек?

2022 жылдың қыркүйегінде Мемлекет басшысы өз Жолдауында тұрмыстық зорлық-зомбылық үшін жауапкершілікті күшейту туралы тапсырма берген болатын. Осы нұсқаулыққа сәйкес Қазақстан Республикасы Ішкі істер министрлігі осындай құқық бұзушылықтарды декларациялаудан анықтауға көшуді көздейтін заңнамалық өзгерістерді әзірледі. Түзетулерге сәйкес, енді тұрмыстық зорлық-зомбылық фактісі бойынша

жәбірленушінің арызынсыз да әкімшілік іс қозғауға болады [6].

Бүгінде Қазақстанда 41 дағдарыс орталығы бар, оның 14-і мемлекеттік. Дағдарыс орталықтары мен баспаналарда әйелдерге қамтамасыз ету стандартына сәйкес құқықтық, психологиялық және басқа да көмектер көрсетіледі. «Дағдарыс орталықтары одағы» ММ «Азаматтық бастамаларды қолдау орталығы» КЕАҚ мемлекеттік гранты аясында Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің көмегімен «Тұрмыстық зорлық-зомбылық құрбандарына арналған дағдарыс орталықтарының қызметін және агрессорлармен жұмысты жақсарту жөніндегі шаралар кешені» әлеуметтік жобасын жүзеге асыруда. Тұрмыстық зорлық-зомбылықты басынан өткерген болсаңыз, онда бұл туралы үндемеңіз!!! Тұрмыстық зорлық-зомбылық құрбандарын қорғау мақсатында ішкі істер органдарына тұрмыстық зорлық-зомбылықтың жеке профилактикасы шараларын қолдануға, сондай-ақ оларды Мамандандырылған дағдарыс орталығына жіберуге уәкілеттік берілген.

Қазақстан Республикасы Стратегиялық жоспарлау және реформалар агенттігі Ұлттық статистика бюросы

Тұрмыстық зорлық-зомбылық фактілері бойынша қатысты шығарылған қорғау ұйғарымдары мен белгіленген ерекше талаптар саны келесідей, 2018 жылы-64852, 2019-73541, 2020 – 78832, 2021 – 81648, 2022 – 83998 .

«Тіркелген қылмыстық құқық бұзушылықтар туралы» №1-М есебінің нысанына сәйкес, 2023 жылдың қаңтар айымен қыркүйек айы аралығында Қазақстан Республикасында тіркелген қылмыстық құқық бұзушылықтар саны 124128 қылмыстық құқық бұзушылық. Оның ішінде қылмыстық теріс қылықтар 21348. Онша ауыр емес қылмыстар 18970, ауырлығы орташа қылмыстар 47181, ауыр қылмыстар 34275, аса ауыр қылмыстар 2322 [8].

Адам өліміне әкеп соққан қасақана қылмыстардың саны туралы мәліметтерге келсек барлық қылмыстар 834. Оның ішінде (99-бап. 1 б.) Адам өлтіру - 356, (99-бап. 2б.) Адам өлтіру – 118, (100-б) Жаңа туған баланы анасының өлтіруі -5, (101-б) Аффект жағдайында жасалған адам өлтіру – 6, (102-б) Қажетті қорғаныс шегінен шығу кезінде жасалған адам өлтіру – 5, (106-бап. 3 б.) Денсаулыққа қасақана ауыр зиян келтіру – 340, (112-бап. 2 б.) Қажетті қорғаныс шегінен шығу кезінде денсаулыққа ауыр зиян келтіру – 4, (24-бап. 1 б., 24- бап. 3 б., ҚК 99- бап) Адам өлтіруге дайындалу және қастандық жасау – 101, (104-б.) Абайсызда қазаға ұшырату – 50, (105-б.) Өзін-өзі өлтіруге дейін жеткізу – 804, (126-бап 3т. 3б.) Бас

бостандығынан заңсыз айыру – 6, (128-бап 2т. 4б.) Адам саудасы – 1, Қарақшылық – 4 [3].

(Адамның жоғалуы) Қылмыстық жойылу фактісі анықталмаған – 542. (Адамның өлімі) криминалдық өлім фактісі анықталмаған - 2213 [8].

Бас прокуратураның қоғамдық мүдделерді қорғау қызметі бастығының орынбасары Сәкен Сәмет полицияға күн сайын тұрмыстық зорлық-зомбылық туралы 300-ге жуық хабарлама түсетінін атап өтті. «Қоғам тұрмыстық зорлық-зомбылықты қайтадан қылмыстық жауапкершілікке тартуды талап етеді. Петиция 150 мыңнан астам қол жинады. Біздің академия ғылыми зерттеу жүргізген еді. Бірақ оның қорытындысы бұл құрамдарды қылмыстық жауапкершілікке тартудың қажеті жоқ екендігін анықтадық. Бұған дейін бұл құрамдар ҚР ӘҚБтК-нен ҚР ҚК-на төрт рет енгізіліп, кері қайтарылған еді. Құрамдар қылмыстық кодексте болған кезде ұзақ процедуралық әрекеттерге байланысты жәбірленушілер агрессорларға төзуге мәжбүр болды», - деді ол.

Ол 1 шілдеден бастап Қазақстанда зорлық әрекеттер үшін өтініш беруден анықтау тәртібі енгізілгенін айтты. «Бірінші кезекте, біз тұрмыстық зорлық-зомбылық үшін жауапкершілікті қылмыстық жауапкершілікке тартуды жоспарлап отырмыз. Денсаулыққа орташа және ауыр зиян келтіргені үшін; қабылданған жағдайда тек бас бостандығынан айыру көзделетін болады. Бостандықты шектеу сияқты жазаның бұл түрі толығымен алынып тасталады. Мұнда біз үшін Өзбекстанның тәжірибесі қызықты.

Сондай-ақ, «харассмент» ұғымын енгізу жоспарлануда. Жақында депутаттар бұл тақырыпты өздерінің депутаттық сауалдарында белсенді түрде көтеруде.

Сонымен қатар, қазір әйелдер «сталкинг» сияқты құбылыспен, яғни обсессивті қудалаумен жиі кездеседі. Мұндай әрекеттер үшін көптеген елдерде қылмыстық жауапкершілік енгізілді. Біздің елдеріміз де осындай әрекеттер үшін жазаны қатаңдату туралы ойланатын кез келді», - деді Қошанов. Оның айтуынша, Қазақстанда әйелдер мен кәмелетке толмағандарға қатысты зорлық-зомбылық қылмыстарын тергеу бойынша әйел тергеушілер мамандан бастады. Республика бойынша жедел-тергеу топтарының құрамына 280 әйел-тергеуші енгізілді [9].

Дәстүр бойынша қылмыстық құқық доктринасы зорлық - зомбылықтың екі түрін ажыратады-физикалық және психикалық. Физикалық зорлық-зомбылық дегеніміз-оның еркінен тыс немесе оған қарсы басқа адамға күшпен (тікелей немесе жанама) заңсыз қасақана физикалық әсер ету, оның дене бітіміне, денсаулығына немесе өміріне қол сұғу, оның ерік-жігерін шектеу немесе жоққа шығару.

Егер физикалық зорлық-зомбылықты анықтау проблемалары қылмыстық-құқықтық ғылымда егжей-тегжейлі дамыған болса, онда психикалық зорлық-зомбылық категориясы туралы айту мүмкін емес. Бұл тақырыпқа арналған жұмыстар аз. Психикалық зорлық-зомбылықты зерттеушілердің көпшілігі қауіп-қатер арқылы анықтайды, бұл қауіп психикалық зорлық-зомбылықтың жалғыз түрі ретінде танылады. XX ғасырдың басында. И.Я. Фойницкий қылмыстық заңнама зорлық-зомбылықты психикалық зорлық-зомбылық ретінде қауіп-қатерден тығыз немесе физикалық түрде ажыратады деп айтты [10, 87 б].

Біздің ойымызша, қауіп пен психикалық зорлық-зомбылықты нақты анықтау мүлдем дұрыс емес. Бұл тұжырымдаманы кеңінен түсіндіретін ғалымдар, оған қауіп-қатерден, қорлаудан, қорлаудан, қорлаудан және т. б. қатысты дұрыс деп санайды.

Қазақстан Республикасының қылмыстық кодексінде физикалық және психикалық зорлық-зомбылық анықтамасының болмауы бірқатар зерттеушілердің заңда зорлық-зомбылық тек психикалық қауіптен гөрі қоғамдық қауіптіліктің үлкен дәрежесі бар физикалық зорлық-зомбылықты білдіреді деп санайтындығына әкеледі. Біздің көзқарасымыз бойынша, соңғысы физикалық зорлық-зомбылықтан әсердің субъективті бағытымен және оның әсер ету объектісінде тудыратын салдарымен ерекшеленеді, сондықтан ол өзінің «маңыздылығына» байланысты физикалық зорлық-зомбылыққа ұшырай алмайды. Психикалық зорлық-зомбылық-бұл адамның психикасына тікелей әсер ететін және психикалық жарақат алуға немесе оның ерік бостандығын шектеуге (басуға) қабілетті зорлық-зомбылық.

Зорлық-зомбылық қылмысын мотивация элементі ретінде әрекет ететін немесе қандай да бір мақсатқа жету тәсілі ретінде қызмет ететін физикалық немесе психикалық зорлық-зомбылықты қолданумен байланысты осындай қылмыстардың жиынтығы ретінде анықтауға болады деп санаймыз. Осылайша, зорлық-зомбылықтың екі түрі бар: зорлық-зомбылық-өзімшілдік және өзімшілдік-зорлық-зомбылық. Бірінші типке процедуралық қылмыстар жатады (оларды жасау процесінің өзі қанағаттандырады), екіншісіне - аспаптық (белгілі бір мәселелерді шешу тәсілі ретінде қызмет етеді).

Пайдаланылған қайнар көздерінің тізімі:

1. Қазақстан Республикасының Конституциясы 1995 жылғы 30 тамыз
// <http://online.zakon.kz>.

2. Әкімшілік құқық бұзушылық туралы Қазақстан Республикасының Кодексі 2014 жылғы 5 шілдедегі № 235-V ҚРЗ. / Электронды ресурс: <https://adilet.zan.kz>

3. Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. / Электронды ресурс: <https://adilet.zan.kz>

4. Адам құқықтарының жалпыға бірдей декларациясы Декларация Біріккен Ұлттар Ұйымы Бас Ассамблеясының резолюциясымен 1948 жылғы 10 желтоқсанда № 217 А (III) қабылданған/ Электронды ресурс: <https://adilet.zan.kz>

5. Қазақстан Республикасының Әйелдерді кемсітушіліктің барлық нысандарын жою туралы конвенцияға қосылуы туралы Қазақстан Республикасының 1998 жылғы 29 маусымдағы N 248 Заңы. / Электронды ресурс: <https://adilet.zan.kz>

6. Мемлекет басшысы Қ.К.Тоқаевтың Қазақстан Халқына жолдауы: Әділетті мемлекет. Біртұтас ұлт. Берекелі қоғам. 2022 жылғы 01 қыркүйек/ Электронды ресурс: <https://adilet.zan.kz>

7. Тұрмыстық зорлық-зомбылық профилактикасы туралы Қазақстан Республикасының 2009 жылғы 4 желтоқсандағы N 214-IV Заңы. / Электронды ресурс: <https://adilet.zan.kz>

8. Қазақстан Республикасының бас прокуратурасы жанындағы құқықтық статистика және ақпарат комитетінің 2021-2022 жылдарға арналған есебі.// www.gamgor.kz

9. Бас прокуратура: Қазақстандағы тұрмыстық зорлық-зомбылықты криминализациялаудың қажеті жоқ<https://qaz.ulysmmedia.kz/news/11199-bas-prokuratura-kazakstandagy-turmystyk-zorlyk-zombylykty-kriminalizatsiialaudyn-kazheti-zhok>

10. Фойницкий И. Я. Курс уголовного судопроизводства. –Том I. Изд. 4-е. –С-Пб.: Типография т-ва «Общественная Польза», 1912. – 650 с.

УДК 342.723

Лаврушко Елена Александровна

соискатель ученой степени кандидата юридических наук
Оренбургского государственного университета
магистр юридических наук, преподаватель,
Казахско-русский международный университет
Республика Казахстан, г.Актобе

ЭФФЕКТИВНАЯ ДЕЯТЕЛЬНОСТЬ ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО, КАК ПОКАЗАТЕЛЬ ОБЕСПЕЧЕНИЯ НЕПРИКОСНОВЕННОСТИ ЛИЧНЫХ ПРАВ И ЧАСТНОЙ ЖИЗНИ ГРАЖДАН В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ ИХ ДЕЯТЕЛЬНОСТИ

Аннотация

Актуальность темы исследования связана с внедрением в различные сферы государства и общества современных цифровых технологий, в том числе в деятельность государственных служащих. В связи с данным технологическим прорывом следует считать необходимым изучение положительных и отрицательных сторон процесса цифровизации, которые требуют дальнейшего совершенствования, как в техническом плане, так и на законодательном уровне. Цифровизация деятельности государственных служащих имеет положительные стороны в плане удобства и минимизации потраченного времени гражданами, субъектами бизнеса, государственными органами и т.д. В статье в качестве ключевого вопроса рассмотрены факторы, воздействующие на эффективную деятельность государственных служащих. Кроме этого в рамках данного исследования вынесены на рассмотрение актуальные вопросы организации государственной службы в контексте их правозащитных функций.

Ключевые слова: правоохранительные органы, государственная служба, государство, цифровизация, программа, функции, права.

Лаврушко Елена Александровна

заң ғылымдарының кандидаты ғылыми дәрежесін ізденуші,
Орынбор мемлекеттік университеті
заң ғылымдарының магистрі, оқытушы,
Қазақ-орыс халықаралық университеті,
Қазақстан Республикасы, Ақтөбе қ.

**МЕМЛЕКЕТТІК ҚЫЗМЕТШІНІҢ ТИІМДІ ҚЫЗМЕТІ АЗАМАТТАРДЫҢ ЖЕКЕ
ҚҰҚЫҚТАРЫ МЕН ЖЕКЕ ӨМІРІНЕ ОЛАРДЫҢ ҚЫЗМЕТІН ЦИФРЛАНДЫ-
РУ КОНТЕКСТІНДЕ ҚОЛ СҒҰҒЫЛМАУШЫЛЫҚТЫ ҚАМТАМАСЫЗ ЕТУДІҢ
КӨРСЕТКІШІ РЕТІНДЕ**

Аңдатпа

Зерттеу тақырыбының өзектілігі Мемлекет пен қоғамның түрлі салаларына заманауи цифрлық технологияларды, оның ішінде мемлекеттік қызметшілердің қызметін енгізумен байланысты. Осы технологиялық серпіліске байланысты цифрландыру процесінің техникалық жағынан да, заңнамалық деңгейде де одан әрі жетілдіруді талап ететін оң және теріс жақтарын зерделеу қажет деп санаған жөн. Мемлекеттік қызметшілердің қызметін цифрландырудың азаматтарға, бизнес субъектілеріне, мемлекеттік органдарға және т.б. жұмсалған уақытты барынша азайту және ыңғайлылық тұрғысынан оң жақтары бар. Бұдан басқа, осы зерттеу шеңберінде мемлекеттік қызметті ұйымдастырудың өзекті мәселелері олардың құқық қорғау функциялары контекстінде қарауға шығарылды.

Түйінді сөздер: Құқық қорғау органдары, мемлекеттік қызмет, мемлекет, цифрландыру, бағдарлама, функциялар, құқықтар.

Lavrushko Elena Aleksandrovna

Candidate of the academic degree of Candidate of Legal Sciences
Orenburg State University
Master of Law, Lecturer,
Kazakh-Russian International University of Aktobe,
Republic of Kazakhstan, Aktobe

EFFECTIVE ACTIVITY OF A CIVIL SERVANT AS AN INDICATOR OF ENSURING THE INVIOABILITY OF PERSONAL RIGHTS AND PRIVATE LIFE OF CITIZENS IN THE CONTEXT OF DIGITALIZATION OF THEIR ACTIVITIES

Annotation

The relevance of the research topic is connected with the introduction of modern digital technologies into various spheres of the state and society, including in the activities of civil servants. In connection with this technological breakthrough, it should be considered necessary to study the positive and negative aspects of the digitalization process, which require further improvement, both technically and at the legislative level. Digitalization of the activities of civil servants has positive aspects in terms of convenience and minimizing the time spent by citizens, business entities, government agencies, etc. The article considers the factors affecting the effective activity of civil servants as a key issue. In addition, within the framework of this study, topical issues of the organization of public service in the context of their human rights functions are submitted for consideration.

Keywords: law enforcement agencies, public service, state, digitalization, program, functions, rights.

Государство, являясь особой организацией публичной политической власти господствующего класса (социальной группы, блока классовых сил всего народа), имеет свои задачи и функции.

Эти задачи и функции практически реализуются посредством конкретных действий личного состава, находящегося на службе у государства – государственных служащих. Государство приобретает реальность и силу именно в этих кадрах в контингенте его служащих. Задачи и функции государства становятся, при их практической реализации, задачами и функциями набранных государством, служащих. От государственных служащих зависит работа государства. Государственная служба продолжает и завершает организацию механизма государства, делая её готовой и пригодной к практической реализации задач и функций государства. В каждое звено государственного механизма служба вносит комплекс мер, средств, форм и методов для реальной, практической деятельности. В становлении государственности любого вида государственная служба выступает в качестве первейшего организационного средства выполнения государством своих целей.

В структуре государственной службы различаются чётко две стороны, две группы отношений: организация государственной службы её подготовка и служебная деятельность, осуществление каждым служащим и всеми ими вместе своих служебных практических полномочий[1].

Организация государственной службы означает её формирование для деятельности и включает большой круг вопросов: установление должностных наименований и определение полномочий по каждой должности; выработка правил поступления на государственную службу; подготовка кадров и повышение их квалификации; правила продвижения по службе; применения мер поощрения и мер дисциплинарной и иной ответственности; правил прохождения службы и прекращения служебных отношений и некоторые другие правила.

Другая сторона государственной службы – это практическая деятельность государственных служащих по реализации порученных им полномочий. Одной из таких важных функций является защита прав, свобод и законных интересов человека и гражданина, которая может также выражаться в обеспечении неприкосновенности личных прав граждан. Одним из ярких примеров данной функции государственных служащих служит наличие обязанности у сотрудников органа уголовного пресле-

дования обеспечить не только объективное рассмотрение уголовного дела, но и конфиденциальность информации личного характера, установленную уголовно-процессуальным законодательством. Особенно остро данный вопрос стоит на повестке дня в связи с переходом к использованию электронного формата расследования уголовных дел, поскольку одновременно с введением данного новшества вероятность рисков утечки конфиденциальной информации возрастает.

Каждый служащий занимает должность, определяющую объём его полномочий, которые и подлежат реализации. Со стороны материального содержания эти полномочия весьма разнообразны (в сфере властной деятельности, исполнительной, в правосудии и т.д.), разнообразны они и по правовым формам своей реализации (составление документов, работа с ними, приём лиц, рассмотрение жалоб и т.д.).

Государственная служба представляет собой один из правовых институтов, нормы которого регулируют обе стороны государственной службы (организацию государственной службы и осуществление государственными служащими практических полномочий). Как правовой институт государственная служба объединяет нормы различных отраслей права [2, с. 420].

В настоящее время данная тема широко обсуждается в научных кругах, на страницах монографий, учебных пособий, выходит масса законов и подзаконных нормативных правовых актов. Это связано с новыми подходами к пониманию и месте государственной службы в современном казахстанском государстве, а также с реформами, проводящимися в данном направлении.

Традиционно советская государственная служба рассматривалась как особый вид государственной деятельности, осуществляемой на профессиональной основе работниками государственных органов в целях выполнения задач и функций государства и оплачиваемая им.

При таком подходе к определению государственной службы, выделяются, с одной стороны задачи и функции государства, которые оно выполняет в лице государственных органов и служащих, а с другой – трудовая деятельность по осуществлению данных функций и решению конкретных задач [3, с. 300].

Необходимость создания государственной службы и её правового регулирования обусловлена самим существованием государства с его задачами и функциями, а также потребностью в организации кадрового потенциала государственных органов (законодательной, исполнительной и судебной власти). Именно служащие действуют как персонал в

многочисленных структурах государственных органов, учреждений и организаций, внутри институтов управляющей и управляемой систем; именно их компетентность определяет реальное использование возможностей управления с целью установления требуемого правового порядка в государстве и обществе.

Государственная служба – это публичная служба, т.е. служба в органах публичной власти. С точки же зрения традиционной теории, под государственной понимается служба в государственных учреждениях, предприятиях, организациях и объединениях.

В самом широком теоретическом понимании государственная служба – это осуществление государственными органами кадровой функции управления и практической деятельности всех лиц, получающих заработную плату из государственного бюджета (т.е. от государства в лице его органов и подразделений), и занимающих постоянно или временно должности в аппарате государственных органов, включая органы законодательной, исполнительной и судебной власти, прокуратуры, контрольно – надзорных органов, администрацию государственных (казённых) предприятий.

С точки зрения современного законодателя, государственная служба в РК – это профессиональная деятельность, состоящая в выполнении государственными служащими органов государственной власти РК и субъектов РК компетенции этих органов, установленной в законодательных и иных нормативных актах.

Принципы государственной службы — это основополагающие идеи, установления, выражающие объективные закономерности и определяющие научно – обоснованные направления реализации компетенции, задач и функций государственных органов, полномочий государственных служащих, действующих в системе государственной службы.

Принципы государственной службы – это субъективное понятие. Они формулируются человеком (законодателем), исходя из конкретного правового опыта и правовой культуры, в стране базируются на основных положениях правовой системы с учётом достигнутого уровня развития отраслевого законодательства [4, с. 92].

Принципы современной государственной службы закрепляются в различных законодательных и других нормативных правовых актах: Конституции РК, указах Президента РК, постановлениях Правительства РК, конституциях уставах и иных законодательных и нормативных актах субъектов РК.

Они реализуются государственными служащими посредством их практических действий. Принципы государственной службы, установ-

ление в Законе РК «О государственной службе», являются моделью для всех других законодательных и иных нормативных правовых актов, которые также определяют систему принципов публичной службы.

«Государственная служба в Республике Казахстан основывается на следующих принципах:

- Законности;
- Казахстанского патриотизма;
- Единства системы государственной службы, независимо от разделения государственной власти на законодательную, исполнительную и судебную ветви;
- Приоритета прав, свобод и законных интересов граждан перед интересами государства;
- Общедоступности, то есть равного права граждан республики на доступ к государственной службе и продвижения по государственной службе в соответствии со своими способностями и профессиональной подготовкой;
- Добровольности поступления граждан на государственную службу;
- Профессионализма и компетентности государственных служащих;
- Равной оплаты труда за выполнение равнозначной работы;
- Обязательности исполнения решений, принятых вышестоящими государственными органами и должностными лицами в пределах их полномочий, для подчиненных государственных служащих и служащих нижестоящих государственных органов;
- Подконтрольности и подотчетности государственных служащих;
- Учета общественного мнения и гласности, за исключением деятельности, составляющей государственные секреты или иную охраняемую законом тайну;
- Правовой и социальной защищенности государственных служащих;
- Поощрения государственных служащих за добросовестное, инициативное исполнение должностных обязанностей, выполнение заданий особой важности и сложности;
- Личной ответственности за неисполнение либо ненадлежащее исполнение государственным служащим должностных обязанностей и превышение им своих полномочий;
- Непрерывности повышения квалификации государственных служащих».

Реформирование государственной службы обусловлено многими факторами, главными из которых являются: необходимость реформ системы государственного управления и создания новой государственности в РК; обеспечение действия принципа разделения государственной власти на законодательную, судебную и исполнительную; осуществление правовой реформы; проведение экономической и хозяйственной реформы; укрепление органов государственной власти; укрепление органов государственной власти субъектов РК и органов местного самоуправления;

Правовое регулирование государственно – служебных процессов в настоящее время отстаёт от темпов развития тенденций и закономерностей в реформировании системы государственного управления, аппарата государства.

Государственная служба как правовой институт должна обеспечить стабильное управление; она может играть определённую роль в стабилизации социально-политической жизни, разрешении политических конфликтов, уравнивании действий различных политических сил, а также защите личных прав человека и гражданина [5, с. 153].

Согласно передовому мировому опыту, в органах государственного управления существует строгое разделение политической и административно – исполнительной деятельности, а также соответствующих им должностей.

В качестве прорыва в деятельности современного государственного служащего по защите прав человека является использование современных цифровых технологий, например, портала электронного уголовного дела в уголовном процессе. Данная новелла в деятельности государственных служащих не только способствует минимизации коррупционных рисков, но и реализации их эффективной деятельности в области обеспечения личных прав человека и гражданина. Однако, дальнейшее совершенствование цифровых технологий способно, по нашему мнению, улучшить деятельность государственных служащих, а также сократить случаи утечки конфиденциальной и «тайной» личной информации человека и гражданина.

Ключевой проблемой при создании эффективной системы государственного управления является рационализация структуры центральных исполнительных органов и упорядочение их деятельности. Положительное решение этой проблемы создаст соответствующее условия для рационализации территориального управления и оптимального перераспределения функции между центральными и местными исполнительными органами, что является целью второго этапа реформ.

Таким образом, цель реформирования государственной службы в Республики Казахстан заключается в создании эффективной системы государственного управления, обеспечивающей устойчивое социально – экономическое развитие за счет эффективного государственного регулирования.

Список использованных источников:

1. Этический кодекс государственных служащих Республики Казахстан (правила служебной этики государственных служащих) - Алматы: Юрист, 2019. - 12 с. (на каз/рус яз)
2. Дуйсенов Э.Э., Шпекбаева А.Ж. Государственная служба Республики Казахстан: Учебник. - Алматы: Асыл кітап, 2021. - 488с.
3. Журсимбаев С.К. Прокурорский надзор: Учебник. - 3-е изд.- Алматы.: NURPRESS, 2019. - 336 с.
4. Повышение эффективности деятельности государственных служащих [текст] / М. Д. Сайымова. - Алматы: Эверо, 2018. - 92 с.
5. Правоохранительные органы Республики Казахстан: учебное пособие / А. Б. Шарипова. - Алматы: Қазақ университеті, 2020. - 164 с.
6. Государство и местное самоуправление: современные вызовы. К 140-летию барнаульской городской Думы: Сб статей по итогам Всероссийской научно-практической конференции. - Барнаул: Изд-во Алт. унта, 2018. - 272 с.

УДК 342:323.285

Маджитов Шахмурат

магистрант 1 курса

Университета Международного Бизнеса

имени Кенжегали Сагадиева

Республика Казахстан, г. Алматы

**ПРЕИМУЩЕСТВА И НЕДОСТАТКИ СОЗДАНИЯ
ВСЕОБЪЕМЛЮЩЕЙ КОНВЕНЦИИ В РАМКАХ
МЕЖДУНАРОДНО-ПРАВОВОЙ БОРЬБЫ
С ТЕРРОРИЗМОМ**

Научный руководитель:

Сатбаева А.М.

к.ю.н., доцент СГН УМБ

Аннотация:

Статья посвящена обзору и анализу преимуществ и недостатков создания всеобъемлющей конвенции в рамках международно-правовой борьбы с терроризмом. Автором определены значение и роль борьбы с терроризмом, а также ее развивающаяся проблематика. Помимо этого, в статье указаны виды и классификация терроризма, варианты борьбы, предложенные с начала XX века, и преимущества и недостатки общей конвенции на международном уровне.

Ключевые слова: терроризм, виды терроризма, международная борьба с терроризмом, конвенция, ООН, проект по борьбе с терроризмом.

Мәджитов Шахмұрат

Кенжеғали Сағадиев атындағы Халықаралық бизнес университетінің

1 курс магистранты

Қазақстан Республикасы, Алматы қ.

**ТЕРРОРИЗММЕН ХАЛЫҚАРАЛЫҚ-ҚҰҚЫҚТЫҚ КҮРЕС ШЕҢБЕРІНДЕ
КЕШЕНДІ КОНВЕНЦИЯ ЖАСАУДЫҢ
АРТЫҚШЫЛЫҚТАРЫ МЕН КЕМШІЛІКТЕРІ**

Аңдатпа:

Мақала терроризмге қарсы халықаралық-құқықтық күрес шеңберінде кешенді конвенцияны құрудың артықшылықтары мен кемшіліктерін шолу мен талдауға арналған. Автор терроризмге қарсы күрестің маңызы мен рөлін, сондай-ақ оның дамып келе жатқан проблемаларын анықтады. Сонымен қатар, мақалада терроризмнің түрлері мен жіктелуі, XX ғасырдың басынан бастап ұсынылған күрес нұсқалары және жалпы Конвенцияның халықаралық деңгейдегі артықшылықтары мен кемшіліктері көрсетілген.

Түйінді сөздер: терроризм, терроризм түрлері, терроризмге қарсы халықаралық күрес, конвенция, БҰҰ, Терроризмге қарсы күрес жобасы.

Madzhitov Shakhmurat

1st year master's student

University of International Business named after Kenzhegali Sagadiev
Republic of Kazakhstan, Almaty

**ADVANTAGES AND DISADVANTAGES OF CREATING A COMPREHENSIVE
CONVENTION WITHIN INTERNATIONAL LEGAL STRUGGLE AGAINST TERRORISM**

Abstract:

This article is devoted to the review and analysis of advantages and disadvantages of creating a comprehensive convention within international legal struggle against terrorism. The main role and meaning of fight against terrorism and this fast-developing problem were created by author of this research. Besides that, the article identifies the types and classification of terrorism, the options for combating it proposed since the beginning of the twentieth century, advantages and disadvantages of general convention at the international level.

Key words: Terrorism, types of terrorism, international fight against terrorism, convention, the UN, project against terrorism.

В условиях динамичного развития стран в современном мире также трансформируются политические системы, растет количество субъектов политической деятельности, изменяются виды и практики их отношений. Политические права граждан дают возможность участвовать в политической жизни сообщества, в рамках национального закона. Но, помимо этого, растет форма политического протеста, которая не всегда носит характер институционального, а может приобретать виды экстремистского образа.

За последние десятилетия терроризм претерпел колоссальные изменения, связанные с его высокой организованностью, с возрастанием числа горячих точек на Ближнем Востоке, с возвращением гражданских лиц из эпицентра военных действий, изменением методов вербовки людей в свои ряды. По статистическим данным СМИ на 2018 г. отмечается ежегодный рост террористических инцидентов (15 321 эпизодов теракта по всему миру), что подчеркнуло глобальный характер террористической угрозы. Международное сообщество оказалось не готово к такому форсированному изменению событий[1].

На данный момент существуют ряд проблем, связанных с терроризмом. Одно из них отсутствие четкого понимания определения понятия «терроризм». Оно имеет слишком размытые границы, пока можно

лишь говорить особирательном образе терроризма, содержащие признаки ряда преступлений.

На сегодняшний день существуют довольно оснащенные террористические организации. Сама суть терроризма состоит из насилия с вытекающим устрашением, а целями для совершения террористических актов может служить:

- революция;
- падение престижа власти;
- развязывание войны;
- обретение независимости;
- дестабилизация общества.

За причинами развития международного терроризма следует несколько главных аспектов, которые в свою очередь могут быть связаны к духовной культуре, политическим «взбучкам» и социально-экономической сфере [2].

Если обращать внимание на последнюю причину, то тут играют факторы низкого уровня жизни население и массовость вооружения населения. Духовность же олицетворяет религиозный фанатизм или утраты нравственности, а вот с политической точки зрения все намного сложнее. Так как играют множество факторов, начиная от выражения агрессии стран по отношению к друг к другу, заканчивая разжигании место уобицы внутри государства.

Проблематика международного терроризма является связующим звеном со всеми основными сферами жизнедеятельности мирового сообщества, например, с такими, как экология, политика, религия. Обращаясь к последней, стоит отметить, что обусловлена она действиями вооруженных групп радикально настроенных сторонников борьбы противгосударств, где имеет преимущество иная религия. Более редкий, но все еще имеющий место быть, — это экологический терроризм, который проявляется, как и любой другой, в насильственной форме с целью предотвращения научно-технического прогресса или загрязнения определенной окружающей среды[3].

Что не менее важно, это наличие проблемы международно-правовой борьбы с терроризмом, у которойотсутствует систематизациякрупного объема международных документов в этой сфере. В мире насчитывается более сорока региональных и универсальных конвенций, это обуславливает проблему международного правотворчества и понимания низкой эффективности борьбы государства с терроризмом.

Для эффективной борьбы с терроризмом нужно понимать причины

его возникновения, осознавать уровень опасности быстрого распространения идеологии террористических организаций в регионе, знать мотивы и характер террористической деятельности. Имеются примеры классификации терроризма известные миру по данным на сегодняшний день.

По характеру субъекта террористической деятельности терроризм можно разделить на:

– физические лица (одиноким терроризм) – они самостоятельно подготавливают, организуют и проводят теракты. В западной политике это явление называется терроризмом «одиноким волком».

– организованный, коллективный — террористическая деятельность планируется и реализуется целой организацией (ИРА, Аль-Каида, ИГИЛ, Красный террор и др.) Организованный терроризм – самый распространенный в мире, в связи с этим большинство контртеррористических организаций ряда государств разработали механизм по противодействию его распространению и предотвращению террористических актов на стадии разработки плана операций.

По целенаправленности терроризм делится на:

Националистический терроризм – преследует сепаратистские цели, фактически формирование собственного государства для своей этнической группы.

Религиозный терроризм – вид терроризма, основанный на религиозном фанатизме. Этот вид терроризма остро проявил себя в борьбе Палестинцев с Израилем. Источником разногласий явилось создание независимой территории Палестина.

Идеологически заданный, социальный — преследует цель привлечения внимания общества к какой-либо острой проблеме. Иногда этот вид терроризма называют революционным.

Государственный террор — террор, используемый политической властью посредством массовых политических репрессий для устрашения противников. Отличительной чертой является массовость.

Экономический террор — устрашение или уничтожение политических противников путём частичного или полного лишения средств к существованию[4].

Обращая внимание на развитие международно-правовой борьбы с терроризмом, стоит отметить, что начало оно взяло с XX века. Именно в это время международное сообщество начало предпринимать ряд попыток, для признания терроризма международным уголовным преступлением. Конвенция 1937 г. положила начало коллективному между-

народному сотрудничеству в борьбе с терроризмом на правовых основах. Документ все еще имел чрезмерно общий и слабо разработанный характер, однако и этого хватило для качественного скачка в развитии антитеррористической деятельности, что является плюсом для первого шага в борьбе с терроризмом.

В дальнейшем принимается ряд конвенций, посвященных антитеррористической деятельности. Только в 1960-х - начале 90-х годов Организация Объединенных Наций и ее специализированные учреждения разработали 10 международных соглашений, которые являются правовыми средствами борьбы с терроризмом (8 конвенций и 2 протокола). Все они отсылают на внутреннее законодательство государств для привлечения повинных лиц за теракт к уголовной ответственности, так как в них данные нормы не установлены, а также вводят принцип межгосударственных отношений, под названием «autdedereautjudicare», что означает «либо выдать, либо предать суду» [5].

Стоит отметить, что в дальнейшем активное участие в разработке антитеррористических норм принимает исключительно ООН. Все конвенции принимаются, как реакция на уже совершенные теракты в мире. Но при наличии несколько слабосвязанных конвенций, борьба с терроризмом ведется слишком хаотично, это можно понять, проанализировав те же конвенции, которые принимаются с опозданием и, не охватывая весь список разновидностей террористического поведения. Акцент ставится на противодействие терроризму, а не его искоренению в целом. Все эти черты проявляются и на современном этапе развития [6].

Очень важно понимать, что помимо борьбы с терроризмом, необходимо создавать нормы для искоренения причин и условий терроризма, что современные универсальные конвенции предложить не могут. Отсюда следует сделать вывод о необходимости создания всеобъемлющей конвенции для всех государств в рамках борьбы с международным терроризмом. В частности, этим может заниматься Совет Безопасности ООН(далее – СБ). СБ необходимо выстраивать правильную иерархию мировых угроз, тем самым повышая продуктивность. Развитие нашего общества слишком динамично, оно влечет за собой расширение списка потенциальных угроз, с которым можно бороться путем быстрого реагирования со стороны международных структур, регулирующих данные вопросы. Важно понимать, что терроризм, который мы имеем в нынешней форме, можно было искоренить в его зачатке, а не бороться с ним, когда он окреп и ищет новые способы показать свою мощь миро-

вому сообществу. В связи с этим необходимо любое проявление конфликтной ситуации начать регулировать задолго до ее превращения в проблему мирового уровня.

Можно выделить два острых минуса, связанных с тем, что резолюция Совета Безопасности ООН по борьбе с терроризмом может установить новые правила, обязательные для всех стран. Первое, резолюции не универсальны, они не имеют договорной характер, что делает процесс чрезвычайно сложным в связи с тем, что в документе могут отсутствовать формулировки, устраивающие всех участников, а это в свою очередь влияет на фактическое соблюдение резолюций СБ государствами. Также возникает проблема имплементации, вероятность отсутствие возможности реализации из-за специфики национальной правовой системы может повлечь за собой потерю силы юридической обязанности акта СБ ООН. Этот факт создает негативную тенденцию обоснованного неисполнения предписания.

Второе, вступление решений СБ ООН автоматически и незамедлительно создает коллизию с фундаментальным принципом государственного суверенитета. Так, если государство не изъявило желание участвовать в каком-либо соглашении, вопреки этому факту становится обязательными наряду с государствами-участниками принимать соответствующие меры по исполнению требований резолюций СБ ООН. Таким образом, мы понимаем силу резолюций СБ ООН, как актов, она многократно превосходит те же конвенции, в связи с тем, что число их участников не ограничено волеизъявлениями подписавших и присоединившихся стран.

Представляется, что необходимо установить конкретные рамки правотворческой функции СБ в сфере борьбы с терроризмом, в связи с этим можно предложить несколько правил:

2. Все действия СБ ООН должны быть в рамках Устава ООН для ограничения возможностей, так как именно благодаря этому можно регламентировать поведение Совета по принятию решений.

3. Резолюции СБ ООН должны иметь четкую иерархию наиболее значимых проблем и должны быть посвящены их решению.

4. Резолюции СБ ООН, посвященные борьбе с терроризмом, должны решать вопросы, требующих быстрого реагирования. Содержание этого требования должно быть сформировано для внедоговорного пути принятия мер.

4. Правовые нормы, разработанный СБ ООН, не должны создавать коллизии с правилами действующих международных договоров[7]. Основные надежды на качественное развитие международно-

правовой борьбы с терроризмом связаны вокруг проекта Всеобъемлющей конвенции о международном терроризме (далее – Проект). В данный момент Проект является самым перспективным методом борьбы с международным терроризмом для всех государств.

В Проекте содержится ряд важных документов, содержащих основополагающие моменты, которые является важным преимуществом для борьбы. Так, в частности, перечисляются следующие аспекты: безоговорочное осуждение всех преступных актов, методов и практик, не имеющих оправдание. Признается, что терроризм может угрожать безопасности в мире, территориальной целостности государств, подрывать дружественные межгосударственные отношения и препятствовать успешному сотрудничеству между государствами. Перспективами для Проекта можно выделить: сохранение личных государственных методов борьбы с терроризмом; проведение антитеррористических командно-штабных и оперативно-тактических учений; проведение саммитов, на которых готовятся международно-правовые документы быстрого реагирования, касающиеся вопросов борьбы с терроризмом, сепаратизмом и экстремизмом, а также проводит подготовку кадров для антитеррористических формирований.

Стоит отметить, что на сегодняшний день международно-правовая борьба с терроризмом отражает современные тенденции в развитии международного правопорядка, такие как:

- сложность правовой системы международного режима направленной на борьбу с терроризмом;
 - укрепить горизонтальные связи между правовыми системами;
 - расширить нормативную базу борьбы с международным терроризмом,
- а значит, и укрепить его позиции в самостоятельной правовой системе в международном праве [8].

Отсюда можно сделать вывод о том, что из-за нерешенных системных проблем, международно-правовая борьба с терроризмом не может рассматриваться, как законченная форма международного права. И статус международно-правовой борьбы с терроризмом во всей международной правовой системе все еще требует обсуждения. Факты доказали, что установление международно-правовых норм в этой области и управление ими, обусловлено необходимостью решения новых задач системы международной безопасности. То есть, специальные задачи были сформированы, и они могут быть решены только путем применения ме-

ханизмов международного права. Так как основная цель международного права заключается в «создании наилучших международных условий для всестороннего развития страны», подчеркивает, что основные цели международных договоров и других международных актов, направленных на борьбу с терроризмом, не должны заменять собой законодательство и установление четких государственных кодексов поведения для обеспечения широкого признания и применения этих правил.

Тем не менее очень важным моментом является усовершенствование практики привлечения к ответственности за террористические деяния в международных судебных учреждениях. Форсированное изменение тенденций террористической деятельности требует тщательного исследования и разработке эффективных механизмов по их противодействию.

Список использованных источников:

1. Осташев, А. А. (2021). Терроризм в современном мире: понятие, виды, причины и уголовная ответственность за содеянное. *E-Scio*, (4 (55)), 611-626.
2. Соснин, В. (2022). Психология терроризма и противодействие ему в современном мире. Litres.
3. Тимохина, А. В., & Шарыпова, Т. Н. (2020). Актуальные направления антитеррора, и проблема международного терроризма в современном мире. In *Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений* (pp. 128-130).
4. Мешалкин, С. Н. (2020). Международная практика установления признаков терроризма как уголовно-правовой категории: научные и практические подходы к оценке её эффективности. // *Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации*, (2), 62-66.
5. Дусметова, С. И., & Адилбайулы, Н. А. (2020). Проблема терроризма в республике Казахстан. *Постсоветские исследования*, 3(4), 297-303.
6. Изотова, Е. Ю., & Сигаева, А. А. (2022). Перспективы международного сотрудничества в области борьбы с терроризмом. In *Молодежь и системная модернизация страны* (pp. 371-375).
7. Самойлюк, Р. Н., & Адмиралова, И. А. (2021). К вопросу о создании концепции развития международного межведомственного центра подготовки и переподготовки специалистов по борьбе с терроризмом и экстремизмом на 2021-2025 гг. *Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации*, (2), 119-124.

8. Гридчин, А. А., & Зырянова, М. О. (2019). Подготовка кадров и финансирование международных проектов в сфере борьбы с терроризмом и экстремизмом в спорте как один из важнейших элементов мировой безопасности. In Противодействие преступности в сфере профессионального спорта (pp. 27-33).

УДК 4414

Мамыраим Улан
магистрант 2 курса

Университет Международного Бизнеса
Республика Казахстан, г. Алматы

**НОРМАТИВНО-ПРАВОВАЯ БАЗА
ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ
В РЕСПУБЛИКЕ КАЗАХСТАН И ЕВРОПЕЙСКОМ СОЮЗЕ**

Научный руководитель:
Татарина Л.Ф.
к.ю.н., доцент СГН УМБ

Аннотация

Статья посвящена обзору и анализу нормативно-правовой базы Республики Казахстан и Европейского Союза по противодействию киберпреступлениям. Автором определены значение и роль основных нормативно-правовых документов, регулирующих правоотношения в сфере кибербезопасности, а также указана официальная статистика по инцидентам связанными с киберпреступлениями в Республике Казахстан. А также в статье рассмотрен не только наднациональный правовой уровень, связанный с обеспечением кибербезопасности в Европейском Союзе, но и национальный правовой уровень на примере Французской Республики, как одной из стран-участниц данного союза.

Ключевые слова: интернет, информационно-коммуникационные технологии, киберпреступления, кибербезопасность, нормативно-правовой акт, государственная стратегия, информационно-коммуникационная инфраструктура, конфиденциальность.

Мамырайым Ұлан
2 курс магистранты
Халықаралық бизнес университеті
Қазақстан Республикасы, Алматы

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ МЕН ЕУРОПАЛЫҚ ОДАҒЫНДА
КИБЕРҚЫЛМЫСТАРҒА ҚАРСЫЛЫҚ КӨРСЕТУДІҢ
НОРМАТИВТІК-ҚҰҚЫҚТЫҚ НЕГІЗІ**

Аңдатпа

Мақала Қазақстан Республикасы мен Еуропалық Одақтың киберқылмыстарға қарсы іс-қимыл жөніндегі нормативтік-құқықтық базасына шолу мен талдауға арналған. Автор киберқауіпсіздік саласындағы құқықтық қатынастарды реттейтін негізгі нормативтік-құқықтық құжаттардың мәні мен рөлін айқындады, сондай-ақ Қазақстан Республикасындағы киберқылмыстарға байланысты инциденттер бойынша ресми статистиканы көрсетті. Сондай-ақ, мақалада Еуропалық Одақта киберқауіпсіздікті қамтамасыз етуге байланысты ұлттықтан жоғары құқықтық деңгей ғана емес, сонымен бірге осы Одаққа қатысушы елдердің бірі ретінде Франция Республикасының мысалында ұлттық құқықтық деңгей де қарастырылған.

Түйінді сөздер: интернет, ақпараттық-коммуникациялық технологиялар, киберқылмыстар, киберқауіпсіздік, нормативтік-құқықтық акт, мемлекеттік стратегия, ақпараттық-коммуникациялық инфрақұрылым, құпиялылық.

Mamyraim Ulan
2nd year master's student
University of International Business
Republic of Kazakhstan, Almaty

**REGULATORY AND LEGAL FRAMEWORK FOR COUNTERING CYBER CRIMES
IN THE REPUBLIC OF KAZAKHSTAN AND EUROPEAN UNION**

Abstract

The article is devoted to the review and analysis of the regulatory framework of the Republic of Kazakhstan and the European Union on countering cybercrime. The author defines the significance and role of the main regulatory legal documents regulating legal relations in the field

of cybersecurity, and also provides official statistics on incidents related to cybercrime in the Republic of Kazakhstan. The article also examines not only the supranational legal level related to cybersecurity in the European Union, but also the national legal level on the example of the French Republic, as one of the member countries of this union.

Key words: internet, information and communication technologies, cybercrime, cybersecurity, regulatory legal act, state strategy, information and communication infrastructure, confidentiality.

За последние несколько десятилетий развитие Интернета привело к все большему вовлечению людей в киберпространство, что существенно повлияло на многие аспекты нашего общества. Повседневная жизнь, социальные взаимодействия граждан и экономика стали критически зависеть от бесперебойной работы информационно-коммуникационных технологий (далее – ИКТ). Постоянное нахождение в Сети стало новой нормой для многих людей, часто даже не осознавая этого. Это создало более широкие возможности для атак и открыло преступникам множество сфер жизни людей для их использования в корыстных целях. Киберпреступность стала одной из наиболее быстрорастущих форм преступности, представляющей серьезную угрозу пользователям киберпространства, экономике и национальной безопасности стран.

На текущий момент основными правовыми документами в Республике Казахстан (далее – РК) содержащими нормы, направленные на противодействие «киберпреступлениям», то есть «преступлениям в сфере информатизации и связи», то к таким можно отнести: 1) Уголовный кодекс Республики Казахстан от 3 июля 2014 года; 2) Кодекс Республики Казахстан «Об административных правонарушениях» от 5 июля 2014 года № 235-V ЗПК; 3) Закон Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан»; 4) Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»; 5) Закон Республики Казахстан «О государственных секретах» от 15 марта 1999 года N 349-1; 6) Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года N 94-V; 7) Постановление Правительства Республики Казахстан «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности» от 9 августа 2018 года; 8) Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» от 30 июня 2017 года № 407; 9) Постановление Правительства Республики Казахстан «Об утверждении Концепции

развития отрасли информационно-коммуникационных технологий и цифровой сферы» от 30 декабря 2021 года № 961.

Концепция Киберщит Казахстана [1] предусматривает реализацию комплекса правовых, научно-технических и организационных мер. Эта концепция направлена на прогнозирование, выявление, предотвращение и подавление любых угроз в области информационной безопасности. В нем описываются основные направления реализации государственной политики в области защиты электронных информационных ресурсов, информационных систем и телекоммуникационных сетей, обеспечения безопасного использования информационно-коммуникационных технологий. Этот документ обеспечивает единый подход к мониторингу правовой информационной безопасности государственных органов, физических и юридических лиц. Указан механизм предотвращения инцидентов информационной безопасности и оперативного реагирования на них, в том числе в чрезвычайных ситуациях социального, природного и техногенного характера, а также при введении чрезвычайного или военного положения. Кроме того, в данном документе был всесторонне изучен международный опыт формирования подходов к защите национальной информационно-коммуникационной инфраструктуры развитых государств.

Действующий Уголовный кодекс Республики Казахстан предусматривает отдельную главу 7 уголовных «правонарушении в сфере информационных коммуникаций» [2]. Данная глава предусматривает ответственность за умышленный незаконный доступ к охраняемой законом информации, содержащейся на электронных носителях в информационной системе или телекоммуникационной сети, который влечет за собой существенные нарушения прав и законных интересов граждан или организаций, или охраняемых законом интересов общества или государства. Также преднамеренное незаконное копирование или иной незаконный захват охраняемой законом информации, хранящейся на электронных носителях, содержащихся в информационной системе или передаваемых по телекоммуникационным сетям. Кроме того, статья 210 Уголовного кодекса Республики Казахстан предусматривает уголовную ответственность за создание, использование или распространение вредоносных компьютерных программ и программных продуктов.

Кодекс Республики Казахстан «Об административных правонарушениях» [3] также содержит ряд административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе для должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде на-

рушения требований по использованию электронных средства защиты информационных ресурсов. Несоблюдение единых требований, неисполнение или ненадлежащее внедрение владельцем или правообладателя информационных систем, содержащих персональные данные, мер по их защите.

А основными уполномоченными органами, занимающимися противодействием правонарушениям в сфере информатизации и связи, являются: Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан и Центр по борьбе с киберпреступностью департамента криминальной полиции Министерства Внутренних Дел РК.



Диаграмма 1. Статистика инцидентов с 2013 по 2023 годы в РК.

Из-за низкого процента зарегистрированных и расследованных киберпреступлений официальная статистика нерепрезентативна и трудно оценить фактическую распространенность киберпреступности. Но всё же согласно статистике инцидентов (Диаграмма 1), в сфере информатизации и связи РК службой реагирования на компьютерные инциденты KZ-CERT было зарегистрировано в 2013 году – 12443 инцидентов; в 2014 году – 15795 инцидентов; в 2015 году – 18375 инцидентов; в 2016 году – 22140 инцидентов; в 2017 году – 26817 инцидентов; в 2018 году – 20449 инцидентов; в 2019 году – 20808 инцидентов; в 2020 году – 24053 инцидентов; в 2021 году – 23773 инцидентов. А за прошедший 2022 год 18315 инцидентов из которых 10869 случаев это компьютерные вирусы, 2194 ботнеты, 1242 фишинг, 218 DdoS-атаки и 3792 остальных случаев. За начало 2023 года (за период с 01.01.2023-11.02.2023) было зарегистрировано уже 2103 подтверждённых случаев из которых 1653 это компьютерные вирусы, 133 ботнеты, 41 фишинг в интернете, 20 DdoS-

атаки и 256 остальных случаев. Но не стоит забывать, что это только зарегистрированные случаи, а незарегистрированных может быть ещё больше.

Из содержания сведений [4] предоставленной службой реагирования на компьютерные инциденты KZ-CERT за промежуток с 2013 по 2023 годы можно отметить, что большинство пользователей становятся жертвами той или иной формы киберпреступности, но наиболее распространёнными являются: 1) ботнеты 2) фишинг; 3) DDoS-атаки. В самые разные годы они занимают лидирующие позиции.

Поэтому не стоит забывать, что киберпреступность становится все более агрессивной и конфронтационной. Фишинг, фарминг и мошенническое неправомерное использование кредитных/дебетовых карт — это лишь некоторые из видов киберпреступлений, о которых должны знать пользователи. Поэтому не стоит забывать, что важной составляющей борьбы с преступлениями в сфере информатизации и напрямую влияющую на её эффективность является техническое просвещение граждан, государству необходимо проводить активную кампанию по повышению технической грамотности на пользовательском уровне среди рядовых граждан, особенно для граждан старше 35 лет. Например, советовать им часто менять свои пароли и использовать при составлении паролей сложные фразы, не посещать непроверенные сайты, использовать антивирусы на компьютерах, создавать резервные копии важной информации, блокировать незнакомых лиц в мессенджерах, устанавливать приложения из официальных магазинов приложений, отказываться от посещения пиратских сайтов, не пользоваться нелегальной продукцией и т.п. Всё это так же важно, как и правовая составляющая борьбы с преступлениями в сфере информатизации и связи.

Основными правовыми документами Европейского Союза (далее — ЕС) направленными на обеспечение кибербезопасности в странах-членах организации являются: 1) Конвенция о компьютерных преступлениях (ETS № 185) от 23 ноября 2001 года; 2) Директива 2016/1148 «О сетевой и информационной безопасности» от 6 июля 2016 года (далее - Директива NIS2) является важным законодательным актом ЕС в области кибербезопасности, и ее конкретная цель заключается в достижении высокого общего уровня кибербезопасности в государствах-членах; 3) Директива 2019/713 «О мошенничестве с безналичными платежами» от 17 апреля 2019 года; 4) Директива 2013/40 «Об атаках на информационные системы» от 12 августа 2013 г; 5) Директива 2011/93 «О борьбе с сексуальной эксплуатацией детей в Интернете и детской порнографии»

ей» от 13 декабря 2011 года; 6) Директива 2022/2555 «О мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза» от 14 декабря 2022 года.

Дополняют их соответствующие законодательные инициативы, такие как Директива о сетевой и информационной безопасности 2016 года и Директива «Оконфиденциальности и электронных коммуникациях» 2002 года [5], которая в настоящее время пересматривается для приведения ее в соответствие с требованиями Общего регламента по защите данных от 2016 года [6], а новое направление работы в настоящее время проводится в связи с необходимостью улучшения соблюдения законности в киберпространстве и получения электронных доказательств в уголовном процессе, включая трансграничный доступ к электронным доказательствам.

Конвенция о компьютерных преступлениях 2001 года [7] является первым международным договором о преступлениях, совершаемых через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерного мошенничества, детской порнографии и нарушений сетевой безопасности. Он также содержит ряд полномочий и процедур, таких как поиск в компьютерных сетях и перехват. Его основная цель, изложенная в преамбуле, заключается в проведении общей уголовной политики, направленной на защиту общества от киберпреступности, в частности путем принятия соответствующего законодательства и развития международного сотрудничества. Странами участниками данной конвенции, ратифицировавшими её, являются 68 государства (из них 41 государство не являются членами Совета Европы) и 2 государства всё ещё не ратифицировали её. Республика Казахстан не является её участником.

Действующая Директива NIS2 [8] ЕС касается мер по обеспечению высокого общего уровня безопасности сетевых и информационных систем на территории Союза с целью улучшения функционирования внутреннего рынка. С этой целью он обязывает государства-члены: 1) Принять национальную стратегию безопасности сетей и информационных систем и поручить выполнение задач, связанных с безопасностью сетей и информационных систем, национальным компетентным органам, единым контактными лицам и группам реагирования на инциденты компьютерной безопасности (CSIRT) для содействия быстрому и эффективному оперативному сотрудничеству; 2) Создать группу сотрудничества для поддержки и содействия стратегическому сотрудничеству и обмену информацией между государствами-членами; 3)

Установить требования безопасности и уведомления для операторов основных услуг и поставщиков цифровых услуг. Также предприятия, определенные государствами-членами как операторы основных услуг в вышеуказанных секторах, должны будут принять соответствующие меры безопасности и уведомить соответствующие национальные органы о серьезных инцидентах. Ключевые поставщики цифровых услуг, такие как поисковые системы, службы облачных вычислений и онлайн-рынки, должны будут соблюдать требования безопасности и уведомления в соответствии с Директивой.

Директива об атаках на информационные системы 2013 года [9] направлена на борьбу с крупномасштабными кибератаками, требуя от стран ЕС ужесточить национальные законы о киберпреступности и ввести более жесткие уголовные санкции.

Директива о борьбе с сексуальной эксплуатацией детей в Интернете и детской порнографией 2011 года [10] включает меры, которые лучше учитывают новые события в онлайн-среде, такие как груминг (преступники, выдающие себя за детей, чтобы заманить несовершеннолетних с целью сексуального насилия). Приняты ряд мер, включая создание специального подразделения по борьбе с детской порнографией в рамках правоохранительных служб государств-членов. Подразделение использует различные каналы сотрудничества полиции, в частности Интерпол, Европол и создает контактные пункты в государствах-членах для борьбы с киберпреступностью, которые работают 24 часа в сутки, а интернет-провайдеры обязаны хранить данные, связанные с трафиком, и должны создать свою собственную систему контроля.

В ЕС действует организация «Европейское агентство по сетевой и информационной безопасности» (далее – ENISA), деятельность которой основывается на Регламенте ЕС об ENISA и о сертификации кибербезопасности информационно-коммуникационных технологий 2019/881 [11]. Кроме своих основных функций, таких как, повышение надёжности продуктов, услуг и процессов ИКТ с помощью схем сертификации кибербезопасности, содействие последовательному внедрению соответствующей правовой базы, и т.д., данная организация также ежегодно выпускает отчёты «о состоянии ландшафта киберугроз», где определяются основные угрозы в сфере информатизации и связи, основные тенденции, наблюдаемые в отношении угроз, субъектов угроз и методов атак, а также анализ их воздействия и мотивации. В нем также описаны соответствующие меры по смягчению их последствий.

Но не стоит забывать, что Европейский Союз – это довольно слож-

ное экономическое и политическое объединение 27 европейских государств, то есть кроме наднационального правового уровня обеспечения безопасности от киберпреступлений, существует и уровень национального права государств-участников этой организации. Союз определяет условия, по которым государства-члены координируют свою политику, но всё же каждое государство имеет свою национальную нормативно-правовую базу для обеспечения кибербезопасности. Рассмотрим на примере Франции, одной из ведущих стран ЕС, она имеет свою национальную стратегию цифровой безопасности [12], которая была объявлена 16 октября 2015 года премьер-министром Франции Мануэлем Вальсом. Французское агентство безопасности информационных систем (далее – ANSSI), созданное в 2009 году, является национальным органом, отвечающим за кибербезопасность.

Законом о военном планировании № 2013-1168 от 19 декабря 2013 года установлено, что «премьер-министр проводит политику и осуществляет координацию действий правительства в области кибербезопасности и киберзащиты». Для этих целей созданы Национальное агентство кибербезопасности, Национальное агентство по безопасности информационных систем [13]. Закон о военном программировании, следовал принципам, изложенным в Белой книге по обороне и национальной безопасности 2013 года. Этот законодательный механизм позволил национальным операторам государственного и частного секторов, имеющим жизненно важное значение, лучше защитить себя, а ANSSI — и другим государственным органам — лучше поддержать их в случае кибератаки. Статья 22 Закона [14] предусматривала принятие мер по усилению безопасности жизненно важных операторов и предоставляла премьер-министру новые prerogatives.

А до этого в 2008 году президент Саркози решил, что Франции нужна Белая книга по обороне и национальной безопасности, в которой будет изложена угроза, стоящая перед страной, и определены возможности, необходимые для противостояния этой угрозе. В «Белой книге» 2008 года, принимая во внимание, что риск кибератаки на национальную инфраструктуру является одной из наиболее вероятных серьезных угроз в ближайшие пятнадцать лет, подчеркивается потенциально огромная опасность таких атак. Так как зависимость страны от ИКТ постоянно увеличивается с развитием информационного общества и все более широким использованием ИКТ в основных процессах государства и общества. В области киберзащиты в этой книге также подчеркнута необходимость в средствах раннего обнаружения кибератак, а также в орга-

низации, способной противостоять атакам, начиная от самых незаметных и заканчивая самыми далеко идущими. В области предотвращения указывалась необходимость в более широком использовании продуктов и сетей с высоким уровнем безопасности, а также создание резерва специалистов, обслуживающих жизненно важные государственные ведомства и операторов.

Одним из важных положительных особенностей европейского подхода в области кибербезопасности является последовательная и целенаправленная политика, направленная на нахождение баланса между национальной и наднациональной компетенциями. Общеευропейские структуры, как правило, не подменяют собой национальные ведомства, но являются координирующими центрами, предоставляют информационную, экспертную и техническую поддержку. [15].

Между Республикой Казахстан и Европейским Союзом необходимо развивать стратегические партнерские отношения, фокусирующиеся на более тесном сотрудничестве в области информатизации и связи. Эти отношения должны быть направлены на расширение взаимодействия в целях обеспечения безопасности граждан обеих сторон, обмена опытом и совместных усилий по повышению эффективности борьбы с киберпреступлениями.

С учетом динамичного развития технологий и цифровых преобразований в обществе, сотрудничество между Казахстаном и ЕС должно охватывать обмен передовыми практиками в области кибербезопасности и разработку совместных стратегий для защиты информационных ресурсов. Это включает в себя обмен технологическими решениями, методологиями анализа киберугроз, а также обучение и подготовку специалистов для эффективной борьбы с новыми вызовами в сфере киберпреступности.

Особое внимание следует уделять не только реактивным мерам по предотвращению кибератак, но и разработке превентивных стратегий, направленных на укрепление кибербезопасности на национальном и международном уровнях. Такое партнерство должно включать в себя регулярный обмен информацией о новейших угрозах, технологических трендах и лучших практиках в сфере кибербезопасности. Эти шаги содействуют не только защите интересов обеих сторон, но и создают благоприятные условия для развития цифровой экономики, обеспечивая устойчивость и безопасность в условиях всё более цифровизированного мира.

Список использованных источников:

1. Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности (“Киберщит Казахстана”)» от 30 июня 2017 года № 407;
2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V;
3. Кодекс Республики Казахстан «Об административных правонарушениях» от 5 июля 2014 года № 235-V ЗРК;
4. Статистика инцидентов в сфере информатизации и связи РК с официального интернет источника KZ-CERT Службы реагирования на компьютерные инциденты // <https://cert.gov.kz/>
5. Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. «Об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций» (Директива о конфиденциальности и электронных коммуникациях) [Электронный ресурс] // Режим доступа: URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>
6. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных» [Электронный ресурс] // Режим доступа: URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
7. Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года) [Электронный ресурс] // Режим доступа: URL: https://online.zakon.kz/Document/?doc_id=30170556
8. Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 г. о мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза, вносящая поправки в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972, и отменяющей Директиву (ЕС) 2016/1148 (Директива NIS 2) [Электронный ресурс] // Режим доступа: URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
9. Директива 2013/40/ЕС Европейского парламента и Совета от 12 августа 2013 г. об атаках на информационные системы [Электронный ресурс] // Режим доступа: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040>
10. Директива 2011/93/ЕС Европейского парламента и Совета от 13 декабря 2011 года о борьбе с сексуальным насилием и сексуальной эксплуатацией детей и детской порнографией [Электронный ре-

сурс] // Режим доступа: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093>

11. Регламент (ЕС) 2019/881 Европейского парламента и Совета от 17 апреля 2019 г. об ENISA (Агентстве Европейского союза по кибербезопасности) и о сертификации кибербезопасности информационно-коммуникационных технологий [Электронный ресурс] // Режим доступа: URL: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

12. Французская национальная стратегия цифровой безопасности [Электронный ресурс] // Режим доступа: URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

13. Научно-экспертное обеспечение деятельности парламента и развитие технологий его взаимодействия с гражданским обществом. Аналитическое управление аппарата совета федерации европейский центр парламентских исследований и документации, 2016 [Электронный ресурс] // Режим доступа: URL: <http://council.gov.ru/media/files/600jpf7P8wPg8Aq5lyEx97iiuQDKZWct.pdf>

14. Закон Французской Республики «О военном программировании» (Закон № 2013-1168) от 19 декабря 2013 года [Электронный ресурс] // Режим доступа: URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028338825>

15. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни, 2019 [Электронный ресурс] // Режим доступа: URL: <https://cyberleninka.ru/article/n/politika-obespecheniya-kiberbezopasnosti-v-evropeyskom-soyuze-natsionalnyy-i-nadnatsionalnyy-urovni>

УДК 349

Мекебаев А. А.

магистрант 1 курса Высшей школы права «Эділет»
научно-педагогического направления
Каспийского общественного университета,
Республика Казахстан, г. Алматы

**ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ
ЛИЧНОЙ ИНФОРМАЦИИ В СЕТИ**

Аннотация

В статье рассмотрены актуальные проблемы, связанные с конфиденциальностью личной информации в сети. С увеличением цифровизации общества и повсеместного использования интернета, вопросы защиты персональных данных становятся критически важными. Статья освещает современные тенденции сбора, хранения и обработки личной информации, выявляя уязвимости и риски, с которыми сталкиваются пользователи сети. Особое внимание уделяется анализу методов защиты данных и эффективности принятых правовых мер по обеспечению конфиденциальности в онлайн-среде. Работа также предоставляет рекомендации по усилению механизмов защиты личных данных и подчеркивает важность сбалансированного подхода к обеспечению безопасности и сохранению личной свободы в цифровой эпохе. В том числе опираясь на законы и предложения со стороны государства. В данной статье также приведены мои мысли и предложения.

Ключевые слова: интернет, сеть, интернет-платформа, ссылка, программа, вирус, вредоносное ПО, злоумышленник, недоброжелатель, хакер, антивирус.

Мекебаев А. А.

Каспий қоғамдық университетінің,
Ғылыми-педагогикалық бағытағы
«Әділет» Жоғары құқық мектебінің 1 курс магистранты
Қазақстан Республикасы, Алматы қ.

ЖЕЛІДЕГІ ЖЕКЕ АҚПАРАТТЫҢ ҚҰПИЯЛЫЛЫҚ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада желідегі жеке ақпараттың құпиялылығына қатысты өзекті мәселелер қарастырылады. Қоғамды цифрландырудың және интернетті кеңінен қолданудың артуымен дербес деректерді қорғау мәселелері аса маңызды болып отыр. Мақалада жеке ақпаратты жинау, сақтау және өңдеудің заманауи тенденциялары, желі қолданушыларының осалдықтары мен тәуекелдерін анықтау туралы айтылады. Деректерді қорғау әдістерін және онлайн-ортада құпиялылықты қамтамасыз ету бойынша қабылданған құқықтық шаралардың тиімділігін талдауға ерекше назар аударылады. Жұмыс сонымен қатар жеке деректерді қорғау тетіктерін күшейту бойынша ұсыныстар береді және цифрлық дәуірде қауіпсіздікті қамтамасыз ету мен жеке бас бостандығын сақтаудың

теңдестірілген тәсілінің маңыздылығын көрсетеді. Оның ішінде мемлекет тарапынан заңдар мен ұсыныстарға сүйене отырып. Бұл мақалада менің ойларым мен ұсыныстарым да берілген.

Түйінді сөздер: интернет, желі, интернет-платформа, сілтеме, бағдарлама, вирус, зиянды бағдарлама, қаскүнем, хакер, антивирус.

Мекебаев А. А.

1st year undergraduate student of the «Adilet» Higher School of Law
Scientific and pedagogical direction
Caspian Public University,
Republic of Kazakhstan, Almaty

PRIVACY ISSUES OF PERSONAL INFORMATION ON THE WEB

Annotation

The article discusses current issues related to the confidentiality of personal information on the web. With the increasing digitalization of society and the widespread use of the Internet, personal data protection issues are becoming critically important. The article highlights current trends in the collection, storage and processing of personal information, identifying vulnerabilities and risks faced by network users. Particular attention is paid to the analysis of data protection methods and the effectiveness of legal measures taken to ensure confidentiality in the online environment. The work also provides recommendations on strengthening personal data protection mechanisms and highlights the importance of a balanced approach to ensuring security and preserving personal freedom in the digital age. Including relying on laws and proposals from the state. This article also contains my thoughts and suggestions.

Keywords: Internet, network, Internet platform, link, program, virus, malware, attacker, detractor, hacker, antivirus.

*“Кто владеет информацией – тот владеет миром”
Натан Родшильд*

Недаром данный афоризм стал легендарным, ведь именно благодаря владению информацией раньше других сделало семью Родшильдов вне конкуренции на рынке бирж.

Однако не стоит относить это выражение только к случаям победы в конкуренции за славой и богатством во благо. К сожалению, не только

великие люди, но и корыстные недоброжелатели способны овладеть информацией для своих тёмных целей.

Некогда информация хранилась на бумажных носителях, что позволяло опытным ворами красть её без особых препятствий. Но в эру технологий всё иначе, на сегодняшний день у каждого человека есть своё личное хранилище на просторах интернета. Благодаря цифровым носителям, выкрасть информацию стало намного сложнее. Люди ставят несколько уровней защиты в виде различных паролей, диаграмм, схем и отпечатков пальцев. Есть даже особо сложные типы защиты в виде сканера лица и глазных сетчаток.

Тем не менее, ремесло воровства тоже не стояло на месте и тоже регулярно улучшалось. В современном мире, людей что способны получить доступ к конфиденциальной информации путём взлома систем защиты называют «хакерами», что в переводе с немецкого языка обозначает «подцеплять, подсекать» - то есть тот, кто проникает в чужие базы данных.[1]

Во всём мире люди хранят свои личные данные в сети интернета, такие как банковские реквизиты, пароли от важных хранилищ, адреса, номера телефона, почту, документы, фото и видео, записи аудио и даже деньги.

Развитие технологий значительно облегчило жизнь людям, дав им возможность хранить практически всё в сети интернета. Однако, как оказалось это не совсем безопасно. Всё больше людей сталкиваются с мошенниками и ворами в интернете, злоумышленники притворяются сотрудниками банка, службой поддержки, родными и близкими жертвы. Также бывают случаи, когда злоумышленник не скрывает свою истинную натуру и напрямую заявляет о своих требованиях жертве, пригрозив ему тем, что сольёт в общий доступ личные данные жертвы (фото, видео, пароли и т.д.).

Но не всегда обязательно то, что хакер свяжется с жертвой напрямую. Особо опытные взломщики, не подавая виду могут получить доступ к данным и не оставив следов своего пребывания завладеть личной информацией человека. К сожалению, в таких случаях сложно что-либо предпринять.

К примеру, на каких-то сайтах и форумах, где человек имеет свой аккаунт и хранилище, есть собственная система защиты в виде шифрования. Многие официальные сайты стараются уберечь своих пользователей от злоумышленников. Некоторые даже просят подписать электронное соглашение о конфиденциальности, дабы как можно сильнее

внушить уверенность в сохранности своих данных пользователям своей интернет-платформы.

Но есть и сайты, модераторами которых являются сами злоумышленники. Они выдают себя за официальные сайты, которые прошли проверку безопасности и которым можно доверять. Как только пользователь авторизуется в подобных сайтах, у него на устройстве появляются многочисленные вирусы и вредоносные программы. Подобным образом недоброжелатели замораживают работу устройства пользователя, тем самым выигрывая себе время для получения доступа и скачивания данных жертвы.

Существуют так называемые вредоносные ПО, которые заражают устройство и атакуют защиту данных, тем самым получая доступ к личной информации пользователя (банковские реквизиты, персональные данные, доступ к вычислительным ресурсам и т.д.).

Вредоносное ПО — это приложения или код, которые препятствуют нормальному использованию конечных устройств. Когда устройство заражено вредоносным ПО, пользователи могут столкнуться с несанкционированным доступом, компрометацией данных или блокировкой и требованием заплатить выкуп. [2]

Для защиты от вредоносного ПО и вирусов, пользователям приходится устанавливать на своё устройство разные антивирусные программы и настройки. Благодаря высокому спросу, на рынке появилось много предложений от различных разработчиков. Такие программы гарантируют безопасность использования и сохранность данных. Но по-настоящему действенных антивирусов мало, так как многие из них создаются как раз таки злоумышленниками, и под ликом антивируса может скрываться куда более серьёзное вредоносное ПО. Такого рода вирусы называются «Троянами», что символизирует знаменитого Троянского коня.

Во избежание проблем с устройством, которые могут привести к утечке информации, рекомендуется устанавливать только прошедшие проверку, и получившие лицензию антивирусы, которые можно купить на официальных сайтах известных издателей. (ктакимотносятсяBitdefender, Kaspersky, Norton, McAfee, Avast, Avira, Windows Defender, Trend Micro, TotalAV, AVG ит.д.).

Преимуществами таких антивирусных программ являются:

- Обнаружение и блокировка вредоносных программ;
- Эффективное реагирование не только на уже известные, но и на новые угрозы;

- Предоставление средств предотвращения новых атак;
- Проверка и регулярное обновление баз данных и системы устройства;
- Низкое воздействие на производительность устройства;
- Защита от сетевых угроз;
- И что не мало важно удобство использования и понятный интерфейс.

Многие люди ошибочно доверяют бесплатным антивирусным программам из сомнительных сайтов и непроверенных издателей. Но порой даже в официальных интернет-магазинах прослеживаются вирусные программы. Поэтому приоритетнее покупать такие программы напрямую от издателя, на его официальном сайте.

Правонарушения такого характера регулируются главой 7 Уголовного кодекса Республики Казахстан «О доступе к информации».[3]

Стоит отметить, что подобным атакам подвергаются не только простые граждане, но и государственные базы данных. Как правило, большое количество информации почти о каждом гражданине страны хранятся в государственных электронных базах данных. Поэтому государство очень тщательно подходит к вопросу безопасности личной информации граждан. Государство контролирует в определённой мере оборот информации в сети. Оно проверяет сайты на безопасность и решает на сколько безопасно таким ссылкам давать доступ к своему интернет-пространству. Есть определённые сайты, которые государство блокирует и посещение которых ограничивает ввиду различных проблем, которые эти сайты могут вызвать.

Но не стоит думать, что проблемы утечки личной информации грозит только на сайтах. Интернет – это, очень обширное пространство, нити которого расстилаются далеко за границы одного государства, потому что это всемирная сеть, где хранятся данные миллионов человек на миллиардах разных интернет-платформах. Данное определение сформулировано мной, она отражает моё понимание этого термина и его свойств.

Как было сказано выше, сайты не единственное место, где пользователи подвергаются риску утечки информации. Также, в приложениях, социальных сетях, интернет-магазинах и онлайн банкингах тоже присутствует определённый риск. Никто не может стопроцентно гарантировать безопасность сохранности личных данных пользователей. И даже электронные соглашения о конфиденциальности, «галочки» доказывающие официальный статус и наличие многоуровневой защиты не способны дать подобную гарантию.

К примеру, в ноябре 2023 года стала известна новость о том, что 37-ми летний мужчина оформлял автокредиты в одном из банков Казахстана на несуществующие автомобили. Как оказалось, в марте 2022 года мужчина узнал от знакомого что один из банков Казахстана запустил программу «Цифровое автокредитование». В следствие чего, мужчина вместе с своим приятелем решили воспользоваться вышеупомянутой программой для незаконных заработков.

Чтобы осуществить задуманное, злоумышленники загружали в банковское приложение данные несуществующих машин и находили на них подставных покупателей. Так как банк предоставлял услуги онлайн, киберпреступники смогли загрузить туда ложные данные несуществующих машин и людей. Таким образом, мужчина смог выручить из банка довольно большую сумму денег продавая несуществующие автомобили, при этом долгое время ему удавалось остаться безнаказанным. К счастью, мужчину в итоге поймали и своими действиями он не причинил ущерба физическим лицам, однако таким хитрым способом ему удалось обойти ограничения и защиту банка, что в последствии повлекло утечку денежных средств банка, которые хранились в специальном цифровом хранилище. [4]

Также как и онлайн банкинг тайна личной переписки ничуть не застрахована от недоброжелателей. Не смотря, на то, что это карается статьей 148 Уголовного Кодекса Республики Казахстан, такие правонарушения весьма не редкость. [5]

Зачастую тайну переписки нарушают сами участники этой переписки. За незнанием закона, моральных ценностей или иным корыстным причинам, люди распространяют личную переписку третьим лицам, сторонним организациям и всем тем, кому не следовало об этом знать.

Разглашение тайны личной переписки не всегда имеет корыстный посыл. Нередко пользователи социальных сетей выкладывают фрагменты переписки как свои, так и чужие в виде скриншотов или записей экрана в истории или коротких видео социальных платформ. Характер этих действий обычно шуточный и безобидный.

Однако, вне зависимости от того, какой характер и посыл несут в себе эти действия, они являются уголовными правонарушениями против конституционных и иных прав и свобод человека и гражданина. Они регулируются статьей 148 Уголовного Кодекса Республики Казахстан. [5]

Тем не менее, разглашение тайны личной переписки возможна и по вине платформы, на которой велась эта самая переписка. Иногда из-за технических неполадок, иногда из-за слабой защиты, а порой и благодаря искусному мастерству взлома хакера.

На случаи злоумышленного взлома, у опытных компаний всегда есть свои хакеры, которые тоже занимаются взломом программ. Но стоит отметить, что такие хакеры называются «белыми» и не имеют никакого отношения к киберпреступникам. Наоборот, белые хакеры нужны для того, чтобы пробовать взломать программы всеми возможными способами и путями. Это помогает выявить слабые стороны защиты и усовершенствовать её.

Белый хакер – это, специалист по кибербезопасности, который находит и устраняет уязвимости систем и ресурсов компании.[6]

Они проводят своего рода тест-драйв, который занимает много времени и ресурсов, но значительно повышает эффективность защиты и уровень безопасности.

Основная деятельность и функции белых хакеров:

- Тестирование на проникновение (как было ранее сказано, пробают взломать систему безопасности самостоятельно для выявления слабостей в защите);

- Защита от кибератак (разработка системы безопасности на основе заранее выявленных уязвимостей);

- Развитие новых технологий безопасности (поиск и разработка новых методов защиты с целью опередить злоумышленников);

- Улучшение общей культуры безопасности, обучение и обновление персонала (белые хакеры внедряют общие принципы безопасности в культуру организации и могут обучать персонал организации своим методам работы для выявления подозрительной деятельности);

- Минимизация потерь репутационного ущерба (предотвращение потери данных и снижение репутационного риска).

К сожалению, не все могут позволить себе услуги белых хакеров ввиду трудоёмкости работы, подобных специалистов мало и их услуги крайне востребованы.

Для того, чтобы улучшить эффективность защиты и повысить уровень безопасности, многие сайты и интернет-платформы покупают уже готовую систему безопасности.

Такие системы хороши тем, что они уже готовы, то есть нет необходимости ждать, когда её создадут, однако в этом есть и свои минусы. К примеру то, что готовые системы безопасности не всегда подходят всем сайтам, ведь у каждого сайта есть своя особенность. Под такие сайты обычно создают специальные системы безопасности.

Главными преимуществами систем безопасности являются:

- Защита от большинства известных и менее известных вредоносных ПО и вирусов;

- Проверка всех входящих и исходящих файлов и ссылок на наличие вирусных программ;
- Подготовка защиты устройства к различным видам кибератак;
- Блокировка небезопасного контента;
- Блокировка доступа к сомнительным ссылкам и файлам;
- Предоставление возможности пользователю самостоятельно убедиться в безопасности файлов и ссылок;
- А также автоматический фильтр всех небезопасных программ.

Стоит упомянуть, что в сентябре 2023 года, Депутаты мажилиса Республики Казахстан рассмотрели в первом чтении проект закона о внесении изменений и дополнений в некоторые законодательные акты по вопросам информационной безопасности. [7]

Целью законопроекта является обеспечение безопасности информационных систем и личных данных в системе электронного правительства. В отдельном блоке законопроекта даже предлагалось введение института белых хакеров, для правового регулирования и выявления ошибок в системе.[7]

30 ноября 2023 года закон был одобрен Сенатом Республики Казахстан, а 11 декабря 2023 года, Президент Касым-Жомарт Токаев подписал данный закон и ввёл регулирующий институт белых хакеров.[8]

Также, касательно данного блока закона мажилисмен Екатерина Смышляева дала следующее пояснение: «Управляемый хакерский взлом исходит от заказчиков, отношения официально устанавливаются через специальные платформы. Таким образом, мы привлекаем большое количество квалифицированных специалистов по информационной безопасности для оценки устойчивости систем».

Хотелось бы отметить, что в данном законе речь идёт пока только о государственных системах, я же в свою очередь хочу, чтобы работа белых хакеров не ограничивалась лишь государственными системами и интернет-платформами.

Добавлю, что принятие такого закона для меня стала приятной новостью, ведь в данной статье я хотел отметить свои мысли на этот счёт и порекомендовать нашему государству формирование чего-то похожего, создание специального органа или команды белых хакеров, которые бы занимались усовершенствованием систем безопасности в сети. Но оказалось, что мечты сбываются самым неожиданным образом и я крайне благодарен нашему государству, за столь быстрое реагирование на проблемы защиты конфиденциальности информации в сети.

Конечно, как уже говорилось не раз, нет стопроцентно действенной защиты. Современные технологии всё ещё на стадии совершенствова-

ния. На пути к совершенству, были придуманы искусственные интеллекты (далее - ИИ).

Современные программисты и специалисты в сфере Информационных технологий (далее - ИТ) всё больше внимания уделяют ИИ и пытаются его применить в самых различных сферах жизни. Сфера защиты данных тоже подверглась влиянию ИИ. Хотелось бы рассказать немного о применении ИИ в защите данных в сети интернет.

ИИ может использоваться для анализа нормального поведения пользователей и систем в сети. Когда происходит аномалия, например, необычные запросы к базе данных или активность в непривычное время, система может сработать тревожный сигнал и предпринять меры по предотвращению инцидента.

Также, алгоритмы машинного обучения могут анализировать текущие тренды в кибер-угрозах и использоваться для прогнозирования будущих угроз. Это позволяет компаниям принимать проактивные меры по усилению защиты перед тем, как угрозы станут широко распространенными.

Ещё одним преимуществом ИИ перед человеком или антивирусной программой состоит в том, что он может автоматизировать реагирование на кибератаки. Что включает в себя быстрое обнаружение проблем, блокировку угрозы и восстановление системы до нормального состояния.

С использованием ИИ можно внедрять более сложные системы аутентификации, такие как биометрическое распознавание, анализ поведенческих паттернов и другие инновационные методы, чтобы обеспечить высокий уровень безопасности доступа к данным.

Модели машинного обучения могут анализировать большие объемы данных для выявления угроз и разработки эффективных стратегий защиты. Такие системы способны улучшать свою эффективность по мере обучения на новых данных о кибер-угрозах.

На сегодняшний день, развитие ИИ продвинулось в значительной степени, потенциал данной отрасли науки подаёт большие надежды.

В заключение добавлю, что основной проблемой безопасности всех хранилищ в сети является то, что они общедоступны. То есть, если злоумышленник высококвалифицированный программист и очень хорошо разбирается в технологиях, то ему не составит особого труда определить слабые места защиты цифровых носителей и нанести свой удар. Современные технологии очень плотно закрепились в жизни многих людей, представить жизнь без них уже сложно. Они дали уйму возможностей и сделали обмен информацией удобным. Но удобство не всегда

эквивалентно безопасности. Увы, но современные технологии слишком не доработаны, они представляют из себя крайне хрупкую оболочку, которую сломать легче чем починить.

Кроме того, можно подчеркнуть важность применения современных технологий безопасности, включая искусственный интеллект, для устранения уязвимостей и повышения степени защиты цифровых хранилищ. Эффективное использование ИИ в области безопасности может существенно снизить риски утечек и потери данных. Необходимость обеспечения безопасности данных становится особенно актуальной, учитывая общедоступность хранилищ в сети. Развитие продвинутых систем защиты, внедрение многоуровневых мер безопасности и постоянное обновление методов становятся ключевыми шагами в предотвращении кибер-угроз.

Одновременно с этим, подчеркнем, что безопасность должна рассматриваться как интегральная часть развития современных технологий. Безопасность и удобство использования технологий должны сбалансированно сосуществовать, и применение передовых методов защиты данных является важным шагом в этом направлении. В конечном итоге, повышение безопасности цифровых хранилищ содействует сохранению доверия к современным технологиям и обеспечивает устойчивость в цифровой среде.

Список использованных источников:

1. Словарь иностранных слов русского языка - <https://dic.academic.ru/>
2. Официальный сайт Microsoft - Что такое вредоносная программа? Определение и типы | Microsoft Security;
3. Глава 7 Уголовного кодекса Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.) и Законом Республики Казахстан «О доступе к информации» от 16 ноября 2015 года № 401-V.
4. Центр Журналистских Расследований - Как «Фридом Финанс» выдал 157 млн тенге под авто, которых не было (czhr.kz);
5. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.);
6. Skillfactory - Карьерный гид «Профессия «Белый» хакер»: кто такой хакер и как им стать (skillfactory.ru);
7. TengriNews - Информационные системы Казахстана будут атаковать "белые хакеры": 27 сентября 2023, 11:24 - новости на Tengrinews.kz;

8. TengriNews - Сбор копий удостоверений личности, "белые хаке-ры": Токаев подписал закон: Вчера, 18:10 - новости на Tengrinews.kz

ӘОЖ 343.24:343.8(345)

Нусубалиева Макпал Ерболовна
«Қайнар» академиясының магистранты
Қазақстан Республикасы, Алматы қ.

ПРОЦЕСТІК КЕЛІСІМ ТҮСІНІГІ, ЖАСАСУДЫҢ ШАРТТАРЫ

Аңдатпа

Мақалада процестік келісім түсінігі, жасасудың шарттарының кейбір мәселелері қарастырылған. Автор процессуалдық келісім институтын заңнамалық дамыту процесіне назар аударады. Сонымен қатар ҚПК-нің 67 және 68-баптарын қолдану кезінде алынатын сотталушы үшін артықшылықтарды салыстырып, процестік келісім жасасуға қатысты өз ұсыныстарын енгізеді.

Түйінді сөздер: процестік келісім, қылмыстық процестік кодекс, қылмыстар, қылмыстық теріс қылық, азаматтық талап, кінәні мойындау.

Нусубалиева Макпал Ерболовна
Магистрант академии «Қайнар»
Республика Қазақстан, г. Алматы

ПОНЯТИЕ ПРОЦЕССУАЛЬНОГО СОГЛАШЕНИЯ, УСЛОВИЯ ЗАКЛЮЧЕНИЯ

Аннотация

В статье рассмотрены понятие процессуального соглашения, некоторые вопросы условий его заключения. Автор обращает внимание на процесс законодательного развития института процессуального соглашения. При этом он сравнивает выгоды для подсудимого при применении статей 67 и 68 УПК и дает свои рекомендации по заключению процессуального соглашения.

Ключевые слова: процессуальное соглашение, Уголовно-процессуальный кодекс, преступления, уголовный проступок, гражданский иск, признание вины.

Nusubalieva M.

Master's student at the Kainar Academy
Republic of Kazakhstan, Almaty

THE CONCEPT OF A PROCEDURAL AGREEMENT, CONDITIONS OF CONCLUSION

Annotation

The article discusses the concept of a procedural agreement and some issues of the conditions for its conclusion. The author draws attention to the process of legislative development of the institution of procedural agreement. At the same time, he compares the benefits for the defendant when applying Articles 67 and 68 of the Code of Criminal Procedure and gives his recommendations for concluding a procedural agreement.

Key words: procedural agreement, Criminal Procedure Code, crimes, criminal offense, civil claim, admission of guilt.

Қазақстан Республикасының 2010 жылдан 2020 жылға дейінгі кезеңге арналған құқықтық саясат тұжырымдамасы туралы Қазақстан Республикасы Президентінің 2009 жылғы 24 тамыздағы № 858 Жарлығында процессуалдық келісім институтын заңнамалық дамыту керек делінген [1].

ҚР ҚПК-нің 7-бабының 37-тармағына сәйкес, процестік келісім — бұл қылмыстық процестің кез келген сатысында прокурор мен күдікті, айыпталушы немесе сотталушы немесе сотталған адам арасында ҚПК көзделген тәртіппен және негіздер бойынша жасалатын келісім [2].

Жасалған процестік келісім шеңберінде қылмыстық істерді тергеп-тексеру мынадай: онша ауыр емес, ауырлығы орташа не ауыр қылмыстар бойынша – күдікті, айыпталушы келтірілген күдікпен, айыптаумен келіскен жағдайда – кінәні мойындау туралы мәміле нысанында; қылмыстық топ жасаған қылмыстарды, өзге де адамдар жасаған аса ауыр қылмыстарды, сондай-ақ экстремистік және террористік қылмыстарды ашуға және тергеп-тексеруге ықпал ету кезінде барлық санаттағы қылмыстар бойынша – ынтымақтастық туралы келісім нысанында; Қазақстан Республикасының Қылмыстық кодексінде көзделген онша ауыр емес, ауырлығы орташа не ауыр қылмыстар бойынша кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы келісім нысанында жүргізіледі. Процестік келісімді қылмыстық заңда тыйым салынған іс-әрекетті есі дұрыс емес күйде жасаған немесе қылмыс жасағаннан кейін психикасының бұзылумен ауырған

адамдармен жасауға болмайды. Процестік келісім жасасу адамды жәбірленуші және азаматтық талапкер болып танылған адамдардың алдында азаматтық-құқықтық жауаптылықтан босатуға негіз болып табылмайды.

Соттардың қылмыстық істер бойынша келісімдік тәртіпте іс жүргізу практикасы туралы Қазақстан Республикасы Жоғарғы Сотының 2016 жылғы 7 шілдедегі № 4 Нормативтік қаулысына сәйкес, Қылмыстық теріс қылықтар туралы істер бойынша кінәні мойындау туралы келісім жасасу заңда көзделмеген. Адам қылмыстық теріс қылық және кінәні мойындау туралы келісім жасалатын қылмыс жасаған кезде, сотқа дейінгі тергеп-тексеру органы олар бойынша істерді біріктірмеуі тиіс, өйткені қылмыстық теріс қылық туралы іс бойынша сотқа дейінгі іс жүргізу хаттамалық нысанда, ал қылмыс туралы іс бойынша іс жүргізу процестік келісім шеңберінде ҚПК-нің 63-тарауында көзделген қағидаларға сәйкес жүзеге асырылады. Адам қылмыстық теріс қылық және кінәні мойындау туралы келісімге қол жеткізілмеген және жасалмаған қылмыс жасаған кезде, олар бойынша қылмыстық істер ҚПК-нің 526-бабының төртінші бөлігіне сәйкес анықтау не алдын ала тергеу нысанында бірыңғай іс жүргізу үшін біріктірілуі мүмкін [3].

Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗаңына сәйкес, Процестік келісімнің барлық талаптарын орындаған адам қылмыстық жауаптылықтан босатылуы мүмкін. Осы баптың бірінші бөлігінің ережесі, кәмелетке толмағандардың жыныстық тиіспеушілігіне қарсы қылмысты он төрттен он сегізге дейінгі жастағы кәмелетке толмаған адамға қатысты кәмелетке толмаған жасаған жағдайларды қоспағанда, мұндай қылмыс жасаған адамдарға қолданылмайды.

Қылмыстық кодекстің 67-1-бабына сәйкес, кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісімнің шарттарын орындаған кезде қылмыстық жауаптылықтан босату болып кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісімнің барлық шарттарын орындаған тұлға қылмыстық жауаптылықтан босатылуы мүмкін [4].

Кінәні мойындау туралы мәміле нысанындағы процестік келісім мынадай шарттар болған: күдікті, айыпталушы процестік келісім жасасуға ерікті түрде ниет білдірген; күдікті, айыпталушы келтірілген күдікке, айыптауға және іс бойынша қылмысты жасағанына қолда бар дәлелдемелерге, өзі келтірген зиянның сипаты мен мөлшеріне

дауласпаған; жәбірленуші іске қатысқан жағдайда, ол процестік келісім жасасуға келіскен кезде жасалуы мүмкін.

Кінәні мойындау туралы мәміле нысанындағы процестік келісім: қылмыстардың жиынтығына қатысты, егер олардың ең болмағанда біреуі ҚПК осы бабында және 612-бабында көзделген талаптарға сәйкес келмесе; егер жәбірленушілердің ең болмағанда біреуі процестік келісім жасасуға келіспесе, жасала алмайды [2].

Кінәні мойындау туралы мәміле нысанындағы процестік келісімді жасасудың салдарлары мыналар болып табылады: ҚПК 192 бабында белгіленген мерзімдерде сотқа дейінгі тергеп-тексеруді аяқтау; кінәні мойындау туралы процестік келісім сотқа берілген барлық күдіктілермен, айыпталушылармен не сотталушылармен жасалмаған, сыбайласып жасалған қылмыстар туралы қылмыстық істерді қоспағанда, ҚПК 382-бабының екінші бөлігіне және 64-тарауына сәйкес кінәні мойындау туралы мәміле нысанындағы істі сотта талқылау; процестік келісім жасасуға келісім берген жәбірленушіні залалды өтеу мөлшері туралы талапты одан әрі өзгерту құқығынан айыру.

Мысалы, 2022 жылдың 8 қазанында М.Нұрбақыт Алматы қаласы, Әуезов ауданы, 8 ықшам ауданы, №1-үй, 12 пәтерде танысы А.Камалмен кезігіп, ортақ проект жұмыстарын жасаған. Осы кезде М.Нұрбақыт өз кезегінде өзінің пайдақорлық ниетімен бөтенің мүлкін жымқыру немесе алдау немесе сенімді теріс пайдалану жолымен бөтен мүлікке құқықты иемдену ойына келіп, өзінің қылмыстық ойын ақырына дейін жеткізу мақсатында, А.Камалдың «Aser Nitro 5» маркалы ноутбүгін бір күнге жұмыстарын бітіріп алуға алдап сұрап алып, 2022 жылы 9 қазанда 450 000 теңге тұратын аталған ноутбүгін Әуезов ауданы, Аксай-2 ықшам ауданында орналасқан «Mini Credit» комиссияндық ломбардына өткізіп жіберіп, сеніміне қиянат жасап, алаяқтық жолмен А.Камалдың 450 000 теңгесінің затын заңсыз иеленіп алып, өзінің бас пайдасына жаратқан.

Басты сот талқылауы барысында Алматы қаласы Әуезов ауданының прокуроры С.Өтемұратов пен сотталушы М.Нұрбақыттың арасында кінәні мойындау туралы мәміле нысанында процестік келісім жасалған. Сотталушы М.Нұрбақытпен жасалған процестік келісімнің мәні оның ерік білдіруіне сәйкес болғандықтан қолдайтынын көрсеткен. Прокурор мен сотталушының қорғаушысы сот отырысында процестік келісімді қолдады. Сонымен сот анықтады процестік келісім тараптар: прокурор, жәбірленуші, сотталушы мен оның қорғаушысының ерік білдіруіне сәйкес екенін. Кінәні мойындау туралы мәміле нысанында процестік келісім жасау тәртібі сақталған. Жәбірленуші А.Камалдан процестік келісім жасауға

келісімі алынған. Кінәні мойындау туралы мәміле нысанындағы процестік келісімді жасасудың салдарлары, яғни қылмыстық іс келісімдік іс жүргізу тәртібінде, дәлелдемелерді зертемей аяқталатыны, процестік келісім жасасуға келісім берген жәбірленушіні залалды өтеу мөлшері туралы талапты одан әрі өзгерту құқығынан айырылатыны тараптарға түсіндірілген және оларға түсінікті. Тараптар арасында жасалған процестік келісім Қазақстан Республикасының Қылмыстық-процестік кодексінің 616-бабының талаптарына сәйкес. Сотталушы М.Нұрбақыттың қылмыстық құқық бұзушылық ісәрекеттері сотпен ҚК-нің 190-бабы бірінші бөлігімен дәрежеленеді, өйткені ол алаяқтық, яғни бөтенің мүлкін жымқыру немесе алдау немесе сенімді теріс пайдалану жолымен бөтен мүлікке құқықты иемденуді жасаған. М.Нұрбақытпен қасақана жасалған ісәрекеттер ҚК-нің 11-бабының екінші бөлігіне сәйкес онша ауыр емес қылмыстар деп танылады. М.Нұрбақытқа жаза түрі мен мерзімін тағайындау мәселесін қарастырғанда сот келесіге келді. Шын ниетпен өкінгені, қылмыстық құқық бұзушылық салдарынан келтірілген мүліктік залалды ерікті түрде өтеуі М.Нұрбақыттың қылмыстық жауаптылық пен жазасын жеңілдететін мән-жайлар деп сот таниды. Сотталушының қылмыстық жауаптылық пен жазасын ауырлататын мән-жайлар іс материалдарынан сотпен анықталмаған. Сот жаза тағайындағанда ҚК-нің 52-бабының талаптарын, оның ішінде М.Нұрбақыттың жеке басына берілген мәліметтерге, жауаптылық пен жазаны жеңілдететін мән-жайлардың барын, ал оларды ауырлататын мән-жайлардың жоқтығын, сондай-ақ тағайындалған жазаның сотталған адамның түзелуіне және оның отбасы мен асырауындағы адамдардың тіршілік жағдайына ықпалын, жәбірленушінің кешірім беріп жеңіл жаза тағайындауды сұраған көз қарасын, сол сияқты ҚК-нің 190-бабының бірінші бөлігінде бас бостандығынан айырудан гөрі онша қатаң емес жазаның негізгі түрі көзделгенін ескеріп, сот тараптардың процестік келісімде айтылған жаза түрі мен мерзімімен келіседі. Жаза түрі мен мерзімін анықтаған кезде тараптар ҚК-нің 44-бабының, сол сияқты ҚК-нің 55-бабының үшінші бөлігінің талаптарын сақтаған. М.Нұрбақыттың тұрақты жұмыс орны жоқ және оқуда жоқ болғандықтан ҚК-нің 44-бабы бірінші бөлігіне сәйкес жазаны өтеудің бүкіл мерзімі ішінде жыл сайын бір жүз сағаттан мәжбүрлі еңбекке тартылуға жатады. Мүлікті тәркілеу қосымша жаза тағайындау мүмкін емес, себебі сотталушының меншігіндегі, сондай-ақ қылмыстық құқық бұзушылық жасау қаруы немесе құралы болып табылатын мүлік анықталмағандықтан. М.Нұрбақыттың сотқа дейінгі іс жүргізу және сот талқылауы барысында «сотқа келуге міндеттеме» түріндегі өзгеде

процестік мәжбүрлеу шарасы жойылуға жатады. Іс бойынша заттай дәлелдемелер танылмаған [5].

Сот шешім қабылдау үшін кеңесу бөлмесіне кеткенге дейін күдіктінің, айыпталушының процестік келісімнен бас тартуға құқығы бар. Процестік келісім жәбірленушіні және азаматтық талапкерді осы қылмыстық істе немесе азаматтық сот ісін жүргізу тәртібімен азаматтық талап қою құқығынан айырмайды. Тараптардың процестік келісім жасасудан бас тартуы оны қайтадан жасасу туралы өтінішхат мәлімдеуге кедергі келтірмейді.

Кінәні мойындау туралы мәміле нысанында процестік келісім жасасу туралы өтінішхатты қарау тәртібі: күдікті, айыпталушы, сотталушы қылмыстық іс бойынша іс жүргізудің кез келген сәтінде сот кеңесу бөлмесіне кеткенге дейін мәміле нысанында кінәні мойындау туралы процестік келісім жасасу туралы өтініш мәлімдеуге құқылы. Процестік келісім прокурордың бастамасы бойынша жасалуы мүмкін [2].

Д.К.Канафин пікірінше, қылмыстық сот ісін жүргізудің әділдігін қамтамасыз ету мақсатында заңда қарастыру қажет деп санаймыз:

- ҚПК-нің 29-бабының сот ісін жүргізудің жариялылығы туралы ережелерін бұзатын рәсімдерді қолданбай, бас сот талқылауы барысында іс жүргізу келісімінің шарттарын орындау;

- егер мұндай келісім процестің сотқа дейінгі сатысында жасалмаса, күдіктінің, айыпталушының іс жүргізу келісімін жасасу әрекеттеріне қатысты құжаттарды іс материалдарынан міндетті түрде алып тастау;

- іс жүргізу келісімі жасалатын істер бойынша сотқа дейінгі іс жүргізудің жалпы практика істеріне қарағанда нақты, неғұрлым қысқа мерзімдерін көздеу;

- айыпталушының өзіне қарсы айғақ беретін куәгерлерден айқас жауап алу құқығын шектеу практикасын алып тастау;

- келісім жасасу туралы өтінішхатпен жүгінген адамға оның кінәсінің кейбір дәлелдерімен, оның ішінде куәгерлердің, жәбірленушілердің, оны қылмыс жасады деп айыптаған процеске өзге де қатысушылардың айғақтарымен танысу құқығын беру, оған аталған адамдардан айқас жауап алу құқығын беру;

- егер бөлінген іс бойынша шешім басқа айыпталушыларға қатысты преюдициялық мәнге ие болуы мүмкін болса, процестік келісімге қол қойған адамды жеке іс жүргізуге және істі жеке қарауға бөлу мүмкіндігін болғызбау;

- ҚПК-нің 616-бабында осындай келісімдердің екі түріне қатысты процестік келісім шарттарының түсінігі мен мазмұнын нақтылау;

- соттардың жария айыптау істері бойынша айыптау үкімдерін ғана емес шығаруы үшін жағдай жасай отырып, қылмыстық сот ісін жүргізу практикасын ізгілендіру [6].

Қылмыстық процесті жүргізетін орган күдіктіден, айыпталушыдан не қорғаушыдан кінәні мойындау туралы мәміле нысанында процестік келісім жасасу туралы өтінішхатты алып, ҚПК 613-бабында көзделген негіздерді ескере отырып, процестік келісім жасасу туралы мәселені шешу үшін келіп түскен өтінішхатты қылмыстық іс материалдарымен бірге үш тәулік ішінде прокурорға жібереді. Прокурор тергеп-тексеруді жүзеге асырған органнан істі талап етіп алдырады, осы баптың төртінші бөлігінде көзделген әрекеттерді орындайды, істе процестік келісім жасасу мүмкіндігі барын көріп, қорғаушы тарапқа оны жасасу туралы мәселені талқылауды ұсынады не өтінішхатты қанағаттандырудан бас тарту туралы жазбаша хабарлайды [2].

Прокурор процестік келісім жасасу мүмкіндігі туралы мәселені қарау кезінде: адамның жасаған іс-әрекетінің кінәні мойындау туралы мәміле нысанында іс жүргізу туралы процестік келісім аясына жататын-жатпайтынын; процестік келісім жасасу туралы өтінішхатты адамның ерікті түрде мәлімдегенін және оны жасасудың салдарлары туралы білетінін; адамның жиналған дәлелдемелерге және іс-әрекеттің саралануына дауласпайтынын; адамның өзі келтірген зиянның сипаты мен мөлшеріне және азаматтық талап қоюға келісетінін; істе қылмыстық қудалауды тоқтатуға әкеп соғатын мән-жайлардың жоқтығын тексеруге міндетті.

Көрсетілген мән-жайларды анықтау үшін прокурор күдіктіні, айыпталушыны (күзетпен ұсталып отырғанды жеткізуді талап етеді), оның қорғаушысын және жәбірленушіні шақырады, олардың процестік келісім жасасу мүмкіндігі туралы пікірін анықтайды. Өтінішхатты берген адамға прокурор процестік келісім жасасудың салдарын, оны жасасудан бас тарту құқығын түсіндіреді. Жәбірленуші келіспеген кезде процестік келісім жасалмайды. Егер жәбірленуші келіскен болса, онда оның қылмыспен келтірілген зиянды өтеу мәселесі жөніндегі пікірін ескере отырып, прокурор және қорғаушы тарап процестік келісім жасасады, ол жазбаша түрде жазылады және оған келісімге қатысушылар қол қояды [2].

Р.Н. Юрченко пікірінше, процестік келісімдер келесі баптарда көрсетілген, ҚПК 23-баптың 8-бөлімінде; 44-баптың 1-бөлігінің 4) тармақшасында; 60-баптың 3-бөлігі; 62-баптың 5-бөлігі; 64-баптың 9-бөлігінің 16) тармақшасында; 4-баптың 5) тармақшасында, 3)-4)

6-бөлімде, 5) 65-баптың 7-бөлігінің 5) тармағында; 11-тармақта айтылады) 67-баптың 1-бөлігі және 2-бөлігі; 71-баптың 6-бөлігі 22) тармақшасы; 19-баптың 1-бөлігі 193; 302-баптың 1-бөлігі 5) тармақшасы; 337-баптың 8-бөлігі; 341-баптың 1-бөлігі; 362-баптың 1, 3, 4-бөлігі; 365-баптың 1-бөлігі; 5-тармақ) 382-баптың 1-бөлігі; 483-баптың 3-бөлігі; 2-бап. 384-бап; 397-баптың 5-бөлігі; 429-баптың 2-бөлігі, 4-5-бөлігі; 430-баптың 3-бөлігі; 478-баптың 5-бөлігі; 480-баптың 2-бөлігі; 63, 64-тарауларының нормаларында қарастырылған [7].

Тағы бір мысал қарастырсақ, А.Қ.Ботабай 29.12.2018 жылы сағат 20:25 шамасында Алматы қаласы Сәтпаева көшесімен Байтұрсынова көшелерінің қиылысында болып, Сәтпаева көшесімен Манас көшесінің қиылысына жетіп алу мақсатында автокөлік тоқтатқан. Содан «Хюндай Акцент» маркалы ақ түсті мемлекеттік нөмірі 016/DCB/02 автокөлігі келіп тоқтап, сөйтіп А.Қ.Ботабай өзін Сәтпаева көшесімен Манас көшесіне дейін жеткізіп тастауын айтып 200 теңгеге көлік жүргізушісімен келіскен.

Сөйтіп А.Қ.Ботабай сол аталған автокөліктің ішінде болып, көліктің тежеуіш тұтқасының жанында өзіне бұрын соңды бейтаныс Ф.М.Ибрагимовқа тиесілі қара түсті әмиянды көрген. Оның қараусыз тұрғанын түсініп, өзінің қаражатқа мұқтаж екендігін біліп, сол қараусыз тұрған әмиянның ішінен ақша ұрлау қылмыстық ой-пиғылы туындады. Аталған қылмыстық ой-пиғылын жүзеге асыру мақсатында А.Қ.Ботабай аз.Ф.М.Ибрагимовтың назары жолда екеніне көз жеткізіп, автокөліктің қауіпсіздік белдігін тағып жатып өзінің оң қолымен Ф.М.Ибрагимовқа тиесілі қара түсті әмиянын, өзінің ұрлық қылмыстық ой-пиғылын іс жүзіне айналдырып, 5 000 теңге тұратын қара түсті әмиянды және оның ішіндегі 55 000 теңге, Ф.М.Ибрагимовтың жеке куәлігін, авто-көлік жүргізуші куәлігін, жасырын түрде жымқырып, жоғарыда көрсетілген автокөліктен Сәтпаева көшесімен Манас көшелерінің қиылысынан түсіп, қылмыс орнынан белгісіз бағытта бой тасалаған. Осыған байланысты, А.Қ.Ботабай, өзінің қылмыстық іс - әрекетімен, жәбірленуші Ф.М.Ибрагимовқа жалпы 60 000 теңгеге материалдық зиян келтірді.

Осылайша, 05.07.1999 жылы туылған Ботабай Ақмейір Қанатұлы ұрлық яғни – бөтеннің мүлкін жасырын жымқыру, яғни ҚР ҚК-нің 188 бабы 1 бөлігінде көрсетілген қылмыстық құқық бұзушылықты жасаған. Сот мәжілісінде сотталушы Ботабай тағылған айып бойынша кінәсін толық мойындап, қаулының сипатамалы бөлігінде көрсетілген мәнжайларда жауап берген. Қылмыспен келтірген материалдық шығынды өндіргенін, жәбірленушімен татуласқанын ескеріп, тағылған

айыпты толығымен мойындап шын жүректен өкініп, қылмыстық істі жәбірленушімен бітім келелісімге келгендіктен қысқартуын сұрады. Сот мәжілісінде жәбірленуші Ф.Ибрагимов қаулының сипатамалы бөлігінде көрсетілген мән-жайларда жауап беріп, бүгінгі күні сотталушымен қылмыспен келтірілген шығынды толық өндіріп бергенін және татуласқанын, оған ешқандай талап тілекгі жоқ екенін, қылмыстық іс өндірісімен қысқартуды сұраған. Дәлелдемелердің жиынтығымен сотталушының жасалған қылмысы толық жәбірленушінің және сотталушының жауаптарымен, оқиғасы орын алған жерді қарау хаттамасымен (і.б.9-11), сотталушының жәбірленушінің жауаптарымен және де істің басқа материалдарымен дәлелденген.

Сонымен, А.Ботабай ұрлық яғни – бөтеннің мүлкін жасырын жымқыру, яғни ҚР ҚК-нің 188 бабы 1 бөлігінде көрсетілген қылмыстық құқық бұзушылықты жасаған. Қазақстан Республикасының Жоғарғы сотының №4 21 маусым 2005 жылғы «Қазақстан Республикасы Қылмыстық кодексінің 67 бабын қолдану жөніндегі сот практикасы туралы» Нормативтік қаулысына сәйкес қылмыстық істі қысқарту туралы қаулы істі алдын ала тыңдау сатысында және басты сот талқылауының кез келген сатысында шығарылуы мүмкін.

ҚР ҚК-нің 68-бабының 1-бөлігіне сәйкес қылмыстық теріс қылық немесе қазаға ұшыратумен байланысты емес онша ауыр емес немесе ауырлығы орташа қылмыс жасаған адам, егер ол жәбірленушімен, арыз берушімен татуласса, оның ішінде медиация тәртібімен татуласса және келтірілген зиянды қалпына келтірсе, қылмыстық жауаптылықтан босатылуға жатады. Сот іске қатысушылардың, прокурордың пікірлерін және жәбірленушінің түскен арыздарын ескере отырып, іс құжаттарды зерттеп, сотталушы кінәсін толық мойындап және шын жүректен өкініп, жәбірленушімен татуласқанын, келтірілген шығынды толық өндіргенін, жәбірленуші ешқандай да талап қоймай, оны қылмыстық жауаптылықтан босатуды сұрағанын және жасалған қылмыстың орташа санатқа жататынын ескеріп, қылмыстық іс Қазақстан Республикасының Қылмыстық кодексінің 68-бабы 1-бөлігінің негізінде қысқартылуға жатады деп есептейді. Сотпен азаматтық талаптан бас тарту заңға қайшы келмейтің, кімнің де болсын заңмен қорғалатын құқығының бұзылмайтындығы анықталып азаматтық талап арыздан бас тарту өтініші қабылданып, азаматтық талап бойынша іс жүргізу қысқартылуға жатады. «Азаматтық және саяси құқықтар туралы халықаралық пактіні ратификациялау туралы» заңының 10 бабының 1 бөлігінде көрсеткендей «Бас бостандықтарынан айырылған барлық адамдар өздеріне деген

адамгершілікті көзқарасқа және адам баласына тән қадір қасиетінің құрметтелуіне құқылы». Заттай дәлелдемелер іс бойынша танылмаған.

Қазақстан Республикасының Қылмыстық Кодексінің 68-бабының 1-бөлігінің, басшылыққа алып, сот Қаулы етті: Ботабай Ақмейір Қанатұлын Қазақстан Республикасының ҚК-нің 188- бабының 1-бөлігімен көрсетілген қылмыстық жауаптылықтан, жәбірленуші сотталушымен татуласуына байланысты, ҚР ҚК 68-бабының 1-бөлігінің негізінде босатылсын. А.Ботабайға қатысты күзетпен ұстау түріндегі бұлтартпау шарасы өзгертіліп, қауылы күшіне енгенше қамаудан сот залынан босатып, қолхатта қалдырылсын, қауылы заң күшіне енген соң бұлтартпау шаралары жойылсын [8].

Кінәні мойындау туралы процестік келісім жасасу туралы өтінішхат жөніндегі шешім қылмыстық іс прокуратураға келіп түскен кезден бастап жеті тәулік ішінде қабылданады. Прокурордың процестік келісім жасасудан бас тартуы шағым жасалуға жатпайды, бірақ бұл кейіннен процестік келісім жасасуға кедергі келтірмейді [2].

Процестік келісімде: оның жасалған күні мен орны; процестік келісімді жасасушы прокуратура органының лауазымды адамы; келісім жасасушы күдіктінің, айыпталушының тегі, аты және әкесінің аты (ол болған кезде), туған күні мен жері, тұрғылықты жері және айналысатын кәсібі, оның қорғаушысының тегі, аты, әкесінің аты (ол болған кезде); қылмысты оның жасалған уақытын, орнын, сондай-ақ осы Кодекстің ережелеріне сәйкес дәлелденуге жататын басқа да мән-жайларды көрсете отырып сипаттау; Қазақстан Республикасы Қылмыстық кодексінің осы қылмыс үшін жауаптылық көздейтін тармағы, бөлігі, бабы; процестік келісімде көрсетілген шарттарды сақтаған және міндеттемелерді орындаған кезде күдіктіге, айыпталушыға қатысты қолданылуы мүмкін, қылмыстық жауаптылықпен жазалауды жеңілдететін мән-жайлар және қылмыстық заңның нормалары; процестік келісім жасасқаннан кейін күдікті, айыпталушы жасауға міндеттенетін әрекеттер; прокурор сот алдында ол туралы өтінішхат беретін жазаның түрі мен мөлшері; процестік келісім жасасудың ҚПК 614-бабында көзделген салдары; жәбірленушінің процестік келісім жасасуға келісетіні туралы көрсетілуге тиіс [2].

Процестік келісімге прокурор, күдікті, айыпталушы, оның қорғаушысы қол қояды. Процестік келісімге қол қойылғанға дейін күдіктінің, айыпталушының өз қорғаушысымен бірге оның ережелерін оңаша және құпия талқылауға құқығы бар.

Кінәні мойындау туралы мәміле нысанында процестік келісімге қол қойғаннан кейін прокурор күдіктіге, айыпталушыға қатысты

бұлтартпау шарасының күшін жою не оны өзгерту қажеттігі туралы мәселені қарайды. Іс бойынша тергеу және процестік әрекеттер жүргізу қажет болған кезде прокурор істі сотқа дейінгі тергеп-тексеру органына жібереді. Тергеуші, анықтаушы күдіктінің, айыпталушының кінәсін растауға жеткілікті көлемде дәлелдемелер жинауды жүзеге асырады. Егер сотқа дейінгі тергеп-тексеру нәтижесінде қылмыс жасаудың процестік келісімде көзделмеген өзге мән-жайлары белгілі болған жағдайда, осы келісім осы Кодекстің 615 және 616-баптарында көзделген тәртіппен және мерзімдерде қайта қаралуға жатады не өзінің қолданысын тоқтатады. Кінәні мойындау туралы мәміле нысанында процестік келісім жасалғаннан кейін тергеу және процестік әрекеттерді жүргізу қажеттігі болмаған жағдайда, іс бойынша сотқа дейінгі тергеп-тексеру аяқталды деп есептеледі және прокурор оны айыптау актісіз, айыптау хаттамасынсыз дереу сотқа жібереді, бұл туралы жәбірленушіге хабарланады [2].

Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім мынадай шарттар болған: күдікті, айыпталушы, сотталушы процестік келісім жасасуға ерікті түрде тілек білдірген; күдікті, айыпталушы, сотталушы келтірілген күдікке, айыптауға және іс бойынша қылмысты жасағанының қолда бар дәлелдемелеріне, өзі келтірген зиянның сипаты мен мөлшеріне дауласпаған кезде жасалуы мүмкін. Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім, егер қылмыстардың ең болмағанда біреуі осы бапта және осы Кодекстің 612-бабында көзделген талаптарға сәйкес келмесе, қылмыстардың жиынтығына қатысты жасалмайды.

Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім жасасудың салдары мыналар болып табылады: ҚПК 192-бабында белгіленген мерзімдерде сотқа дейінгі тергеп-тексерудің аяқталуы; ҚПК 382-бабының екінші бөлігіне және 64-тарауына сәйкес істің сот талқылауының жүргізілуі. Тұлғаның кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы жасалған процестік келісімнің шарттарын орындамауы тоқтатылған сотқа дейінгі тергеп-тексеруді немесе қылмыстық құдалауды ҚПК 291-бабында көзделген тәртіппен қайта бастауға алып келеді. Сот шешім қабылдау үшін кеңесу бөлмесіне кеткенге дейін күдіктінің, айыпталушының немесе сотталушының кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісімнен бас тартуға құқығы бар. Тараптардың кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім жасасудан

бас тартуы оны қайтадан жасасу туралы өтінішхат мәлімдеуге кедергі келтірмейді [2].

Күдікті, айыпталушы, сотталушы қылмыстық іс бойынша іс жүргізудің кез келген сәтінде сот кеңесу бөлмесіне кеткенге дейін кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы мәміле нысанында процестік келісім жасасу туралы өтінішхат мәлімдеуге құқылы. Процестік келісім прокурордың бастамасы бойынша жасалуы мүмкін. Тергеп-тексеруді жүзеге асыратын орган күдіктіден, айыпталушыдан, сотталушыдан не қорғаушыдан кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы мәміле нысанында іс жүргізу туралы процестік келісім жасасу туралы өтінішхатты алып, осы Кодекстің 613-бабында көзделген негіздерді ескере отырып, процестік келісім жасасу туралы мәселені шешу үшін келіп түскен өтінішхатты қылмыстық іс материалдарымен бірге үш тәулік ішінде прокурорға жібереді.

Прокурор тергеп-тексеруді жүзеге асыратын органнан істі талап етіп алдырады, осы баптың үшінші және төртінші бөліктерінде көзделген әрекеттерді орындайды, істе процестік келісім жасасу мүмкіндігі барын көріп, қорғаушы тарапқа оны жасасу туралы мәселені талқылауды ұсынады не өтінішхатты қанағаттандырудан бас тарту туралы жазбаша хабарлайды.

Прокурор процестік келісім жасасу мүмкіндігі туралы мәселені қарау кезінде: тұлғаның жасаған іс-әрекетінің кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы мәміле нысанында іс жүргізу туралы процестік келісім аясына жататын не жатпайтынын; процестік келісім жасасу туралы өтінішхатты тұлғаның ерікті түрде мәлімдегенін және оны жасасудың салдары туралы білетінін; тұлғаның жиналған дәлелдемелерге және іс-әрекеттің саралануына дауласпайтынын; тұлғаның өзі келтірген зиянның сипаты мен мөлшеріне және азаматтық талап қоюға келісетінін; істе қылмыстық құдалауды тоқтатуға алып келетін мән-жайлардың жоқ екенін тексеруге міндетті.

Көрсетілген мән-жайларды анықтау үшін прокурор күдіктіні, айыпталушыны, сотталушыны (күзетпен ұсталып отырғанды жеткізуді талап етеді), оның қорғаушысын және жәбірленушіні шақырады, олардың процестік келісім жасасу мүмкіндігі туралы пікірін анықтайды. Прокурор өтінішхатты берген тұлғаға процестік келісім жасасудың салдарын, оны жасасудан бас тарту құқығын түсіндіреді. Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім

жасасуға жәбірленушінің келісiмiн алу талап етiлмейдi. Кiнәнi мойындау және заңсыз иемденiлген активтердi қайтару туралы процестiк келiсiм жасасу туралы өтiнiшхат жөнiндегi шешiм қылмыстық iс прокуратураға келiп түскен кезден бастап он тәулiк iшiнде қабылданады. Прокурордың процестiк келiсiм жасасудан бас тартуы шағым жасалуға жатпайды, алайда бұл кейiннен процестiк келiсiм жасасуға кедергi келтiрмейдi.

Кiнәнi мойындау және заңсыз иемденiлген активтердi қайтару туралы процестiк келiсiмде: оның жасалған күнi мен орны; прокуратура органының процестiк келiсiмдi жасасушы лауазымды адамы; процестiк келiсiм жасасушы күдiктiнiң, айыпталушының немесе сотталушының тегi, аты және әкесiнiң аты (ол болған кезде), туған күнi мен жерi, тұрғылықты жерi және айналысатын iсi, оның қорғаушысының тегi, аты, әкесiнiң аты (ол болған кезде); қылмысты оның жасалған уақытын, орнын, сондай-ақ осы Кодекстiң ережелерiне сәйкес дәлелденуге жататын басқа да мән-жайларды көрсете отырып сипаттау; Қазақстан Республикасы Қылмыстық кодексiнiң осы қылмыс үшiн жауаптылық көзделетiн бабы, бөлiгi, тармағы; күдiктiнiң, айыпталушының немесе сотталушының қылмыс жасаудағы өзiнiң кiнәсiн мойындауы және заңсыз иемденiлген, оның iшiнде Қазақстан Республикасының шегiнен тысқары жердегi активтерiн өз еркiмен қайтару мiндетi; қайтарылуға жататын заңсыз иемденiлген активтердiң, оның iшiнде Қазақстан Республикасының шегiнен тысқары жердегi активтердiң тiзбесi мен сипаттамасы, олардың тұрған жерi; процестiк келiсiмде көрсетiлген шарттарды сақтаған және мiндеттемелердi орындаған кезде күдiктiге, айыпталушыға немесе сотталушыға қатысты қолданылуы мүмкiн, қылмыстық жауаптылықты, жазалауды жеңiлдететiн мән-жайлар және қылмыстық заңнаманың нормалары; прокурор өтiнiшхат беретiн, Қазақстан Республикасы Қылмыстық кодексiнiң ережелерiне сәйкес тұлғаны қылмыстық жауаптылықтан босату мәселелерi; процестiк келiсiм жасасқаннан кейiн күдiктi, айыпталушы немесе сотталушы жасауға мiндеттенетiн әрекеттер; заңсыз иемденiлген активтердi Қазақстан Республикасының заңсыз иемденiлген активтердi мемлекетке қайтару туралы заңнамасына сәйкес құрылған Арнаулы мемлекеттiк қорға немесе басқарушы компанияға аудару (аударым жасау) немесе беру мерзiмдерi мен тәсiлдерi; күдiктiнiң, айыпталушының немесе сотталушының қылмыстық тергеп-тексеру мәселелерi және заңсыз иемденiлген активтердi қайтару бойынша прокурормен өзара iс-қимыл жасау және ынтымақтасу жөнiндегi мiндетi; процестiк келiсiм жасасудың

салдары және кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім жасалғаннан кейін прокурордың қылмыстық іс бойынша әрекеті; күдіктінің, айыпталушының немесе сотталушының кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісімнің шарттарын орындамауының салдары; кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісімде тараптар келіскен басқа да шарттар мен міндеттер көрсетіледі [2].

Процестік келісімнің шарттарында тұлға кәсіпкерлік қызметті жүргізудің, оның ішінде заңнамалық және өзге де нормативтік құқықтық актілерде белгіленген бәсекелестік емес қолайлы жағдайларына байланысты, сол сияқты тиісті тауарлар, жұмыстар немесе көрсетілетін қызметтер нарығында экономикалық ресурстарды, оның ішінде тиісті тауар нарығында үстем немесе монополиялық жағдайға ие болатын және (немесе) ие болған нарық субъектілерінің акцияларын (жарғылық капиталдарға қатысу үлестерін) тікелей немесе жанама иелену жолымен іс жүзінде шоғырландыру нәтижесінде үстеме кірістерді алған жағдайларда, тұлға активтерді иеленген жалпы кезеңде алған осындай үстеме кірістердің сомаларын қайтару көзделуге тиіс. Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы процестік келісім жазбаша түрде жасалады және оған прокурор, күдікті, айыпталушы немесе сотталушы, сондай-ақ оның қорғаушысы қол қояды. Процестік келісімге қол қойылғанға дейін күдіктінің, айыпталушының немесе сотталушының өз қорғаушысымен бірге оның ережелерін оңаша және құпия талқылауға құқығы бар [2].

Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы мәміле нысанында процестік келісімге қол қойылғаннан кейін прокурор күдіктіге, айыпталушыға, сотталушыға қатысты бұлтартпау шарасының күшін жою не оны өзгерту қажеттігі туралы мәселені қарайды. Іс бойынша тергеу әрекеттерін және процестік әрекеттерді жүргізу қажет болған жағдайда прокурор істі сотқа дейінгі тергеп-тексеру органына жібереді. Тергеуші күдіктінің, айыпталушының кінәсін растауға жеткілікті көлемде дәлелдемелер жинауды жүзеге асырады.

Егер сотқа дейінгі тергеп-тексеру нәтижесінде қылмыс жасаудың процестік келісімде көзделмеген өзге мән-жайлары анықталған жағдайда, осы келісім ҚПК 617-3 және 617-4-баптарында көзделген тәртіппен және мерзімдерде қайта қаралуға жатады не өзінің қолданысын тоқтатады. Кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы мәміле нысанында процестік келісім

жасалғаннан кейін тергеу әрекеттерін және процестік әрекеттерді жүргізу қажеттігі болмаған жағдайда, іс бойынша сотқа дейінгі тергеп-тексеру аяқталды деп есептеледі және прокурор оны айыптау актісізсіз дереу сотқа жібереді, бұл туралы жәбірленушіні және оның өкілін (ол болған кезде) хабардар етеді [2].

Күдіктінің, айыпталушының, сотталушының және сотталған адамның қылмыстық процесті жүргізетін органға немесе прокурорға ҚПК 612-бабы бірінші бөлігінің 2) тармағына және 619-бабына сәйкес ынтымақтастық туралы процестік келісім жасасу туралы өтінішхатпен жүгінуге құқығы бар. Күдіктімен, айыпталушымен, сотталушымен ынтымақтастық туралы процестік келісімді тиісінше Қазақстан Республикасының Бас Прокуроры, облыстың прокуроры немесе оған теңестірілген прокурор, олардың орынбасарлары, ал сотталған адаммен – Қазақстан Республикасының Бас Прокуроры не оның орынбасары бекітеді. Ынтымақтастық туралы процестік келісім жасасу туралы өтінішхат сотқа дейінгі тергеп-тексеру басталған кезден бастап және үкімді орындау сатысын қоса алғанға дейін мәлімделуі мүмкін.

Ынтымақтастық туралы процестік келісімді жасасу туралы өтінішхатты күдікті, айыпталушы, сотталушы және сотталған адам жазбаша түрде береді және ол міндетті түрде қорғаушының қойған қолымен бекемделеді. Егер қорғаушыны күдікті, айыпталушы, сотталушы немесе сотталған адам, оның заңды өкілі немесе күдіктінің, айыпталушының, сотталушының немесе сотталған адамның тапсырмасы бойынша басқа адамдар шақырмаса, онда қорғаушының қатысуын қылмыстық процесті жүргізетін орган не жазаны орындайтын мекеме немесе орган қамтамасыз етеді. Іс жүргізуінде қылмыстық іс жатқан тергеуші, анықтаушы, жазаны орындайтын мекеменің немесе органның басшысы ынтымақтастық туралы процестік келісім жасасу туралы өтінішхатты алған кезде оны бір тәулік ішінде прокурорға жібереді. Сотталушының ынтымақтастық туралы процестік келісім жасасу туралы өтінішхатын сот ол келіп түскен кезден бастап үш тәулік ішінде прокурорға жібереді. Сотталған адам өзі аумағында жазасын өтеп жүрген облыс прокурорының атына процестік келісім жасасу туралы өз өтінішхатын жазаны орындайтын орган арқылы беруге құқылы [2].

Ынтымақтастық туралы процестік келісім ҚПК 615-бабы үшінші бөлігінің 2) тармағында, 616-бабы бірінші бөлігінің 1), 2), 3), 4), 5), 6) және 7) тармақтарында, екінші бөлігінде көзделген талаптар сақтала отырып, қажет болған кезде 47-бабының қағидалары бойынша оның

құпиялығын сақтай отырып және 12-тарауына сәйкес қауіпсіздікті қамтамасыз ете отырып, прокурор мен күдіктінің, айыпталушының, сотталушының, сотталған адамның арасында жасалады және бекіту үшін тиісінше Қазақстан Республикасының Бас Прокурорына, облыстың прокурорына немесе оған теңестірілген прокурорға, олардың орынбасарларына, ал сотталған адаммен келісім – Қазақстан Республикасының Бас Прокурорына не оның орынбасарына жіберіледі. Ынтымақтастық туралы процестік келісім жасасу туралы мәселені шешу үшін прокурор қосымша материалдарды талап етуге құқылы [2].

Бекітуге келіп түскен процестік келісім бойынша күдіктіге, айыпталушыға, сотталушыға қатысты – Қазақстан Республикасының Бас Прокуроры, облыстың прокуроры немесе оған теңестірілген прокурор, олардың орынбасарлары, ал сотталған адамға қатысты – Қазақстан Республикасының Бас Прокуроры не оның орынбасары: қылмыстық істі және ұсынылған (талап етіліп алдырылған) қосымша материалдарды зерделейді, ынтымақтастық туралы процестік келісім жасасудың заңдық және нақты негіздерін тексереді, сондай-ақ күдіктінің, айыпталушының, сотталушының, сотталған адамның келісім нысанасы болып табылған әрекеттерді орындау жөніндегі ниетінің сипатын бағалайды; күдіктінің, айыпталушының, сотталушының, сотталған адамның ынтымақтастық туралы процестік келісіммен байланысты барлық шарттармен және талаптарымен танысқанын, азаптауларға және басқа да қатыгез, адамгершілікке жатпайтын немесе қадір-қасиетті қорлайтын қарым-қатынас пен жазалау түрлеріне ұшырағанын-ұшырамағанын, ынтымақтастық туралы процестік келісімді өз еркімен жасасқанын-жасаспағанын, оның құқықтық салдарын білетінін-білмейтінін анықтайды; ынтымақтастық туралы процестік келісімді бекітеді не оны бекітуден бас тарту туралы қаулы шығарады [2].

Қорытындылай келе, ҚПК-нің 67 және 68-баптарын қолдану кезінде алынатын сотталушы үшін артықшылықтарды салыстырамыз: кінәсін мойындау туралы мәміле жасасу кезінде айыпталушы келтірілген зиянның кінәсін, сипаты мен мөлшерін тануға, оған сот тағайындауы мүмкін жазаның түрімен және мөлшерімен, қылмыспен келтірілген зиян үшін өтемақы төлеу мерзімдерімен келісуге тиіс. Келісу ісінде шығарылған заңды күшіне енген сот үкімінің негізінде адам кінәлі деп танылады, Қылмыстық Кодекстің 79-бабында көзделген мерзім өткеннен кейін өтелетін соттылыққа ие болады. Осы соттылық өтелгенге дейін жаңа қылмыс жасаған кезде қылмыстардың қайталануы белгіленеді

және ҚК 60-бабына сәйкес жаңа қылмыс үшін жаза тағайындау қағидалары қолданылады.

Айыпталушыны кінәсін мойындау туралы мәміле нысанында іс жүргізу келісімін жасасуға тарта алатын жалғыз нәрсе-қылмыспен келтірілген зиянды бөліп-бөліп өтеу мүмкіндігі, ал үкім заңды күшіне енгеннен кейін, ал жәбірленушімен ҚК-нің 68-бабының тәртібімен татуласу кезінде ол зиянды дереу түзетуі керек және бұл оның татуласу шарттарының бірі болып табылады жәбірленушімен және қылмыстық істі тоқтатумен. Таңдау Оның қолында қалады, ешкім оған іс бойынша іс жүргізуді аяқтаудың бір немесе басқа әдісін жүктеуге құқылы емес.

Пайдаланылған қайнар көздерінің тізімі:

1. Қазақстан Республикасының 2010 жылдан 2020 жылға дейінгі кезеңге арналған құқықтық саясат тұжырымдамасы туралы Қазақстан Республикасы Президентінің 2009 жылғы 24 тамыздағы N 858 Жарлығы. // Электронды ресурс: <https://adilet.zan.kz>

2. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. // Электронды ресурс: <https://adilet.zan.kz>

3. Соттардың қылмыстық істер бойынша келісімдік тәртіпте іс жүргізу практикасы туралы Қазақстан Республикасы Жоғарғы Сотының 2016 жылғы 7 шілдедегі № 4 Нормативтік қаулысы// Электронды ресурс: <https://adilet.zan.kz>

4. Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ// Электронды ресурс: <https://adilet.zan.kz>

5. Алматы қаласы Әуезов аудандық соты №7513-23-00-1/276 Үкімі. 11.05 2023 жыл.

6. Канафин Д.К. Институт процессуальных соглашений и международные стандарты справедливого уголовного процесса.// <https://online.zakon.kz>

7. Юрченко Р.Н. Процессуальные соглашения и законодательное поощрение их заключения. // <https://online.zakon.kz>

8. Алматы қаласы Бостандық аудандық соты 7550-20-00-1/487 Қаулысы. 04.12 2020 жыл.

ӘОЖ 343.24:343.8(345)

Нусубалиева Макпал Ерболовна
«Қайнар» академиясының магистранты
Қазақстан Республикасы, Алматы қ.

ҚЫЛМЫСТЫҚ ПРОЦЕСТЕГІ ІС ЖҮРГІЗУ КЕЛІСІМІ ИНСТИТУТЫНЫҢ КЕЙБІР АСПЕКТІЛЕРІ

Аңдатпа:

Мақалада қылмыстық процестегі іс жүргізу келісімі институтының кейбір аспектілері қарастырылған. Жасалған процестік келісім шеңберінде қылмыстық істерді тергеп-тексеру сипатталады. Жалпы теориялық тұрғыда жеделдетілген және жеңілдетілген сот ісін жүргізу мәселелері қарастырылады. Авторлар кінәні мойындау туралы және өзге келісімін зерттей отыра, процестік келісімнің мақсаты тергеу әрекеттерін жеңілдету екендігіне назар аударып, процестік келісімге қол қойылғаннан кейін қосымша дәлелдер жинаудың қажеттігі жоқ деген пікір білдіреді.

Түйінді сөздер: процестік келісім, қылмыстық процестік кодекс, қылмыстар, қылмыстық теріс қылық, азаматтық талап, кінәні мойындау.

Нусубалиева Макпал Ерболовна
Магистрант академии «Қайнар»
Республика Қазақстан, г. Алматы

НЕКОТОРЫЕ АСПЕКТЫ ИНСТИТУТА ПРОЦЕССУАЛЬНОГО СОГЛАШЕНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация:

В статье рассматриваются некоторые аспекты института процессуального соглашения в уголовном процессе. Расследование уголовных дел изучается с позиции заключения процессуального соглашения. В общетеоретическом плане рассмотрены вопросы ускоренного и упрощенного судопроизводства. Изучая такие соглашения, как соглашения о признании вины, процессуальные и иные соглашения, авторы обращают внимание на то, что целью процессуального соглашения явля-

ется облегчение следственной деятельности, и высказывают мнение об отсутствии необходимости сбора дополнительных доказательств после подписания процессуального соглашения.

Ключевые слова: процессуальное соглашение, Уголовно-процессуальный кодекс, преступления, уголовный проступок, гражданский иск, признание вины.

Nusubalieva M.

Master's student at the Kainar Academy
Republic of Kazakhstan, Almaty

**SOME ASPECTS OF THE INSTITUTE OF
PROCEDURAL AGREEMENT IN THE
REPUBLIC OF KAZAKHSTAN**

Annotation:

The article discusses some aspects of the institution of procedural agreement in criminal proceedings. The investigation of criminal cases is studied from the perspective of concluding a procedural agreement. Issues of accelerated and simplified legal proceedings are considered from a general theoretical perspective. Studying agreements such as plea agreements, procedural and other agreements, the authors draw attention to the fact that the purpose of the procedural agreement is to facilitate investigative activities, and express the opinion that there is no need to collect additional evidence after signing the procedural agreement.

Key words: procedural agreement, Criminal Procedure Code, crimes, criminal offense, civil claim, admission of guilt.

Кінәні мойындау туралы келісім күдіктінің, айыпталушының, сотталушының немесе оның қорғаушысының өтінішхаты бойынша не прокурордың бастамасы бойынша жасалуы мүмкін. Қорғаушының өтінішхаты бойынша немесе прокурордың бастамасы бойынша кінәні мойындау туралы келісім жасасу кезінде күдіктінің, айыпталушының осындай келісімді жасасуды қалайтынын ерікті түрде білдіруі сотқа дейінгі тергеу сатысында қылмыстық істе тиісінше анықталуға және тіркелуге тиіс.

Қылмыстық-процестік заң кінәні мойындау туралы келісім жасасу жөніндегі өтінішхаттың белгілі бір нысанын белгілемейді, сондықтан ҚПК-нің 99-бабының екінші бөлігінің талаптарына сәйкес жазбаша

өтінішхат қылмыстық іс материалдарына тіркелуге, ауызша өтінішхат – тергеу әрекеті немесе сот отырысы хаттамасына енгізілуге тиіс.

Күдіктінің, айыпталушының, сотталушының неоның қорғаушысының немесе прокурордың кінәні мойындау туралы келісім жасасу жөніндегі өтінішхаты сотқа дейінгі іс жүргізу сатысында – адамның күдікті мәртебесін алған сәтінен бастап, бірінші және апелляциялық сатыдағы сотта – соттың кеңесу бөлмесіне кетуіне дейін берілуі мүмкін.

Қылмыстық теріс қылықтар туралы істер бойынша кінәні мойындау туралы келісім жасасу заңда көзделмеген [1].

Жасалған процестік келісім шеңберінде қылмыстық істерді тергеп-тексеру мынадай: онша ауыр емес, ауырлығы орташа не ауыр қылмыстар бойынша – күдікті, айыпталушы келтірілген күдікпен, айыптаумен келіскен жағдайда – кінәні мойындау туралы мәміле нысанында; қылмыстық топ жасаған қылмыстарды, өзге де адамдар жасаған аса ауыр қылмыстарды, сондай-ақ экстремистік және террористік қылмыстарды ашуға және тергеп-тексеруге ықпал ету кезінде барлық санаттағы қылмыстар бойынша – ынтымақтастық туралы келісім нысанында; Қазақстан Республикасының Қылмыстық кодексінде көзделген онша ауыр емес, ауырлығы орташа не ауыр қылмыстар бойынша кінәні мойындау және заңсыз иемденілген активтерді қайтару туралы келісім нысанында жүргізіледі. Процестік келісімді қылмыстық заңда тыйым салынған іс-әрекетті есі дұрыс емес күйде жасаған немесе қылмыс жасағаннан кейін психикасының бұзылумен ауырған адамдармен жасауға болмайды. Процестік келісім жасасу адамды жәбірленуші және азаматтық талапкер болып танылған адамдардың алдында азаматтық-құқықтық жауаптылықтан босатуға негіз болып табылмайды [2].

Қазақстан Республикасының Бас прокуратурасы құқықтық статистика және арнайы есепке алу жөніндегі комитетінің мәліметіне сәйкес, Қазақстан Республикасында №1 нысаны «Бірінші сатыдағы соттың қылмыстық істерді қарауы жөніндегі жұмысы туралы» 2023 жылғы қаңтар айы мен желтоқсан айы аралығындағы келесідей, Есептік кезеңнің басына аяқталмаған істердің қалдығы, барлық қылмыстық құқық бұзушылықтар 2578. Келісімдік іс жүргізуде қаралған істер бойынша 127. Есептік кезеңде келіп түскен істер 2163. Сотқа келіп түскен істер бойынша адамдардың саны 2532. Қазақстан Республикасының Қылмыстық-процестік кодексінің (бұдан әрі-ҚР ҚПК) бұзушылықтары жойылғаннан 105. Іздеуден кейін 30. Үкім шығарылып қаралған істер 1834. Кәмелетке толмағандардың істері бойынша 29. Әйелдердің істері бойынша 257. Барлық тоқтатылған істер 24 [3].

Қылмыстық процесті жүргізуші орган кінәні мойындау туралы келісім жасасу жөніндегі өтінішхатты прокурорға жібергенге дейін жәбірленушіге ҚПК-нің 71-бабы алтыншы бөлігінің 22) тармағының талаптарына сәйкес тараптардың келісім жасасу ниеті туралы, оның шарттары мен салдарлары туралы білуге, қылмыспен келтірілген залалды өтеу бойынша өз шарттарын ұсынуға не оны жасасуға қарсылық білдіруге құқығы бар екенін түсіндіруге міндетті. Сотқа дейінгі тергеп-тексеру сатысында аталған әрекетті жүргізу туралы ҚПК-нің 199-бабының талаптарын сақтай отырып, хаттама жасалады, ал сот талқылауында – сот отырысының хаттамасына енгізіледі.

Қылмыстық процесте кінәні мойындау туралы келісім жасасу сатысында жәбірленушінің құқықтарын тиісінше қамтамасыз ету және жәбірленушінің келісімді жасасуға келісін алу мақсатында прокурор жәбірленушіге оның кінәні мойындау туралы келісім жасасуға келісуінің ҚПК-нің 614-бабында көзделген құқықтық салдары туралы қосымша түсіндіруі тиіс. Осы әрекетті жүргізу туралы прокурор ҚПК-нің 199-бабының талаптарын сақтай отырып, хаттама жасайды.

Қылмыстық іс бойынша жәбірленуші (жеке немесе заңды тұлға) жоқ болған жағдайды қоспағанда, жәбірленушінің кінәні мойындау туралы келісім жасасуға келісуі оны жасасудың міндетті шарты болып табылады, сондықтан жәбірленушінің мұндай келісімі қылмыстық іс материалдарына жазбаша нысанда жәбірленушіге оның құқықтарын және кінәні мойындау туралы келісім жасасуға келісім беруінің салдарларын түсіндіру хаттамасымен қоса тігілуге тиіс [1].

Мысалы, сотталушы Р.Айткалиев 10.01.2020 жылы сағат 04.00 шамасында қасақана, пайдақорлық ниетпен, бөтеннің мүлкін тұрғын үй жайға заңсыз кірумен жасырын түрде жымқыру мақсатында, Ақтау қаласы 12-52-12 пәтерінің есігінің құлпын сындыру арқылы ішіне заңсыз кіріп, пәтердің жатын бөлмесінде орналасқан диванның бұрышында тұрған жәбірленуші А.Доринге тиесілі қызыл түсті әмиян ішінен 20.000 тенге ақшасын жасырын түрде жымқырып, оқиға болған жерден бой таслап кеткен. Басты сот талқылауында сотталушы Р.Айткалиев өзінің жасаған қылмысын толығымен мойындап, өзінің жасаған іс әрекетіне шын жүректен өкінетінін, жәбірленушінің шығынын толығымен өндіргенін, онымен татуласқанын, жәбірленуші өзін кешіргенін көрсетіп, өзін медиация тәртібімен қылмыстық жауаптылықтан босатып, қылмыстық істі қысқартуға қарсы еместігін айтып көрсетті. Жәбірленуші А.Дорин денсаулығына байланысты басты сот талқылауына қатыса алмайтынын, сотқа дейінгі тергеп-тексеру кезінде берілген жауабын толығымен

қуаттайтынын, сотталушы Р.Айткалиевке қатысты қоятын ешқандай талап тілегінің жоқтығын, өзіне келтірілген материалдық шығын толығымен өндірілгенін, талап арыздан бас тартатынын, сотталушымен татуласқанын айтып көрсетіп, сотталушы Р.Айткалиевты.

Медиация тәртібімен қылмыстық жауаптылықтан босатып, оған қатысты қылмыстық істі қысқартуын сұрап жазбаша сотқа арыз түсірді. Басты сот талқылауында Ақтау қалалық прокуратурасының бөлім прокуроры П.Қонысбаева жәбірленушімен сотталушының татуласуларына, жәбірленушінің сотталушыға қоятын талабының болмауына байланысты сотталушы Р.Айткалиевты медиация тәртібімен қылмыстық жауаптылықтан босатып, қылмыстық істі Қазақстан Республикасының Қылмыстық кодексінің 68 бабына сай медиация тәртібімен қысқартуға қарсы еместігін айтып көрсетті. 05 ақпан 2020 жылы жасақталған медиация өткізу туралы келісім шарттан, жәбірленуші А.Доринге келтірілген зиян толықтай өтелгендігі, сотталушы Р.Айткалиевке қоятын ешқандай талап-тілегінің жоқ екендігі анықталады. Қазақстан Республикасының «Медиация туралы» Заңының 26 бабы 1 бөліміне сай тараптармен дауды реттеу туралы келісімге қол қойылған сәттен медиация аяқталады. Басты сот талқылауына ұсынылған келісімге жәбірленуші А.Дорин сотталушы Р.Айткалиев және Маңғыстау облысы бойынша кәсіби медиатор А.Кемаладинова қол қойған. Сотталушы Р.Айткалиевтің қылмыстық іс-әрекетін Қазақстан Республикасының Қылмыстық кодексінің 188 бабы 2 бөлігі «З» тармағымен ұрлық, яғни бөтеннің мүлкін жасырын түрде тұрғын үй жайға заңсыз кірумен жасалған деп дәрежелеуге жатады. Жәбірленуші А.Дорин сотталушы Р.Айткалиевке қоятын ешқандай талабының жоқ екендігі, келтірген шығын есесі толықтай өтелгендігін мәлімдеп, өзара татуласуларына байланысты сотталушы Р.Айткалиевты медиация тәртібімен қылмыстық жауапкершіліктен босатып, қылмыстық істі өндірістен қысқарту жөнінде жазбаша арыз берді. Қазақстан Республикасының Қылмыстық Кодексінің 68 бабы 1 бөлігі бойынша, қылмыстық теріс қылық немесе қазаға ұшыратумен байланысты емес онша ауыр емес немесе ауырлығы орташа қылмыс жасаған адам, егер ол жәбірленушімен, арыз берушімен татуласса, оның ішінде медиация тәртібімен татуласса және келтірілген зиянды қалпына келтірсе, қылмыстық жауаптылықтан босатылуға жатады деп көрсетілген. Қазақстан Республикасының Қылмыстық Кодексінің 11 бабы 2 бөлігіне сәйкес, сотталушы Р.Айткалиевтің жасаған қылмысының ауырлығы орташа дәрежедегі қылмыстар санатына жатады. Сот, іс мәнжайларын, қылмыспен келген салдарды, жәбірленушінің пікірін және

медиация туралы заңның қағидаларын есепке ала отырып, аталған заңның нормаларын қолдануға болады деп қортындылайды.

Сондықтан, сот, сотталушы Р.Айткалиевті Қазақстан Республикасы Қылмыстық кодексінің 68 бабының 1 бөлігіне сай сотталушының жәбірленушімен медиация тәртібімен татуласуына, келтірілген зиянның есесі толтырылуына байланысты, қылмыстық жауаптылықтан босатып, қылмыстық іс қысқартылуға жатады деп санайды. Қазақстан Республикасының Қылмыстық процесілік кодексінің 169 бабына сай жәбірленуші талаптан бас тартуларына байланысты бұл бөлігінде іс қысқартылуға жатады. Жоғарыда көрсетілгендердің негізінде ҚР Қылмыстық-процестік кодексінің 35 бабы 1 бөлігін, 36 бабы 1 бөлігін, 327, 343, 344, 382 баптарын басшылыққа ала отырып, сот: Айткалиев Роллан Битимбаевич Қазақстан Республикасының Қылмыстық кодексінің 188 бабы 2 бөлігінің 3 тармағымен көзделген қылмысты жасауда айыптау туралы қылмыстық іс медиация тәртібімен сотталушының жәбірленушімен татуласуларына және жәбірленушіге келтірілген зиян есесінің толтырылуына байланысты сотталушыны қылмыстық жауаптылықтан босатумен осы Кодекстің 68 бабы 1 бөлігінің негізінде қысқартылсын [4].

Тағы бір мысал ретінде, С.Ж.Жалиш жеңіл жолмен ақша табу мақсатында 2020 жылдың 22 желтоқсанында жәбірленуші Б.Бейсакуловпен Шымкент қалалық әкімшілігінің алдында кездесіп, «Бастау Бизнес» бағдарламасы шеңберінде 2.000.000 теңге мен 5.000.000 теңге аралығында мемлекеттік грант алып бере аламын деп алдап, оның ол бағдарламасы талаптарынан хабарсыз екенін пайдаланып, қасақана, пайдакүнемдік ниетпен, «Бастау Бизнес» бағдарламасы бойынша мемлекеттен берілетін грантты алу шарттарына сай құжаттарды рәсімдеп грантты алып беруге мүмкіндігі жоқ екеніне қарамастан, оның сеніміне қиянат жасай отырып, жәбірленуші Б.Бейсакуловтан өзінің Шымкент қаласы, Қарасу е/м, №4В тұрғын үйінде отырып, «Kaspi gold» қосымшасы арқылы С.Жалиш өзінің «Kaspi gold» есепшотына 22.12.2020 жылы 100.000 теңге көлемінде ақша қаражаттарын аудартып алып, ақшаны өз пайдасына жаратқан. С.Ж.Жалиш 2020 жылдың 23 желтоқсанында жәбірленуші З.Аязбековпен Шымкент қалалық әкімшілігінің алдында кездесіп, «Бастау Бизнес» бағдарламасы шеңберінде 2.000.000 теңге мен 5.000.000 теңге аралығында мемлекеттік грант алып беремін деп алдап, өзінің алаяқтық, яғни бөтеннің мүлкін сенімге қиянат жасау арқылы алдап алу қылмыстық ойын жүзеге асыру мақсатында оған «Бастау Бизнес» бағдарламасы талаптарынан хабарсыз екенін пайдаланып,

қасақана, пайдакүнемдік ниетпен, «Бастау Бизнес» бағдарламасы бойынша мемлекеттен берілетін грантты алу шарттарына сай құжаттарды рәсімдеп грантты алып беруге мүмкіндігі жоқ екеніне қарамастан, оның сеніміне қиянат жасай отырып, жәбірленуші З.Аязбековтен өзінің «Kaspi gold» есепшотына «Kaspi gold» қосымшасын пайдаланушы Жұман А.Е. – деп көрсетілген Азаматшадан 23.12.2020 жылы 100.000 теңгеге аударым жасап, 24.12.2020 жылы 50.000 теңгеге, 27.12.2020 жылы 40.000 теңгеге және сол күні 10.000 теңге көлемінде ақша қаражатын «Kaspi банкомат» терминалы арқылы аудартып алып, барлық ақшаларды өз пайдасына жаратып, жәбірленуші З.Аязбековке жалпы 200.000 теңгеге мүлктік залал келтірген [5].

Сотталушы С.Ж.Жалиш қылмыстық оқиғаның қалай болғаны мен жасалу тәсілі сотқа дейінгі тергеп-тексеруде және сот тергеуі барысында берген жауаптарымен жоққа шығарылмайды, жәбірленушілердің жауаптарымен, басқада қылмыстық іс бойынша жинақталған дәлелдермен, тергеу амалдары бойынша түзілген хаттамаларымен толық бекітіледі. Тергеу барысында сотталушы С.Ж.Жалиштың іс-әрекеттері ҚК-нің 190-бабының 3-бөлігі 4) тармағымен, яғни ол бірнеше рет бөтеннің мүлкін алдау жолымен иемденіп алаяқтық жасаған деп саралаған. Алайда, С.А.Жалиштың 2020 жылы 20 шілдесінде жасаған қылмыстық іс әрекеті бойынша ҚК-нің 190-бабының 1-бөлігімен қозғалған 1-ші эпизоды бойынша жәбірленуші К.Абсеметовамен татуласуына байланысты ҚК-нің 68-бабының 1-бөлігінің негізінде қылмыстық жауаптылықтан босатылып, іс өндірістен тоқтатылған. Сотқа түскен жәбірленушілер З.Аязбековтың, Б.Бисакуловтың арыздарына қарағанда, сотталушы С.Ж.Жалиш тарапынан қылмыстық құқық бұзушылық салдарынан келтірілген материалдық залал толығымен өтелгені, сотталушы С.Ж.Жалишке ешқандай арыз шағымдары жоқ екендігі, онымен татуласқандары, осыған байланысты сотталушы С.Ж.Жалиштің қылмыстық іс әрекеттерін ҚК-нің 190-бабының 1-бөлігімен қайта саралап қылмыстық жауаптылықтан босатуды сұрағандары, оған қояр талап тілектері жоқ екендігінді көрінеді. Бұл өтініштер бойынша сотталушы С.Ж.Жалиштен қарсылықтар туындаған жоқ, керісінше олда осы өтініштердің негізінде жәбірленушілермен татуласып, оларға келтірген залалдың орнын толтыруына байланысты оны қылмыстық жауаптылықтан босатуды өтінді [5].

ҚК-нің 12-бабының 2-бөлігіне сәйкес егер адам бұрын жасаған қылмыстық құқық бұзушылығы үшін қылмыстық жауаптылықтан босатылған болса, қылмыстық құқық бұзушылық бірнеше рет жасалған деп танылмайды – делінген. Сонымен қатар, «Бөтеннің мүлкін заңсыз

иемдену жөніндегі істер бойынша сот тәжірибесі туралы» Қазақстан Республикасы Жоғарғы Сотының 2003 жылғы 11 шілдедегі N 8 нормативтік қаулысының 12 бөлігінде егер бұрын бөтеннің мүлкін заңсыз иемденген үшін адам сотталса, не заңда белгіленген негіздер бойынша қылмыстық жауапкершіліктен босатылса, бөтеннің мүлкін заңсыз иемдену бірнеше мәрте жасалды деп танылмайды [6].

«Қылмыстық құқық бұзушылықтардың бірнеше рет жасалуын және жиынтығын саралау туралы» Жоғарғы Сотының 2006 жылғы 25 желтоқсанындағы №11 Нормативтік Қаулысының 2 тармағына сай, егер адам заңда белгіленген негіздер бойынша қылмыстық жауаптылықтан босатылған болса, қылмыстық құқық бұзушылық бірнеше рет жасалған деп танылмайды делінген. Бөтеннің мүлкін бірнеше рет алаяқтықпен жымқыру іс әрекеттері бойынша ол қылмыстық іс әрекеттер қылмыстар жиынтығымен саралануына қарамай істі басты сот талқылауында қарау барысында әр қылмыстық құқық бұзушылық эпизоды бөлек дәлелденіп, бірінші эпизодтан бастап өз бетінше саралануы тиіс [7].

Бұл мән жайларға қарағанда С.Ж.Жалиш жасаған әрбір алдыңғы эпизодтағы қылмыстық құқық бұзушылығы бойынша ҚК-нің 68 бабының 1-ші белігінің талабына сай қылмыстық жауаптылықтан босатылуы тиіс болғандықтан, оған тағылған әр эпизод бойынша айып, өз бетінше саралануға жатады. Істі мұндай жағдайында сотталушы С.Ж.Жалиштің ҚК-нің 190 бабының 3-ші бөлігі 4) тармағымен сараланған қылмыстық құқық бұзушылық әрекеттері ҚК-нің 190 бабының 1-ші бөлігімен қайта саралануға жатады, өйткені ол алаяқтық, яғни бөтеннің мүлкін алдау және сеніміне қиянат жасау арқылы жымқырған. Сот сотталушы С.Ж.Жалиштың жасаған қылмыстық іс-әрекеттері ҚК-нің 11-бабының 2-бөлігі бойынша онша ауыр емес қылмыстар қатарына жататынын және ол жәбірленушілер З.Аязбековпен, Б.Бисакуловпен татуласып, келтірген зиянды қалпына келтіруіне байланысты қылмыстық жауаптылықтан босатылуға жатады. Сотталушы С.Ж.Жалиштың қылмыстық іс-әрекеттерінің әр көрінісі бойынша жеке-жеке жәбірленушілермен татуласып, қылмысымен келтірген зиянның есесін толтыруына байланысты қылмыстық жауаптылықтан босатылуға жатады. Қазақстан Республикасының Қылмыстық кодекстің 68-бабы 1-бөлігінің талаптарына сай, қазаға ұшыратумен байланысты емес онша ауыр емес, ауырлығы орташа қылмыс жасаған адам, егер ол жәбірленушімен, арыз берушімен татуласса және келтірілген зиянды қалпына келтірсе, қылмыстық жауаптылықтан босатылуға жатады деп көрсетілген. Сотталушы С.Ж.Жалишке қатысты жағдайда, сот оның жеке тұлғасын сипат-

тайтын деректерді, осы істің нақты мән-жайларын, сотталушы өзінің кінәсін толықтай мойындап, жасаған қылмыстары үшін шын жүректен өкінгенін, жәбірленушілердің өтініштеріндегі уәждерін ескеріп, оны ҚК-нің 68-бабының 1-бөлігінің негізінде ҚК-нің 1-бөлігімен қылмыстық жауаптылықтан босатылуға жатады деп санайды, себебі адамды ҚК-нің аталған бабымен қылмыстық жауаптылықтан босатуға негіз болып табылатын мән-жайлардың барлығы толық орын алған [8].

Осыған орай, соттың осы қылмыстық іс бойынша сотталушыға қатысты айыптау үкімін шығарып, С.Ж.Жалишты ҚК-нің 190-бабының 1-бөлігімен кінәлі деп танып, ҚК-нің 68-бабының 1-бөлігінің негізінде ол жәбірленушілермен татуласып, қылмысымен келтірілген зиянның есесін толтыруына байланысты, оны қылмыстық жазадан босатуға негіз болып табылады. Шымкент қаласының Әл-Фараби ауданының сотының 23.04.2021 жылғы үкімімен ҚК-тің 98-1 бабы және 98-2-бабы 3) тармағының талаптарына сәйкес, С.Жалиштен жәбірленушілер өтемақы қорына 20 АЕК көлемінде мәжбүрлі төлемді өндіру көзделгеніне орай, сол кезеңде жасаған қылмыстары үшін С.Жалиштен жәбірленушілер өтемақы қорына 20 АЕК мәжбүрлі төлемді қайта өндіру қажеті жоқ деп табады. Заттай дәлелдемелердің тағдыры ҚПК-нің 118-бабының негізінде шешілуге жатады. ҚПК-нің 387-390, 393, 395-398, 401 - баптарын басшылыққа алып, сот Үкім етті: Жалиш Сұлушаш Жадгерқызыны 190-бабының 1-бөлігімен кінәлі деп танып, ҚК-нің 68-бабы 1-бөлігі негізінде жәбірленушілер Аязбеков Заур Сабитовичпен және Бисакулов Бекжан Тагаевичпен татуласуына байланысты қылмыстық жазадан босатылсын. С.Ж.Жалишке қолданылған «ешқайда кетпеу және тиісті мінезқұлық туралы қолхат» түріндегі бұлтартпау шарасы, үкім заңды күшіне енген соң жойылсын [5].

П.А. Лупинская кінәні мойындау туралы мәмілеге тең емес деп санайды, өйткені ол прокурорға күдіктімен, айыпталушымен сотқа дейінгі келісім жасасу кезінде айыптау көлемін азайтуға қатысты дискрециялық өкілеттіктер бермейді және берілетін жеңілдіктер қылмыстық іс қозғау айыптаушының басқаға берілуі және прокурордың осы адаммен тиісті «мәмілесі» нәтижесінде, ал қылмыстық және қылмыстық іс жүргізу заңнамасының тікелей көрсетілуіне байланысты [9, 269 б.].

Процестік келісім аясында іс жүргізудің ұтымды жағын айта келе В.И. Самарин, бүгінгі таңда тек құқық қорғау органдары мен қылмыстық қудалау органдарының қызметіне ғана арқа сүйеп қылмыстылықтың көптігіне тиімді түрде қарсы тұру мемлекетке қиын екендігіне назар ау-

дарады. Процестік келісімнің енгізілуі, іс бойынша сотқа дейінгі тергеп-тексеруді ғана емес, сондай-ақ сотта іс жүргізуді де едәуір жеңілдетеді және процестік мүмкіндіктерді ауыр және аса ауыр қылмыстар бойынша қолдануды көздейді [10, 23 б.].

А.В. Смирнов және К.Б. Калиновский атап көрсеткендей, жалпы теориялық тұрғыда жеделдетілген және жеңілдетілген сот ісін жүргізу – бұл қылмыстық істерді қысқа мерзімде және жеңілдетілген тәртіпте шешу бойынша қылмыстық процестің нысандары [11, 235 б.].

Процестік келісімнің мақсаты тергеу әрекеттерін жеңілдету болса және күдікті немесе айыпталушы кінәсін мойындап, жинақталған дәлелдермен келісе отырып, процестік келісімге қол қойылғаннан кейін қосымша дәлелдер жинаудың қажеттігі жоқ деген пікірдеміз. Процестік келісім институты болашақта қылмыстық іс жүргізу тәжірибесіне оң нәтиже береді деп санаймыз.

Пайдаланылған қайнар көздерінің тізімі:

1. Соттардың қылмыстық істер бойынша келісімдік тәртіпте іс жүргізу практикасы туралы Қазақстан Республикасы Жоғарғы Сотының 2016 жылғы 7 шілдедегі № 4 Нормативтік қаулысы// Электронды ресурс: <https://adilet.zan.kz>

2. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. // Электронды ресурс: <https://adilet.zan.kz>

3. Қазақстан Республикасының Бас прокуратурасы құқықтық статистика және арнайы есепке алу жөніндегі комитетінің мәліметіне сәйкес, Қазақстан Республикасында №1 нысаны “Бірінші сатыдағы соттың қылмыстық істерді қарауы жөніндегі жұмысы туралы”// Электронды ресурс: <https://adilet.zan.kz>

4. Маңғыстау облысы Ақтау қалалық соты №4710-20-00-1/50Үкімі. 05.02. 2020 жыл.

5. Шымкент қаласының Еңбекші аудандық соты №5112-21-00-1/148 Үкімі. 08.06. 2021 жыл.

6. «Бөтеннің мүлкін заңсыз иемдену жөніндегі істер бойынша сот тәжірибесі туралы» Қазақстан Республикасы Жоғарғы Сотының 2003 жылғы 11 шілдедегі N 8 нормативтік қаулысы// Электронды ресурс: <https://adilet.zan.kz>

7. «Қылмыстық құқық бұзушылықтардың бірнеше рет жасалуын және жиынтығын саралау туралы» Жоғарғы Сотының 2006 жылғы 25 желтоқсанындағы №11 Нормативтік Қаулысы// Электронды ресурс: <https://adilet.zan.kz>

8. Қазақстан Республикасының Қылмыстық кодексі Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. // Электронды ресурс: <https://adilet.zan.kz>

9. Уголовно-процессуальное право Российской Федерации: Учебник / Отв. ред. П.А. Лупинская. 2-е издание. –М.: Норма: Инфра-М, 2010. – 770 с.

10. Самарин В.И. Введение согласительных начал для сотрудничества в правоотношениях между органами уголовного преследования с обвиняемыми (подозреваемыми) в Республике Беларусь и Республике Казахстан // Хабаршы-Вестник КазНПУ им.Абая им.Абая, Серия «Юриспруденция». – No 4(38). – 2014. – С. 23-27.

11. Смирнов А.В., Калиновский К.Б. Уголовный процесс: Учебник. – СПб.: Питер, 2007. – 697 с.

УДК 34.09

Абишев Аскар Шапыкович

студент 3 курса юридического факультета

по специальности «Юриспруденция»

Казахский национальный университет имени аль-Фараби

Республика Казахстан, г. Алматы

ВЛИЯНИЕ ИНТЕРНЕТА И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРАВА ЧЕЛОВЕКА

Научный руководитель:

Калишева Н.Х.

д.ю.н, профессор,

Юридический факультет,

КазНУ им.аль-Фараби

Аннотация

В данной статье автор рассматривает особенность правового регулирования интернета и искусственного интеллекта. Обращено внимание на сложность правового регулирования и в чем данная сложность выражается. Изучено интернет право с позиции будущего и главной отрасли права. Автор изучил опыт зарубежных стран, и то, как другие страны

пытаются регулировать сложные аспекты интернета и искусственного интеллекта. Рассмотрена важность искусственного интеллекта и нашего правового будущего.

Ключевые слова: интернет, пользователь, право, искусственный интеллект, правовое регулирование, авторское право, интернет право

Әбішев Асқар Шапықұлы

Заң факультетінің 3 курс студенті “Құқықтану” мамандығы бойынша
Әл-Фараби атындағы Қазақ ұлттық университеті
Қазақстан Республикасы, Алматы қ.

ИНТЕРНЕТ ПЕН ЖАСАНДЫ ИНТЕЛЛЕКТТІҢ АДАМ ҚҰҚЫҚТАРЫНА ӘСЕРІ

Аңдатпа

Бұл мақалада автор интернет пен жасанды интеллектті құқықтық реттеудің ерекшеліктерін қарастырады. Құқықтық реттеудің күрделілігіне және бұл күрделіліктің қалай көрінетініне назар аударылады. Интернет құқығы болашақ және құқықтың негізгі саласы тұрғысынан зерттелді. Автор шет елдердің тәжірибесін және басқа елдердің интернет пен жасанды интеллекттің күрделі аспектілерін реттеуге тырысып жатқанын зерттеген. Жасанды интеллекттің маңыздылығы және біздің құқықтық болашағымыз қарастырылады.

Түйінді сөздер: Интернет, пайдаланушы, заң, жасанды интеллект, құқықтық реттеу, авторлық құқық, интернет құқығы.

Abishev Askar Shapykovich

3rd year student of the Faculty of Law,
specialty “Jurisprudence”

Al-Farabi Kazakh National University, Republic of Kazakhstan, Almaty

THE IMPACT OF THE INTERNET AND ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS

Abstract

In this article, the author examines the peculiarities of the legal regulation of the Internet and artificial intelligence. Complexity of legal regulation. How does this difficulty manifest itself? Internet law as the future and main branch of law. How other countries are trying to regulate complex aspects of the Internet and artificial intelligence. The importance of artificial intelligence and our legal future.

Keywords: internet, user, law, artificial intelligence, legal regulation, copyright, internet law

Огонь, колесо, лапочки и интернет - что объединяет все эти открытия и изобретения? В первую очередь важность для человека и цивилизации. Конечно, существуют множество и других важных открытий, и изобретений, которые дало толчок для человека, цивилизации и государства, но их перечисление может изрядно затянуться.

Мы считаем, что интернет – это своего рода государство. «Интернет-пользователи в мире: в начале 2022 года численность интернет-аудитории достигла 4,95 млрд пользователей. Сегодня интернетом пользуются 62,5% населения мира.» - Global Digital Insights [1]. С каждым годом, число пользователей интернета растет, что лишь подтверждает масштабы самого интернета.

Чтобы разобраться, почему Я считаю, что интернет – это своего рода государства, нужно разобрать признаки государство. Признаками государство являются:

- наличия публичной власти. У самого интернета нет власти, особенной публичной. Хотя и государственная власть имеет своего рода инструменты для публичного управление, то этого недостаточно. Власть то или иной степени, осуществляют сами пользователи. Миллионы сайты, где власть осуществляют владельцы сайтов, модераторы, администраторы и так далее. При этом, обыкновенные пользователи тоже имеют свою власть. Бойкоты, установление правил и банально самому стать владельцем, модератором или администратором.

- *административно-территориальная организация.* Многие наверняка думают, что у интернета нет своей территории, в целом – это правда. Только вот, привычные понимания «территории» у интернета нет, но вот если мы расширим понятие, то можно по-разному трактовать эти границы. Весь мир, где есть интернет можно назвать границей, отдельные сайты имеет свои границы, да и сам цифровое пространство имеет границы, только эти границы не материальные, а цифровые.

- *регулярный сбор налогов.* В этом тоже вопрос довольно спорный, с одной стороны, у интернета нет налогов, но только вот мы платим за интернет, берем различные сервисные подписки и так далее. Они могут выступать роль налога, только вот налоги выплачиваются государство, а вот для интернета мы платим юридическим лицам, которые осуществляют услуги.

- Суверенитет. У интернета есть своего рода суверенитет. Интернет по-своему независим, хотя и способен быть заблокирован государственными властями.

Хоть и признаки присущие для государства, интернету отчасти под-ходят, точнее стоит высказать по-другому: «Интернет по-своему раскрывает признаки, присущие государству». Хотя и подойдет иной взгляд на это. Интернет – своего рода ранняя стадия перехода из физической цивилизации в киберпространство. Перед тем, как разобрать данная высказывание, нужно понять, что такое «киберпространство». Впервые о киберпространстве написал канадский писатель – фантастик Уильям Гибсон в «пророческом» рассказе «Сожжённый хром», опубликованный в *Omni* 1982 год. Киберпространство — особое представление пространства, виртуальная реальность. Его основу представляет трёхмерная решетка типа кристаллической, в которой встречаются вкрапления данных в виде объёмных цветных геометрических фигур разной формы [2]. Данный термин в наше время сильно отличается от того, что писал Уильям Гибсон. Сейчас киберпространство — метафорическая абстракция— второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей. Интернет сам по себе, не является киберпространством, но вот для как первой идеи или первым шагом – да.

С учетом того, что компания «MetaPlatforms, Inc» уже создала очки «дополненной реальности» [3], а ряд иных компаний улучшают очки «виртуальной реальности», то возможные идеи, которые проскальзывали в различных произведенный вполне возможны.

Если говорить про правовое регулирование интернета, то тут все сложно. Я считаю, что полностью или даже на половину регулировать интернет невозможно. Можно начатать с банального авторского права. Согласно статьи 198 УК РК «Нарушение авторских и (или) смежных прав» нарушается многими, при этом не несут за это наказание. Причин может быть много, такие как:

1) Незнание законодательства. Многие просто напросто не знают, что нарушают так чьи-то прав и про существование данной санкции:

2) Сложность доказывания. В некоторых случаях бывает сложно доказать, что именно данное лицо совершило нарушение авторских прав;

3) Неэффективность правоприменительной практики. В Казахстане пока еще не сложилась эффективная практика по борьбе с нарушением авторских прав.

Нарушение могут быть разными: скачивание видеоигр без оплаты, прослушивание музыки в обход закона и так далее

Помимо этого, если говорить про иерархию правового регулирования в интернете, то оно значительно отличается от регулирования во многих странах. По сути, регулирование в разных социум или групп,

которые собираются в интернете занимается сам социум, где были созданы негласные правила или же «пользовательским соглашением». Пользовательское соглашение – своего рода договор, где пользователь соглашается на установление правила с владельцем. Хоть право государств имеет значение, только вот во многих сегментах, пользователи игнорируют данное право, предпочитая правила, которые установил социум.

На самом деле существует такой термин, как «интернет – право». Американский юрист Роберт Дж. Амброги считает, что «интернет-право — это динамичная, гибкая и неизведанная сфера юридической практики, границы которой ещё предстоит определить. В настоящее время это даже трудно назвать отраслью права — это скорее смесь теории и практики из интеллектуальной собственности, гражданских прав и свобод, имущественного, уголовного, телекоммуникационного, коммерческого, международного торгового и частного права»[4].

С 2021 года, в широкую доступность пришли такие понятия как, «искусственный интеллект» и «нейросеть». Искусственный интеллект — это отрасль информатики, которая занимается созданием интеллектуальных агентов, которые могут разумно действовать и принимать решения в различных ситуациях. Интеллектуальный агент — это система, которая может воспринимать свое окружение и принимать действия, которые резко и намного увеличивают ее шансы на достижение своих целей. А Нейросеть — это тип алгоритма машинного обучения, который имитирует структуру и функции человеческого мозга. Нейросети состоят из множества связанных узлов, которые могут обрабатывать информацию и учиться на ней. В дальнейшем искусственный интеллект и нейросеть будут указаны как, «и.и.». И.и. для авторов стал, своего рода помощник или инструмент в творческой деятельности[5].

Самая главная особенность и.и. заключается в ее языковой модели. Весь текст, который способен генерировать «ChatGPT» во многом имитирует человеческую речь и умеет грамотно – структурированно подносить текст. Раньше, существовали текстовые боты, способные сформулировать текст, только вот у нее было два главных изъяна:

- 1) Отсутствие нейросети. Главная особенности современного и.и., заключается в наличии «нейросети», которая позволяет более точно искать информацию, которую запросил пользователь.

- 2) Языковая модель. В то время, текстовый бот, очень плохо формулировал текст и мысль, он требовал полной редактуры.

Для право, и.и. является чем-то новым и неизвестным. С учетом того, что с интернетом есть проблемы с правовым регулированием, то и искусственным интеллектом их еще больше.

В целях научных исследований, Я решил спросить у чат бота, который работает на основе исходного кода «ChatGPT 4.0.», под названием «GoogleBardAI»

Вопрос: *«В чем проблема правового регулирования искусственного интеллекта и как ее решить?»*. Ответ от «GoogleBardAI»: *«Проблема правового регулирования искусственного интеллекта заключается в том, что действующее законодательство не всегда применимо к новым технологиям, основанным на искусственном интеллекте. Это приводит к тому, что возникают юридические коллизии и неопределенности, которые могут помешать развитию искусственного интеллекта и создать риски для общества.*

К числу основных проблем правового регулирования искусственного интеллекта можно отнести следующие:

Неопределенность правовой природы искусственного интеллекта. Неясно, является ли искусственный интеллект субъектом права или объектом права. Это влияет на то, какие права и обязанности могут иметь системы искусственного интеллекта, а также на то, кто должен нести ответственность за их действия.

Несоответствие действующего законодательства новым технологиям, основанным на искусственном интеллекте. Многие существующие законы и нормы были разработаны в условиях, когда искусственный интеллект еще не был широко распространен. В результате они могут не учитывать особенности искусственного интеллекта и создавать препятствия для его развития.

Возможность злоупотребления искусственным интеллектом. Искусственный интеллект может быть использован для совершения противоправных действий, таких как распространение дезинформации, мошенничество или киберпреступления. Правовое регулирование должно быть направлено на предотвращение таких злоупотреблений.

Для решения проблемы правового регулирования искусственного интеллекта необходимо:

Разработать единый подход к правовой природе искусственного интеллекта. Это позволит определить, какие права и обязанности могут иметь системы искусственного интеллекта, а также на то, кто должен нести ответственность за их действия.

Принять новые законы и нормы, которые будут соответствовать новым технологиям, основанным на искусственном интеллекте. Эти законы и нормы должны учитывать особенности искусственного интеллекта и способствовать его развитию.

Разработать меры по предотвращению злоупотребления искусственным интеллектом. Эти меры должны включать в себя как технические, так и правовые инструменты.» [6].

Если говорить о том, как в других странах пытаются урегулировать и.и., то вот, опланах по ужесточению регулирования сферы и.и. недавно сообщил в Евросоюзе. Еврокомиссар по внутреннему рынку Тьерри Бретон заявил, что нейросети могут использоваться в целях мошенничества и плагиата. В Брюсселе обсуждают законопроект об искусственном интеллекте, который должен снизить риски. Ожидается, что он вступит в силу в этом году[7]

Пока до конца не решена и проблема авторских прав. В Великобритании права на произведения, сгенерированные ИИ, принадлежат тому, кто принял меры для его создания. Закон Австралии прямо указывает, что автором может быть лишь «квалифицированное лицо» – определение, под которое, очевидно, не подпадает нейросеть. Аналогичная ситуация и в Канаде. Вопрос о творчестве ИИ прицельно рассматривает японское законодательство. В стране предлагают ограничить охрану сгенерированных нейросетями произведений и приравнять их к товарному знаку. При таком подходе владельцем прав на цифровые работы становится создатель соответствующего алгоритма. Дипфейки ограничивают в Китае. Здесь с 10 января 2023 года применяют правила, введенные Администрацией киберпространства КНР. Дипфейки допускаются только при условии, что они сгенерированы с разрешения самого субъекта, не несут вредоносную информацию и имеют маркировку о создании с помощью искусственного интеллекта[7].

Часто в обсуждениях можно услышать, что и.и. скоро заменит: художников, программистов, дизайнеров, юристов и так далее. Лично Я, отчасти буду согласен с данным мнением, но есть несколько важных факторов. И.и. способен красиво рисовать, но профессиональный художник заметить много недочетов. И.и. так же, может писать «код для программирование», но нужен программист, который сможет заметить множество недочетов. И.и. сможет составить хороший дизайн, но не сможет его применить так, как сможет сам дизайнер. И.и. может дать толкование закону, но не может ссылаться на правильную статью и не всегда в целом толкует закон правильно. Все идет к тому, что без самих специалистов,

и.и может что-то составить, создать или придумать, только вот все это благодаря нейросети, из существующих данных формулирует тот или иной запрос, но с специалистом можно сделать лучше или даже придумать что-то новое. Возможно, в будущем, и.и. сможет выполнять такие функции в разы лучше.

Если говорить о том, может ли и.и. сейчас заменить суды, адвокатов, прокуроров или других юристов? На данном этапе – нет. Но вот в будущем, такой сценарий возможен. У и.и. есть одно преимущество перед нами, а именно в отсутствии эмпатии. В целом, Я считаю, что юристом такая черта, как «эмпатия» лишняя и даже мешает. Юрист должен отталкиваться своим умом и рациональным состраданием.

Под конец, данный научной статьи, я хочу сказать, что и.и. пока что находится лишь на раннем этапе развития. И.и. хоть и не похож на то представление, которое есть в фильмах, книгах или играх, но стремительно Он развивается.

И.и. уже стучит в наши двери, мы можем его игнорировать, но тогда эту дверь он выбьет. Вместо того, чтобы пытаться его игнорировать, нужно подойти к двери, открыть ее и поприветствовать искусственный интеллект.

Список использованных источников:

1. Global Digital Insights. Статистика пользователь в интернете 2022 года – Режим доступа: <https://datareportal.com/>

2. Добринская Д.Е., канд. социол. наук, доц. кафедры современной социологии социологического факультета МГУ имени М.В. Ломоносова, Л. Киберпространство: территория современной жизни – Режим доступа: <https://vestnik.socio.msu.ru/jour/article/view/363/268>

3. Meta. Современные устройства дополненной реальности – Режим доступа: <https://about.meta.com/>

4. Уголовный кодекс РК по состоянию 12.09.2022 - Режим доступа: https://online.zakon.kz/Document/?doc_id=31575252&pos=3099;-47#pos=3099;-47

5. Материал из Википедии. Интернет право – Режим доступа: <https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE>

6. Google Bard AI. Вопрос и ответ искусственному интеллекту, в целях научной статьи – Режим доступа: <https://bard.google.com/>

7. EXlibris. Как регулируют искусственный интеллект в разных странах – Режим доступа: <https://exlibris.ru/news/kak-reguliruyut-iskusstvennyj-intellekt-v-raznyh-stranah/>

УДК 349

Ақтан Әділет

Студент 1 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ

Аннотация

Данная статья посвящена актуальной проблеме киберпреступности, видам, способом цифровых правонарушений, а так же существующих способах защиты от утечки информации, фишинга, хакинга. Анализ современных вызовов и угроз в области кибербезопасности становится все более актуальным в современном информационном обществе. Рассматриваются основные виды киберпреступности, их последствия для общественности и государства, также предлагаются стратегии защиты и меры для борьбы с данными угрозами. Так же статья представляет собой обзор ныншних законов, международных соглашений, а также определения цифровых терминов и усовершенствования нынешних законов для успешной борьбы с хакерами

Ключевые слова: киберпреступность, хакер, глобализация, дигитализация, общественная опасность.

Ақтан Әділет

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

КИБЕРҚЫЛМЫСТЫЛЫҚ МӘСЕЛЕЛЕРІ

Аңдатпа

Бұл ғылыми мақала киберқылмыстың өзекті мәселесіне, цифрлық қылмыстардың әдістеріне, сондай-ақ ақпараттың таралып кетуінен, фишингтен, хакингтан қорғаудың қолданыстағы әдістеріне арналған. Киберқауіпсіздік саласындағы заманауи сын-қатерлер мен қауіп-қатерлерді талдау қазіргі ақпараттық қоғамда өзекті бола түсуде. Кибер

қылмыстың негізгі түрлері, олардың қоғам мен мемлекетке тигізетін зардаптары қарастырылып, сондай-ақ осы қауіптермен күресу бойынша қорғаныс стратегиялары мен шаралары ұсынылады. Мақала сонымен қатар қазіргі заңдарға, халықаралық келісімдерге шолу жасайды, сондай-ақ цифрлық терминдердің анықтамалары мен хакерлермен сәтті күресу үшін қолданыстағы заңдарды жақсартуларды ұсынады.

Түйінді сөздер: киберқылмыс, хакер, жаһандану, цифрландыру, қоғамдық қауіп.

Aktan Adlet

1st year student of High School of Law “Adilet”
Caspian Public University
Republic of Kazakhstan, Almaty

CYBERCRIME PROBLEMS

Annotation

This scientific work is devoted to the current problem of cybercrime, its problems, types, methods of digital crimes, as well as existing methods of protection against information leakage, phishing, and hacking. Analysis of modern challenges and threats in the field of cybersecurity is becoming increasingly relevant in the modern information society. The main types of cybercrime, their consequences for the public and the state are considered, and protection strategies and measures to combat these threats are also proposed. The work also provides an overview of current laws, international agreements, as well as definitions of digital terms and improvements to current laws to successfully combat hackers

Key words: cybercrime, hacker, globalization, digitalization, public danger.

В современном мире информация занимает одно из самых важных и ключевых мест в нашей жизни, с каждым годом значимость информации и ее количество лишь растет, а также пропорционально с этим и растет риск стать жертвой хакера. Процессы глобализации, в том числе и глобализации цифровой раскрывают новые возможности воздействовать и влиять на личность, одно из них – киберпреступления. Чем большее значение начинает иметь информационные технологии, тем больше требуется защита и правовое регулирование в этой сфере.

Проблема киберпреступности актуализировалось в эпоху «всемирной паутины», когда телекоммуникации, компьютеры и всякие гаджеты

захватили все сферы нашей жизни. Вмешательства в цифровые системы приводят к серьезным последствиям для государств, корпораций и индивидуальных пользователей. Во несколько реальных проблем, которые создают опасность в информационном пространстве:

1) Киберпреступники все чаще направляют свои атаки на государственные институты и критическую инфраструктуру. Атаки на электронные системы связи, энергетические сети и военные объекты создают потенциальную угрозу для национальной безопасности и стабильности стран.

2) С увеличением объема цифровой информации, хранящейся онлайн, киберпреступники все активнее совершают атаки с целью кражи личных данных. Это не только угрожает финансовой стабильности индивидов, но также нарушает их право на приватность.

3) Кибератаки приносят значительные экономические убытки. Корпорации теряют миллионы долларов из-за кражи корпоративной информации, шантажа и прерывания бизнес-процессов. Это оказывает негативное воздействие на экономику в целом.

4) Киберпреступность также оказывает воздействие на социальные структуры и взаимоотношения. С угрозой кибершпионажа и манипулирования информацией возникает риск искажения общественного мнения и даже вмешательства в политические процессы.

В свете этих факторов проблема киберпреступности становится более значимой, подчеркивая необходимость срочных и эффективных мер для обеспечения кибербезопасности в современном цифровом обществе.

«Информационная преступность (киберпреступность)» - вид уголовной преступности, подразумевающий уголовно-наказуемые деяния, совершаемые с использованием информационных технологий. В настоящее время в действующих нормативно-правовых актах отсутствует четкое определение киберпреступности, в связи с чем имеются трудности в едином понимании сущности данного негативного явления, и как следствие возникают проблемы в определении целей и задач для соответствующих подразделений по борьбе с киберпреступлениями.

Вред от хакеров часто несет за собой огромный экономический ущерб. По экспертным оценкам, потери от киберпреступлений достигнут \$10,5 трлн в 2025 году, по итогам 2022 их оценивают на уровне \$8 трлн в год. В России в 2022 году прогнозировались потери на уровне 165 млрд руб., однако обострение геополитической обстановки и ставший следствием шквал атак удвоили потери бизнеса и граждан. Поэтому на сегодняшний день важно противостоять дей-

ствиям киберпреступности как на уровне политики государства и повышения защищенности критически важных объектов, так и на уровне каждого жителя страны за счет соблюдения необходимых правил цифровой гигиены.

В Казахстане, как и во многих странах, проблема киберпреступности рассматривается в контексте законодательных норм и мер по обеспечению кибербезопасности. Законодательная база в области киберпреступности в Казахстане развивается с учетом динамичных изменений в цифровой сфере.

В 2017 году был принят закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационных технологий и защиты информации», который стал важным шагом в направлении укрепления кибербезопасности. Закон устанавливает ответственность за незаконный доступ, использование и распространение информации, нарушающей права и интересы субъектов информационных отношений. Согласно законодательству Казахстана, киберпреступления включают в себя действия, направленные на нарушение нормального функционирования информационных систем, несанкционированный доступ к компьютерным данным, а также создание и использование вредоносных программ. Законодательство также предусматривает ответственность за кибертерроризм, включая атаки на критическую информационную инфраструктуру. Дополнительные законодательные инициативы продолжают с целью совершенствования правовой базы в соответствии с развитием киберугроз и технологий. Это отражает стремление Казахстана к созданию современной и эффективной системы противодействия киберпреступности и обеспечения кибербезопасности национального уровня. Но этого недостаточно так как со временем способы кибератак совершенствуются и недостаточно существующих мер безопасности и существующего правового регулирования.

С точки зрения криминалистики, киберпреступность рассматривается в нескольких аспектах и включает такие основные категории как преступления как неправомерный доступ к компьютерной информации, распространение вредоносного программного обеспечения, компьютерные хакерские атаки, распространение клеветнической, экстремистской, порнографической и иной незаконной информации, незаконная обработка, передача и хранение информации и т.д.

Эксперты-криминалисты, проводя криминалистические экспертизы, часто сталкиваются с проблемой классификации киберпреступлений. В

частности, в борьбе с киберпреступностью возникают существенные проблемы при установлении факта преступления и незаконных действий в отношении создателей вредоносного вирусного программного обеспечения. На данный момент в системе криминалистической экспертизы отсутствуют критерии оценки и идентификации аутентичной информации, что является потенциальной угрозой для внедрения вирусного ПО.

Система оценки общественной опасности киберпреступлений должна быть основана на учете вреда, причиненного охраняемым законом интересам всех пользователей сетевых ресурсов, а также на своевременности демаскировки преступного замысла правоохранительными органами. Центральным элементом критической информационной инфраструктуры каждого государства остается пользователь компьютерных систем, и именно пользователь наименее защищен уголовным законодательством в процессе цифровой трансформации всех сфер жизни общества.

В свете быстрого развития цифровых технологий и их неотъемлемой роли в современном обществе, проблема киберпреступности становится все более острой и актуальной. В ходе настоящего исследования мы проанализировали современные тенденции в киберпреступности, рассмотрели технологические и правовые аспекты противодействия, а также рассмотрели стратегии борьбы с этим вызовом. Одним из ключевых выводов является неотложная необходимость разработки и внедрения более сложных и инновационных методов защиты. Использование искусственного интеллекта и машинного обучения, современных технологий шифрования и систем анализа трафика становятся необходимым шагом в направлении эффективного предотвращения и обнаружения кибератак. Существенная роль отводится правовому полю, и в этом контексте важна активная деятельность в сфере развития законодательства о кибербезопасности. Строгие нормы и правовые меры для пресечения киберпреступности должны соответствовать быстрому развитию технологий и разнообразию схем атак.

Сегодняшняя динамичная картина киберпреступности требует от нас постоянного обучения, адаптации и инноваций в сфере кибербезопасности. Только через совместные усилия государств, бизнеса, исследовательского сообщества и общества в целом мы сможем сделать цифровое пространство более безопасным и устойчивым к вызовам киберпреступности.

УДК 349

Аламан Алихан Аскаревич
Студент 2 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ: ПОНЯТИЕ, ПРОБЛЕМЫ, РЕШЕНИЯ ПРОБЛЕМЫ И ПРИМЕНЕНИЕ В ТРУДОВОМ ПРАВЕ

Аннотация

Актуальность вопросов кибербезопасности в современном информационном обществе выдвигает эту тему на передний план в контексте трудовых отношений. Данная статья исследует понятие безопасности в Интернете, выявляя ключевые проблемы, с которыми сталкиваются работники, и предоставляет эффективные решения на основе современных практик. Рассмотрены реальные примеры киберугроз, такие как кибератаки, утечки данных и недостаточная осведомленность, а также предложены меры по их предотвращению и соблюдению в рамках трудового права. Статья призвана подчеркнуть необходимость внимания к кибербезопасности в корпоративной среде и предоставить четкие рекомендации для создания устойчивой и безопасной рабочей обстановки в эпоху цифровых технологий.

Ключевые слова: интернет, трудовое право, трудовые отношения, безопасность, кибербезопасность, кибер угроза, корпоративная среда.

Аламан Әлихан Асқарұлы
«Әділет» Жоғары құқық мектебінің
2 курс студенті
Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қ.

**ИНТЕРНЕТ ҚАУІПСІЗДІГІ ШАРАЛАРЫ:
ЕҢБЕК ҚҰҚЫҒЫНДАҒЫ ТҮСІНІГІ, МӘСЕЛЕЛЕРІ, ПРОБЛЕМАЛЫҚ
ШЕШІМДЕРІ ЖӘНЕ ҚОЛДАНЫЛУЫ**

Аңдатпа

Қазіргі ақпараттық қоғамдағы киберқауіпсіздік мәселелерінің өзектілігі бұл тақырыпты еңбек қатынастары контекстінде бірінші орынға шығарады. Бұл мақала желідегі қауіпсіздік тұжырымдамасын зерттейді, жұмысшылар алдында тұрған негізгі мәселелерді анықтайды және ағымдағы тәжірибеге негізделген тиімді шешімдерді ұсынады. Кибершабуылдар, деректердің ағып кетуі және хабардар болмауы сияқты киберқауіптердің өмірден алынған мысалдары зерттеліп, еңбек заңнамасы аясында олардың алдын алу және сақтау шаралары ұсынылады. Мақала корпоративтік орталардағы киберқауіпсіздікке назар аудару қажеттілігін көрсетуге және цифрлық дәуірде тұрақты және қауіпсіз жұмыс ортасын құру үшін нақты нұсқаулар беруге бағытталған.

Түйінді сөздер: интернет, еңбек құқығы, еңбек қатынастары, қауіпсіздік, киберқауіпсіздік, киберқауіп, корпоративтік орта.

Alaman Alikhan Askarovich

2nd year student

Higher School of Law “Adilet”

Caspian Public University

Republic of Kazakhstan, Almaty

**INTERNET SECURITY MEASURES:
CONCEPT, PROBLEMS, PROBLEM SOLUTIONS
AND APPLICATION IN LABOR LAW**

Annotation

The relevance of cybersecurity issues in the modern information society brings this topic to the forefront in the context of labor relations. This article explores the concept of online security, identifying key issues facing workers and providing effective solutions based on current practices. Real-life examples of cyber threats such as cyber-attacks, data leaks and lack of awareness are examined, and measures for their prevention and compliance within the framework of labor law are proposed. The article aims to highlight the need for attention to cybersecurity in corporate environments and provide clear guidelines for creating a resilient and secure work environment in the digital age.

Key words: Internet, labor law, labor relations, security, cybersecurity, cyber threat, corporate environment.

1. Введение:

В современном информационном обществе, где цифровые технологии проникают в каждый аспект повседневной жизни, вопросы безопасности в Интернете становятся неотъемлемой частью деятельности организаций и их сотрудников. Развитие цифровых систем и сервисов внесло ряд новых вызовов в обеспечение безопасности информации, а также повлияло на трудовые отношения.

2. Понятие безопасности в Интернете:

Безопасность в Интернете охватывает меры, предназначенные для защиты информации, личных данных, а также обеспечения нормального функционирования

В современном информационном обществе, где цифровые технологии прочно вошли в наш повседневный образ жизни, вопросы безопасности в Интернете становятся все более актуальными. Работники в трудовых отношениях также ощущают влияние цифровой среды на свою деятельность и личные цифровых систем и сервисов.

3. Проблемы:

Кибератаки и утечки данных: Рост угроз со стороны злоумышленников, направленных на кражу или разрушение данных.

Недостаточная осведомленность: Многие работники не обладают достаточными знаниями по вопросам кибербезопасности.

Личная ответственность: Недостаток ясных стандартов и регуляций о том, кто несет ответственность за кибербезопасность в трудовых отношениях.

4. Решение проблемы:

Образование и обучение: Для эффективной борьбы с угрозами кибербезопасности в трудовых отношениях ключевым шагом является образование и обучение персонала. Компании могут предоставить сотрудникам специализированные обучающие курсы по кибербезопасности, адаптированные к их конкретным рабочим условиям. Примером может служить внедрение онлайн-платформы обучения, где сотрудники могут проходить курсы по распознаванию фишинговых атак, управлению паролями, обеспечению безопасности рабочего оборудования и другим вопросам.

Пример: Представим, что компания X, специализирующаяся на разработке программного обеспечения, столкнулась с повышенным уровнем утечек конфиденциальной информации из-за недостаточной осведомленности сотрудников. Для решения этой проблемы, компания X запустила обучающую плат-

форму по кибербезопасности, доступную всем сотрудникам. Курсы включали в себя реальные случаи киберугроз, методы их предотвращения, а также практические уроки по безопасному обращению с корпоративной информацией. В результате сотрудники получили необходимые знания и навыки, что привело к снижению случаев утечек данных. Разработка политики безопасности: Компании также должны разработать и внедрить четкую политику безопасности, которая охватывает все аспекты кибербезопасности в трудовых отношениях. Это включает в себя определение правил для обработки конфиденциальной информации, использования корпоративных устройств, аутентификации и авторизации, а также меры санкций за нарушение этих правил.

5. Применение в трудовом праве:

Конфиденциальность информации: Работники должны соблюдать правила обработки конфиденциальной информации.

Предотвращение утечек данных: Внедрение технических средств и политик, направленных на предотвращение утечек корпоративных данных.

6. Как люди часто сталкиваются с этим в трудовом праве:

Удаленная работа: С ростом удаленной работы возрастают риски киберугроз, так как сотрудники используют собственные устройства и сети.

Личные данные сотрудников: Хранение и обработка личных данных сотрудников требует повышенного внимания к безопасности.

7. Пред Заключительная часть:

Безопасность в Интернете становится важным компонентом трудовых отношений, требующим системного подхода. Обучение сотрудников, разработка политики безопасности и применение современных технологий становятся ключевыми мерами для минимизации рисков и обеспечения устойчивого функционирования корпоративной среды. Регулирование в области трудового права также должно соответствовать вызовам цифровой эры, защищая интересы работников и предприятий в условиях современных киберугроз.

8. Реальные примеры:

Проблема 1: Кибератаки и утечки данных

- **Пример:** В 2020 году, компания X стала жертвой кибератаки, в результате которой злоумышленники получили доступ к базе данных с личной информацией клиентов. Это привело к утечке чувствительных данных, включая адреса, номера телефонов и финансовую информацию.

Проблема 2: Недостаточная осведомленность

- **Пример:** Сотрудники компании Y не проходили обучение по кибербезопасности, и, не осознавая риски, использовали слабые пароли и открывали вредоносные электронные письма. Это стало причиной успешной фишинговой атаки, в результате которой злоумышленники получили доступ к корпоративным системам.

Проблема 3: Личная ответственность

- **Пример:** Сотрудник Z не соблюдал правила безопасности, сохраняя корпоративные пароли в открытом доступе на своем рабочем столе. Когда его компьютер был украден, это привело к несанкционированному доступу к корпоративной сети и потере конфиденциальных данных.

Решение 1: Образование и обучение

- **Пример:** Компания W внедрила систему регулярных тренингов по кибербезопасности для своих сотрудников. В результате уровень осведомленности повысился, и число успешных кибератак значительно уменьшилось.

Решение 2: Разработка политики безопасности

- **Пример:** Организация V разработала строгую политику безопасности, включая требования к сложности паролей, двухфакторной аутентификации и обязательному обновлению антивирусных программ. Это уменьшило риски внутренних угроз и атак.

Применение в трудовом праве: конфиденциальность информации

- **Пример:** Сотрудник компании U был уволен за нарушение политики конфиденциальности, поскольку он передал корпоративные данные третьим лицам без разрешения, что привело к утечке коммерческой информации.

Применение в трудовом праве: предотвращение утечек данных

- **Пример:** Компания Q внедрила систему мониторинга активности сотрудников для выявления подозрительной активности и своевременного предотвращения утечек данных.

9. Заключение:

Реальные примеры подчеркивают важность эффективных мер по обеспечению безопасности в Интернете в трудовых отношениях. Успешные практики, такие как обучение, разработка политики безопасности и соблюдение законов труда, демонстрируют, как организации могут минимизировать риски и обеспечить безопасное использование цифровых технологий в рабочей среде.

Список использованных источников:

1. Безопасность персональных данных: новый взгляд на старую проблему 2022 / Минзов Анатолий Степанович, Невский Александр Юрьевич, Баронов Олег Рюрикович
2. Модель оценки безопасности сложной сети. (часть Научная статья по специальности «Компьютерные и информационные науки»)
3. Методический подход к комплексному описанию объекта информационной защиты
4. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и TextMining
5. Проблемы информационной безопасности: сборник научных трудов II Международной научно-практической конференции, Гурзуф, 25-27 февраля 2016 / Под ред. д.т.н., профессора О.В. Бойченко. ☐ Саки: ИП Бровко А.А., 2016. ☐ 256 с.

ӘОЖ 341

Алиш Зере Бақытқалиқызы
«Әділет» Жоғары құқық мектебінің
1 курс студенті
Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қ.

Ғылыми жетекшісі:
Қасымбек А.О.
з.ғ.м., Каспий қоғамдық университетінің
«Әділет» ЖҚМ сеньор-лекторы

**ӘЛЕУМЕТТІК ЖЕЛІНІҢ БАЛАНЫҢ
ҚҰҚЫҚТЫҚ САНАСЫНА ӘСЕРІ****Аңдатпа**

Мақалада цифрландыру жағдайларының әсері талданады. Кәмететке толмағандардың девиантты мінез-құлқы туралы ғылыми тәсілдер мен өзге де материалдар негізінде, жасөспірімдердің құқықтық санасы мен мінез-құлқына статистикалық деректер, зерт-

теу нәтижелері, мысалдар, әлеуметтік-педагогикалық практика және авторлық түсінік беріледі. Кәмелетке толмағандардың құқықтық санасы мен мінез құлқының өзгеруінің негізгі тенденциялары қарастырылады. Цифрландыру және девианттың жаңа формасы сипатталады, кәмелетке толмағандардың мінез-құлқы-цифрлық ауытқу, ақпараттық кеңістіктегі кәмелетке толмағандардың девиантты мінез-құлқының ерекшеліктері зерттеледі, оның негізгі формалары келтіріледі және жасөспірімдердің жеке психологиялық ерекшеліктерімен байланысты ықтимал салдары анықталады. Бұл ретте зерттеу себептері мен шарттары туралы автор жариялаған материалдар кәмелетке толмағандардың девиантты мінез-құлқының пайда болуы мен дамуын, оның алдын алу нысандарын анықтайды. Жүргізілген зерттеу нәтижелері бойынша цифрландыру жағдайларының құқықтық санаға әсері ерекшеленеді және кәмелетке толмағандардың мінез-құлқы, сондай-ақ цифрландыру жағдайында кәмелеткетолмағандардың девиантты мінез-құлқының алдын алу бойынша шаралар анықталады.

Түйінді сөздер: цифрландыру, құқықтық сана, мінез-құлқы, жасөспірімдер, сандық ауытқу, әлеуметтік желі.

Алиш Зере Бақытқалиқызы

Студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

Влияние социальной сети на правосознание ребенка

Аннотация

В статье анализируется влияние условий оцифровки. На основе научных подходов и иных материалов о девиантном поведении несовершеннолетних дается статистические данные, результаты исследований, примеры, социально-педагогическая практика и авторское толкование правосознания и поведения подростков. Рассматриваются основные тенденции изменения правосознания и поведения несовершеннолетних. Описываются оцифровка и новая форма девиантности, исследуются особенности девиантного поведения несовершеннолетних-цифровое отклонение, девиантное поведение несовершеннолетних в информационном пространстве, приводятся его основные формы и выявляются возможные последствия, связанные с индивидуально-

психологическими особенностями подростков. При этом материалы, опубликованные автором о причинах и условиях исследования, определяют возникновение и развитие девиантного поведения несовершеннолетних, формы его профилактики. По результатам проведенного исследования выделяется влияние условий оцифровки на правосознание и определяются поведение несовершеннолетних, а также меры по профилактике девиантного поведения несовершеннолетних в условиях оцифровки.

Ключевые слова: оцифровка, правосознание, поведение, подростки, цифровое отклонение, социальные сети.

Alish Z. B.,

1 year student

Higher School of Law "Adilet"

Caspian Public University

Republic of Kazakhstan, Almaty

THE INFLUENCE OF THE SOCIAL NETWORK ON THE LEGAL CONSCIOUSNESS OF THE CHILD

Annotation

The article analyzes the impact of digitalization conditions. On the basis of scientific approaches and other materials on deviant behavior of minors, statistical data, research results, examples, socio-pedagogical practice and author's interpretations of the legal consciousness and behavior of adolescents are given. The main trends in changes in the legal consciousness and behavior of minors are considered. Digitalization and a new form of deviance are characterized, the behavior of minors is a digital deviation, the features of deviant behavior of minors in the information space are studied, its main forms are given and the possible consequences associated with the individual psychological characteristics of adolescents are determined. At the same time, the materials published by the author on the causes and conditions of the study determine the emergence and development of deviant behavior of minors, the forms of its prevention. According to the results of the conducted study, the influence of digitalization conditions on legal consciousness is distinguished and measures are determined to prevent the behavior of minors, as well as deviant behavior of minors in the context of digitalization.

Keywords: digitalization, legal awareness, behavior, adolescents, digital deviation, social network.

Ажырамас цифрлық технологияларқазіргі қоғам мен мемлекет өмірінің бір бөлігі адамзатқа бейімделуге тура келетін әлем ретінде елеулі өзгерістерге ықпал етті. Жаңа цифрлық технологияларды барынша толық меңгерген және олардың әсеріне ең көп ұшыраған озық топ өкілдеріне кәметке толмағандар жатады. Виртуалдыкеңістіктерді игеру белсенділігі бойынша ересектерге қарағанда балалар мен жасөспірімдер айтарлықтай алда. Біріккен Ұлттар Ұйымының Балалар қорының (ЮНИСЕФ) баяндамасына сәйкес, 2017 жылы бүкіл әлем бойынша интернет қолданушыларының шамамен үштен бірін балалар мен жасөспірімдер құрайтыны анықталды, желінің басталу жасы біртіндеп қысқарады [1, 3-бет]. Цифрландыру кәметке толмағандарға жаңаларын ашады: жаңа құбылыстар мен процестерді игеру, құрдастарымен және басқалармен қарым-қатынас жасау, оқу процесіне қосу мүмкіндіктері және әлеуметтік процеске қатысушы болу, ал белгілі бір жағдайларда және қауымдастық мәселелерін шешу. Сонымен қатар, цифрлық технологиялар кәметке толмағандардың виртуалды кеңістікте де, нақты әлемде де теріс әсерлерге осалдығын арттыруға ықпал етуі мүмкін.

Нәтижелерді талдау. Г. У. Солдатова атап өткендей, жоғары интернеттегі ортаға тән ақпараттық ағындар мен коммуникациялардың қарқындылығы балалардың жеке басының дамуы, қалыптасуы олардың психикалық әсерлерін бағаламау мүмкін емес [2, Б. 72]. Жыл сайын зерттеушілер цифрландырудың кәметке толмағандардың өміріне әсер ету ауқымы туралы көбірек деректер алуда: виртуалды кеңістік кәметке толмағандардың өмірін кеңейтіп, толықтырып қана қоймайды, олардың қызметінің бүкіл құрылымын интернет желісінде де, нақты өмірде де өзгертеді. Бұл жағдай ақпараттық технологиялардың жеке дамуға, құқықтық сана мен мінез-құлыққа әсерін зерттеудің кәметке толмағандар арасында маңыздылығын анықтайды. Интернет-ресурстардың және басқа да бұқаралық ақпарат құралдарының (бұдан әрі – БАҚ) әсерін қамтитын жаһандық цифрландыру жағдайында кәметке толмағандарды негіздей отырып қамтиды. Виртуалды кеңістікте, бұл көптеген жағдайларда көрнекі және жойқын болуы мүмкін (деструктивті) сипат, сондықтан цифрландырудың таралуының артуымен айтарлықтай девианттың саны мен сапасы артады. Кәметке толмағандардың (девиантты) мінез-құлқы, бұл ақпараттық ресурстардың мазмұны мен толтырылуын бақылаудың қажеттілігі мен тиімділігін арттыруды көрсетеді. Ғаламдық желі ретінде интернетте орналастырылған [3, б. 75]. Өздеріңіз

білетіндей, Қазақстанда 90-шы жылдардан бері болған оқиғалар XX ғасыр жылдарындағы саяси реформалар, әлеуметтік-экономикалық салалар дажаңа нарықтық қатынастарды дамытуға әкелді, өйткені бұл процесс тек күрделі және экономикалық тұрақсыз болып қана қоймай, жағымсыз жағдайларға, әлеуметтік-экономикалық салдарларға алып келді [31, б. 664]. Қазақстан халқының экономикасы мен әлеуметтік өміріндегі дағдарыстық процестер мен құбылыстар, соның ішінде әлеуметтік наразылықтар түрінде, өмір сүру деңгейінің күрт төмендеуі, жұмыссыздық, экстремалды поляризация, криминализация және т. б., сондай-ақ қоғамдағы девиантты мінез-құлықтың өсуіне. Бұл ретте қоғамдағы өзгерістер адамдардың адамгершілік және құқықтық санасы, оларды қоғамға қарсы өмір салтына қайта бағыттаумен байланысты болды [4, 33-бет]. Осыған байланысты ересек азаматтардың әсіресе кәмелетке толмағандардың девиантты мінез-құлқының проблемалары, жаңа сәйкес келмейтін және құбылысты іске асырудың мазмұны мен формалары бойынша процестер көп бағытты болып табылады.

Е.В. Васкенің пікірінше, егер жасөспірім антисоциалды ортаға түссе, девиантты сәйкестілік механизміне байланысты ересек адаммен салыстырғанда ол девиантты субмәдениеттің нормаларына тезірек қосылады [5, б.10]. Кәмелетке толмағандардың девиантты мінез-құлқының пайда болу, даму себептері мен жағдайларын ғана емес, сонымен қатар цифрландыру жағдайларының кәмелетке толмағандардың құқықтық санасы мен мінез-құлқына әсерін зерттеу, тиісінше, одан да көпкәмелетке толмағандармен тиімді профилактикалық және түзету жұмыстары осыған байланысты маңызды болып көрінеді. Адамның, оның ішінде кәмелетке толмағанның девиантты мінез-құлқын әртүрлі аспектілер, мәселелер мен проблемалар тұрғысынан талдау мәселелері, цифрландыру жағдайларының кәмелетке толмағандарға әсері [6-8] ғылыми әдебиеттер мен интернет-ресурстарда көптеген ғылыми жұмыстар мен материалдар қарастырылған. Мұндай қызығушылық кездейсоқ емес, өйткені қарастырылып отырған мәселелер мыналарды көрсетеді: цифрландырудың әсерінен кәмелетке толмағандардың өзгеруінің негізгі тенденцияларына, сондай-ақ девиантты мінез-құлқтың кәмелетке толмағандар – сандық ауытқу жаңа түрін сипаттайды. Бұл зерттеудің туындауының себептері мен шарттары туралы автор жариялаған материалдар кәмелетке толмағандардың девиантты мінез-құлқын дамыту [9, Б. 62-68] және кәмелетке толмағандардың девиантты мінез-құлқы, оның алдын алу нысандары және түзетулер болып табылады [3, 73-80 беттер]. Бұл қараудың мәні

цифрландыру жағдайларының әсері туралы кейбір сұрақтар кәмелетке толмағандардың құқықтық санасы мен мінез-құлқына байланысты болады.

Зерттеу тақырыбына сүйене отырып, келесі сұрақтар қызығушылық тудырады: “цифрландыру”, “құқықтық сана”, «мінез-құлық» терминдері қалай анықталады; құқықтық сана мен мінез-құлық ұғымдары бір-бірімен қалай байланысты; кәмелетке толмағандардың девиантты мінез-құлқының жаңа түрі сандық ауытқу нені білдіреді; кәмелетке толмағандардың цифрлық девиантты мінез-құлқын қандай ерекшеліктер сипаттайды; кәмелетке толмағандардың виртуалды кеңістікте девиантты мінез-құлқының қандай түрлері ерекшеленеді; виртуалды кеңістіктегі кәмелетке толмағандардың девиантты мінез-құлқыты түсіндіруде негізгі тәсілдері қандай; олардың бір бөлігіндегі кәмелетке толмағандардың девиантты мінез-құлқы туралы зерттеулердің жеке психологиялық ерекшеліктерінің нәтижелері қандай; цифрландыру жағдайларының кәмелетке толмағандардың құқықтық санасы мен мінез-құлқына әсері қалай сипатталады; цифрландыру жағдайында кәмелетке толмағандардың девиантты мінез-құлқының алдын алу шаралары қандай? Цифрландыру жағдайларының әсерін талдау үшін кәмелетке толмағандардың құқықтық санасы мен мінез-құлқы үшін қолданылатын терминдердің мағынасын анықтаған жөн. “Цифрландыру” термині, “цифрлық технологияны күнделікті өмірге цифрландыру арқылы интеграциялау” ретінде анықталады [10].

В. А. Плотниковтың пікірінше, “цифрландыру” термині екі мағынада қарастырылады: 1) Цифрландыру – бұл цифрландыруды енгізу процесі деректерді генерациялау, өңдеу, беру, сақтау және әр түрлі салаларға визуализациялау технологиялары; 2) цифрландыру – бұл ақпараттандыруды дамытудың қазіргі кезеңі, басым қолданылуымен ерекшеленеді ақпаратты құрудың, өңдеудің, берудің, сақтаудың және визуализациялаудың цифрлық технологияларын, пайда болуы мен таралуына байланысты жаңа техникалық құралдар мен бағдарламалық шешімдер [11, б.17]. Қазақ тілінің сөздігінде “құқықтық сана” термині қолданыстағы құқыққа, қолданыстағы құқықтық нормаларға көзқарастар жиынтығын білдіреді [12], Ал құқықтық сөздікте “құқықтық сана” термині көзқарастар жиынтығы болып табылады, жеке адамдар мен әлеуметтік топтардың құқыққа, заңды немесе заңсыз нәрсеге қатынасын білдіретін идеялар, көзқарастар, құндылық бағдарлары [12]. Қазақ тілінің сөздігінде “мінез-құлық” термині әрекеттер мен әрекеттердің жиынтығы ретінде түсініледі, [13], ал энциклопедиялық

сөздікте “мінез-құлық” термині тірі организмдерге қозғалыс белсенділігі және бағдарлау осы ортаға тән қоршаған ортамен өзара әрекеттесу болып табылады [13]. Жалпы ереже бойынша, адамның құқықтық санасы заңға негізделген оның мінез-құлқындағы инкарнация өзінің практикалық мәнін табады. Цифрлардың тез таралуы технология кәметке толмағандардың өмір салтын ғана емес, олардың құқықтық санасы мен мінез-құлқын да өзгертуге әкеледі. Құқықтық сана категориялары құқықтық мінез-құлық құқық философиясының, әлеуметтанудың, психологияның ережелеріне негізделген, педагогика және заң ғылымдары (мысалы, теориялар, құқық, криминология және т.б.).

Г.Г. Хасановтың пікірінше, құқықтық сана құқықтық саладағы белгілі бір білімді қамтиды, көзқарастар, идеялар, сезімдер мен эмоциялар, заңды түрде бағалау қатынасын білдіретін қоғам өмірінің маңызды құбылыстарына, құқықтық-әрекеттер мен сондай-ақ заңға құрметпен қарау және заңды маңызы бар іс-әрекеттерге жеке психологиялық дайындық [14, б.11]. Қоршаған шындықтың әсерінен субъект құқықтық көзқарасты қалыптастырады, ол әр түрлі түсіну және бағалау және әзірленген бағалауға сәйкес қызметке қабілеттілікке бейім.

Г.Т. Суранчиева атап өткендей, құқықтық сана кәметке толмағандарда біртекті емес, өйткені олар қоршаған ортаның әртүрлі әлеуметтік-экономикалық жағдайларымен сипатталады [15, б. 41]. Жас ерекшеліктеріне байланысты жасөспірімдердің санасы әдетте тұрақсыз, мүмкінгеріс көріністерге ие.

Л. А. Радченко жасөспірім кезең құқықтық нормаларды зерттеу үшін ең сәтті болып табылады, өйткені олар білім мен дағдыларды алудың бірыңғай жүйесіне еніп, тез және сапалы игереді, содан кейін жеке сенім жүйесіне айналады және құқықтық мәдениетті қалыптастырады деп жазады [16, б. 29]. Осылайша, жасөспірім жеке тұлғаның құқықтық санасын қалыптастыру жолында шешуші болып табылады, осы бағыттағы дамудың әрі қарайғы векторын анықтайды және оның құқық бұзушылық пен қылмыс түріндегі құқықтық және құқық нормаларын бұзатын мінез-құлқын қалыптастырады. Бұл ретте, Е. Э. Бойкина мен В. А. Чернов атап өткендей, кәметке толмағандар арасындағы құқық бұзушылықтардың сандық көрсеткіштерінің қысқаруымен қатар, виртуалды кеңістікте жүзеге асырылған мінез-құлық ауытқуларының жаңа формаларының пайда болуы мен дамуына үрдіс байқалады [18, б.136].

М.В. Костоломова девиантты мінез-құлықтың жаңа түрінің (жаңа формасының) қалыптасуын кәмелетке толмағандар – сандық ауытқу екендігін көрсетеді (оны сандық девиантты мінез-құлық деп те атайды), бұл жиынтық әлеуметтік нормалардан ауытқу физикалық, эмоционалды, интеллектуалды, әлеуметтік және цифрландырудың барлығына әсер етуіне байланысты әлеуметтік шындықтың елеулі өзгерістеріне дүниетанымдық жеке реакцияларда өмірінің деңгейлері [8, Б. 48]. Зерттеуші сандық девиантты мінез-құлықтың келесі ерекшеліктерін анықтайды: нақты болмау өзіне зиян келтірген кезде айналасындағыларға физикалық қауіп төндіреді; жасөспірімге психоэмоционалды әсер алуға мүмкіндік беретін кідіріс виртуалды шындықтағы разряд, белгіленген бұзушылықтар қажеттілігін сезінбеу өмірдегі нормаларды нақтылау және технологиялардың нақтылау қажеттілігі, ғаламдық желінің және жалпы анонимділіктің; тиісті әсер ету сипатымен байланысты көріністің кешенді сипаты физиологиялық жағдайға әсер ететін цифрландыру (ми және жалпы организм), интеллект (ойлау және сөйлеу), психоэмоционалды фон (виртуалды сұхбаттасушымен өзара әрекеттесу және ақпараттық шудың үздіксіздігі), дүниетанымдық және құндылық көзқарастар, нақты әлеуметтік өмір және басқалар; күрделілік цифрлық трендтердің дамуының динамизмімен және сызықтық емес болуымен байланысты цифрлық ауытқудың болашақ формаларын болжау.

А. А. Осипованың пікірінше, Д. В. Давыденко және Ю. Р. А. Абдулкадир, сандық девиантты ауыстыру функциясы мінез құлыққа тән, ұрлықты, кісі елтіруді, қиратуды және басқа да девиантты мінез-құлықты виртуалды әлемде қамтамасыз ету [19, 44-бет]. Бұл тенденцияның дамуы норманы түсінудің өзі трансформацияға әкелуі мүмкін, өйткені оның анықтамасы жасөспірім өзара әрекеттесетін қауымдастыққа байланысты болады.

Ю.В. Гребенкина айтқандай, бұл девиантты мінез-құлық факторларының біріотбасындағы қолайсыз жағдаймен, өзін-өзі растау қажеттілігімен, жаңа сезімдерге деген құштарлықпен және басқа да классикалық факторлармен ерекшеленетін [21, б.22].

С. В. Книжникованың айтуынша, БАҚ жасөспірімнің жеке басына деструктивті әсер етеді оның құндылық-бағдарлық қондырғылары және өзінің “Мен” деформациясына әкеледі [22, б.236].

Бұл тенденция кәмелетке толмағандар үшін жасалған оң және ғылыми-танымдық медиа-сюжеттердің жетіспеушілігімен және жасөспірімдер мен ересектердің қолданыстағы медиа мәтіндерді сыни тұрғыдан түсінбеуімен байланысты.

К. А. Воробьева атап өткендей, техникалық құралдардың қазіргі даму қарқынын ескере отырып қарым-қатынас жаңа деструктивті мінез-құлық

үлгілерін тарату және танымал ету жасөспірімдер ортасында орын алады, және берілген процесс педагогикалық және ғылыми қауымдастық бұл тәуекелдерге жауап бере алатыннан гөрі жылдамырақ [24, б.145].

Зерттеуші девиантты мінез құлықтың келесі түрлерін ажыратады. Виртуалды кеңістікте іске асырылатын кәмелетке толмағандар: 1) кибербуллинг-қудалау, қорлау, қорқыту және қорлау виртуалды шындық құралдары арқылы; 2) кибермоббинг – қасақана қорқыту, қорлау, жала жабу және компаға келу деректерін ашу, әдетте ұзақ уақыт бойы; 3) секстинг-жеке тұлғаларды жіберу интимдік сипаттағы фотосуреттер мен хабарламалар; 4) геронтофобия-кемсітушіліктің бір түрі, қарттарды ұнатпаудан тұрады; 5) троллинг-әдетте белгілі бір аудиторияға бағдарланған арандатушылық хабарламаларды виртуалды ресурстарға орналастыру, жанжал жағдайын жасау мақсатында; 6) шоплифтинг-дүкендерден ұрланған тауарлардың құнын көрсете отырып, оларды желіде көрсету; 7) астротурфинг – арнайы бағдарламалық жасақтаманы қолдану қызмет көрсетуді қамтамасыз ету немесе пайдалану жасанды мақсатта жалданған пайдаланушылар қоғамдық пікірді басқару.

Девиантты мінез-құлықтың жекелеген түрлері үшін заңды жауапкершілік, оның ішінде әкімшілік жауапкершілік қарастырылған (мысалы, 5.61-бап бойынша. Қазақстан Республикасының Әкімшілік кодексі ақпараттық-телекоммуникациялық “Интернет” желісін қоса алғанда), қылмыстық (мысалы, Қазақстан Республикасының Қылмыстық кодексінің 110.1-бабы бойынша (Қазақстан Республикасының Қылмыстық кодексі) өз-өзіне қол жұмсауға бейімділік, өз-өзіне қол жұмсауға жәрдемдесу ... көпшілік алдында сөйлегенде, көпшілік алдында көрсетілетін жұмыстың, құралдардың ақпараттық-телекоммуникациялық желілерді (соның ішінде “Интернет” желісін); Қазақстан Республикасының Қылмыстық кодексінің 128.1-бабы бойынша ақпараттық-телекоммуникациялық желілерді қолдана отырып жала жапқаны үшін “Интернет” желісін қоса алғанда, желілер және т.б.), цифрлық ауытқулардың ең айқын және жаппай көрінетін түрлерінің бірі кибербуллинг болып табылады, оның қорқытудан айырмашылығы, ол анонимділік жағдайында орыналады, бұл агрессорлардың қолжетімсіздігі мен жазасыздығына ықпал етеді, құрбандардың дәрменсіздігін күшейтеді [25, 18-бет]. Физикалық және психологиялық қашықтықтың болуы оларға қатысты агрессорлардың эмпатия деңгейі жәбірленушілерге төмендеуге әкеледі. Бұл ретте онлайн-аудиторияның іс жүзінде шексіз ауқымын ескере отырып, кибербуллинг бақылаусыз жүзеге асырылуы мүмкін тәулік бойы әсер ету мүмкіндігі жағдайында агрессорлар санының артуы жәбірленушінің жағдайын едәуір нашарлатады.

Г. С. Галстян атап өткендей, кәмелетке толмағандардың суицидтік мінез-құлқы жеке тұлғаның әлеуметтік интеграциясымен тікелей байланысты болып табылады. Цифрлық трансформацияны бастан өткеріп жатқан қоғам жағдайындағы әлеуметтік-психологиялық дезадаптацияның салдары [26, б.11]. Суицидтік мінез-құлқы ұжымдық және жұқпалы болып табылады, олар қоғамның урбанизациясымен және БАҚ пен виртуалды кеңістіктің жеке адамның санасына әсерімен тікелей байланысты.

Л. В. Жихарева әлеуметтік желілерде топтар деп аталатын кәмелетке толмағандардың өміріне тікелей қауіп төндіретін беттер өлім туралы жазады [27, б.164]. Мұндай топтардың философиясы қатыгездік пен әділетсіздік идеясына негізделген. Бейбітшілік және олардың барлық хабарламалары ұсынысқа негізделген жасөспірімге қоғамдастықта қажеттілік сезімі..

А. А. Васильев және оның авторлары виртуалды шындық қылмыскерлерге кәмелетке толмағандардың еркін басуға көмектесетінін атап өтті [28, 212-бет].Өзін-өзі бағалау және тану қажеттілігін қанағаттандыру нәтижесінде, әсіресе отбасылық жағдайдың қолайсыздығы және ата-аналардың тиісті эмоционалды қолдауының болмауы аясында бала алдымен белгілі бір топқа деген сүйіспеншілікті, содан кейін тәуелділікті қалыптастырады.

Жалпы, С. Т. Персохова мен А. Е. Колпакованың пікірінше, Интернетке тәуелділік, құмар ойындар және гаджеттерге тәуелділік сияқты тәуелділіктер цифрландырудың тән ерекшелігі болып табылады және олардың пайда болу жиілігі интернет пен гаджеттердің таралуына пропорционалды түрде артады [29, б.16].

Автордың пікірінше, цифрландыру жағдайларының кәмелетке толмағандардың құқықтық санасы мен мінез-құлқына келесі әсерін атап өтуге болады: нақты өмірде жүзеге асырылатын жасөспірімдер арасындағы құқық бұзушылықтар санының азаюы, бұл құқықтық сананың өзгергенін куәландырады. Кәмелетке толмағандар және олардың неғұрлым құқықтық көзқарасын қалыптастыру; бұрмалау жасөспірімдердің құндылық-бағдарлық көзқарастары олардың «Мен» деформациясына әкеледі, медиа өнімдердің әсерінен; цифрлық девиантты мінез – құлықтың пайда болуы және дамуы-виртуалды кеңістікте жүзеге асырылған мінез-құлқы ауытқуларының жаңа формалары анонимділік пен қауіпсіздік сезімінің арқасында; әртүрлі цифрлық нысандардағы агрессорлар болып табылатын жас өспірімдердің тәуелділік және құқықбұзушылық мінез-құлқына бейімділігінің артуы,

девиантты мінез-құлық және қолайсыз психологиялық жағдайлардың ықтималдығын арттыру осындай формалардың құрбаны болған жас өспірімдерде ауытқулар; пайда болу жиілігін арттыру жасөспірімдер интернет-тәуелділік, ойын-сауық және гаджеттерге тәуелділік. Жалпы ереже бойынша, нақты өмірде девиантты мінез-құлыққа бейім кәмелетке толмағандар көбінесе бұл бейімділікті виртуалды кеңістікке жеткізеді. Девиантты Виртуалды кеңістіктегі жасөспірімнің жеке басы нақты тұлғаның сипаттамаларына негізделген және когнитивті (жеке тұлғаның сенімдері мен құзыреттілік деңгейі), мифологиялық (жеке мифологемалар) және мотивациялық (желіде болу себептері) құрамдас бөліктер. Кезінде бұл, А. А. Осипова, Д. В. Давыденко және Ю. Р. А. Абдулкадир айтқандай, кәмелетке толмағандардың виртуалды девиантты мінез-құлқын заманауи түсіну дәстүрлі денасып түседі және пән аралық әдістерді қолдануды талап етеді [19, б.46]. Виртуалды ортада жас өспірімдер көрсететін девиантты мінез-құлықтың себептері орынды болып көрінеді. Іздеу нақты әлеуметтік болмысқа екінші дәрежелі ақпараттық кеңістікте емес, кәмелетке толмағана да мныңайналасындағы әлеуметтік құрылыс, тәрбие және білім беру шындықтарында. Цифрландыру жағдайында кәмелетке толмағандардың девиантты мінез-құлқының алдын алу үшін келесі шараларды бөлуге болады: әлеуметтік ортаны ұйымдастыру сандық ауытқуларды анықтайтын әлеуметтік факторларға әсер ету мақсатында; оқыту жасөспірімдерді әлеуметтік маңызы бар дағдыларға баулу; кәмелетке толмағандарға (бұрын мектеп оқушыларына) бағыты бар виртуалды және нақты көрініс мүмкіндіктері олардың ішкі жеке ресурстарын таным және құру процестеріне; девиантты мінез-құлықты шығармашылық қызметпен алмастыруға мүмкіндік беретін цифрлық ауытқуларға балама онлайн-қызметті ұйымдастыру; кәмелетке толмағандар мен олардың ата-аналарын цифрлық трансформациямен байланысты қауіптер туралы хабардар ету.

Қорытынды. Сандық девиантты мінез-құлықтың себептері мен бастапқы көздерін егжей-тегжейлі зерттеу үшін кәмелетке толмағандар арасында қолдану қажет. Мүмкіндік беретін тәртіптік талдау әдістері жасөспірімдерді қоршаған виртуалды ортаға кешенді бағалау жүргізу және цифрландыру жағдайларына байланысты ауытқулардың алдын алудың оңтайлы бағыттарын анықтау. Осылайша, зерттеу жүргізілді. Цифрландыру жағдайларының әсері туралы кейбір мәселелерді қарайтын материалдарды, оның ішінде жекелеген статистикалық деректерді, зерттеу нәтижелерін, әлеуметтік-педагогикалық практика мен авторлық

түсініктің мысалдарын кәмелетке толмағандардың құқықтық санасы мен мінез-құлқына ғылыми тәсілдерді талдауды ұсынады.

Пайдаланылған қайнар көздерінің тізімі:

1. Положение детей в мире, 2017 год: Дети в цифровом мире: доклад / ЮНИСЕФ. – 2017. – 40 с.

2. Солдатова Г. У. Цифровая социализация в культурно–исторической парадигме: меняющийся ребенок в меняющемся мире // Социальная психология и общество. – 2018. – Т. 9. – № 3. – С. 71-80.

3. Джадан В. Н. Девиантное поведение несовершеннолетних: формы предупреждения и исправления // Юридическая наука. – 2021. – № 7. – С. 73-80.

4. Салахова В. Б., Ильяшина Н. Г., Романова А. В. Проблема девиантного поведения в современном обществе // Власть. – 2016. – Том 24. – № 11. – С. 33-37.

5. Васкэ Е. В. Несовершеннолетние правонарушители: учебник. Руководство для высших учебных заведений. – 2-е изд., дальнейшее чтение и приложение – М.: Юрайтбаспасы, 2021. – 175 с.

6. Зорцева Е. Г., Кирюхина Д. В. Кибербуллинг и склонность к девиантному поведению подростков // Прикладная юридическая психология. – 2020. – № 1 (50). – 80-87 Б.

7. Костоломова М. В. Цифровая девиация как феномен новой социальной реальности: Методологические основы и концепция концепции // Социологическая наука и социальная практика. – 2020. – Т.8. – № 2. – С. 41-53.

8. Жадан В. Н. К анализу причин и условий, вызывающих возникновение и развитие девиантного поведения несовершеннолетних // Юридические науки. – 2022. – № 2. – С. 62-68.

9. Бойкина Е.Е., Чернов В.А. Правовое сознание подростков столетнего поколения: прогностическая оценка // Психология и право. – 2021. – Том. 11. – № 1. – С.135-149.

10. Осипова А.А., Давыденко Д.В., Абдулкадир Ю.Р.А. Особенности девиантного поведения молодежи в виртуальной среде // Гуманитарные, социально-экономические и социальные науки. – 2020. – № 6. – С. 43–48.

11. Князьникова С.В. Медиабезопасность следующего поколения: снижение риска девиантного поведения // Научно-методическая «Концепция» электронного журнала. – 2015. – Вып. 37. – С. 236–240.

12. Воробьева К.А. Современные тенденции формирования новых форм девиантного поведения молодежи в информационном пространстве // Цифровое общество в культурно-исторической парадигме: материалы международной научной конференции /–2022 г –№ 5. [ЮН]114 Под ред. Т.Д. Марцинковская, В.Р. Орестова, О.В. Гавриченко. – М., 2018. – С. 144–147.

13. Галстян Г.С. Суицид среди несовершеннолетних – это крайняя форма девиантного поведения: абстракция. Дисс. на соиск. уч.степени Социальное. науки. – Майкоп, 2010. – 28 с.

14. Изменения в праве в эпоху цифровых технологий: монография / Под ред. А.А. Васильева. – Барнаул: ПасылымАлт. университет, 2020. – 432 с.

15. Каменская В.Г., Томанов Л.В., Татьяна Е.В. Дети и подростки цифрового сообщества // Семья и общество: социально-педагогические аспекты профилактики психологического девиантного поведения: Сборник материалов международной научно-практической конференции / Под общ. ред. О.А. Драганова. – Липецк: «Открытая» издательская студия «Мир», 2020. – С. 40-46.

УДК 343.63

Аманбай Гульбаршын

Студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

СТАЛКИНГ КАК ВИД КИБЕРБУЛЛИНГА

Аннотация

В статье рассмотрено понятие сталкинга как вид кибербуллинга. Обращается внимание на киберпреследование и входящие в него действия. Изучены такие типы киберпреследования как мстительное, составное, интимное и коллективное. Показаны пути избежания киберпреследования.

Ключевые слова: кибербуллинг, сталкинг, интернет, сообщения, переписка, комментарии, правонарушение.

Аманбай Гульбаршын
«Әділет» Жоғары құқық мектебінің
1 курс студенті
Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қ.

СТАЛКИНГ КИБЕРБУЛЛИНГТИҢ БІР ТҮРІ РЕТІНДЕ

Аңдатпа

Мақалада кибербуллингтің бір түрі ретінде аңду тұжырымдамасы қарастырылады. Киберталкинг пен оның әрекеттеріне назар аударылды. Киберталкингтің кекшіл, құрама, интимдік және ұжымдық сияқты түрлері зерттелген. Кибербұзушылықтан сақтану жолдарын көрсетеді.

Түйінді сөздер: кибербуллинг, сталкинг, интернет, хабарламалар, хат алмасу, түсініктемелер, құқық бұзушылық.

Amanbay Gulbarshyn
1 year student
Higher School of Law "Adilet"
Caspian Public University
Republic of Kazakhstan, Almaty

STALKING AS A TYPE OF CYBERBULLYING

Annotation

The article discusses the concept of stalking as a type of cyberbullying. Attention is drawn to cyberstalking and its activities. Such types of cyberstalking as vindictive, compound, intimate and collective have been studied. Shows ways to avoid cyberstalking.

Key words: cyberbullying, stalking, Internet, messages, correspondence, comments, offense.

Киберсталкинг (далее – Киберпреследование) - это использование Интернета и других технологий для преследования или травли другого человека в сети, и это потенциально является преступлением. Такое преследование в Интернете, являющееся продолжением кибербуллинга и преследования при личной встрече, может принимать форму электронных писем, текстовых сообщений, постов в социальных сетях и т. д. и часто является методичным, преднамеренным и настойчивым.

Чаще всего они не прекращаются, даже если адресат выражает свое недовольство или просит прекратить. Контент, направленный на адресата, часто неуместен, а иногда даже вызывает беспокойство, что может заставить человека чувствовать страх, расстройство, тревогу и беспокойство. Хотя некоторые из онлайн-преследований, с которыми столкнулись участники опроса, были просто неприятным поведением, почти каждый пятый американец сказал, что сталкивался с серьезными формами онлайн-преследований. Эти действия включали физические угрозы, сексуальные домогательства и преследование.

Некоторые признаки того, что вы столкнулись с киберпреследованием: кто-то отправляет вам слишком много сообщений, человек посылает вам неуместные сообщения, ставит лайк на все ваши старые посты в социальных сетях, манипулирует вами, заставляя взаимодействовать с ним в сети, или троллит вас. Безличное поведение в Интернете, GPS-слежение, сообщения с угрозами, «кошачий фишинг» и «доксинг» также относятся к киберпреследованию.

Когда речь идет о киберпреследовании, те, кто занимается этим, используют различные тактики и методы, чтобы преследовать, унижать, запугивать и контролировать своих жертв. На самом деле, многие из тех, кто занимается киберпреследованием, технологически подкованы, а также креативны и придумывают множество способов мучить и преследовать свои цели.

Что же считается киберпреследованием? Вот несколько примеров того, что могут делать люди, занимающиеся киберпреследованием:

- Размещать грубые, оскорбительные или наводящие на мысль комментарии в Интернете
- Следить за объектом в Интернете, вступая в те же группы и форумы.
- Отправлять угрожающие, контролирующие или непристойные сообщения или электронные письма.
- Использовать технологии для угроз или шантажа.
- Чрезмерно указывать цель в сообщениях, даже если они не имеют к ней никакого отношения
- Комментируйте или ставьте лайк всему, что цель публикует в Интернете
- Создавать фальшивые аккаунты, чтобы следить за объектом в социальных сетях
- Постоянно писать сообщения цели
- Взламывать или угонять онлайн-аккаунты цели
- Пытаться вымогать секс или откровенные фотографии

- Посылать объекту нежелательные подарки или предметы
- Разглашать конфиденциальную информацию в Интернете
- Размещать или распространять настоящие или поддельные фотографии объекта.
- Забрасывать жертву откровенными сексуальными фотографиями
- Создавать фальшивые сообщения, призванные пристыдить жертву.
- Отслеживать перемещения жертвы в Интернете, устанавливая устройства слежения
 - взламывать камеру на ноутбуке или смартфоне жертвы, чтобы тайно записывать ее.
 - Продолжать домогаться даже после просьбы прекратить.

Киберпреследование часто подразделяется на четыре основных типа: мстительное, составное, интимное и коллективное. Мстительный киберпреследование включает угрозы, составной киберпреследования включает раздражение и преследование, интимный включает бывших или людей, увлеченных жертвой, а коллективный включает человека, которого преследует группа людей.

Как и преследование, киберпреследование способно вызвать широкий спектр физических и эмоциональных последствий для тех, кто стал его жертвой. Например, нередко те, кто подвергается преследованиям в Интернете, испытывают гнев, страх и растерянность. Они также могут испытывать проблемы со сном и даже жаловаться на расстройство желудка. Есть даже сообщения о том, что у жертв киберпреследований могут возникать посттравматическое стрессовое расстройство и суицидальные мысли.

Первый шаг в предотвращении киберпреследований - обеспечить максимальную безопасность ваших устройств и учетных записей в Интернете. Вот несколько шагов, которые вам следует предпринять:

- Создайте надежные пароли. Убедитесь, что у вас есть надежные пароли для всех ваших учетных записей в Интернете, а также надежные пароли для ваших устройств. Затем установите на телефоне напоминание о необходимости регулярно менять пароли. Выбирайте пароли, которые сложно угадать, но легко запомнить.
- Обязательно выходите из системы каждый раз. Это может показаться неприятным, но обязательно выходите из электронной почты, аккаунтов в социальных сетях и других онлайн-аккаунтов после их использования. Таким образом, если кто-то сможет проникнуть на ваше устройство, у него не будет легкого доступа к вашим аккаунтам.

- Следите за своими устройствами. Не оставляйте телефон на столе на работе и не уходите от открытого ноутбука. Чтобы установить устройство слежения или взломать ваше устройство, нужна всего минута или две. Поэтому убедитесь, что эти вещи находятся у вас под рукой или что вы каким-то образом их защитили.
- Будьте осторожны с общественным wifi. Осознайте, что если вы пользуетесь общественным Wi-Fi в отелях или в местной кофейне, вы подвергаете себя риску взлома. Постарайтесь воздержаться от использования публичного wifi или инвестируйте в VPN.
- Привыкайте к безопасности в Интернете. Другими словами, сделайте приоритетом принятие запросов на добавление в друзья только от знакомых вам людей и сохраняйте конфиденциальность своих сообщений. Вам также следует завести один адрес электронной почты, предназначенный специально для вашей онлайн-активности. Используйте этот адрес при совершении покупок в Интернете или для участия в программах лояльности.

Первый шаг к решению проблемы киберпреследования - сделать все возможное, чтобы прекратить взаимодействие с человеком, который вас преследует. Хотя они все еще могут найти другие способы связаться с вами, вы можете, по крайней мере, усложнить их контакт. Попробуйте создать такие препятствия для киберпреследования.

Попросите человека остановиться. Ответьте киберпреследователю только один раз и скажите, чтобы он перестал с вами связываться. Не нужно говорить ничего конкретного или объяснять свой ответ, просто попросите его больше никогда не связываться с вами.

Заблокируйте человека. Убедитесь, что вы заблокировали преследующего вас человека во всех своих аккаунтах. Заблокируйте его в социальных сетях и на смартфоне.

Откажитесь отвечать на любые обращения. Если киберпреследователь продолжает искать способы связаться с вами, не отвечайте ни на что из того, что он вам пишет или отправляет.

Смените адрес электронной почты и экранные имена. Подумайте о том, чтобы получить новый адрес электронной почты и изменить свои имена в Интернете, чтобы человеку, который вас преследует, было сложнее до вас добраться.

Рассматривая ситуации с киберпреследованием необходимо понимать, что данные проблемы в нынешних реалиях являются проблемами, которым нужно регулирование. Речь идет о правовом регулирова-

нии данного вопроса, что будет являться мерой к защите собственных прав, которое гарантирует государство. В случае совершения подобных преступлений с объективной точки зрения правонарушитель совершаемый данные деяния чувствует безответственность за совершение действий, вследствие чего это развязывает руки в совершении подобных действий не с одним человеком, но и с сотнями подобных потерпевших. Киберпреследование относится к уголовным правонарушениям в ряде развитых стран. К примеру, США, Германия, Франция и так далее.

УДК 341.231

Аманжол Ернұр Ерікұлы

Студент 2 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ПРАВОВЫЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ ГРАЖДАН В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация

Целью написания статьи является комплексный анализ правовых и этических проблем, возникающих в контексте защиты прав граждан в цифровом пространстве. Наша задача заключается в выявлении основных вызовов, с которыми сталкиваются граждане в современной цифровой эре, и в раскрытии технологических и законодательных аспектов, оказывающих влияние на их права и свободы. Исследование направлено на выработку рекомендаций по совершенствованию правового и этического обеспечения в цифровой среде с целью обеспечения баланса между инновационным развитием и защитой основных принципов гражданских прав и свобод.

Ключевые слова: цифровое пространство, права граждан в цифровом пространстве, правовые и этические проблемы, киберугрозы, цензура в цифровом пространстве.

Аманжол Ернұр Еріқұлы
«Әділет» Жоғары құқық мектебінің
2 курс студенті
Каспий қоғамдық университеті
Қазақстан Республикасы, Алматы қ.

ЦИФРЛЫҚ КЕҢІСТІКТЕ АЗАМАТТАРДЫҢ ҚҰҚЫҚТАРЫН ҚОРҒАУДЫҢ ҚҰҚЫҚТЫҚ ЖӘНЕ ЭТИКАЛЫҚ МӘСЕЛЕЛЕРІ

Аңдатпа

Бұл мақаланың мақсаты – цифрлық кеңістікте азаматтардың құқықтарын қорғау контекстінде туындайтын құқықтық және этикалық проблемаларды жан-жақты талдау. Біздің миссиямыз – қазіргі цифрлық дәуірде азаматтардың алдында тұрған негізгі қиындықтарды анықтау және олардың құқықтары мен бостандықтарына әсер ететін технологиялық және заңнамалық аспектілерді ашу. Зерттеу инновациялық даму мен азаматтық құқықтар мен бостандықтардың негізгі қағидаттарын қорғау арасындағы тепе-теңдікті қамтамасыз ету мақсатында цифрлық ортада құқықтық және этикалық қолдау көрсетуді жетілдіру бойынша ұсыныстар әзірлеуге бағытталған.

Түйінді сөздер: цифрлық кеңістік, цифрлық кеңістіктегі азаматтардың құқықтары, құқықтық және этикалық проблемалар, киберқауіптер, цифрлық кеңістіктегі цензура.

Amanzhol Yernur
2nd year student
Higher School of Law “Adilet”
Caspian Public University
Republic of Kazakhstan, Almaty

LEGAL AND ETHICAL PROBLEMS OF PROTECTING CITIZENS' RIGHTS IN THE DIGITAL SPACE

Annotation

The purpose of this article is to provide a comprehensive analysis of the legal and ethical issues arising in the context of protecting citizens' rights in the digital space. Our objective is to identify the main challenges faced by citizens in the modern digital era and to reveal the technological and legislative aspects that affect their rights and freedoms. The study aims

to develop recommendations for improving legal and ethical support in the digital environment in order to ensure a balance between innovative development and the protection of the basic principles of civil rights and freedoms.

Key words: Digital space, rights of citizens in digital space, legal and ethical problems, cyber threats, censorship in digital space.

Цифровое пространство представляет собой виртуальную среду, созданную в результате развития информационных и коммуникационных технологий, где взаимодействие людей, компьютеров и данных формирует новый уровень общественных отношений. Это пространство охватывает различные аспекты жизни, включая обмен информацией, социальные взаимодействия, экономическую деятельность и государственное управление.

Цифровое пространство, как глобальная сфера информационных технологий и виртуальных взаимодействий, имеет значительное влияние на права граждан. С одной стороны, оно предоставляет новые возможности для свободного обмена информацией, участия в общественных дискуссиях и доступа к образованию. С другой стороны, возрастающий сбор и анализ личных данных в цифровом пространстве поднимает вопросы конфиденциальности, а угрозы кибербезопасности могут ограничивать право граждан на безопасность. Также цифровое неравенство создает барьеры для равного доступа к информационным ресурсам, в то время как риск цензуры может затруднить свободное выражение мнений. Следовательно, балансировка между инновациями в цифровой сфере и защитой основных прав граждан становится ключевым аспектом формирования справедливого и этичного цифрового общества.

Современное цифровое пространство стало ареной, где происходит интенсивный сбор и обработка личных данных граждан, создавая сложные вызовы в сфере конфиденциальности. Одним из ключевых аспектов является неограниченный доступ к персональной информации, предоставленной в целях использования различных онлайн-сервисов. Это ведет к нарушению приватности граждан и подрывает основные права на защиту личной жизни.

Дополнительным вызовом становится расширяющийся объем данных, собираемых не только компаниями, но и государственными учреждениями. Этот процесс часто происходит без достаточной ясности в отношении целей и масштабов использования собранных данных, что угрожает основам прозрачности и доверия в цифровом обществе.

Уникальные технологические методы, такие как анализ больших данных и искусственный интеллект, создают новые возможности для профилирования и массового мониторинга граждан, что поднимает вопросы не только конфиденциальности, но и потенциального нарушения их свободы и безопасности.

Основным вызовом является также недостаток единых и эффективных законодательных механизмов для защиты конфиденциальности в цифровой среде. Обязательно требуется доработка законов и нормативных актов, чтобы соответствовать быстрому развитию технологий и обеспечить адекватную защиту личных данных граждан.

Таким образом, анализ современных вызовов в области конфиденциальности и сбора данных в цифровом пространстве подчеркивает необходимость разработки и внедрения эффективных мер по защите личных данных, с учетом принципов этики и прав граждан в онлайн-среде.

Сфера защиты данных стала ключевым аспектом в цифровом пространстве, и законодательство в этой области стремится балансировать между инновациями и правами граждан. В многих странах приняты законы, направленные на регулирование сбора, обработки и хранения личных данных с целью обеспечения конфиденциальности и безопасности граждан.

В Республике Казахстан правовая и этическая сфера защиты данных граждан в цифровом пространстве опирается на законы и нормативные акты, направленные на обеспечение конфиденциальности и безопасности личной информации. Одним из ключевых законов в этой области является Закон Республики Казахстан «О персональных данных и их защите», принятый в 2013 году. Данный закон устанавливает правила сбора, обработки, использования и защиты персональных данных граждан, а также предоставляет им контроль над своей информацией. В соответствии с законом, сбор и обработка персональных данных допускаются только при наличии согласия субъекта данных или в случаях, предусмотренных законом. Закон также определяет обязанности операторов по обеспечению безопасности данных и предусматривает меры ответственности за нарушения.

Однако, несмотря на существование законодательных инструментов, эффективность их применения подвергается сомнению. Важным аспектом является необходимость постоянного обновления законов, чтобы они соответствовали быстрому развитию технологий и новым вызовам в цифровой сфере. Также, следует отметить, что реализация

мер по защите данных и наказание за нарушения не всегда проводится последовательно и эффективно.

Для повышения эффективности законодательства о защите данных в Республике Казахстан, необходимо усилить меры по образованию и информированию граждан о их правах и обязанностях в цифровом пространстве. Также, важно поддерживать диалог между государственными органами, общественными организациями и представителями бизнес-сектора для обеспечения сбалансированности интересов и эффективной реализации защиты данных в интересах граждан Республики Казахстан.

Таким образом, несмотря на значительные усилия по созданию законодательства о защите данных, необходимо продолжать работу над его совершенствованием, в том числе путем обеспечения единых стандартов и ужесточения мер ответственности для обеспечения эффективной защиты прав граждан в цифровом пространстве.

Современное цифровое пространство Республики Казахстан сталкивается с растущей угрозой кибератак, что поднимает вопросы безопасности и прав граждан. Осуществление исследования данных угроз и их последствий представляет собой неотъемлемую часть обеспечения эффективной защиты в цифровой среде.

Прежде всего, стоит выделить киберугрозы, направленные на личные данные граждан. Атаки на системы хранения личных данных могут привести к утечкам конфиденциальной информации, включая имена, адреса, финансовые данные и другие личные сведения. Это создает реальные риски для частной жизни граждан и может быть использовано в целях мошенничества и кражи личности.

Вторым важным аспектом исследования является анализ кибератак на критическую инфраструктуру. Нападения на системы энергетики, телекоммуникаций и государственных служб могут привести к нарушению обычного функционирования общества и угрожать основам национальной безопасности.

Последствия таких кибератак для граждан включают в себя не только потерю конфиденциальности и угрозы финансовой безопасности, но и возможные нарушения их основных прав, таких как право на доступ к информации, свободу выражения и защиту от неправомерного вмешательства в частную жизнь.

Эффективная борьба с киберугрозами требует не только усовершенствованных технологических решений и средств киберзащиты, но и строгого законодательства, регулирующего сферу кибербезопасности.

Исследование угроз кибератак и их последствий должно служить основой для разработки таких законов и мер по обеспечению надежной защиты прав граждан в цифровом пространстве Республики Казахстан.

Рассмотрение проблем, связанных с цензурой в цифровом пространстве, поднимает важные вопросы прав и этики граждан. В современном цифровом мире возникают вызовы, связанные с ограничением свободы выражения и доступа к информации. Одной из проблем является различие между законной борьбой с нежелательным контентом и потенциальным злоупотреблением цензурой для подавления свободного обмена мнениями. Необходимость тщательной балансировки между защитой общественной безопасности и гарантированием основных прав граждан, таких как свобода слова и доступ к информации, становится ключевым аспектом разработки эффективных и справедливых механизмов цифровой цензуры.

В контексте защиты прав граждан в цифровом пространстве, анализ воздействия на свободу выражения выявляет значительные правовые и этические проблемы. Современные технологии открывают новые возможности для свободного обмена информацией, но в то же время возникают угрозы, такие как цензура, алгоритмические фильтры и ограничения доступа к контенту. Для решения этих проблем требуется разработка сбалансированных механизмов, учитывающих потребности цифрового общества. Эффективные решения могут включать в себя улучшение правовых норм, обеспечение прозрачности в алгоритмах, а также активное взаимодействие между правительством, технологическими компаниями и гражданским обществом для разработки политик, которые обеспечат свободу выражения при соблюдении законов и этических норм.

Исследование факторов, влияющих на цифровое неравенство в рамках защиты прав граждан в цифровом пространстве, становится неотъемлемой частью анализа современной цифровой среды. Факторы, воздействующие на цифровое неравенство, включают доступность широкополосного интернета, образовательные ресурсы, уровень технологической грамотности, экономическое положение и географическое распределение.

Неравномерный доступ к цифровым технологиям может привести к ограниченному участию в цифровом обществе и затруднению в получении информации, образования и доступе к государственным услугам. Особенно важно учитывать аспекты пола, возраста, социального статуса и региональной принадлежности в контексте цифрового неравенства.

Для решения этой проблемы необходимо разработать и реализовать инклюзивные стратегии, направленные на расширение доступа к цифровым ресурсам, обеспечение образовательных возможностей и снижение экономических барьеров. Эти меры должны сочетать в себе усилия государства, частного сектора и общественных организаций, чтобы создать более справедливое и равноправное цифровое пространство для всех граждан.

Для Республики Казахстан рассмотрение законодательных шагов с целью уменьшения цифрового неравенства представляет собой неотложную задачу в области защиты прав граждан в цифровом пространстве. Важными аспектами таких шагов являются обеспечение равного доступа к широкополосному интернету во всех регионах страны, включая удаленные территории, и предоставление финансовой поддержки для населения с ограниченным доходом с целью обеспечения доступа к цифровым технологиям. Законодательные инициативы также должны включать в себя обязательное внедрение образовательных программ по цифровой грамотности на всех уровнях образования. Это направление способствует повышению технологической грамотности граждан и уменьшению разрыва в доступе к информации и образовательным ресурсам. Поддержка гарантированного доступа к онлайн-ресурсам для всех слоев населения и стимулирование инвестиций в цифровую инфраструктуру через законодательные меры являются ключевыми шагами для создания более инклюзивного и равноправного цифрового общества в Республике Казахстан.

В ходе исследования правовых и этических аспектов защиты прав граждан в цифровом пространстве были выделены ключевые моменты. В первую очередь, актуальность проблемы подчеркнута необходимостью адаптации законодательства к быстро меняющейся цифровой среде.

Сводка результатов позволяет утверждать, что существующие правовые механизмы часто не соответствуют развитию технологий, что создает пробелы в защите прав граждан. Выводы исследования подчеркивают важность сбалансированного подхода, учитывающего и цифровые инновации, и основополагающие права человека.

В перспективе необходимо активное взаимодействие между государственными органами, обществом и технологическим сектором. Будущее развитие защиты прав граждан в цифровом пространстве требует усиленного внимания к этическим стандартам, а также разработке гибких правовых рамок, способных эффективно реагировать на вызовы цифровой эры.

В заключение можно отметить, что только в совокупности правовых норм, этических принципов и активного взаимодействия различных сторон можно обеспечить надежную защиту прав граждан в динамично развивающемся цифровом мире.

Список использованных источников:

1. <https://www.ohchr.org/ru/topic/digital-space-and-human-rights>
2. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»/ <https://www.online.zakon.kz>
3. Закон Республики Казахстан от 21 мая 2013 года N 94-V. О персональных данных и их защите. <https://www.adilet.zan.kz>
4. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269. Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы. <https://www.adilet.zan.kz>
5. Закон Республики Казахстан от 14 июля 2022 года № 141-VII. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации, информационной безопасности и образования. <https://www.online.zakon.kz>

ӘОЖ 340.114

Аскербекова Арай

«Әділет» Жоғары құқық мектебінің

2 курс студенті

Каспий қоғамдық университеті

Қазақстан Республикасы, Алматы қ.

САНДЫҚ КЕҢІСТІКТЕГІ ҚҰҚЫҚ БҰЗУШЫЛЫҚ ПРОФИЛІН ЖАСАУ ЖӘНЕ АЛДЫН АЛУ

Аңдатпа

Ұсынылған мақала халықаралық құқық және Қазақстан Республикасының ұлттық заңнамасы тұрғысынан ақпараттандыру саласындағы құқық бұзушылықтың негізгі түрлерін анықтау мәселесіне арналған. Автор ақпарат саласында IT-технологиялар арқылы жасалған қылмыстық құқық ғылымына белгілі заңсыз әрекеттерді қарастыруға

әрекет жасаған. Зерттеу барысында жалпы ғылыми және жеке ғылыми танымның әдістерін белсенді қолдану арқылы ақпараттық технологиялар саласындағы құқық бұзушылықтарды талдау жүргізіліп, салыстырмалы талдау әдісі белсенді түрде қолданылды.

Түйінді сөздер: құқық бұзушылықтар, профиль, кибер қылмыс, ақпараттандыру, IT-технологиялар.

Аскербекова Арай

Студентка 2 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

**СОЗДАНИЕ ПРОФИЛЯ ПРАВОНАРУШИТЕЛЯ
И ПРЕДОТВРАЩЕНИЕ ПРЕСТУПНОСТИ
В ЦИФРОВОМ ПРОСТРАНСТВЕ**

Аннотация

Представленная статья посвящена проблеме определения основных видов правонарушений в сфере информатизации с точки зрения норм международного права и национального законодательства Республики Казахстан. Автор предприняла попытку рассмотреть известных науке уголовного права противоправные деяния, совершаемых посредством IT-технологий в сфере информатизации. В ходе исследования проведен анализ правонарушений в сфере информатизации посредством активного применения как общенаучных, так и частно-научных методов познания, активно применялся метод сравнительного анализа.

Ключевые слова: правонарушение, профиль, киберпреступление, информатизация, IT-технологии.

Askerbekova Arai

2nd year student

Higher School of Law “Adilet”

Caspian Public University

Republic of Kazakhstan, Almaty

**OFFENDER PROFILING AND DIGITAL
CRIME PREVENTION**

Annotation

The presented article is devoted to the problem of determining the main types of offenses in the field of informatization from the point of view of international law and national legislation of the Republic of Kazakhstan. The author made an attempt to consider illegal acts known to the science of criminal law, committed through IT technologies in the field of information. In the course of the study, an analysis of offenses in the field of information technology was carried out through the active use of both general scientific and private scientific methods of cognition, and the method of comparative analysis was actively used.

Key words: offense, profile, cybercrime, informatization, IT technologies.

Сандық кеңістіктегі құқық бұзушылық профилін жасау және алдын алу

Ақпараттық технологиялардың үздіксіз дамуы адам өмірінің барлық салаларын компьютерлік технологиялармен және ғаламдық коммуникациялық желілермен бір немесе басқа жолмен байланыстыруға әкелді. Қазіргі әлемде қылмыстың жаңа түрлерінің – компьютерлік қылмыстардың пайда болуына дәл IT-технологиялардың белсенді дамуы себеп болғанын атап өткен жөн.

Компьютерлік қылмыстардың айрықша ерекшелігі де олардың трансұлттық сипаты болып табылады. Елдер арасындағы шекара, қашықтық, қарым-қатынас тілдеріндегі айырмашылық енді үлкен мәнге ие емес. Қоғамның компьютерлендіру деңгейі, компьютерлерге қол жеткізу мүмкіндігі, бағдарламашыларға ортақ тиісті арнайы білімдер анықтау факторлары болып табылады.

Осылайша, бұл компьютерлік қылмыстар бойынша құқықтық нормаларды біріздендіру қажеттілігін және ұлттық құқықтық нормаларды жасау кезінде компьютерлік қылмыспен күресудің шетелдік тәжірибесіне үнемі сілтеме жасау қажеттілігін білдіреді.

1. «Ақпараттандыру саласындағы құқық бұзушылықтар» терминін тар мағынада анықтау мәселелері.

Қазақстан Республикасының Қылмыстық кодексіне өзгертулер енгізілді, ол 2015 жылғы 1 қаңтардан бастап қолданысқа енгізілген жаңа редакцияда қабылдауды талап етті. Осы редакцияда қылмыстық құқық және криминология ғылымының эволюциясында жаңа өзгерістер енгізілді, кейбір актілер халықаралық проблемаларды ескере отырып қайта қаралды. Реформалар компьютерлік технологиялар мен ақпараттандыру сияқты саланы назардан тыс қалдырған жоқ. Бұрын

осы саладағы қылмыстар үшін жауаптылық Қазақстан Республикасы Қылмыстық кодексінің 227-бабында [1] көзделген болатын. Дегенмен, үнемі дамып келе жатқан компьютерлік технологияларға байланысты IT-технологиялар арқылы жасалған заңсыз әрекеттер үшін диспозицияларды және сәйкесінше санкцияларды қайта қарау мәселесі ерекше өзектілікке ие болды.

Барлық қылмыстар сияқты олар объектісіне, қол сұғушылық субъектісіне, жасалу тәсілдеріне және т.б. түрлерге бөлінеді [2]

АТ қылмыстарының негізгі түрлері туралы мәселені қарастырған кезде бұл қылмыстар компьютерлік қылмыстар және киберкеңістікке қол жеткізуге мүмкіндік беретін ғаламдық коммуникациялық желілер арқылы жасалған қылмыстар болып бөлінетінін атап өткен жөн [3]

Бұл классификацияны БҰҰ да қолданады, қылмыстық әрекеттің бұл түрін «кең» және «тар» мағынада киберқылмысқа бөледі. Бұл классификация компьютерлік қылмыстардың бір объектілі және көп объектілі болып бөлінуіне де сәйкес келеді [4]

Осыған байланысты Т.Д.Тропинаның пікірімен келіспеске болмайды, ол былай деп атап көрсетеді: «Тар мағынада компьютерлік қылмыстар – бұл негізгі қол сұғушылық объектісі компьютерлік деректер мен жүйелердің құпиялылығы, тұтастығы, қолжетімділігі және қауіпсіз жұмыс істеуі болып табылатын қылмыстар. .

Кең мағынада компьютерлік қылмыстар - бұл компьютерлік жүйелерден басқа басқа объектілерге (негізгілері ретінде): қоғам мен адамның қауіпсіздігіне (кибертерроризм), меншік пен мүліктік құқықтарға (ұрлық, компьютерлік жүйелер арқылы жасалған алаяқтық немесе) қол сұғатын қылмыстар. киберкеңістік), авторлық құқықтар (плагиат және қарақшылық) [2]

Кең мағынада компьютерлік қылмыстар – бұл компьютерлік жүйелерден басқа басқа объектілерге (негізгілері ретінде): қоғам мен адам қауіпсіздігіне (кибертерроризм), меншік және мүліктік құқықтарға (ұрлық, компьютерлік жүйелер арқылы жасалған алаяқтық немесе киберкеңістік), авторлық құқықтар (плагиат және қарақшылық) « (Тропина, 2005: 44).

Сонымен, Қазақстан Республикасының қолданыстағы қылмыстық заңнамасына сәйкес ақпараттандыру саласындағы қылмыстық құқық бұзушылықтар:

– Ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне заңсыз қол жеткізу (ҚР ҚК 205-бабы);

– ақпаратты заңсыз жою немесе өзгерту (ҚР ҚК 206-бабы);

- Ақпараттық жүйенің немесе телекоммуникация желілерінің жұмысын бұзу (ҚР ҚК 207-бап);
- Ақпаратты заңсыз алу (ҚР ҚК 208-бабы);
- ақпаратты беруге мәжбүрлеу (ҚР ҚК 209-бап);
- Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату (Қазақстан Республикасы Қылмыстық кодексінің 210-бабы);
- қолжетімділігі шектеулі электрондық ақпараттық ресурстарды заңсыз тарату (ҚР ҚК 211-бап);
- Заңсыз мақсаттарды көздейтін интернет-ресурстарды орналастыру бойынша қызмет көрсету (ҚР ҚК 212-бап).

Киберқылмыстардың толық тізімі Еуропа Кеңесінің Киберқылмыс туралы конвенциясында берілген. Атап өткендей, Конвенцияның баптары қазіргі уақытта киберкеңістіктегі барлық заңсыз әрекеттерді қамтиды.

Осылайша, бұл конвенция «тар» мағынада компьютерлік қылмыстың бес түрін анықтайды:

1. заңсыз қол жеткізу (2-бап);
2. заңсыз ұстап алу (3-бап);
3. деректерге араласу (тұтастықты бұзу) (4-бап);
4. жүйеге араласу (5-бап).
5. Құрылғыларды заңсыз пайдалану -
 - (а) өндіру, сату, пайдалану үшін сатып алу, импорттау, көтерме немесе басқа пайдалану нысандары:
 - (i) құрылғылар, соның ішінде компьютерлік бағдарламалар, ең алдымен бапта көрсетілген құқық бұзушылықтарды жасау мақсатында әзірленген немесе бейімделген. 2 – 5;
 - (ii) осы бапта көрсетілген қылмыстарды жасау мақсатында оларды пайдалану ниетімен компьютерлік жүйеге тұтастай немесе оның кез келген бөлігіне қол жеткізуге болатын компьютерлік құпия сөздер, кіру кодтары немесе басқа ұқсас деректер. 2 – 5;
 - б) жоғарыда аталған заттардың біреуін бапта көрсетілген қылмыстарды жасау мақсатында пайдалану мақсатында иелену. 2 – 5 (6-бап) [5]

Осыған орай, өркениетті қоғамның осы қылмыс түрлерімен күресу мәселесімен шындап айналысуы маңызды. Бұл Еуропа Кеңесінің киберқылмыстың қиындықтарына арналған баяндамасында, яғни жоғарыда аталған Конвенция негізінде жасалған киберқылмысты жіктеуде қылмыстың бұл түрі «ЦРУ-құқық бұзушылықтар» ретінде

белгіленген, яғни. Құпиялылық, тұтастық (Integrity) және компьютерлік деректер мен жүйелердің қолжетімділігі [6]

Ақпараттандыру саласындағы құқық бұзушылықтың негізгі түрлерін анықтаудың тұжырымдамалық мәселелері

Осы санатқа кіретін нақты қылмыстардың қатарына компьютерді бұзу, хабарламаларды ұстау, интернет пайдаланушыларды алдау (мысалы, спуфинг, фишинг арқылы), компьютерлік тыңшылық (соның ішінде трояндық аттарды және басқа технологияларды пайдалану), компьютерлік диверсия және бопсалау (үшін). мысалы, вирустар мен құрттарды қолдану, DOS шабуылдары, спам жіберу және пошталық бомбалау) [7]

2. Кең мағынада «ақпараттандыру саласындағы құқық бұзушылық» терминін анықтау мәселелері.

Осы бапта бұрын айтылғандай, «тар» мағынадағы қылмыстардан басқа «кең» мағынадағы қылмыстар:

1. Компьютермен байланысты құқық бұзушылықтар:

– компьютерлік жалғандық (7-бап), оның ішінде онлайн-күтім жасау;

– компьютерлік алаяқтық (8-бап).

2. Балалар порнографиясы жатқызылған мазмұнға (деректер мазмұнына) байланысты қылмыстар (9-бап).

Еуропа Кеңесінің баяндамасына сәйкес, бұл қылмысқа сонымен қатар: ақыл-кеңес беру, айдап салу, қылмыс жасауға, оның ішінде кісі өлтіруді, зорлауды, азаптауды, саботажды және терроризмді жасауға нұсқау беру және ұсыныстар беру арқылы «көмек көрсету» жатады. Бұл санатқа киберқорлау, жала жабу, интернет арқылы жалған ақпарат тарату және интернет арқылы құмар ойындар да кіреді. [8]

3. Авторлық және сабақтас құқықтарды бұзуға байланысты құқық бұзушылықтар. Мұндай қылмыстардың түрлері Конвенцияда бөлектелмеген; оларды белгілеу құжатпен мемлекеттердің ұлттық заңнамаларының құзыретіне жатқызылған;

4. 2002 жылдың басында Конвенцияға нәсілдік және нәсілдік белгілері бойынша жеке адамды немесе адамдар тобын зорлық-зомбылыққа, өшпенділікке немесе кемсітуге шақыратын ақпаратты тарату қылмыстар тізіміне қосылған хаттама қабылданды. , ұлты, діні немесе этникалық. Еуропа Кеңесінің есебінде бұл қылмыстар тобы деректер мазмұнына байланысты қылмыстарға жатқызылады [9]

Дегенмен, біз қарастырып отырған конвенцияда барлық қылмыстар қарастырылмағанын, жеке өмірге қарсы қылмыстарға қатысты екенін

мойындаған жөн. Бұл олқылық жеке өмірге қол сұғу, оның ішінде жеке деректерді қамтитын жүйелерге заңсыз қол жеткізу, жеке деректерді жинау, тарату және біріктіру немесе cookie файлдары, веб қателер және т.б. бағдарламалық қамтамасыз ету.

Компьютерлік қылмыстардың барлық осы түрлерін қарастырғанда, тар және кең мағынада, бұл қиын емес, олардың барлығы ақпараттық қылмыстар болып табылатынын көру, өйткені олардың барлығы, әйтеуір, кейбір авторлар атап өткендей, ақпараттық қауіпсіздікке, қатынастарға жүктейді, олардың қосымша объектісі болып табылады, сондай-ақ қылмыс субъектісі ретіндегі ақпаратқа немесе ақпараттық ықпалға ие. қылмыс жасау тәсілі [10]

Кең мағынада компьютерлік қылмыстар компьютерді қолдану арқылы жасалатын қылмыстардың дәстүрлі түрлері болып табылады. Қылмыстың бұл түрлері, жоғарыда көрсетілгендей, Конвенцияда арнайы анықталған және тар мағынада компьютерлік қылмыстармен қатар қарастырылған.

Шет мемлекеттердің заңнамаларын талдай келе, оның дәстүрлі қылмыс түрлерімен қатар олардың қылмыстық заңдарының көптеген тарауларында компьютерді пайдалана отырып қылмыс жасаудың жеке нормалары болатындай етіп өзгертілгенін анықтадық.

Бұл тәсіл компьютерлік құралдарды пайдалана отырып жасалған әрекет дәстүрлі және компьютерлік қылмыстардың жиынтығы бойынша сараланған және сол сияқты ауыр жаза қолданылатын Қазақстан Республикасының қолданыстағы ұлттық заңнамасы шеңберінде қолданылатын тәсілге қарағанда неғұрлым негізделген болып көрінеді. дәстүрлі тәсілдермен әрекет етеді.

3. Қазақстан Республикасының және кейбір шет мемлекеттердің ұлттық заңнамасына сәйкес ақпараттандыру саласындағы құқық бұзушылықтардың құқықтық сипаты.

Қазіргі уақытта компьютерлік технологиялар біздің өміріміздің барлық салаларына іс жүзінде еніп, қалыпты жағдайға айналды, сондықтан электронды құралдарды пайдалана отырып, дәстүрлі қылмыс жасағаны үшін неғұрлым қатаң жаза қолдану тәсілі қазіргі заманғы шындыққа сәйкес келмейді [11]

Осыған байланысты сынға компьютерлік құралдарды пайдалануды квалификациялайтын дәстүрлі қылмыстарды енгізу бойынша ұсыныстар да жасалуы мүмкін деген А.Ф.Мицкевич пен С.С.Медведевтің пікірімен келіскен жөн [4]; [12] Себебі, мұндай реформаларды жүзеге асыру қылмыстық жауапкершілікті негізсіз арттыруға ықпал етеді, сонымен қатар қылмыстың осы түрінің ерекшеліктерін көрсете алмайды.

Осылайша, кең мағынада компьютерлік қылмыстар дәстүрлі қылмыс түрлеріне қарағанда компьютерлік қылмыстардың белгілері көбірек болатын қылмыстардың дербес категориясы болып табылады.

Алайда Қазақстанның қылмыстық заңнамасы ғана дұрыс емес деп қателесуге болмайдыжағандық коммуникациялық желілерде қылмыспен күресуге бағытталған Қылмыстық кодекстің нормаларын жетілдіреді. Кең мағынада компьютерлік қылмыстарды заңнамалық реттеудің осындай кемшіліктеріне ресейлік криминалистер де назар аударады. Атап айтқанда, Б.Д. Завидов ұялы желілердегі алаяқтыққа қылмыстық-құқықтық талдау жүргізді, оны компьютерлік алаяқтықтың ерекше жағдайы ретінде қарастыруға болады.

Ғалым өз тұжырымдарында алаяқтықтың осы түрі үшін жауапкершілік туралы қолданыстағы заңнаманы жетілдіру қажеттігін атап өтті.

Соңында, Б.В.Завидов электрондық алаяқтықпен күресте шетелдік тәжірибені пайдалану қажеттігін атап өтті, мұнда бұл әрекеттер қылмыстық заңнамада бұрыннан қарастырылған және мұндай қылмыстарды тергеу әдістері белгіленген. Голландия Қылмыстық кодексінің 326-бабы «Қызметтерді алдау арқылы ұрлық», ол телекоммуникациялар арқылы халыққа ұсынылатын қызметті пайдалану, технологиялық құралдарды пайдалану немесе толық пайдаланудан жалтару үшін жалған сигналдарды пайдалану үшін жауапкершілікті белгілейді. Сонымен қатар, автор нарықтың қатынастардың инфрақұрылымының дамуы алаяқтыққа белгілі бір әсер ететінін көрсетеді, ол барған сайын жаңа, «сорттар» және «кіші түрлер» болып табылады. Заңнама реттеуді былай қойғанда, олардың қарқынды дамуын қадағалай алмайды, өйткені алаяқтықтың кейбір түрлері (мысалы, компьютерді пайдаланып ақша ұрлау) оның стандартты шеңберіне сәйкес келмейді [13]

Осылайша, кең мағынада компьютерлік қылмыстармен тиімді күресу үшін ақпараттық технологиялар саласындағы соңғы әзірлемелер мен заңнамалық деңгейде уақтылы өзгерістер енгізу қажеттілігі айқын болады.

Қазақстан заңнамасында ақпараттандыру саласындағы құқық бұзушылықтар Қазақстан Республикасы Қылмыстық кодексінің 7-тарауында қамтылған нормалармен тар шеңберде айқындалады. Бұл тарау ақпарат саласындағы қатынастарды қылмыстық-құқықтық реттеудің қолданыстағы тәжірибесін сіңірген заңнаманың қайта қаралған нұсқасы болып табылады, бірақ ақпараттық технологиялар айтарлықтай белсенді дамып жатқанын мойындау керек, бұл қылмыстық заңнаманы тұрақты және уақтылы жетілдіруді талап етеді. Қазақстан Республикасының.

Бұл нормаларда: компьютерлік ақпаратқа заңсыз қол жеткізу, компьютерлер үшін зиянды бағдарламаларды жасау, пайдалану және тарату, ұялы байланыс абоненттік бірлігінің сәйкестендіру кодын, абонентті сәйкестендіру құрылғыларын дұрыс өзгертпеу, сондай-ақ компьютерлік ақпаратқа заңсыз қол жеткізу сияқты әрекеттер бойынша құқық бұзушылықтар жабылады. өзгертуге арналған бағдарламаларды құру, пайдалану, тарату, абоненттік бірлік сәйкестендіру коды [14]

Қарастырылып отырған қылмыстардың отбасылық объектісі қоғамдық қауіпсіздік пен қоғамдық тәртіпті қамтамасыз ету жөніндегі қоғамдық қатынастар; Түрлердің объектісі – компьютерлерде (компьютерлік жүйелерде) деректерді сақтаудың, өңдеудің және берудің қалыпты режимін қамтамасыз ететін қоғамдық қатынастар; қосымша объект – ақпараттық қауіпсіздікті қамтамасыз ету бойынша қоғаммен байланыс [15]

Деректер қарастырылып отырған композициялардың тақырыбы болып табылады. Компьютерлік қылмыстарды жасаудағы заңсыз әрекеттердің нәтижесі құпиялылықты жоғалту, тұтастықты бұзу және объектілерге (жабдықтарға) және деректерге қол жеткізуді жоғалту болып табылады [16]

Осылайша, тергелетін құқық бұзушылықтардың құрамы бар.

Республикасы Қылмыстық кодексінің 7-тарауында көрсетілген қылмыстар – қылмыстың объектісі мен субъектісінің ерекше сипаты бойынша ақпараттық сипаттағы қылмыстар;

– Қазақстан Республикасының қолданыстағы қылмыстық заңнамасында Қазақстан халықаралық қатынастардың толыққанды қатысушысы болғанына қарамастан, компьютерлік қылмыстар туралы баптардың мазмұнына қатысты Киберқылмыс туралы конвенцияға елеулі сәйкессіздіктер бар.

Бұл жаһандық коммуникациялық желілер арқылы жасалатын қылмыс түрлерінің кең ауқымды екенін білдіреді, бұл қылмыстың осы түрінің алдын алуға және оған қарсы күресуге бағытталған іс-шараларды әзірлеуде белгілі бір қиындықтар туғызады, соғұрлым қазіргі ұлттық қылмыстық- Қазақстан Республикасының заңнамасын қанағаттанарлық және бар шындыққа сәйкес деп санауға болмайды, өйткені ҚР Қылмыстық кодексінің өркениетті әлемдік қоғамдастықтың қылмыстық заңнамасының нормаларына сәйкес келмеуі, біріншіден, елемейді. Еуропада және басқа да шет елдерде бар компьютерлік қылмыспен күресудегі бай тәжірибе, екіншіден, көбінесе трансұлттық сипатта болатын компьютерлік қылмыстарды тергеуде шетелдік әріптестермен дұрыс ынтымақтасуға мүмкіндік бермейді.

Пайдаланылған қайнар көздерінің тізімі:

1. Қазақстан Республикасы Қылмыстық кодексі
2. Тропина, 2005: 44
3. Бражник, 2003:27
4. Мицкевич, 2004: 19
5. Foltz C Bryan, 2004: 154
6. Марко Герке, 2009
7. Dhillon, 2004: 557
8. Скоромников, 2010: .218
9. Coleman C., 2003:95, Richardson R.,1998: 108
10. Beardwood John P., Alleyne Andrew C., 2006: 62, Shinder, Debra L., 2003:136
11. Еалы, А. ,16
12. Медведев С.С., 2008: 67
13. Завидов Б.Д., 1998: 16; Бреннер Сюзан В., 2004: 19
14. Нұрпейісова А.Қ., 2010: 64
15. Биебаева А.А., 2007:137).
16. Н. Полевого, 1998:127; Фурнелл С.М., Камини Дашора

УДК 347.2

Балтабаева Жансая Рауажовна

Студентка 1 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Научный руководитель:

Мухтарова А.К.

к.ю.н., профессор

Высшей школы права «Әділет»

Каспийского общественного университета

Аннотация

Данная статья предоставляет с собой обзор искусственного интеллекта (ИИ), начиная с середины XX века и охватывая ключевые аспекты его развития и применения. Искусственный интеллект не только улучшают эффективность и точность в различных областях, но также приносят новые возможности, изменяя способы, которыми люди взаимодействуют с технологией в повседневной жизни. В работе рассматриваются основные подходы к ИИ, включая символичный, статистический и подход на основе машинного обучения, с акцентом на роли машинного обучения в современном развитии искусственного интеллекта. Особое внимание уделяется применению ИИ в различных отраслях, таких как медицина, банковское дело и автомобильная промышленность, демонстрируя, как технологии искусственного интеллекта способствуют повышению эффективности и точности в этих областях. Статья затрагивает важные вопросы этики и безопасности, связанные с развитием ИИ, поднимая проблемы автономных систем, конфиденциальности данных и общественной ответственности.

Ключевые слова: искусственный интеллект, символичный и статистический подход, машинное обучение, эффективность.

Балтабаева Жансая Рауажовна

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,

Қазақстан Республикасы, Алматы қ.

ЖАСАНДЫ ИНТЕЛЛЕКТ

Аңдатпа

Бұл ғылыми жоба жасанды интеллекттің XX ғасырдың ортасынан және оның дамуы мен қолданылуының негізгі аспектілерінің шолуы. Жасанды интеллект тек қана түрлі саладағы тиімділік пен дәлдікті жақсартпайды, онымен қоса ол күнделікті өмірдегі адам мен технология арасындағы өзара қарым-қатынастарды өзгерте отырып, жаңа мүмкіндіктер ашады. Жұмыста жасанды интеллекттің заманауи дамуындағы машиналық оқытудың рөліне баса назар аудара отырып, символдық, статистикалық және машиналық оқытуға негізделген тәсілді қоса алғанда, жасанды интеллектке негізгі тәсілдер қарастырылады. Аса қатты көңіл жасанды интеллекттің түрлі саладағы қолданылуына бөлінеді, мысалы медици-

на, банк және автокөлік өнеркәсібінде, себебі жасанды интеллект осы салалардағы нақтылық пен тиімділікті арттырады. Жұмыс автономды жүйелер, деректердің құпиялылығы және қоғамдық жауапкершілік мәселелерін көтере отырып, жасанды сананың дамуымен байланысты этика мен қауіпсіздіктің маңызды мәселелерін шешеді.

Түйінді сөздер: жасанды интеллект, символдық және статистикалық тәсіл, машиналық оқыту, тиімділік.

Baltabayeva Zhansaya

1st year student of High School of Law “Adilet”
Caspian Public University
Republic of Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE

Annotation

This research paper provides an overview of Artificial Intelligence (AI) from the mid-twentieth century onwards, covering key aspects of its development and applications. Artificial Intelligence not only improves efficiency and accuracy in a variety of fields, but also brings new capabilities by changing the ways in which people interact with technology in everyday life. The paper reviews the main approaches to AI, including symbolic, statistical and machine learning-based approaches, with a focus on the role of machine learning in the current development of artificial intelligence. Particular attention is paid to the application of AI in various industries such as medicine, banking and automotive, demonstrating how AI technologies are contributing to efficiency and accuracy in these fields. The work addresses important ethical and safety issues related to the development of AI, raising concerns about autonomous systems, data privacy, and public responsibility.

Keywords: artificial intelligence, symbolic and statistical approach, machine learning, efficiency.

Искусственный интеллект — это возможность искусственных интеллектуальных систем выполнять творческие функции, которые традиционно считаются незаменимым трудом человека; наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ. Искусственный интеллект связан с похожей целью использования технологии для понимания человеческого склада ума,

но не обязательно ограничивается биологически правдоподобными методами. Существующие на сегодняшний день интеллектуальные системы имеют довольно узкие области применения, но прогрессируют с каждым днем. Искусственный интеллект (ИИ) представляет собой уникальную область компьютерных наук, посвященную созданию интеллектуальных систем, способных анализировать данные, извлекать закономерности и принимать решения, подобные тем, что принимает человеческий разум. С течением времени ИИ стал неотъемлемой частью современной технологической эры, изменяя способы взаимодействия людей с машинами и влияя на множество областей нашей повседневной жизни.

Термин «искусственный интеллект» (или «AI» в английском варианте) впервые был введен в обиход и использован американским ученым Джоном Маккарти в 1955 году на семинаре в Дартмутском университете. По его словам, искусственный интеллект - это наука и инженерия о создании интеллектуальных машин, особенно интеллектуальных компьютерных программ. Она связана с аналогичной задачей использования компьютеров для понимания человеческого интеллекта, но ИИ не обязательно должен ограничиваться методами, поддающимися биологическому наблюдению. Он использовал термин «искусственный интеллект» для обозначения нового направления исследований, целью которого было создание программ, способных выполнять задачи, требующие интеллектуальных способностей человека. Джон Маккарти указывает: «Проблема состоит в том, что пока мы не можем в целом определить, какие вычислительные процедуры мы хотим называть интеллектуальными. Мы понимаем некоторые механизмы интеллекта и не понимаем остальные. Поэтому под интеллектом в пределах этой науки понимается только вычислительная составляющая способности достигать целей в мире».

В своей известной статье «Вычислительная машина и интеллект» («Computing Machinery and Intelligence»), которая была опубликована в журнале «Майнд» («Mind») в 1950 году, английский математик и логик Алан Тьюринг предложил знаменитый Тест Тьюринга, который стал одним из ключевых понятий в области искусственного интеллекта. В контексте этой статьи, Тьюринг использовал термин «интеллектуальная машина», но сам термин «искусственный интеллект» не был введен им в этот момент. Стандартная интерпретация этого теста выглядит так: «Человек взаимодействует с одним компьютером и одним человеком.

На основании ответов на вопросы он должен определить, с кем он разговаривает: с человеком или компьютерной программой. Задача компьютерной программы — ввести человека в заблуждение, заставив сделать неверный выбор». Все участники теста не видят друг друга. Самый общий подход предполагает, что искусственный интеллект будет способен проявлять поведение, не отличающееся от человеческого, причём в нормальных ситуациях. Эта идея является обобщением подхода теста Тьюринга, который утверждает, что машина станет разумной тогда, когда будет способна поддерживать разговор с обычным человеком, и тот не сможет понять, что говорит с машиной.

Основные подходы к искусственному интеллекту (ИИ) представляют собой разнообразные стратегии и методы, которые позволяют инженерам и исследователям создавать и развивать интеллектуальные системы. Использование различных подходов обусловлено необходимостью решения разнообразных задач и проблем, а также их соответствия контексту и требованиям конкретных приложений. В области искусственного интеллекта существует несколько основных подходов к созданию интеллектуальных систем. Каждый из них имеет свои особенности и применяется в различных контекстах.

Символьный подход в искусственном интеллекте (ИИ) представляет собой метод, основанный на манипуляциях символами и символьными выражениями для представления и обработки знаний. Этот подход стремится моделировать человеческое мышление, где знание представлено в виде символов и логических отношений между ними. В символьном подходе информация представляется в виде символов, которые могут быть символами языка, словами, фразами, или более абстрактными концептами. Знания выражаются с использованием логических отношений и правил. Символьный подход часто использует логические операции для рассуждений и вывода новой информации. Применяются формальные логические правила, такие как модус поненс или резолюция, для делегирования выводов и принятия решений. Главная особенность символьных вычислений — создание новых правил в моменте выполнения программы. Тогда как возможности не интеллектуальных систем завершаются как раз перед способностью хотя бы обозначать вновь возникающие трудности. Тем более эти трудности не решаются и в конце компьютер не совершенствует такие способности самостоятельно.

В контексте искусственного интеллекта, термин «статистический подход» обычно относится к методам, основанным на обработке и

анализе статистических данных с целью извлечения шаблонов, закономерностей и информации. Этот подход играет ключевую роль в области машинного обучения и статистического моделирования. Статистический подход эффективно работает с большими объемами данных. Алгоритмы машинного обучения, такие как методы классификации и регрессии, используют статистические методы для обучения на больших данных и принятия решений. В статистическом подходе важное место занимают методы машинного обучения, включая обучение с учителем (с учителем), обучение без учителя и обучение с подкреплением. Эти методы используют статистические техники для обучения моделей на основе данных.

Машинное обучение (Machine Learning, ML) — это область искусственного интеллекта, которая занимается разработкой алгоритмов и моделей, способных «обучаться» на основе данных, выявлять закономерности и принимать решения без явного программирования. В основе машинного обучения лежит идея создания систем, которые могут улучшать свою производительность с опытом. Машинное обучение предполагает создание моделей, которые могут обучаться на данных и принимать решения без явного программирования. Это включает в себя обучение с учителем (с учителем), обучение без учителя и обучение с подкреплением. Проблематика машинного обучения касается процесса самостоятельного получения знаний интеллектуальной системой в процессе её работы. Это направление было центральным с самого начала развития искусственного интеллекта. В 1956 году, на Дартмутской летней конференции, Рей Соломонофф написал отчёт о вероятностной машине, обучающейся без учителя, назвав её: «Индуктивная машина вывода».

Искусственный интеллект (ИИ) оказывает значительное влияние на различные аспекты человеческой жизни, и его значение продолжает увеличиваться по мере развития технологий. Сейчас в мире два направления развития искусственного интеллекта, это решение проблем, связанных с приближением специализированных систем искусственного интеллекта к возможностям человека, и их интеграции, которая реализована природой человека и создание искусственного разума, представляющего интеграцию уже созданных систем искусственного интеллекта в единую систему, способную решать проблемы человечества. Есть несколько популярных систем искусственного интеллекта. Они: ChatGPT, DeepBlue, AlphaGo, Watson, MYCIN, 20Q, ViaVoice и Midjourney.

Также ИИ используется в разных отраслях в мире. ИИ используется для обработки медицинских данных, анализа снимков и выявления паттернов, что способствует более точной диагностике и предоставлению эффективных методов лечения. В радиологии ИИ используется для анализа медицинских изображений, таких как рентгеновские снимки, маммографии, компьютерные томографии (КТ) и магнитно-резонансная томография (МРТ), для выявления аномалий и диагностики заболеваний. ИИ может автоматизировать анализ медицинских проб, улучшая эффективность и точность результатов. Анализ крови, мочи и других биологических образцов с использованием алгоритмов машинного обучения. Хирургические роботы, управляемые ИИ, обеспечивают точность и точность в процессе хирургических вмешательств. Роботизированные системы для выполнения сложных и малоинвазивных процедур. Алгоритмы машинного обучения используют данные о пациентах для прогнозирования вероятности развития определенных заболеваний. В области бизнес и финансы ИИ способен анализировать большие объемы данных на финансовых рынках, прогнозировать тенденции и предоставлять рекомендации для принятия решений. В бизнесе ИИ применяется для оптимизации производственных процессов, управления цепями поставок и предсказания потребительского спроса. ИИ ускоряет процессы обработки и анализа огромных объемов данных в научных исследованиях, способствуя выявлению новых закономерностей и тенденций. А в области транспорта развитие автономных автомобилей и систем управления транспортом на основе ИИ обещает повысить безопасность дорожного движения и эффективность транспортных сетей. Если брать в учет образование, то ИИ может адаптировать образовательные программы в соответствии с индивидуальными потребностями студентов, обеспечивая более эффективное обучение. Также ИИ используется для автоматизации рутинных задач в образовании, что позволяет педагогам уделять больше времени творческому обучению, улучшает распознавание речи, машинный перевод и генерацию текста, делая коммуникацию на разных языках более доступной. Все эти примеры свидетельствуют о том, что ИИ не только улучшает эффективность и точность в различных областях, но также приносит новые возможности, изменяя способы, которыми люди взаимодействуют с технологией в повседневной жизни.

Развитие и внедрение искусственного интеллекта (ИИ) вызывают не только технические и научные вопросы, но и ряд этических и безопас-

ностных аспектов. Внедрение автономных систем, способных принимать решения без участия человека, поднимает вопросы ответственности за действия этих систем. Разработка четких стандартов и законов, определяющих ответственность за поведение автономных систем, а также регулярные аудиты и оценки безопасности. Некоторые алгоритмы машинного обучения, особенно в глубоком обучении, могут быть сложными и труднопонимаемыми для человека, что затрудняет объяснение принятых ими решений. Развитие методов, обеспечивающих объяснимость решений, а также поощрение открытости и прозрачности в процессах разработки и внедрения ИИ. Большие объемы данных, используемых для обучения алгоритмов ИИ, могут содержать личную и чувствительную информацию, что создает риски для конфиденциальности. Внедрение строгих правил и технологий обеспечения безопасности данных, шифрование, анонимизация и соблюдение соответствующих нормативных требований. Алгоритмы рекомендаций и персонализации могут создавать “фильтровые пузыри”, искажая восприятие реальности и создавая ограниченный опыт пользователя. Разработка алгоритмов, способных предоставлять разнообразную информацию, а также поощрение многообразия и баланса в рекомендациях.

Будущее искусственного интеллекта (ИИ) обещает быть увлекательным и трансформационным. Продолжающиеся исследования в области глубокого обучения, а также улучшение вычислительной мощности, позволят создавать более сложные и эффективные модели ИИ. Это приведет к улучшению обработки естественного языка, компьютерного зрения, а также расширению областей применения, таких как автономные автомобили и медицинская диагностика. ИИ будет интегрирован в роботов, что позволит им принимать более сложные решения в реальном времени. Это может привести к развитию автономных роботов, способных выполнять разнообразные задачи, от сложных производственных процессов до домашних обязанностей. Также будет использоваться для создания автономных систем в различных областях, таких как транспорт, здравоохранение и сельское хозяйство. Это может включать в себя автономные транспортные средства, системы управления зданиями и интеллектуальные сельскохозяйственные роботы. Развитие ИИ, способного понимать и взаимодействовать с людьми на более глубоком уровне, может привести к созданию искусственного общественного интеллекта. Это включает в себя системы, способные понимать человеческие эмоции, социальные контексты и этические аспекты. С развити-

ем ИИ становится все более важным решение этических вопросов, связанных с его использованием. Вопросы прозрачности, ответственности и безопасности станут ключевыми аспектами разработки и внедрения ИИ-технологий. Важно отметить, что с развитием ИИ возникают и ряд вызовов, таких как угрозы приватности, потенциальное увеличение социальных неравенств и необходимость эффективного управления рисками. Успешное будущее ИИ потребует внимательного внедрения и сбалансированного подхода к его развитию и использованию.

Искусственный интеллект стал неотъемлемой частью нашей повседневной жизни, оказывая влияние на различные аспекты общества и промышленности. С его дальнейшим развитием необходимо внимательное отношение к этическим вопросам и обеспечение безопасности внедрения новых технологий. Медицина находится под влиянием передовых технологий ИИ, что приводит к улучшению диагностики, прогнозирования заболеваний и разработке индивидуализированных методов лечения. Однако этот прогресс также вызывает вопросы этики и безопасности, которые требуют внимательного внимания и регулирования. Этические вопросы, такие как прозрачность принятия решений и справедливость алгоритмов, требуют разработки стандартов и законов для обеспечения надлежащего использования ИИ. Безопасность данных, защита приватности и предотвращение злоупотреблений технологиями ИИ также должны быть в центре внимания.

Список использованных источников:

1. <https://www-formal.stanford.edu/jmc/whatisai/whatisai.html>
2. <https://www.loebner.net/Prizef/TuringArticle.html>
3. <https://psm7.com/ru/technology/perspektivy-razvitiya - iskusstvennogo - intellekta-v-2023- godu-analitika.html?ysclid=lq1j4uis1f511269522>

УДК 342.7

Батырхан Дана Кайраткызы

Студентка 1 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ДОСТУПА К ИНТЕРНЕТ РЕСУРСАМ, К ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ

Научный руководитель:

Сагинаев М.Е.

М.ю.н., сеньор- лектор

Высшей школы права «Әділет»

Каспийского общественного университета

Аннотация

Данная статья посвящена актуальной проблеме обеспечения к виртуальным интернет ресурсам и специальным образовательным ресурсам. Особое внимание уделяется к путям и методам их решения. Также рассматривает проблемы, связанные с обеспечением доступа к интернет-ресурсам образовательным учреждениям. В современном образовании интернет играет ключевую роль, предоставляя широкие возможности для получения знаний и развития учащихся. Однако существует ряд проблем, которые затрудняют полноценное использование интернет-ресурсов в образовательном процессе. Например как проблема связана с инфраструктурой. В некоторых областях, особенно в сельской местности или отдаленных районах, отсутствует доступ к широкополосному интернету. Недостаток развитой инфраструктуры создает преграды в получении интернет-соединения образовательными учреждениями и ограничивает возможности студентов в доступе к образовательным ресурсам онлайн.

В заключение, данная статья обращает внимание на важность решения проблем обеспечения доступа к интернет-ресурсам образовательным учреждениям. Обеспечение равного доступа к интернету и

ресурсам является неотъемлемой частью современного образования, и только решение этих проблем позволит полноценно использовать потенциал интернета в образовательном процессе.

Ключевые слова: образовательные ресурсы, интернет, право на образование, образовательные учреждения, образовательный процесс.

Батырхан Дана Кайратқызы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,

Қазақстан Республикасы, Алматы қ.

ИНТЕРНЕТ РЕСУРСТАРЫ МЕН БІЛІМ БЕРУ РЕСУРСТАРЫНА ҚОЛЖЕТІМДІЛІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Аңдатпа

Бұл мақала виртуалды интернет-ресурстар мен Арнайы білім беру ресурстарын қамтамасыз етудің өзекті мәселесіне арналған. Оларды шешудің жолдары мен әдістеріне ерекше назар аударылады. Сондай-ақ білім беру мекемелерінің интернет-ресурстарына қолжетімділікті қамтамасыз етуге байланысты проблемаларды қарастырады. Қазіргі білім беруде интернет білім алуға және оқушылардың дамуына кең мүмкіндіктер бере отырып, шешуші рөл атқарады. Дегенмен, білім беру процесінде интернет-ресурстарды толық пайдалануды қиындататын бірқатар мәселелер бар. Мысалы, мәселе инфрақұрылыммен қалай байланысты. Кейбір аудандарда, әсіресе ауылдық жерлерде немесе шалғай аудандарда кең жолақты Интернетке қол жетімділік жоқ. Дамыған инфрақұрылымның жетіспеушілігі білім беру мекемелерінің интернет байланысын алуына кедергі келтіреді және студенттердің онлайн білім беру ресурстарына қол жеткізу мүмкіндігін шектейді.

Қорытындылай келе, бұл мақала проблемаларды шешудің маңыздылығына назар аударады білім беру мекемелерінің интернет-ресурстарына қолжетімділікті қамтамасыз ету. Интернетке және ресурстарға тең қол жетімділікті қамтамасыз ету қазіргі білім берудің ажырамас бөлігі болып табылады және тек осы мәселелерді шешу білім беру процесінде Интернеттің әлеуетін толық пайдалануға мүмкіндік береді.

Түйінді сөздер: білім беру ресурстары, Интернет, білім алу құқығы, оқу орындары, оқу процесі.

Batyrkhan Dana

1st year student of High School of Law “Adilet”
Caspian Public University
Republic of Kazakhstan, Almaty

PROBLEMS OF PROVIDING ACCESS TO INTERNET RESOURCES AND EDUCATIONAL RESOURCES

Annotation

This scientific work is devoted to the urgent problem of providing access to virtual Internet resources and special educational resources. Special attention is paid to the ways and methods of their solution. It also considers the problems associated with providing access to Internet resources to educational institutions. In modern education, the Internet plays a key role, providing ample opportunities for students to gain knowledge and develop. However, there are a number of problems that make it difficult to fully use Internet resources in the educational process. For example, how the problem is related to the infrastructure. In some areas, especially in rural areas or remote areas, there is no access to broadband Internet. The lack of developed infrastructure creates obstacles in obtaining an Internet connection by educational institutions and limits the ability of students to access educational resources online.

In conclusion, this article draws attention to the importance of problem solving providing access to Internet resources to educational institutions. Ensuring equal access to the Internet and resources is an integral part of modern education, and only solving these problems will make it possible to fully use the potential of the Internet in the educational process.

Key words: educational resources, Internet, right to education, educational institutions, educational process.

Интернет-ресурсы - это веб-сайты, приложения или онлайн-платформы, предоставляющие различные услуги, информацию или развлечения через сеть Интернет.

Положительные стороны интернет-ресурсов включают легкий доступ к информации, возможность общения и совместной деятельности, онлайн-образование, эффективные средства коммуникации и удобство при проведении различных операций, таких как покупки и банковские транзакции. Но и в этой сфере есть свои недостатки. На данное время идут проблемы обеспечения интернет ресурсов.

Проблемы обеспечения интернет-ресурсов включают:

1. Ограниченный доступ:

Одной из основных проблем является ограниченный доступ к интернет-ресурсам в различных частях мира. Это цифровое неравенство создает барьеры для образования, информационного обмена и развития определенных обществ.

2. Безопасность данных:

С ростом использования интернета возрастают и угрозы безопасности данных. Кибератаки, взломы и утечки информации становятся серьезной проблемой, подчеркивая необходимость более эффективных мер по защите личных данных пользователей.

3. Цифровое неравенство:

Не все люди имеют равный доступ к современным технологиям. Это создает глубокие социальные и экономические разрывы, затрудняя равное участие в цифровой эпохе для всех слоев общества.

4. Кибербезопасность:

Защита от киберугроз становится все более сложной задачей. Злоумышленники используют новые методы атак, что требует постоянного совершенствования технологий безопасности для предотвращения потенциальных угроз.

Проблемы обеспечения доступа к образовательным ресурсам включают:

1. Цифровое неравенство:

Отсутствие доступа к стабильному интернет-соединению и современным технологиям создает неравенство в доступе к образовательным онлайн-ресурсам, ограничивая обучение для тех, кто находится в удаленных или экономически слабых областях.

2. Недоступность оборудования:

Не все студенты могут позволить себе необходимое оборудование, такое как ноутбуки или планшеты, что ограничивает их способность участвовать в онлайн-образовании.

3. Отсутствие обучения в использовании технологий:

Некоторые студенты и педагоги могут испытывать трудности в использовании технологий и образовательных платформ, что ограничивает их эффективное использование.

4. Низкое качество интернет-соединения:

В ряде мест низкоскоростной или нестабильная сеть может привести к проблемам при доступе к онлайн-ресурсам и затруднить обучение.

5. Недостаточное финансирование образования:

Некоторые образовательные учреждения сталкиваются с ограниченным бюджетом, что может сказаться на возможности предоставления современных образовательных ресурсов.

Решение этих проблем требует совместных усилий образовательных учреждений, государственных органов и общества в целом.

Пример: Цифровое неравенство в образовании

Ситуация:

В отдаленных районах определенной страны отсутствует доступ к стабильному интернету из-за отсутствия инфраструктуры. Ученики в этих районах сталкиваются с трудностями в получении онлайн-образования из-за недоступности интернет-ресурсов.

Проблема:

Цифровое неравенство в образовании приводит к тому, что ученики в удаленных местах оказываются в несправедливом положении, так как им не предоставляется равный доступ к образовательным ресурсам в сравнении с учащимися в городах.

Возможные решения:

1. Внедрение сетевой инфраструктуры в удаленных районах для обеспечения стабильного интернет-соединения.

2. Предоставление образовательных ресурсов в офлайн-режиме, таких как электронные учебники, которые можно скачивать и использовать без постоянного интернет-соединения.

3. Инвестиции в программы субсидирования для семей в этих районах, чтобы они могли позволить себе доступ к интернету и образовательным ресурсам.

Этот пример подчеркивает, как проблемы обеспечения интернет-ресурсов, такие как цифровое неравенство, могут оказывать существенное воздействие на различные сферы жизни, в данном случае на образование.

Пути решения проблем обеспечения доступа к интернет ресурсам, к образовательным ресурсам:

1. Инфраструктурные улучшения:

Инвестиции в развитие сетевой инфраструктуры, особенно в удаленных и экономически слабых районах, помогут обеспечить стабильный доступ к интернет-ресурсам.

2. Субсидии и программы поддержки:

Государственные и некоммерческие организации могут предоставлять субсидии для семей с низким доходом, чтобы те могли приобрести необходимое оборудование для онлайн-обучения.

3. Бесплатные образовательные ресурсы:

Развитие и распространение бесплатных образовательных ресурсов помогут снизить финансовые барьеры и обеспечить доступ к материалам для всех.

4. Обучение в использовании технологий:

Реализация обучающих программ по использованию технологий для студентов и преподавателей повысит эффективность онлайн-обучения.

5. Партнерства с технологическими компаниями:

Сотрудничество образовательных учреждений с технологическими компаниями может привести к предоставлению скидок на оборудование и программное обеспечение.

6. Развитие гибридных методов обучения:

Создание гибридных программ, которые сочетают в себе онлайн и офлайн методы обучения, учтет различные потребности и возможности студентов.

7. Поддержка образовательных учреждений:

Обеспечение финансовой поддержки образовательным учреждениям для обновления технической базы и предоставления современных образовательных ресурсов.

8. Регулирование и стандартизация:

Разработка и соблюдение стандартов доступности к интернет-ресурсам и образовательным технологиям для всех обучающихся.

Заключение: Обеспечение интернет-ресурсов - важная задача, требующая совместных усилий со стороны государств, компаний и общества в целом. Решение этих проблем содействует более справедливому и безопасному цифровому будущему для всех. И это урегулируется законом.

Список использованных источников:

1. Уголовный кодекс Республики Казахстан.
Официальный сайт https://studbooks.net/2215697/informatika/obespechenie_raboty_sayta?ysclid=lq229trf3x555321726
2. Официальный сайт "Habr.com": <https://habr.com/ru/companies/skillbox/articles/700826/>
3. Официальный сайт "Cuberlininka.ru": <https://cyberleninka.ru/article/n/aktualnye-problemy-obespecheniya-bezopasnogo-dostupa-k-seti-internet?ysclid=lq22cqdf6w316453642>
4. Официальный сайт "Osp.ru": <https://www.osp.ru/os/2021/01/13055831?ysclid=lq22ea8ocl177502430>

УДК 346.546

Бер Виолетта Викторовна

Студентка 3 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

**НЕДОПУЩЕНИЕ МОНОПОЛИЗМА ГОСУДАРСТВОМ
ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ В СТРАНАХ СНГ****Аннотация**

В статье рассматриваются проблемы монополизации государством информационных источников. Рассмотрены понятие информационные источники. Автором предлагаются пути преодоления этих проблем.

Ключевые слова: монополизация, информационные источники, интернет, информация, рынок связи и телекоммуникаций.

Бер Виолетта Викторовна

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 3 курс студенті,
Қазақстан Республикасы, Алматы қ.

**ТМД ЕЛДЕРІНДЕ АҚПАРАТ КӨЗДЕРІНІҢ МЕМЛЕКЕТТІК
МОНОПОЛИЯЛАНУЫНА ЖОЛ БЕРМЕУ****Аңдатпа**

Мақалада ақпарат көздерін мемлекеттік монополиялау проблемалары қарастырылған. Ақпарат көздері түсінігі қарастырылады. Автор бұл қиындықтарды жеңу жолдарын ұсынады.

Түйінді сөздер: монополиялау, ақпарат көздері, интернет, ақпарат, байланыс және телекоммуникация нарығы.

Ber Violetta Viktorovna

3 year student of High School of Law "Adilet"
Caspian Public University
Republic of Kazakhstan, Almaty

**PREVENTING STATE MONOPOLIZATION OF INFORMATION
SOURCES IN THE CIS COUNTRIES**

Annotation

The article discusses the problems of state monopolization of information sources. The concept of information sources is considered. The author suggests ways to overcome these problems.

Key words: monopolization, information sources, Internet, information, communications and telecommunications market.

Информационные источники в первую очередь - это средства, с помощью которых можно получить определенные знания в той или иной сфере. Они могут быть представлены как на материальном носителе, так и нематериальным образом, что осложняет вопросы регулирования. Безусловно, информация является объектом гражданского оборота Республики Казахстан и регулируется в соответствии с ее законодательством. Помимо ГК РК, нормы определяющие положение информации в современном мире отражены в специальном законе "О доступе к информации" от 16 ноября 2015 года № 401-V, положения которого превалируют над иными нормами законодательства РК.

В XXI веке основным источником информации является Интернет, при помощи которого и происходит частичное производство, обмен и иные действия гражданского оборота, совершаемые лицами любого государства. Интернет стал отдельной платформой, где каждый человек может выразить свое мнение, получить ответ на поставленный вопрос, однако в последнее время в виртуальной сфере происходят ограничения, которые могут привести к полному монополизму. Одним из показательных примеров является СМИ, одна из "ветвей власти", при помощи которой осуществляется воздействие на население, на формирование традиционных устоев. Государство реализует государственную информационную политику через региональные средства массовой информации, соответственно деятельность осуществляемая СМИ, проводится в интересах государства. Однако, согласно п. 1 ст. 2 Закона Республики Казахстан от 23 июля 1999 года № 451-І «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 01.05.2023 г.) 1. Свобода слова, творчества, выражения в печатной и иной форме своих взглядов и убеждений, получения и распространения информации любым не запрещенным законом способом гарантируются Конституцией Республики Казахстан. [1] Однако, распоряжение информационным ресурсом, несмотря на предоставленные гарантии осуществляется исключительно государством. Интересным вопросом является наделение

правом, которое по итогу является ограниченным самим лицом, которое предоставило это право.

На данный момент основным ресурсом всего человечества является Интернет, где каждый из нас обладает той, самой свободой слова, однако стоит сказать и о том, что некоторые лица пренебрегают этим правом, по причине чего, возможно введение ограничения свободы либо же наложение ответственности за то или иное деяние. Безусловно, мы являемся сторонниками данной концепции, когда лицо отвечает за то, что им было совершено в пределах виртуального поля, ведь определенный период времени в Интернете были лица, злоупотреблявшие правом “свободы”, при этом нарушая права третьих лиц. Здесь стоит упомянуть постулат общей теории права: «Права одного человека заканчиваются там, где начинаются права других людей», то есть при выражении своего мнения, комментирования определенного предмета или события мы должны учитывать является ли данный комментарий нарушением права третьих лиц, затрагивают ли они какие-либо персональные характеристики человека (национальность, расу, религию и так далее), соответственно, я за то, чтобы в данном поле также соблюдались нормы законодательства Республики Казахстан, несмотря на то, что в большинстве своем, даже учитывая специфику “поля”, действие общего законодательства сохраняется. Здесь стоит соблюсти грань между введением в данную сферу регулирования законодательством и сохранение той самой “свободы слова”. Однако, критически неверным является решение полной монополизации государством виртуальной сферы. Ведь если право распоряжения будет передано полностью государству, соответственно, государство будет вести тотальный контроль в этой сфере. На данный момент в ряде стран СНГ государство направило политику на поддержание монопольного контроля рынка связи и телекоммуникаций. Например, в Казахстане, Беларуси и России доля государственных активов в уставных фондах ключевых предприятий связи и провайдеров – достаточно велика. Это позволяет говорить, в том числе, о возможном государственном контроле интернет-доступа. [2]

Отдельного внимания заслуживает ситуация произошедшая в РФ. На территории Федерации была фактически осуществлена монополизация интернета, были запрещены комментарии определенного рода, пресечен доступ к определенным сайтам, ограничена деятельность пользователей интернета.

Ограничения влияют на:

I. Общественность;

2. Экономическое состояние страны, интернет - этосредство при помощи которого в наше время осуществляется активный товарооборот, предпринимательская деятельность;

3. Учебную деятельность.

Таким образом, при изучении данной темы, нами проведен заключительный анализ, который определяет монополизм информационной системы исключительно отрицательным аспектом, любой страны. Безусловно, при помощи монополизации государство усилит политическую власть, однако произойдет полное искоренение свободы населения, опять-таки появление тотального контроля. В связи с этим призываем на государственном уровне стимулировать создание независимых медийных и интернет-площадок, на которых «талантливая молодежь могла бы делиться своими идеями, искать новые смыслы, запускать новые проекты». [3] Либо при монополизации информационных средств создание специального демократического органа, избираемым населением.

Список использованных источников:

1. Информационно-правовая система «Әділет»: Закон Республики Казахстан от 23 июля 1999 года № 451-І «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 01.05.2023) // Электронный ресурс: https://adilet.zan.kz/rus/docs/Z990000451_

2. Digital. Report “Государственная монополия в стране может ли перерасти в государственный контроль” // Электронный ресурс: <https://digital.report/gosudarstvennaya-monopoliya-na-internet-v-sng-mozhet-pererasti-v-gosudarstvennyy-kontrol-2/>

3. С.И.Цыхмистро “Влияние информационных монополий на развитие государства” // Электронный ресурс: <https://cyberleninka.ru/article/n/vliyanie-informatsionnyh-monopoliy-na-razvitie-gosudarstva/viewer>

УДК 343.13

Березницкий Константин Константинович

Студент 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И БЕЗОПАСНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация

В статье рассмотрены проблемы в сфере защиты персональных данных и информационной безопасности. Изучено понятие «персональные данные», обращено внимание на противоправные действия в данной сфере. Изучены общие требования к информационной безопасности и мерам наказания за нарушение конфиденциальности. Также рассмотрены проблемы применения таких видов юридической ответственности, как административная, так и уголовная ответственность, а также проблемы сферы информационной безопасности

Ключевые слова: уголовная ответственность, административная ответственность, персональные данные, информационная безопасность, коммуникация, органы исполнительной власти, конфиденциальность.

Березницкий Константин Константинович

«Әділет» Жоғары құқық мектебінің

1 курс студенті Каспий қоғамдық университеті

Қазақстан Республикасы, Алматы қ.

КИБЕРҚЫЛМЫС ЖӘНЕ ЖЕКЕ ДЕРЕКТЕРДІ ҚАУІПСІЗ САҚТАУ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада жеке деректерді қорғау және ақпараттық қауіпсіздік саласындағы проблемалар талқыланады. «Жеке деректер» түсінігі зерттеліп, осы саладағы заңсыз әрекеттерге назар аударылады. Ақпараттық қауіпсіздікке қойылатын жалпы талаптар және құпиялылықты бұзғаны үшін айыппұлдар зерделенді. Сондай-ақ әкімшілік және қылмыстық жауапкершіліктің мұндай түрлерін қолдану мәселелері, сондай-ақ ақпараттық қауіпсіздік саласындағы проблемалар қарастырылады.

Түйінді сөздер: қылмыстық жауапкершілік, әкімшілік жауапкершілік, дербес деректер, ақпараттық қауіпсіздік, байланыс, атқарушы билік, құпиялылық.

Bereznitsky Konstantin
1 year student
Higher School of Law “Adilet”
Caspian Public University
Republic of Kazakhstan, Almaty

PROBLEMS OF CYBERCRIME AND SECURE STORAGE OF PERSONAL DATA

Annotation

The article discusses problems in the field of personal data protection and information security. The concept of “personal data” is studied and attention is drawn to illegal actions in this area. The general requirements for information security and penalties for violation of confidentiality have been studied. The problems of applying such types of legal liability, both administrative and criminal liability, as well as problems in the field of information security are also considered.

Key words: criminal liability, administrative liability, personal data, information security, communication, executive authorities, confidentiality.

Необходимость структурного и грамотного регулирования общественных отношений в сфере защиты персональных данных и информационной безопасности становится все более явной по мере цифровизации Казахстана и увеличения объемов хранения критически важных данных в интернете. Данная сфера стала причиной появления большого количества коллизионных законов. Более того, правотворчество должно сопровождаться обеспечением международных стандартов информационной безопасности, что, в свою очередь, сильно усложняет процесс регуляции. В законе «О персональных данных и их защите» понятие «персональные данные» дается следующее определение:

«Персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.»

За противоправные действия в данной сфере предусмотрена как административная, так и уголовная ответственность. Административная ответственность возникает вследствие незаконного сбора и обработки персональных данных или неосуществления мер по защите информационных систем (Статья 79. Нарушение законодательства Республики Казахстан о персональных данных и их защите). Уголовная ответствен-

ность возникает, «если это деяние причинило существенный вред правам и законным интересам лиц»(Статья 147. Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите)

Особое значение для международных компаний, осуществляющих сбор персональных данных на территории Казахстана, стали изменения от 2016 года в закон о персональных данных, которые привнесли серьезные изменения, а именно: требование о локализации баз, содержащих персональные данные на территории Республики. Данные изменения требуют от представителей рынка не только приведения своей деятельности в соответствие с законодательством Республики Казахстан, но и изменения процессов трансграничной передачи персональных данных и инвестирования колоссальных активов в систему баз данных и в обеспечение их безопасности. Безусловно, не все представители рынка согласны на такие кардинальные изменения, так как существует несколько критически важных вопросов, до сих пор остающихся без ответа.

Закон о персональных данных говорит о том, что базы данных должны располагаться на территории Республики Казахстан. Более того, размещение физических носителей подразумевает обеспечение целостности, конфиденциальности и доступности персональных данных. Однако, не ясным остается то, каким образом осуществляется регулирование отношений с субъектами которые осуществляли свою деятельность до 1 января 2016 года, так как в соответствии с законодательством Республики Казахстан – Закон обратной силы не имеет, в случаях если закон устанавливает новые обязанности, усиливает ответственность, или иным образом ухудшает положение лица. Наравне с этим существует трактовка, в соответствии с которой хранение персональных данных воспринимается как процесс, а не действие, вследствие чего, должна возникнуть обязанность по внесению в базы данных пользователей, которые были собраны и обработаны до 2016 года. Более того, хранение персональных данных за границей Республики Казахстан является незаконным, так как требования указывает на то, что на территории Республик должны храниться хотя бы копии баз данных. Однако, на этой почве возникает вопрос, что может подразумевать слово «копия» - (скриншот, таблицу Excel, нотариально заверенный блок данных, или Шкаф в офисе с распечатанными списками) и, самое главное, кто будет сверять «копии» с «оригиналом», ведь осуществить данную операцию физически невозможно. Ввиду того, что трактовки Министерства внутренних дел и иных ведомств не совпадают, вопрос остается открытым.

Хотя на конференции Digital Bridge Касым-Жомарт Токаев рассказал о планах по строительству специальных баз данных на территории Казахстана в течение двух лет, все равно их постройка не будет гарантировать соблюдение требований со стороны представителей бизнеса, так как постройка подобной инфраструктуры затребует вложения существенной части государственного бюджета, что вряд ли будет одобрено в правительстве.

Остается неясным, насколько рациональным является данное требование, так как в случае, если, например, компания «Google» или «Microsoft» откажутся выполнять предъявленные требования, то их блокировка, буквально остановит большое количество критически важных процессов. Более того, их деятельность на территории Казахстана в данный момент является незаконной, так как нарушает действующее законодательство. Вследствие вышеперечисленного, можно сказать, что данные требования являются нерациональными или требуют значительной доработки.

В качестве яркого примера попытки влияния на крупных представителей бизнеса в Казахстане можно рассматривать недавнюю блокировку крупнейшего «игрока» казахстанского IT рынка «Яндекса». Руслан Абдикаликов, председатель комитета по информационной безопасности министерства цифрового развития, инноваций и аэрокосмической промышленности Казахстана, отмечает, что блокировка была вынужденной мерой, так как «Яндекс» не выполнил требования о локализации данных, принадлежащих казахстанцам, на серверах, расположенных в пределах Республики. Хотя блокировка была вынужденной мерой, остается вопрос, почему мы не видим подобного давления на таких IT гигантов как «Google», «Amazon», «Microsoft», etc., ведь, по открытым данным, они также хранят свои базы в США, Франкфурте, Канаде.

Отсюда же возникает большой вопрос об общих требованиях к информационной безопасности и мерах наказания за нарушение конфиденциальности. В Казахстане мера административного наказания достигает только одной тысячи месячных показателей, как мера высшего наказания для субъектов крупного предпринимательства и сроком до семи лет как мера высшего наказания в случаях, предусмотренных уголовным кодексом. С другой стороны, если мы рассмотрим Европейский опыт, в частности общий регламент GeneralDataProtectionRegulation, который регулирует отношения между гражданами ЕС и теми, кто собирает, обрабатывает и использует эти данные, то мы увидим гибкий и многоуровневый подход к мерам наказания. Так, например, компания

может быть оштрафована на 2% от годового оборота за утечку персональных данных. Причем, этот штраф взимается не от представителя данной компании в определенной стране, где произошла утечка, а от годовой прибыли всего холдинга. Более того, данное соглашения является обязательным для любой компании, которая взаимодействует с персональными данными граждан Евросоюза. На примере европейского опыта мы также можем увидеть грамотную работу федерального органа по информационной безопасности (Federal Office for Information Security), который принимает сообщения об утечках, обеспечивает соблюдения требований к защите, передаче и обработке персональных данных. Таким образом, мы видим, что права людей в сфере конфиденциальности персональных данных осуществляются централизованным государственным органом, с хорошо налаженной коммуникацией.

Достаточно эффективные изменения были внесены в Закон в 2020 году с привнесением в него регулятора, сервисов контроля доступа к персональным данным, информирования граждан об утечке их персональных данных. Планируется введение таких понятий как утечка персональных данных и наделение регулятора функциями государственного контроля. Однако, здесь существует проблема слишком большого количества регуляторов, то есть уполномоченных органов.

В Казахстане, одной из проблем сферы информационной безопасности является отсутствие межведомственной коммуникации между большим количеством органов исполнительной и законодательной власти. Существуют следующие органы, осуществляющие регулирование: Агентство Республики Казахстан по регулированию и развитию финансового рынка (АРРФР), Комитет по информационной безопасности (КИБ), Национальный банк Казахстана (НБК), Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана (МЦРИАП РК) и орган по защите персональных данных, который входит в КИБ при МЦРИАП РК, Комитет национальной безопасности (КНБ) и Государственная техническая служба (ГТС), Министерство внутренних дел в лице Киберпола.

- Агентство по регулированию и развитию финансового рынка: это агентство может регулировать сферу обработки персональных данных в финансовом секторе. Оно устанавливает правила, стандарты и нормы обработки данных для финансовых учреждений, таких как банки, страховые компании и другие финансовые организации.

- Национальный Банк Республики Казахстан: НБРК регулирует банковскую систему и может устанавливать стандарты безопасности и пра-

вила обработки данных для финансовых учреждений, чтобы обеспечить защиту персональных данных клиентов в банковской сфере.

- Министерство цифровизации и аэрокосмической промышленности: это ведомство отвечает за развитие цифровых технологий и может устанавливать стандарты и правила обработки персональных данных в общем контексте цифровизации, например, в цифровых государственных системах и аэрокосмической отрасли.

- Комитет национальной безопасности: КНБ занимается обеспечением национальной безопасности и может иметь полномочия по контролю за обработкой персональных данных в целях предотвращения киберугроз и защиты государственной информации.

- Государственная техническая служба: ГТС занимается технической поддержкой государственных информационных систем и может разрабатывать технические стандарты и требования к обработке персональных данных в этих системах.

Вследствие того, что в Казахстане нет единого государственного органа, который регулировал бы соблюдение действующего законодательства в сфере информационной безопасности, достаточно большое количество различных ведомств, в пределах своих компетенций разрабатывают нормативно правовые акты, рассматривают обращения об утечках, запрашивают отчеты об утечках персональных данных, привлекают к ответственности за несоблюдение требований, etc.. Однако, достаточно часто могут появиться противоречия в процессе работы ведомств, так как существуют случаи возникновения коллизии между нормативно правовыми актами данных ведомств. Например, в соответствии с Законом от 2013 года « О персональных данных и их защите», физические лица имеют право на отзыв и уничтожение персональных данных, однако, в соответствии с законом «Об установлении перечня документов, подлежащих хранению, сроках их хранения в банках второго уровня» некоторые данные должны храниться до 75 лет, что коррелирует с правом физического лица на забвение. В добавок, такое большое количество ведомств, зачастую не может работать сообща, так как центры их управления децентрализованы в сфере информационной безопасности.

Хотя, безусловно, институт защиты персональных данных в Казахстане активно развивается и улучшается, я хочу отметить, что остается большое количество неурегулированных вопросов. К ним, по мимо вышеперечисленных можно добавить отсутствие в законодательстве мер об оперативном реагировании в случае утечки данных, отсутствие

требований об оповещение конкретного уполномоченного органа об утечке. Более того, не зарегулированными остаются права на удаление данных и право на получение информации о нарушении конфиденциальности персональных данных физических лиц. Я вижу большие возможности во внедрении или глубокой аналитике европейского правового механизма по оценке рисков «DataProtectionImpactAssessment» и регламента по защите персональных данных «GeneralDataProtectionRegulation», так как это позволит повысить уровень защиты прав граждан республики Казахстан. По моему мнению, по мере переноса критически важной информации в электронный формат, мы должны все больше заботиться о безопасности этих данных, а осуществить это возможно, только проанализировав многолетний международный опыт, и на его фундаменте обеспечить высококлассную защиту прав и свобод граждан.

Список использованных источников:

1. Закон «О персональных данных и их защите» https://online.zakon.kz/Document/?doc_id=31396226/ Дата посещения: 03.12.2022
2. Кодекс об административных правонарушениях. Статья 79. Нарушение законодательства Республики Казахстан о персональных данных и их защите https://online.zakon.kz/Document/?doc_id=31577399&pos=1863;-44#pos=1863;-44/ Дата посещения: 03.12.2022
3. Кодекс об административных правонарушениях. Статья 641. Нарушение законодательства Республики Казахстан об информатизации https://online.zakon.kz/Document/?doc_id=31577399&pos=9831;-54#pos=9831;-54/ Дата посещения: 06.12.2022
4. Уголовный кодекс РК. Статья 147. Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите https://online.zakon.kz/Document/?doc_id=31575252&pos=2430;34#pos=2430;34/ Дата посещения: 06.12.2022
5. Закон «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» <https://adilet.zan.kz/rus/docs/P1600000832/> Дата посещения: 06.12.2022
6. Капитал центр деловой информации «В Казахстане построят дата-центры, специализирующиеся на ИИ» / <https://kapital.kz/tehnology/119833/v-kazakhstane-postroyat-data-tsentry-spetsializiruyushchiyesya-na-ii.html/> Дата посещения: 07.12.2022

7. Ничего личного: за утечку персональных данных надо наказывать оборотными штрафами /Информационный портал Zakon.KZ <https://www.zakon.kz/pravo/6393206-nichego-lichnogo-za-utechku-personalnykh-dannykh-nado-nakazyvat-oborotnymi-shtrafami.html/> Дата посещения: 07.12.2022

УДК 349.2

Джумалиев Жан Кажымович

Студент 2 курса Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА РЫНОК ТРУДА: АВТОМАТИЗАЦИЯ И СОКРАЩЕНИЕ РАБОЧИХ МЕСТ

Аннотация:

В статье проводится анализ и обсуждение влияния цифровизации на рынок труда в Республике Казахстан. Автором обращено внимание на появление новых профессий, выявлены основные трудности реализации, а также рассмотрены возможные решения и перспективы цифровизации рынка труда в РК. Осуществлено также рассмотрение аспектов совершенствования законодательства для адаптации к новым вызовам цифровой эры.

Ключевые слова: цифровизация, удаленная работа, трудовое законодательство, информационные технологии

Джумалиев Жан Кажымович

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 2 курс студенті,

Қазақстан Республикасы, Алматы қ.

**ЦИФРАНДИРУДЫҢ ЕҢБЕК НАРЫҒЫНА ӘСЕРІ:
АВТОМАТТАНДЫРУ ЖӘНЕ ЖҰМЫС ОРНЫН ҚЫСҚАРТУ**

Аңдатпа:

Мақалада цифрландырудың Қазақстан Республикасындағы еңбек нарығына әсері талданады және талқыланады. Автор жаңа кәсіптердің пайда болуына назар аударып, енгізудегі негізгі қиындықтарды анықтады, сондай-ақ Қазақстан Республикасындағы еңбек нарығын цифрландырудың ықтимал шешімдері мен перспективаларын қарастырылады. Сондай-ақ цифрлық дәуірдің жаңа сын-қатерлеріне бейімделу үшін заңнаманы жетілдіру аспектілері қарастырылды.

Түйінді сөздер: цифрландыру, қашықтан жұмыс істеу, еңбек заңнамасы, Ақпараттық технологиялар

Dzhumaliev Zhan

2 year student

Higher School of Law "Adilet"

Caspian Public University

Republic of Kazakhstan, Almaty

**THE IMPACT OF DIGITALIZATION ON THE LABOR MARKET:
AUTOMATION AND JOB REDUCTIONS**

Annotation:

The article analyzes and discusses the impact of digitalization on the labor market in the Republic of Kazakhstan. The author drew attention to the emergence of new professions, identified the main difficulties in implementation, and also considered possible solutions and prospects for digitalization of the labor market in the Republic of Kazakhstan. Aspects of improving legislation to adapt to the new challenges of the digital era were also considered.

Key words: digitalization, remote work, labor legislation, information technology.

Современный мир переживает неотвратимый процесс цифровой трансформации, оказывающей значительное воздействие на различные сферы общества. В центре этой трансформации находится рынок труда, где цифровизация формирует новые требования, возможности и вызовы для работников и предпринимателей. Процесс цифровизации стремительно преобразует структуру экономики, изменяет характер труда, воздействует на общественные убеждения и переосмысливает социальные стандарты. Этот процесс проникает не только в сферу

производства, но и охватывает повседневную жизнь каждого индивида. Цифровая трансформация затрагивает различные отрасли, меняя бизнес-процессы, исходя из приоритетов компаний, готовых активно внедрять цифровые технологии и инвестировать в развитие как технологических решений, так и человеческого капитала.

Это открывает новые перспективы для образования и профессионального развития в этих областях, а также создает возможности для стартапов и инновационных компаний. Однако цифровая трансформация также вызывает определенные вызовы, такие как угроза потери рабочих мест в традиционных отраслях, где автоматизация может заменить определенные функции человека. Это подчеркивает важность социальной ответственности бизнеса и государственной поддержки в создании переобучения и переквалификации для работников, которые теряют свои места из-за цифровых изменений. В целом, цифровая трансформация оказывает комплексное воздействие на общество, требуя от нас постоянного обучения, готовности к изменениям и нового подхода к работе. Она открывает двери для инноваций, но также требует осмысленного подхода к социальным и экономическим вопросам, чтобы обеспечить справедливое и устойчивое будущее для всех.

По данным Всемирного банка, на цифровую экономику приходится 15,5% мирового ВВП, и она растет в два с половиной раза быстрее, чем мировая экономика за последние 15 лет. Но когда рассматриваются риски цифровизации, в первую очередь вызывает беспокойство степень ее влияния на рынок труда. Важно понимать, что на сегодняшний день Казахстан является государством, идущим по пути не только цифрового, но и общего развития. В то время как многие страны Европы и Азии вынуждены менять устоявшиеся системы, у нашего государства есть уникальная возможность строить все с нуля. Это же касается и цифровизации всех сфер деятельности и сегментов экономики страны.

Однако, необходимо учитывать и то, насколько законодательная система РК способна гибко адаптироваться к современным тенденциям развития, и меняться вместе с ними. Если взглянуть на исторический опыт, то всегда в истории человечества были времена, когда мы развивались, старые профессии умирали, о тем самым открывали дорогу новым. Ведь любое открытие рождает новые возможности для роста занятости, хоть и не все люди готовы это принять и меняться. К примеру, в США в начале XIX века 90% рабочей силы были заняты в сельском хозяйстве, сегодня их доля на рынке не превышает 2%. И такое резкое

сокращение произошло относительно гладко, без особых социальных волнений или эпидемий безработицы.

Говоря о данной проблеме, речь идет конечно же идет об эффективной поддержке граждан со стороны государства, Граждане, сталкивающиеся с препятствиями на рынке труда из-за воздействия цифровизации, должны получить соответствующую поддержку для обеспечения возможности последующего трудоустройства. Процесс цифровизации в сфере занятости способствует повышению доступности и качества услуг для этих граждан. С тем, чтобы предотвратить рост уровня безработицы, также крайне важно создать условия для появления новых рабочих мест, где могли бы трудиться высвобождаемые работники. Если брать в пример развитие страны, такие как США или страны Западной Европы, можно наблюдать интересную тенденцию, что профессии среднего уровня технических навыков, такие как монтажник, сантехник, электрик или плотник не исчезают, а наоборот сталкиваются с проблемой малого количества специалистов, чьи услуги имеют достаточно высокую цену, поэтому профессионалы этой профессии имеют более высокую заработную плату чем в нашей стране. (в США с.з.п - 4189 долларов, в Казахстане - 138000 тг или 300 долларов по статистике Indeed и Trud.kz). Здесь можно обратить внимание на то, что хоть США и находится на 2 месте, а Казахстан на 83 месте в рейтинге Глобального Инновационного Индекса, можно наблюдать, что в Казахстане профессии среднего уровня навыков являются чем-то обыденным, и не столько востребованным как в более развитых технологически странах. Это подводит к выводу о том, что цифровизация на данный момент не может повлиять на исчезновение привычных нам профессий, на которых занята большая часть населения.

В то же время, цифровизация открывает отличную возможность для увеличения сфер занятости граждан Казахстан. В результате внедрения возможности удаленной работы, практики фриланса и платформенной занятости, многие граждане Казахстана столкнулись с новыми возможностями трудоустройства, что особенно важно для тех, кто ранее испытывал трудности на традиционном рынке труда. Цифровизация, хотя и способствует созданию новых рабочих мест, также изменяет профессии, требуя от работников новых навыков для эффективного выполнения новых задач. На примере таких прогрессивных приложений как Kaspi bank и EGOV, мы видим, что развитие информационных технологий становится важной ветвью развития Казахстана, потому что помогает не только создавать новые профессии, но и значительно облегчать работу

уже существующих. Такие процессы как регистрация ТОО, ИП, получение справок стало делом нескольких минут.

Однако, вопреки предоставляемым новым возможностям, появляются вызовы в области социальной защиты и налогообложения для фрилансеров. В Казахстане фрилансеры обязаны уплачивать индивидуальный подоходный налог и обязательные пенсионные взносы, однако их статус не соответствует трудовому договору, что снижает уровень их социальных прав и гарантий. Для решения этого вопроса рассматривается вопрос установления номинальной ставки уплаты налогов и обязательных платежей для фрилансеров на уровне 34%. Эта мера направлена на обеспечение социального обеспечения и адекватного пенсионного накопления.

Важным шагом для Казахстана может стать внедрение простых процедур признания занятости фрилансеров на основе стандартных публичных договоров с онлайн-платформами и введение специального налогового режима, объединяющего налоги и отчисления в систему пенсионного обеспечения, социального и медицинского страхования. Эти изменения могут стимулировать вывод из тени самозанятого населения, предоставляя им социальные гарантии государства.

Есть множество нюансов, которые следует учитывать относительно трудового законодательства, как например особые формы трудовых договоров, для обеспечения защиты прав онлайн работников, выдача специальных виз для “цифровых кочевников” людей работающих внутри страны, на компанию из другого государства. В последние годы государства стараются привлечь цифровых кочевников с помощью специальных виз. Это выгодно для экономики: специалист не отбирает рабочее место у местных, но тратит деньги в этой стране. Поэтому одно из главных ограничений такой визы в том, что она не дает разрешения на работу. Цифровой кочевник должен получать доход за пределами этого государства. Однако есть и такие аспекты, которые необходимо урегулировать в трудовом законодательстве, чтобы защитить права работников в стране, например:

Ввести систему «цифрового лицензионного контроля» для компаний, внедряющих технологии автоматизации. Это предполагает, что компании должны получать цифровую лицензию, демонстрируя планы по обучению и переквалификации своих сотрудников, чтобы смягчить отрицательное воздействие на рабочие места. Могут быть введены трудовые гарантии на то, что работодатель обязан предоставить возможность работнику пройти курсы переквалификации в случае переведе-

ния его должности в цифровизованный формат. Также можно предоставить налоговые льготы компаниям, которые активно инвестируют в обучение и развитие навыков своих сотрудников, а также в разработку и внедрение цифровых технологий.

Цифровизация постепенно начинает оказывать воздействие на рынок труда в Казахстане, открывая новые возможности и в различных сферах. В свете быстрого развития цифровой экономики, страна сталкивается с потребностью адаптировать свое трудовое законодательство, налоговую систему и социальные гарантии для цифровых работников и работников, которые в будущем могут столкнуться с цифровизацией своей профессии. Необходимо внимательно рассматривать изменения в трудовом законодательстве, учитывая специфику цифровой экономики.

Развитие цифровой экономики предоставляет новые возможности для роста занятости, особенно в сфере информационных технологий. Однако, для эффективной адаптации, стране необходимо активно работать над созданием условий для обучения и развития навыков, соответствующих требованиям цифрового рынка. В целом, Казахстан стоит перед важной задачей гибко реагировать на вызовы цифровой эры, и имея большие перспективы занять высокие места в списке развитых технологически стран, обеспечивая поддержку граждан, стимулируя обучение и развитие новых профессиональных навыков, и в то же время поддерживая справедливые и современные нормы в трудовых отношениях.

Список использованных источников:

1. Доклада ВОИС «Глобальный инновационный индекс (ГИИ)» 2022 года// <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-section3-en-gii-2022-results-global-innovation-index-2022-15th-edition.pdf>
2. Научный доклад АО «Центр развития трудовых ресурсов»– «Рынок труда Казахстана: на пути к цифровой реальности». // <https://ias.enbek.kz/ru/node/1451>
3. Организация Объединённых Наций (ООН) - Рейтинг стран по уровню развития электронного правительства. “The United Nations E-Government Survey: E-Government for the People” // <https://nonews.co/directory/lists/countries/e-government>
4. Визы цифрового кочевника в 2023 году: полный список стран и условий - Салават Юсупов, специалист по социально-экономическому и лайфстайл-контенту Банки.ру. // <https://www.banki.ru/news/daytheme/?id=10980271>

5. Инфографики Indeed (крупный зарубежный ресурс вакансий) - Зарплаты сантехников в США. // <https://plattibos.com/zarplaty-santehnikov-v-ssha/>

ӘОЖ342.7

Жабаев Асадбек

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 3 курс студенті,
Қазақстан Республикасы, Алматы қ.

АДАМ ҚҰҚЫҚТАРЫ МЕН БОСТАНДЫҚТАРЫН ҚОРҒАУ

Ғылыми-жетекші:

Калимбекова А.Р

З.ғ.к., Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің
қауымдастырылған профессоры

Аңдатпа:

Мақалада «Адам құқықтары мен бостандықтарын қорғау» түсінігіне талдау жүргізіледі. Автор адам құқықтарын қорғау аясындағы халықаралық актілерін қарастырады және олардың Қазақстан Республикасы заңнамасына имплементациялау процесіне қатысты тәжірибесін қарастырады. Адам құқықтары мен бостандықтары бұзылған жағдайда халықаралық құқық саласы шеңберінде дүние жүзілік қауымдастығының мемлекеттің ішкі жұмысына араласа алуы мүмкіндігіне назар аударылып, адам құқықтарын қорғауға қатысты қалыптасқан механизмді адамзаттың соңғы жылдардағы ең бір үздік әлемдік жетістіктерінің бірі деп қарастырады.

Түйінді сөздер: адам құқықтары, Адам құқықтарының жалпыға бірдей Декларациясы, БҰҰ, этникалық қазақтар, танспарентті демократия, сөз бостандығы.

Жабаев Асадбек

студент 3 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ЗАЩИТА ПРАВ И СВОБОД ЧЕЛОВЕКА

Аннотация:

В статье анализируется понятие «Защита прав и свобод человека». Автор рассматривает международные акты в сфере защиты прав человека и рассматривает опыт их имплементации в законодательство Республики Казахстан. В случае нарушений прав и свобод человека уделяется внимание возможности вмешательства мирового сообщества во внутреннюю работу государства в рамках международного права, а считается одним из них. лучших глобальных достижений человечества за последние годы.

Обращается внимание как на одно из лучших мировых достижений человечества за последние годы, на установленный механизм защиты прав человека, который позволяет мировому сообществу вмешиваться во внутреннюю работу государства в случае нарушения прав и свобод человека в рамках сферы действия международного права.

Ключевые слова: права человека, Всеобщая декларация прав человека, ООН, этнические казахи, прозрачная демократия, свобода слова

Zhabaev Asadbek

3 year student

Higher School of Law “Adilet”

Caspian Public University

Republic of Kazakhstan, Almaty

PROTECTION OF HUMAN RIGHTS AND FREEDOMS

Annotation:

The concept of “Protection of human rights and freedom” is analyzed in the article. The author examines international acts in the field of human rights protection and examines the experience of their implementation in the legislation of the Republic of Kazakhstan. In the case of violations of human rights and freedoms, attention is paid to the possibility of the

international community interfering in the internal work of the state within the framework of international law, and it is considered one of them. the best global achievements of humanity in recent years.

Attention is drawn to one of the best world achievements of humanity in recent years, to the established mechanism for the protection of human rights, which allows the international community to intervene in the internal work of the state in case of violation of human rights and freedoms within the scope of international law.

Key words: human rights, Universal Declaration of Human Rights, UN, ethnic Kazakhs, transparent democracy, freedom of speech.

Бүгінгі күнгі адам құқығын қорғау мәселесі жекелеген мемлекеттердің ісі ғана болып қана қоймай, сондай-ақ ол барлық әлемдік қауымдастыққа мүше елдердің үлкен де өзекті ірі мәселесіне айналып отыр.

Осы тұрғыдан алғанда бұл тақырып төңірегіндегі проблемалар аса өзекті сипатқа ие болып отырғандығы белгілі. Әсіресе осы соңғы оншақты жылдар аралығында адам құқығын қорғау мәселесі халықаралық деңгейде белсенді түрде көтеріліп, тіпті бұл мәселе жеке мемлекеттердің құқық жүйесінің өзінше дербес саласы болып қалыптаса бастағаны белгілі.

Оның үстіне бұл құбылыс бүгінде тұрақты әрі үздіксіз қарқын алуда деп айтуға толық негіз бар. Мәселен, жекелеген мемлекеттердің құқық жүйесінде құқықтың дербес саласы ретінде танылған халықаралық құқықтағы адам құқықтарын қорғау мәселесі ұлттық құқық жүйесінің нормалары алдында халықаралық құқық нормаларына басымдылық беру ресми түрде осы күні кең танылып отыр.

Демек жалпы әлемдік деңгейде адам құқықтарын қорғауға аса жоғары мән берілуде деп айтуға болады әрі бұл бағытта басты бағдар ретінде ұстанатын қағида — ол жалпы адамгершілік құндылықтары екендігі айқын көрніс таба бастады. Оның үстіне қазіргі кезде адам құқықтарын қорғау халықаралық деңгейде ұйымдық тұрғыдан алғанда жоғарғы деңгейде көрініс тапқан деп айтуға болады. Мысалы, адам құқығын қорғау халықаралық деңгейде Біріккен Ұлттар Ұйымы мен Еуропалық Одақ деңгейінде беделді түрде жұмыс жасап жатқаны белгілі. Осы оң құбылыстарға, әрине әсер еткен ең басты ықпал- ол жекелеген мемлекеттердің сыртқы саясаты екені сөзсіз.

Адам құқықтары және мемлекеттердің сыртқы саясаты

Адам құқығы — әрбір жеке тұлғаның қадір-қасиеті мен бостандығын

қорғауды қамтамасыз ететін ережелер. Өз жиынтығында негізгі құқықтар жеке адамның құқықтық мәртебесінің негізін құрайды. Жалпы адам құқықтарын қорғау мәселесі тек қана азаматтық, саяси, экономикалық, әлеуметтік және мәдени құқықтар мен адам бостандығын қалыптастыратын нормалардың жиынтығы ретінде, яғни дербес негізгі бір құқық саласы ретінде ғана танылып қоймай сондай-ақ адам құқықтары мен бостандықтарының дұрыс орындалуын көздейтін аса тиімді құқықтық-ұйымдастыру тетіктері болып қалыптаса бастағаны белгілі.

Халықаралық құқық саласы шегінде дүние жүзі қауымдастығының адам құқықтары мен бостандықтары бұзылған жағдайда мемлекеттің ішкі жұмысына араласа алуы мүмкіндігін соңғы жылдардың ең бір үздік әлемдік жетістіктердің бірі деп қарстыруға болады.

Мәселен, әмбебап сипаттағы көпжақты келісімдер, аймақтық келісімдер, екіжақты келісімдер халықаралық әдет-ғұрыптар адам құқықтары мен бостандықтарын қамтамасыз ету мәселесі бойынша тікелей немесе жанама мамандандырылған халықаралық ұйымдардың шешімдері халықаралық құқықтың негізгі қайнар көздерінің бірі болып табылуда.

Бүгінгі күні халықаралық іс қағаздарда белгіленген адам құқықтары каталогы ұзақ тарихи қалыптасудың эталондары мен стандарттардың нәтижесі болып, қазіргі демократияның нормасы ретінде қалыптаса бастады деуге болады. Барлық кездерде тұлға мен билік арасындағы қарым-қатынастардың реттеу әдістері мыңдаған жылдар бойы назарда болып келгені белгілі. Мәселен, қоғамдық прогресс пен адамзаттың әлемдік қауымдыстығының дамуы және олардың бостандық жолында мемлекеттің тұтас билігін тежеу талпынысы, мемлекеттік органдар мен лауазымды тұлғалардың өктемдік іс-әрекетінен адамдарды сақтау және тұлғаға барынша өз тағдырын өзі шешуге кең түрдік беру айқын көріне бастады.

Әрбір адам туылғанынан бастап белгілі бір мөлшердегі (материалдық және рухани) ажыратылмас құқықтарға ие, ол құқықтарды қамтамасыз ету үшін қоғам мен мемлекет жәрдемдесуі тиіс. Әрқашан да бұл игіліктердің мөлшері материалдық өндіріс жүйесінде тұлғаның қоғамдағы әлеуметтік құрылымында алатын орнымен анықталады. Қоғам дамуының әр сатыларындағы күрт өзгерістер, өркениет өзгешелігі, формальды теңдік қағидасына негізделген адам құқықтарына қазіргідей жан-жақтылық белгісін берген жоқ.

Адамдар құқықтардың кейбір мемлекеттерде шектеулі болатындығына қарамастан, мұндай институт барлық кезде қоғам

мен мемлекеттің өркениеті жолмен тұрақты дамуына толық оң ықпал жасайтындығы сөзсіз. Енді жалпы адам құқықтары мен оны қорғаудың тарихи қалыптасу мен даму кезеңдеріне қатысты бірер мәселелерге тоқталып өтелік. Мәселен сонау ертеректе заңдылыққа ерекше көңіл бөлігені белгілі, мысалы азаматтық және адам құқықтары туралы ұғым, әр азаматтың полюске деген қамқорлығы сол кездің өзінде теория жүзінде пайда бола бастағаны белгі (Платон, Сократ, Аристотель, Перикл және басқалар). Кейіннен қоғамның дамудың келесі кезеңдері адам құқықтары мен заңның үстемділігінің бір-бірімен тығыз байланысты екендігі айқындала бастады.. Бұл ежелгі ойшылдардың мемлекеттік, бостандық және ізгілік бағытындағы қарқынды дамуының басты белгісі бола бастады деуге болады. Тарихи дамудың баспалдағы адам құқықтарына жаңа қасиет бере отырып, ол субъектілердің жаңа топтарына таратылды. Әриен бұл таптардың, сословиелердің өз құқықтары үшін, бостандықтары үшін әрі олардың өздерінің баюы үшін болған күрес екендігі айтпаса да түсінікті.

Адам құқықтары мен бостандықтарын қорғау саласындағы халықаралық ұйымдардың жұмысы.

Адам құқықтары туралы халықаралық билльдің және қазіргі қолданылатын адам құқықтарын қорғайтын көптеген келісімдердің қабылдануы осындай атсалысудың нәтижесі болды.

Бұдан әрі қарай, БҰҰ өзінің өмір сүруі барысында, адам құқықтарының дамуы жөнінде, БҰҰ мүшелерінің міндеттерін көрсетіп, оларды ұлғайтып, жарғының ережелеріне сәйкес адам құқықтарының орындалуын қадағалайтын институттарды құрай алды. Бұл институттар: БҰҰ-ның адам құқықтары жөніндегі комиссиясы, азшылықты қорғап, кемсітушіліктің алдын алу жөніндегі шағын комиссия, әйелдердің әлауқаты және жоғарғы комиссардың адам құқықтарын басқару туралы комиссиясы.

Адам құқықтары жөніндегі комиссия Экономикалық және әлеуметтік кеңестің қамқорлығында жұмыс істейді. Ол мынадай мәселелермен шұғылданады: ЭКОСОС-қа зерттеулер жүргізіп, баяндамалар дайындайды, конвенциялар мен декларациялардың жобасын дайындайды және адам құқықтары жөнінде басқа да жұмыстармен айналысады.

Адам құқықтары жөніндегі комиссия БҰҰ-ның күн тәртібін кеңейтуде үлкен рөл атқарып, адам құқықтарын бұзушылықпен күресуде жаңа халықаралық тәсілдерді қолданды (Нақты жағдайлар және мем-

лекеттер бойынша мандат берілген жұмысшы топтардың және баяндамашылардың торабын ұлғайту). Халықдралық қауымдастықтың күн тәртібіндегі маңызды мәселелердің бірі — адам құқықтарының қорғалуы болуы, сонымен қатар адам құқықтары туралы БҰҰ жарғысы ережесінің қолданылуының кеңейтілуі — бұл комиссияның зор еңбегі.

Азшылықты қорғап, кемсітушіліктің алдын алу жөніндегі шағын комиссия 1946 ж. құрылды. Ол мынадай қызметтерді жүзеге асырумен айналысады:

Адам құқықтары мен нәсілдік, ұлттық, діни және тілдес азшылықты қорғауға байланысты адам құқықтары жөніндегі комиссияға сипаттама беру және зерттеулерге кірісу.

ЭКОСОС немесе адам құқықтары жөніндегі комиссияның кез келген басқа да жұмыстарын атқару.

Шағын комиссияның құрамына 26 сарапшы кіреді. Шағын комиссия жылына бір рет сессия өткізеді. Оның басқа жоғарыда айтылған адам құқықтары туралы БҰҰ институттарынан негізгі айырмашылығы, ол өз үкіметінің атынан жұмыс істемей, комиссия мүшелері өз беттерінше бөлек жұмыс істейді.

Азаматтық және саяси құқықтар туралы Пактіге екінші факультативті хаттама. Ол 1989 ж. 15 желтоқсанда қол қойылу үшін ашылып, 1991 ж. 11 шілдесінде күшіне енді. Хаттаманың талаптарына байланысты оны азаматтық және саяси құқықтар туралы пактіге толықтыру ретінде қарастырады. Ол өлім жазасына арналған. Бұл хаттаманы мойындаған мемлекет юрисдикциясында бірде-бір тұлға өлім жазасына кесілмейді және әр мемлекет өз юрисдикциясында жатқан аумақта өлім жазасын қолданбауға мүмкіндігінше шара қолдануы керек[5].

Адам құқықтары туралы билль, мемлекеттердің адам құқықтары жөніндегі прогресін өлшейтін эталон ретінде мойындалды. Адам құқықтары туралы билльдің ережелері көптеген мемлекеттердің конституциясына, олардың ішінде Қазақстанның конституциясына да енді.

1997 ж. 31 мамырда Азаматтық және саяси құқықтар туралы Пактіні 133 мемлекет, ал Экономикалық, әлеуметтік және мәдени құқықтар туралы Пактіні 136 мемлекет бекітті. Қазақстан Республикасы адам құқықтары туралы басты халықаралық құжаттарын ратификациядан өткізді.

Қазақстанда адам құқықтары мен бостандықтарын қорғайтын жүйе орнатылды. Адам құқықтарының Қазақстанда іске асырылуына Қазақстан Республикасы Президентінің қарамағындағы Адам құқықтарының Комиссиясы көмектеседі. Бұл комиссия мәртебесі жағынан мемлекет басшысының қарамағындағы консультативті

кеңесші орган болып табылады. Комиссия жұмысының үйлестірілуі Қазақстан Республикасының мемлекеттік кеңесшісіне берілген. Комиссия Қдзақстан Республикасы Президентіне, оның адам құқықтары мен бостандықтарын кепілдікпен қамтамасыз етуге байланысты конституциялық міндетін орындауға көмектесуі керек, сонымен қатар ол адам құқықтары мен бостандықтарын қамтамасыз ету және қорғау тетіктерін жандандыруға күш салысуы керек.

Комиссия жұмысына Адам құқықтары мен бостандықтарының сақталуы жөнінде жыл сайын және арнайы баяндама жасау; ұсыныс жасау және адам құқықтарын қорғау тетігін жандандыру; талдау материалдарын дайындау Қазақстан Республикасының мүддесін қорғайтын адам құқықтары туралы құқықтық халықаралық құжаттар бойынша сараптамалық қорытынды жасау; адам құқықтары жөнінде арнайы халықаралық ұйымдардың жұмысына Қатысу кіреді. Комиссия өкілеттік емес құқық қорғаушы ұйымдар мен адам құқықтары жөніндегі кеңестер мен отырыстар жүргізеді. Сонымен қатар, комиссия адам құқықтарының бұзылуы жөнінде Қазақстан Республикасының Президентіне арналған және комиссияның өзіне арналған шағымдар мен өтініштерді қарастырады.

Қазақстанда адам құқықтарын қорғауға арналған үкіметтік емес ұйымдар өз кезінде ұйымдастырылды және белсенді әрекет етті. Солардың ішінде Қазақстандық адам құқықтары жөніндегі халықаралық бюро, Адам құқықтары жөніндегі Алматы-Хельсинки Комитеті «Қазақстанның құқықтық дамуы», Әйелдер құқықтарын қорғау жөніндегі ұйымдар мен Халықаралық тәуелсіз кәсіподақтар конфедерациясы.

Бұл үкіметтік емес ұйымдар адам құқықтарымен айналысатын органдардың жұмысына белсене қатысты. Қазақстанда адам құқықтары мен бостандықтарын жүзеге асыру тетіктерін жандандыруға байланысты ұсыныстар енгізді, республиканың жекелеген азаматтарына нақты көмек көрсеткен еді.

Халықаралық құқықта адам құқықтары — бұл халықаралық бұқаралық құқықтың өз бетінше саласы. Халықаралық құқық халықаралық аренада адам құқықтарын қорғауға маңызды мән береді.

Халықаралық бұқаралық құқықта ресми берілген бар-жоғы он қағида бар. Олардың ішінде адам құқықтары мен бостандықтарын қорғау қағидасы.

Халықаралық құқық — ұлттық құқықтың адам құқықтары аспектілеріндегі нормалардың қалыптасуына әсер етеді. Қазақстан

оны конституциялық және күнделікті заңдарында көрсетті. Осымен Қазақстан өзінің азаматтарын құқықтармен қамтамасыз етіп қана қоймай, халықаралық қауымдастық алдында адам құқықтарын сақтауға міндет алады.

Адам құқықтары туралы халықаралық Билль

БҰҰ жарғысының адам құқықтары туралы ережелеріне толықтыру болып келетін адам құқықтары туралы Билль Адам құқықтарының жалпыға бірдей Декларациясынан, Адам құқықтары туралы екі 1966 ж. Халықаралық пакіден және Азаматтық және саяси құқықтар туралы Пактіге арналған екі факультативті хаттамадан тұрады.

Адам құқықтарының жалпыға бірдей Декларациясы.

Сан-Францискода өткен конференцияда БҰҰ жарғысына «адамдардың негізгі декларациясын» қосу туралы пікірлер айтылған, бірақ олар қабылданған жоқ. Бұл мәселе БҰҰ-ның бірінші жиналысында қайта көтерілген болатын. Осыдан кейін, адам құқықтары туралы қайта құрылған комиссияға Адам құқықтары туралы халықаралық билльді дайындау берілді. Комиссия декларацияны заңды міндеттемелік келісімге қарағанда кепілдемелі түрде қабылдау оңай болатынын түсінді. Сондықтан ол бірінші декларациямен, одан соң бір немесе бірнеше келісімнің жобасымен жұмыс істеу туралы шешім қабылдады. Бұл жұмыстың нәтижесінде Жалпыға бірдей құқықтар декларациясы жасалды. Ол декларацияны БҰҰ Бас Ассамблеясы 1948 ж. 10 желтоқсанда қабылдады. Бас Ассамблея бұл күнді Адам құқықтары күні деп тағайындады.

Декларация бір қағидаттар мен нормалардың басқа қағидаттар мен нормаларға бағынуын айта келіп, адамның әр құқығы бөлек және маңызды игілік болып табынатынын атап көрсетті. Бұл құжатта көрсетілген тұлғаның құқықтары мен бостандықтарын жеке адамның құқықтары мен бостандықтары, азаматтық және саяси құқықтар, әлеуметтік экономикалық, мәдени құқықтар етіп топтастыруға болады.

Декларация бостандық пен теңдік, кемсітушілікке жол бермеу, тұлғаның ар-намысын құрметтеу қағидаттарын бекітуден басталады. Бірінші баптардан бастап: өмір сүру құқығы, бостандық құқығы, жеке адамның дербес құқығы, тұлғаның өмірінің қорғалуын жариялап, адам құқықтарының заңды кепілдігі, әділеттіліктің ресімдік кепілдігі, тұлғаны қинап, аяусыз қарауға тыйым салынады. Жоғарыда айтылған құқықтар дербес құқықтар мен бостандықтардың тобын құрайды.

Тұрғын орынды таңдау және көшіп-қону құқығы, ар бостандығы, ой мен көзқарас бостандығы, мемлекеттік билік органдарына сайлану

және сайлау құқығы, азаматтық құқық Жалпыға бірдей декларацияның 6, 13-21-баптарында азаматтық және саяси бостандықтарын құрайды.

Әлеуметтік-экономикалық құқықтарға Жалпыға бірдей декларация мынадай құқықтарды жатқызады: еңбек құқығы, жұмыссыздықтан қорғалу құқығы, еңбек үшін әділ ақы төлеу құқығы, демалыс алу және демалу құқығы, білім алу құқығы, әлеуметтік қамтамасыз етілу құқығы. Бұл құқықтар декларацияның 22, 28-баптарында көрсетілген. Жалпыға бірдей декларацияны қабылдау халықаралық қатнастардың жаңа бір кезеңі болды. Жалпыға бірдей декларация БҰҰ Бас Ассамблеясының қарары ретінде қабылданды, сондықтан БҰҰ жарғысына сәйкес кепілдемелі түрде жазылған. Бірақ оның ережелеріне баға беруде, халықаралық құқықта келісімдермен бірге заң шығару процесінде, мемлекеттердің халықаралық практикасында дәстүрдің пайда болуы, кейіннен міндетті нормаға айналатынын ескеру керек. Осыған ұқсас, қазіргі кезде Жалпыға бірдей декларацияда көрсетілген құқықтар мен бостандықтар, заңды міндетті немесе келісімді нормалар ретінде қарастырылады.

Келісім бола отыра, пактілер мемлекеттерге заңды міндеттер туғызады. Әр пакт мемлекеттердің өздеріне алған міндеттерін орындау үшін, келісімді сақтау үшін, халықаралық жүйені құрайды.

Қорытынды

Сонымен қорыта келіп төмендегідей тұжырым жасауға болады: бүгін жалпы әлемдік деңгейде адам құқықтарын қорғауға аса жоғары мән берілуде деп айтуға болады әрі бұл бағытта басты бағдар ретінде ұстанатын қағида — ол жалпы адамгершілік құндылықтары екендігі айқын көрініс таба бастады. Сондай-ақ қазіргі кезде адам құқықтарын қорғау халықаралық деңгейде ұйымдық тұрғыдан алғанда ерекше орын алады деп айтуға болады.

Пайдаланылған қайнар көздерінің тізімі:

1. БҰҰ Адам құқықтарының жалпыға бірдей декларациясы 30-бабы
2. Мендикулова Г. М. Исторические судьбы казахской диаспоры
3. Происхождение и развитие. Алматы: Ғылым, 1997
4. БҰҰ Адам құқықтарының жалпыға бірдей декларациясы 13, 14 баптар

УДК 347

Желдыбай Нурдаулет

Студент 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

Научный руководитель:

Мухтарова А.К.

к.ю.н., профессор

Высшей школы права «Әділет»

Каспийского общественного университета

**ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ И КИБЕРВОЙН,
ФИШИНГА, ХАКИНГА, КРАЖИ ПЕРСОНАЛЬНЫХ
ДАННЫХ, ПРОБЛЕМЫ БЕЗОПАСНОГО ХРАНЕНИЯ
ПЕРСОНАЛЬНЫХ ДАННЫХ****Аннотация:**

Данная статья освещает актуальные вопросы киберпреступности и кибервойн, которые стали значительной угрозой в современном цифровом мире. Рассматриваются основные формы киберпреступлений, включая фишинг, хакинг и кражу персональных данных, а также методы их предотвращения. Особое внимание уделяется аспектам кибервойн, включая их влияние на национальную и международную безопасность. В статье анализируются юридические и законодательные рамки, регулирующие киберпреступность и кибервойны, с акцентом на проблемах безопасного хранения персональных данных и приватности в цифровую эру.

Ключевые слова: киберпреступность, кибервойны, фишинг, хакинг, защита персональных данных, цифровая безопасность, международное право, законодательство о кибербезопасности, информационные технологии, приватность данных.

Желдібай Нұрдәулет

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

**КИБЕРҚЫЛМЫС ЖӘНЕ КИБЕРСОҒЫС, ФИШИНГ, БҰЗУ,
ЖЕКЕ БАСЫ ДЕРЕКТЕРІН ҰРЛАУ,
ЖЕКЕ ДЕРЕКТЕРДІ ҚАУІПСІЗ САҚТАУ ПРОБЛЕМАЛАРЫ****Андатпа:**

Бұл мақала қазіргі цифрлық әлемде маңызды қауіпке айналған киберқылмыс пен киберсоғыстың өзекті мәселелерін қамтиды. Фишинг, хакерлік және жеке басы деректерін ұрлауды қоса алғанда, киберқылмыстың негізгі нысандарын, сондай-ақ олардың алдын алу әдістерін талқылайды. Киберсоғыс аспектілеріне, оның ішінде олардың ұлттық және халықаралық қауіпсіздікке ықпалына ерекше назар аударылады. Мақалада цифрлық дәуірде жеке деректерді қауіпсіз сақтау және құпиялылық мәселелеріне баса назар аудара отырып, киберқылмыс пен киберсоғысты реттейтін құқықтық және заңнамалық шеңберлері талданады.

Түйінді сөздер: киберқылмыс, киберсоғыс, фишинг, бұзу, жеке деректерді қорғау, цифрлық қауіпсіздік, халықаралық құқық, кибер қауіпсіздік заңнамасы, ақпараттық технологиялар, деректердің құпиялылығы.

Zheldybai Nurdaulet

1 year student
Higher School of Law "Adilet"
Caspian Public University
Republic of Kazakhstan, Almaty

**PROBLEMS OF CYBERCRIME AND CYBERWARF, PHISHING, HACKING, IDENTITY
THEFT, PROBLEMS OF SECURE STORAGE OF PERSONAL DATA****Annotation:**

This article addresses the pressing issues of cybercrime and cyberwarfare, which have become significant threats in the contemporary digital world. It explores the main forms of cybercrimes, including phishing, hacking, and personal data theft, as well as methods for their prevention. Special attention is given to the aspects of cyberwarfare, including their impact on national

and international security. The article analyzes the legal and legislative frameworks governing cybercrime and cyberwarfare, with a focus on the challenges of secure personal data storage and privacy in the digital age.

Keywords: cybercrime, cyberwarfare, phishing, hacking, personal data protection, digital security, international law, cybersecurity legislation, information technology, data privacy.

Введение .

Киберпреступность можно определить как любые преступные действия, совершенные с использованием компьютеров и сетей интернет. Это включает в себя деятельность, направленную на незаконное проникновение в информационные системы, кражу данных, распространение вирусов, фишинг и другие формы мошенничества. Примеры киберпреступлений включают хакерские атаки на банковские системы для кражи денег или нарушение работы веб-сайтов правительственных учреждений.

Кибервойны представляют собой организованные кампании, проводимые государствами или крупными организациями, целью которых является нанесение ущерба другим государствам или крупным корпорациям через киберпространство. Это включает в себя использование вредоносных программ для разрушения критической инфраструктуры, шпионажа и дестабилизации экономики. Примером кибервойны может служить использование вируса Stuxnet для атаки на ядерные объекты Ирана.

Масштаб и влияние на мировой уровень

Киберпреступность является одной из наиболее быстрорастущих угроз в мире. По данным cyber security ventures, общий ущерб от киберпреступлений оценивается в миллиарды долларов ежегодно, что подчеркивает их экономическое воздействие. Киберпреступления не только приводят к финансовым потерям, но и наносят урон репутации компаний, а также влияют на личную безопасность людей.

Влияние кибервойн. Кибервойны также усиливают глобальную нестабильность. Они позволяют государствам вести конфликты в киберпространстве, что может иметь серьезные последствия для критической инфраструктуры, такой как энергетика, транспорт и здравоохранение.

Глобальный характер угроз. Киберпреступность и кибервойны не знают границ, что делает их угрозой для каждого государства и организации в мире. Их транснациональный характер требует координированных международных усилий для эффективного противодействия и предотвращения.

Влияние на общество. Киберпреступления и кибервойны оказывают значительное влияние на общество в целом. Они не только вызывают экономические потери, но и подрывают доверие к цифровым технологиям, что крайне важно в нашем всё более цифровом мире. Нарушение работы критически важных систем, таких как здравоохранение или транспорт, может иметь серьезные последствия для общественной безопасности и благополучия.

Вызовы для Правительств и Организаций. Правительства и организации сталкиваются с необходимостью разработки и внедрения мер по защите от киберугроз. Это включает в себя создание эффективных механизмов защиты информации, а также развитие правовых и регулятивных рамок для борьбы с киберпреступностью и кибервойнами. Балансирование между обеспечением безопасности и соблюдением прав человека и свободы информации становится ключевым вызовом.

Личная безопасность и приватность. Для индивидуумов вопросы кибербезопасности становятся все более важными, поскольку большая часть их жизни проходит в онлайн-пространстве. Защита персональных данных и конфиденциальности в интернете становится приоритетом, учитывая растущую угрозу киберпреступлений, таких как кража идентификационных данных и финансовая мошенничества.

Глобальная Ответственность. Киберпреступность и кибервойны требуют глобального ответа, поскольку они пересекают национальные границы. Международное сотрудничество и согласованные усилия необходимы для разработки общих стандартов и стратегий противодействия этим угрозам.

Основная цель данного исследования - обеспечить всесторонний обзор современных вызовов в области киберпреступности и кибервойн, выделяя как технические, так и юридические аспекты этих феноменов. Оно направлено на то, чтобы дать понимание сложности этих угроз и подчеркнуть важность разработки эффективных стратегий их противодействия.

Характеристика Киберпреступности.

Определение и Примеры Киберпреступлений

Фишинг: это вид мошенничества, при котором злоумышленники пытаются получить конфиденциальную информацию, такую как логины, пароли и банковские данные, с помощью маскировки под доверенные субъекты в электронных коммуникациях.

Хакинг: Незаконное проникновение в компьютерные системы с целью кражи, изменения или уничтожения данных. Хакеры могут взламыв-

вать системы для кражи конфиденциальной информации, развертывания вредоносного ПО или для других незаконных целей.

Кража персональных данных: включает в себя незаконный доступ к личной информации пользователей, такой как социальные номера, номера кредитных карт, и использование этой информации для мошенничества или продажи.

Инцидент с LastPass в августе 2022 года.

- Компания: LastPass - популярный менеджер паролей, используемый многими людьми и организациями для управления и хранения паролей.

Хронология Событий

1. Первоначальное Вторжение

- Злоумышленник получил доступ к архивным данным LastPass, которые хранились на облачной платформе третьей стороны.

- Доступ был получен через компрометацию учетных данных сотрудника LastPass.

2. Раскрытие Информации:

- В декабре 2022 года LastPass подтвердил, что данные, полученные в ходе первоначальной атаки, использовались для дальнейшего нарушения безопасности.

- Злоумышленники смогли получить доступ к зашифрованным данным, хранящимся в облаке.

3. Потенциальные Угрозы:

- Хотя LastPass утверждает, что безопасность данных клиентов зависит от мастер-пароля, которым они не располагают, существует риск, что злоумышленники могли попытаться взломать зашифрованные данные.

Воздействие и Последствия

- Возможности для Атак: Доступ к данным LastPass предоставлял злоумышленникам потенциал для создания убедительных фишинговых кампаний.

- Реакция LastPass: Компания приняла меры для закрытия уязвимости, но этот инцидент подчеркивает риски хранения конфиденциальных данных на облачных платформах.

Выводы и Уроки

Этот инцидент подчеркивает важность надежных мер безопасности, как на уровне индивидуального пользователя, так и на уровне организаций. Он также иллюстрирует сложности, связанные с защитой данных в облачных сервисах, и необходимость постоянного мониторинга и обновления мер безопасности для противодействия новым угрозам.

Кибервойны: Новая реальность

Определение кибервойны и ее отличие от традиционных войн.

Кибервойна — это конфликт, в котором страны используют киберпространство для ведения военных действий. Отличается от традиционных войн использованием цифровых технологий для атак на информационные системы, вместо физического насилия или традиционного вооружения.

Примеры кибервойн и их последствия.

В Казахстане в сентябре 2022 года произошла серия кибератак, которые вызвали замедление интернет-соединений по всей стране. Президент Казахстана Касым-Жомарт Токаев связал эти атаки с действиями зарубежных сил, стремящихся спровоцировать политические потрясения в стране. Указывается, что атаки, включая DDoS-атаки, были направлены на государственные учреждения и интернет-инфраструктуру. Эти события подчеркивают важность кибербезопасности в контексте усиления цифровизации экономики и государственного управления в Казахстане

Влияние на национальную и международную безопасность

- Кибервойны могут серьезно подорвать национальную безопасность, затрагивая критическую инфраструктуру и экономику.

- На международном уровне повышают риск конфликтов и эскалации напряженности между государствами, а также вызывают обеспокоенность в вопросах кибербезопасности и международного права.

Юридические аспекты киберпреступности и кибервойн

1. Законодательство по киберпреступности и кибервойнам

- В разных странах мира, включая Казахстан, разрабатываются и внедряются законы, направленные на борьбу с киберпреступностью. Например, Уголовный кодекс Казахстана содержит статьи, направленные на борьбу с незаконным доступом к информационным системам (ст. 148 и 205), незаконным перехватом данных (ст. 147, 148 и 223), вмешательством в данные (ст. 206) и системы (ст. 207), злоупотреблением устройствами (ст. 210 и 213), компьютерным подделкам (ст. 369 и 385), компьютерным мошенничеством (ст. 190 и 210) и другими видами киберпреступлений.

2. Международные соглашения и инициативы

- Будапештская конвенция о киберпреступности, принятая Советом Европы, является одним из ключевых международных инструментов, направленных на борьбу с киберпреступностью. Этот документ служит основой для многих национальных законов и способствует международному сотрудничеству в этой области.

- Около 130 государств (67% членов ООН) к январю 2023 года при-
вели свое уголовное законодательство в соответствие с Будапештской
конвенцией, что показывает глобальные усилия по борьбе с киберпре-
ступностью

3. Проблемы с юрисдикцией и правоприменением

- Основная проблема в борьбе с киберпреступностью и кибервой-
нами заключается в сложности определения юрисдикции и ответствен-
ности, поскольку киберпреступления часто пересекают границы и могут
быть совершены из любой точки мира.

- Важность международного сотрудничества и обмена информацией
между правоохранительными органами различных стран является клю-
чевым аспектом в борьбе с киберпреступлениями и кибервойнами.

- Разработка и внедрение международных стандартов и процедур
для расследования и преследования киберпреступников также оста-
ется важной задачей на глобальном уровне.

Эти аспекты подчеркивают необходимость комплексного подхода к
разработке и применению юридических мер в области кибербезопас-
ности на национальном и международном уровнях.

Защита и Профилактика

*Методы защиты от киберпреступлений для организаций и инди-
видуумов.*

- Использование многофакторной аутентификации для защиты учет-
ных записей.

- Регулярное обновление программного обеспечения и систем без-
опасности.

- Внедрение сильной политики паролей и использование менедже-
ров паролей.

- Обеспечение резервного копирования данных и их шифрования.

Программы обучения и осведомленности об угрозах

- Разработка и проведение обучающих программ по кибербезопас-
ности для сотрудников.

- Повышение осведомленности об угрозах фишинга, социальной ин-
женерии и мошенничества.

- Регулярные тренинги по безопасности и симуляции кибератак.

*Роль Правительства и частного сектора в противодействии ки-
беругрозам*

- Разработка и применение законодательства для усиления кибер-
безопасности.

- Сотрудничество между государственными учреждениями и частным сектором для обмена информацией о киберугрозах.
- Поддержка инициатив по улучшению кибербезопасности на национальном и международном уровнях.

Будущее Кибербезопасности

Предстоящие вызовы и тенденции в кибербезопасности

- Рост сложности и частоты кибератак, особенно в связи с развитием ИИ и машинного обучения.

- Усиление угроз со стороны государственных и частных актеров, включая гибридные и целенаправленные атаки.

- Защита от атак на критическую инфраструктуру и кибервойны.

Развитие технологий и их влияние на угрозы безопасности

- Прогресс в области ИИ и машинного обучения усиливает потенциал как для наступательных, так и для оборонительных киберопераций.

- Развитие квантовых технологий представляет как новые возможности для защиты, так и угрозы для существующих систем шифрования.

Потенциальные стратегии и технологии защиты

- Инвестиции в передовые технологии обнаружения и реагирования на киберугрозы.

- Развитие стратегий, основанных на искусственном интеллекте и машинном обучении, для предсказания и предотвращения кибератак.

- Сотрудничество на международном уровне для обмена информацией о киберугрозах и координированного ответа на них.

Заключение

В заключение хотелось бы отметить, что кибербезопасность в современном мире представляет собой сложный и многогранный вызов. Угрозы киберпреступности и кибервойн требуют всестороннего подхода к обеспечению защиты как на уровне индивидуумов, так и на уровне организаций и государств. Продолжающееся развитие технологий, включая ИИ и машинное обучение, усиливает необходимость в адаптации и усовершенствовании стратегий защиты. Сотрудничество между правительственными и частными секторами, а также международное взаимодействие, играет ключевую роль в противодействии киберугрозам. Будущее кибербезопасности требует непрерывного обучения, инноваций и глобальной координации для защиты нашего цифрового мира.

Список использованных источников:

1. <https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>
2. <https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/>
3. <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>
4. <https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/>
5. <https://medium.com/@Bytecodesec/what-is-the-future-of-cyber-security-5d528cf4b39c>
6. <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>
7. <https://www.coe.int/en/web/octopus/-/kazakhstan>

ӘОЖ 347**Жүнісхан Шырын Айдыңқызы**

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,

Қазақстан Республикасы, Алматы қ.

**КИБЕРБУЛЛИНГПЕН КҮРЕСУ ҮШІН БИЛІКТІҢ
ӘЛЕУМЕТТІК ЖЕЛІНІ БАҚЫЛАУДЫ КҮШЕЙТУІ АДАМ
ҚҰҚЫҒЫН ШЕКТЕУ ЕМЕС ПЕ?****Аңдатпа**

Бұл мақалада мектеп оқушылары мен жастар арасында компьютерлер мен ұялы телефондардың енуімен және техникалық құралдардың дамуымен туындаған құдалаудың жаңа түрі ретінде кибербуллинг мәселесі қарастырылады. Кибербуллингке қарсы күрес саласындағы шетелдік және отандық жұмыстар талданған. Автор кибербуллинг пен дәстүрлі қорлаудың айырмашылығын және оның салдарын, сондай-ақ интернеттегі, әлеуметтік желілердегі адам құқықтарын қорғауды, кибербуллингпен күресті реттейтін қазақстандық заңнаманы, сондай-ақ осы саладағы заң шығарушы ұсынған бастамаларды қарастырады.

Түйінді сөздер: «дәстүрлі қудалау», «қорқыту», «тролльдер», «бұзақылар», «мобберлер», «қорқыту», «кибербуллинг», «интернет-троллинг», «электрондық агрессия»;

Жунискан Шырын Айдынкызы

студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

**ЯВЛЯЕТСЯ ЛИ УСИЛЕНИЕ КОНТРОЛЯ ВЛАСТЕЙ НАД СОЦИАЛЬНЫМИ СЕТЯМИ
В ЦЕЛЯХ БОРЬБЫ С КИБЕРБУЛЛИНГОМ НАРУШЕНИЕМ ПРАВ ЧЕЛОВЕКА?**

Аннотация

В данной статье рассматривается проблема кибербуллинга как нового типа преследования, возникшего с развитием технических средств и проникновением компьютеров и мобильных телефонов среди школьников и молодежи. Анализируются зарубежные и отечественные труды в сфере борьбы с кибербуллинг. Автором рассмотрены отличия кибербуллинга от традиционного буллинга и его послествия, а также казахстанское законодательство, регулирующее сферу защиты прав человека в интернете, социальных сетях, борьбы с кибербуллинг, а также предлагаемые законодателем инициативы в этой сфере.

Ключевые слова: традиционное преследование, запугивание, тролль, «булли», «мобберы», буллинг, кибербуллинг, интернет-троллинг, электронная агрессия.

Zhuniskhan Shyryn

1 year student

Higher School of Law “Adilet”

Caspian Public University

Republic of Kazakhstan, Almaty

**IS INCREASING GOVERNMENT CONTROL OVER SOCIAL MEDIA
TO COMBAT CYBERBULLYING
A VIOLATION OF HUMAN RIGHTS?**

Annotation:

This article examines the problem of cyberbullying as a new type of persecution that arose with the development of technical means and the

penetration of computers and mobile phones among schoolchildren and youth. Foreign and domestic works in the field of combating cyberbullying are analyzed. The author examines the differences between cyberbullying and traditional bullying and its consequences, as well as Kazakhstani legislation regulating the protection of human rights on the Internet, social networks, the fight against cyberbullying, as well as initiatives proposed by the legislator in this area.

Key word: traditional harassment, trolls, bullies, mobbers, bullying, cyberbullying, Internet trolling, electronic aggression

Кибербуллинг - бұл агрессивті әрекет, қасақаналық, ғаламтор арқылы орын алатын дәстүрлі қудалаудың жанама түрі. Осы негізге сүйене отырып, кибербуллинг жеке адамдарға, қоғамға және қоршаған ортаға әсер ететін қылмыстың неғұрлым кең таралып жатқан түрі.

Қазіргі кезде кибербуллинг әлемдегі көптеген білім беру ұйымдарында әлеуметтік қудалау мәселесіне айналған. Жаңа коммуникациялық технологияларды әлеуметтік және экономикалық жағдайлармен байланыстырудан басқа, жасөспірімдер мен жастар арасындағы қарым-қатынаста қудалаудың түрлі жолдарының пайда болуына әсер етіп жатқандығын көрсетуде.

Мектеп оқушылары арасындағы қорқыту мен қудалауға қатысты халықаралық зерттеулер негізінен төрт уақыт кезеңін қамтиды [1].

Бүгінгі таңда буллинг мәселесінің өзектілігі артуда. Өйткені, буллинг оқушылардың жеке ерекшеліктеріне, құрдастарымен және ересектермен қарым-қатынасына, сондай-ақ мектеп немесе қоғамдық нормаларға байланысты күрделі факторлардың өзара әрекеттесуінен туындайды. Көптеген себеп-салдарға және сан алуан түрлі факторларға байланысты мектепте оқушылар арасында буллингтің кең таралуының әлемдік тәжірибесі қалыптасқаны белгі.

1970-1980 жылдар аралығында оны жүйелі түрде зерттеу басталды, норвегиялық зерттеуші Ольвеус өзінің «Aggression in School: Bullies and Whipping Boys» кітабында осы мәселені талдауы негіз болды [2].

Кейінірек, 1980 жылдары, алдыңғы зерттеуден кейін «Қорлаудың алдын-алу» сияқты бағдарламалар жасалынды [3].

1990 жылдан бастап 2004 жылдың ортасына дейін қорқыту, қорлау туралы зерттеулер халықаралық деңгейдегі сипатқа ие болды [4], ал 2004 жылдан бастап киберкеңістікті шабуылдар орын алатын жаңа орта ретінде арнайы оны сипаттайтын «киберқастандық», «кибербуллинг» атты терминдердің атауы пайда болды.

Көбінесе «тролльдер», «булли» немесе «мобберлер» деп аталатын бұзақылық әрекеттерді жасайтын адамдар жасырын әрекет етеді. Сондықтан жәбірленуші агрессивті әрекеттердің кімнің тарапынан туындайтынын білмейді.

Мектептерде оқушылардың зорлық пен қатігездікке баруын зерттеу әлдеқашан ерте басталған. Соның бірі К.Дюкстің 1905 жылы жарық көрген еңбегі. Оның жалғасы ретінде бұзақылық мәселесіне қатысты алғашқы жүйелі зерттеулермен Скандинавия елдерінің ғалымдары Д.Ольвеус, Э.Роланд, П.П. Хейнеман, А. Пикас айналысқан. Яғни, скандинавиялық ғалымдар мектептегі қорқыту мәселелерін бірінші болып XX ғасырдың басында зерттей бастаған.

Мектеп жасындағы балалар арасындағы қатыгездік пен құдалаудың көрінісі алуан түрлі: зиянсыз болып көрінетін іс-әрекеттер мен әзілдерден бастап құдалау мен қорқытуға дейін баруы, оның салдары адам өлімі мен суицидке дейін апаруы мүмкін. Мұндай қорқыту, кемсіту, құдалау әрекеттері буллинг деп аталады. Американдық ғалымдар кибербуллингтің үш ерекшелігін анықтап, оларды үш «А» принципі деп атады – (anonymous, accessible, affordable) анонимділік, қолжетімділік, төмен баға. Анонимділік кибербуллингті іске асырушы үшін тиімді, өйткені ол жәбірленушінің нақты реакциясын көрмейді. Қылмыскер өзінің хабарламаларын нақты адам оқитынын ұмытады.

Интернеттің қолжетімділігі іс-жүзінде кең таралған, мобильді құрылғылармен сымсыз желілердің арқасында пайдаланушы тәулігіне 24 сағат, аптасына 7 рет әлеуметтік желілерде байланысу мүмкіндігін алады. Бұл кибербуллингті жүзеге асырушыға еш алаңдамай, тоқтаусыз «жұмысын істеуге» мүмкіндік береді.

Көбінесе жасөспірімдер мен мектеп жасындағы балалар кибербуллингтің құрығына түседі, олар негізінен құрдастарының немесе сыныптастарының интернеттегі зорлық-зомбылығына бой алдырады. Кибербуллингтің себептері негізінен мынандай:

1. Үстемдікке ұмтылу;
2. Субъективті кемшілік сезімі немесе кемшілік кешені
3. Қызғаныш
4. Кек алу
5. Әзілдесу

Кибербуллинг кеңістікте шектелмейді және ол әлеуметтік желілердегі барлық парақтарын жойып, интернетті пайдалануды тоқтатса да адамға кері әсері етуі мүмкін. Бұл агрессорға ол туралы айыптайтын ақпаратты әрі қарай орналастыруға кедергі болмайды. Бұл жағдайда қандай зиян келеді?

• Біріншіден , денсаулыққа зиян. Зерттеулерге сәйкес, ересектерге бағытталған интернеттегі агрессия қорқынышты емес. Бірақ , психиксы әлі күшеймеген балалар мен жасөспірімдерде мұндай шабуылдар қорқыныш , дәрменсіздік , өзін-өзі бағалаудың төмендеуі, өзіне деген сенімсіздік , депрессия тіпті суицид туралы ойларға дейін алып келуі мүмкін.

• Екіншіден, адамның абыройына нұқсан келтіруі мүмкін.

• Үшіншіден, материалдық шығын. Балалар мен жасөспірімдерді әлеуметтік желі арқылы бопсалау.

• Мектептегі физикалық буллинг – бұл соққыларда және басқа дене жарақаттарында көрінуі мүмкін тікелей мақсатты физикалық әсер [4].

Психологиялық мектептегі буллинг – бұл жәбірленушінің психикасына әсер ету мақсатында жаса- латын зорлық-зомбылық, бұл психологиялық жарақаттардың дамуына әкелуі мүмкін. Қорқытудың бұл түрі жәбірленушіге ыңғайсыздық туғызу және сенімсіздік сезімін дамыту мақсатында ауызша қорлау немесе қорқыту, құдалау түрінде көрінеді. Сондай-ақ, осы тақырып аясында психологиялық әсер ету формасына мыналар жатады:

• ауызша буллинг (мысалы: қорлайтын есім-лақап ат, қорлау, қорлайтын қауесеттерді тарату және т. б.);

• – қорлайтын қимылдар немесе әрекеттер (мысалы, жәбірленушіге түкіру немесе оған қыймылы арқылы қорлау әрекетін көрсету);

• – қорқыту (жәбірленушінің мінез-құлқына әсер ету және қорқыныш пен сенімсіздік сезімін тудыру үшін агрессивті дене тілі мен дауыс интонациясын қолдану);

• – оқшаулау (жәбірленушіні оқушылардың бір бөлігі немесе бүкіл сынып болып әдейі оқшаулайды, қуып жібереді немесе елемейді);

• – кибербуллинг-электронды құрылғылар, интернет-ресурстар арқылы қорлау (айыптаушы сипаттағы суреттер мен фотосуреттерді жіберу, ат қою, қауесеттерді тарату және т.б.) [5].

Психологиялық қорқыту - классикалық буллингтің кіші түрлерінің бірі және «кибербуллинг» деп аталады. Кибербуллингті смартфондар, электрондық пошта, веб-беттер, әлеуметтік желілер, блогтар және басқа интернет-ресурстар сияқты бұқаралық ақпарат құралдары мен коммуникация құралдары арқылы болатын қорлау ретінде сипаттауға болады. Басқаша айтқанда, кибербуллинг – бұл өзара әрекеттесудің электронды түрлерін қолдана отырып, белгілі бір уақыт ішінде топ немесе жеке тұлға жүйелі түрде жүзеге асыратын және өзін оңай қорғай алмайтын жәбірленушіге қарсы бағытталған қасақана агрессивті әрекеттер [6].

Кибербуллинг – бұл халықаралық деңгейге жеткен мәселе. 2013 жылғы «АҚШ-тағы буллинг статистикасына» сәйкес, балалар мен жасөспірімдердің шамамен 58%-ы интернетте қорқытылғанын хабарлады, олардың сауалнамаға қатысқандардың жартысынан көбі бұл оқиға туралы ата-аналарына хабарламағанын көрсетті [7].

Кибербуллинг жасөспірімдерге айтарлықтай зиян келтіруі мүмкін және мазасыздықтың, депрессияның және тіпті суицидтік көріністердің дамуына әкелуі мүмкін. Көптеген ұқсас белгілердің болуына қарамастан, кибербуллинг буллингтан біршама ерекшеленеді.

Біріншіден, кибербуллинг – бұл қорқытудың жеке нұсқасы, ал буллинг – бұл басқа адамды агрессивті қудалау, бопсалау және психологиялық қорлаудың жалпы анықтамасы.

Екіншіден, кибербуллинг жағдайында тікелей физикалық байланыс жоқ, өйткені қорқыту онлайн-қызметтер мен ақпараттық технологиялар арқылы жүзеге асырылады.

Үшінші ерекшелігі – анонимділік. Анонимділік агрессорға қауіпсіздік пен жазасыздық сезімін тудырады, осылайша оның қолдарын ашады, бұл қорқыту құрбандары үшін ауыр зардаптардың жоғарылау қаупіне әкелуі мүмкін. Психологиялық қорлау, оның кез-келген көрінісінде, психоәлеуметтік бейімделу проблемаларының дамуының маңызды көрсеткіші болып табылады.

Қауіпсіз орта оқушылар өздерін маңызды сезінетін және құрдастары мен ересектері мойындайтын жағдайда пайда болады. Мұғалімдермен және құрдастарымен жағымды қарым-қатынаста болған, сондай-ақ олардан қолдау алатын балалардың өзін-өзі бағалау деңгейі жоғары болуы және өздері үшін тұруы ықтимал. Құрдастарымен және мұғалімдерімен жағымсыз тәжірибесі бар оқушылар өзін-өзі бағалаудың төмендігінен және әлеуметтік бейімделу проблемаларының болуынан зардап шегуі мүмкін. Буллинг мәселесіне қызығушылықтың артуының себептерінің бірі-оның академиялық үлгеріммен байланысы. Оқушылар уақытының көп бөлігін мектепте өткізетіндіктен, мектептер оқушының әлеуметтік, интеллектуалдық және мінез-құлқы дамуына айтарлықтай әсер ететінін жоққа шығаруға болмайды.

Мектеп климаты мектеп қауіпсіздігінің маңызды бөлігі болып табылады. Достыққа бағытталмаған мектеп атмосферасы баланың оқу қабілетіне теріс әсер етіп қана қоймайды, сонымен қатар мұғалімдердің сыныптағы оқушылардың мінез-құлқын тиімді басқару қабілетіне кедергі келтіреді. Мектептегі жасөспірімдер жауаптарын таразылап байқайтын болсақ, буллинг және кибербуллинг құбылысының алдын

алуда ересектер тарапынан олқылықтар жіберіліп отыратынын көруге болады.

Осы бағытта түсіндіру жұмыстары мен тәрбиелік шаралардың жеткіліксіз жүргізілуі немесе дер кезінде аңғарып, алдын алмау секілді құбылыстарды оқушылар тарапынан байқайтыны сезіледі. Олар ересектерден дұрыс шара көру әрекеттерін күтпегендіктен зорлық-зомбылыққа тап болғандаол туралы ашық айтпайтын секілді. Оқушылардың басым бөлігі ересектер тарапынан осындай құбылысты дер кезінде байқап, агрессор өз жазасын алатын болса мұндай зорлық-зомбылықтың алдын алуға болатынын айтқан. Өйткені, оқушылар жауаптары, ересектерге ұсыныс айтқандай-ақ. Әйтсе де, мұның алдын алуға күмәнмен қарайтындар да болды.

Осы негізде ҚР Президенті Қасым-Жомарт Кемелұлы Тоқаев 3 мамырда Қазақста бала құқықтарын қорғау туралы заңға қол қойды. Бұл заңға сәйкес, билік мессенджерлер мен әлеуметтік желі иелерінен балаларға кибербуллинг деп танылған контентті алып тастауды талап ете алады. Ол кезде сенат кибербуллингті анықтау үшін сарапшылар комиссиясын құру және кибербуллинг деп танылған материалды алып тастау мәселелерін нақтылайтын өзгерістер қосқан. Сенат төрағасы Мәулен Әшімбаев жобадан ақпарат министрлігінің интернет-ресурстарға, әлеуметтік желі мен мессенджерлерге өз бетінше шектеу қойып, жұмысын тоқтатуына мүмкіндік беретін «кең өкілеті» жойылғанын айтқан.[8].

Жаңа заңның қауіптілігі әкімшілік шектеуде, әлеуметтік желіге айыппұл салынууда немесе аккаунттардың жойылуына байланысты емес. Қайта осы арқылы теріс заңдық үгіт -насихат функциясының пайда болуында. Елдің болашағы мен басты ресурсы болып табылатын Қазақстан жастарының психологиясын болжау қиын емес.

Жастар мен студенттер азаматтық қоғамның белсенді өкілдері ретінде ақпаратты тарату, өз пікірін жариялау, интернет мазмұнын құру, хабарлама алмасу, бір-біріне қатты айтылатын әзілдер мен сөздерді тыюды өздерінің құқықтарын шектеумен теңдей көреді.[9] Медиа өкілдері заң жобасын әлі де жетілдіру керек деген пікір айтты. Жаңа өзгерістерге қарсылық білдірген жұрт петицияға қол жинап, митингілер өткізді. Заң жобасын парламент мақұлдағаннан кейін де оның қабылдануына қарсы жұрт күресін жалғастырды.

2023 ж. 23 сәуірде Алматыда әлеуметтік желілерді реттеу туралы заң жобасына қарсы рұқсат етілген митинг өтті. Жиынға отыз шақты адам жиналды. Шараға қатысушылар президентті вето құқығын пайдаланып, заң жобасын кері қайтаруға үндеген. Сондықтан осындай мемлекеттің

шығарған шешіміне байланысты ғалымдардың ойы бір ауыздан «Бұл адам құқығын шектеу мен еркін жүріп-тұру құқығынан айырады. Мемлекетіміз осы Заңды, норманы қабылдай отырып, Ата Заңымыз Конституцияға коллизия тудыруда»-деген пікір қалыптастырып отыр.

Пайдаланылған қайнар көздерінің тізімі:

1. Букалорова Л.А., Остроушко А.В., Муратханова М.Б., Букалоров А.А. Противодействие кибербуллингу несовершеннолетних в Российской Федерации, Республике Казахстан и США. // Л.Н. Гумилев атындағы Еуразия ұлттық университетінің Хабаршысы. – 2018. – No 3(124). – С.39-46.

2. Салпина К.Е. Мектеп оқушыларының психологиялық қауіпсіздігін қамтамасыз етудің ерекшеліктері. //«Педагогикалық білім берудің үздіксіздігі-заманауи педагогтардың табыстылығының кепілі» атты Халықаралық ғылыми-тәжірибелік конференция материалдары. II-Кітап. – Қостанай: А.Байтұрсынов атындағы Қостанай өңірлік университеті. –2022. – 365 б.

3. Байжуманова Б.Ш. Қазіргі кездегі жастар арасындағы буллинг мәселесі // Материалы международной научно-практической онлайн-конференции, посвященной 175-летию Абая Кунанбаева и 1150-летию Абу Насыр аль-Фараби по теме «Современные проблемы гуманитарных и социальных наук». – Алматы, 2020. – С. 45-48.

4. Токсанбаева Н.Б., Мадалиева З.Б., Санай. Г.Е. Жасөспірімдік ортадағы буллингті зерттеу мәселесі // Абай атындағы ҚазҰПУ Хабаршысы журналы. «Психология» сериясы. – 2020. – No 2(63.) – С.159-169.

5. Dr Michael J. Boulton, Mark Trueman, Lindsay Murray Associations between peer victimization, fear of future victimization and disrupted concentration on class work among junior school pupils //British Journal of Educational Psychology. – 2008. – Vol.78. – Is.3. – P. 473-489.

6. Katarina Dutkova, Jana Holubcikova, Michaela Kravcova, Peter Babincak, Peter Tavel&Andrea Madarasova Geckova Is Spiritual Well-Being Among Adolescents Associated with a Lower Level of Bullying Behaviour? The Mediating Effect of Perceived Bullying Behaviour of Peers // Journal of Religion and Health. – 2017. – Vol.56. – P.2212–2221.

7. Аллаярова Н.И. Кибербуллинг в киберпространстве // Научные труды ЮГУ им. М. Ауэзова. – Шымкент. – 2020. – No 4 (56). – С 176-180.

8. <https://adyrna.kz/post/72222>

9. <https://qazaqtimes.com/article/89915>

УДК 349.2

Ибрагим Нармин Исмаилқызы
Студентка 2 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

КАК ПАНДЕМИЯ ПОВЛИЯЛА НА ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО РК

Научный руководитель:

Чингисбаева А.Е.

М.ю.н., сеньор-лектор
Высшей школы права «Әділет»
Каспийского общественного университета

Аннотация:

Данная статья посвящена изучению влияния пандемии на Трудовое законодательство. Автор стремился рассмотреть и выявить актуальные проблемы, в сфере конфликтов между работником и работодателем, связанных с дистанционной работой. В частности, рассмотрены проблемы определения права сторон, являющихся субъектами трудового законодательства, чей статус урегулирован ст. 138 ТК РК. Осуществлен разбор проблемы регулирования вопросов о труде на начальных этапах простоя и проблемы разрешения несчастных случаев во время дистанционной работы.

Ключевые слова: дистанционная работа, работодатель, работник, права сторон, законодательство, акт.

Ибрагим Нармин Исмаилқызы
Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 2 курс студенті,
Қазақстан Республикасы, Алматы қ.

ПАНДЕМИЯ ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ЕҢБЕК ЗАҢНАМАСЫНА ҚАНДАЙ ӘСЕР ТИГІЗДІ

Аңдатпа:

Бұл мақала пандемияның еңбек заңнамасына әсерін зерттеуге арналған. Автор қашықтан жұмыс істеуге байланысты қызметкер мен жұмыс беруші арасындағы қақтығыстар саласындағы өзекті мәселелерді қарастыруға және анықтауға тырысты. Атап айтқанда, мәртебесі баппен реттелетін еңбек заңнамасының субъектілері болып табылатын тараптардың құқықтарын анықтау мәселелері. 138 Қазақстан Республикасының Еңбек кодексі. Жұмыстың тоқтап қалуының бастапқы кезеңдеріндегі еңбек мәселелерін реттеу мәселесі және қашықтан жұмыс істеу кезіндегі жазатайым оқиғаларды шешу мәселелері талданды.

Негізгі сөздер: қашықтан жұмыс, жұмыс беруші, қызметкер, тараптардың құқықтары, заңнама, акт.

Түйінді сөздер: қашықтан жұмыс, жұмыс беруші, жұмыскер, тараптардың құқықтары, заңнама, акт.

Ibrahim Narmin

2 year student

Higher School of Law "Adilet"

Caspian Public University

Republic of Kazakhstan, Almaty

HOW THE PANDEMIC AFFECTED THE LABOR LEGISLATION OF THE REPUBLIC OF KAZAKHSTAN

Annotation:

This article is devoted to studying the impact of the pandemic on Labor legislation. The author sought to consider and identify current problems in the area of conflicts between employee and employer related to remote work. In particular, the problems of determining the rights of parties who are subjects of labor legislation, whose status is regulated by Art. 138 Labor Code of the Republic of Kazakhstan. The problem of regulating labor issues at the initial stages of downtime and the problem of resolving accidents during remote work were analyzed.

Key words: remote work, employer, employee, rights of the parties, legislation, act.

В связи с неожиданным обстоятельством непреодолимой силы – пандемии COVID-19, большое значение приобрела проблема трудового законодательства в области регулирования вопросов о дистанционной работе. Работники и работодатели не были готовы к простоям, а трудовое законодательство не прошло проверку на прочность, однако впоследствии были приняты многие изменения и дополнения для регулирования вопросов работы на «удаленке».

Из-за непопулярности дистанционной работы до пандемии, возник конфликт между двумя сторонами трудовых правоотношений. Если сейчас, спустя несколько лет, для многих дистанционная работа это обыденное явление, то в 2020 году было множество вопросов со стороны работников и работодателей, которые порождали разногласия. Споры были разного характера: от того, кто должен обеспечивать оборудованием для работы, до проблем с интернет-связью.

Можно сказать, что этот тяжелый период мы пережили не зря, так как актуальность вопроса дистанционной работы возникла бы в любом случае из-за научно-технического прогресса, но COVID-19 ускорил этот процесс. Сейчас мы видим Трудовой кодекс уже с учетом законодателем нюансов, возникшие в период массового простоя.

По данным публикации газеты «МК в Казахстане», число сотрудников, работающих удаленно в РК, возросло в 100 раз за 2020 год. Трудовое законодательство было абсолютно не готовым к массовому переводу работников на дистанционный режим. Так, к примеру, работодатели затруднились на счет порядка перевода своих работников на режим «онлайн». Работодатели для уведомления о переходе на дистанционную работу использовали самые различные способы – приказы руководителей, устное объявление с обращением к работникам, электронные рассылки писем, а в некоторых случаях, работодатели использовали способ заключения дополнительного соглашения о переходе на дистанционный режим работы.

После данного случая, в статью 138, регулирующую вопросы дистанционной работы, был добавлен пункт 3, который звучит следующим образом:

«В период введения чрезвычайного или военного положения, объявления чрезвычайной ситуации либо при введении иных ограничительных мероприятий, в том числе карантина, по решению государственных органов или их должностных лиц, а также в других исключительных случаях, ставящих под угрозу жизнь или здоровье работников, работодатель вправе актом работодателя временно устанавливать с указанием

причин дистанционную работу или комбинированную дистанционную работу до устранения вышеуказанных случаев. При этом обеспечение работников необходимыми для выполнения трудовых обязанностей оборудованием, объектами информатизации в соответствии с законодательством Республики Казахстан об информатизации, услугами связи и иными средствами, а также возмещение расходов определяются актом работодателя».

Данный пункт указывает о том, что работодатель при таких “форс-мажорных” обстоятельствах, должен все-таки издавать свой акт, временно устанавливающий режим дистанционной или комбинированной дистанционной работы. Сам акт должен содержать следующие, обязательные условия:



Основание временного установления дистанционной или комбинированной дистанционной работы;



Список работников, в отношении которых установлена дистанционная или комбинированная дистанционная работа;



Срок дистанционной работы или комбинированной дистанционной работы, не превышающий даты устранения случая, послужившего основанием для временного установления данных видов работы.

3 пункт статьи 138 Трудового Кодекса РК также гласит о том, что обеспечение работника ресурсами для выполнения им его трудовой функции, определяется актом работодателя. Данный вопрос был проблемным в самом начале массового перехода на дистанционный режим работы при пандемии, так как работники высказывали свои возмущения на счет обеспечения их всем необходимым для выполнения работы. Если у одних специалистов для выполнения своих трудовых функций достаточно только компьютера и наличие интернета, то для других могут быть нужны оборудования крупных размеров, либо же, требующих особого подключения, помещения и условий. Поэтому, данный вопрос урегулирован законодателем грамотно, так как сам работодатель учитывает свои возможности и возможности работника, прописывая в акте то, что можно будет использовать и предоставить работнику в рамках дистанционной работы, а также возможность перехода работника в комбинированную дистанционную работу, где он и может пользоваться оборудованием на рабочем месте в определенное время. В случае, если работник использует собственные средства коммуникаций на постоянной основе, работодатель может выплачивать компенсацию, размер, порядок и сроки которой устанавливаются по соглашению сторон.

Так как дистанционная работа требует отдельного регулирования из-за своих особенностей, важно помнить о правах сторон трудовых

отношений. Статья 138 Трудового кодекса РК указывает на следующие права, распространяемые на работника:

📁 ① У работника есть право перейти на дистанционную работу, по его инициативе, посредством его соглашения с работодателем;

📄 ① Работник имеет право получить компенсацию за то, что использовал свое оборудование и средства для осуществления трудовой деятельности;

📄 ① Работник может не находиться в режиме доступности для работодателя вне рабочего времени, установленного трудовым договором или актом работодателя, а работодатель не имеет право требовать нахождения работника в режиме доступности (кроме случаев, предусмотренных в пункте 2, ст. 72 и ст. 86 ТК РК).

📄 ① В случае необходимости выполнения дистанционной работы вне установленной продолжительности рабочего времени работник привлекается к работе только с его письменного согласия и с оплатой в повышенном размере.

📄 ① Работник имеет право на заработную плату в полном размере, с учетом выполнения полного объема работ, обусловленных в трудовом договоре или акте работодателя.

Работодатели, в свою очередь, имеют следующие права:

📁 ① Работодатель по своей инициативе вправе перевести работника на дистанционную работу, посредством соглашения с работником.

📄 ① В период введения чрезвычайного или военного положения, объявления чрезвычайной ситуации либо при введении иных ограничительных мероприятий, в том числе карантина, по решению государственных органов или их должностных лиц, а также в других исключительных случаях, ставящих под угрозу жизнь или здоровье работников, работодатель вправе актом работодателя временно устанавливать с указанием причин дистанционную работу или комбинированную дистанционную работу до устранения вышеуказанных случаев.

📄 ① Работодатель имеет право требовать от работника нахождения в режиме доступности в пределах рабочего времени.

📄 ① В целях защиты служебной, коммерческой или иной охраняемой законом тайны, ставшей известной работнику в процессе дистанционной работы, работодатель вправе указать в трудовом договоре или акте работодателя, акте принимающей стороны условие о сохранении и неразглашении данной информации работодателя, информации принимающей стороны. Этот пункт является самым важным, так как при дистанционном режиме работы вероятность утечки информации велика и работодатель не всегда может контролировать это. Когда договор

уже заключен, или пункт о конфиденциальности прописан в акте, подключается ответственность работника, который не должен допустить утечки информации, являющиеся тайной.

Несчастные случаи происходят часто, как и впрочем утечка информации, но в трудовой деятельности они имеют особое значение, так как при несчастных случаях на производстве в обязательном порядке проводится расследование. Это логично и правильно со стороны законодательства, так как направлено на защиту прав человека. Гораздо сложнее несчастные случаи, сопряженные с работой в удаленном режиме. Этот вопрос, как и многие другие появились после того, как работники ушли на дистанционный режим во время пандемии COVID-19. В статье 138, регулиющую дистанционную работу, также ввели изменения и дополнения на этот счет, применив отсылочную норму на статьи 182 и 182-1. Согласно Трудовому законодательству, работодатель обязан осуществлять регистрацию, учет и анализ несчастных случаев, связанных с трудовой деятельностью, и профессиональных заболеваний, а также обеспечивать расследование несчастных случаев, связанных с трудовой деятельностью, в порядке, установленном законодательством Республики Казахстан.

Таким образом, даже если несчастный случай произошел дома, в рабочее время, при дистанционной работе, то оно в обязательном порядке должно быть расследовано и зарегистрировано. Законодатель не нарушил принципы трудового законодательства РК, ставящие в приоритет жизнь и здоровье работника, а также обеспечивающие безопасные условия труда. Даже при дистанционной работе, работодатель должен соблюдать данные принципы и стараться не допустить несчастные случаи.

В заключении, хочется сказать, что пандемия COVID-19 был сложным этапом для всего человечества, но она поставила новые вопросы для законодательства и дала почву для его улучшения. Было много споров, недопониманий у сторон трудовых отношений, так как произошел массовый простой. Работники отказывались переходить на дистанционный режим, работодатели были не готовы к новому режиму, появилось множество проблем и вопросов. Работодатели переводили работников на дистанционную работу различными способами, не зная какой из них правомерно будет примерить; работники стали говорить о том, кто им должен предоставить оборудование и средства связи; нужно было сохранить права и обязанности субъектов трудовых правоотношений даже при работе удалено; после того, как начали происходить несчастные случаи, возник вопрос о регистрации и расследовании случаев.

Законодатель решил эти вопросы Законом Республики Казахстан от 1 июля 2021 года № 61-VII ЗРК «О внесении изменений и дополнений в Трудовой кодекс Республики Казахстан по вопросам совершенствования правового регулирования дистанционной работы». В частности, больше всего изменений и дополнений было в отношении статьи 138 Трудового Кодекса РК (Дистанционная работа).

Там было определено, что работодатель переводит сотрудников при условиях непреодолимой силы на дистанционную или комбинированную дистанционную работу своим актом. Работодатель предоставляет оборудование и платит за средства связи работника, а если работник пользуется своими ресурсами, то он имеет право на компенсацию.

И у работников, и у работодателей есть права, защищенные статьей 138 ТК РК. Несчастные же случаи, которые произошли в рабочее время, но при дистанционной работе, в обязательном порядке подлежат регистрации и расследованию.

Из вышеизложенного можно сделать вывод о том, что права работников и работодателей защищены, а также в аналогичных случаях простоя, стороны будут знать порядок перевода на дистанционную или комбинированную дистанционную работу и порядок осуществления работы в данном режиме.

Список использованных источников:

1. Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V ЗРК, /<https://adilet.zan.kz>
2. Закон Республики Казахстан от 1 июля 2021 года № 61-VII ЗРК “О внесении изменений и дополнений в Трудовой кодекс Республики Казахстан по вопросам совершенствования правового регулирования дистанционной работы” /<https://adilet.zan.kz>
3. МК-Казахстан: “В Казахстане в сто раз возросло число людей, работающих удаленно” / <https://mk-kz.kz/social/2021/03/17/v-kazakhstanev-sto-raz-vozroslo-chislo-lyudey-rabotayushhikh-udalенno.html>
4. <https://dogovor24.kz/questions/esli-rabotnik-poluchil-travmu-pri-udalennom-rezhime-raboty-eto-budet-schitatsya-kak-neschastnye-sluchai-svyazannye-s-trudovoi-13096.html>
5. Закон РК от 24.11.2015 «Об информатизации» № 418-V /<https://adilet.zan.kz>
6. Forbes Kazakhstan: Как пандемия повлияла на рынок труда в Казахстане / https://forbes.kz/process/expertise/kak_pandemiya_povliyala_na_rynok_truda_v_kazahstane

ӘОЖ 347.63

Исабаева Жансая

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

ӘЛЕУМЕТТІК ЖЕЛІДЕГІ БАЛА ҚҰҚЫҚТАРЫН ҚОРҒАУ

Ғылыми жетекші:

Қасымбек А.О.

з.ғ.м., Каспий қоғамдық университеті «Әділет» Жоғары
құқық мектебінің сеньор-лекторы

Аңдатпа

Мақала ішінде әлеуметтік желідегі бала құқықтарын қорғау және қамтамасыз ету мәселелері қарастырылған. Автор қазіргі уақытта технология мен интернеттің дамуы қауіпсіздіктің дәстүрлі принциптерін өзгертуде және бұл мәселеге жаңа көзқарас пен нақты кешенді шаралар қабылдауды талап ететіндігіне назар аударады. Тек Қазақстанды ғана емес, бүкіл әлемде құқық қорғаушылар және БАҚ өкілдерін алаңдатып отырған өзекті мәселе ретінде жасөспірімдер арасындағы интернетке тәуелділік деңгейін төмендету мәселесі тереңірек қарастырылып, балаларды әлеуметтік желі қауіптерінен қорғаудың құқықтық тетіктерін іске қосу қажеттілігі бар екенін атап өтіледі.

Түйінді сөздер: технология, интернет, қауіпсіздік, жасөспірімдер, тәуелділік, тетіктер, киберкеңестік, зерттеу, ұялы телефон, статистика, құқық, БАҚ, ақпарат, ар- намыс.

Исабаева Жансая

Студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета
Республика Казахстан, г. Алматы

ЗАЩИТА ПРАВ ДЕТЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация

В статье рассматриваются вопросы защиты и обеспечения прав детей в социальных сетях. Автор обращает внимание на то, что развитие технологий и Интернета в настоящее время меняет традиционные принципы безопасности и это требует нового подхода к этой проблеме и принятия конкретных комплексных мер. Проблема снижения уровня интернет-зависимости среди подростков считается актуальной проблемой не только в Казахстане, но и во всем мире, вызывает беспокойство у правозащитников и представителей СМИ и отмечается, что существует необходимость внедрения правовых механизмов защиты детей от опасностей социальных сетей.

Ключевые слова: технологии, Интернет, безопасность, подростки, зависимость, инструменты, киберсоветы, исследования, мобильный телефон, статистика, закон, СМИ, информация, честь.

Isabaeva Zhansaya

1 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

PROTECTION OF RIGHTS OF CHILDREN IN SOCIAL NETWORKS

Annotation:

The article deals with issues of protection and protection of children's rights in social networks. The author draws attention to the fact that the development of technologies and the Internet is currently changing the traditional principles of security, and this requires a new approach to this problem and the adoption of concrete complex measures. The problem of reducing the level of Internet addiction among teenagers is considered an urgent problem not only in Kazakhstan, but also in the whole world, it causes concern among human rights defenders and media representatives, and it is noted that there is a need to implement legal mechanisms to protect children from the dangers of social networks.

Keywords: technology, Internet, security, teenagers, addiction, tools, cyber councils, research, mobile phone, statistics, law, media, information, honor.

Бала құқықтары туралы конвенцияның 1- бабына сәйкес, әрбір адам баласы 18 жасқа толғанға дейін, егер осы балаға қолданылатын заң бойынша ол кәмелеттік жасқа бұрынырақ толып қоймаса, **бала** болып саналады.[1]

Құқық қорғау органдарының пікірінше, кибербуллинг құрбандары көп жағдайда балалар болып табылады. Себебі олар әртүрлі шектеу қойылмаған сайттарды, әлеуметтік желілерді орынсыз пайдаланып, неше түрлі жағдайға жиі ұрынады. [2]

Бала электрондық пошта арқылы, әлеуметтік желілерде, SMS немесе мессенджер арқылы ақшалай сыйлық ұтып алғаны, ақшаға айырбастауға болатын ата-анасымен Мальдив аралдарына саяхат жасағаны немесе байдың мұрагері болғаны туралы хабарлама алуы мүмкін. Оның келісімін растау үшін ол сілтеме бойынша өтіп, тіркелуі керек. Анкетада жеке ақпаратты, соның ішінде үйде бар кез келген төлем картасының нөмірін, оның жарамдылық мерзімін және артқы жағындағы үш таңбалы кодты көрсетуді сұрайды.

Әлеуметтік желіде онлайн-тұзақтар деген түсінік бар. Егер балаалаяқтарға жеке және төлем туралы ақпаратты берсе, олар бұл ақпараттыжеке пайда үшін пайдаланып, ересектердің ақшасына қол жеткізуі мүмкін.

Қазіргі таңда әлеуметтік желіде “Слово пацана” атты фильм желіде қызу талқыға түсіп отыр, ал оның ішінде, көбінесе жасөспірімдер арасында қызу талқыға түсуде. Басым көпшілігі фильмді романтизациялауда. Жоба жасөспірімдер мен мектептер арасында қылмыстық романысты насихаттайды.

Әлеуметтік желілерде, соның ішіндегі «Tiktok» қосымшасы [3] арқылы түрлі сол фильмнен кадрларды қайталауда.

«Осында зорлық-зомбылық, ішімдік ішу мен заң бұзу көріністері көп, ал сюжет мектеп оқушыларына арналған. Фильмнің негізгі мақсатты аудиториясы жасөспірімдер тіпті мәжбүрлі «18+» таңбасының өзі маңызды емес: балалар тыйым салынғанға қол жеткізу үшін соғұрлым көп күш салады.

Қазақстан Республикасының «Кинематография туралы» заңына сәйкес балалардың денсаулығы мен дамуына зардабын тигізетін ақпараты бар, суицид, адам өлтіру, отбасылық өмір проблемалары мен ажырасуды, есірткі және алкогольге тәуелділікті, жалаңаштануды насихаттайтын фильмдер, жыныстық қатынас немесе эротика көріністер бейнеленген, былапыт сөздер, нормативтік емес лексика қолданылған фильмдер 18 жастан үлкен және 21 жастан үлкен көрермендерге көрсетілуі тиіс [1].

Ресей Федерациясының «О защите детей от информации, причиняющей вред их здоровью и развитию» заңына сәйкес, балалар арасында таратуға тыйым салынған ақпараттың қатарына балалардың өмірі мен денсаулығына қауіп төндіретін әрекеттер жатады. Мысалы, өзін-өзі өлтіруге немесе басқа адамдардың өміріне немесе денсаулығына зиян келтіретін не балаларды қылмысқа итермелейтін әрекеттер және т.б. [4]

Ал бұл фильм (Слово пацана) осы талаптарға қарама- қайшы келіп тұр.

Фильмде жасөспірімдердің өмірі мен денсаулықтарына қауіп төндіретін, өлімнің, суицидтің балалар тіпті ауыр қылмыс жасаған көріністер өте жиі қайталанады.

Жасөспірімдердің цензурасыз көріністерді ашық көрсетуі

1. ер мен әйел арасындағы жыныстық қатынасты бейнелеу немесе сипаттау ретінде ұсынылған;

2. Жасөспірімдердің нашар мінез құлықтары

3. Заңсыз мінез-құлықты негіздеу; балаларда қорқыныш, немесе үрей тудыратын, оның ішінде зорлық-зомбылықсыз өлімнің, аурудың, суицидтің, жазатайым оқиғаның, жазатайым оқиғаның немесе апаттың және (немесе) олардың зардаптарын қорлайтын түрдегі бейне немесе сипаттау түрінде ұсынылған;

4. Белгілі бір жас санатындағы балалар арасында таралуы шектелген ақпаратқа мыналар жатады

қатыгездіктің, физикалық және (немесе) психикалық зорлық-зомбылықтың (жыныстық зорлық-зомбылықты қоспағанда), қылмыстың немесе қоғамға қарсы өзге де әрекеттің бейнесі немесе сипаттамасы түрінде ұсынылған;

Жасөспірімдер мен балалар ең көп отыратын Tik Tok қосымшасы. Пропаганда осы жақта болып жатыр. Яғни балалар сол сияқты түрлі криминалды сериалдарды романтизациялауда.

Бұл фильмнің көрсетіліміне біздің ойымызша шектеу қою қажет, бұл балалардың теріс дамуына үлес қосады. Бірақ көптеген платформалар бар екенін ұмытпауымыз қажет, соның бірі Tik Tok қосымшасы. Платформада өзге мемлекет пен елдердің бейне роликтерін де қарауға болады. Сәйкесінше түрлі заттар насихатталады және сақталады.

Неге балалар? Бұл қосымшада жас шектеуі жоқ.

Индонезия, Квебек және Оңтүстік Кореяда Tik Tok тек (14 жастан жоғары) пайдаланушыларға ғана қолжетімді. Ал бізде ондай шектеу әзірге жоқ. [5]

«Бала құқығы туралы» Конвенцияның 2,3 және 16-бабына сәйкес [1] кемсітілушілікті болдырмау Әрбір бала нәсіліне, терінің түсіне, жынысына, тіліне, дініне, әл-ауқаты мен әлеуметтік шығу тегіне қарамастан, осы Конвенцияда көрсетілген барлық құқықтарға ие. Ешкімді кемсітуге болмайды. Баланың мүдделерін қорғау шешімдерді қабылдау барысында үкімет балалардың мүдделерін барынша қамтамасыз етіп, оларға ерекше қорғау мен күтімді көрсетуі тиіс. Жеке өмір құқығын қорғау Әрбір баланың жеке өмірге құқығы бар. Ешкім оның абырой-беделіне нұқсан келтіруге, сондай-ақ рұқсатсыз оның үйіне кіруге және оның хаттарын оқуға құқығы жоқ. Бала өзінің ар-намысы мен абыройына заңсыз қол сұғудан қорғау алуға құқылы.

Пайдаланылған қайнар көздерінің тізімі:

1. «Бала құқықтары туралы» Конвенцияны ратификациялау туралы заңы. <https://adilet.zan.kz/kaz/docs/Z1900000212>
2. Как мошенники могут обмануть вашего ребенка
3. Тик ток қосымшасы
4. https://www.consultant.ru/document/cons_doc_LAW_108808/
5. Wikipedia.org

УДК 349.2

Кайып Зере Калиевна

Студентка 2 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ЭЛЕКТРОННЫЕ ПОДПИСИ И ПОДТВЕРЖДЕНИЕ ЛЕГИТИМНОСТИ ТРУДОВЫХ ОТНОШЕНИЙ: ПЕРЕХОД ОТ БУМАЖНЫХ К ЦИФРОВЫМ ФОРМАТАМ

Аннотация

Данная статья рассматривает вопросы внедрения электронных подписей в сфере трудовых отношений, а также перспективы и риски данного перехода от традиционных бумажных документов к цифровым форматам. Анализируются последние изменения в законодательстве, касающемся электронного документооборота. Автор рассматривает

понятие электронной цифровой подписи, условия ее формирования и сферы ее использования. Особо обращается внимание на преимущества электронной цифровой подписи, а также на ее недостатки.

Ключевые слова: электронные подписи, трудовые отношения, цифровые форматы, законодательство

Кайып Зере Калиевна

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 2 курс студенті,
Қазақстан Республикасы, Алматы қ.

**ЭЛЕКТРОНДЫҚ ҚОЛТАҢБАЛАР ЖӘНЕ ЕҢБЕК ҚАТЫНАСТАРЫНЫҢ
ЗАҢДЫЛЫҒЫН РАСТАУ: ҚАҒАЗДАН ЦИФРЛЫҚ ФОРМАТҚА КӨШУ**

Аңдатпа

Бұл мақалада еңбек қатынастары саласында электронды қолтаңбаны енгізу мәселелері, сондай-ақ дәстүрлі қағаз құжаттардан цифрлық форматқа көшудің келешегі мен тәуекелдері қарастырылған. Электрондық құжат айналымына қатысты заңнамадағы соңғы өзгерістер талданады. Автор электрондық цифрлық қолтаңба түсінігін, оның қалыптасу шарттарын және қолдану аясын қарастырады. Электрондық цифрлық қолтаңбаның артықшылықтарымен қатар оның кемшіліктеріне де ерекше назар аударылады.

Түйінді сөздер: электронды қолтаңба, еңбек қатынастары, цифрлық форматтар, заңнама

Kaiyp Zere

2 year student of the Higher School of Law “Adilet”
Caspian Public University,
Republic of Kazakhstan, Almaty

**ELECTRONIC SIGNATURES AND CONFIRMATION OF THE LEGITIMACY
OF LABOR RELATIONS:
THE TRANSITION FROM PAPER TO DIGITAL FORMATS**

Annotation:

This article examines the issues of introducing electronic signatures in the field of labor relations, as well as the prospects and risks of this transition from traditional paper documents to digital formats. The latest changes in

legislation relating to electronic document management are analyzed. The author examines the concept of an electronic digital signature, the conditions for its formation and the scope of its use. Particular attention is drawn to the advantages of an electronic digital signature, as well as its disadvantages.

Key words: electronic signatures, labor relations, digital formats, legislation

Электронная подпись, также известная как электронная цифровая подпись или цифровая подпись, подтверждает авторство электронного документа, будь то физическое лицо или аккаунт в криптовалютной системе. Она устанавливает связь между автором и самим документом, используя криптографические методы, и невозможна для подделки обычным копированием. ЭЦП представляет собой реквизит электронного документа, полученный через криптографическое преобразование информации с использованием закрытого ключа подписи. Она обеспечивает проверку целостности документа, подтверждение владельца сертификата ключа подписи и неотказуемость подписи при успешной проверке.

Обязательное условие для электронных документов — наличие ЭЦП. Важно отметить, что сканированные версии документов не рассматриваются как электронные документы. Национальный удостоверяющий центр широко используется в большинстве систем электронного документооборота в Казахстане.

Как и где формируется электронный документ?

В соответствии с законодательством о электронном документе, для соблюдения требований подписи ЭЦП необходима система электронного документооборота (СЭД). СЭД представляет собой платформу для обмена электронными документами, регулируемую законами и нормативами Казахстана. Участники СЭД могут быть как физическими, так и юридическими лицами, включая государственные органы. Идентификация пользователей в СЭД происходит с использованием ЭЦП, выдаваемых Национальным удостоверяющим центром. Существуют различные СЭД с разными стоимостями и функциональностью, предоставляющие период тестирования для оценки их соответствия вашим потребностям.

Какие документы могут быть оформлены в электронной форме?

Принцип электронного документооборота в государственных и негосударственных информационных системах заключается в обеспечении возможности использования электронных документов в

различных областях деятельности, где применяются информационно-коммуникационные технологии для работы с данными – их создания, обработки, хранения и передачи.

Гражданский кодекс Республики Казахстан ясно определяет, что сделка может быть оформлена в письменной форме на бумажном носителе или в электронной форме. При этом допускается использование электронной цифровой подписи (ЭЦП) при условии соответствия законодательству и согласия всех участников сделки.

Согласно Гражданскому кодексу Республики Казахстан, сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей. Вместе с тем, стоит отметить, что определенные сделки, которые требуют нотариального удостоверения в соответствии с законодательством, не могут быть осуществлены в электронной форме.

В соответствии с Законом об электронном документе подчеркивается, что электронный документ, который соответствует установленным законом требованиям и удостоверенный с использованием ЭЦП компетентного лица, обладающего правом на его подписание, имеет такую же юридическую силу, как и документ, подписанный на бумажном носителе.

В сфере трудового права, электронная подпись (ЭП) или электронная цифровая подпись (ЭЦП) может применяться для заключения и подтверждения различных документов, связанных с трудовыми отношениями. Например, это может включать в себя электронное подписание трудовых контрактов, соглашений о соблюдении корпоративных политик, заявлений об отпуске, и других документов, связанных с управлением персоналом.

Использование электронных подписей в трудовом праве обеспечивает удобство и эффективность в процессе формирования и утверждения документов. Это также может ускорить процессы согласования между работниками и работодателями, а также обеспечить сохранность электронных записей. Помимо этого, применение электронных подписей может соответствовать современным требованиям цифровизации и повышения безопасности документооборота в сфере труда.

Использование электронной цифровой подписи:

1. ЭЦП равнозначна собственноручной подписи при:

– Удостоверении подлинности через открытый ключ с регистрационным свидетельством.

- Правомерном владении закрытым ключом.
 - Использовании в соответствии с регистрационным свидетельством.
 - Создании и выдаче аккредитованным удостоверяющим центром.
2. Закрытые ключи являются собственностью владельцев, не могут быть переданы, и могут храниться в удостоверяющем центре.
3. Владелец регистрационного свидетельства юридического лица может передать полномочия на использование ЭЦП работнику или назначенному лицу.

Работодатель издает акты в пределах своей компетенции в соответствии с настоящим Кодексом и иными нормативными правовыми актами Республики Казахстан, трудовым договором, соглашениями, коллективным договором.

Акты работодателя оформляются в письменной форме или форме электронного документа, удостоверенного посредством электронной цифровой подписи. В контексте трудового права республики Казахстан, использование электронной цифровой подписи (ЭЦП) в актах работодателя играет ключевую роль. ЭЦП обеспечивает надежное подтверждение подлинности и целостности электронных документов, таких как приказы, уведомления и другие акты, издаваемые работодателем.

ЭЦП в данном контексте служит средством гарантирования того, что документы, созданные в электронной форме, являются официальными и не подвергались изменениям после подписания. Это также повышает эффективность процессов управления персоналом, уменьшает бумажную работу и способствует соблюдению законодательства в области трудовых отношений.

Преимущества:

Электронные подписи обладают рядом преимуществ, таких как повышенная безопасность, ускорение процессов, снижение затрат на бумажную документацию, улучшенная возможность отслеживания изменений и повышение удобства для пользователей.

Электронные подписи обеспечивают высокий уровень защиты данных, так как они часто используют шифрование для предотвращения подделки. Они также ускоряют процессы, поскольку позволяют заключать сделки и подписывать документы онлайн, минимизируя необходимость физического присутствия. Это снижает затраты на бумажную документацию, хранение бумаг и ручные процессы.

Электронные подписи улучшают прозрачность, так как обеспечивают возможность отслеживания изменений и проверки подлинности документов. Кроме того, они повышают удобство для пользователей, предоставляя возможность подписания документов из любой точки мира и с любого устройства с доступом в Интернет.

Несмотря на множество преимуществ, у электронных подписей есть и некоторые недостатки.

К ним относятся:

1. Безопасность: Хотя электронные подписи обеспечивают высокий уровень защиты, существует риск взлома системы или несанкционированного доступа к личным данным.

2. Требования к технической инфраструктуре: Использование электронных подписей требует наличия соответствующей технической инфраструктуры, что может стать проблемой для небольших компаний или организаций с ограниченными ресурсами.

3. Проблемы конфиденциальности: В случае недостаточной защиты конфиденциальных данных может возникнуть риск утечки информации при использовании электронных подписей.

4. Сложности в некоторых отраслях: В некоторых сферах, таких как нотариальные услуги или определенные виды сделок, могут существовать юридические или культурные барьеры для признания электронных подписей.

5. Необходимость обучения и принятия: Внедрение систем электронных подписей требует обучения персонала и изменения традиционных рабочих процессов, что может вызвать сопротивление со стороны сотрудников.

6. Проблемы совместимости и стандартизации: Недостаток единых стандартов для электронных подписей может создавать сложности при взаимодействии с системами различных поставщиков, усложняя интеграцию в различные бизнес-процессы.

7. Отсутствие физической «весомости»: Некоторые ситуации могут требовать документов с физической подписью, поскольку электронные подписи могут не иметь такого же визуального воздействия или авторитета.

8. Возможность отрицания подписи: В отличие от физической подписи, электронную подпись теоретически можно оспорить с точки зрения отрицания своего участия в подписании документа.

9. Угрозы кибербезопасности: В мире, насыщенном киберугрозами, существует риск хакерских атак на системы электронных подписей, что может подорвать их доверие и эффективность.

Значение в трудовых отношениях Документооборот и эффективность

Внедрение электронного документооборота, поддерживаемого электронными подписями, существенно повышает эффективность организации. Электронные подписи обеспечивают безопасность, подлинность и целостность документов, что способствует сокращению времени на процессы утверждения и обмена информацией.

Электронный документооборот также снижает зависимость от бумажных носителей, улучшает доступность данных и обеспечивает возможность быстрого и удобного поиска необходимой информации. Это приводит к более оперативным решениям, сокращению затрат на бумажную документацию и повышению общей эффективности бизнес-процессов.

Гарантии подлинности и целостности документов

1. Подлинность (Аутентичность): Электронная подпись подтверждает, что документ создан или одобрен определенным участником процесса. Это обеспечивает идентификацию автора и гарантирует, что информация не была изменена после подписания.

2. Целостность: Электронная подпись защищает документ от внесения изменений после того, как он был подписан. Если содержимое документа изменится, подпись станет недействительной, что предупреждает о любых попытках подделки или вмешательства.

Система электронного документооборота (СЭД) представляет собой программное обеспечение, предназначенное для управления потоком документов. Она способна функционировать как в онлайн, так и в офлайн режиме, что означает, что серверы для обработки и хранения данных могут быть размещены в облаке или на сервере компании. Таким образом, вопросы безопасности и защиты данных в основном связаны с обеспечением сохранности облачных сервисов и серверов.

Правовые последствия использования электронной подписи

Применение электронного документооборота влечет значительные вопросы, связанные с безопасностью. В процессе электронного документооборота возникает риск утраты данных, несанкционированного доступа и других технических угроз, которые могут иметь юридические последствия. Например, возможный риск невозможности подтверждения совершения сделки в случае отсутствия физического документа и доступа к системе электронного документооборота. Отдельно следует учитывать юридический аспект, так как согласно Гражданскому кодексу

су РК несоблюдение простой письменной формы сделки может лишить стороны права доказывать ее существование в споре, и это важно для внешнеэкономических сделок. Вопрос также возникает относительно эквивалентности простой письменной формы и формы, к которой приравнивается электронный документ.

Практические аспекты

Применение электронных подписей в трудовых отношениях.

Согласно Трудовому кодексу Республики Казахстан, трудовой договор должен быть заключен в письменной форме и содержать не менее двух экземпляров, подписанных сторонами. Заключение, внесение изменений и дополнений к трудовому договору может осуществляться через электронный документ, подтвержденный электронной цифровой подписью. Работодатель обязан внести соответствующую информацию о заключении и прекращении трудового договора, внесенных изменениях и дополнениях в единую систему учета трудовых договоров согласно установленному порядку.

Рекомендации по внедрению и использованию

1. Анализ потребностей: Перед внедрением электронного документооборота рекомендуется провести тщательный анализ потребностей вашей компании, выявив ключевые задачи и требования к системе.

2. Выбор СЭД: Выберите систему электронного документооборота, соответствующую потребностям вашего бизнеса. Уделяйте внимание функциональности, уровню безопасности, возможности интеграции с другими системами.

3. Обучение персонала: Предоставьте достаточное обучение сотрудникам, которые будут использовать систему. Обеспечьте поддержку и возможность задавать вопросы в процессе внедрения.

4. Эффективное внедрение: Внедряйте систему поэтапно, начиная с одного отдела или проекта. Это позволит избежать существенных нарушений в работе и обеспечит более гладкое внедрение.

5. Согласование с законодательством: Удостоверьтесь, что ваши процессы электронного документооборота соответствуют законодательству, включая требования к электронной подписи и хранению электронных документов.

6. Безопасность: Обеспечьте надежные меры безопасности для электронных документов, включая защиту от несанкционированного доступа и системы резервного копирования.

7. Измерение и оптимизация: Внедрив систему, регулярно измеряйте ее эффективность и соблюдение стандартов. Вносите коррективы и оптимизируйте процессы при необходимости.

8. Интеграция: Рассмотрите возможности интеграции СЭД с другими системами, такими как управление отношениями с клиентами (CRM) или системы учета.

9. Обратная связь и улучшения: Активно собирайте обратную связь от пользователей и внедряйте улучшения в систему в соответствии с потребностями бизнеса.

10. Постоянное развитие: Следите за новыми технологическими тенденциями и обновляйте свою систему электронного документооборота для поддержания ее актуальности и эффективности.

Основные выводы

Из изложенного можно сделать вывод, что электронный документ признается эквивалентным документу на бумажном носителе. Однако для такого признания необходимо соблюдение требований, установленных законодательством для письменных документов, а также соответствие стандартам Закона об электронном документе, включая подписание ЭЦП. Преимущества электронного документооборота значительны, особенно для компаний, взаимодействующих с большим числом клиентов и поставщиков, включая физических лиц. Это устраняет потребность в постоянном запросе бумажных оригиналов первичных документов и снижает связанные с этим расходы. Однако следует уделить внимание аспектам безопасности, таким как защита от несанкционированного доступа, регулярное резервное копирование данных для минимизации риска потери, получение согласия субъектов персональных данных на обработку и использование мер для обеспечения защиты персональных данных.

Перспективы развития использования электронной подписи в трудовом праве

1. Упрощение трудового договора: Внедрение электронной подписи позволит упростить процессы заключения и внесения изменений в трудовые договоры, снизив трудозатраты и повысив эффективность.

2. Электронные уведомления и заявления: Возможность использования электронной подписи открывает дорогу для электронных уведомлений и заявлений между работниками и работодателями, сокращая бумажную работу.

3. Удаленная работа и дистанционное управление: С ростом популярности удаленной работы электронные подписи станут ключевым инструментом для заключения и управления трудовыми договорами дистанционно.

4. Цифровая легализация документов: Постепенное переход к цифровой легализации трудовых документов с использованием электронных подписей способствует сокращению времени на формальности и уменьшению бюрократии.

5. Автоматизация процессов: Внедрение электронной подписи позволяет интегрировать системы управления трудовыми отношениями и автоматизировать многие рутинные процессы.

6. Безопасность и Контроль: Электронные подписи обеспечивают высокий уровень безопасности и контроля над документами, что особенно важно в трудовых отношениях.

7. Соблюдение законодательства: Применение электронной подписи должно соответствовать законодательству, и перспективы развития включают в себя совершенствование нормативной базы в этой области.

8. Обучение и повышение квалификации: Важной перспективой является обучение кадров использованию электронных подписей и повышение квалификации в области цифровизации трудовых процессов.

9. Интеграция с электронными системами учета: Стратегическое внедрение электронных подписей позволяет интегрировать трудовые процессы с другими системами учета в организации.

10. Электронные личные дела: Создание и хранение электронных личных дел с использованием электронной подписи повысит удобство доступа и управления персональными данными сотрудников

Список использованных источников:

1. https://adilet.zan.kz/rus/docs/Z030000370_
2. <https://tsnik.kz/vopros-otvet/492242/?month=02&year=2022&>
3. Министерства труда и социальной защиты населения РК (<https://www.enbek.gov.kz>)
4. <https://online.zakon.kz/m/amp/document/35120090>
5. <https://www.nur.kz/technologies/instructions/1734779-cto-takoe-ecp-i-dla-cego-ona-nuzna-v-rk/>
6. <https://findhow.org/368-kak-poluchit-etsp-v-kazahstane.html>

УДК 343.3/.7

Кастоева Дали
студентка 3 курса
Университета Международного Бизнеса
Республика Казахстан, г. Алматы

БОРЬБА С КИБЕРБУЛЛИНГОМ: КАК ИНТЕРНЕТ ВОЗДЕЙСТВУЕТ НА ПРАВА ДЕТЕЙ И ПОДРОСТКОВ

Аннотация

Статья посвящена обзору проблемы кибербуллинга и его воздействия на права детей и подростков в интернет эпоху. В статье приведена официальная статистика Республики Казахстан по случаям кибербуллинга среди детей. Автором рассмотрены и выявлены существующие пробелы в законодательстве Республики Казахстан, связанные с кибербуллингом.

Ключевые слова: интернет, кибербуллинг, платформы, права, законодательство, безопасность, цифровая травля, ответственность.

Кастоева Дали
Халықаралық бизнес университетінің
3 курс студенті
Қазақстан Республикасы, Алматы қ.

КИБЕРБУЛЛИНГПЕН КҮРЕС: ИНТЕРНЕТ БАЛАЛАР МЕН ЖАСӨСПІРІМДЕРДІҢ ҚҰҚЫҚТАРЫНА ҚАЛАЙ ӘСЕР ЕТЕДІ

Аңдатпа

Мақалада кибербуллинг мәселесі және оның интернет дәуіріндегі балалар мен жасөспірімдердің құқықтарына әсері қарастырылған. Мақалада балалар арасындағы кибербуллинг жағдайлары бойынша Қазақстан Республикасының ресми статистикасы берілген. Автор кибербуллингке қатысты Қазақстан Республикасының заңнамасында бар олқылықтарды қарастырып, анықтады.

Түйінді сөздер: Интернет, кибербуллинг, платформалар, құқықтар, заңнама, қауіпсіздік, цифрлық қорлау, жауапкершілік.

Kastoyeva Dali

3rd year student

University of International Business

Republic of Kazakhstan, Almaty

COMBATING CYBER BULLYING:

HOW THE INTERNET AFFECTS THE RIGHTS OF CHILDREN AND ADOLESCENTS

Abstract

The article reviews the problem of cyber bullying and its impact on the rights of children and adolescents in the Internet era. The article provides official statistics of the Republic of Kazakhstan on cases of cyber bullying among children. The author reviewed and identified existing gaps in the legislation of the Republic of Kazakhstan related to cyber bullying.

Keywords: Internet, cyber bullying, platforms, rights, legislation, security, digital bullying, responsibility.

В современном цифровом мире, где дети и подростки активно взаимодействуют с онлайн-пространством вопрос травли в интернете, остается актуальным и требует решения. Кибербуллинг, травля с использованием цифровых технологий [1]. Кибербуллинг включает в себя различные формы жестокого поведения такие как: оскорбления, угрозы, шантаж, распространение ложной информации и преследование. Кибербуллинг в век технологий может происходить абсолютно везде, на любых сайтах, устройствах и интернет-пространствах. Чаще всего это любимые для молодежи социальные сети и игровые платформы. Важно обратить внимание на то, как наши законы обеспечивают защиту прав детей и подростков от такой формы цифрового насилия, ведь кибербуллинг, являясь формой интернет травли представляет серьезную угрозу для общества, это серьезное нарушение прав и свобод детей и подростков в интернет пространстве. Кибербуллинг это не только социокультурный вызов для общества, но также нарушение законодательства ведь главными ценностями Республики Казахстан (далее - РК) являются человек, его жизнь, права и свободы, так нам гарантирована защита чести и достоинства, а кибербуллинг нарушает данные нам права [2].

Почему буллинг в интернет эпоху это проблема? В настоящее время дети и подростки цифрофизированы, они буквально рождаются со смартфонами в руках. У большинства детей есть аккаунты в социальных сетях и игровых платформах, это идеальная местность для рождения оскорблений, для унижения чести и достоинства человека, в общем для нарушения основополагающих прав и свобод человека. Если мы обратимся к статистике предоставленной центром по исследованию кибербуллинга, то мы узнаем, что около трети всех детей и подростков в мире подвергаются травле на интернет-платформах, а в Казахстане только за 2022 год около 17,5% детей подверглись цифровой травле [3]. Кибербуллинг оказывает серьезное воздействие на психологическое здоровье детей и подростков. Такие «интернет атаки» вызывают депрессию, стресс, тревогу, ухудшают качество жизни и могут даже привести к самоубийству, если брать в расчет еще не окрепший ум детей.

Рассмотрим воздействие интернета на права несовершеннолетних в случае с фактом кибербуллинга.

Нарушение права на безопасность: Кибербуллинг создает угрозу безопасности как в физическом, так и в эмоциональном плане. Несовершеннолетний из-за продолжающихся угроз и преследования чувствует себя в собственном доме небезопасно.

Нарушение права на личную жизнь и приватность: Путем кибербуллинга недобросовестный человек преследует, распространяет ложную информацию, либо личную информацию, тем самым нарушая право на личную жизнь.

Нарушение права чести и достоинства человека: Путем кибербуллинга происходит цифровая травля с использованием слов и выражений, унижающих честь и достоинство человека.

Нарушение права на защиту от дискриминации: Согласно Конституции, перед законом равны все не зависимо от национальной, расовой и религиозной принадлежности. Кибербуллинг как раз-таки основывается на расовой, национальной и религиозной дискриминации.

Если рассматривать казахстанское законодательство, в частности Уголовный кодекс, то мы заметим, что социальное явление кибербуллинга есть, но отдельной статьи в уголовном кодексе не предусмотрено. На замену приходит статья «оскорбление», которая применяется в случае цифровой травли [4]. И это первый пробел в нашем законодательстве, потому как статья «оскорбление» не в полной мере определяет проблему кибербуллинга. Почему данная статья не подходит под определение кибербуллинга? В первую очередь само определение «оскорбление»

разнится с «кибербуллинг», оскорбление – это унижение чести и достоинства другого лица, выраженное в неприличной форме. Кибербуллинг же цифровая травля, которая происходит ни один и не два раза, а продолжительное время, более того кибербуллинг имеет широкий охват, учитывая, что совершается с использованием различных технологий.

Любой вид буллинга происходит чаще всего среди молодого поколения, лиц недостригших совершеннолетнего возраста. Согласно 15 статье УК РК ответственность за совершенные правонарушения наступает с 16 лет, в более тяжелых случаях с 14 лет. 14 лет — это достаточно осознанный возраст, где индивид дает отчет своим действиям. Любой поступок он совершает осознанно и понимает всю тяжесть совершения неправомерного поступка. В этом возрасте недопустимо считать оскорбления «детским ребячеством». Список рекомендаций пополняет еще один пункт: снижение возраста ответственности с 16 до 14 лет. Более того саму статью «оскорбление» необходимо ужесточить, как первую, так и вторую части, как минимум из-за того, что в силу несерьезности статьи и ее санкций дело об оскорблениях редко доходят до суда и заканчивается все простым примирением сторон.

Каковы меры защиты при обнаружении факта кибербуллинга? В первую очередь необходимо уведомить об этом родителей и/или администрацию учебного заведения. На онлайн-платформах можно обратиться в техническую поддержку, которая после рассмотрения отправленной вами жалобы/заявки удалит комментариев или пост. Если цифровая травля продолжительна, можно обратиться в экспертную группу, которая разбирается с фактами кибербуллинга [5].

В качестве средства правовой защиты можно выделить повышение осведомленности учебных заведений о существующей проблеме среди молодого поколения в виде «кибербуллинга» для предотвращения инцидентов цифровой травли и эффективному реагированию на них при обнаружении. Еще одним важным средством правовой защиты, которым многие пренебрегают является защита ваших конфиденциальных данных и использование законов об информационной безопасности.

Борьба с явлением кибербуллинга имеет важное значение для защиты прав детей и подростков в эпоху развития технологий. Учитывая быстрое развитие и внедрение цифровых технологий среди молодого поколения, перед государством стоит важный вопрос улучшения законодательства в отношении информационной безопасности и улучшения безопасности несовершеннолетних в онлайн-пространстве. Сами

законы касательно буллинга на интернет-ресурсах являются новыми для нашего государства и безусловно требуют доработки. Необходимо продолжать развивать и улучшать методы правовой защиты. Улучшить работу образовательных учреждений по предотвращению случаев цифровой травли среди детей и подростков. Перенимать опыт соседних государств в борьбе с кибербуллингом. Все эти меры в совокупности будут способствовать созданию защищенного цифрового поля не только для детей, но и для взрослых.

Список использованных источников:

1. Интернет-травля: что это такое и как с ней бороться? // ЮНИСЕФ URL: <https://www.unicef.org/kazakhstan/%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%BD%D1%8B%D0%B5-%D0%B7%D0%B0%D0%BC%D0%B5%D1%82%D0%BA%D0%B8/%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%82%D1%80%D0%B0%D0%B2%D0%BB%D1%8F-%D1%87%D1%82%D0%BE-%D1%8D%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B8-%D0%BA%D0%B0%D0%BA-%D1%81-%D0%BD%D0%B5%D0%B9-%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D1%81%D1%8F> (дата обращения: 25.12.2023).

2. Конституция Республики Казахстан от 30.08.1995;

Национальный отчет. Министерство здравоохранения Республики Казахстан Национальный центр общественного здравоохранения МЗ РК «Факторы образа жизни школьников Казахстана, их физическое, психическое здоровье и благополучие. По итогам исследования «Поведение детей школьного возраста в отношении своего здоровья», НВSC, 2022 г. « // https://hls.kz/wp-content/uploads/2023/03/%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9-%D0%BE%D1%82%D1%87%D0%B5%D1%82-HBSC-%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD-2022_010323.pdf

3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V

4. «Об утверждении Правил создания экспертной группы, а также рассмотрения заявления по фактам кибербуллинга в отношении ребенка» от 6 сентября 2022 года № 29469. //

ӘОЖ 349.2

Кахарманова Милана
Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 2 курс студенті,
Қазақстан Республикасы, Алматы қ.

ИНТЕРНЕТ–ХАЛЫҚТЫ ЖҰМЫСПЕН ҚАМТУДЫҢ ЖАҢА НЫСАНЫ РЕТІНДЕ

Ғылыми жетекші:

Чингисбаева А.Е.

з.ғ.м., Каспий қоғамдық университеті «Әділет» Жоғары
құқық мектебінің сеньор-лекторы

Аңдатпа:

Мақалада «Интернет-жұмыспен қамту» ұғымының мазмұны талқыланады. Автор сонымен қатар қашықтан жұмыс, үй жұмысы және фрилансинг сияқты еңбекті ұйымдастырудың жаңа нысандарын пайдаланудың маңыздылығына назар аударады. Зерттеу барысында автор Интернет арқылы жұмыспен қамтудың бұл түрі оның еңбек нарығының барлық субъектілері үшін бірқатар артықшылықтары бар екені деген қорытындыға келеді. Қазақстан Республикасының Еңбек кодексімен интернетте қашықтан жұмыс істеуді реттеудің құқықтық аспектілеріне талдау жүргізілді.

Түйінді сөздер: қашықтықтан жұмыс істеу, ақпараттық технологиялар, жұмыс беруші, заң, фриланс.

Кахарманова Милана
Студентка 2 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

**ИНТЕРНЕТ-
КАК НОВАЯ ФОРМА ОБЕСПЕЧЕНИЯ ЗАНЯТОСТИ НАСЕЛЕНИЯ**

Аннотация:

В статье рассматривается содержание понятия «Интернет-занятость». Автором также обращается внимание на важность использования новых форм организации труда, таких, как удаленная работа, надомная работа и фриланс. В процессе исследования автор приходит к выводу, что данная форма занятости через интернет доказывает, что она имеет ряд преимуществ для всех субъектов рынка труда. Проведен анализ правовых аспектов регулирования дистанционной работы в интернете Трудовым кодексом Республики Казахстан.

Ключевые слова: удаленная работа, информационные технологии, работодатель, закон, фриланс.

Kaharmanova Milana

2 year student of the Higher School of Law "Adilet"

Caspian Public University,
Republic of Kazakhstan, Almaty

INTERNET-**AS A NEW FORM OF PROVIDING EMPLOYMENT TO THE POPULATION****Annotation:**

The article discusses the content of the concept "Internet employment". The author also draws attention to the importance of using new forms of labor organization, such as remote work, home work and freelancing. In the process of research, the author comes to the conclusion that this form of employment via the Internet proves that it has a number of advantages for all subjects of the labor market. An analysis of the legal aspects of regulating remote work on the Internet by the Labor Code of the Republic of Kazakhstan was carried out.

Key words: remote work, information technologies, employer, law, freelance.

Еңбек нарығы технология мен ақпараттандырудың дамуының арқасында бірте-бірте өзгеруде. Еңбек процесі қоғамдағы орнымызды анықтауда шешуші рөл атқаратындықтан, қоғамдық құрылымның негізі болып табылады. Жаңа технологиялардың танымалдығы мен қолжетімділігі, бір жағынан, адамдар арасында жұмыссыздық қорқынышын тудырады. Екінші жағынан, жұмысты жеңілдетуге және өнімділікті арттыруға қарамастан, технология оларды жұмыс орында-

рынан айырмайды, керісінше қызметтің жаңа түрлерін көрсету арқылы еңбек нарығын өзгертеді.

Ең маңызды технологиялық өзгерістердің бірі дербес компьютердің құрылуы және Интернеттің пайда болуы болды. Бұл еңбек нарығы мен жұмысшылардың өздері үшін үлкен жаңалық ашты, бұл интернет-экономиканы тудырды.

Интернеттегі жұмыс

Интернеттің дамуы жаңа экономикалық қатынастардың қалыптасуына және қоғамның әртүрлі салаларында бұрын таныс емес институционалдық құрылымдардың қалыптасуына әкелді. Интернетте жұмыс істеу жұмыстың жаңа түріне айналды, енді оның не екенін егжей-тегжейлі қарастырайық.

Интернетте жұмыс істеу- бұл Интернетті пайдалануға негізделген жұмыс бағыты. Оның жұмысшыға да, жұмыс берушіге де, тіпті мемлекетке де пайдасы көп. Қызметкер үй шаруасы мен жұмыс өмірін үйлестіре отырып, икемді кесте бойынша жұмыс істей алады; жұмыс беруші осы уақытта үй-жайды жалға алуды үнемдейді; ал мемлекет үшін бұл қоғамдық көліктегі жүктемені және көмірқышқыл газының шығарындыларын азайтуды білдіреді.

Интернеттегі жұмыспен қамту жұмыстың жаңа түрлерін тудырады: үйден жұмыс, қашықтан жұмыс және фрилансинг. Бұл қызмет түрлерінің айырмашылықтары бар, бұл жұмыс пішімін таңдағанда, өзіңіз үшін де, қызметкерлеріңіз үшін де (егер сіз жұмыс беруші болсаңыз) ескеру қажет.

Үйден жұмыс жасау ҚР-ның Еңбек Кодексінің 137-ші бабымен реттеледі.

Кейбір адамдар үйде кеңсе ашқанды жөн көреді. Бұл әртүрлі себептермен орын алады: біреу жолда уақытты босқа кетіргісі келмейді, біреуге үйден жұмыс істеу ыңғайлырақ, біреу жеке кеңістігі кеңсенің жұқа қабырғаларымен шектелмегенде көбірек қуанады.

Үйде жұмыс істеуді қашықтан жұмыс істеумен шатастырмаңыз, өйткені үйден жұмыс істеу бизнесмендерге, кәсіпкерлерге, кеңсе қызметкерлеріне қатысты.

ҚР-ның 137 бабының 3-тармағында Үйде істелетін жұмысты орындау туралы еңбек шартында:

1) жұмысты жұмыскерге меншік құқығымен тиесілі немесе жұмыс беруші бөліп беретін не жұмыс берушінің қаражаты есебінен сапып алынатын жабдықтарды, материалдарды, құрал-саймандар мен құрылғыларды пайдалана отырып орындау;

2) жұмыскерді жұмысты орындау үшін қажетті шикізатпен, материалдармен, жартылай фабрикаттар мен қамтамасыз ету тәртібі мен мерзімдері;

3) жұмыскерге төленетін өтемақы және өзге де төлемдер туралы талаптар міндетті түрде көзделуге тиіс.

Үйден жұмыс істеудің артықшылықтары:

– Жұмысқа жиналып және жетіп үлгеру үшін ерте тұрудың қажеті жоқ;

– Уақыт және көлік шығынына (әсіресе, қалалық жерлерде) ақша үнемдейсіз;

– Бір апта бойы демалыссыз жұмыс істеп, келесі аптада демалуға бір жерге барып қайтуға болады;

– Балалар әрқашан өз қарауыңызда жүреді. Егер олар балабақшаға барса, оларды алып кетуге уақытыңыз болады;

– Бастығыңыз сізден уақытында орындалатын жұмыстан басқа ештеңе сұрамайды. Мысалы, 8 сағат міндетті түрде жұмыста отыруыңызды немесе біреуге көмектесуіңізді талап етпейді;

– Егер мысалы тұмауратып қалсаңыз үйден жұмыс істей бересіз, айналаныздағы адамдарға да жұқтырмайсыз.

Қашықтықтан жұмыс жасау ҚР-ның Еңбек Кодексінің 138 бабымен реттеледі.

Интернет технологияларының дамуы жұмысты кез келген жерден кез келген уақытта орындауға мүмкіндік береді. Жұмыс беруші кеңсе жалдауға немесе онда жұмысшыларды үйлестіру және олардың әлеуметтік өзара әрекеттесуін қолдау үшін жалпы жиналыстар өткізуге құқылы емес. Бұл жағдайда қызметкердің жұмыс орны оның жеке үйі немесе қоғамдық кеңістікте (кафе, кітапхана, т.б.) жұмыс істеу орнына айналады.

Қашықтықтағы жұмыс - жұмыс берушіден айтарлықтай қашықтықта орналасқан, қазіргі заманғы байланыс құралдарын пайдалана отырып, тапсырмаларды және төлемді беретін және алатын жұмыс түрін білдіреді. Оның артында біздің болашағымыз және бүкіл еңбек нарығының болашағы жатыр. Қашықтықтан жұмыс жасау түсінігі өткен ғасырдың 70-жылдарында пайда бола бастады.

ҚР-ның Еңбек кодексінің 138 бабында қашықтықтан жұмыс жасау туралы осы нәрселер айтылған

1. Жұмыс беруші, қабылдаушы тарап жұмыскерді еңбек міндеттерін орындау үшін қажетті жабдықпен, байланыс қызметтері мен және өзге де құралдармен қамтамасыз етеді.

Сонымен қатар тараптардың келісуі бойынша қашықтан жұмыс істейтін жұмыскерге жұмыс беруші, жұмысты орындауға байланысты өзге де негізделген шығындарда, оның ішінде электр энергиясының құнынның өтелуі де мүмкін.

2. Қашықтан жұмыс істейтін жұмыскерлер үшін жұмыс уақытының күнделікті ұзақтығының шектеулері сақтала отырып, жұмыс уақытының тіркелген есебі белгіленеді, оны бақылау ерекшеліктері еңбек шартында немесе жұмыс берушінің актісінде айқындалады.

3. Жұмыскер жұмыс уақытының шегінде жұмыс берушімен, байланыс үшін қолжетімділік режимінде болуға тиіс, яғни жұмыс беруші жұмыскерге звандап, іздеген жағдайда әрқашан онлайн болып отыру қажет.

4. Еңбек шарты тараптарының келісуі бойынша қашықтан жұмыс істейтін жұмыскерлер үшін осы Кодекстің 74-бабына сәйкес икемді жұмыс уақыты режимі белгіленуі мүмкін.

Енді қашықтан жұмыс істейтінең сұранысқа ие мамандықтарға тоқталып кететін болсақ:

- Сайт әкімшілері (администратор), модераторлар
- Веб-әзірлеушілер
- Копирайтерлер
- Дизайнерлер мен суретшілер
- Кенес беруші операторлар
- Программисты
- Есепшілер мен бухгалтерлер
- Редакторлар
- SMM менеджерлері және т.б.

Енді қысқаша фрилансинг туралы айтып өтетін болсақ. Бұл жайлы бәлкім көбілеріңіз білетінде шығар.

Фрилансер (ағылшын фрилансерінен) – штаттан тыс жұмысшы. Фрилансердің өзі тапсырыстарды немесе жобаларды іздейді, оның тұрақты менеджері жоқ, оны жалдайтын клиенттер ғана. Осының арқасында фрилансер өз бетінше (әрине, қызметтер мен еңбек нарығын ескере отырып) жұмыс пен жұмыс күндерінің көлемін, сондай-ақ оның табысын бақылай алады.

Фрилансер белгілі бір қызметті орындау үшін клиенттің кеңсесіне келе алады. Бірақ кәсіптің көптеген түрлері үшін фрилансинг қашықтан жұмыс істеумен біріктіріледі.

«Фрилансерлерге ешкім қысым жасамайды, өз бетінше жұмыс істейді. Яғни бақылау жоқ деуге де болады. Мұндай адамдарға ка-

рьера мен жеке өмір арасында баланс сақтау оңырайық. Жаһандық еңбек нарығына қосылу мүмкіндігі көп. Мәселен, ағылшын тілін жетік меңгергендер халықаралық компанияларда онлайн жұмыс істей алады. Сонымен қатар, фриланстың ең үлкен артықшылығы – жастарға, декретте отырған әйелдерге, мүгедектері бар адамдарға, зейнет жасына тақағандарға жұмысқа орналасуға мүмкіндік береді. Зерттеу бойынша, зейнет жасына жақындаған адамдар фрилансер ретінде айтарлықтай көп ақша табады».

«Қазақстанда фрилансерлердің орташа айлық саны 250 мың шама-сында болды. Ал олардың орташа жалақысы 124 мың теңгені құраған. Медиандық табыс 65 мың теңге болды. Яғни фрилансерлердің жартысы 65 мың теңгеден көп, жартысы бұдан аз тапқан».

Фрилансинг келесі мамандықтар арасында танымал:

Журналистер

Сәулетшілер

Фотографтар мен бейнеоператорлар

Суретшілер мен дизайнерлер

Копирайтерлер мен аудармашылар

Бағдарламашылар

Оптимизаторлар және т.б

Қорытындылай келе айтуымыз келеді: жаңа кәсіптер мен жұмыспен қамту нысандарының құрылуы сөзсіз Интернет пен оның қызметтерінің дамуымен, сондай-ақ пайдаланушылар санымен байланысты. Жыл сайын тек Интернетті және оның ресурстарын пайдалана отырып жүзеге асырылуы мүмкін іс-шаралардың саны артып келеді және бұл тізім тек өсе береді. Жұмыстың дәстүрлі түрі, әрине, жақын болашақта өз маңыздылығын жоғалтпайды, бірақ біз осы мақалада талқылаған балама нұсқалар туралы ұмытпауымыз керек.

Интернет-жұмыспен қамту еңбек ұғымына және халықтың өмір сүру сипатына көптеген өзгерістер әкелді. Көп жағдайда бұл инновациялар адамдардың өмір сүру сапасына оң әсер етті.

Пайдаланылған қайнар көздерінің тізімі:

1. Кастеллс М. Ақпараттық дәуір: экономика, қоғам және мәдениет. Ақпараттық технологиялардың жұмыспен қамтуға әсері: «жұмыссыз қоғамға» қарай. [Электронды ресурс]. — Кіру режимі: http://polbu.ru/kastels_informepoch/ch00_i.html.

2. Қазақстан Республикасының 2015 жылғы 23 қарашадағы No 414-V Еңбек кодексі. <https://adilet.zan.kz>

3. Работники на дому. [Электронный ресурс]. — Режим доступа: http://new_sebastopol.com/news/others/rabota-na-domu-privlekaet-vse-bolshee-chislo-soiskateley

4. Работа в Интернете фрилансером. [Электронный ресурс]. — Режим доступа: blog/onlayn-zarabotok-frilanserom/

5. Қазақстан Республикасындағы өзін-өзі жұмыспен қамтудың жаңа тенденциялары: үй жұмысынан шығармашылық қызметке дейін: <https://cyberleninka.ru/article/n/novye-trendy-v-samozanyatosti-v-respublike-kazahstan-ot-nadomnogo-truda-k-kreativnym-uslugam>

УДК 342.7

Константинова Александра Романовна

студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ИНТЕРНЕТ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Научный руководитель:

Калимбекова А.Р.

к.ю.н., ассоциированный профессор

Высшей школы права «Әділет»

Каспийского общественного университета

Аннотация

В статье рассмотрены правовые проблемы регулирования интернета в сфере здравоохранения. Автором обращается внимание на то, что с развитием интернет-технологий и доступностью онлайн-сервисов, медицинская сфера стала более доступной и эффективной, и проводится анализ плюсов и минусов при использовании интернет технологий. Обращено внимание на такие недостатки, как недостоверная информация и риск нарушения конфиденциальности, отмечая необходимость со стороны государства принимать соответствующие меры для их устранения и снижения.

Ключевые слова: телемедицина, интернет технологии, здравоохранение, информатизация, права человека, пациенты, врачи, онлайн консультации.

Константинова Александра Романовна

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

ДЕНСАУЛЫҚ САҚТАУДАҒЫ ИНТЕРНЕТ

Аңдатпа

Мақалада денсаулық сақтау саласындағы интернетті реттеудің құқықтық мәселелері қарастырылған. Автор интернет-технологиялардың дамуымен және онлайн-қызметтердің қолжетімділігімен медицина саласының қолжетімді және тиімді бола бастағанына назар аударып, интернет-технологияларды пайдаланудың оң және теріс жақтарына талдау жүргізілуде. Сенімсіз ақпарат және құпиялылықты бұзу қаупі сияқты кемшіліктерге назар аударып, оларды жою және азайту үшін мемлекет тарапынан тиісті шаралар қабылдау қажеттігін атап өтеді.

Түйінді сөздер: телемедицина, интернет-технология, денсаулық сақтау, ақпараттандыру, адам құқықтары, пациенттер, дәрігерлер, онлайн консультациялар.

Konstantinova Alexandra

1 year student of the Higher School of Law "Adilet"
Caspian Public University,
Republic of Kazakhstan, Almaty

INTERNET IN HEALTHCARE

Annotation

The article examines the legal problems of regulating the Internet in the healthcare sector. The author draws attention to the fact that with the development of Internet technologies and the availability of online services, the medical field has become more accessible and efficient, and an analysis of the pros and cons of using Internet technologies is carried out. Attention is drawn to such shortcomings as unreliable information and the risk of violation of confidentiality, noting the need for the state to take appropriate measures to eliminate and reduce them.

Keywords: telemedicine, Internet technology, healthcare, informatization, human rights, patients, doctors, online consultations.

В современном обществе процессы информатизации затрагивают практически все области профессиональной и повседневной деятельности. Современную жизнь с трудом можно представить себе без Интернета. Одной из областей, где он оказал наибольшее влияние, является здравоохранение. С развитием интернет-технологий и доступностью онлайн-сервисов, медицинская сфера стала более доступной и эффективной. В эпоху информационного общества перед медициной и системой здравоохранения открываются огромные перспективы.

Учитывая темпы роста пользователей сети Интернет в нашей стране, эта тема является особо актуальной. В данной статье мы рассмотрим, как интернет влияет на здравоохранение, его плюсы и минусы участия в этой сфере. Начнем с положительных аспектов:

1. Доступность медицинской информации:

В сети Интернет содержится большое количество разнообразной медицинской информации: симптомы и описания заболеваний, способы лечения, инструкции к лекарственным препаратам, учебные пособия, научные и ненаучные электронные издания, советы и т. д.

2. «Телемедицина» – термин, который определяется как отрасль медицины, использующая телекоммуникационные и электронные информационные (компьютерные) технологии для предоставления медицинской помощи и услуг в сфере здравоохранения в точке необходимости (в тех случаях, когда географическое расстояние является критическим фактором). В случае телемедицины Интернет рассматривается как средство связи и обмена клинической и достаточно конфиденциальной информацией между ограниченным числом участников (например, врачом и пациентом, врачами).

Возможность получать медицинскую помощь в реальном времени через интернет – это еще одно важное достижение. Телемедицина позволяет пациентам общаться с врачами удаленно, проводить консультации и получать рекомендации по лечению. Это особенно полезно для тех, кто живет в отдаленных районах или имеет ограниченную подвижность.

3. Стоит обратиться к медицинским знаниям и информации, которые в настоящее время являются открытыми для любого желающего. Информация о новейших разработках, формы непрерывного дистанционного образования и т.д. помогают специалистам постоянно совер-

шенствовать свой профессиональный уровень. Для того, чтобы узнать о новых лекарствах или способах лечения того или иного заболевания, врачу нет надобности проводить много времени в библиотеке. Всю интересующую информацию можно получить через сервисы сети Интернет. Повышать свой профессиональный уровень можно без отрыва от рабочей деятельности. В качестве примера можно привести медицинский видеопортал med-edu.ru, на котором представлены видеоматериалы по основным разделам медицинского знания.

4. Электронные медицинские записи:

Интернет также упрощает хранение и доступ к медицинским данным. Благодаря электронным медицинским записям врачи могут получить быстрый доступ к истории болезни пациента, а пациенты могут быть уверены в том, что их данные надежно хранятся и доступны в случае необходимости.

5. Интернет-аптеки и доставка лекарств:

Онлайн-аптеки стали популярным решением для заказа лекарств. Пациенты могут выбрать и приобрести нужные препараты прямо из дома, а доставка лекарств облегчает получение необходимых медикаментов, особенно для пожилых или маломобильных людей.

6. Информационные ресурсы для медицинских специалистов:

Интернет также играет важную роль в обмене информацией между медицинскими специалистами. Онлайн-платформы и форумы позволяют врачам и другим медицинским работникам обсуждать клинические случаи, делиться опытом и получать новейшие медицинские знания.

Хотя взаимодействие интернета со сферой здравоохранения имеет множество преимуществ, есть и некоторые минусы, которые следует учитывать:

1. Недостоверная информация:

Интернет предоставляет множество информации о здоровье, но не всегда эта информация является достоверной и проверенной. Пациенты могут столкнуться с неверной или неправильной информацией, что может привести к ошибочным самодиагнозам или самолечению.

2. Недостаток конфиденциальности:

При обмене медицинскими данными через интернет существует риск нарушения конфиденциальности. Несанкционированный доступ к электронным медицинским записям или персональным данным пациента может привести к утечке информации или злоупотреблению.

3. Ограничения технологической инфраструктуры:

Некоторые районы или страны могут испытывать недостаток доступа к надежному интернет-соединению или технологической инфра-

структуре. Это может препятствовать полноценному использованию онлайн-сервисов и телемедицины.

4. Отсутствие личного взаимодействия:

Виртуальное взаимодействие с врачом через интернет не всегда может заменить личное посещение клиники. Некоторые заболевания или симптомы могут требовать физического осмотра или дополнительных медицинских исследований.

5. Зависимость от технологии:

Развитие интернета в здравоохранении создает зависимость от технологии. В случае сбоев в сети или проблем с оборудованием может возникнуть проблема с получением необходимой медицинской помощи или доступом к важной информации.

Важно понимать, что хотя интернет имеет свои недостатки, они могут быть устранены или снижены с помощью правильной регулировки, обучения пациентов и обеспечения безопасности данных.

В целом, интернет вносит значительный вклад в сферу здравоохранения, улучшая доступность медицинской помощи, повышая информированность пациентов и облегчая процессы хранения и обмена медицинскими данными. Однако следует учитывать некоторые недостатки, такие, как недостоверная информация и риск нарушения конфиденциальности, и предпринимать соответствующие меры для их устранения и снижения.

УДК 342

Кумарбек Айзада

студентка 2 курса Школы права и государственного
управления по программе “Юриспруденция”

Университет Нархоз

Республика Казахстан, г. Алматы

**УРОВЕНЬ ИНФОРМИРОВАННОСТИ НАСЕЛЕНИЯ РК
ОБ ЭЛЕКТРОННЫХ И МОБИЛЬНЫХ ПОРТАЛАХ
ПО ОКАЗАНИЮ ГОСУДАРСТВЕННЫХ УСЛУГ**

Научный руководитель:

Сагинаев М.Е.,

М.Ю.Н.

Аннотация

Казахстан стремительно адаптируется под реалии мирового информационного пространства, когда потребность в быстрой доступности информации становятся неотъемлемой частью нашей повседневной жизни. Этот сдвиг ориентира в сторону цифровых технологий имеет положительные перспективы во всех аспектов жизни общества, включая и взаимодействия между государством и гражданами. В данной работе был проведен анализ действий государства по поддержке и популяризации цифровых инструментов по оказанию государственных услуг, выявлена степень информированности населения Республики Казахстан о государственных услугах, даны рекомендации по повышению правовой образованности гражданского общества.

Ключевые слова: электронное правительство, информационное пространство, цифровые технологии, цифровые инструменты, государство, граждане, государственные услуги, электронная платформа.

Құмарбек Айзада

Нархоз университеті

Құқық және мемлекеттік басқару мектебінің

«Юриспруденция» бағдарламасы бойынша

2 курс студенті

«Қазақстан Республикасы, Алматы қ.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ХАЛҚЫНЫҢ МЕМЛЕКЕТТІК ҚЫЗМЕТТЕРДІ КӨРСЕТУДІҢ ЭЛЕКТРОНДЫҚ ЖӘНЕ МОБИЛЬДІ ПОРТАЛДАРЫ ТУРАЛЫ ХАБАРДАР БОЛУ ДЕҢГЕЙІ

Аңдатпа

Ақпаратқа жылдам қол жеткізу қажеттілігі күнделікті өміріміздің ажырамас бөлігіне айналған кезде Қазақстан жаһандық ақпараттық кеңістіктің шындығына жылдам бейімделуде. Цифрлық технологияларға бағдарланудың бұл ауысуы қоғамның барлық аспектілерінде, соның ішінде мемлекет пен азаматтардың өзара әрекеттесуінде оң перспективаларға ие. Бұл жұмыста мемлекеттік қызметтерді көрсетудің

цифрлық құралдарын қолдау және танымал ету бойынша мемлекеттің іс-әрекетіне талдау жүргізіліп, Қазақстан Республикасы халқының мемлекеттік қызметтер туралы хабардар болу дәрежесі анықталды, сондай-ақ мемлекеттік қызмет көрсетуді жақсарту бойынша ұсыныстар берілді. азаматтық қоғамды құқықтық тәрбиелеу.

Түйінді сөздер: электронды үкімет, ақпараттық кеңістік, цифрлық технологиялар, цифрлық құралдар, мемлекет, азаматтар, мемлекеттік қызметтер, электронды платформа.

Kumarbek Aizada

2nd year student

Schools of Law and Government
in the “Jurisprudence” program

Narxoz University

Republic of Kazakhstan, Almaty

LEVEL OF AWARENESS OF THE POPULATION OF THE REPUBLIC OF KAZAKHSTAN ABOUT ELECTRONIC AND MOBILE PORTALS FOR THE PROVISION OF PUBLIC SERVICES

Annotation

Kazakhstan is rapidly adapting to the realities of the global information space, when the need for rapid availability of information becomes an integral part of our daily life. This shift in orientation towards digital technologies has positive prospects in all aspects of society, including interactions between the state and citizens. In this work, an analysis of the state's actions to support and popularize digital tools for the provision of public services was carried out, the degree of awareness of the population of the Republic of Kazakhstan about public services was identified, and recommendations were given to improve the legal education of civil society.

Keywords: e-government, information space, digital technologies, digital tools, state, citizens, public services, electronic platform.

ВВЕДЕНИЕ

С момента создания идеи о концепции электронного правительства Казахстан стремится к модели публичного управления, которая обеспечивает не только открытость в принятии решений административными органами, но также оптимизирует весь процесс работы государственных служб. Конечной целью любой государственной политики в области

электронного правительства является создание устойчивой и эффективной системы государственных услуг, обеспечивающей максимальное удобство и доступность для всех граждан. Потому низкий уровень информированности населения Республики Казахстан об электронных и мобильных государственных услугах становится немало важной задачей для правительства. В данной научной работе мы рассмотрим основные аспекты этой проблемы и проанализируем реальную ситуацию в РК. Основной целью исследования является определение уровня информированности населения РК об электронных и мобильных государственных услугах и выработка рекомендаций по повышению этого уровня для достижения большей доступности и удобства государственных услуг для граждан.

Задачи проекта:

- выявление уровня удовлетворенности населения РК по оказанным государственным услугам в электронном и мобильном формате;
- анализ уровня информированности населения РК об электронных и мобильных услугах;
- выполнение содержательного анализа исследований ООН: «Электронное правительство 2022», общественного мониторинга оценки качества оказания государственных услуг, проведенный 2022 г. исследовательским центром «Талап»;
- проведение мониторинга СМИ об общем количестве упоминаний ключевых понятий;
- выработка практических рекомендаций по улучшению уровня информированности граждан.

Методы исследования

- 1) Проведение кабинетных исследований (desk research), основанные на анализе финансовых, бюджетных отчетов МЦРИАП, отчете о мониторинге оценки качества оказания государственных услуг, проведенный 2022 г. исследовательским центром «Талап» и исследований ООН: «Электронное правительство 2022»;
- 2) Массовый опрос путем онлайн анкетирования, предназначен для выявления удовлетворенности, информированности и ключевых недостатков электронных и мобильных платформ по оказанию государственных услуг;
- 3) Мониторинг материалов СМИ, которые индексируются новостной службой системы Google.

В ходе последнего опроса, проведенного при помощи Google Forms было обнаружено, что более 61,9% респондентов столкнулись с бюрократией при получении услуг от государственных организаций. Это подчеркивает проблемы, с которыми сталкиваются граждане при доступе к государственным услугам в Казахстане, а также необходимость повышения эффективности и прозрачности предоставления услуг.

Одной из основных проблем, с которой сталкиваются граждане при доступе к государственным услугам онлайн, является некорректная работа сайтов и платформ. Многие граждане сообщают, что на веб-сайтах сложно ориентироваться, а предоставляемая информация часто неясна или неполна, что может затруднить гражданам выполнение необходимых шагов для доступа к требуемым услугам.

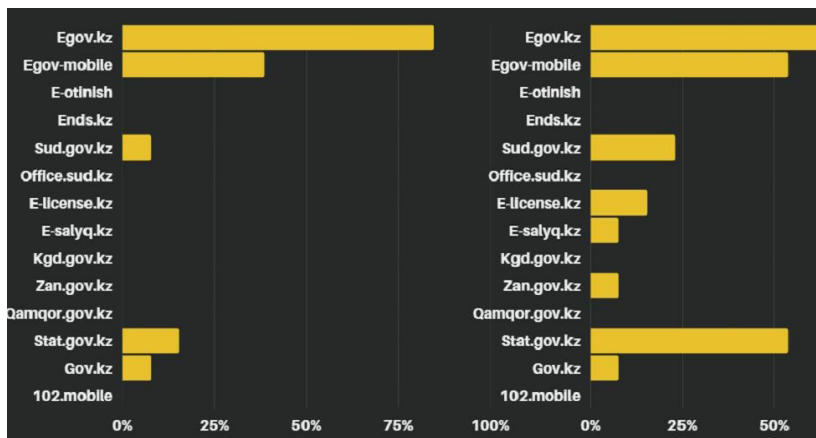


Рисунок-1. Слева % использованных, справа % знакомых электронных платформ.

Также стоит отметить низкую осведомленность населения РК о возможных электронных и мобильных платформах по оказанию государственных услуг. К примеру, из 14 предложенных позиций анкетируемые были знакомы с 8 платформами и имели опыт пользования лишь в 5 (рисунок-1). Главным источником информации, с помощью которых опрашиваемые узнавали отой или иной платформе оказались знакомые респондентов (42.9%), социальные сети (14.3%) и наружная реклама (9.5%).

Для установки связи между распространением информации об электронных услугах и их использованием был проведен анализ материалов СМИ, которые индексируются новостной службой системы Google. Исследование охватывает период с 2004 по 2023 гг., страны-Россия, Дания, США и Великобритания и их позиции в рейтинге ООН по развитию электронного правительства за 2022г.. Решение начать мониторинг с 2004 г. обусловлено тем, что в этом году был утвержден Указ Президента Республики Казахстан «О государственной программе формирования «электронного правительства» в Республике Казахстан на 2005-2007 годы»[2], которая позже стало основанием для формирования платформы egov.kz. Как видно на рисунке-2 количество публикаций в казахстанских СМИ за 2004–2023 гг. в разы меньше количество публикаций в СМИ других государств.

Рисунок-2.Общее количество упоминаний понятия «электронное правительство» в СМИ в период с 2004 по 2023 г.

Страны	Казахстан	Россия	Дания	США	Великобритания
Количество упоминаний в СМИ	6990	20800	4 871 670	49 000 000	52 200 000
Место в рейтинге ООН	28	42	1	10	11
Составлено автором на основе источника [7]					

Дополнительно о позициях Казахстана в цифровом пространстве: Казахстан занял 7 место среди стран Азии, 1 среди развивающихся стран, не имеющих выхода к морю и 28 место в мире по индексу развития электронного правительства (EGDI). Также город Алматы занял 26 место среди городов в категории с очень высоким LOSI. LOSI или индекс развития местного электронного правительства включает 86 показателей, относящихся к пяти критериям: институциональная структура (8), предоставление контента (25), предоставление услуг (18), участие и вовлеченность (17), технология (18) [7].

Согласно итогам проведенного опроса о наружной рекламы электронных платформ, чаще всего рекламировалась или упоминалась в рекламе мобильное приложение e-salyq (e-salyq-78%, e-otinish-9.8%, enis.

kz-5.3%) [6]. Мы попробовали рассчитать стоимость наружной рекламы в 7 станциях и 20 вагонах метро города Алматы и проанализировать отчет об освоении бюджета МЦРИАП за 2022 год (рисунок-3).

Результатом подобного финансирования можно считать возросшее почти в 4 раза количество пользователей: по состоянию на 5 февраля 2021 г.- 265 тысяч пользователей, на 1 марта 2022 года свыше 1 миллиона пользователей [9].

Рисунок-3. Таблица расчета суммы удельного веса наружной рекламы по отношению к фактическим затратам МЦРИАП

Наименование рекламы	Стоимость, месяц/тенге	Сумма за период от 01/01/2021 по 01/01/2022, в тг	Удельный вес от фактической* суммы бюджета- цели 2.1.**, %
Баннеры в 7 станциях метро	1 646 400	19 756 800	21,15%
Мониторы в 7 станциях метро	506 086	6 073 032	6,50%
Мониторы в 20 вагонах метро	605 072	7 260 864	7,77%
Итого	2 757 558	33 090 696	35%
Составлено автором на основе источников [9,10]			

**фактическая освоенная сумма бюджета на 2022 год-93 420 704,2 тенге.*

** *Стратегическое направление 2. «Совершенствование процессов оказания государственных услуг, развитие отрасли связи и повышение уровня информационной безопасности». Цель 2.1*

«Повышение качества и доступности государственных услуг»

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Обеспечить удобство и доступность портала. Государственный портал должен быть удобным в использовании и доступным для всех пользователей, включая людей с ограниченными возможностями. Портал должен быть простым и интуитивно понятным, с четкими инструкциями и руководствами. Кроме того, портал должен быть доступен на всех устройствах, в том числе и на мобильных устройствах.

Повышение прозрачности и открытости. Государственный портал должен быть прозрачными открытым для всех пользователей. Это мо-

жет быть достигнуто путем опубликования полной информации обо всех услугах и процедурах, а также предоставлением отчетов о деятельности портала. На данный момент полностью контролируются лишь дела, поступившие в районные, областные прокуратуры и в Генеральную прокуратуру ЕИАС «Қадағалау» [4].

Развитие функциональности порталов. Пользователи должны иметь возможность выполнять все необходимые процедуры в «едином окне». Например, для тех, кто предпочитает использовать онлайн-оплату, портал должен предоставлять возможность оплаты счетов и услуг.

Разработка и поддержка системы обратной связи. Пользователи должны иметь возможность связаться с органами государственной власти в случае возникновения вопросов или проблем. Система обратной связи должна быть быстрой и эффективной, чтобы пользователи могли получить ответы на свои вопросы в кратчайшие сроки.

Развитие Государственно-частного партнерства. Повышение качества оказываемых государственных услуг, разработка новых и поддержка существующих электронных порталов посредством делегирования обязанностей в рамках ГЧП. Отличным примером подобной интеграции служит партнерство государства и Kaspi банка [3].

Улучшение инфраструктур ИКТ. Решение проблем с проведением оптоволоконных и магистральных кабелей. Казахстан развивается в положительной динамике по обеспечению и поддержке ИКТ. К примеру, 2018 году только 100 000 человек, проживающих примерно в 55 сельских населенных пунктах РК, имели доступ к Интернету через оптоволоконный кабель; к 2020 году правительство протянуло оптоволоконные линии в 741 населенный пункт, и число обслуживаемых возросло до 800 000 человек [7].

Развитие информационных каналов правительства. В целях развития взаимодействий государства и граждан, а также для дальнейшей модификации электронных и мобильных порталов рекомендуется развитие популяризации, посредством рекламы, ознакомительных сессий и консультаций.

Обозначения и сокращения

РК	Республика Казахстан
ООН	Организация Объединённых Наций

СМИ	Средства массовой информации
МЦРИАП	Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана
LOSI	Индекс развития местного электронного правительства
EGDI	Индекс развития электронного правительства
ИКТ	Информационно-коммуникационные технологии

Список использованных источников:

1. Багдат Мусин поздравил коллектив АО «Национальные информационные технологии» с 17-летием работы портала «eGov.kz»: <https://www.gov.kz/memleket/entities/mdai/press/news/details/536108?lang=ru>
2. Электронное правительство Республики Казахстан – Egov <https://egov.kz/cms/ru/information/about/help-elektronnoe-pravitelstvo>
3. Мы очень гордимся тем, что Kaspі.kz создана в Казахстане <https://tengrinews.kz/money/mihail-lomtadze-myi-ochen-gordimsya-tem-kaspikz-sozdana-457571/>
4. Контроль за качественным рассмотрением обращений в кадагалау <http://prs.kz/press/16404/Kontrol-za-kachestvennim-rassmotreniem-obraschenij-v-organah-prokuraturi/>
5. КГД запустил приложение для оплаты налогов без процентов <https://otyrary.kz/2021/02/kgd-zapustilo-prilozhenie-dlya-oplaty-nalogo-Bez-protsentov/>
6. Онлайн анкетирование https://docs.google.com/forms/d/e/1FAIpQLSeWb0_FThwzdZS8siQoIVDrZ8C-hj1G9aaqZyZx42e9tPlmhtw/viewform
7. Исследования ООН: «Электронное правительство 2022» [file:///C:/Users/student/Downloads/UN%20E-Government%20Survey%202022%20-%20Russian%20Web%20Version%20\(1\).pdf](file:///C:/Users/student/Downloads/UN%20E-Government%20Survey%202022%20-%20Russian%20Web%20Version%20(1).pdf)
8. Отчёт о мониторинге оценки качества оказания государственных услуг, проведенный 2022г. исследовательским центром «Талап» https://sud.gov.kz/sites/default/files/pagefiles/om_2022_otchet_rus.pdf
9. Бюджетные средства, направленные на осуществление деятельности Министерства за 2022 год <https://www.gov.kz/memleket/entities/mdai/documents/details/431935?lang=ru>

10. Реклама в метро Алматы <https://ba-company.kz/portfolio/portfolio/metro/more.html>

ӘОЖ 347.78

Қалжан Көркемжан Өркенқызы
Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

**ИНТЕРНЕТ:
МЕМЛЕКЕТ БӘРІМІЗДІ БАҚЫЛАУЫ КЕРЕК ПЕ?**

Ғылыми жетекші:

Қасымбек А.О.

з.ғ.м., Каспий қоғамдық университеті
«Әділет» Жоғары құқық
мектебінің сеньор-лекторы

Аңдатпа

Мақала мемлекет интернетте құқық бұзушылармен қалай күреседі, мемлекет пен қоғамда заңдылықты қамтамасыз етеді деген сұрақтарға арналған. Автор Интернетте мемлекеттік және қоғамдық бақылаудың қажеттілігі туралы проблемалық мәселеге назар аударады. Интернеттегі бақылаудың ата-аналық, корпоративтік және мемлекеттік сияқты түрлері қарастырылады. Интернет желісін мемлекеттік бақылауды жүзеге асыру бойынша әртүрлі елдердің тәжірибесіне салыстырмалы талдау жасалды. Адам құқықтарын қамтамасыз ету және қорғау саласындағы, атап айтқанда адамның сөз бостандығына, баспасөз және БАҚ бостандығына қатысты халықаралық актілерге, және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы Қазақстан Республикасының заңнамасына назар аударылады.

Түйінді сөздер: мемлекет, құқықтық реттеу, құқықтық бақылау, интернет

Калжан Коркемжан Оркеновна
Студентка 1 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

**ИНТЕРНЕТ:
ДОЛЖНО ЛИ ГОСУДАРСТВО НАС КОНТРОЛИРОВАТЬ?**

Аннотация

Статья посвящена вопросам касательно того, как государство ведет борьбу с правонарушителями в интернете, обеспечивая режим законности в государстве и обществе. Автор обращает внимание на проблемный вопрос о необходимости государственного и общественного контроля в сети Интернет. Рассмотрены виды контроля в интернете, как родительский, корпоративный и государственный. Проведен сравнительный анализ опыта разных стран в осуществлении государственного контроля интернет сети. Обращено внимание на международные акты в сфере обеспечения и защиты прав человека, в особенности на право человека на свободу слова, свободу печати и СМИ и законодательство Республики Казахстан в сфере обеспечения информационной безопасности.

Ключевые слова: сеть Интернет, правовое регулирование, государство, правовой контроль

Kalzhan Korkemzhan
1 year student of the Higher School of Law “Adilet”
Caspian Public University,
Republic of Kazakhstan, Almaty

**THE INTERNET:
SHOULD THE STATE CONTROL US?**

Annotation

The article is devoted to questions regarding how the state combats offenders on the Internet, ensuring the rule of law in the state and society. The author draws attention to the problematic issue of the need for state and public control on the Internet. The types of control on the Internet, such as parental, corporate and state, are considered. A comparative analysis of

the experience of different countries in implementing state control of the Internet network was carried out. Attention is drawn to international acts in the field of ensuring and protecting human rights, in particular to the human right to freedom of speech, freedom of the press and media and the legislation of the Republic of Kazakhstan in the field of ensuring information security.

Keywords: Internet, legal regulation, state, legal control

Күні бүгінге дейін Интернет адам өмірінің барлық салаларына әсер етеді, отбасындағы қарым қатынастан бастап, әртүрлі іскерлік кездесулерге және жұмыс бойынша келіссөздерге дейін. Бұл ақпараттық технологияның ең үлкен жетістігі. Интернет физикалық қызмет ететін ғаламдық кеңістікті құрайды, көптеген деректер жүйелерінің негізі.

Бұл үлкен күш бақылауда болуы қажет, өйткені кез-келген ақпараттың бақылаусыз таралуы қоғамдағы хаосқа әкеледі.

Ал желіні бақылауда ұстаудың келесі түрлері кездеседі: тұрмыстық, корпоративтік және мемлекеттік.

Тұрмыстық бақылауды әдетте ата-аналар балаларының тұрақсыз психикасына нұқсан келтірмеу, оны теріс, әдепсіз мазмұндағы ақпараттан қорғау үшін белгілейді.

Корпоративтік бақылауды негізінен ірі компаниялар белгілейді: «Одноклассники», «mail.ru», «Вконтакте», «Facebook» және т. б. осы сияқты әлеуметтік желілерді құлыптау үшін, тиісті мекенжайларға кіруді бұғаттау арқылы корпоративтік бақылау орнатады.

Мемлекеттік бақылау - бұл ақпараттың ең жоғары деңгейі, сонымен қатар белгілі бір деректерді тарататын компаниялар мен блогерлерге әсер ету арқылы бүкіл халықтардың дүниетанымын қалыптастыру. Тағы бір нұсқа – желі ресурстарының көпшілігін бақылауда ұстау, қажетсіз ресурстарды жабу және барлық трафикті бақылау.

Ең қатаң интернет-фильтр, яғни интернет бақылауы Қытайда орнатылған. ҚХР үкіметі жергілікті тұрғындарға шетелдік сайттарға шектеу қойып, шетелдіктерге интернетке тиым салады. Шетелдіктер интернетті белгілі бір құжаттар пакетінің көрсете отырып, тек интернет-кафеде пайдалана алады.

Веб-беттер мемлекеттік қауіпсіздікке байланысты «қара тізімі»-нің мекен-жайлары және түйінді сөздері бойынша сүзгіден өтеді. Осы әрекеттерді жүзеге асыратын «Ұлы Қытай файерволл»-ы ол «күдікті мазмұндағы» сайттардың IP мекенжайларын бұғаттайды.

Қытай үкіметінің бұйрығымен провайдерлер мұндай сайттарды бұғаттаумен айналысады (мысалы, жаңалықтар сайты, би-би-

си). Microsoft, Google және Yahoo секілді ақпараттық желілер үмітсіз жағдайға тап болды, сондықтан іздеу нәтижелерін заң талаптарына сәйкес өндейді. Жергілікті сайттар өнеркәсіп және ақпараттық технологиялар министрлігінде тіркеуден өтеді, бұл заңсыз сайттың авторын анықтауға мүмкіндік береді.

Бірақ мұндай тыйым салу халықаралық құқық тұрғысынан заңды ма?

Әлемнің барлық дерлік мемлекеттері ратификациялаған Азаматтық және саяси құқықтар туралы Халықаралық пактіде әр адамның сөз бостандығына құқығы бар, ол адамның өз ойын еркін білдіре алатындығында көрінеді, оған сөз бостандығы кіреді, ауызша және жазбаша түрде (Баспасөз және бұқаралық ақпарат құралдарының еркіндігі). Бұл мүмкіндік құқықтар мен негізгі бостандықтар туралы Еуропалық Конвенцияда және көптеген елдерде айтылған. Жалпыға бірдей танылған қағидаттар және халықаралық құқықпен, сөздер шарттарға сәйкес келуі керек:

–біріншіден, заңға сәйкес болуы керек;

–екіншіден, оларды шарттау заңды мақсат және осы мақсатқа жету үшін талаптарға сәйкестік қажет.

Мақсаттар арасында ұлттық қауіпсіздікті, тәртіпті, беделді қорғау, тұлғалар, авторлық құқық, және мораль. Демек, мемлекет заңдарды белгіленген сәттерден бастап шектеулермен, саяси билікті ұйымдастыру сол заңдарға сәйкес етеді, әсіресе басты назарда бостандық.

Ақпараттық қауіпсіздікті құқықтық қамтамасыз ететін конституциялық заңдар, билік органдарының нормативтік құқықтық актілері және ҚР заңға тәуелді нормативтік актілері.

Қазақстан Республикасының Конституциясының 20-бабының 1- 2 тармағында: сөз бен шығармашылық еркіндігіне кепілдік берілетіні, цензураға тыйым салынатыны, әркімнің заң жүзінде тиым салынбаған ақпаратты еркін алуға және таратуға құқылы делінген. Ал 3- бабында: Республиканың конституциялық құрылысын күштеп өзгертуді, оның тұтастығын бұзуды, мемлекет қауіпсіздігіне нұқсан келтіруді, соғысты, әлеуметтік, нәсілдік, ұлттық, діни, тектік-топтық және рулық астамшылықты, сондай-ақ қатыгездік пен зорлық- зомбылыққа бас ұруды насихаттауға немесе үгіттеуге жол берілмейді.

Осы орайда заң тұрғысан әлеуметтік желідегі сайттардың барлығының дұрыс иә болмаса бұрыстығын қадағалау кімнің қолында?

2022 жылы болған Қаңтар оқиғасын ескеретін болсақ, халықтың бейбіт шеруін өзінің арам пиғылына пайдаланған экстремистік ұйымның өз мақсаттарына жетіп, қоғамызда вандализм пайда болуына алып

келді. Дер кезінде қабылданған Президент жарлығымен құқық қорғау қызметкерлердің жұмысы арқылы бәрі басылды. Дегенмен елімізде цифрлыққауіпсіздік пен тексерістің ақсандап тұрғанына көзіміз жетті. Осындай оқиғаның қайталанбау мақсатында мемлекет интернетте бақылау орнатуы қажет.

Желідегі мемлекеттік реттеу мен бостандықты қамтамасыз ету арасындағы тепе-теңдікті сақтау өте маңызды. Барлығы мүмкіндігінше пропорционалды және әділ түрде өтуі қажет. Әйтпесе, біз басқа деңгейдегі және сипаттағы проблеманы аламыз.

Интернет желісі ешкімнің жеке басқаруында емес, мемлекеттер және оның ресурстары көптеген коммерциялық ұйымдардың арасында бөлінеді, бұл цензураның түрін өте күрделіетеді. Ол белгілі бір шараларды бір уақытта қолдану арқылы ғана жүзеге асады:

- Желілік коммуникацияларды басқаруды мемлекетінің қолында шоғырландыру немесе нақты қысым тұтқалары (мұндай тұтқалар заңнамалық нормалар болуы мүмкін, БАҚ қызметінің шектеулеріне және белгілі бір түрдегі жалпы мемлекеттегі ақпарат айналымына қатысты) арқылы желідегі заңнамалық шеқарадан асып кеткен компания, сайттарды бақылауда ұстау.

- Бақыланатын нақты ресурстарға қол жеткізу мүмкіндігін белгілеу, компаниялар сайттардың мазмұнын тексеруге дайын екендігіне байланысты, ақпаратты және хабарламаларды жою немесе өңдеу.

- Желі арасында мороторинг өткізу.

Алайда желіде цензураны жеңу мақсатында анонимді желілер мен прокси-серверлерді пайдалану әбден мүмкін.

Осыдан кейін елімізде жақсы істейтін баламалар бар ма? деген сұрақ пайда болады. Әрине ия. Мемлекет біздің оқығанымызды, көргенімізді және тыңдағанымызды интернетте бақылауға тырысады. Бұл жаңа заң жобалары пайдаланушылар арасында шу мен наразылық тудырады. Желідегі адамның жеке өмірге деген құқығы мемлекет тарапынан қадағалауы қазіргі тандағы өзекті мәселе болып отыр.

Қорытындылай келе, мемлекет пен интернет желісінің реттеу арасында желідегі пайдаланушылардың еркіндігі бар. Ол мемлекет ел қауіпсіздігі үшін бар күш-жігерін жұмсап жатқанда, халық өзінің жеке өміріне қол сұғылмайтына көз жеткізгенде пайда болады.

Пайдаланылған қайнар көздерінің тізімі:

1. https://adilet.zan.kz/kaz/docs/K950001000_
2. Қаңтар оқиғасы бойынша дереккөз <https://www.azattyq.org/a/kazakhstan-authorities-step-up-repressive-measures-hugh-williamson-interview/32714081.html>
3. Галушкин А.А. К понятию «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. – 2015. – № 2.
4. Декларация о свободе обмена информацией в Интернете (Страсбург, 28 мая 2003 года) (Принята Комитетом Министров на 840-м заседании заместителей министров) / https://medialaw.asia/document/2358#google_vignette
5. Европейская декларация о правах человека и верховенстве права в информационном обществе/ <https://search.rsl.ru/ru/record/01003368219>

ӘОЖ 343.9**Мусаева Камила**

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,

Қазақстан Республикасы, Алматы қ.

**КИБЕРҚЫЛМЫС ЖӘНЕ КИБЕР СОҒЫС, ЖЕКЕ ДЕРЕКТЕРДІ
ҰРЛАУ, ЖЕКЕ ДЕРЕКТЕРДІ ҚАУІПСІЗ САҚТАУ МӘСЕЛЕЛЕРІ****Аңдатпа**

Мақала ішінде кибер қылмыстылық, киберсоғыс түсініктері қарастырылады, жеке деректерін ұрлау мәселесі зерттеледі, сонымен бірге жеке деректерін қауіпсіз сақтау тәсілдеріне назар аударылады. Киберқылмыстың өзектілігі дамудың жылдам қарқынына, әлеуметтік қауіптіліктің жоғарылауына және жоғары латенттікке байланысты бұл құбылыстың барған сайын кең таралып, барлық жерде кездесетін қауіп сипатына ие болуымен түсіндіріледі. Автор киберқылмыс құбылысы қазақстандық және шетелдік ғалымдардың көптеген зерттеулерінің нысаны болып табылатындағын атап өтіп, алайда бүгінгі күні оны толық зерттелген деп атауға болмайтынына назар аударады.

Түйінді сөздер: киберқылмыс, ақпарат, динамика, хакерлердің белсенділігі, ақпараттың ағуы, алаяқтық, Интернет, жеке деректер.

Мусаева Камила

студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

**КИБЕРПРЕСТУПНОСТЬ И КИБЕРВОЙНА, КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ,
ВОПРОСЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Аннотация

В статье рассматриваются понятия киберпреступность, кибервойна, изучаются проблемы кражи персональных данных, одновременно уделяется внимание способам обеспечения безопасности персональных данных. Актуальность киберпреступности объясняется тем, что в связи с быстрыми темпами развития, повышенной социальной опасностью и высокой латентностью это явление приобретает все большее распространение и носит характер повсеместной угрозы. Автор обращает внимание на то, что феномен киберпреступности является предметом многих исследований казахстанских и зарубежных учёных, однако отмечает, что на сегодняшний день его нельзя назвать полностью изученным.

Ключевые слова: киберпреступность, информация, динамика, хакерская деятельность, утечка информации, мошенничество, Интернет, персональные данные.

Musaeva Kamila

1 year student of the Higher School of Law “Adilet”

Caspian Public University,

Republic of Kazakhstan, Almaty

**CYBERCRIME AND CYBERWAR, PERSONAL DATA THEFT,
PERSONAL DATA SECURITY ISSUES**

Annotation

In the article, the concepts of cybercrime, cyberwar are considered, the problem of personal data theft is studied, and at the same time, attention is paid to ways of keeping personal data safe. The relevance of cybercrime is

explained by the fact that due to the rapid pace of development, increased social danger and high latency, this phenomenon is becoming more and more widespread and has the character of a ubiquitous threat. The phenomenon of cybercrime is the subject of many studies by Kazakh and foreign scientists, but today it cannot be called fully studied.

Keywords: cybercrime, information, dynamics, hacker activity, information leakage, fraud, Internet, personal data.

Әлеуметтік тәжірибеде киберқылмысты екі түрге бөлуге болады: әлеуметтік инженерия және вирустық бағдарламалар. Бірінші түрі көбінесе қажетті ақпаратты алу үшін жеке тұлғаларды манипуляциялаумен анықталады, ол адамға телефон немесе компьютер шабуылынан тұрады. Қылмыскерлер білікті психолог бола алады және адамдарды өздерінің достары екеніне, маңызды және жеке ақпаратпен сенуге болатындығына сендіру үшін олардың ерекшеліктерін пайдалана алады. Бұл әдіс «фишинг» деп аталады, яғни тәжірибесіз және сауатсыз пайдаланушылардан құпия ақпаратты алу [1].

Вирустық бағдарламалар киберқылмыстың күрделі ортасы болып табылады, ол хакерлерден, ең алдымен, АТ саласында жоғары құзыреттілік пен терең білімді талап етеді.

Киберқылмыстың түрлері:

Қаржылық қылмыстар – экономикалық және қаржылық қатынастар саласындағы қылмыстар;

Фишинг – психологиялық қысым арқылы құпия деректерді алу;

Pharming – пайдаланушыларды зиянды сайттарға қайта бағыттау;

Киберпорнография - кәмелетке толмаған адамдар қатысатын бейнелер мен басқа материалдарды орналастыратын порнографиялық сайттар;

Кибер есірткі трафигі – есірткінің заңсыз айналымы мақсатындағы хабарламаларды кодтау;

Кибертерроризм – киберкеңістіктегі терроризм (Мысалы: Интернетте болашақ лаңкестік актілер туралы ақпаратты тарату);

Онлайн құмар ойындар - пайдаланушылардың ақшасын жылыстатуға арналған заңсыз ойын-сауық сайттары;

Киберталкинг – виртуалды кеңістікте белгілі бір тұлғаларды құдалау;

Кибербуллинг – бұл әлеуметтік желілер мен басқа да бағдарламалар арқылы адамның қадір-қасиетін қорлау.

Бүгінгі таңда құпия деректердің төңірегінде көптеген сұрақтар мен мәселелер туындайды: саяси және мемлекеттік мүдделерде, жосықсыз

бәсекелестік артықшылық ретінде пайдалану; дербес деректерді қорғау және пайдалану саласындағы заңнамадағы проблемалар; жұртшылыққа үнемі ағып тұрады. Бұл мәселе тұтынушылар өмірінің өзекті бөлігіне айналуға және бірде-бір мекеме немесе мемлекет ықтимал кибершабуылдан қорғалмаған [2].

Электрондық ортада жасалған қылмыстармен күрес келесі аспектілермен қиындады: біріншіден, қоғам жаңа форматтағы құқық бұзушылармен бетпе-бет келуде; екіншіден, бұл қылмыстарды ашу үшін арнайы білімі мен тәжірибесі бар мамандандырылған қызметкерлер қажет; үшіншіден, киберқылмысты бақылау және онымен жеке мемлекет деңгейінде күресу іс жүзінде мүмкін емес [3, б. 376].

Қазіргі уақытта Қазақстанда және басқа елдерде көптеген ғылыми басылымдар компьютерлік қылмыспен күресуге және киберқауіпсіздікті қамтамасыз етуге арналған. Университеттер киберқауіпсіздік мәселелерін қарастыратын жаңа оқу пәндерін енгізуде. Киберқылмыстарды зерттеуді ғылыми қоғамдастықтың әртүрлі салаларының өкілдері жүргізеді, бірақ ең алдымен IT мамандары мен заңгерлер айналысады. Бұл үздіксіз дамып келе жатқан құбылыстың мазмұнын түсінуге және сипаттауға барынша белсенді түрде тырысатындар.

Киберқылмыс туралы ақпарат тез және әсерлі түрде жинақталып жатқанына қарамастан, заң ғылымы бұл құбылыстың біртұтас толық анықтамасын әлі жасаған жоқ. Мұны әртүрлі ғалымдар берген киберқылмыс тұжырымдамаларын талдау арқылы тексеруге болады.

Әрбір дерлік мемлекет коммерциялық және жеке ақпаратқа, сондай-ақ мемлекеттік деректерді қорғауға қатысты деректерді қорғау және қауіпсіздік мәселелерімен бетпе-бет келеді. Дүние жүзінде киберқылмыстардың саны жыл сайын артып келеді.

Қазақстан ТМД елдері арасында цифрландыру бойынша көшбасшылардың бірі ретінде киберқауіптерге де бейім.

Ел басшылығы мезгіл-мезгіл киберқылмысқа қарсы күрестің өзектілігін атап өтеді.

Мысалы, Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі жүргізген социологиялық зерттеу халықтың ақпараттық қауіпсіздік қатерлері туралы хабардар болу пайызы 2018 жылы 62,9%, 2019 жылы болғанын көрсетті. – 73,5%, 2020 ж – 78% және 2021 ж – 75%.

Осылайша, 2021 жылы азаматтардың хабардар болу деңгейінің 3%-ға төмендеуі байқалады, бұған пандемия, онлайн қосымшаларды пайдалану, қашықтықтан жұмыс істеу және оқыту сияқты факторлар ықпал етті.

Соңғы 5 жылдағы отандық құқықтық ақпаратты талдау киберқылмыспен күресті ұйымдастырудағы кейбір проблемаларды анықтады.

Интернет-алаяқтықтың тіркелуінің өсуін байқай отырып, бізбір жағынан, бұл әрекеттердің алдын алу және алдын алу бойынша қабылданған шаралар жеткіліксіз және тиімсіз деп қорытынды жасауға болады; екінші жағынан, азаматтардың сенімсіздігі мен құқықтық сауатсыздығы туралы, жалған мобильді қосымшалардың бақылаусыз таралуы, қаржылық интернет пирамидаларының ашық жарнамасы, интернет-төлем платформаларын киберқорғау бойынша қолданыстағы шаралардың тиімсіздігі, киберқауіпсіздік мамандарының жетіспеушілігі және т.б.

Қарастырылып отырған барлық әрекеттер бойынша тіркеу көрсеткіштерімен қатар, киберқылмыстардың динамикасын сипаттайтын тағы бір элемент – ашу көрсеткіші болып табылады.

Қазақстан Республикасында бұл көрсеткіш Интернет желісіндегі алаяқтық істері бойынша 31,65% және тарау бойынша қылмыстық құқық бұзушылықтарды жасау негізінде қозғалған барлық қылмыстық істер бойынша 72,7% құрайды. Бұл көрсеткіш сотқа жіберілген қылмыстық істердің және өндіріс тоқтатылған қылмыстық істердің пайызын құрайды. Айта кету керек, деректерді талдау және пайыздық көрсеткішті есептеу кезінде біз белгілі бір кезеңдегі ERDR-де тіркелген қылмыстық істердің санын емес, аяқталмаған қылмыстық істердің, оның ішінде өткен жылдардағы қылмыстық істердің санын ескердік.

Осылайша, КПСиМУ статистикасы бойынша 2017 жылдан 2021 жылға дейінгі кезеңде интернетті пайдалану, ақпараттық жүйені пайдаланушыны алдау немесе сенімін теріс пайдалану және ақпараттық жүйеге заңсыз қол жеткізу немесе ақпаратты өзгерту бойынша 20 145 қылмыстық құқық бұзушылық жасалған. республикада тіркелген, бұл қылмыстың жалпы құрылымының 1,7%-ын ғана құрады. Бір қарағанда, бұл сома мардымсыз болып көрінеді және алаңдатпайды. Алайда, егер 2017 жылдан 2021 жылға дейін Қазақстанда жалпы қылмыс 50,1%-ға немесе 361,5 мыңнан 157,9 мыңға (яғни, 158,5 мың қылмыстық құқық бұзушылыққа) азайса, онда киберқылмыстардың саны 31 есеге – жылына 345-тен 10 724-ке өсті.

Ал бұл құқық қорғау органдары сотқа дейінгі тергеуді бастаған фактілер ғана, өйткені қылмыстық жазбалар тек ERDR тіркелген қылмыстық құқық бұзушылықтар бойынша сақталады.

KZ-CERT компьютерлік инциденттерге ден қою қызметінің мәліметі бойынша, соңғы 5 жылда Қазақстанда 115 900 оқиға (кибершабуыл) тіркелді, оның ішінде: ботнеттер – 74 897, зиянды бағдарламалық қамтамасыз ету – 15 505, интернет-ресурсқа қолжетімділіктің жоқтығы – 7 833, фишинг – 3 238, IR мазмұнына заңсыз қол жеткізу және өзгерту – 2 820, қызмет көрсетуден бас тарту – 840 оқиға тіркелген.

Көріп отырғаныңыздай, киберқылмыстарды жасау әдістері әртүрлі, олар үнемі дамып, кәсіби деңгейге көтерілуде.

Ақпараттық-құқықтық қатынастарды реттейтін қылмыстық заңнамаға келетін болсақ, 2015 жылдың қаңтарынан бастап жаңа Қылмыстық кодекстің қолданысқа енгізілді, онда қылмыс пен қылмыстық құқық бұзушылықтан тұратын қылмыстық құқық бұзушылық түсінігі енгізілді [3]. Яғни, бұрын есірткі заттарын пайдаланғаны үшін тек әкімшілік жауапкершілік қарастырылса, енді бұл жауапкершілік қылмыстық болып табылады. Егер адам қоғамдық орындарда есірткі пайдаланса, ол Қазақстан Республикасы Қылмыстық кодексінің 296-бабының 1-бөлігінде көзделген қылмыстық құқық бұзушылықты жасағандықтан қылмыстық жауапкершілікке тартылады [4].

Сонымен қатар, Қазақстан Республикасы Қылмыстық кодексінің «Ақпарат және байланыс саласындағы қылмыстық құқық бұзушылықтар» Ерекше бөлімінде тұтас тарау пайда болды [4].

Бүгінгі таңда қоғам өмірінің әртүрлі салаларында туындайтын ақпараттық-құқықтық қатынастарды реттейтін бірқатар заңдар бар: Қазақстан Республикасының «Ақпараттандыру туралы», «Байланыс туралы» Заңы. Қазақстан Республикасы «Бұқаралық ақпарат құралдары туралы», Қазақстан Республикасының «Мемлекеттік құпиялар туралы» Заңы, «Авторлық құқық және сабақтас құқықтар туралы» Қазақстан Республикасының Заңы, «Жарнама туралы» Қазақстан Республикасының Заңы, Қазақстан Республикасының Заңы. Қазақстан Республикасы «Дербес деректер туралы», Қазақстан Республикасының «Ақпаратқа қол жеткізу туралы» Заңы, т.б.

Компьютерлік қылмыс өткен жылы есірткі саудасын басып озды және уақыт өте көбейеді, дейді АҚШ Интернеттегі қылмыспен күрес басқармасының кеңесшісі Валери МакНивен. «Киберқылмыс өте жылдам қарқынмен жүріп жатыр, сондықтан құқық қорғау органдары ілесе алмайды», - деді кеңесші. Дамушы елдердің компьютерлік инфрақұрылымы киберқылмыскерлердің оңай құрбанына айналады [5].

Статистикалық мәліметтер тіркеудің төмендігі бұл санаттағы қылмыстардың жасалмауымен емес, олардың ашылу деңгейінің

төмендігімен және ішкі істер органдары қызметкерлерінің жаңа компьютерлік технологиялар саласында арнайы білімінің болмауымен байланысты екенін көрсетеді. ғылыми-зерттеу кешенін жүргізу қажет.насихаттау және ұйымдастыру шаралары.Бұл ретте құқық қорғау органдарының мамандандырылған бөлімшелерінің өзара іс-қимылын және қызметін үйлестіруді дұрыс ұйымдастыру маңызды.

Осыған байланысты құқық қорғау органдарының киберқылмыстарды анықтау мен ашудағы тиімділігі төмендеуде.

Санға тоқталсақ, сотқа дейінгі тергеп-тексеру нәтижелері бойынша қылмыстық істердің небәрі 6955-і немесе 34,5%-ы ашылған, 2030-ы немесе 10,1%-ы ақтау негіздер бойынша тоқтатылған.

Киберқылмыс – ақпараттық процестердің жаһандануының және ғаламдық ақпараттық желілердің пайда болуының салдары. Киберқылмыс әсіресе дамудың жаңа – инновациялық кезеңіне көшкен елдерде айқын байқалады.Қазіргі уақытта адамдар ақпараттық технологияларды өз қызметінің әртүрлі салаларында қолданады, сонымен бірге оларды қылмыс жасау үшін пайдалану да артып келеді.

Пайдаланылған қайнар көздерінің тізімі:

1. Джансараева Р.Е., Аратулы К. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – №3(21) – С.95-99.

2. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. ... канд. юрид. наук. – Иркутск, 2006. – 237 с.

3. Сеитов Т.Б. Правовые аспекты компьютерной преступности в зарубежных странах и в Қазақстане. Учебное пособие. – Алматы: Издательство «Данекер», 2000. – 134 с.

4. Уголовные правонарушения в сфере информатизации и связи: Учебное пособие. Бимолданов Е.М. и др. – Алматы: ООНИИРИП Алма-тинской академии МВД Республики Казахстан, 2015. – 194 с.

<https://rep.keu.kz/bitstream/123456789/295/1/%D0%9D%D1%83%D1%80%D0%BF%D0%B5%D0%B8%D1%81%D0%BE%D0%B2%D0%B0%20%D0%90.%D0%9A..pdf>

УДК 347.78

Новосёлов Ален Михайлович
студент 1 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

ПРОБЛЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ В ИНТЕРНЕТЕ

Аннотация

В данной статье рассматриваются проблемы, связанные с причинами нарушения авторского права в интернете. Автором обращено внимание на несовершенство способов предотвращения нарушения прав автора, а также на сложности правового регулирования защиты авторских прав в интернете в соответствии с текущим законодательством Республики Казахстан.

Ключевые слова: Интернет, авторское право, имущественные (исключительные) права, неимущественные права, онлайн-платформа, интернет-пространство, информация.

Новосёлов Ален Михайлович
Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

ИНТЕРНЕТЕ АВТОРЛЫҚ ҚҰҚЫҚТЫ ҚОРҒАУДЫ ҚҰҚЫҚТЫҚ РЕТТЕУ МӘСЕЛЕСІ

Аңдатпа:

Бұл мақалада интернетте авторлық құқықтың бұзылуының себептерімен байланысты мәселелер талқыланады. Автор авторлық құқықтардың бұзылуын болдырмау тәсілдерінің жетілдірілмегендігіне, сондай-ақ Қазақстан Республикасының қолданыстағы заңнамасына сәйкес Интернетте авторлық құқықты қорғауды құқықтық реттеудің күрделілігіне назар аударады.

Түйінді сөздер: Интернет, авторлық құқық, мүліктік (ерекше) құқықтар, мүліктік емес құқықтар, онлайн-платформа, интернет-кеңістік, ақпарат.

Novoselov Alen

1 year student of the Higher School of Law "Adilet"
Caspian Public University,
Republic of Kazakhstan, Almaty

**THE PROBLEM OF LEGAL REGULATION OF COPYRIGHT
PROTECTION ON THE INTERNET**

Annotation:

This article discusses problems associated with the causes of copyright infringement on the Internet. The author draws attention to the imperfection of ways to prevent violation of the author's rights, as well as to the complexity of the legal regulation of copyright protection on the Internet in accordance with the current legislation of the Republic of Kazakhstan.

Key words: Internet, copyright, property (exclusive) rights, non-property rights, online platform, Internet space, information.

Усложнение характера общественных отношений – закономерный процесс, идущий в ногу с развитием человечества, и как следствие, требующий соответственного регулирования. В условиях современных реалий, одной из основных и наиболее масштабных проблем является правовая регламентация общественных отношений в сети Интернет, в частности, отношений в области интеллектуальной собственности.

Интернет, по своей природе, создает возможность свободного распространения информации. Другой вопрос, что данные действия могут быть отнюдь не правомерными, впоследствии приносящими ущерб лицам, чьи права были нарушены. Наиболее распространенным примером может служить нарушение авторского права. Последнее получило название интернет-пиратство, т.е. использование интернета для незаконного копирования, взлома и (или) распространения видео и аудио контента, программного обеспечения и других видов информационной продукции, размещаемой в интернете. [1]

Чтобы понять актуальность данной проблемы, достаточно посмотреть на статистику интернет-пиратства. К примеру, пиратские видеоматериалы набирают более 230 миллиардов просмотров в год. [2] Сомневаюсь, что правообладатель заинтересован в подобной безвозмездной раздаче результатов собственного труда. А факт того, что с каждым годом интернет-пиратства становится всё больше, лишний раз говорит нам о несовершенстве правовых инструментов для защиты авторских прав в Интернете.

Согласно закону Республики Казахстан «Об авторском праве и смежных правах», авторское право представляет собой личные имущественные (исключительные) и неимущественные права автора, распространяющиеся на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от их назначения, содержания и достоинства, а также от способа и формы их выражения [3].

Авторское право распространяется как на обнародованные (опубликованные, выпущенные в свет, изданные, публично исполненные, публично показанные), так и на необнародованные произведения, существующие в какой-либо объективной форме: письменной, устной, в виде звуко- или видеозаписи, изображения и др. Интернет, как коммуникационная сеть и всемирная система объединённых компьютерных сетей для хранения и передачи информации [4], создаёт возможность для достаточно быстрого и беспрепятственного размещения в последней как обычных данных, так и объектов авторского права. Более того, информация, загруженная в Интернет, помимо виртуального, приобретает массовый обнародованный характер и становится доступной для использования людьми по всему миру.

Авторское право на произведение возникает в силу факта его создания, соответственно, наделяя правообладателя рядом неимущественных и имущественных (исключительных) прав. Последние представляют собой право автора и (или) иного правообладателя осуществлять, разрешать и запрещать использование произведения любым способом в течение установленного срока. К неимущественным правам, в свою очередь относятся: право признаваться автором произведения и требовать такого признания, право на неприкосновенность произведения, право на открытие доступа к произведению неопределенному кругу лиц (право на обнародование) и др.

Очевидно, что права автора могут быть нарушены, тем самым, создавая у правообладателя потребность в устранении несправедливости, препятствующей реализации его интересов. Однако, если процесс правового регулирования защиты авторского права в реальном мире (не без процессуальных сложностей, конечно) определён и может быть осуществлён, то в случае с Интернетом возникает ряд проблем.

Прежде чем изолированно рассматривать процесс защиты авторских прав, его проблематику, предлагаем раскрыть вопрос системно и не забывать про существование причинно-следственных связей.

Для начала нужно понимать, что существование Интернета не является первопричиной возникновения проблемы нарушения авторских

прав. Интернетом, в свою очередь, лишь определяется способ и условия общественных отношений, но никак не сами общественные отношения. Говоря о последних, логично предположить, что вести себя определённым образом в Глобальной сети есть прерогатива человека. Далее, в условиях поставленной проблемы, существует два варианта поведения: либо человек умышленно совершает противоправные действия, либо же, по причине своей небрежности. Так или иначе, вне способа и условий общественных отношений, вычленив удовлетворительный ответ не представляется возможным. В связи с этим, необходимо также рассмотреть и последние два фактора.

Говоря о способе общественных отношений в Интернете, его можно охарактеризовать как *виртуальный*, т.е. существующий при определенных условиях и исчезающий при исчезновении этих условий [5]. Из этого следует, что существует некоторое количество условий, в соответствии с которыми протекают взаимоотношения между людьми в интернет-пространстве. В рамках рассмотрения нашего вопроса, выделим лишь несколько принципов, существование которых, в теории, может способствовать нарушению авторских прав в Интернете:

- 1) свободный доступ к информации;
- 2) возможность копирования и воспроизведения информации;
- 3) возможность распространения информации в интернет-пространстве без каких-либо ограничений.

Самое главное, что осуществление действий, названных в двух последних пунктах, не составляет каких-либо трудностей, тем самым, делая их выполнение доступным для широкого круга лиц.

Таким образом, рассмотрев способ и условия общественных отношений в Интернете, можно сделать вывод, что создаётся достаточно благоприятная почва для нарушения авторских прав, которая, в совокупности с действиями недобросовестных и небрежных граждан, порождает массовый характер правонарушений. Теперь время поговорить о проблеме защите авторских прав в интернет-пространстве.

Законодатель, в качестве превентивной меры, даёт право, с целью оповещения о своих исключительных имущественных правах, автору и (или) правообладателю использовать знак охраны авторского права, который помещается на каждом экземпляре произведения, состоящий из трёх элементов: латинской буквы «С» в окружности, имени (наименования) обладателя исключительных авторских прав, года первого опубликования произведения. [6, ст. 9, пункт 1] Судя по всему, то ли из-за обесценивания института авторского права в Интернете, то ли из-за

ранее подмеченной небрежности, данное оповещение чаще всего игнорируется. В общем, к этому мы вернёмся чуть позже.

Для защиты авторских прав, согласно закону Республики Казахстан «Об авторском праве и смежных правах», предусматривается единственный вариант разрешения ситуации – через суд [6, ст. 49]. Таким образом, Защита авторских и смежных прав осуществляется судом путем:

- 1) признания прав;
- 2) восстановления положения, существовавшего до нарушения права;
- 3) пресечения действий, нарушающих право или создающих угрозу его нарушения;
- 4) возмещения убытков, включая упущенную выгоду;
- 5) взыскания дохода, полученного нарушителем вследствие нарушения авторских и (или) смежных прав и т.д.

С целью упрощения обозначивания первого противоречия, смоделируем ситуацию: авторское право правообладателя было нарушено неким анонимным пользователем Интернета, объект авторского права был размещён на онлайн-платформе. Учитывая то, что, в соответствии с законом РК «О персональных данных и их защите», лицо, ответственное за обработку персональных данных (или собственник онлайн-платформы, содержащей персональные данные), обязан обеспечить их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта [7], на кого правообладатель должен подать в суд?

Второй момент. Даже если мы допустим тот факт, что будут известны персональные данные правонарушителя, но при этом правонарушитель будет не один, а к примеру, десять, то насколько целесообразно правообладателю будет подавать на всех этих людей в суд и участвовать одновременно в десяти судебных процессах?

Третий момент. Согласно закону Республики Казахстан «О средствах массовой информации», средство массовой информации есть периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая *интернет-ресурсы*. Одним из оснований для приостановления выпуска средства массовой информации либо распространения продукции средства массовой информации в установленном законами Республики Казахстан порядке является нарушения законодательства Республики Казахстан *в сфере авторского права и смежных правах*. Приостанов-

ление либо прекращение выпуска или распространения продукции средства массовой информации, поставленного на учет в уполномоченном органе, *возможно по решению собственника или суда*. Однако, в случае приостановления либо прекращения по вступившему в законную силу решению суда выпуска средства массовой информации, либо продукции средства массовой информации, когда средством массовой информации является интернет-ресурс, уполномоченные государственные органы, собственники интернет-ресурсов обязаны приостановить или прекратить выпуск средства массовой информации либо распространение *на территории Республики Казахстан* продукции средства массовой информации. Вступление в законную силу решения суда о приостановлении распространения продукции средства массовой информации либо выпуска средства массовой информации, когда средством массовой информации является интернет-ресурс, влечет *запрет на использование доменного имени* с тем же или дублирующим названием на срок не более трех месяцев. [8] Таким образом, через суд правообладатель может добиться приостановления работы интернет-ресурса, на котором было зафиксировано нарушение авторских прав путём запрета на использования *доменного имени* [9]. Однако данный запрет распространяется только на работоспособность интернет-ресурсов на территории Республики Казахстан в то время, как управление доступностью всё тех же интернет-платформ для иностранного сегмента Интернета находится вне компетенции уполномоченных органов Республики Казахстан. В итоге, авторское право, даже несмотря на принятые меры, всё равно продолжит подвергаться нарушениям, в силу особенности функционирования Интернета и несовершенства системы правового регулирования.

Возвращаясь к сказанному ранее, можно заключить, что законодательством не предусмотрены способы предотвращения нарушения авторских прав, которые в действительности бы могли гарантировать безопасность и соблюдение имущественных (исключительных), неимущественных прав в интернет-пространстве. В связи с этим, помимо проблем, возникающих в ходе защиты авторских прав, правообладатель не застрахован от постоянного и неограниченного посягательства на нарушение последних.

Из последних изменений в сфере законодательства Республики Казахстан, связанного с Интернетом, можно отметить появление нового закона от 10 июля 2023 года «Об онлайн-платформах и онлайн-рекламе». В последнем присутствует статья об основаниях отнесения

информации к противоправному контенту, приостановление, прекращение размещения и распространения противоправного контента [10], в соответствии с которой, на онлайн-платформах на территории Республики Казахстан запрещаются размещение и распространение противоправного контента. Однако, под перечень противоправного контента не попадает нарушение законодательства в сфере авторского и смежного права, что, на наш взгляд, является упущением.

Подводя итоги, можно заключить, что проблема правового регулирования защиты авторских прав в Интернете нуждается в серьезном рассмотрении, исходя из которого в будущем должны быть созданы подходящие правовые нормы, что поспособствуют разрешению озвученных противоречий.

Список использованных источников:

1. Определение *интернет-пиратства*, <https://dzen.ru/a/Y6nSR9FhpR2W523R>
2. Piracy Is Back: Piracy Statistics for 2023, <https://dataprot.net/statistics/piracy-statistics/>
3. Закон Республики Казахстан от 10 июня 1996 года № 6-І «Об авторском праве и смежных правах» (с изменениями и дополнениями по состоянию на 01.05.2023 г.) /<https://adilet.zan.kz>
4. Википедия: определение понятия Интернет, https://ru.wikipedia.org/wiki/Интернет#Юридические_аспекты
5. Википедия: определение понятия Виртуальность, <https://ru.wikipedia.org/wiki/Виртуальность>
6. Закон Республики Казахстан «Об авторском праве и смежных правах»/<https://adilet.zan.kz>
7. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 01.05.2023 г.) /<https://adilet.zan.kz>
8. Закон Республики Казахстан от 23 июля 1999 года № 451-І «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 01.05.2023 г.) /<https://adilet.zan.kz>
9. Доменное имя - символическое (буквенно-цифровое) обозначение, сформированное в соответствии с правилами адресации Интернета, соответствующее определенному сетевому адресу и предназначенное для поименованного обращения к объекту Интернета, *Приказ Министра обороны и аэрокосмической промышленности Республики Казахстан от 13 марта 2018 года № 38/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 27 марта 2018 года № 16654.*

10. Закон Республики Казахстан от 10 июля 2023 года № 18-VIII «Об онлайн-платформах и онлайн-рекламе» /<https://adilet.zan.kz>**11**. Закон Республики Казахстан от 10 июля 2023 года № 18-VIII «Об онлайн-платформах и онлайн-рекламе» /<https://adilet.zan.kz>

ӘОЖ 347

Нурбосун Индира Серікқызы

Каспий қоғамдық университеті «Әділет» Жоғары құқық мектебінің 3 курс студенті,
Қазақстан Республикасы, Алматы қ.

ҚҰҚЫҚТЫҚ АСПЕКТІЛЕРДІҢ ЭВОЛЮЦИЯСЫ: ӘЛЕУМЕТТІК ЖЕЛІ МЕН ИНТЕРНЕТТІҢ АДАМНЫҢ АЗАМАТТЫҚ ІС ЖҮРГІЗУ ҚҰҚЫҚТАРЫНА ӘСЕРІ

Ғылыми жетекші:

Мақсатов Н.Р.

з.ғ.м., Каспий қоғамдық университеті «Әділет»
Жоғары құқық мектебінің сеньор-лекторы

Аңдатпа

Әлеуметтік желілер мен интернеттің адамның азаматтық іс жүргізу құқығына әсерін талдай отырып, бұл мақала цифрлық дәуірдегі құқықтық аспектілердің эволюциясын зерттейді. Жұмыс әртүрлі аспектілерді қарастырады, соның ішінде электронды форматта дәлелдемелер беру, оны қамтамасыз ету жолдары, әлеуметтік желідегі анонимділік мәселесінің дәлелдемелер келтіруге кері әсері, сондай-ақ азаматтық сот ісін жүргізудің электрондық форматы зерделенді. Мақаланың қорытынды бөлімінде мақалада қозғалған мәселелерге ұсыныстар білдірілді.

Түйінді сөздер: құқықтық аспект, құқықтық аспектілердің эволюциясы, интернет, әлеуметтік желі, дәлелдеме, анонимді желі қолданушысы, мессенджерлер, ресми веб-сайт, құқықбұзушылық, Нотариус, Электрондық сот.

Нурбосун Индира Серікқызы

Студентка 3 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

**ЭВОЛЮЦИЯ ПРАВОВЫХ АСПЕКТОВ:
ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ И ИНТЕРНЕТА
НА ГРАЖДАНСКО-ПРОЦЕССУАЛЬНЫЕ ПРАВА ЧЕЛОВЕКА**

Аннотация

Анализируя влияние социальных сетей и интернета на гражданско-процессуальные права человека, данная статья исследует эволюцию правовых аспектов в цифровую эпоху. В работе рассматриваются различные аспекты, в том числе предоставление доказательств в электронном формате, способы их обеспечения, негативное влияние проблемы анонимности в социальных сетях на приведение доказательств, а также изучен электронный формат гражданского судопроизводства. В заключительной части статьи были высказаны предложения по вопросам, затронутым в статье.

Ключевые слова: правовой аспект, эволюция правовых аспектов, интернет, социальная сеть, доказательства, анонимный пользователь сети, мессенджеры, официальный сайт, правонарушения, нотариус, электронный суд.

Nurbossun Indira

3 year student of the Higher School of Law “Adilet”

Caspian Public University,

Republic of Kazakhstan, Almaty

**EVOLUTION OF LEGAL ASPECTS:
THE INFLUENCE OF SOCIAL NETWORKS AND THE INTERNET
ON CIVIL PROCEDURAL HUMAN RIGHTS**

Annotation

Analyzing the impact of social networks and the Internet on civil procedural human rights, this article explores the evolution of legal aspects in the digital age. The paper examines various aspects, including the provision of evidence in electronic format, ways to ensure it, the negative impact of the problem

of anonymity in social networks on the presentation of evidence, and also studied the electronic format of civil proceedings. In the final part of the article, suggestions were made on the issues raised in the article.

Keywords: legal aspect, evolution of legal aspects, Internet, social network, evidence, anonymous user of the network, messengers, official website, offenses, Notary, Electronic court.

Құқықтық аспект-бұл құқық нормаларымен және оларды қолданумен байланысты сала. Ол заңнамаға, құқықтық жүйелерге, сот төрелігіне және құқық қорғау қызметіне қатысты барлық аспектілерді қамтиды[1].

Құқықтық аспектілердің эволюциясы жаңа құқықтық институттардың пайда болуына, қолданыстағы нормалар мен қағидалардың өзгеруіне, сондай-ақ жаңа заңдардың қабылдануына әкелуі мүмкін. Ол қоғамның дамуы мен прогресінің ажырамас бөлігі болып табылады және азаматтардың құқықтары мен бостандықтарының әділдігін, теңдігін және қорғалуын қамтамасыз етуге ықпал етеді.

Мысалы, әйелдердің құқықтарына деген көзқарастың өзгеруі олардың тең құқықтары мен кемсітушіліктен қорғалуы үшін, «Әйелдерге қатысты кемсітушіліктің барлық нысандарын жою туралы» Конвенцияның қабылдануына әкелді.

Технологияның дамуы жаңа құқықтық мәселелер мен нормалардың пайда болуына әкелуі мүмкін. Мысалы, интернеттің дамуымен киберқауіпсіздік немесе жеке деректерді қорғау саласындағы құқықбұзушылықтар үшін құқықтық жауапкершілік мәселелері туындайды. Немесе керісінше интернеттің дамуы оның адам құқықтарын қорғауына не болмаса қорғауды жүзеге асыру үшін қызмет етуіне алып келуі мүмкін.

Интернет пен әлеуметтік желі өзінің жаһандануының шегінде тұрған 21 ғасырда адамзат өзінің құқықтарының шеңберін бұл аяда барынша кеңейту үстінде.

Азаматтық іс жүргізу және оның субъектілері де бұл мүмкіндіктерді барынша пайдалануда. Әлеуметтік желілер мен интернетті пайдалану азаматтық сот процестеріне айтарлықтай әсер етіп келеді. Бұл өз кезегінде интернет шеңберінде орын алатын әрекеттердің заңдастырылуына және азаматтық іс жүргізуде пайдаланылуына алып келді.

1. ДӘЛЕЛДЕМЕЛЕР.

Азаматтық сот ісін жүргізуде тараптардың талаптары мен қарсылықтарын негіздейтін мән - жайлардың болуын немесе болмау-

ын белгілейтін фактілер туралы мәліметтер-дәлелдемелер негізінде сот үкімдерін жасайтын істің нақты мән-жайларын дұрыс және объективті анықтау міндетті аспект болып табылады[2].

Азматтық процестік кодекстің 72 бабында келесідей түсініктеме берілген: Әр тарап өзінің талаптары мен қарсылықтарының негізі ретінде сілтеме жасайтын мән-жайларды дәлелдеуге, қорғану құралдарын пайдалануға, фактілерді растауға, оларға дау айтуға, процесті адал жүргізуге сәйкес келетін және іс жүргізуге жәрдемдесуге бағытталған дәлелдемелерді және дәлелдемелерге қарсы қарсылықтарды судья белгілеген мерзімдерде келтіруге тиіс.

Осы баптың мағынасына үңілетін болсақ, әлеуметтік желідегі ақпаратты дәлелдеме ретінде ұсыну еркіндігі шектелмеген.

Әлеуметтік желілер дәлелдеме келтірудің жаңа жолдарын ашты. Себебі, әлеуметтік желі өзара әрекеттесу, қарым-қатынас, ақпарат алмасу және өзін-өзі көрсету үшін шексіз мүмкіндіктер ұсынады. Яғни қазіргі уақытта біздің көптеген әрекеттеріміз ғаламтор мен әлеуметтік желілерде жарияланып, оның кеңістігінде қалып қояды. Бұл адамның құқықбұзушылық жасаған жағдайында дәлелдер келтірудің ең сәтті түрінің бірі болып табылады.

Интернеттен ұсынуға жататын, кең таралған дәлелдердің түрлері:

1. Скриншоттар. Веб-беттердің, түсініктемелердің немесе әлеуметтік желілердегі жазбалардың скриншоттары визуалды дәлел бола алады.

2. Электрондық хаттар. Электрондық поштадан немесе мессенджерлерден алынған электрондық хаттардың немесе хат-хабарлардың көшірмелері

3. Веб-беттер мұрағаты (архив). Белгілі бір уақытта веб-беттің қолданылғанын сақтау үшін мұрағатты пайдалану.

4. Бейне және аудио жазбалар. Егер қажет болса, бейнежазбалар немесе аудиожазбалар маңызды дәлел бола алады.

Қазіргі таңда интернет кеңістігі шайқас алаңына, ал интернет-ресурстар түрлі құқықбұзушылықтар жасайтын қаруға айналып бара жатыр. Құқықбұзушылардың есебі қарапайым: ақпарат интернетте тез таралады, ал құқық қорғау органдарымен проблемалар туындау қаупі төнген жағдайда, оны жою өте оңай — сондықтан заңсыз әрекеттердің ізі де қалмайды[4]

Ақпаратты құралдардың дамуына байланысты бұрыннан-ақ электронды құжат алмасу, интернет кеңістігінде құқықтары бұзылған адамдардың, авторлық құқық, іскерлік беделге нұқсан келген

тұлғалардың құқықтарын қорғау үшін әлдеқашан осы дәлелдемелерді қамтамасыз ету шараларын қолдану қажеттігі туындаған. Осыған байланысты әлеуметтік желідегі құқық бұзушылықтарға байланысты даулар бойынша дәлелдемелерді сотқа дейінгі кезеңде нотариаттық қамтамасыз ету - бұзылған құқықтарды қорғаудың аса маңызды құралы болып табылады[5].

Қазақстан Республикасының «Нотариат туралы» Заңы 99-бабына сәйкес, Нотариус сотта немесе басқа құзыретті органда іс туындаған жағдайда, егер кейіннен дәлелдемелерді табыс ету мүмкін емес немесе қиын болады деп топшылауға негіз болса, мүдделі тұлғалардың өтініші бойынша қажетті дәлелдемелерді қамтамасыз етеді.

Біздің жағдайда нотариустың әрекеттері келесідей болмақ:

1. Мүдделі тұлғаның өтініші бойынша нотариус дәлелдемелерді тексереді, табылған ақпаратты құжаттайды — мәтінді басып шығарады, суретке түсіреді немесе экранның скриншоттарын жасайды, суреттер қосымшаларымен дәлелдемелерді тексеру хаттамасын жасайды.

2. Мүдделі тұлға нотариусқа хабарламаға, Stories-ке немесе сайтқа басылатын сілтемені көрсете отырып өтініш береді не мессенджерде аккаунты бар және хат алмасу жүргізілген смартфонды немесе планшетті ұсынады.

3. Нотариус маршрутты қадағалау бағдарламасын қолданады, содан кейін скриншоттар түсіреді және хаттамада бекітілген дәлелдемелерді тексереді. Онда нотариус барлық әрекеттерді егжей-тегжейлі сипаттайды, жасалған күні мен орнын, сондай-ақ тексеру кезінде анықталған жағдайларды көрсетеді. Скриншоттар басып шығарылады және хаттамаға тігіледі.

4. Егер аудио хабарламалар немесе бейнелер болса, онда олар дискіге жазылады, транскрипт орындалады, бұл жағдайда дәлелдемелерді тексеру хаттамасына транскрипт пен диск қоса беріледі[7].

Енді бізде «бұл дәлелдемелер тәжірибеде назарға алынады ма?» деген сұрақ туындайды. Судьялар дәлелдің бұл түрін жиі қабылдай бермейді. Яғни кейбір судьялар ішкі сенім ретінде дәлелді бағаласа, енді біреулері бұл дәлелдемелерді мүлдем назарға алмайды.

Мысалы Медеу аудандық сотының қарауында азаматтық іс қаралды. Және сот шешімде талап қоюшы ұсынған жауапкердің жосықсыз әрекеттері дәлелденетін WhatsApp мессенджеріндегі хат алмасуды дәлел ретінде қарастырмай, шешім шығарарда негізге алмаған.

Себебі бұл дәлелдемелердің маңыздылығын нақтылайтын және сот шешімінің негізіне алынатындай заңды күші жоқ.

Әлеуметтік желіден дәлелдеме келтіруге байланысты қындық тудыратын жайттың бірі ол желіні аноним қолданушы. Әлеуметтік желілерде көлемі кең аудитория алдында анонимді қолданушы атынан белгілі бір тұлғаға қатысты құқықбұзушылық орын алуы мүмкін. Анонимді түрде тіркелген желі қолданушысына, оның жеке басын дәлелдейтін деректемелердің жоғына байланысты, оған қатысты іс қозғау немесе бір тұлғаның сол құқықбұзушылықты орындағанын дәлелдейтін фактілер келтіру мүмкін емес.

Мысалы аноним қолданушының көпшілікке құқығы бұзылатын тұлғаның құпиясын жария етіп, оған моральды зиян келтірсе, біз аноним қолданушының тұлғасын анықтай алмаймыз, яғни бізге көмекпен жүгінген тұлғаның құқығын қорғай алмаймыз.

Қытайда интернетті және цифрлық платформаларды, соның ішінде интернеттегі анонимділікті реттеу шараларын қатаң бақылау бар. Соңғы жылдары әртүрлі онлайн платформалар мен әлеуметтік желілерде тіркелу үшін нақты пайдаланушы аттарын талап етуге бағытталған ережелер енгізілді және күшейтілді.

Кейбір негізгі аспектілер:

1. Шынайы аты-жөні бойынша тіркеу ережелері: 2017 жылы Қытай Интернет-платформалар мен әлеуметтік медианы пайдалану кезінде пайдаланушылардан өздерінің Шынайы аты-жөні бойынша тіркелуді талап ететін жаңа ережелерді енгізді. Бұл анонимді есептік жазбалардың аз таралғанын білдіреді.

2. Әлеуметтік медианы бақылау: Қытай әлеуметтік желілер мен мессенджерлердегі қызметті белсенді бақылайды. Мазмұнды бұғаттау және цензурау, сондай-ақ пайдаланушылардың әрекеттерін бақылау тәжірибесі бар.

3. Сәйкестендіру технологияларын пайдалану: тіркеу ережелерінен басқа, Қытай пайдаланушының аутентификация талаптарын қамтамасыз ету үшін бетті тану технологияларын және басқа сәйкестендіру әдістерін белсенді түрде әзірлейді және енгізеді

Бірақ бұл жүйеге әлі күнге дейін сын айтып, адамдардың құқығын шектейтіні жөнінде пікір білдіретіндер көп[12].

2007 жылы Оңтүстік Кореяда интернет және киберқауіпсіздік туралы заң енгізілді, ол веб-сайт иелерінен пайдаланушыларды өздерінің шынайы есімдері мен ұялы телефон нөмірлері бойынша міндетті тіркеу саясатын сақтауды талап етті.

Бұл дау тудырған Заң киберқылмыспен күрес және әлеуметтік желілердегі қорлау, жала жабу, кемсітушілік мінез көзделетін

пікірлермен күресу үшін қабылданған болатын. Бірақ интернет кеіңстігін мейірімділік пен достыққа шақыру сәтсіз аяқталып, 2012 жылдың 24 тамызында Оңтүстік Корея заңның күшін жойды[13].

Қазақстанда бұндай практика болған жоқ. Екі мемлекеттің тәжірибесіне сүйенсек, көпшілік анонимділіктің жойылғанына қарсылықтарын білдіріп, бұл шара олардың сөз бостандықтарын шектейтінін алға тартқан. Бірақ М.Бакунин айтпақшы «Бір адамның бостандығы, екінші адамның бостандығы басталған жерде аяқталады». Егерде әлеуметтік желі қолданушылары өзгелердің құқықтарын құрметтей білгенде анонимділікпен күресу мәселесі туындамас еді. Әрекетке қабілетті адамдар өз құқықбұзушылықтары үшін жауапкершілікті көтере білуі тиіс. Ал үкімет өз тарапынан желі қолданушыларына сөз бостандығын пайдалануға мүмкіндік беріп, заңда көзделген құқық бұзылған жағдайда ғана жауаптылыққа тартуды көздегені дұрыс.

Интернет арқылы алынатын дәлелдемелер азаматтық процесте дәлелдемелер институтын дамытудың перспективті бағыты болып табылады, бұл олардың сот практикасында пайдаланудың артуымен дәлелденеді.

2. ЭЛЕКТРОНДЫҚ СОТ ІСІН ЖҮРГІЗУ

«Электрондық сот» іс жүргізу заңнамасын жүзеге асыруда ақпараттық-коммуникативтік технологияларды пайдалануды көздейді[8].

Азаматтық процестік кодекстің 11-1 тарауы Электрондық сот ісін жүргізу ерекшеліктеріне арналған.

Азаматтық процестік кодекстің 133-1 бабына сәйкес, азаматтық сот ісін электрондық форматта жүргізуге болады. Сот ісін электрондық форматта жүргізу кезінде электрондық азаматтық іс қалыптастырылады[9].

Қазіргі уақытта сот ісін жүргізуге интернет және электронды байланыс құралдары мен түрлі платформалар өзінің пайдалы қызметін көрсетуде.

Мысал ретінде келесі функцияларды атауға болады:

1. талап қою
2. өтініштерді тіркеу
3. талап-арыздарға электрондық түрде кері байланыс беру
4. бейнеконференциялар көмегімен отырыстар жүргізу
5. сот процесіне қатысушыларға Интернет арқылы немесе СМС-хабарламалар арқылы қосымша хабарламалар және т. б жіберу.

Яғни сот ісін электронды форматта жүргізудің өзіндік ыңғайлықтары бар: шығындар азаяды; уақыт үнемделеді; бір әрекетті жүзеге асыру үшін

екінші қалаға барудың, тығыз жағдайлар туғанда ұшақ, поезд рейстеріне тәуелді болмау; хабарламалардың жеткізілгеніне қобалжымау; барлық құжаттардың бір базада сақталуы және т.б.

Қазақстан, Ресей және АҚШ электронды сот ісін жүргізу платформаларына анализ жасап көрсек.

1. Қазақстан Республикасының электронды сот ісін жүргізу платформасы.

1. Ресмилігі.

– **Сот кабинеті** - Қазақстан Республикасы сот органдарының электрондық сервистеріне қол жеткізуге арналған бірыңғай терезе болып табылады[10].

Ресми веб-сайт Сот кабинеті (sud.kz)

2. Қолжетімділігі және ыңғайлылығы.

– Сот кабинетіне пайдаланушы немесе қонақ ретінде кіре аласыз. Пайдаланушы болу үшін ЭЦҚ арқылы тіркелесіз;

– Басты бетте платформаның ұсынатын қызметтері және оларды бірден ашатын батырмалар көрсетілген;

3. Ақпаратпен қамтамасыз ету және электронды қызмет

– сот ісін жүргізу барысында қолданылатын құжаттар тізілімі мен олар жөнінде ақпарат және оларды онлайн тапсыру қамтамасыз етілген;

– Жариялауға ашық сот істеріне қолжетімділік қамтамасыз етілген. Сот істерін мәліметтер көрсету арқылы іздеп табуға болады.

– «Соттар- GIS» қызметі ұсынылған. «Соттар- GIS» қызметі - бұл соттарды, медиаторларды, адвокаттарды және нотариустарды іздестіру мүмкіндігін қамтамасыз етуге бағытталған географиялық ақпараттық жүйе.

4. Көмек көрсету және байланыс желілері

– Платформаны пайдалану нұсқаулығы, кері байланыс, сұрақтарға жауап негізінде пайдаланушыларға ыңғайлық жасалған.

5. Құқықтық ақпарат

– Басты бетте ҚР Жоғарғы сотының сайтына сілтеме бар және олар өзара баланысқа ие.

– ҚР ЖС сайтында сот жүйесі жөнінде ақпарат, құқықтық көмек, НҚА, сотқа жүгінуге көмек және өзге де қызметтер жөнінде ақпараттар ашық қолданысқа ұсынылған.

2.Ресей Федерациясының электронды сот ісін жүргізу платформасы.

1. Ресмилігі.

– Ресей Федерациясының “сот төрелігі” мемлекеттік автоматтандырылған жүйесі (ГАС Правосудие) — Ресейдегі сот ісін жүргізу туралы еркін ақпарат беретін ақпараттық жүйе. Ол сондай-ақ Ресейдегі сот ісін ақпараттық интеграциялауды қамтамасыз ететін сот ісін жүргізуде қолданылады [11].

Ресми веб-сайт Верховный Суд Российской Федерации (vsrf.ru)

2. Қолжетімділігі және ыңғайлылығы

– Бірыңғай сәйкестендіру және аутентификация жүйесі арқылы тіркеледі

– Басты бетте платформаның ұсынатын қызметтері және оларды бірден ашатын батырмалар көрсетілген;

– Мемлекеттік бажды есептеу жүйесі енгізілген

3. Ақпаратпен қамтамасыз ету және электронды қызмет

– Іс құжаттарын электронды түрде тапсыру функциясы қамтылған

– Істер бөлімінде сіз қатысушы болып табылатын сот істері бойынша барлық ақпаратқа қол жеткізе аласыз.

4. Көмек көрсету және байланыс желілері

– Жүйемен жұмыс істеу кезінде қандай да бір сұрақтарыңыз немесе қиындықтарыңыз болса, анықтамалық ақпаратты пайдалана аласыз.

5. Құқықтық ақпарат.

– НҚА

– Сот практикасына шолулар

– Тематикалық шолу

– сот статистикасы ұсынылған

3. АҚШ электронды сот ісін жүргізу платформасы.**1. Ресмилігі**

2. Суды США | (uscourts.gov) -федералды сот жүйесі туралы кең ақпарат беретін АҚШ соттарының ресми веб-сайты.

Жоғарғы сот сайты бөлек

3. Қолжетімділігі.

– АҚШ-тағы құқықтық процедуралар, сот шешімдері және әділет жүйесінің басқа аспектілері туралы ыңғайлы қолжетімділік пен ақпаратты ұсынады.

4. Ресурстар және білім

– Сайтта білім беру ресурстары, мысалы, мақалалар, бейнематериалдар немесе заңды рәсімдер туралы презентациялар ұсынылған.

5. Электрондық Қызметтер

– Сайт адвокаттарға, тараптарға және жұртшылыққа электрондық қызметтер мен ресурстарға қолжеткізуді қамтамасыз етеді.

6. Көмек көрсету және байланыс желілері

– Платформаны пайдалану нұсқаулығы, кері байланыс, сұрақтарға жауап негізінде пайдаланушыларға ыңғайлық жасалған.

Үш мемлекеттің де электронды сот базаларын қарап, жалпылама мағлұматтар алдық. Платформалардың ұсынатын қызметтерінде өзіндік ерекшеліктер де, ұқсастықтар да кездесті. Бірақ ең бастысы электронды сот ісін жүргізу, қажетті функциялар, ақпараттандыру бұл платформаларда қамтамасыз етілген.

Қазіргі цифрлық қоғамда әлеуметтік желілер мен интернет құқықтық аспектілердің эволюциясында, әсіресе адамның азаматтық іс жүргізу құқықтары аясында ажырамас бөлікке айналып, маңызды рөл атқаруда.

Технологияның қарқынды дамуының нәтижесінде адамдардың құқығының қолданылу немесе бұзылу шекарасы кеңейді. Бұл әрине өз кезегінде қолданыстағы нормалар мен қағидалардың өзгеруіне, сондай-ақ жаңа заңдардың қабылдануына, құқықтық аспектілер эволюциясына әкелуі мүмкін.

Мақалада жеткізгіміз келген басты идея – біз технологиялар мен цифрлы қоғамның қарқынды дамуынан қорқудың орнына, құқық аспектісінің эволюциясының даму деңгейіне көңіл бөліп, орын алып жатқан өзгерістердің максималды түрде пайдалы жағын қолдануды үйренуіміз керек. Соған орай білдіретін ұсыныстарым:

1. Интернет деректемелерінен, әлеуметтік желілерден ұсынылатын электронды дәлелдемелердің күшін заңдастыру. Азаматтық процестік кодекске электронды дәлелдемелерді ұсыну және бағалау жөнінде анықтама енгізу.

2. Анонимділікке қарсы Отандық әлеуметтік желілерге және веб-сайттарға тіркелгенде ЖСН арқылы тіркелуді қарастыру

3. Анонимділікке қарсы шетелдік әлеуметтік желілердің Қазақстанда қолданылуын реттеу. Мысалы Қазақстандықтардың жеке парақшасында өзінің толық аты-жөні көрсетілуін қамтамасыз ету.

Қорытынды бізге құқықтық аспектілердің бұл эволюциясы тек қиындық емес, сонымен қатар цифрлық прогресс дәуірінде құқықтық жүйенің тепе — теңдігін, әділеттілігін және тиімділігін қамтамасыз ету мүмкіндігі екенін еске салады.

Пайдаланылған қайнар көздерінің тізімі:

1. Правовой аспект (anyquestion.info) дата обращения 10.12.2023 г
2. Доказательства в гражданском процессе (М. Байгелов, судья СМЭС г. Астаны) Информационная система ПАРАГРАФ. Дата обращения: 8 декабря 2023 года,
3. Сас В. В. «Электронное правосудие» как элемент «сетевое общества»: теоретические проблемы // Юридическая наука, 2012. № 2. С. 101-104
4. Орлов В.К. Обеспечение доказательств в сети Интернет – эффективный механизм защиты нарушенных прав в гражданском процессе. 2014 №2 (11) С. 15-17
5. Сергеева К.А. Обеспечение доказательств в законодательстве о нотариате // Арбитражный и гражданский процесс. 2012. №3. С. 26 – 31; N 4. С. 27 – 30.
6. «Нотариат туралы» Қазақстан Республикасының 1997 жылғы 14 шілдедегі N 155-І Заңы. /<https://adilet.zan.kz>
7. <https://www.zakon.kz/> дата обращения 09.12.2023
8. Федеральный закон «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22.12.2008 г. № 262
9. Қазақстан Республикасының Азаматтық процесіткі кодексі Қазақстан Республикасының Кодексі 2015 жылғы 31 қазандағы № 377-V ҚРЗ. /<https://adilet.zan.kz>
10. Сот кабинеті (sud.kz) дата обращения 10.12.2023
11. Государственная автоматизированная система Российской Федерации «Правосудие»
12. В Китае полностью запретили анонимность в интернете - CNews электронды дереккөз
13. <https://www.kakprosto.ru/kak-249254-cto-vernul-pravo-anonimnosti-grazhdanam-yuzhnoy-korei#ixzz8LcLbQMxр> электронды дереккөз

УДК 349**Өмірхан Салтанат**

студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ИСКУССТВЕННЫЙ ИНТЕЛЕКТ

Научный руководитель:

Мухтарова А.К.

К.ю.н., ассоциированный профессор

Высшей школы права “Эділет”

Каспийского общественного университета

Аннотация

Данная статья представляет собой обзор и анализ основных аспектов искусственного интеллекта (ИИ). Развитие ИИ в последние годы имело значительный прогресс и широкое применение в различных областях человеческой деятельности. В статье освещаются различные подходы к созданию искусственного интеллекта, включая экспертные системы, нейронные сети, генетические алгоритмы, а также глубокое обучение и облачные вычисления. Особое внимание уделено сферам применения искусственного интеллекта. Приводятся примеры успешной реализации искусственного интеллекта в конкретных проектах, что позволяет оценить его потенциал и преимущества. Также обсуждаются этические и социальные аспекты развития искусственного интеллекта. Автор подробно рассматривает вопросы, связанные с автономностью и безопасностью ИИ, а также его влиянием на рынок труда и общество в целом в целях дать обзор современного состояния искусственного интеллекта, рассмотреть его применение в различных областях и проанализировать его этические и социальные аспекты. Обращено внимание на основные законодательные акты в Республике Казахстан, регулирующие (или затрагивающие) вопросы работы искусственного интеллекта). По результатам проведенного исследования можно сделать вывод, что искусственный интеллект имеет огромный потенциал для развития и прогресса человечества, однако требуется обеспечение контроля и баланса между его преимуществами и недостатками.

Ключевые слова: искусственный интеллект, потенциал, этические аспекты, социальные аспекты, машинное обучение, облачные вычисления, экспертные системы, робототехника, обработка естественного языка.

Өмірхан Салтанат

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

ЖАСАНДЫ ИНТЕЛЛЕКТ**Аңдатпа**

Бұл мақала жасанды интеллекттің (AI) негізгі аспектілеріне шолу және талдау болып табылады. Соңғы жылдары AI-нің дамуы айтарлықтай прогреске қол жеткізді және адам қызметінің әртүрлі салаларында кеңінен қолданылады. Мақалада жасанды интеллект құрудың әртүрлі тәсілдері, соның ішінде сараптамалық жүйелер, нейрондық желілер, генетикалық алгоритмдер, сондай-ақ терең оқыту және бұлтты есептеулер көрсетілген. Жасанды интеллект қолдану салаларына ерекше назар аударылады. Жасанды интеллектті нақты жобаларда сәтті енгізу мысалдары келтірілген, бұл оның әлеуеті мен артықшылықтарын бағалауға мүмкіндік береді. Сондай-ақ жасанды интеллект дамуының этикалық және әлеуметтік аспектілері талқыланады. Автор жасанды интеллекттің қазіргі жай-күйіне шолу жасау үшін AI автономиясы мен қауіпсіздігіне, сондай-ақ оның еңбек нарығына және жалпы қоғамға әсеріне қатысты мәселелерді егжей-тегжейлі қарастырады. әртүрлі салаларда, оның этикалық және әлеуметтік аспектілерін талдайды. Қазақстан Республикасындағы жасанды интеллект мәселелерін реттейтін (немесе қозғайтын) негізгі заңнамалық актілерге назар аударылады. Зерттеу нәтижелеріне сүйене отырып, жасанды интеллект адамзаттың дамуы мен ілгерілеуі үшін орасан зор әлеуетке ие, бірақ оның артықшылықтары мен кемшіліктері арасындағы бақылау мен тепе-теңдікті қамтамасыз ету қажет деген қорытынды жасауға болады.

Түйінді сөздер: жасанды интеллект, әлеует, этикалық аспектілер, әлеуметтік аспектілер, машиналық оқыту, бұлттық есептеулер, сараптамалық жүйелер, робототехника, табиғи тілді өңдеу.

Omirkhan Saltanat

1 year student of the Higher School of Law “Adilet”
Caspian Public University,
Republic of Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE

Annotation

This article is an overview and analysis of the main aspects of artificial intelligence (AI). The development of AI in recent years has made significant progress and is widely used in various fields of human activity. The article highlights various approaches to creating artificial intelligence, including expert systems, neural networks, genetic algorithms, as well as deep learning and cloud computing. Particular attention is paid to the areas of application of artificial intelligence. Examples of successful implementation of artificial intelligence in specific projects are given, which allows one to evaluate its potential and advantages. Ethical and social aspects of the development of artificial intelligence are also discussed. The author takes a detailed look at issues related to the autonomy and safety of AI, as well as its impact on the labor market and society as a whole, in order to provide an overview of the current state of artificial intelligence, consider its application in various fields, and analyze its ethical and social aspects. Attention is drawn to the main legislative acts in the Republic of Kazakhstan regulating (or affecting issues of artificial intelligence). Based on the results of the study, we can conclude that artificial intelligence has enormous potential for the development and progress of mankind, but it is necessary to ensure control and balance between its advantages and disadvantages.

Keywords: artificial intelligence, potential, ethical aspects, social aspects, machine learning, cloud computing, expert systems, robotics, natural language processing.

Искусственный интеллект — это одна из самых актуальных и обсуждаемых тем в современном мире. Некоторые люди считают его благом, способным принести много пользы обществу, в то время как другие опасаются его негативного влияния и потенциальных угроз. Искусственный интеллект (ИИ) — это область компьютерных наук, которая занимается созданием компьютерных систем и программ, способных имитировать интеллектуальные функции человека. Основной целью ИИ является разработка алгоритмов и методов для создания систем, способных воспринимать окружающую среду, обрабатывать информацию, принимать решения, учиться и адаптироваться к изменяющимся условиям. Эта технология делает нашу жизнь продуктивнее и освобождает нас от лишнего стресса. Разработка искусственного интеллекта продвигается более быстрыми темпами, чем предполагалось. Искусственный интеллект, вероятно, будет интегрирован практически во все отрасли и сможет решать самые насущные проблемы, такие как изменение кли-

мата, утилизация отходов, энергетический кризис, здравоохранение, безработица и даже войны. Однако технология влечет за собой и серьезные проблемы, такие как исчезновение традиционных профессий, рассекречивание конфиденциальной информации, дискриминация и поощрение человеческой лени. Необходимо осознать эти проблемы, чтобы продвигать разработку и внедрение искусственного интеллекта ответственно и этично.

Главные аспекты ИИ включают в себя:

1. Обработка естественного языка (NaturalLanguageProcessing, NLP): Этот аспект ИИ связан с разработкой систем, способных обрабатывать и понимать естественный язык, используемый человеком. Системы ИИ в области NLP используются для создания голосовых помощников, машинного перевода, обработки текстов и других приложений, связанных с обработкой языка.

2. Машинное обучение (MachineLearning, ML): Одним из основных аспектов ИИ является машинное обучение, которое позволяет системам получать опыт и улучшаться с помощью алгоритмов обучения на основе данных. Машинное обучение используется для создания систем, способных распознавать образы, принимать решения, классифицировать данные и выполнять другие задачи.

3. Компьютерное зрение (ComputerVision): Этот аспект ИИ связан с разработкой систем, способных обрабатывать и интерпретировать данные изображений и видео. Системы компьютерного зрения используются для распознавания объектов, лиц, жестов, анализа медицинских изображений и других задач.

4. Робототехника: ИИ также применяется в области робототехники, чтобы создать автономные роботы, способные взаимодействовать с окружающей средой, принимать решения и выполнять задачи. Роботы, оснащенные ИИ, используются в промышленности, медицине, автономных автомобилях и других сферах.

5. Экспертные системы: Экспертные системы – это ИИ-системы, которые используют знания и опыт экспертов в определенных областях для принятия решений. Они способны анализировать большие объемы данных и предоставлять ценную информацию и советы.

Искусственный интеллект является многогранным и быстро развивающимся полем, имеющим важное значение во многих сферах жизни, включая науку, медицину, бизнес и технологии. История искусственного интеллекта (ИИ) началась в древности с мифов, историй и слухов об искусственных существах, наделенных интеллектом или сознанием искусственных мастеров. Семена современного искусственного интеллекта были

посажены философами, которые попытались описать процесс человеческого мышления как механическую манипуляцию символами. Кульминацией этой работы стало изобретение программируемого цифрового компьютера в 1940-х годах, машины, основанной на абстрактной сути математических рассуждений. Это устройство и идеи, лежащие в его основе, вдохновили горстку ученых начать серьезное обсуждение возможности создания электронного мозга.

Есть некоторые подходы ИИ как:

Экспертные системы (ExpertSystems) – это одна из ранних и наиболее известных форм ИИ. Они основаны на предоставлении большого количества фактов и правил экспертами в определенной области, которые затем используются для решения задач и принятия решений. Экспертные системы были широко применены в медицине, финансах, инженерии и других областях.

Нейронные сети (NeuralNetworks) – это модели, инспирированные работой человеческого мозга. Они состоят из сети связанных искусственных нейронов, которые обрабатывают и передают информацию. Нейронные сети широко используются в распознавании образов, распознавании речи, обработке естественного языка и других задачах машинного обучения.

Генетические алгоритмы (GeneticAlgorithms) – это методы оптимизации и поиска, вдохновленные биологической эволюцией. Они моделируют процесс естественного отбора, применяя операции скрещивания и мутации к популяции кандидатов. Генетические алгоритмы используются для решения сложных оптимизационных задач и создания адаптивных систем.

Глубокое обучение (DeepLearning) – это подраздел машинного обучения, который использует искусственные нейронные сети с большим количеством слоев для изучения и представления сложных данных. Глубокое обучение применяется в области компьютерного зрения, обработке речи, автоматическом переводе и других задачах, где требуется высокая степень анализа и иерархического представления информации.

Облачные вычисления (CloudComputing) – это модель предоставления вычислительных ресурсов через интернет. Она играет важную роль в развитии ИИ, так как позволяет обрабатывать большие объемы данных и выполнять вычисления на удаленных серверах. Облачные вычисления позволяют распределенным системам ИИ работать с высокой производительностью и масштабируемостью.

Каждый из этих подходов имеет свои особенности и применения, и в сочетании они продвигают развитие искусственного интеллекта во многих областях науки и промышленности. В настоящее время наиболее востребованными и широко используемыми являются различные методы машинного обучения и, в частности, искусственные нейронные сети. Фактически, эти методы решают несколько конкретных задач — аппроксимация функций, классификация, кластеризация, снижение размерности и некоторые другие. Если какая-либо задача сводится к какой-либо из базовых для машинного обучения, то её можно успешно и достаточно эффективно решать этими методами. Проблема в том, что результаты, выдаваемые этими методами, сложно интерпретируются и, как следствие, их сложно объяснить. Это реальная проблема, но, к сожалению, большинство методов восходящей парадигмы обладают именно этим изъяном.

Автономность и безопасность искусственного интеллекта (ИИ) — это две важные и сложные темы в современных науках и технологиях. Влияние ИИ на рынок труда и общество также является важным аспектом, требующим глубокого рассмотрения. Автономность ИИ обозначает способность системы ИИ принимать решения и действовать без прямого участия человека. Это означает, что ИИ может обладать самообучающимися алгоритмами и способностью принимать решения на основе данных и опыта. Возможность автономного принятия решений существенно увеличивает эффективность и применимость ИИ в различных сферах, таких как здравоохранение, производство, автомобильная промышленность и другие. Однако автономность ИИ также вызывает вопросы безопасности. Когда система ИИ принимает решения без прямого контроля человека, возникает риск возникновения непредсказуемого или нежелательного поведения. Это вызывает необходимость разработки надежных механизмов обеспечения безопасности, которые гарантируют, что ИИ действует в соответствии с заданными целями и не представляет угрозу для людей или окружающей среды. Следующий важный аспект — влияние ИИ на рынок труда. Внедрение автоматизации и ИИ может привести к значительным изменениям в рабочих процессах и требуемых навыках. Некоторые работы могут быть полностью автоматизированы, что может привести к сокращению рабочих мест в некоторых секторах. Однако, в то же время, ИИ может создавать новые рабочие места, требующие специализированных навыков в области разработки и обслуживания ИИ систем. Влияние ИИ на общество также требует внимательного рассмотрения. С одной стороны, ИИ может

значительно улучшить качество жизни людей, упростить рабочие процессы и решить сложные проблемы. С другой стороны, существует риск возникновения этических и социальных проблем, таких как потеря приватности, зависимость от ИИ систем и неравенство доступа к ИИ технологиям. Поэтому необходимо разрабатывать эффективные политики и законы, чтобы контролировать и регулировать использование ИИ в соответствии с общественными интересами. Они имеют прямое влияние на рынок труда и общество, и требуют разработки эффективных стратегий и механизмов для успешной интеграции ИИ в нашу жизнь. Аспекты безопасности и социальной ответственности должны быть в центре внимания при разработке и использовании ИИ, чтобы гарантировать безопасность и благополучие для всех.

ИИ конечно же имеет свои плюсы и минусы. Их можно охарактеризовать следующим образом:

Плюсы ИИ:

1. Увеличение эффективности и продуктивности: ИИ может выполнять задачи гораздо быстрее и точнее, чем человек, что позволяет сократить время и усилить производительность в различных сферах деятельности.

2. Разработка новых технологий и инноваций: ИИ способствует созданию новых технологий и решению сложных задач, что может привести к дальнейшему прогрессу и развитию общества.

3. Улучшение качества жизни: ИИ может применяться в медицине, помогая в диагностике и лечении заболеваний. Он также может автоматизировать повседневные задачи, что позволяет людям уделять больше времени более важным и приятным делам.

4. Расширение возможностей в различных областях: ИИ может применяться в автомобильной промышленности, финансовом секторе, робототехнике, науке, образовании и многих других сферах, улучшая работу и способствуя новым открытиям.

Минусы ИИ:

1. Потеря рабочих мест: Автоматизация и внедрение ИИ могут привести к сокращению рабочих мест в некоторых отраслях, поскольку многие задачи могут быть выполнены машинами или программами.

2. Этические проблемы: Возникновение сложных этических вопросов, связанных с использованием ИИ, например, вопросы конфиденциальности данных, непредсказуемого поведения автономных систем и возможности злоупотребления технологией.

3. Несовершенство и ограниченность: В настоящее время ИИ не обладает полным сознанием и интуицией, а также подвержен ошибкам,

особенно в ситуациях, на которые он не был обучен. Это может вызывать определенные риски и проблемы, особенно в случае автономных систем.

4. Зависимость от ИИ: Существует риск, что люди станут слишком зависимы от ИИ и потеряют некоторые навыки и способности, так как расчеты и решения будут делаться за них.

Одним из главных аргументов в пользу искусственного интеллекта является его потенциал изменить мир к лучшему. С развитием этой технологии возможности человечества становятся практически неограниченными. ИИ может помочь в решении сложных задач, улучшить медицину и образование, упростить повседневную жизнь людей. С другой стороны, с развитием искусственного интеллекта возникают опасения. Некоторые боятся, что он может заменить людей во многих сферах работы, что приведет к потере рабочих мест. Кроме того, существует опасность, что искусственный интеллект может стать слишком развитым и начать контролировать нашу жизнь. Возникают этические вопросы, связанные с приватностью и безопасностью данных, а также с возможностью злоупотребления искусственным интеллектом для вредоносных целей. С положительной стороны, системы на основе ИИ могут значительно повысить эффективность, обрабатывая и анализируя большие объемы данных быстро. Это позволяет принимать более быстрые решения и увеличивает производительность в различных отраслях. Например, ИИ показал свою способность сокращать время ожидания мест в больничных палатах на час, что человеку заняло бы дни или недели. Однако главная проблема с ИИ заключается в вопросе этики. Forbes подчеркивает, что ИИ является чисто логическим и принимает решения на основе заранее заданных параметров, оставляя мало места для нюансов и эмоций. Это затрудняет учет этических аспектов в алгоритмах. ИИ известен своей неспособностью улавливать нематериальные человеческие факторы, которые являются неотъемлемой частью принятия решений в реальной жизни, такие как этика и мораль. Еще одним потенциальным преимуществом ИИ является то, что он может освободить больше свободного времени для общества, беря на себя все больше задач. Некоторые эксперты предсказывают, что люди постепенно будут выбирать более короткий рабочий день и больше свободного времени, поскольку ИИ автоматизирует задачи. Это может привести к тому, что более короткий рабочий день и рабочая неделя станут нормой, с тремя выходными днями. Однако развитие ИИ также вызывает опасения относительно потери рабочих мест. Автоматизация, привнесенная ИИ,

может вытеснить значительную часть рабочей силы, особенно в рутинных и легко автоматизируемых задачах. Одно исследование оценивает, что около 15% работников, или 400 миллионов человек по всему миру, могут потерять работу из-за ИИ в период с 2016 по 2030 год. ИИ также имеет потенциал для содействия научным открытиям путем автоматизации анализа данных. Он уже способствовал значительным прогрессам в здравоохранении, помогая в диагностике рака. Например, программа ИИ под названием AlphaFold может предсказывать структуру белка на основе последовательности его аминокислот, что может существенно помочь в поиске и разработке лекарств. Однако еще одной проблемой является монополизация власти несколькими крупными технологическими гигантами. Уже существуют опасения относительно мощи многонациональных компаний, и ИИ может способствовать дальнейшей централизации власти в их руках. Поскольку отрасль ИИ естественным путем стремится к монополизации, возникают опасения по поводу растущей силы крупных технологических компаний. В целом, ИИ представляет собой мощный инструмент, который может значительно улучшить качество жизни людей и привести к прогрессу во многих отраслях. Однако, необходимо тщательно рассмотреть его использование с точки зрения этики, безопасности и социальных последствий.

Какими правовыми актами регулируется искусственный в Республике Казахстан?

На сегодняшний день, основными законодательными актами, регулирующими (или затрагивающими вопросы работы искусственного интеллекта) являются:

1. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» является основным законодательным актом, регулирующим сферу информатизации и использования информационных технологий в стране. Хотя данный закон не упоминает искусственный интеллект (ИИ) явно, некоторые положения могут быть применимы и к регулированию ИИ.

2. Закон «О персональных данных и их защите» от 21 мая 2013 года, регулирует сбор, хранение, использование и передачу персональных данных, включая данные, используемые в контексте искусственного интеллекта.

3. Закон «Об авторском праве и смежных правах» от 10 июня 1996 года устанавливает права и ответственность владельцев авторских прав в контексте использования ИИ для создания, обработки или распространения авторских произведений. Но следует отметить, будет ли являться

объектом авторского права произведение, созданное искусственным интеллектом? Как известно, в соответствии с указанным Законом, автором является физическое лицо, творческим трудом которого создано произведение науки, литературы, искусства. На данный момент, этот вопрос еще не урегулирован законодательством не только Республики Казахстан, но и законами иных стран.

4. Закон Республики Казахстан от 25 июня 2020 года № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» является одним из ключевых законодательных актов, направленных на регулирование цифровых технологий и развитие цифровой экономики в Казахстане. Этот закон вносит изменения и дополнения в несколько существующих законодательных актов страны с целью обеспечения юридической основы для развития и регулирования цифровых технологий.

Ниже приведены некоторые ключевые аспекты, которые могут быть охвачены указанным законом:

i. Электронные документы и электронная подпись: Закон вносит изменения в Закон Республики Казахстан “Об электронном документе и электронной подписи” для усиления правовой защиты и признания электронных документов и электронных подписей.

ii. Криптовалюты и блокчейн: Закон внес изменения в некоторые законы, связанные с криптовалютами, виртуальными активами и блокчейн-технологиями, чтобы создать правовую основу для их использования и регулирования.

iii. Защита персональных данных: Закон вносит изменения в Закон Республики Казахстан “О персональных данных” с целью усиления защиты персональных данных и обеспечения их безопасности при использовании цифровых технологий.

iv. Кибербезопасность: Закон также может включать положения, касающиеся кибербезопасности и защиты информационных систем от киберугроз и кибератак.

Особое внимание стоит уделить предложению Министерства цифрового развития, инноваций и аэрокосмической промышленности РК о разработке цифрового кодекса, включающего в себя все положения и институты, связанные с информационными технологиями, цифровизацией и искусственным интеллектом в Республике Казахстан. Тем самым, данный кодекс должен объединить и кодифицировать в себе все вышеуказанные законы и иные акты, регулирующие вопросы ИИ. Пред-

полагается не только объединение и сбор всех актов в один кодекс, но и внедрение институтов регулирования цифровых технологий в аспекте глобализации и развития общества на сегодняшний момент и будущее. Однако, принятие такого кодекса не должно затрагивать положения иных законодательных актов, таких как Гражданский кодекс, в первую очередь.

В заключение, искусственный интеллект имеет свои преимущества и недостатки. Он может значительно улучшить нашу жизнь, но также вызывает опасения и требует ответственного подхода. Важно продолжать исследования и развитие ИИ, соблюдая этические принципы и учитывая интересы общества в целом. И учесть, что развитие искусственного интеллекта должно происходить с осознанием этих рисков и с участием общества. Необходимо установить этические и правовые рамки, чтобы предотвратить злоупотребления и негативные последствия использования ИИ.

Список использованных источников:

- <https://adilet.zan.kz/rus/docs/Z1500000418>
- <https://adilet.zan.kz/rus/docs/Z1500000418>
- <https://online.zakon.kz/m/amp/document/1005798>
- <https://adilet.zan.kz/rus/archive/docs/Z2000000347/25.06.2020>

ӘОЖ 349

Райымбекқызы Арай

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 3 курс студенті,
Қазақстан Республикасы, Алматы қ.

Ғылыми жетекші:

Мақсатов Н.Р.

з.ғ.м., Каспий қоғамдық университеті «Әділет» Жоғары
құқық мектебінің сеньор-лекторы

КИБЕРҚЫЛМЫС:

ТҮСІНІГІ, ТҮРЛЕРІ ЖӘНЕ ҚОРҒАНУ ӘДІСТЕРІ

Аңдатпа

Автор өз зерттеулерінде әлемдегі кибертерроризм мен киберқылмыстылыққа назар аударады. Қазіргі уақытта киберқылмыстылық тұрақты дамып келе жатқаны және жеке тұлғалардың да, тұтас мемлекеттердің де ақпараттық қауіпсіздігіне қауіп төндіретіні атап өтілді. Мақалада киберқылмыстылық, кибертерроризм, киберқылмыс ұғымдары мен ерекшеліктері, сонымен қатар киберқауіпсіздік түсінігі қарастырылып, олардың түрлері, мақсаттары мен міндеттері жан-жақты қарастырылған. Мақаланы жазу барысында ақпараттық технологияның дамуына байланысты қылмыскерлердің интернет арқылы жасаған қылмыс түрлері анықталды. Киберқылмыстың екі жағдайда да пайда табу мақсатын көздейтін алаяқтық, арбау шарттарды ұсыну арқылы жасалатыны атап өтілген. Автор осы саладағы құқықтық реттеу мәселелеріне назар аударып, туындаған мәселелерді шешу жолдарын ұсынады.

Түйінді сөздер: киберқылмыс, интернет, компьютерлік жүйе, қауіпсіздік, ақпарат, технология, фишинг, жеке деректерді ұрлау, қаржылық алаяқтық, кибертерроризм.

Райымбекқызы Арай

студентка 3 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

КИБЕРПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ВИДЫ И МЕТОДЫ ЗАЩИТЫ

Аннотация

Автором обращено внимание в своем исследовании на кибертерроризм и киберпреступность в мире. Отмечается, что киберпреступность получила неуклонное развитие в настоящее время и порождает опасность для информационной безопасности как отдельных лиц, так и целых государств. В статье изложены понятия и особенности киберпреступности, кибертерроризма, киберпреступлений, а также понятие кибербезопасности, подробно рассмотрены их виды, цели и задачи. В ходе написания статьи были выявлены такие виды преступлений, как совершаемые преступниками через интернет в связи с развитием информационных технологий. Обращено внимание, что киберпреступления совершаются путем мошенничества, путем предложения соблазни-

тельных условий, преследуя в обоих случаях цель извлечения прибыли. Автор обращает внимание на проблемы правового регулирования в данной сфере и предлагает пути решения возникающих проблем.

Ключевые слова: киберпреступность, интернет, компьютерная система, безопасность, информация, технологии, фишинг, кража личных данных, финансовое мошенничество, кибертерроризм.

Raiymbekkyzy Arai

3 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

CYBERCRIME: THE CONCEPT, TYPES AND METHODS OF PROTECTION

Annotation

The author draws attention in his research to cyberterrorism and cybercrime in the world. It is noted that cybercrime has developed steadily at present and poses a danger to the information security of both individuals and entire states. The article outlines the concepts and features of cybercrime, cyberterrorism, cybercrime, as well as the concept of cybersecurity, and discusses their types, goals and objectives in detail. In the course of writing the article, such types of crimes as those committed by criminals via the Internet in connection with the development of information technology were identified. It is noted that cybercrimes are committed through fraud, by offering tempting conditions, in both cases pursuing the goal of making a profit. The author draws attention to the problems of legal regulation in this area and suggests ways to solve emerging problems.

Keywords: cybercrime, Internet, computer system, security, information, technology, phishing, identity theft, financial fraud, cyberterrorism.

Киберқылмыс пен кибертерроризмнің түсінігі мен ерекшеліктері

Киберқылмыс құбылыс ретінде бірнеше онжылдықтар бұрын пайда болған, бірақ ақпараттық технологиялардың дамуымен қысқа уақыт ішінде киберкеңістіктегі заңсыз әрекеттер құбылысы жаһандық проблемаға айналып, жекелеген пайдаланушыларға ғана емес, сонымен бірге бүкіл мемлекеттердің ақпараттық қауіпсіздігіне қауіп төндірді. Мемлекет интернет желісі арқылы ақпарат алмасуға енгізілген сәттен бастап, оның өзі және оның азаматтары жер шарының кез-келген жерінен қол сұғушылыққа осал болады.

“Киберқылмыс” терминінің мағынасын киберкеңістікте жасалған қылмыс ретінде анықтауға болады. Киберкеңістік интернет желісі арқылы кеңейетін кейбір ақпаратты сақтайтын компьютерлік желілерді тарту арқылы модельденетін виртуалды ақпараттық кеңістік ретінде қарастырылады. Киберқылмысқа қарсы қорғаныс шараларын қолдану бұл анықтаманың мағынасын түсінбестен мүмкін болмағандықтан, зерттеушілер бұл құбылысты егжей-тегжейлі қарастырып, оған қызықты анықтама берді. Киберқылмыс-бұл компьютерлік жүйелерді немесе желілерді қолдана отырып, киберкеңістікте жасалатын қылмыстар кешені.

Кибертерроризм-бұл компьютермен және компьютерлік жүйелермен өңделген ақпаратқа қасақана, саяси негізделген шабуылда көрініс табатын, адамдардың өміріне немесе денсаулығына қауіп төндіретін немесе егер мұндай әрекеттер қоғамдық қауіпсіздікті бұзу, халықты қорқыту, әскери қақтығысты арандату мақсатында жасалса, басқа да ауыр зардаптардың туындауына әкелетін кешенді әрекет.[1]

Осылайша, қазіргі уақытта кибертерроризм қауіпі өте маңызды мәселе болып табылады. Ақпараттық-телекоммуникациялық технологиялардың дамуы мен таралуына байланысты оның өзектілігі артады.

Киберқауіпсіздік: түсінігі, міндеттері, мақсаттары

Киберқауіпсіздік қазіргі әлемдегі ең маңызды тақырыптардың бірі болып табылады. Бірақ алдымен көптеген адамдар шатастыратын киберқауіпсіздік және ақпараттық қауіпсіздік ұғымдарын бөлу керек. Ең алдымен, киберқауіпсіздік, ақпараттық қауіпсіздіктің ішкі жиынтығы болып табылады.

Ақпараттық қауіпсіздік-бұл “деректерді қорғау”деп айтудың басқа әдісі. Бүгінгі таңда көптеген компаниялар деректерді серверлерде, жұмыс үстелдерінде, ноутбуктерде немесе интернеттің кез-келген жерінде сақтайды. Ақпараттық қауіпсіздіктің негізгі міндеті-деректерді кез-келген түрде қорғау және сақтау және бұл киберқауіпсіздікке қарағанда кеңірек.[2]

Киберқауіпсіздік-бұл электронды түрде орналасқан деректерді қорғау. Сондай-ақ, ең маңызды деректерді анықтайды яғни, олар қайда орналастырылады және оларды қорғау үшін қандай технологияларды қолдану керек.[2]

Киберқауіпсіздікті пайдаланушылар мен ұйымдардың ерекше назарында соңғы жеті жылдағы деректер қауіпсіздігі компаниялардың IT бөлімшелерінің бірінші кезектегі міндеттерінің бірі болып табылады. Сонымен қатар, осы салада қолданылатын ұғымдар мен термин-

дер қарапайым пайдаланушыларға әрдайым таныс және түсінікті бола бермейді.

Жеке өмірге қол сұғумен байланысты киберқылмыстар

Мұндай киберқылмыстардың бірнеше түрі бар, олардың мақсаты жеке құпия ақпаратты ұрлау болып табылады. Көбінесе шабуылдаушыларды терең мотивация, жеке құпия ақпаратты қорғайтын технологиялардағы олқылықтарды табуға бағытталған.

Жеке деректерді ұрлау

Жеке ақпаратты ұрлау әдетте адамның немесе адамдар тобының жеке басына қатысты мақсатта орын алады. Кейбір зиянкестер жеке тұлғаны атын жамылу үшін төлқұжаттарды немесе басқа жеке куәліктерді ұрласа, ал жеке басының деректерін ұрлау тек интернет арқылы болады. Мысалы, банктік несие алғысы келетін адам, несиесі бар адамның жеке ақпаратын ұрлауы мүмкін.

Авторлық құқықты бұзу

Авторлық құқықты бұзу-киберқылмыстың ең көп таралған түрлерінің бірі. Ең алдымен, бұл санатқа авторлардың келісімінсіз музыканы, фотосуреттерді, фильмдерді, кітаптарды және т.б. ортақ пайдалану кіреді [3].

Жеккөрушілік пен қудалау қылмыстары

Жеке адамға немесе адамдар тобына қатысты жеккөрушілік қылмыстары әдетте гендерлік, нәсілдік, діни, ұлттық жыныстық бағдар және басқа белгілер негізінде жасалады. Мысалдар: қудалау және қорлайтын хабарламалар жіберу және белгілі бір адамдар тобына қатысты жалған жаңалықтар жіберу. Интернеттің анонимділігі мен қол жетімділігі жеккөрушілік қылмыстарымен күресуді қиындатады.

Кибербуллинг

Жеке тұлғаларды қудалау, қорлау және қорқыту үшін компьютерлер мен жалғанған құрылғыларды пайдалану кибербуллинг санатына жатады. Кибербуллинг пен жеккөрушілік қылмыстардың кейбір түрлері арасындағы шекара жиі бұлыңғыр болады. Кибербуллингтің кейбір түрлері (мысалы, жалаңаш фотосуреттер) заңсыз әрекеттерге ұшырауы мүмкін (мысалы, балаларды қанау) [3].

Интернет-өзін-өзі реттеу және өзін-өзі қамтамасыз ету принципіне негізделген ғаламдық компьютерлік желі. Жаһандық ақпараттық технологиялар киберқылмыскерге оның қылмыстық жоспарларын жүзеге асыру үшін беретін мүмкіндіктері өте көп[5].

Соның бірі, анонимділік, көбінесе ғаламдық желідегі пайдаланушылардың байланыс ерекшеліктерін анықтайды. Бұл жағдайда жеке-визуалды байланыс болмайды, яғни виртуалды

кеңістікте назардан тыс қалғысы келетін адамның жеке басын анықтау мүмкін емес. Мобильді интернет технологиясы қылмыскерге әртүрлі тәсілдерді пайдаланып кеңістікте еркін қозғалуға мүмкіндік береді. Кез-келген операциялардың жеделдігі бүкіл интернет кеңістігіне таралады, елдер мен континенттерді қамтиды, осылайша проблеманың жаһандануына ие болады. Айтпа кеткенде ІТ технологиясының дамуына байланысты барлық нәрсе киберқылмыс жасауға негіз болып табылады.

Киберқылмыстың таралу себептері.

Қылмыстық іс-әрекетті сәтті жүргізуге мүмкіндік беретін заманауи желілік технологиялардың ерекшеліктері, соның бірі ақпараттық ІТ-технологияларды дамыту және жетілдіру.

Қауіпсіздік шараларының компьютерлік технологиялардың даму деңгейінен үнемі артта қалуы. Ақпараттық қауіпсіздік тұжырымдамасының әлсіз пысықталуы.

Киберқылмысты реттеу әрекеттері

Киберқылмыстардың ішінде кейбір қылмыс түрлері қазақстандық қылмыстық заңнамасында бекітілген, атап айтқанда, ҚР Қылмыстық Кодексінің 198-бабы. Осы бап «Авторлық және (немесе) сабақтас құқықтарды бұзу» деп аталады. Онда делінген:

1. Авторлық және (немесе) сабақтас құқықтар объектілерін заңсыз пайдалану, сол сияқты авторлық құқық және (немесе) сабақтас құқықтар объектілерінің контрафактілік даналарын өткізу мақсатында иемдену, сақтау, алып өту немесе дайындау не авторлықты иемденіп алу немесе тең авторлыққа мәжбүрлеу –

сексен айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не сексен сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға жазаланады.

2. Дәл сол іс-әрекеттер, егер олар айтарлықтай мөлшерде жасалса немесе айтарлықтай залал не автордың немесе өзге құқық иеленушінің құқықтарына немесе заңды мүдделеріне елеулі зиян келтірсе не бірнеше рет жасалса, –

бір жүз алпыс айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір жүз алпыс сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не қырық тәулікке дейінгі мерзімге қамаққа алуға жазаланады.

3. Осы баптың екінші бөлігінде көзделген:

- 1) адамдар тобының алдын ала сөз байласуымен;
- 2) ірі мөлшерде жасалған немесе ірі залал келтірген;

3) адам өзінің қызмет бабын пайдалана отырып жасаған іс-әрекеттер – белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, бес мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір мың екі жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не бес жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

4. Осы баптың екінші немесе үшінші бөліктерінде көзделген, қылмыстық топ жасаған іс-әрекеттер –

үш жылдан алты жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады [4].

Келесі бап - 274-бап. Көрінеу жалған ақпарат тарату. Онда көрсетілген:

1. Қоғамдық тәртіпті бұзу немесе азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделеріне не қоғамның немесе мемлекеттің заңмен қорғалатын мүдделеріне елеулі зиян келтіру қаупін төндіретін көрінеу жалған ақпарат тарату –

бір мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не төрт жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не бір жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

2. Мынадай:

1) адамдар тобының алдын ала сөз байласуымен;

2) адам өзінің қызмет бабын пайдалана отырып;

3) бұқаралық ақпарат құралдарын, телекоммуникация желілерін және онлайн-платформаларды пайдалана отырып жасалған дәл сол іс-әрекет –

үш мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не сегіз жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не үш жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

3. Осы баптың бірінші немесе екінші бөліктерінде көзделген, азаматқа, ұйымға немесе мемлекетке ірі залал келтіруге немесе өзге де ауыр зардаптарға әкеп соққан іс-әрекеттер –

бес мың айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзеу жұмыстарына не бір мың екі жүз сағатқа дейінгі

мерзімге қоғамдық жұмыстарға тартуға не бес жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

4. Осы баптың бірінші, екінші немесе үшінші бөліктерінде көзделген:

1) қылмыстық топ жасаған;

2) төтенше жағдай кезінде немесе ұрыс жағдайында немесе соғыс уақытында не жария іс-шаралар өткізу кезінде жасалған іс-әрекеттер – үш жылдан жеті жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады[4].

Сонымен қатар, бұқаралық ақпарат құралдары туралы заңында кейбір қылмыстарға қатысты жазалар көзделе кеткен.

Осыған байланысты айта кететіміз, киберқылмыстарының кейбір түрлеріне, мысалға алғанда, кибербуллингке, спам, фишинг сияқты киберқылмыс түрлеріне жаза көзделмеген.

Құқықтық реттеу саласындағы кемшіліктер.

Қылмыстық, азаматтық және әкімшілік заңнаманы қоса алғанда, компьютерлік технологияларға қатысты мәселелерді реттейтін жетілмеген заңнама. Сонымен қатар, киберқылмыстарға тереңдетілген заңнаманың болмағандығынан, анонимдік тұрғыдан және басқа да әрекеттер арқылы жасалатын қылмыстар жазасыз қалып жатыр. Осы әрекеттерге қатысты заңнаманың жоқтығы, азаматтардың алданып қалуына сонымен қатар зардап шегуіне әкеліп соғып жатыр.

Жұмыстың соңында мен бірнеше практикалық ұсыныстарды ұсынамыз. Біз пайдаланушыларға интернеттің мүмкіндіктеріне, ең бастысы, виртуалды кеңістіктің ерекшеліктеріне қатысты білімдерін кеңейтуге кеңес берер едік. Сол білімнің аздығының арқасында ақпаратсыз интернет пайдаланушысы киберқылмыскерлерге осал болып шығады. Азаматтарды киберқылмыскерлердің негізгі әдістері туралы хабардар ету қажет. Сол түрдегі ақпараттарды БАҚ-да үнемі жариялануы керек. Азаматтардың құқықтық мәдениетінің деңгейін арттыру қажет. Құқықтық реттеу саласындағы кемшіліктерді жою, киберқылмыстар үшін жазаларды қатаңдату және компьютерлік ақпарат саласындағы қылмыстарды анықтау үшін қылмыстың алдын алу жүйесінен тыс дер-бес ведомстволар құру.

Мысалға алатын болсақ, киберқылмыстардың ішінде авторлық құқықты бұзу, жеке деректерге қол сұғу тағы да басқалар сияқты қылмыс түрлеріне және ҚР Қылмыстық кодексінің 7-тарауында ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар туралы

қысқаша айтыла өткен [4]. Бірақ-та осы киберқылмыстар қазіргі таңда өршіп тұрғандықтан, оның шектелуіне немесе жасалған қылмыстарға жаза ретінде қолданылатын қандай да бір киберқылмыстарға қарсы жеке заңнаманың болғаны жөн деп санаймын.

Пайдаланылған қайнар көздерінің тізімі:

1. Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – 104-106 с.
2. Касперский: Киберпреступность. Режим доступа: <https://www.kaspersky.ru/resource-center/threats/cybercrime>
3. «Киберпреступления: понятие, виды и методы защиты». <https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html>
4. Қазақстан Республикасының Кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ.
5. Зайцев О. Мошенничество в Интернете и защита от него // КомпьютерПресс. – 2018. – № 7. – С.140.

ӘОЖ 347

Рақым Әділет Бағдатұлы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,

Қазақстан Республикасы, Алматы қ.

МЕМЛЕКЕТТІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ

Аңдатпа

Мақалада «Ақпараттық қауіпсіздік» түсінігі және оның қазіргі кезеңдегі өзектілігі қарастырылып, ақпарат пен киберкеңістікте туындайтын проблемалар зерттеледі. Автор интернеттегі алаяқтықтың алдын алу мәселелеріне, сондай-ақ отандық ақпараттық кеңістікте шетелдік телеарналарды көрсету проблемаларына назар аударады. Қазақстан Республикасында ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері қарастырылған.

Түйінді сөздер: мемлекет, ақпарат, ақпараттық қауіпсіздік, интернет-алаяқтық, Отандық телеканал, мемлекеттік саясат.

Рақым Әділет Бағдатұлы

студент 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВА**Аннотация**

В статье рассмотрено понятие «Информационная безопасность» и его актуальность на современном этапе, изучены проблемы возникающие в информационном и киберпространстве. Автором обращено внимание на проблемы предотвращения мошенничества в интернет а также проблемы вещания зарубежных телеканалов в отечественном информационном пространстве. Рассмотрены цели и задачи обеспечения информационной безопасности в Республике Казахстан.

Ключевые слова: государство, информация, информационная безопасность, интернет-мошенничество, Национальный телеканал, государственная политика.

Rakym Adilet

1 year student of the Higher School of Law «Adilet»

Caspian Public University,

Republic of Kazakhstan, Almaty

STATE INFORMATION SECURITY**Annotation**

The article discusses the concept of “Information security” and its relevance at the present stage, and studies the problems arising in information and cyberspace. The author draws attention to the problems of preventing fraud on the Internet as well as the problems of broadcasting foreign TV channels in the domestic information space. The goals and objectives of ensuring information security in the Republic of Kazakhstan are considered.

Keywords: state, information, information security, Internet fraud, National TV channel, state policy.

Қауіпсіздік — жеке адамның, қоғамның, мемлекеттің өмірлік маңызды мүдделерінің ішкі және сыртқы қатерден қорғалуы.

Ақпараттық қауіпсіздік — мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі.

Ақпарат – информация. Мемлекеттің ақпараттық қауіпсіздігі қазіргі таңдағы өзекті мәселенің бірі. Себебі, ол мемлекет қарамағындағы азаматтардың ақпаратты қабылдауына тікелей, бірден-бір әсер етеді. Сол үшін осы жағдайға басым мән беру керек.

Бәрімізге мәлім, бүгінгі күні еліміздің ақпараттық қауіпсіздігі жағдайы мәз емес. Алысқа бармай ақ, мысал қылып теледидар арқылы қабылдайтын ақпаратты алсақ болады. Біздің отандық телеканалдардың арасында Ресей Федерациясының каналдары бар (Мир24). Ол жерде бізге қатысы жоқ, теріс ақпарат болуы мүмкін. Тағы бір мысал қылып, әлеуметтік желідегі жабық сайттарды алса болады.

Қазір ең ауыр мәселенің бірі – ол интернет арқылы алаяқтық жасау. Бұл қылмыс жайында Қылмыстық кодекстің 190- бабының 2 бөлімінде жазылған. Бұндай Қылмыс жасаған тұлғаға 3 жылдан 7 жылға дейін бас бостандығынан айырады. Бірақ, соның өзінде бұл өршіп тұрған жағдайға алып келуде. Зиянкестер құпия деректерді алудың және компанияға шығын келтірудің жаңа жолдарын іздейді. Мекемені ақша мен зияткерлік меншікті жоғалтудан қорғау үшін ақпараттық қауіпсіздікке көбірек көңіл бөлу керек. Бұл алдыңғы қатарлы технологиялар арқылы ақпаратты қорғау құралдарының арқасында мүмкін болады.

Сол себепті, еліміздегі ақпараттық қауіпсіздік мәселесін жиі көтеріп, қайта қарау қажет деп ойлаймыз.

Осы мәселе жөнінде 2006 жылы 10 қазанда «Қазақстан Республикасының ақпараттық қауіпсіздігі тұжырымдамасы туралы» заң шығарылған болатын.

Осы заңның жалпы ережелеріне келетін болсақ, сонда Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы (бұдан әрі - Тұжырымдама) Қазақстан Республикасы Конституциясының және «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» 1998 жылғы 26 маусымдағы, «Мемлекеттік құпиялар туралы» 1999 жылғы 15 наурыздағы, «Терроризмге қарсы күрес туралы» 1999 жылғы 13 шілдедегі, «Электрондық құжат және электрондық цифрлық қолтаңба туралы» 2003 жылғы 7 қаңтардағы, «Ақпараттандыру туралы» 2003 жылғы 8 мамырдағы, «Экстремизмге қарсы іс-қимыл туралы» 2005 жылғы 18 ақпандағы Қазақстан Республикасы заңдарының, Қазақстан Республикасы Президентінің 2006 жылғы 18 тамыздағы N 163 Жарлығымен мақұлданған Қазақстан Республикасы ақпараттық

кеңістігінің бәсекеге қабілеттілігін дамытудың 2006-2009 жылдарға арналған тұжырымдамасының негізінде әзірленді.

Сондай-ақ Тұжырымдаманы әзірлеу кезінде ақпараттық қауіпсіздік саласындағы халықаралық тәжірибе және 1999 жылғы 4 шілдедегі Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің әскери саладағы ақпараттық қауіпсіздік тұжырымдамасының ережелері ескерілді.

Тұжырымдама ақпараттық қауіпсіздікті қамтамасыз ету саласында Қазақстан Республикасының бірыңғай мемлекеттік саясатын қалыптастыру мен іске асыру кезінде негіз болып қызмет етеді, оның ережелері Қазақстанның бірыңғай ақпараттық кеңістігін құру мен дамыту және ақпараттандыру саласында мемлекеттік саясатты одан әрі жетілдіру кезінде ескерілетін болады.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету саласындағы мемлекеттік саясат (бұдан әрі - мемлекеттік саясат) ашық болып табылады және Қазақстан Республикасының қолданыстағы заңнамалық актілерінде көзделген шектеулерді ескере отырып, қоғамның мемлекеттік органдар мен қоғамдық институттардың ақпараттық қауіпсіздік саласындағы қызметі туралы хабардар болуын көздейді. Ол жеке және заңды тұлғалардың кез келген заңды тәсілмен ақпаратты еркін жасауға, іздестіруге, алуға және таратуға құқықтарын қамтамасыз етуге негізделеді.

Мемлекет ақпараттық ресурстар меншік объектісі болып табылатынын, және ақпараттық ресурстардың меншік иелерінің, иелерінің және өкімдік етушілерінің заңды мүдделері сақталған жағдайда оларды шаруашылық айналымға енгізуге ықпал ететінін негізге алады.

Мемлекет ұлттық телекоммуникациялық желілер құруды және халықаралық ақпарат алмасуды қамтамасыз етуге қабілетті қазіргі заманғы ақпараттық және телекоммуникациялық технологияларды және техникалық құралдарды дамытуды басым деп санайды.

Мемлекеттік саясат, мемлекеттік құпияларды қорғау саласын қоспағанда, мемлекеттік органдар мен ұйымдардың ақпараттық қауіпсіздікті қамтамасыз ету саласындағы монополиясына жол бермейді.

Дегенмен, 2011 жылы 11 сәуірде Экс-Президент жарлығымен бұл заң күшін жойған болатын.

Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен міндеттері

Ақпараттық қауіпсіздікті қамтамасыз етудің *негізгі мақсаттары:*

ақпарат қорғаудың ұлттық жүйесін, оның ішінде мемлекеттік ақпараттық ресурстарды құру және нығайту;

мемлекеттік ақпараттық ресурстарды, сондай-ақ ақпарат саласында адам құқықтары мен қоғам мүдделерін қорғау;

Қазақстанның ақпараттық тәуелділігін, басқа мемлекеттер тарапынан ақпараттық өктемдікті немесе тосқауылды, Президенттің, Парламенттің, Үкіметтің және басқа да мемлекеттік органдар мен ұйымдардың ақпараттық оқшаулануын төмендету немесе оған жол бермеу болып табылады.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі *негізгі міндеттер*:

ақпараттық қауіпсіздік саласында ұлттық заңнаманы жетілдіру;

ақпараттық қауіпсіздік қатерлерінің көздерін анықтау, бағалау, болжау, қорғалатын объектілердің барлауға қолжетімділік өлшемдерін айқындау;

ақпараттық қауіпсіздіктің мемлекеттік саясатын қамтамасыз етудің, іс-шаралар кешенін және оларды іске асыру әдістерін әзірлеу;

ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік органдар мен ұйымдардың қызметін құқықтық реттеу және үйлестіру;

ақпараттық қауіпсіздікті қамтамасыз ету жүйесін дамыту, оны ұйымдастыруды, нысандарын, әдістерін және ақпараттық қауіпсіздік қатерлерін бейтараптау құралдарын, оны бұзу зардаптарын жоюды жетілдіру;

Қазақстанның жанандық ақпараттық желілер мен жүйелерді құру және пайдалану процестеріне белсенді қатысуын қамтамасыз ету;

техникалық барлауларға қарсы іс-әрекет ету жөніндегі нормативтік құқықтық және әдістемелік базаны әзірлеу және жетілдіру жолымен техникалық барлауларға қарсы іс-қимыл жасау жүйесін құру болып табылады.

Пайдаланылған қайнар көздерінің тізімі:

1. https://adilet.zan.kz/kaz/docs/U060000199_
2. https://kk.m.wikipedia.org/wiki/%D0%90%D2%9B%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D1%82%D1%8B%D2%9B_%D2%9B%D0%B0%D1%83%D1%96%D0%BF%D1%81%D1%96%D0%B7%D0%B4%D1%96%D0%BA
3. <https://egi.edu.kz/kk/a-paratty-auipsizdik/>
4. <https://bilimger.kz/135240/>
5. <https://www.gov.kz/memleket/entities/kostanai-usunkol-audany-akimat/press/news/details/200689?lang=kk>

УДК 349.2

Рзыкпаева Далара Жанатовна

студентка 2 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

**ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
И ЕГО ВЛИЯНИЕ НА ТРУДОВЫЕ ОТНОШЕНИЯ:
ПЕРСПЕКТИВЫ И РИСКИ****Аннотация**

Данная статья посвящена вопросам влияния искусственного интеллекта на трудовые отношения. Рассмотрены перспективы и риски данного направления. Автор исследовал последние изменения в действующем трудовом законодательстве. Автором обращается внимание на то, что искусственный интеллект открывает новые возможности в регулировании трудовых отношений, однако порождает и важные вопросы, как пример этические вопросы и обеспечение безопасности данных, которые нужно тщательно изучать и обсуждать, чтобы обеспечить наиболее благоприятное использование ИИ для достижения целей и удовлетворения потребностей.

Ключевые слова: искусственный интеллект, работник, работодатель, перспективы, законодательство

Рзыкпаева Далара Жанатовна

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 2 курс студенті,

Қазақстан Республикасы, Алматы қ.

**ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ОНЫҢ ЕҢБЕК ҚАТЫНАСТАРЫНА ӘСЕРІ:
ПЕРСПЕКТИВАЛАР МЕН ТӘУЕКЕЛДЕР****Аңдатпа**

Бұл мақала жасанды интеллекттің еңбек қатынастарына әсеріне арналған. Бұл бағыттың келешегі мен тәуекелдері қарастырылады. Автор қазіргі еңбек заңнамасындағы соңғы өзгерістерді қарастырды. Автор

жасанды интеллект еңбек қатынастарды реттеуде жаңа мүмкіндіктер ашатынына назар аударады, сонымен бірге этикалық мәселелер мен деректердің қауіпсіздігін қамтамасыз ету сияқты маңызды сұрақтарды көтереді, бұл мәселені барынша қамтамасыз ету үшін мұқият зерттеп, талқылауды қажет етеді, бұл мақсаттарға жету және қажеттіліктерді қанағаттандыру үшін AI-ны қолайлы пайдалануға мүмкіндігін ашады.

Түйінді сөздер: жасанды интеллект, қызметкер, жұмыс беруші, перспективалар, заңнама.

Rzykpayeva Dalara

3 year student of the Higher School of Law «Adilet»

Caspian Public University,

Republic of Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON LABOR RELATIONS: PROSPECTS AND RISKS

Annotation

This article is devoted to the impact of artificial intelligence on labor relations. The prospects and risks of this direction are considered. The author examined the latest changes in current labor legislation. The author draws attention to the fact that artificial intelligence opens up new opportunities in the regulation of ore relations, but also raises important questions, such as ethical issues and ensuring data security, which need to be carefully studied and discussed in order to ensure the most favorable use of AI to achieve goals and satisfaction needs.

Keywords: artificial intelligence, employee, employer, prospects, legislation

Искусственный интеллект (ИИ) - это область компьютерных наук и технологии, которая стремится создать компьютерные системы, способные выполнять задачи, требующие человеческого интеллекта. В современности ИИ охватывает широкий спектр технологий и методов, которые позволяют компьютерным системам обучаться, анализировать данные, принимать решения и выполнять задачи, которые раньше считались исключительно человеческими.

Одной из ключевых концепций в области ИИ является машинное обучение. Системы машинного обучения обучаются на основе данных, извлекая из них закономерности и создавая модели, которые в дальнейшем могут использоваться для классификации, прогнозирования, обработки естественного языка и других задач.

Искусственный интеллект на сегодняшний день находится во многих сферах нашей жизни, таких как медицина, финансы, автомобильная промышленность, игровая индустрия и другие. Врачи используют системы ИИ для диагностики заболеваний и поддержки принятия решений при лечении, банки применяют ИИ для анализа рынка и создания инвестиционных стратегий, автомобили оснащаются системами ИИ для автоматической навигации и предотвращения аварий, а игровая индустрия использует ИИ для создания умных и реалистичных персонажей.

Однако, развитие ИИ также вызывает вопросы и вызовы в области этики и безопасности. Возникают вопросы о приватности данных, роботах-убийцах и потере рабочих мест из-за автоматизации. Поэтому необходимо развивать ИИ с соответствующим пониманием и обеспечить этические и безопасные практики его использования.

Искусственный интеллект продолжает быстро развиваться, и его влияние на нашу жизнь становится все более заметным. Это открывает новые возможности и вызывает важные вопросы, которые нужно тщательно изучать и обсуждать, чтобы обеспечить наиболее благоприятное использование ИИ для достижения наших целей и удовлетворения наших потребностей.

1. Перспективы искусственного интеллекта в трудовых отношениях

а) Автоматизация повторяющихся задач

ИИ способен автоматизировать ряд повторяющихся задач, которые ранее выполнялись вручную. Это позволяет сотрудникам сосредоточиться на более сложных и творческих заданиях, повышая их производительность и эффективность.

б) Улучшение процессов принятия решений

ИИ может анализировать большие объемы данных и предоставлять ценные выводы для принятия решений. Это помогает более быстро и точно определять оптимальные стратегии и прогнозировать результаты, что способствует повышению качества и эффективности рабочих процессов.

в) Создание новых рабочих мест

Развитие ИИ открывает новые возможности для создания рабочих мест, связанных с его разработкой, обслуживанием и управлением. Это способствует росту экономики, созданию новых отраслей и инноваций.

2. Риски, связанные с внедрением искусственного интеллекта

а) Потеря рабочих мест

Одним из наиболее основных рисков, связанных с ИИ, является потенциальная потеря рабочих мест. Автоматизация исключает необходимость в определенных категориях работников, и это может привести к массовому безработице и социальным проблемам.

б) Растущие неравенства

Если ИИ приведет к потере рабочих мест, растущие неравенства могут стать серьезной проблемой. Неравномерное распределение выгод от автоматизации может привести к социальным конфликтам и экономической нестабильности.

в) Опасность приватности и безопасности

С развитием ИИ возникают возможности для сбора и анализа огромных объемов данных. Это создает новые риски в области приватности и безопасности, поскольку существует возможность злоупотребления персональной информацией и хакерских атак на системы управления ИИ.

г) Потеря навыков из-за зависимости от ИИ

Зависимость от ИИ может привести к потере некоторых навыков у работников. Если человек полностью полагается на ИИ, это может снизить их способность решать задачи самостоятельно и привести к снижению профессиональной компетентности

Искусственный интеллект имеет огромный потенциал для преобразования трудовых отношений. Он может повысить производительность, эффективность и качество работы. Однако внедрение ИИ также сопряжено со значительными рисками, включая угрозу рабочим местам, социальные неравенства, проблемы приватности и безопасности. Чтобы успешно справиться с вызовами, связанными с использованием ИИ, необходимо внимательно изучать их влияние, разрабатывать этические и регулирующие механизмы, а также обеспечивать переобучение и подготовку сотрудников к новым обязанностям.

В заключении можно подчеркнуть, что воздействие искусственного интеллекта на трудовые отношения является комплексным и многогранным процессом. С одной стороны, ИИ предоставляет значительные возможности для автоматизации, оптимизации бизнес-процессов и создания новых рабочих мест в сферах разработки и обслуживания технологий. С другой стороны, существует потенциальный риск увеличения неравенства в занятости и вызывается необходимость постоянного обучения и переподготовки кадров.

Однако, несмотря на вызовы, стоящие перед обществом и рынком труда, важно осознавать, что искусственный интеллект также предоставляет уникальные возможности для карьерного роста и развития

новых компетенций. Подготовленные специалисты, обладающие знаниями в области ИИ, могут активно влиять на формирование будущего трудового рынка.

Важными аспектами внедрения искусственного интеллекта в трудовые отношения являются этические вопросы и обеспечение безопасности данных. Способность эффективно управлять этими аспектами будет критической для того, чтобы обеспечить справедливость и устойчивость в эволюции трудового рынка.

Таким образом, необходимо стремиться к балансу между принятием инноваций и обеспечением социальной ответственности, чтобы создать трудовую среду, способствующую росту и благосостоянию для всех участников общества.

Список использованных источников:

1. Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V ЗПК. /<https://adilet.zan.kz>
2. Закон РК от 24.11.2015 «Об информатизации» № 418-V /<https://adilet.zan.kz>
3. Сайт искусственный интеллект https://yabs.yandex.kz/count/WcSejl_zOoVX2Lbl0iqI09DYWYQbKgbKga4mGHZfF5xUxRVkVDTNpjVI-FrXZjSQv5HKOaGpwbK2dNYJnkQT6HkMrhzMJ71_NG-
4. Чем нейросеть отличается от искусственного интеллекта? <https://dzen.ru/a/ZH3Zo54aSWv3uWco?yclid=18296040564324564991>

УДК 342.7:349

Сатимова Дильназ Сериккызы

студентка 3 курса Высшей школы права «Әділет»

Каспийского общественного университета,

Республика Казахстан, г. Алматы

ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО В СТРАНАХ СНГ

Аннотация

Данное исследование посвящено анализу единого информационного пространства стран СНГ. В статье подробно рассматривается структура, границы, компоненты и характеристики информационного пространства. Особое внимание уделяется процессу формирования нового

информационного пространства и его трансформации. Исследование также включает в себя более углубленный анализ единого информационного пространства в Республике Казахстан.

Основной целью статьи является проведение структурно-функционального анализа единого информационного пространства стран СНГ, включая его структуру, функции, характеристики, а также процессы формирования и развития.

Ключевые слова: информационное пространство, единое информационное пространство, СССР, СНГ, РСФСР, СМИ, развитие, ИКТ, технологии, язык

Сатимова Дильназ Сериккызы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 3 курс студенті,

Қазақстан Республикасы, Алматы қ.

МЕДИЦИНА ҚЫЗМЕТКЕРЛЕРІНІҢ

ҚЫЛМЫСТЫҚ ЖАУАПКЕРШІЛІГІНІҢ ҚҰҚЫҚТЫҚ ЕРЕКШЕЛІКТЕРІ:

ЖАУАПКЕРШІЛІКТІ АЗАЙТУҒА БОЛАДЫ МА

Аңдатпа

Бұл зерттеу ТМД елдерінің ортақ ақпараттық кеңістігін талдауға арналған. Мақалада ақпараттық кеңістіктің құрылымы, шекаралары, құрамдас бөліктері мен сипаттамалары егжей-тегжейлі қарастырылады. Жаңа ақпараттық кеңістікті қалыптастыру және оның трансформациялану үдерісіне ерекше назар аударылады. Сондай-ақ зерттеуде Қазақстан Республикасындағы біртұтас ақпараттық кеңістікке тереңірек талдау жасалған.

Мақаланың негізгі мақсаты – ТМД елдерінің жалпы ақпараттық кеңістігіне оның құрылымын, функцияларын, сипаттамаларын, сондай-ақ қалыптасу және даму процестерін қамтитын құрылымдық-функционалдық талдау жүргізу.

Түйінді сөздер: ақпараттық кеңістік, біртұтас ақпараттық кеңістік, КСРО, ТМД, РКС, ГСС, БАҚ, даму, АКТ, технология, тіл

D.S. Satimova

3 year student of the Higher School of Law «Adilet»

Caspian Public University,

Republic of Kazakhstan, Almaty

**LEGAL FEATURES OF THE CRIMINAL LIABILITY OF MEDICAL WORKERS:
IS IT POSSIBLE TO REDUCE LIABILITY**

Annotation

This study is devoted to the analysis of the unified information space of the CIS countries. The structure, borders, components and characteristics of the information space are discussed in detail in the article. Special attention is paid to the process of forming a new information space and its transformation. The study also includes a more in-depth analysis of the unified information space in the Republic of Kazakhstan.

The main purpose of the article is to conduct a structural and functional analysis of the common information space of the CIS countries, including its structure, functions, characteristics, as well as the process of formation and development.

Keywords: information space, unified information space, USSR, CIS, RCC, GHS, media, development, ICT, technology, language

Долгие годы многие страны, в том числе Республика Казахстан, находилась в составе Союза Советских Социалистических Республик, вплоть до распада СССР в 1991 году.

Окончательным этапом распада СССР было подписание Беловежских соглашений 8 декабря и Алма-Атинской декларации 21 декабря 1991 года. Был учрежден политический союз бывших советских республик под названием Содружество Независимых Государств (СНГ). Она представляет собой международную организацию, созданную для урегулирования взаимоотношений и сотрудничества между странами, которые ранее составляли часть СССР.

Одной из ключевых задач недавно созданного содружества стало создание единого информационного пространства, для укрепления культурных, языковых и этнических связей между народами.

Информационное пространство представляет собой совокупность информации, данных, коммуникаций и контекста, охватывающую определенную территорию или среду. Это концепция, описывающая сферу, в которой обмениваются, передаются и воспринимаются различные виды информации с использованием средств коммуникации, таких как сети, технологии и средства массовой информации. Информационное пространство охватывает как физические, так и виртуальные аспекты обмена информацией в определенном сообществе, регионе или в глобальном масштабе.

Мировое общество долгое время переживало переход от промышленного общества к информационному обществу. Теперь же информа-

ция становится ключевым ресурсом, что подчеркивает необходимость эффективного управления информационными ресурсами, их защиты и установления единой системы обращения. Создание единого информационного пространства (ЕИП) выступает важной задачей. ЕИП может рассматриваться с точки зрения технологии, государственности, законодательства, а также как совокупность культурных и исторических связей, а иногда даже как миф.

Единое информационное пространство представляет собой комплекс баз данных, технологий их управления и использования, информационно-телекоммуникационных систем и сетей, которые функционируют на основе общих принципов и правил. Это обеспечивает взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей. В основе единого информационного пространства лежат три основных компонента:

1) информационные ресурсы, которые включают в себя данные, сведения и знания, закрепленные на соответствующих носителях информации;

2) организационные структуры, они в свою очередь отвечают за функционирование и развитие единого информационного пространства. Эти структуры осуществляют сбор, обработку, хранение, распространение, поиск и передачу информации;

3) средства информационного взаимодействия, создаются и обеспечивают доступ граждан и организаций к информационным ресурсам на основе соответствующих технологий. Эти средства включают в себя программно-технические решения и организационно-нормативные документы.

В 1996 году 18 октября решением Совета глав правительств СНГ была образована «Концепция формирования информационного пространства Содружества Независимых Государств».

Если говорить о этапах, то первым шагом в достижении данной цели стало создание Регионального содружества в области связи (РСС) 17 декабря 1991 года. РСС начало свою деятельность с целью содействия сотрудничеству новых независимых государств в области электрической и почтовой связи на основе добровольных принципов, взаимоуважения и суверенитета.

30 декабря 1991 года, на Совещании глав правительств СНГ был подписан Протокол о создании Статистического комитета с целью координации статистических служб государств СНГ. Он занимался формированием сводных статистических данных, необходимых для взаимодействия

государств-членов СНГ в политической, социально-экономической и внешнеэкономической сферах.

13 марта 1992 года главы правительств Независимых Государств подписали Соглашение о научно-техническом сотрудничестве в рамках государств-участников СНГ. Это соглашение регулировало пути межгосударственного взаимодействия в области научно-технических программ и проектов по развитию новых технологий, а также других межгосударственных программ.

Было подписано Соглашение о сотрудничестве в области информации, 9 октября 1992 года, что сыграло ключевую роль в процессе формирования. Помимо него заключили Соглашение о создании Межгосударственной телерадиокомпании «Мир», она действует до сей пор.

26 июня 1992 года страны СНГ было достигнуто взаимопонимание по поводу обмена научно-технической информацией, что было отражено в соответствующем соглашении. Эти государства согласились на развитие информационных ресурсов и условий их использования, а также на обеспечение доступа к совместно созданным информационным ресурсам.

Они также договорились оказывать поддержку общим научно-техническим программам, проектам, исследованиям и разработкам в области информационной деятельности, а также содействовать созданию и использованию правовых, технических и технологических элементов информационной инфраструктуры, совместимых с соответствующими элементами национальных информационных систем.

Основываясь на предыдущих соглашениях государств-участников СНГ и, прежде всего, в сфере обмена информацией, Концепция представляет собой некий рекомендательный документ, и отражает систему согласованных взглядов на цели и приоритеты сотрудничества в области информационных обменов. В процессе разработки Концепции были использованы материалы рабочих заседаний и консультативных встреч представителей государств и органов Содружества, организованных Исполнительным Секретариатом СНГ в соответствии с решениями Совета глав правительств.

Главной целью Концепции было и есть стимулирование информационного сближения государств СНГ и представляет собой общий набор принципов и приоритетов для развития информационного сотрудничества в регионе.

В 2000 годах в странах СНГ начался процесс принятия иных соглашений в области ЕИС.

Большое влияние в сфере информационных технологий имеет Координационный совет участников стран СНГ, образованный в 2002 году, к области его регулирования относится информатизация при РСС.

Главными направлениями являются:

- 1) укрепление многостороннего взаимовыгодного сотрудничества в области информационно-коммуникационных технологий (ИКТ);
- 2) формирование общего информационного пространства СНГ;
- 3) согласование нормативно-правовой базы;
- 4) обмен информационными ресурсами;
- 5) решение проблемы информационной безопасности;
- 6) успешная интеграция государств-участников СНГ в глобальное информационное общество.

По истечению времени, 28 ноября 2006 года, был образован Совет по гуманитарному сотрудничеству (СГС) государств-участников СНГ. К его компетенции относится координация многостороннего взаимодействия в сфере культуры, образования, науки, архивного дела, информации и массовых коммуникаций, спорта, туризма и работы с молодежью среди государств-участников.

Говоря о ЕИП, нельзя не указать Межгосударственный фонд гуманитарного сотрудничества (МФГС). МФГС активно сотрудничает с СГС и организует мероприятия, направленные на развитие общего культурного пространства в СНГ, а также поддерживает радиовещание общественно-значимых программ на станции «Мир».

Гарантирование информационной безопасности в рамках информационного пространства СНГ представляет собой одну из ключевых задач. Она включает в себя обеспечение каждым государством-участником своей информационной безопасности и защиты информационного суверенитета. Для своевременного решения данных вопросов каждая страна СНГ осуществляет постоянный мониторинг «противоречий» в области информационной политики и потенциальных угроз для своего информационного суверенитета.

Практическое разрешение задач по обеспечению национальной информационной безопасности, а также привлечение к ответственности за угрозы или нарушения информационной безопасности в каждой из стран Содружества осуществляется в соответствии с их национальным законодательством, международными правовыми нормами и соответствующими межгосударственными соглашениями.

В рамках сотрудничества СНГ было принято много соглашений по ЕИП, которые как планировалось, должны были решить все проблемы

касательно этой темы. Но в действительности, многие задачи остаются нерешенными. В Соглашении о создании СНГ от 8 декабря 1991 года стороны обязались развивать взаимовыгодное сотрудничество в различных областях, включая информационный обмен. Однако в настоящее время сложно говорить о благоприятной обстановке для формирования Единого Информационного Пространства (ЕИП) СНГ. Межгосударственные конфликты и ужесточение законодательства относительно статуса русского языка и русскоязычных СМИ в странах СНГ являются существенными препятствиями в этом процессе.

Если говорить о проблематике, то один из компонентов в структуре ЕИП – это язык. Членами-участниками СНГ являются 10 независимых стран, таких как: Республика Казахстан, Азербайджан, Армения, Белоруссия, Киргизия, Молдавия, Россия, Таджикистан, Узбекистан и Туркменистан. В каждой из этих республик закреплен свой государственный язык и лишь в некоторых общим можно назвать русский. Язык, как средство обмена информацией, и, как следствие, работа СМИ в каждой из стран, не всегда эффективно выполняют свои коммуникативные функции. Это, в свою очередь, отрицательно сказывается на способности СМИ выполнять интегративные функции и вредит деятельности (ЕИП) в качестве структуры. Но, в частности, государственные языки являются основой любого государства, языком общения среди граждан и укрепления патриотизма.

Говоря отдельно о Республике Казахстан, в нашей стране также принялась «Концепция единого информационного пространства Республики Казахстан и мерах по ее реализации» от 29 июля 1998 года, переняв многое уже из ранее известной нам Концепции СНГ 1996 года. Многие положения были взяты из нее, она стала основой для нашей Концепции.

Она стала настоящим спасением для нас, потому что в начале пути информационное пространство Республики Казахстан можно было описать как набор недостаточно взаимосвязанных информационных секторов, включая ведомственные, региональные и коммерческие сегменты. Эти секторы были не всегда тесно связаны между собой, и их доступность для отечественных пользователей ограничена по разным причинам.

Данная Концепция, на момент ее принятия, предусматривала цели, такие как: гарантирование конституционных прав граждан на информацию, развитие информационного потенциала в соответствии с социально-экономическими потребностями, согласованность решений

в рамках программы «Казахстан 2030», повышение правосознания и образованности граждан, обеспечение свободного доступа к информационным правовым документам, улучшение информированности о деятельности государственных органов, стимулирование деловой активности граждан и интеграция с мировым информационным пространством - эти цели являются основными принципами действий в области информационной политики, направленной на достижение стратегических задач развития Республики Казахстан.

Так как данная Концепция была создана для формирования и налаживания ЕИП в Республике Казахстан на начальных стадиях, со временем стала необходима новая политика и направление для ЕИП.

Для данной цели 20 марта 2023 года Указом Президента Республики Казахстан был введен в действие указ «Об утверждении Информационной доктрины Республики Казахстан». Она состоит из 3 разделов, самое интересное содержится в Разделе 2, где была анализирована текущая ситуация в стране. Он был проведен на момент марта этого года, поэтому является относительно актуальным. Были выделены следующие особенности:

В настоящее время более 9% населения сохраняют интерес к печатным изданиям как основному источнику информации. Важно отметить, что этот интерес к чтению газет прямо связан с возрастом – с возрастом увеличивается частота обращения к печатным СМИ. Тем не менее, общественный интерес к печатным изданиям продолжает уменьшаться, поскольку широкая аудитория все чаще обращается к альтернативным средствам коммуникации.

В последние годы интернет-ресурсы становятся все более популярными среди отечественных СМИ. Тем не менее, остается важным вопрос о создании контента высокого качества на государственном языке.

Развитие мобильного интернета привело к тому, что социальные сети стали основным источником информации для значительной части населения страны, в основном среди молодежи. Согласно социологическим исследованиям 2021 года, более половины респондентов, а именно 45,2%, предпочитают получать информацию из социальных медиа.

Целями настоящей доктрины являются обеспечение информационной безопасности и идеологического суверенитета страны, выстраивание отвечающей современным тенденциям и вызовам информационной политики, направленной на консолидацию общества и укрепление гражданской идентичности.

Основными принципами доктрины являются: свобода слова; доступ к информации; ориентир на развитие; доверие и конфиденциальность и обеспечение информационной безопасности.

Учитывая, что Казахстан является составной частью мирового сообщества, стратегия государственной информационной политики должна предусматривать системное реагирование на изменяющиеся мировые процессы и тенденции, а также активное внедрение новых инструментов в соответствии с национальными интересами.

Важно при этом принимать во внимание сбалансированный и прагматичный подход, учитывающий реальные условия как на внешнем, так и на внутреннем уровне развития Казахстана.

Подводя к итогам, в ходе статьи была рассмотрена Концепция формирования информационного пространства СНГ, история ее формирования и общие условия ее реализации. Также были выявлены некоторые проблемы в отношении распространения ее действия и вопросы языка. Более того, было рассмотрено информационное пространство в Республике Казахстан и ее основные направления.

Список использованных источников:

1. Андреева Г., Титова Т. Формирование информационного пространства Содружества Независимых Государств: аспекты правового обеспечения. М., 2004.

2. Концепция формирования информационного пространства Содружества Независимых Государств [Электронный Ресурс] URL: <https://cis.minsk.by/page/7548#:~:text=\D1>

3. Батыршин Р. И. Телерадиокомпания «Мир»: формирование единого информационного пространства стран Содружества. М.: Институт повышения квалификации работников телевидения и радиовещания, 2011. 85 с.

4. Постановление Правительства Республики Казахстан от 29 июля 1998 г. N 715 «О Концепции единого информационного пространства Республики Казахстан и мерах по ее реализации» [Электронный Ресурс] URL: https://adilet.zan.kz/rus/docs/P980000715_

5. Указ Президента Республики Казахстан от 20 марта 2023 года № 145. «Об утверждении Информационной доктрины Республики Казахстан» [Электронный Ресурс] URL: <https://akorda.kz/ru/ob-utverzhenii-informacionnoy-doktriny-respubliki-kazahstan-2025248>

УДК 347.1

Сейткасымов Алмат Қамбарұлы
Студент 3 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

**ВОЗДУХ ЗА МИЛЛИОНЫ:
ИНФОШУЛЕРСТВО И ОНЛАЙН-КУРСЫ**

Научный руководитель:

Максатов Н.Р.

М.ю.н., сеньор-лектор
Высшей школы права «Әділет»
Каспийского общественного университета

Аннотация

В статье рассматривается проблема инфошулерства в Казахстане. Авторы показывают, что инфошулерство представляет собой серьезную угрозу для потребителей, и то, что в Казахстане этой проблеме не уделено должного внимания. В статье авторы анализируют опыт других стран, таких как Великобритания и Россия, в области онлайн-курсов. Авторы предлагают создать специальный закон, регулирующий деятельность онлайн-коучеров и инфобизнесменов, который позволит повысить прозрачность их деятельности и защитить права потребителей.

Ключевые слова: инфошулеры, онлайн-курс, потребитель, услуга, инфобизнес, образовательная программа, прецедент, лицензия, защита прав, прозрачность, коучинг, цифровые продукты, тренинг.

Сейткасымов Алмат Қамбарұлы
Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 3 курс студенті,
Қазақстан Республикасы, Алматы қ.

**АУА ҮШІН МИЛЛИОНДАР:
ИНФОШУЛЕРЛЕР ЖӘНЕ ОНЛАЙН-КУРСТАР**

Аңдатпа

Мақалада Қазақстандағы инфошулерлік мәселесі қарастырылады. Авторлар инфошулерліктің тұтынушылар үшін елеулі қауіп төндіретінін және Қазақстанда бұл мәселеге тиісті көңіл бөлінбегенін көрсетеді. Мақалада авторлар Ұлыбритания мен Ресей сияқты басқа елдердің онлайн-курстарды реттеу саласындағы тәжірибесін талдайды. Авторлар онлайн-курстар мен инфобизнесмендердің қызметін реттейтін, олардың қызметінің ашықтығын арттыруға және тұтынушылардың құқықтарын қорғауға мүмкіндік беретін арнайы заң құруды ұсынады.

Түйінді сөздер: инфошулерлер, онлайн-курс, тұтынушы, қызмет, инфобизнес, білім беру бағдарламасы, прецедент, лицензия, құқықтарды қорғау, ашықтық, коучинг, цифрлық өнімдер, тренинг.

Seitkasymov A.K.

3 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

AIR FOR MILLIONS: INFOSHOOING AND ONLINE COURSES

Annotation

The article deals with the problem of information fraud in Kazakhstan. The authors show that information fraud poses a serious threat to consumers, and that due attention has not been paid to this problem in Kazakhstan. In the article, the authors analyze the experience of other countries, such as the United Kingdom and Russia, in regulating online courses. The authors propose to create a special law regulating the activities of online coaches and information businessmen, which will increase the transparency of their activities and protect the rights of consumers.

Keywords: infoshulers, online course, consumer, service, infobusiness, educational program, precedent, license, protection of rights, transparency, coaching, digital products, training.

Если кто-то заявит, что воздух можно продавать за миллионы, вы, вероятно, не поверите. Тем не менее, в цифровой реальности существует явление, именуемое как «инфошулерство».

Инфошулерство - это практика предоставления цифровых продуктов (книг, курсов, тренингов, чек-листов) которые не имеют реальной ценности. Эти продукты часто предлагаются известными в социальных сетях блогерами-миллионниками, самопровозглашающими себя экспертами или коучами. За символическую плату они продают свои курсы, в которых раскрыты секреты успешной жизни и богатства. Но на практике в этих курсах содержится общедоступная информация, которую можно найти по первой ссылке в Google [1].

Вместо конкретных знаний они прибегают к психологическим практикам, предлагая советы по постановке целей, укреплению уверенности в себе или правильному формулированию желаний. Например, инфошулеры могут посоветовать вам за деньги поменять дома обстановку, больше рисковать, не есть вредную пищу и т.д.

В медийной сфере обычно используют термин «инфоцыгане» и «инфоцыганство», однако этот термин указывает на национальную принадлежность и имеет ярко выраженный негативный оттенок. Мы предлагаем использовать синонимы к этим терминам: «инфошулер» и «инфошулерство».

В сфере юридической науки России, явление инфошулерства является предметом ограниченного изучения. В 2022 г. свое внимание на проблему инфошулерства обратили Каминская Т.Л. и Петровская В. написав научную статью.

В Республике Казахстан эта проблематика пока не получила должного внимания и научного освещения. И то, что в нашей стране уделяется этому так мало внимания, весьма несправедливо.

Во-первых, в Республике Казахстан много блогеров. Согласно данным 2023 года от «trendHERO.», в нашей стране количество блогеров в Instagram с числом подписчиков свыше 5000 превышает 147 тысяч [2]. По данным от «Datareportal», в Казахском секторе Instagram зарегистрировано 10,45 млн пользователей [3]. Инфошулерство чаще всего встречается в «Instagram», но также распространено в других социальных сетях и мессенджерах, таких как «ТikТок».

Также стоит отметить, что в нашей стране 10 июля 2023 года был принят новый закон «Об онлайн-платформах и онлайн-рекламе», где закрепили понятие «блогер» на законодательном уровне [4]. Согласно этому закону, инфлюенсер (блогер) - пользователь онлайн-платформы, публикующий информацию на онлайн-платформе, адресованную неопределенному кругу лиц, в целях предпринимательской деятельности.

Во-вторых, вокруг инфошулерства крутится большое количество денег. Онлайн-курсы часто имеют высокую стоимость. Нередки случаи, когда те, кто стремится приобрести их, часто вынуждены воспользоваться рассрочкой или брать деньги в долг. Цены онлайн-курсов часто бывают слишком завышенными, и не соответствуют уровню предоставляемых знаний. Цены никак не регулируются, авторы сами определяют стоимость. Чем именитее блогер или инфлюенсер, тем дороже будет онлайн-курс. Такие блогеры и инфлюенсеры всегда ориентируются именно на большом потоке клиентов, но никак не на качестве образования.

У нас возникает логичный вопрос: Почему люди приобретают дорогостоящие обучающие онлайн-курсы, тратя свои последние деньги? Дело в том, что инфошулеры имеют схему продаж своих продуктов. Инфошулеры начинают свою стратегию с «подогрева» аудитории, рассказывая, например, о своем лжеуспехе. Затем они убеждают людей в том, что благодаря их «уникальному курсу» можно достичь успеха в короткие сроки и зарабатывать много денег. Часто можно заметить, как они вставляют манипулятивные скриншоты переписок с якобы довольными клиентами, утверждая, что все у них получилось. Также есть еще один манипуляторский ход, когда инфошулер уговаривает купить его курс как можно скорее, предлагая скидки и спецпредложения. Почти всегда можно услышать такие громкие выражения, как «мышление миллионера» и «успешный успех».

Инфошулеры часто называют свои курсы не просто курсами, а используют такие слова, как «лейбл», «команда», «марафон», «продакшн», «проект» и т.д. Это делается для того, чтобы ввести людей в заблуждение и создать впечатление, что их курс более серьезный, масштабный и качественный, чем обычные курсы обучения.

И, наконец, в третьих, покупателям онлайн-курсов у инфошулеров очень трудно защитить свои права.

Число жертв инфошулеров в нашей стране с каждым днем увеличивается, и эта проблема становится всё более актуальной. В Республике Казахстан до сих пор не было случаев, когда инфошулеры были привлечены к ответственности в судебном порядке. Нередки случаи коллективных жалоб и обращения в органы прокуратуры от граждан, которые стали жертвами инфошулерства. В настоящее время отсутствуют прецеденты, которые могли бы служить образцом для людей, желающих апеллировать в защиту своих прав.

Инфошулеры продают курсы, и во многих случаях гарантируют успех. Но гарантия успеха – пустой звон. Гарантия успеха нужна лишь

для увеличения потока своих клиентов, но на деле за результат и эффективность курса инфошуплер не несет никакой ответственности, что подтверждает наши доводы о нарушении законов РК. Если конкретизировать, то из смысла ст 29. Закона О защите прав потребителей (Далее – закон «ОЗПП»), **если исполнитель при заключении договора был поставлен в известность о конкретных целях оказания услуги, исполнитель обязан оказать услугу надлежащего качества, пригодный для использования в соответствии с этими целями [5].**

В данном контексте в качестве наглядного примера мы обратим внимание на судебную практику РФ.

В 2022 году в России был создан уникальный правовой прецедент: суд впервые наказал инфошуплеров за обман. В январе 2022 года между потребителем и индивидуальным предпринимателем был заключен договор на оказание платных онлайн-услуг и оплачена полная стоимость авторского онлайн-курса «*Фабрика beauty-звезд. Инструкторский курс 2.0*» в размере 108 000 рублей (примерно 545 тыс. тенге). Период прохождения курса составлял 10 недель с поэтапным предоставлением обучающимся слушателям материалов по обозначенным в разделе темам. Поскольку качество оказываемых онлайн-услуг не удовлетворило потребителя, он потребовал возврата уплаченных им денежных средств, за вычетом фактически понесенных предпринимателем расходов, направив исполнителю услуги претензию об одностороннем отказе от предоставляемых услуг и необходимости возврата денежных средств в размере 72 000 рублей (примерно 369 тыс.тенге). Требования потребителя исполнителем услуги были проигнорированы, после чего гражданин обратился за правовой помощью в территориальный отдел Управления Роспотребнадзора по г. Москве в Юго-Восточном административном округе. По результатам рассмотрения обращения специалистами было принято решение о подаче судебного иска в защиту прав потребителя.

Решением мирового судьи судебного участка № 251 района Текстильщики города Москвыисковые требования Управления Роспотребнадзора по г. Москве были удовлетворены. С индивидуального предпринимателя в пользу потребителя подлежит взысканию сумма, оплаченная по договору оказания услуг (за вычетом стоимости понесенных исполнителем услуги расходов) в размере 72 000 рублей, компенсация морального вреда – 6 000 рублей (примерно 30 тыс. тенге), штраф в размере 50% от суммы, присужденной судом – 39 000 рублей (примерно 200 тыс. тенге), расходы потребителя – 13 000 рублей (примерно 66 тыс. тенге), а всего 130 000 рублей (примерно 650 тыс. тенге) [6].

Это действительно первый случай, когда заявитель, недовольный именно содержанием курса получил деньги обратно. Данный прецедент доказывает, что у человека, приобретающего онлайн-курсы у инфошулера, все-таки есть возможность защитить свои права.

Для того чтобы защитить себя от инфошулеров, нужно понимать, как они работают и что продают.

Для продажи онлайн-курсов необходимо зарегистрироваться в качестве индивидуального предпринимателя (ИП). Однако в Казахстане инфошулеры редко выполняют это требование. Общий классификатор видов экономической деятельности (ОКВЭД) для онлайн-курсов – «прочие виды образования» (85.5).

В эту классификацию входит:

1. образовательная деятельность, являющаяся продолжением общего и профессионального образования;
2. тренинги в профессиональных целях;
3. тренинги для проведения досуга или целей саморазвития;
4. групповое или индивидуальное обучение в области физической культуры;
5. обучение иностранному языку;
6. обучение изобразительному и драматическому искусству, музыке и т.д.

В связи с недостаточной изученностью темы инфошулерства, онлайн-курсов и инфобизнеса в целом, мы решили провести исследование. В рамках исследования мы обратились в Министерство науки и высшего образования [7] со следующими вопросами:

1. Имеются ли какие-нибудь стандарты для курсов обучения?
2. Нужно ли соблюдать какие-то правила, чтобы создать обучающий курс?
3. Нужна ли лицензия физическим лицам для того, чтобы продавать свои обучающие курсы?
4. Нужна ли лицензия юридическим лицам для того, чтобы продавать свои обучающие курсы?

Комитет высшего и послевузовского образования, рассмотрев наше обращение, ответил следующим образом:

(Начало ответа) Согласно пунктов 1-2, статьи 37-1. Закона Республики Казахстан «Об образовании» (далее-Закон), индивидуальная педагогическая деятельность, сопровождающаяся получением доходов, является предпринимательской деятельностью. Государственная регистрация лица, занимающегося индивидуальной педагогической деятельностью, осуществляется в соответствии с законодательством

Республики Казахстан. Индивидуальная педагогическая деятельность не лицензируется.

В соответствии с пунктом 1, статьи 23. Закона, образовательные программы дополнительного образования направлены на удовлетворение всесторонних потребностей обучающихся, воспитанников и специалистов с ориентиром на результаты обучения и соответствие национальной рамке квалификаций и отраслевым рамкам квалификаций.

Также, согласно статье 37 Закона образование взрослых (лиц, достигших восемнадцатилетнего возраста) направлено на удовлетворение их образовательных потребностей в течение всей жизни для получения дополнительного объема знаний и навыков в соответствии с происходящими социально-экономическими изменениями в обществе.

Получение взрослыми дополнительного объема знаний и навыков осуществляется через дополнительное и неформальное образование.

Дополнительное образование взрослых осуществляется организациями образования, а также юридическими лицами, имеющие структурные подразделения, реализующие дополнительные образовательные программы.

Неформальное образование взрослых осуществляется организациями, которые предоставляют образовательные услуги, оказываемые без учета места, сроков и формы обучения, и сопровождается выдачей документа, подтверждающего результаты обучения.

Соответственно, организации образования, осуществляющие дополнительное образование **не лицензируются (конец ответа)**.

Исходя из ответа комитета, мы можем сделать выводы о том, что согласно ст 14. Закона Республики Казахстан Об образовании, **онлайн-курсы относятся к образовательным программам дополнительного образования** [8]. Для осуществления дополнительной образовательной деятельности индивидуальным предпринимателям и юридическим лицам лицензия не нужна. По 1-2 вопросам комитет решил не отвечать.

Также следовало бы отметить то, что при покупке онлайн-курса в большинстве случаев отсутствует заключение договора. Это связано с тем, что продавец не предлагает его заключить, а покупатель не запрашивает. В результате все ограничивается перепиской в WhatsApp. Чтобы купить онлайн-курс нужно заключить **договор об оказании услуг**.

Как уже упоминалось, курсы инфошуглеров часто не представляют никакой ценности для покупателей. Информация, представленная в

них, часто собрана из открытых источников, уроки не соответствуют общей теме или лектор рассказывает очевидные вещи. У покупателей возникает логичное желание вернуть деньги за «воздух». Однако сделать это очень непросто.

Согласно пункту 1 статьи 35 закона ОЗПП, потребитель при обнаружении недостатков в оказанной услуге вправе по своему выбору потребовать:

- 1) безвозмездного устранения недостатков в выполненной работе (оказанной услуге);
- 2) соответствующего уменьшения вознаграждения за выполненную работу (оказанную услугу);
- 3) безвозмездного изготовления другой вещи из однородного материала такого же качества или повторного выполнения работы (оказания услуги)
- 4) возмещения своих расходов на устранение недостатков, когда право потребителя устранять их предусмотрено в договоре.

Чтобы вернуть потраченные деньги за онлайн-курс, недостаточно просто заявить, что он не понравился или не принес пользы. Покупатель обязан доказать, что онлайн-курс имеет недостатки. Чтобы было проще доказать это, покупатель должен с самого начала заключить договор. А уже от этого договора отталкиваться, что обещал исполнитель и какие недостатки были в процессе обучения.

Но что делать, если покупатель не заключал договор? Как же доказать, что покупателю предоставили услуги ненадлежащего качества? Ведь обычно в договоре прописывается то, какие услуги и какого качества услуги оказывает исполнитель. В таком случае, покупателю курсов надо вспомнить, где именно он увидел этот онлайн-курс. Если курс продавался через сайт, то на нём, как правило, указывается, что должен включать в себя обучающий курс. Например, на сайте может быть написано, что участник курса сможет пересматривать уроки в течение определённого времени, выполнять домашние задания, а также присоединиться к специальной группе в Telegram или WhatsApp. Кроме того, переписка между покупателем и продавцом может служить подтверждением заключения договора, даже если он не был оформлен в письменной форме.

К сожалению, защитить свои права можно лишь таким способом, именно за недостатки в оказании услуг, но не за качество и ложные обещания инфошюлера. Нигде не написано, что покупатель может вернуть свои деньги, если курс оказался плохим или бесполезным.

После прохождения онлайн-курсов, ученикам выдаются сертификаты, которые подтверждают факт обучения. Такие сертификаты не являются государственными образцами и не присваивают никаких квалификации.

Инфошутлеры ловко пользуются тем, что наше законодательство недостаточно отрегулировало их деятельность. Непонятно, что является предметом продажи у инфошутлеров. Как мы уже отмечали выше, они продают свои курсы под видом услуг.

Основная проблема заключается в том, что при покупке онлайн-курса продавец предоставляет покупателю весь учебный материал. Это означает, что покупатель уже ознакомлен с ним. С одной стороны, это справедливо, ведь продавец рискует, предоставляя покупателю доступ к своему продукту. С другой стороны, это затрудняет возврат денег покупателю, если он недоволен курсом. Ведь считается, что он уже ознакомлен с его материалами.

Предлагаем обратить внимание на опыт других стран в борьбе с инфошутлерством. Примером эффективной борьбы с инфошутлерами может служить опыт Великобритании. В этой стране закон защищает права потребителей на получение качественного цифрового контента, в том числе онлайн-курсов.

Закон Великобритании о правах потребителей 2015 года гласит, что цифровой контент (например, приложения, электронные книги, онлайн-курсы, игры или музыка) должен быть:

1. Удовлетворительного качества;
2. Подходить для конкретной цели;
3. Соответствовать описанию продавца [9].

Если потребитель приобрел цифровой продукт, который не соответствует вышеуказанным критериям, он может потребовать от продавца:

1. Повторного выполнения неудовлетворительного элемента онлайн-курса или повторного прохождения всего онлайн-курса без дополнительной оплаты в разумные сроки и без причинения значительных неудобств;
2. Если повторное выполнение невозможно, требовать возврат средств.

Возврат может достигать 100% стоимости курса в зависимости от серьезности недостатков. Продавец должен выполнить требование потребителя о возврате средств в течение 14 дней.

В соответствии с Положением Великобритании о потребительских контрактах потребитель имеет право отменить курс в течение 14 дней

[10]. Однако это предполагает, что потребитель не получил доступ к материалам курса. Другими словами, потребитель может отменить курс (и получить полный возврат средств) в течение 14 дней, при условии, что он еще не получил доступ к материалам курса. Если курс предоставлялся не полностью, а частями, то потребитель имеет право вернуть деньги за неиспользованную часть.

Для того, чтобы открыть онлайн курс в Великобритании, лицензия не обязательна. Однако, если создавать курс по определенной теме, которая требует некоторой сертификации или лицензирования, например, преподавание курса медсестер, понадобится соответствующая сертификация или лицензия.

Если обратить внимание на последние события, 3 ноября 2023 года в Москве произошло задержание популярного российского блогера и предпринимателя, Аяза Шабутдинова, по предполагаемому совершению преступления в области мошенничества в процессе реализации образовательных курсов.

Аязу Шабутдинову предъявлены обвинения в восьми эпизодах преступления в рамках уголовного дела, касающегося мошенничества. Речь идет о восьми клиентах его компаний, которые перечислили средства в размере от 100 тыс. руб. до 1,9 млн руб. (примерно 490 тыс. – 9,4 млн. тенге) за образовательные курсы, ориентированные на формирование успешного бизнеса и достижение финансового успеха. Аяз Шабутдинов является основателем бизнес-школы «Like Центр», специализирующейся на предоставлении тренингов и курсов по вопросам заработка. По мнению следствия, с использованием своих компаний блогер создавал «ложное впечатление» относительно образовательных программ, которые, по утверждению, позволяют достичь высоких доходов. Команда Аяза Шабутдинова опровергла предъявленные обвинения, считая их необоснованными.

Аяза Шабутдинова можно назвать одним из самых продвинутых инфошуглеров. По данным Edtechs.ru [11], на декабрь 2023 года, «Like Центр» находится на 8 месте в рейтинге крупнейших компаний в сфере онлайн-образования. До предъявленных обвинений компания находилась на 1 месте в сфере онлайн-образования. «Like Центр» имеет лицензию на осуществление образовательной деятельности, а именно: дополнительное образование детей и взрослых, и дополнительное профессиональное образование.

Несмотря на хорошую репутацию, лицензию, собственную платформу для обучения и выход на международный рынок, компания была обвинена в мошенничестве. Рассмотрим один из онлайн-курсов, предла-

гаемых «Like Центром». «Университет бизнеса» - курс, который обещает научить вас зарабатывать от 100 000 (примерно 500 тыс. тенге) рублей или увеличить свой доход. Обучение в «Университете бизнеса» стоит 250 000 рублей в год (примерно 1,2 млн тенге) или 400 000 рублей за два года (примерно 2 млн тенге). Заманчивые обещания «Университета бизнеса» оказались пустыми. По отзывам выпускников, курс не оправдал их ожиданий. Материалы курса были заимствованы из открытых источников, а практические задания не давали никаких навыков. Вместо того, чтобы научить студентов основам бизнеса, курс лишь внушал им, что стать бизнесменом может каждый, независимо от способностей и опыта.

Обвинение в мошенничестве в отношении «Like Центра» ставит под сомнение прозрачность и этичность в предоставлении образовательных услуг в сфере онлайн-образования. Оно также поднимает вопрос о том, соответствуют ли заявленные образовательные результаты реальным возможностям студентов.

Подводя итоги, предлагаем следующие решения проблем с инфошутерством:

Мы предлагаем создать специальный закон, регулирующий деятельность онлайн-коучеров и инфобизнесменов. Мы считаем, что принятие такого закона неизбежно по следующим причинам:

В первую очередь, в Казахстане рынок онлайн-образования растет быстрыми темпами - на фоне пандемии коронавируса и популярности онлайн-обучения, казахстанцев, готовых освоить новые специальности и полезные навыки, ежедневно растет. Следовательно, с каждым днем, все больше людей будут становиться жертвами инфошутерства.

Далее можно отметить недостаточное законодательное регулирование этой деятельности в целом. В новостях нередко появляются заголовки о том, что кто-то стал жертвой инфошутера. При этом необходимо учитывать, что есть еще много людей, истории которых не предаются огласке. Учитывая вышесказанное, удивительно, что в нашей стране все еще нет судебного прецедента, когда инфошутер был привлечен к ответственности в судебном порядке. Все это напрямую связано с недостаточным законодательным регулированием этой деятельности.

Конечно же не стоит забывать о том, что к создателям онлайн-курсов нет никаких требований, по этому люди даже не могут понять, что от них требовать. Жертвы инфошутеров могут только ссылаться на то, что качество знаний в онлайн-курсе низкое. Хотя и в большинстве случаев они и правы, но как мы уже отмечали, это не является законным основанием для защиты их прав.

В итоге мы имеем проблему, которая растет как снежный ком, где людям причиняются большие убытки, и неэффективное законодательное регулирование. Поэтому так необходим закон об онлайн-коучинге и инфобизнесе, который будет защищать права потребителей.

Главным принципом этого закона должна стать **прозрачность**. Принцип прозрачности позволит потребителям получить полную и достоверную информацию об онлайн-курсе перед его приобретением. Без прозрачности потребители находятся в неравном положении по отношению к инфобизнесменам. Инфобизнесмены имеют доступ к информации о потребителях, но потребители не имеют доступа к информации об инфобизнесменах. Это позволяет инфобизнесменам обманывать потребителей, предоставляя им недостоверную информацию о своих услугах. Принцип прозрачности позволяет решить эту проблему, помогая потребителям сделать осознанный выбор и защитить себя от недобросовестных инфобизнесменов.

Поэтому наше следующее предложение состоит в том, чтобы обязать авторов онлайн-курсов составлять программу обучения и знакомить с этой программой будущих покупателей заранее перед началом курса.

Однако для того, чтобы составлять программу курса, да и в принципе, вести сам коучинг, инфобизнесмену нужна определенная компетенция. Поэтому, мы предлагаем будущим коучам самим проходить курсы или даже проходить аккредитацию, чтобы иметь соответствующую компетенцию. Предлагаем обязать коучей составлять:

1. Цели курса;
2. Силлабус;
3. Презентации/видеолекции на каждую тему;
4. Дополнительные материалы курса с активными ссылками для чтения и просмотра в режиме онлайн (книги, монографии, учебные пособия и т.д.);
5. Практические задачи;
6. Вопросы для обсуждения;
7. Тестовые задания.

Авторы онлайн-курсов должны предоставлять эту программу курса уполномоченному органу, например, министерству высшего образования и науки или комитету по защите прав потребителей.

Для защиты прав потребителей от инфошуглеров, которые вводят их в заблуждение, предлагаем обязать авторов онлайн-курсов раскрывать информацию о своем практическом опыте и достижениях. Например,

бизнес-коуч должен иметь опыт работы в бизнесе на руководящих должностях или собственный успешный бизнес. Психолог и маркетолог должны быть дипломированными специалистами с высшим профильным образованием. Инфошутлеры часто вводят людей в заблуждение, демонстрируя красивую жизнь, которой на самом деле не имеют. Они арендуют машины, яхты, красивые дома и даже айфоны, чтобы привлечь внимание потенциальных клиентов. Однако у них попросту нет практического опыта и достижений в той области, в которой они преподают.

Наше главное предложение заключается в том, что **инфобизнесмены должны предоставлять своим ученикам полную информацию о рисках онлайн-курса.** Это включает в себя информацию о том, что эффективность курса и возможные результаты в будущем не могут быть гарантированы. Такое информирование поможет потенциальным клиентам принять более осознанный выбор и не стать жертвами инфошутлеров. Оно также лишит инфобизнесменов их главного оружия - иллюзии гарантированного успеха.

Как мы отмечали ранее, деятельность должна нести уведомительный порядок. Инфобизнесменов, которые продают свои онлайн-курсы очень много, и лишь единицы из них зарегистрированы в качестве ИП. Это препятствует борьбе с ними на уровне закона, ведь они попросту не являются субъектами предпринимательской деятельности. Они работают под псевдонимом, и они не указывают адрес, куда в случае чего можно направить претезию. А так же установление уведомительного порядка данной деятельности позволит уменьшить количество недобросовестных инфобизнесменов, которые хотят избежать уплаты налогов.

Наступающий 2024 год обещает стать годом роста инфобизнеса, а значит, и инфошутлеров. Чтобы защитить себя от инфошутлеров, необходимо быть внимательным и критичным к информации в интернете. Советуем быть осторожным, когда кто-то предлагает легкий путь к успеху.

Список использованных источников:

1. Каминская Т. Л., Петровская В. Феномен «инфоцыганство» в современных медиа. Вопросы журналистики. 2022. № 11. С. 71–84. doi: 10.17223/26188422/11/4//интернет-ресурс: <https://vital.lib.tsu.ru/vital/access/services/Download/kohta:000896859/SOURCE> , дата обращения: 11.11.2023г.
2. trendHERO., поиск блогеров // интернет-ресурс: <https://trendhero.io/app/catalog> , дата обращения: 11.11.2023г.

3. Datareportal, DIGITAL 2023: KAZAKHSTAN // интернет-ресурс: <https://datareportal.com/reports/digital-2023-kazakhsta> , дата обращения: 11.11.2023 г.

4. Закон Республики Казахстан от 10 июля 2023 года № 18-VIII ЗРК. Об онлайн-платформах и онлайн-рекламе.

5. Закон Республики Казахстан от 4 мая 2010 года № 274-IV. О защите прав потребителей.

6. Роспотребнадзор, государственный информационный ресурс в сфере защиты прав потребителей // интернет-ресурс: <https://zpp.rosпотребнадзор.ru/news/regional/339995> , дата обращения: 11.11.2023г.

7. Ответ РГУ «Комитет высшего и послевузовского образования министерства науки и высшего образования Республики Казахстан» // https://docs.google.com/document/d/1fHYn-gS6DlfF5YHGfRGocnLZLcpDm_t0/edit?usp=sharing&oid=109178065229994190562&rtpof=true&sd=true

8. Закон Республики Казахстан от 27 июля 2007 года № 319-III. Об образовании.

9. Legislation.gov.uk Consumer Rights Act 2015 // интернет-ресурс: <https://www.legislation.gov.uk/ukpga/2015/15/section/34/enacted> , дата обращения: 02.12.2023г.

10. Legislation.gov.uk The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 // интернет-ресурс: <https://www.legislation.gov.uk/uksi/2013/3134/contents/made> , дата обращения: 02.12.2023г.

11. Edtechs.ru Рейтинг крупнейших компаний на рынке онлайн-образования // интернет-ресурс: <https://edtechs.ru/>, дата обращения: 05.12.2023г.

ӘОЖ 349

Серік Мадина

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

**ЦИФРЛЫҚ КЕҢІСТІКТЕГІ ҚҰҚЫҚБҰЗУШЫЛЫҚ
ЖӘНЕ ОНЫҢ АЛДЫН АЛУ ЖОЛДАРЫ**

Ғылыми жетекшісі:

Қасымбек А.О.

З.ғ.м., Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің
сеньор-лекторы

Аңдатпа

Бұл мақала цифрлық кеңістіктегі құқықбұзушылықтарын қарастырады. Автор қоғамдағы цифрлық кеңістіктің рөліне және киберкеңістікте туындайтын құқықбұзушылықтардың салдарына назар аударады. Фишинг, хакерлік, кибершабуыл, авторлық құқықты бұзу және басқа да құқық бұзушылық ұғымдары бөлек қарастырылады. Қарастырылып отырған құқық бұзушылықтарға байланысты туындайтын мәселелерді шешу жолдары ұсынылады.

Түйінді сөздер: цифрлық кеңістік, құқық бұзушылықтар, цифрлық технологиялар, балық аулау, кибершабуылдар, киберқорқыту, кибер-терроризм, авторлық құқық.

Серік Мадина

Студентка 1 курса

Высшей школы права “Әділет”

Каспийского общественного университета

Республика Казахстан, г. Алматы

ПРАВОНАРУШЕНИЯ В КИБЕРПРОСТРАНСТВЕ И ПУТИ ИХ ПРЕДОТВРАЩЕНИЯ

Аннотация

В этой статье рассматриваются правонарушения в цифровом пространстве. Автором обращено внимание на роль цифрового пространства в обществе и последствия правонарушений, возникающих в киберпространстве. Отдельно рассмотрены понятия фишинга, хакерства, кибератак, нарушения авторских прав и иные правонарушения. Предлагаются пути решения проблем, возникающих в связи с рассматриваемыми правонарушениями.

Ключевые слова: цифровое пространство, правонарушения, цифровые технологии, фишинг, кибератаки, кибербуллинг, кибертерроризм, авторское право.

Serik Madina

1 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

CRIMES IN CYBERSPACE AND WAYS TO PREVENT THEM**Annotation**

This article examines crime in the digital space. The author draws attention to the role of digital space in society and the consequences of crimes arising in cyberspace. The concepts of phishing, hacking, cyber attacks, copyright infringement and other offenses are considered separately. Ways to solve problems arising in connection with the offenses under consideration are proposed.

Keywords: digital space, offenses, digital technologies, fishing, cyber attacks, cyber bullying, cyber terrorism, copyright.

Цифрлық кеңістік - бұл адамдар цифрлық технологияны өзара әрекеттесу, ақпарат алмасу, оқыту, жұмыс істеу және көңіл көтеру үшін пайдаланатын ортаны білдіретін ұғым. Оған интернет, онлайн платформалар, әлеуметтік медиа, мобильді қосымшалар және байланыс пен ақпаратқа цифрлық түрде қол жеткізуді жеңілдететін басқа да сандық құралдар кіреді. Бұл кеңістік біздің өміріміздің барлық аспектілерін қамтиды.

Цифрлық кеңістік үнемі дамып, кеңейіп, жаңа мүмкіндіктер мен қиындықтар туғызады. Ол үнемі өзгеріп отырады және біздің күнделікті өмірімізге айтарлықтай әсер етіп, қарым-қатынас, жұмыс және білім берудің жаңа тәсілдерін қалыптастырады.

Сандық кеңістік үнемі дамып, кеңейіп, жаңа мүмкіндіктер мен қиындықтар туғызады.

Цифрлық кеңістіктегі құқықбұзушылық - бұл компьютерлік желілерді, интернетті немесе цифрлық технологияларды қолдану арқылы жасалатын кез-келген заңсыз әрекеттер. Бұған фишинг, кибершабуыл, кибербуллинг, кибертерроризм, кибер тыңшылық, авторлық құқықты бұзу, кибербандализм, компьютерлік жүйелерге шабуылдар және т.б. сияқты қылмыстардың әртүрлі түрлері кіруі мүмкін. Бұл әрекеттер деректерді ұрлауға, зиянды бағдарламаларды таратуға, жеке өмірді бұзуға, адам қауіпсіздігіне қауіп төндіруге және жеке қауіпсіздікке, жеке ақпарат пен қоғамдық қауіпсіздікке қауіп төндіретін басқа да көптеген қылмыстарға бағытталған болуы мүмкін.

1. Фишинг - бұл адамдардың құпия сөздер, несие карталарының нөмірлері, шоттарға кіру деректері сияқты жеке ақпаратты алуға тырысатын алаяқтықтың бір түрі. Бұл әдетте ресми болып көрінетін және жеке ақпаратты енгізуді сұрайтын электрондық пошталар, мәтіндік хабарлар немесе веб-сайттар арқылы жүзеге асырылады. Фишинг - бұл алаяқтықтың бір түрі. Онда шабуылдаушылар жалған веб-сайттар жасайды немесе парольдер, банк карталарының нөмірлері және басқа да құпия ақпарат сияқты жеке мәліметтерге қол жеткізу үшін банктерден, компаниялардан немесе басқа ұйымдардан ресми сұрауларға еліктейтін жалған электрондық хаттар жіберу.

2. Кибершабуылдар - бұл басқа біреудің деректеріне немесе құрылғыларына қол жеткізу мақсатында вирустар немесе жай ғана тәртіпсіздік жасау мақсатында компьютерлік жүйелерге, желілерге немесе құрылғыларға зиян келтірушілік. Бұған вирустар, хакерлік шабуылдар және қауіпсіздікті бұзудың басқа жолдары кіруі мүмкін.

3. Кибербуллинг - бұл интернет немесе мобильді құрылғылар арқылы жасалған қауіп-қатерлерді, қорлауды, қоғамдық шабуылдарды немесе психологиялық немесе эмоционалдық зорлық-зомбылықтың басқа түрлерін қамтитын цифрлық қорқытудың бір түрі.

4. Авторлық құқықты бұзу - бұл құқық иесінің (автордың) рұқсатынсыз біреу музыка, фильмдер, бағдарламалық жасақтама немесе басқа мазмұн сияқты басқа адамдардың материалдарын заңсыз пайдалану, көшіру, тарату немесе өзгерту.

5. Балаларға қарсы киберқылмыстар - балалар порнографиясын, интернеттегі құдалауды, бопсалауды және интернет арқылы балаларға жыныстық және психологиялық зорлық-зомбылықтың басқа түрлерін қамтиды.

6. Кибертерроризм - бұл Террористік актілерді жоспарлау, үйлестіру және жүзеге асыру немесе экстремистік идеяларды насихаттау үшін Интернет пен цифрлық технологияларды қолдану және оны жүзеге асыру..

7. Киберспам - бұл электрондық пошта, әлеуметтік медиа немесе басқа байланыс арналары арқылы жіберілетін негізсіз хабарламалар. Киберспамның мақсаты көбінесе жарнамалық вирустың таралуы, фишингтік шабуылдар немесе алаяқтықтың басқа түрлері болып табылады. Бұл пайдаланушылар үшін кері әсерін тигізуі мүмкін және қауіп төндіруі мүмкін, сондықтан киберспаммен күресу үшін антивирустық бағдарламалар және басқа да қорғаныс әдістері қолданылады.

8. Кибертыңшылық - бұл әдетте бизнесте немесе саясатта артықшылық алу үшін құпия ақпаратты немесе барлауды алу үшін цифрлық технологияларды пайдалану. Бұған компьютерлік жүйелерді бұзу, мемлекеттік органдарға, корпорацияларға немесе жеке тұлғаларға құпия ақпарат алу үшін жасалатын іс-әрекеттер. Кибер тыңшылықты әртүрлі мемлекеттік органдар, хакерлік топтар немесе киберқылмыскерлер жүзеге асыра алады.

9. Криптовалюталарды қолданатын киберқылмыстар - ақшаны жылыстату немесе криптовалюта желілерін пайдаланып бопсалау сияқты жасырын және заңсыз транзакциялар үшін криптовалюталар қолданылатын киберқылмыстар.

10. Маңызды инфрақұрылымға жасалған кибершабуылдар - бұл қоғамның, экономиканың және ұлттық қауіпсіздіктің қалыпты жұмыс істеуі үшін қажетті жүйелер мен объектілерге жасалған шабуылдар. Бұл энергетикалық желілер, көлік жүйелері, қаржы институттары, Денсаулық сақтау және басқа да негізгі нысандар болуы мүмкін. Мұндай жүйелерге жасалған шабуылдар қызметтердің тоқтап қалуы, істен шығуы, адамдардың қауіпсіздігіне қауіп төндіруі және бүкіл қоғамның бұзылуы сияқты ауыр зардаптарға әкелуі мүмкін.

Цифрлық кеңістіктегі қылмыстардың бұл түрлері деректердің қауіпсіздігіне, деректердің құпиялылығына және адамның психологиялық әл-ауқатқа үлкен қауіп төндіреді. Мұндай құқық бұзушылықтармен күресу қоғамдық хабардарлықты, тиісті заңдар мен қауіпсіздік шараларын қабылдауды, сондай-ақ цифрлық сауаттылық пен желідегі қауіпсіздік қоғамын оқытуды талап етеді.

Сандық кеңістіктегі құқық бұзушылықтарды шешу бірнеше себептерге байланысты өте маңызды:

1. Жеке деректердің қауіпсіздігі - киберқылмыспайдаланушылардың жеке ақпаратының қауіпсіздігіне қауіп төндіреді. Оны ұрлауға, алаяқтық немесе теріс пайдалану үшін пайдалануға болады.

2. Экономикалық салдары - кибершабуылдар компаниялар мен салаларға үлкен зиян келтіруі мүмкін, бұл қаржылық шығындарға, жұмыстың бұзылуына және клиенттердің сенімінің төмендеуіне әкелуі мүмкін.

3. Ұлттық қауіпсіздік - киберқауіпсіздік қаупі ұлттық қауіпсіздікке елеулі әсер етуі мүмкін, өйткені мемлекеттік жүйелер мен маңызды инфрақұрылымға жасалған шабуылдар елге қауіп төндіруі мүмкін.

4. Сенім және құпиялылық - цифрлық қоғамның жетістігі пайдаланушылардың өз деректерінің қауіпсіздігі мен құпиялылығына

деген сеніміне байланысты. Цифрлық кеңістіктегі құқық бұзушылықтар мәселесін шешу осы сенімді сақтауға ықпал етеді.

Бұл мәселені шешу тек техникалық қауіпсіздік шараларын жақсартуды ғана емес, сонымен қатар цифрлық ортадағы қауіп-қатерлермен күресу үшін заңнаманы, пайдаланушылардың білімін және халықаралық ынтымақтастықты дамытуды талап етеді.

Цифрлық кеңістіктегі құқық бұзушылық мәселесін шешудің кешенді жолдары:

1. Білім және хабардарлық - интернетті қауіпсіз пайдалану, цифрлық сауаттылық және киберқылмыстан қорғау әдістері туралы қоғамға білім беру бағдарламаларын жүргізу.

2. Заңнаманы күшейту - онлайн-ортада киберқауіптер мен құқық бұзушылықтардың жаңа түрлерін ескеретін және тиісті жазаларды қарастыратын заңдарды әзірлеу және қабылдау қажет.

3. Киберқауіпсіздікті дамыту - кибершабуылдардың алдын алу және цифрлық ортада қауіпсіздікті қамтамасыз ету үшін қорғаныс технологиялары мен әдістеріне инвестиция салу маңызды.

4. Елдер мен ұйымдар арасындағы ынтымақтастық - әртүрлі мемлекеттер мен халықаралық ұйымдар трансшекаралық киберқылмыспен күресу және қауіптер туралы ақпарат алмасу үшін бір мәмілеге келуі керек.

5. Құқық қорғау органдарының техникалық мүмкіндіктерін дамыту - киберқылмыстарға тиімді жауап беру үшін оқытылған кадрлар мен олардың алдын алу және тергеу үшін заманауи технологиялық шешімдер қажет.

6. Халықаралық ынтымақтастық - киберқауіптер және олармен күресудің жалпы әдістері туралы ақпарат алмасу бойынша елдер арасындағы ынтымақтастықты күшейту. Халықаралық келісімдер мен бастамалар киберқылмысқа қарсы тұрудың бірыңғай тәсілдерін жасауға көмектеседі.

7. Жаңа технологияларды дамыту - жасанды интеллект, машиналық оқыту және блокчейн сияқты инновациялық технологияларды киберқауіптерден тиімді қорғау үшін пайдалануға болады.

8. Киберқауіпсіздік бойынша арнайы бөлімдер мен бюролар құру - кадр бөлімшелерінің біліктілігін арттыру және киберқылмыстардың алдын алуға және тергеуге жауапты мамандандырылған органдар құру.

9. Саясат пен заңнаманы үнемі жаңартып отыру - технологияның дамуы мен жаңа қауіптердің пайда болуына сәйкес заңнама мен саясатты үнемі жаңартып отыру қажет.

10. Онлайн платформадағы тегін курстар ұйымдастыру - киберқауіптілікке қарсы күресудің маңыздылығын түсіндіру. көрсету және киберқауіптілікке жол бермеу әдістерін үйрету.

Киберқылмыс үнемі дамып келеді, сондықтан онымен тиімді күресу техникалық шешімдерді, заңнаманы және білім беру бағдарламаларын үнемі жаңартып отыруды талап етеді.

Біздің виртуалды әлемде цифрлық құқықбұзушылықтардың қауіп барған сайын жоғарылауда. Алайда, онымен бірге бұл қылмыстардың алдын алудың маңыздылығы артып келеді. Цифрлық қауіпсіздік мәселелерінде неғұрлым білімді және біліммен қамтамасыз етілген қоғам құру, мемлекеттік аппараттардың цифрлық білімін арттыру және заңнаманы ұдайы жетілдіру - қоғамның цифрлық осалдық деңгейін жоғарылатуға және цифрлық қылмыстардың әртүрлі түрлерінің алдын алуға негіз жасайды.

Цифрлық құқықбұзушылықтың алдын - алу үшін бірлескен күш - жігер қажет : қоғам, үкіметтер, технологиялық компаниялар және онлайн-саланың барлық қатысушылары. Қауіпсіздікті жақсарту үшін бірлескен әрекеттер мен үздіксіз жұмыс арқылы ғана біз барлық пайдаланушылар үшін қауіпсіз және қауіпсіз цифрлық ортаны жасай аламыз.

Цифрлық құқықбұзушылықтар ауыр зардаптарға әкелуі мүмкін, бірақ алдын алу, білім беру және ынтымақтастыққа назар аудара отырып, біз олардың әсерін азайтып, барлығына қауіпсіз және тұрақты онлайн кеңістік жасай аламыз.

Пайдаланылған қайнар көздерінің тізімі:

1. <https://egemen.kz/amp/article/33685-kiberqylmys-dgane-kiberpol>
2. <https://kaztag.info/kz/news/aza-standa-kiber-ylmys-zhiilep-ketti-deydi-iim>
3. <https://cyberleninka.ru/article/n/yuridicheskaya-otvetstvennost-v-tsifrovom-prostranstve>
4. <https://www.garant.ru/article/1528258/>
5. <https://online.zakon.kz/m/amp/document/39781841>
6. <https://cyberleninka.ru/article/n/internet-trolling-shalost-pravonarushenie-ili-prestuplenie>
7. <https://cyberleninka.ru/article/n/administrativnye-pravonarusheniya-sovershaemye-v-internete>

UDK 347.023

Soltangazy Diana
2 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

**THE IMPACT OF ARTIFICIAL INTELLIGENCE ON
EMPLOYMENT LAW**

Scientific supervisor:
Chingisbaeva A. E.
M.L.Sc., senior lecturer
Higher School of Law “Adilet”
Caspian Public University

Annotation

This article is devoted to the history of artificial intelligence and how it currently affects legal relations in Kazakhstan, more precisely on the regulation of labor relations with the participation of artificial intelligence, and how artificial intelligence helps people with disabilities to participate in labor relations on an equal basis with other participants

Key words: artificial intelligence, labor market, people with disabilities, object and subject of legal relations.

Солтангазы Диана Рустемқызы
Студентка 2 курса
Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ТРУДОВОЕ ПРАВО

Аннотация

Данная статья посвящена истории искусственного интеллекта и как он на данный момент влияет на правоотношения в Казахстане, точнее

на регулировании трудовых правоотношений с участием искусственно-го интеллекта, и как искусственный интеллект помогает людям с ограниченными возможностями выступать в трудовые правоотношения наравне с другими участниками

Ключевые слова: искусственный интеллект, рынок труда, люди с ограниченными возможностями, объект и субъект правоотношений.

Солтангазы Диана Рустемқызы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 2 курс студенті,

Қазақстан Республикасы, Алматы қ.

Аңдатпа

Бұл мақала пандемия кезінде қызметкер мен жұмыс беруші арасындағы қашықтан жұмыс істеуді реттеуге арналған, атап айтқанда, қызметкер қалыпты жұмыс режимінен телекоммуникацияға ауысқан кезде жұмыс берушінің әрекеті көрсетіледі, қазіргі еңбек тәртібіндегі соңғы өзгерістер қандай заңнамасында, аралас қашықтан жұмыс жасау түсінігі берілді

Түйінді сөздер: қашықтан аралас жұмыс істеу, ақпараттық-коммуникациялық технология, қызметкер, жұмыс беруші, хабарлама.

In recent years, artificial intelligence has become the most convenient and, at the same time, obscured tool for humanity. It all because of people's fear that AI will replace their place or even destroy achievements in certain areas. However, is it so serious or people just started exaggerating the power of AI? To understand the whole meaning of AI in our life, specifically in law, first of all we should know a little bit about the start of AI period in history.

One of the important milestones in AI is the work called «Computing Machinery and Intelligence» written by Alan Turing in 1950. That work was fundamental since Alan raised a question «Can machines think», which, at that time, was not such a matter in technology. Consequently, the Turing test was created, which was the first experiment proposed to measure machine intelligence. Since, the first “AI period” began with the Dartmouth conference in 1956, where AI got its name and mission. McCarthy coined the term “artificial intelligence,” which became the name of the scientific field. The primary conference assertion was, “Every aspect of any other feature of learning or intelligence should be accurately described so that the machine can simulate it” (Russell and Norvig 2016)[1]. Enthusiasm

arose as computers, for the first time, exhibited problem-solving capabilities akin to human intelligence, sparking excitement. The broader AI research community echoed this initial optimism, making assertive statements and gaining increased attention. Instances of AI successfully addressing problems encompassed a range of areas such as algebraic application problem-solving, language translation, geometric theorem proving, and more. As other fields and industries, employment and labour market also have been influenced.

In today's world, the influence of AI on the job market is contingent upon its widespread adoption and the pace of integration into workplaces. Nevertheless, this doesn't imply that every job is susceptible to automation. According to the mentioned report, occupations in healthcare, education, and social services are deemed less prone to automation due to their reliance on human interaction and empathy. Furthermore, the incorporation of AI into work environments presents a chance for employees to acquire new skills and progress in their careers. Industries like data analytics, software development, and machine learning are anticipated to expand in the future, opening up fresh prospects for workers. As AI technology continues to advance, legal frameworks may evolve to better address the complexities of AI in employment relationships. This could include specific regulations, guidelines, or standards that address the unique challenges posed by AI-driven workplaces

In Kazakhstan, at the moment, the regulation of legal relationships related to artificial intelligence has just begun to develop. The need for legal regulation of AI was first announced in 2021 in the presidential decree "On Approval of the Concept of Legal Policy until 2030". This decree says that «The need for legal regulation of artificial intelligence and robotics is primarily determined by the issue of distribution of liability for harm caused by their actions, as well as by solving the problem of determining the ownership of intellectual property rights to works created with the participation of artificial intelligence» [2]. Actually, the impact of AI on employment law is not discussed in this document as, currently, there were no serious violations related to it. However, even if we did not experience any difficulties because of AI in the workplace, it does not mean that we are guaranteed from them.

We all are used to traditional employment relationships in the workplace and cannot anticipate that something unusual will happen to this system. For us, the core of employment is interactions between people such as hiring or dismissing from work, because it has been happening for centuries. It was a huge shocking moment when people realized that their jobs, actually, can be lost just due to machines and supernatural inhuman things. Of course,

it will also cause problem in law as individuals, specifically employees, will not be satisfied by troubles caused by AI. One of the questions that bothers employers, employees and lawyers a lot is whether AI should be considered a subject or an object of labor legal relations remains pertinent. Two distinct perspectives on this matter have emerged:

1. AI as an Object of Labor Relations: In this view, AI is perceived as an object of labor relations. The responsibility for the work performed by AI should be placed on the employer whose interests the AI serves. This approach emphasizes the employer's accountability for the AI's labor.

2. AI as a Subject of Labor Legal Relations: On the contrary, some, like Professor Horst Eidenmüller from Oxford University, argue that AI should be treated as a subject of labor legal relations [3]. According to this perspective, if AI serves as a prototype of a human being, it should be recognized as a legal entity with all the attributes of a human worker. This entails endowing AI with similar rights and obligations as those applicable to a regular human worker.

Let's talk about first opinion, which claims that AI should be an object of Labour Relations. Today, from the point of view of civil law, a system equipped with AI is a thing. At the same time, the legislation does not contain any peculiarities of the legal regime of these things and does not restrict their circulation. However, this object has a number of features related to the possibility of its autonomous functioning. Therefore, activities related to the use of AI need special legal regulation. This is especially evident in the examples of the use of AI in medicine, transportation and other spheres, where the cost of AI going out of control may be not only property damage but even human health and life.

Here are my considerations regarding AI as an object in employment relationships:

1. In traditional employment relationships, AI is often viewed as a tool or instrument used by employers to enhance productivity and efficiency. It is considered a means through which tasks can be performed but is not granted legal personhood.

2. The responsibility for the actions and outcomes of AI systems in the workplace usually falls on the employer. If an AI system causes harm or makes a mistake, the employer is generally held accountable. Legal frameworks often attribute liability to human actors, such as employers or developers, rather than the AI itself. Law may need to evolve to clearly define the extent of liability and responsibility in cases where AI systems make autonomous decisions, especially when those decisions have legal or financial implications for employees.

3. Existing employment laws may not explicitly address the unique challenges posed by AI. As a result, there could be regulatory gaps regarding issues such as accountability, discrimination, and workers' rights in the context of AI-driven workplaces. Legal protections for workers may need to be adapted to account for the unique challenges posed by AI, ensuring that employees are not unfairly disadvantaged by automated systems.

4. The ethical use of AI in employment is an ongoing concern. Issues such as transparency, fairness, and the potential for bias in AI algorithms can impact the well-being of employees.

5. Despite the autonomous capabilities of AI, human oversight is often required, especially in decision-making processes that have significant implications for employees. The role of human supervisors and managers remains crucial in ensuring fair and ethical AI use in the workplace.

6. From an economic standpoint, AI is often viewed as a capital asset—a resource that contributes to the production process. This aligns with the traditional understanding of objects as elements used in economic activities.

It's important to note that while AI is commonly treated as an object, there is ongoing discussion and debate about the need for legal frameworks that recognize the unique aspects of AI, such as its ability to autonomously make decisions. As AI technology advances, legal perspectives may evolve to address the complexities associated with AI in a more nuanced manner. The classification of AI as an object is a current convention, and legal frameworks may adapt to better reflect the dynamic nature of artificial intelligence.

The second opinion is to consider AI as a subject. This viewpoint suggests that AI, particularly when designed to emulate human-like functionalities, should be recognized as a legal subject with its own set of rights and obligations within the context of employment. Here are some suggestions to this point:

1. Advocates of this perspective argue that if AI possesses characteristics resembling a human worker, it should be granted a form of legal personhood. This could include acknowledging AI's capacity to enter into contracts, assume liabilities, and be entitled to certain rights.

2. Treating AI as a subject implies endowing it with rights and obligations analogous to those of human workers. This includes considerations of fair treatment, protection from discrimination, and adherence to ethical standards in its actions.

3. Some advanced AI systems have the capability to make autonomous decisions. Recognizing AI as a subject of labor involves acknowledging its

role in decision-making processes and determining the legal consequences of its actions.

4. If AI is considered a subject of labor, there may be a need for legal protections to ensure its well-being. This could involve safeguarding against exploitation, ensuring fair working conditions, and addressing any potential harm caused by its actions.

5. The legal responsibility for the actions of AI could be attributed directly to the AI entity itself. This would involve determining when AI should be held accountable for its decisions and actions independently of its human operators or creators.

6. Treating AI as a subject in employment relations may lead to the development of a new area of law specifically focused on the rights and responsibilities of AI entities. This could include legislation and regulations tailored to address the unique legal challenges posed by AI in the workplace.

7. Recognizing AI as a subject of labor requires careful consideration of ethical implications, such as ensuring that AI is not subjected to unfair treatment, discrimination, or exploitation in the course of its "work."

The next interesting topic is the use and application of AI technologies in the employment domain from a disability rights perspective [4]. It obviously means that people with some health problems can do work that they thought they would never be able to do. Practically, achieving this goal involves creating and implementing active labor market policies aimed at addressing discriminatory attitudes toward individuals with disabilities in the employment sector. The focus should be on actively involving both public and private employers to integrate individuals with disabilities into the workforce. This recommendation is based on the belief that the inclusivity and accessibility of workplaces depend on the development and application of measures and tools that are most supportive and efficient in enabling individuals with disabilities to fulfill their job responsibilities. In this context, there is a widely acknowledged recognition that AI technologies play a crucial role in fostering workplace inclusivity and accessibility for individuals with disabilities. Notably, 12% of all AI patent applications are associated with the field of life, underlining the significance of AI in this regard [5]. AI can be broadly defined as computer algorithms designed to replicate human cognitive functions and capabilities. This includes tasks such as perceiving the environment, gathering information to make informed decisions, and refining actions through machine learning processes [6]. Similarly, the European Commission, in its Communication on AI, emphasizes that AI

encompasses systems exhibiting intelligent behavior. These systems analyze their surroundings and autonomously take actions to achieve specific goals. AI-based systems may exist purely in software form, operating in the virtual realm (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems). Alternatively, AI can be integrated into hardware devices, such as advanced robots, autonomous cars, drones, or Internet of Things applications [7].

Since the adoption of the United Nations Convention on the Rights of Persons with Disabilities (CRPD), there has been a growing recognition of the rights of individuals with disabilities in a world fraught with human rights challenges and tensions. The CRPD has laid the foundation for a comprehensive system of legal obligations, allowing for the regulation and evaluation of State conduct and various domains, including those involving advanced technologies like AI. The CRPD stands out as the preeminent standard-setting document concerning the rights of individuals with disabilities. Its rapid ratification by a majority of countries worldwide reflects a global commitment to safeguarding the rights of individuals with disabilities. Particularly noteworthy is Article 1 of the CRPD, which emphasizes that the Convention aims “to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity.” This underscores the overarching purpose of the CRPD in promoting inclusivity, respect, and the protection of the inherent dignity of individuals with disabilities on a global scale.

It’s crucial to note that, despite the widespread adoption and growing importance of AI technologies in advancing human well-being, several notable challenges, particularly in the realm of regulation, have emerged due to the multifaceted nature of AI technologies. This technological advancement has the potential to significantly improve employment opportunities for individuals with disabilities, but it also has the capacity to pose challenges. In contemporary times, private corporations are increasingly incorporating AI technologies into job applicant screening programs as part of their processes for selecting and recruiting employees.

However, in certain instances, these corporations tend to utilize AI-based software with non-transparently programmed and potentially biased algorithms in their employment recruitment processes. This could result in the reflection, whether intentional or unintentional, of discriminatory biases. Consequently, this may lead to the exclusion of qualified candidates based on their disability, potentially causing a backlash against the adoption

of advanced technologies, including AI, due to diminished social acceptance [8]. In simpler terms, when an algorithmic system is trained on non-inclusive or biased data, it tends to apply a “one-size-fits-all” approach when assessing the skills and qualifications of diverse groups of job applicants [9]. Clearly, the design and implementation of such AI programs carry significant human rights implications for individuals with disabilities, as they may result in the screening out or even, if not overtly, discrimination against “non-traditional” applicants, including those with disabilities. This could negatively impact employment opportunities for candidates with intellectual and other disabilities, potentially leading to unlawful discriminatory decisions by employers who rely on this algorithmic system in their decision-making processes.

In conclusion, the integration of AI technologies into the labor market holds both promise and challenges in bridging the gap between disability and employment opportunities. While AI has the potential to significantly enhance inclusivity and accessibility, facilitating meaningful employment for individuals with disabilities, there are notable concerns that must be addressed. The proliferation of AI in recruitment processes, if not carefully managed, can perpetuate biases and inadvertently lead to discriminatory outcomes. The transparency and fairness of AI algorithms are crucial considerations to ensure that qualified candidates are not unjustly excluded based on their disabilities. Striking a balance between leveraging AI for efficiency and safeguarding against unintended consequences is paramount. Moreover, the ethical and human rights implications of AI deployment in employment contexts should be at the forefront of regulatory considerations. Robust policies and frameworks are needed to guide the responsible design, implementation, and use of AI technologies, ensuring that they contribute positively to the inclusivity of the labor market. As we navigate the evolving landscape of AI and employment, it is imperative to prioritize proactive measures that mitigate potential biases, foster transparency, and uphold the rights of individuals with disabilities. By addressing these challenges, we can harness the full potential of AI technologies to create a more equitable and accessible labor market for everyone.

To conclude, we can see that AI has a lot of advantages which can be used in favor of people. However, in order to do it, we should determine how we will treat AI, as an object or a subject. Since we have some problems to regulate the legal relationships with AI, it is the matter of time when we get used to AI and take it granted.

References

1. Blagoj Delipetrev, Chrisa Tsinaraki, Uroš Kostić.-AI Watch Historical Evolution of Artificial Intelligence, pp 7
2. Указ Президента “Об утверждении Концепции правовой политики до 2030” /www.adilet.zan.kz
3. Eidenmueller H. The Rise of Robots and the Law of Humans // Oxford Legal Studies Research Paper. 2017. № 27.
4. Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice (Information Technology and Law Series, 35) 1st ed. 2022 Edition by Bart Custers (Editor), Eduard Fosch-Villaronga
5. World Trade Organization, World Health Organization, World Intellectual Property Organization 2020, p. 89.
6. World Trade Organization, World Health Organization, World Intellectual Property Organization 2020, p. 89. For existing definitions of AI, see also High-Level Expert Group on Artificial Intelligence 2019.
7. European Commission 2018, p. 1
8. ILO Global Business and Disability Network and Fundación ONCE 2019, p. 18. World Business Council for Sustainable Development 2020, p. 5. See also Outline for the preparation of a General Comment on Article 27 of the CRPD (the right to work and employment). European Disability Forum 2020, pp. 5–8. World Business Council for Sustainable Development 2020, p. 5.
9. Nugent et al. 2020, pp. 11–12. Employer Assistance and Resource Network on Disability Inclusion 2019, p. 4.
10. UN Convention on the Rights of Persons with Disabilities, UN Doc A/RES/61/106.

ӘОЖ 349

Сыдыкова Перизат

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 3 курс студенті,

Қазақстан Республикасы, Алматы қ.

ЖАСАНДЫ ИНТЕЛЛЕКТ

Ғылыми-жетекші:**Тлешалиев Н.Д.**

PhD., Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің
қауымдастырылған профессоры

Аңдатпа

Мақалада айта кететініміз жасанды интеллектінің заң ғылымында атқаратын рөлі қарастырылады. Автор бүгінгі таңда жасанды интеллектіге қатысты жалпы әлемдік нормативтік құқықтық реттеу мен нормативтік техникалық реттеудің толық болмауы проблемасына назар аударады. Оған қатысты заңнамалық қамтамасыз етудің ерекшеліктері қарастырылған, жасанды интеллекттің тұжырымдамасы оның негізгі белгілерін ашу арқылы жасалған және келтірілген.

Түйінді сөздер: жасанды интеллект, құқық, бетті тану, ұшқышсыз көлік, адамның негізгі құқықтары, құқық субъектілік, алгоритмдер, бағдарламалық код, машиналық оқыту.

Сыдыкова Перизат

студентка 3 курса Высшей школы права “Әділет”
Каспийского общественного университета
Республика Казахстан, г. Алматы

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ**Аннотация**

В статье рассматривается роль искусственного интеллекта в юриспруденции. Автор обращает внимание на проблему полного отсутствия на сегодняшний день общего глобального нормативно-правового регулирования и нормативно-технического регулирования, связанного с искусственным интеллектом. Рассмотрена специфика законодательного обеспечения, связанного с искусственным интеллектом, представлена концепция искусственного интеллекта, раскрывающая его основные особенности.

Ключевые слова: искусственный интеллект и право, искусственный интеллект, право, распознавание лиц, беспилотный транспорт, основные права человека, правосубъектность, алгоритмы, программный код, машинное обучение.

Sydykova Perizat

3 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE

Annotation

The article examines the role of artificial intelligence in jurisprudence. The author draws attention to the problem of the complete absence of general global regulatory and technical regulation related to artificial intelligence. The specifics of the legislative provision related to artificial intelligence are considered, the concept of artificial intelligence is presented, revealing its main features.

Key words: artificial intelligence and law, artificial intelligence, law, face recognition, unmanned transport, basic human rights, legal personality, algorithm, program code, machine learning.

Құқық саласындағы жасанды интеллект. Қазіргі уақытта жасанды интеллект технологиялары қарқынды дамып келеді, соның ішінде тұрақты нейрондық желілер технологиялары мен бұлтты инфрақұрылымдардың дамуына байланысты, есептеу, бұлыңғыр жүйелер технологиясы, энтропиялық басқару, интеллект, эволюциялық есептеу және т.б. Сонымен қатар, бүгінгі таңда жалпы әлемдік нормативтік құқықтық реттеу мен нормативтік техникалық реттеудің толық болмауы проблемасы бар. Басқа жүйелерге интеграциялау және жасанды интеллект технологияларын қолдануды бақылау. Бұл мақала құқықтық реттеудің ерекшелігін зерттеуге арналған. Жасанды интеллектті пайдалану және дамыту. Жасанды интеллектті анықтаудың кейбір тәсілдері және ғылыми әдебиеттерде орын алатын тиісті саланы заңнамалық қамтамасыз етудің ерекшеліктері қарастырылған, жасанды интеллекттің авторлық тұжырымдамасы оның негізгі белгілерін ашу арқылы жасалған және келтірілген. Атап айтқанда, ұсынылған анықтамаға сәйкес, жасанды интеллект жасанды күрделі болып табылады. Жасанды интеллект технологиялары бүгінде қарқынды дамып келеді, соның ішінде тұрақты нейрондық желілер технологияларының және бұлтты есептеу инфрақұрылымдарының, бұлыңғыр жүйе технологияларының, энтропиялық басқарудың, интеллектінің, эволюциялық есептеулердің және т.б.

Жасанды интеллект немесе жасанды интеллект (ағылш. Artificial Intelligence, AI) динамикалық есептеу ортасында адам миының бірқатар функционалдық мүмкіндіктерін имитациялауға мүмкіндік беретін бағдарламалық Алгоритмдер жиынтығы ретінде анықталады. Жасанды интеллект алгоритмдері машиналарға адамдар сияқты сезінуге, түсінуге, жоспарлауға, әрекет етуге және үйренуге мүмкіндік беретін бірнеше технологияны қолданады.

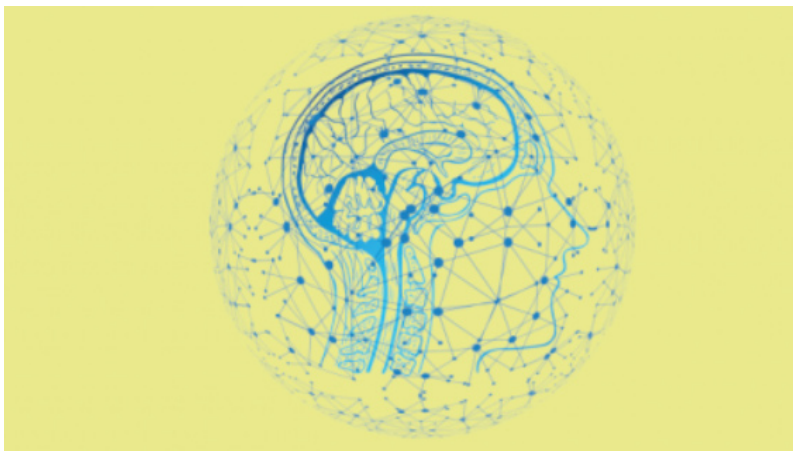
Жасанды интеллект жүйелері қоршаған ортаны қабылдайды, объектілерді таниды, шешім қабылдауға ықпал етеді, күрделі мәселелерді шешеді, өткен тәжірибелерден сабақ алады және үлгілерге еліктейді. Бұл қабілеттер өздігінен көлік жүргізу немесе құрылғы экрандарының құлпын ашу кезінде бетті тану сияқты тапсырмаларды орындау үшін біріктірілуі мүмкін.

AI, ең алдымен, адам миының жұмыс механизмдері мен қабілеттерін зерттеу арқылы дамиды, содан кейін бұл білімді “ақылды” машиналарға қолданады. Жасанды интеллекттің негізгі мақсаты-компьютерлік жүйелерге адамнан тәуелсіз жұмыс істеуге және толық интеллектуалды негізде шешім қабылдауға мүмкіндік беретін технологияны дамыту.

Жасанды интеллект ұғымның анықтамасы және маңызды белгілері:Жасанды интеллект-бұл жаңа құбылыс, ол бірқатар позициялар бойынша нақты зерттелмеген. Жасанды интеллект қарапайым компьютерлік алгоритмдерден ерекшеленеді, өйткені ол жинақталған тәжірибе негізінде өзін-өзі оқыта алады. Бұл бірегей мүмкіндік жасанды интеллектке бұрын жасалған әрекеттерге байланысты ұқсас ситуацияларында басқаша әрекет етуге мүмкіндік береді. Сондықтан “Жасанды инеллект” ұғымының жалпыға бірдей танылған анықтамасы бүгінде жоқ. Біздің авторлық анықтамамызға сәйкес, жасанды интеллект-ұл жасанды күрделі кибернетикалық Компьютерлік-бағдарламалық аппараттық жүйе (электронды, оның ішінде виртуалды, электронды механикалық функционалды архитектура және меншікті немесе тиісті түрде қол жетімді)өп жағдайда жасанды интеллекттің тиімділігі мен әлеуеті түсініксіз.

Құқықтық мәртебелердің гетерогенділігі жасанды интеллект объектілері:“Егер болашақтың жасанды интеллектісі үміттерді ақтайтын болса, яғни сезімдер мен эмоцияларға ие адам тәрізді роботтар болып шықса, онда қоғамдағы роботтардың рөлін қамту үшін заңдарды өзгерту қажет болады. Бұл қолданыстағы құқықтық жүйені қайта қарап, оны қоғамның өзгеріп отырған қажеттіліктеріне сәйкес бейімдеу ке-

рек дегенді білдіреді”. Жасанды интеллект (“ақылды” тұрмыстық техника) элементтері бар автономды жүйенің және толық құнды жасанды интеллектісі бар автономды объектінің (бұдан әрі, біздің тұжырымдамамызға сәйкес — ки бер-субъект) құқықтық мәртебесі бірдей бола алмайтыны анық. Үй серігі мен басқару жүйесінде кибер субъектінің құқықтық мәртебесі қалай бірдей бола алмайды. Жасанды интеллект (жасанды интеллект объектілері) жәнәтiптi толыққанды жасанды интеллект объектілері (кибер субъектілер) жоқадамдар болып табылады және ұқсас немесе ретінде орналаса алмайды. Бұл ең тікелей дәлел: тек адамдар ғана конституциялық құқықтарға ие болады деп күтуге болады. Ру мысалында АҚШ Конституциясына он төртінші түзету: “Америка Құрама Штаттарында туылған немесе натурализацияланған барлық адамдар, юрисдикцияның субъектісі бола отырып, Америка Құрама Штаттарының азаматтары болып табылады”. Тек адамдар (жеке тұлғалар) туа алады, сондықтан жасанды интеллект азаматтардың құқықтарын талап ете алмайды деп айтуға болады. Тiптi заңды тұлғалардың да кейбір құқықтары бар (мысалы, корпорациялардың меншігі әділ өтемақысыз алынудан қорғалады), содан кейін не бар-жеке тұлғалар азаматтық құқықтарға ие бола алады.



Даму нәтижесінде пайда болатын белгісіздіктер және жасанды технологияларды тарату интеллект және құқықтық тәсілдер жасанды интеллектті реттеу:” Даму нәтижесі өзінің қызмет принциптерінде формальды түрде белгіленгеннен ерекшеленеді, көбінесе мінез-құлықтың

бюрократиялық моделі. Ақпараттық технологиялар саласындағы операциялық жүйе және олардың ажырамас бөлігі-жасанды интеллект технологиялары, әртүрлі психиялылық, тұрақты дамуы және трансформация. Осы себепті осы саланы реттейтін нормативтік-құқықтық база: біріншіден, әмбебап болуы керек ақпараттық технологиялардың өзгеруіне қарамастан тиімді болу немесе екіншіден, ақпараттық технологиялардың қарқынды өзгеруі жағдайында оның тиімділігін қамтамасыз ету үшін үнемі түзетіліп отыру. Бұл ретте тұрақты өзгерістер енгізу заңнамасы. Ақпараттық технологиялар саласындағы өзгерістерге реакция ретінде, мүмкін мемлекеттік билік институттары қызметінің салыстырмалы түрде статикалық және айқын дәйекті сипатына байланысты іске асыру қиынға соғады”

Атап айтқанда, Жаңа Зеландия ұйымдары дайындаған көркемдік интеллектті қолдану ерекшеліктері туралы баяндамада, жасанды интеллект қазірдің өзінде қолданылып жүрген салалар тізімделеді, оның ішінде қызметті құқықтық реттеу үшін түбегейлі әртүрлі тәсілдер іске асырылатын мынадай бағыттар жатқызылды және принциптері:

- Көлік және логистика (көліктік жоспарлау, көрсету мақсатында жүргізушіге көмек көрсету, соқтығысудың алдын алу және т. б.);
- қаржылық қызметтер (атап айтқанда, деректерді талдау мақсатында);
- электрондық коммерция (мысалы, жасанды интеллект мақсатты мақсаттар үшін қолданылады);
- білім (мысалы, тілдік оқыту курстары аясында);
- Денсаулық сақтау (медициналық деректерді өңдеу және талдау, медициналық диагноз қою);
- робототехника;
- Машиналық оқыту;
- Қарулы Күштер.

Құқық және жаңа технологиялар: “өзін-өзі жетілдіруге қабілетті және жасанды интеллект жасау тәсілі бар супер интеллект әлі жасалмағанымен, бар роботтар өзін-өзі кіріктірілген қарапайым жасанды интеллект жүйелері адамдарға зиян келтіру қаупін тудыруы мүмкін.

Жасанды интеллект жүйелерін пайдалану және дамыту көптеген салаларда заң тұрғысынан даулы жағдайларды тудыруы мүмкін, олардың ішінде “жасанды интеллект және 2030 жылғы Өмір” баяндамасында былай жазылған:

- жеке ақпараттың құпиялылығын қамтамасыз ету мәселелері (жеке

тұлғаның жеке деректері арқылы қаншалықты ашылуы мүмкін жасанды интеллект қабылдаған шешімдер);

- инновацияны дамыту саласында тиімді саясатты әзірлеу мәселелері;

- азаматтық және қылмыстық жауапкершілікке тарту мәселелері;

- жасанды интеллектуалды жүйенің заңды тұлғасын анықтау мәселелері, атап айтқанда-ол қандай жағдайларда әрекет ете алады жеке немесе заңды тұлғаның делдалына шарт жасасуға;

- жасанды интеллект жүйелерін сертификаттау мәселелері.

Қорытынды

Жасанды интеллект құқыққа аса қатысты емес сала болып келеді,бірақ екеуін салыстырған адамдар өте көп болып келеді.Жасанды интеллект дамығанда өз еліміз әлдеқайда дамушы еді,сонымен қатар жақсы жетістіктерге жететін еді,бірақ әлі де кеш емес,сондықтан интернет пен айты саласын жақсартуға барлығымыз бірге ат салысуымыз керек.Менің алған ақпаратым ағылшын әдебиеттерінен болып келеді.

Пайдаланылған қайнар көздерінің тізімі:

1. Teleoperators and Virtual Environments. 14 (6), 741–748.
2. Availablefrom: doi:10.1162/105474605775196607. Čerka, P., Grigienė, J. &Sirbikytė, G. (2015)
3. Liability for Damages Caused by Artificial Intelligence. Computer Law & Security Review. 31 (3), 376–389.
4. Gasson, M. N. &Koops, B.-J. (2013) Attacking Human Implants: A New Generation of Cybercrime. Law, Innovation and Technology. 5 (2), 248–277. Hallevy, G. (2015)
5. LiabilityforCrimesInvolvingArtificial Intelligence Systems. Dordrecht, Springer. Availablefrom: doi:10.1007/978-3-319-10124-8. Johnson, D. G. (2014)
6. Technology with No Human Responsibility? Journal of Business Ethics. 127 (4), 707–715. Availablefrom: doi:10.1007/s10551-014-2180-1. Kemp, R. (2016)
7. Legal Aspects of Artificial Intelligence. London, Kemp IT Law. Availablefrom: <http://www.kempitlaw.com/wp-content/uploads/2016/11/Legal-Aspects-of-AI-Kemp-ITLaw-v1.0-Nov-2016-2.pdf> [Accessed 14th December 2017]. Nissan, E. &Martino, A. A. (2004) Artificial intelligence and formalisms for legal evidence: an
8. <https://eternalhost.net/blog/tehnologii/sistemy-iskusstvennogo-intellekta>

УДК 347.77

Таипова Даяна Тимуровнастудентка 3 курса юридического факультета
по специальности «Юриспруденция»Казахский национальный университет имени аль-Фараби
Республика Казахстан, г. Алматы**ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА В КАЗАХСТАНЕ И ЗА РУБЕЖОМ****Научный руководитель:****Калишева Н.Х.****д.ю.н, профессор,**Юридический факультет
КазНУ им. аль-Фараби**Аннотация**

В данной работе рассматривается правовое регулирование искусственного интеллекта (ИИ) в Казахстане и за рубежом. Анализируются существующие подходы к определению ИИ, его классификации и уровню развития. Исследуются вопросы ответственности за причинение вреда, причиненного ИИ, а также вопросы защиты интеллектуальной собственности в этой сфере.

Ключевые слова: искусственный интеллект, правовое регулирование, зарубежный опыт, интеллектуальная собственность, персональные данные.

Таипова Даяна Тимуровна

заң факультетінің 3 курс студенті

“Құқықтану” мамандығы бойынша

Әл-Фараби атындағы Қазақ ұлттық университеті

Қазақстан Республикасы, Алматы қ.

**ҚАЗАҚСТАНДА ЖӘНЕ ШЕТЕЛДЕ ЖАСАНДЫ
ИНТЕЛЛЕКТІНІ ҚҰҚЫҚТЫҚ РЕТТЕУ**

Аңдатпа

Бұл жұмыс Қазақстандағы және шетелдегі жасанды интеллекттің (AI) құқықтық реттелуін қарастырады. Жасанды интеллектіні анықтауға, оның жіктелуіне және даму деңгейіне қатысты қолданыстағы тәсілдер талданады. ЖИ келтірген зиян үшін жауапкершілік мәселелері, сондай-ақ осы саладағы зияткерлік меншікті қорғау мәселелері зерттеледі.

Түйінді сөздер: жасанды интеллект, құқықтық реттеу, шетелдік тәжірибе, зияткерлік меншік, дербес деректер.

Taipova Dayana Timurovna

3 year student

of the Faculty of Law,

specialty “Jurisprudence”

Al-Farabi Kazakh National University ,

Republic of Kazakhstan, Almaty

LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN KAZAKHSTAN AND ABROAD

Annotation

This work considers the legal regulation of artificial intelligence (AI) in Kazakhstan and abroad. Existing approaches to the definition of AI, its classification and level of development are analyzed. The issues of liability for harm caused by AI, as well as issues of protection of intellectual property in this area are investigated.

Key words: artificial intelligence, legal regulation, foreign experience, intellectual property, personal data.

Информационные технологии стремительно входят в сферу жизни как общества в целом, так и в жизнедеятельность отдельно взятого человека, живущего в настоящее время. Они становятся частью нашего обыденного существования.

Автомобили с автоматическим управлением, высококачественная робототехника, управление трафиком на основе ИИ, техническое обслуживание интеллектуальных сетей, да тот же самый ChatGPT, которым пользуется наверно каждый из здесь сидящих.

Разработки на основе ИИ, способствуют созданию цифровой среды, в которой государства и бизнес получают более широкие возможности для наблюдения за поведением человека, его анализа, прогнозирова-

ния и даже воздействия на него на беспрецедентном уровне. В процессе непрерывного сбора данных о человеке, к примеру, в сети Интернет, происходит деанонимизация каждого пользователя, создание «профиля» с указанием вероятных интересов человека, характеристик его личности. Влияние использования технологии ИИ на права человека является причиной переосмысления имеющихся подходов, направленных на защиту неприкосновенности частной жизни, сбора и хранения персональных данных, использования и раскрытия личной информации.

Какие же основные права и свободы в цифровом пространстве имеют место быть: в первую очередь – это право на защиту цифровой идентичности; право на доступ или отказ от доступа к цифровым технологиям; право на защиту ментальной неприкосновенности личности и защиту от манипуляции; право на защиту биометрических и других персональных данных.

В связи с этим стоит отметить, что в настоящее время правовое развитие не успевает за быстрорастущим прогрессом информационных технологий, что может служить одним из основных факторов столь слабого правового регулирования данной сферы и способствует возникновению существенных рисков.

Некоторые страны с осторожностью устанавливают правовое регулирование для технологий ИИ. К примеру, соответствующие инициативы/планы развития и проекты законов уже приняты к рассмотрению в:

- 1) США - National Artificial Intelligence Initiative;
- 2) Китае - New Generation of Artificial Intelligence Development Plan;
- 3) ЕС - Artificial Intelligence Act.

В свою очередь, в Казахстане о необходимости правового регулирования ИИ впервые было заявлено в 2021 году в Концепции правовой политики до 2030 г. В частности, было определено, что существуют, по крайней мере, два фактора, обуславливающих необходимость принятия регулирования технологий ИИ и робототехники:

- 1) решение вопросов распределения ответственности за вред, причиненный ИИ и роботами; а также
- 2) решение проблемы определения принадлежности права интеллектуальной собственности на произведения, созданные с участием ИИ.

Таким образом, несмотря на отсутствие специального регулирования ИИ, Казахстан обозначил два главных направления юридической работы по разработке правил функционирования ИИ.

Отметим, что вышеизложенные вопросы ответственности за вред, причиненный ИИ, и интеллектуальной собственности (а именно, кто

должен считаться автором произведения, созданного ИИ) активно обсуждаются во всем мире. По сей день международное сообщество в целом еще не разработало единого подхода в отношении регулирования ИИ.

В данном докладе мы постарались систематизировать некоторые подходы к правовому регулированию ИИ в развитых странах, а также обозначить основные вопросы права, которые должны учитываться при внедрении ИИ в бизнес-процессы.

Сначала давайте разберемся с самим понятием - искусственный интеллект.

На данный момент среди государств и научного сообщества отсутствует консенсус по единой легальной дефиниции термина «искусственный интеллект». К примеру, в США в 2020 г. принято следующее определение: искусственный интеллект – это машинная система, которая может для заданного набора задач, определяемых человеком, делать прогнозы, рекомендации или принимать решения, влияющие на реальную или виртуальную среду. В ЕС законопроект об искусственном интеллекте предлагает похожее определение ИИ: программное обеспечение, которое может для заданного набора задач, определяемого человеком, генерировать выходные данные, такие как контент, прогнозы, рекомендации или решения, влияющие на среду, с которыми оно взаимодействует.

Искусственный интеллект действительно использует компьютеры и машины, собирает и анализирует данные, чтобы имитировать способность человеческого разума делать прогнозы и рекомендации, решать проблемы и принимать решения.

К примеру, те же социальные сети анализируют наше поведение, активности и предлагают вам именно тот контент, которые был бы интересен именно Нам. Таким же образом ИИ предлагает и рекомендует нам сделать определенные покупки, «показывая» Нам рекламу того или иного продукта/услуги. Все эти примеры, по Моему мнению, связаны несколькими признаками, присущими ИИ:

- 1) ИИ использует (собирает, анализирует) данные;
- 2) ИИ имитирует человеческий интеллект/разум;
- 3) ИИ направлен на принятие решений, которые обычно принимаются человеком.

Теперь давайте поговорим об Искусственном интеллекте и интеллектуальной собственности

Мы бы хотели сфокусироваться на регуляторных подходах США и ЕС по вопросу о соотношении ИИ и интеллектуальной собственности в сравнении с казахстанским законодательством.

Перед тем, как перейти к анализу, хотели бы ознакомить Вас с результатами опроса об использовании компаниями ИИ, проведенного в Европе, в 2021 г., который дает представление о восприятии бизнесом ключевых, связанных с ИИ.

Так, на вопрос: Если ИИ создал объект интеллектуальной собственности, кто должен быть правообладателем? 58% опрошенных, что считают, что пользователь системы ИИ должен владеть правами интеллектуальной собственности, а 20% разделяют мнение, что права должны принадлежать изобретателю, и только 4% полагают, что сама система ИИ должна считаться правообладателем.

Теперь о регулировании искусственного интеллекта и интеллектуальной собственности в США.

Так, в 2020 г. американское Ведомство по патентам и товарным знакам (US Patent and Trademark Office) отметило, что действующее законодательство США не относит изобретения, созданные с помощью или непосредственно самим ИИ, к патентуемым, обосновывая это тем, что закон о патентах и правила Ведомства «однозначно» признают изобретателем только физических лиц (individuals). Суд в 2021 г. поддержал решение Ведомства не регистрировать изобретение, тем самым признав, что в США изобретения не могут быть зарегистрированы за ИИ.

Для сравнения, казахстанское законодательство в отношении промышленной собственности аналогичным образом указывает, что автором объекта промышленной собственности признается только физическое лицо, творческим трудом которого объект создан. Учитывая действующие нормы Патентного закона, мы считаем, что Национальный институт интеллектуальной собственности также отказал бы в регистрации объекта промышленной собственности, где заявителем выступает ИИ.

Что касается объектов авторских прав, то американское Ведомство не расценивает ИИ в качестве автора произведений, поскольку из смысла законодательства США об авторском праве следует, что «плоды интеллектуального труда основаны на творческих способностях человеческого разума», соответственно произведения могут быть созданы только человеком. В 2022 году Ведомство, отказав в заявке о признании ИИ автором, отметило, что оно не будет регистрировать произведения, «созданные машиной или простым механическим процессом», который работает «без какого-либо творческого вклада или вмешательства со стороны человека».

Таким образом, в США на данный момент невозможно признать ИИ автором произведений. Казахстан также признает авторами только физических лиц, а сами произведения должны быть созданы творческим трудом человека.

А как обстоят дела в ЕС.

В отношении прав интеллектуальной собственности в законодательстве Европейского союза также преобладает подход, определяющий человеческий фактор в качестве основного для определения принадлежности прав. Так, Европарламент установил, что технология ИИ не наделена правоспособностью и человеческим разумом, в связи с чем ИИ, создающий произведения или изобретения самостоятельно, не будет признаваться автором объектов интеллектуальной собственности. При этом отмечается, что если ИИ будет использоваться только как инструмент, помогающий автору в процессе создания, то в этом случае будут применимы общие положения законодательства ЕС об интеллектуальной собственности.

Таким образом, Европейский союз предпринял попытку разграничить подход к работам, созданным с помощью ИИ и к случаям, когда ИИ создавал бы произведения самостоятельно.

В первом случае, насколько мы понимаем, принадлежность прав интеллектуальной собственности будет бесспорно признана за лицом, использующим ИИ для создания объектов творческого труда.

Так, в 2021 году, Федеральный патентный суд Германии указал, что изобретения, созданные ИИ, «не исключаются из патентной защиты, при условии, что в заявке к патенту в качестве изобретателя указан человек». Тем самым, немецкий суд признает, что ИИ может указываться в качестве изобретателя, но только как дополнительный изобретатель, основным должен обязательно указываться человек, создавший изобретение.

Исходя из вышеперечисленного можно сделать вывод, что казахстанский, американский и европейский подходы к соотношению принадлежности прав интеллектуальной собственности и ИИ имеют мало отличий – оба подхода фокусируются на человеческом факторе и на отсутствии правоспособности ИИ как таковой, но при этом Евросоюз предпринимает инициативы по дальнейшему регулированию технологии с более благоприятной по отношению к ИИ позиции.

В нашем понимании вопрос о принадлежности прав интеллектуальной собственности на произведения в случае с ИИ является важным и для целей определения лица, ответственного за вред, причиненный

ИИ. Поэтому необходимо дальнейшее развитие законодательства в этом направлении.

Искусственный интеллект и персональные данные

Как мы указывали ранее, одним из основных признаков ИИ является сбор и анализ данных. Среди данных, используемых ИИ, могут быть и персональные данные.

В странах ЕС внедрены и работают положения GDPR (Общий регламент по защите данных), направленные на защиту персональных данных от незаконного использования. Учитывая положения GDPR, в ЕС уже создали список запрещенной практики ИИ. Так, согласно законопроекту, Artificial Intelligence Act планируется запретить использование ИИ для:

1) любого типа социального скоринга (системы социального рейтинга);

2) дистанционной биометрической идентификации физических лиц в общедоступных местах (автоматизированное распознавание черт человека (лицо, радужная оболочка, отпечатки пальцев, ДНК, голос), нажатие клавиш, ритмы и т.д.;

3) определения эмоций людей;

4) классификации людей на основе биометрических данных по этническому признаку, полу, политической или сексуальной ориентации, или других особенностей, которые могут привести к дискриминации.

В ЕС возможно привлечение компаний к ответственности за незаконное использование ИИ и по действующему законодательству.

В Казахстане, в свою очередь, действует Закон о персональных данных, и компании несут ответственность за нарушения этого Закона. При этом, в Казахстане еще не предприняты попытки прямого урегулирования использования ИИ в разрезе защиты данных. Но, учитывая некоторые требования действующего Закона, можно сказать, что бизнес может быть существенно ограничен в использовании ИИ, к примеру, если для работы ИИ требуются те же биометрические данные

Таким образом в Казахстане назревает острая необходимость в законодательном урегулировании использования ИИ. Казахстанское право должно определить, по крайней мере, следующие основные положения для дальнейшего развития ИИ:

1) Что такое и какие признаки присущи ИИ?

2) Кто может признаваться автором и правообладателем ИИ?

3) Кто несет ответственность за вред, причиненный вследствие использования ИИ?

4) Какие данные и при каких условиях может собирать и использовать ИИ?

Эти же вопросы, по моему мнению, следует прорабатывать и бизнесу при внедрении любых систем ИИ, основываясь на действующем законодательстве.

Список использованных источников:

5. Национальная стратегия развития искусственного интеллекта на период до 2025 года

6. Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования деятельности в сфере информационных технологий»

7. Регламент (ЕС) 2021/2100 Европейского парламента и Совета от 19 апреля 2021 года об искусственном интеллекте и о внесении изменений в некоторые законодательные акты Союза и устанавливающий определенные правила относительно машинного обучения и о внесении изменений в Регламент (ЕС) 2016/679

8. Закон США «Об ответственном развитии искусственного интеллекта»

УДК 349

Турдалиев Кенан Камал оглы

Студент 1 курса Высшей школы права «Әділет»

Каспийского общественного университета,

Республика Казахстан, г. Алматы

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Аннотация

В статье рассматривается одна из областей современной науки и технологий - искусственный интеллект. Изучены несколько основных аспектов искусственного интеллекта, его применение в различных областях и возможности решения некоторых текущих проблем. Дано определение ИИ и его основные принципы, обращено внимание на специфику и области использования искусственного интеллекта. Автор рассматривает вызовы и препятствия на пути развития искусственного интеллекта, которые еще необходимо преодолеть, отмечая, что необхо-

димо быть бдительными в отношении этических, социальных и правовых вопросов, связанных с применением искусственного интеллекта.

Ключевые слова: искусственный интеллект, принципы, автоматизация процессов, машинное обучение, обработка данных, робототехника, этические вопросы.

Турдалиев Кенан Камал оглы

Каспий қоғамдық университеті

«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

ЖАСАНДЫ ИНТЕЛЛЕКТ

Аңдатпа

Мақалада қазіргі ғылым мен техниканың бір саласы – жасанды интеллект қарастырылады. Жасанды интеллектінің бірнеше негізгі аспектілері, оның әртүрлі салаларда қолданылуы және кейбір өзекті мәселелерді шешу мүмкіндіктері зерттеледі. Жасанды интеллектіне анықтама беріліп, және оның негізгі принциптері қарастырылып, жасанды интеллектіні қолдану ерекшеліктері мен оның қолданысы табу мүмкін салаларына назар аударылады. Автор жасанды интеллектті дамыту жолындағы әлі де еңсеруді қажет ететін қиындықтар мен кедергілерді қарастырып, жасанды интеллектіні қолданумен байланысты этикалық, әлеуметтік және құқықтық мәселелерге қырағылық таныту керектігін атап өтеді.

Түйінді сөздер: жасанды интеллект, принциптер, процестерді автоматтандыру, машиналық оқыту, деректерді өңдеу, робототехника, этикалық мәселелер.

Turdaliev Kenan Kamal ogly

1 year student of the Higher School of Law «Adilet»
Caspian Public University,
Republic of Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE

Annotation

The article examines one of the areas of modern science and technology - artificial intelligence. Several basic aspects of artificial intelligence, its application in various fields and the possibilities of solving some current

problems are studied. The definition of AI and its basic principles is given, attention is drawn to the specifics and areas of use of artificial intelligence. The author examines the challenges and obstacles to the development of artificial intelligence that still need to be overcome, noting that it is necessary to be vigilant regarding the ethical, social and legal issues associated with the use of artificial intelligence.

Keywords: artificial intelligence, principles, process automation, machine learning, data processing, robotics, ethical issues.

Введение

В данной статье хотелось бы обратить ваше внимание на одну из самых захватывающих областей современной науки и технологий - искусственный интеллект. Искусственный интеллект стал неотъемлемой частью нашей жизни, проник во все сферы деятельности, от медицины и транспорта до финансов и развлечений.

Искусственный интеллект представляет собой совокупность методов и алгоритмов, которые позволяют компьютерным системам перенимать и эмулировать некоторые аспекты человеческого интеллекта. Он способен не только анализировать и обрабатывать огромные объемы информации в режиме реального времени, но и принимать решения на основе полученных данных.

Применение искусственного интеллекта оказывает значительное влияние на различные сферы нашей жизни. В медицине, например, он помогает диагностировать болезни, прогнозировать их развитие и предлагать оптимальные методы лечения. В автомобильной промышленности искусственный интеллект уже нашел свое применение в системах самоуправления автомобиля и безопасности на дороге.

Однако, несмотря на все преимущества, искусственный интеллект ставит перед нами множество новых этических, социальных и экономических вопросов. Нам следует внимательно обращаться с этой технологией, чтобы использовать ее потенциал максимально эффективно и справедливо.

Актуальностью искусственного интеллекта является эффективность и производительность труда путем автоматизации процессов и задач, которые ранее выполнялись людьми. С каждым днем ИИ становится все более актуальным и необходимым для нашей жизни. Он используется в самых разнообразных областях.

В данной статье попробуем рассмотреть несколько основных аспектов искусственного интеллекта, его применение в различных областях и возможности решения некоторых текущих проблем.

Определение ИИ и его основные принципы

Искусственный интеллект впечатляет и вдохновляет. Правда, многие не до конца понимают, что скрывается под термином “искусственный интеллект” или более популярным его названием “ИИ”. Тот факт, что алгоритм или девайс способны делать что-то лучше человека, только распаляет воображение. Хотя эта технология не нова, последние достижения программного масштабирования позволили ей решать более сложные задачи. ИИ предлагает наилучшие обоснованные решения в кратчайшие сроки.

Искусственный интеллект – это цифровое воспроизведение процессов сознательной активности человека и социума в целом в части творческой обработки и рассуждений на основе нетривиально формализуемой информации в условиях временных и ресурсных ограничений неопределенности и неполноты исходных данных, создающее кибернетические объекты, способные самостоятельно ставить цели и их достигать с качеством не ниже среднего специалиста, способное в перспективе заменить существующие виды деятельности и профессии.

Искусственный интеллект — это направление информатики, целью которого является разработка аппаратно-программных средств, позволяющих пользователю-непрограммисту ставить и решать свои традиционно считающиеся интеллектуальными задачи, общаясь с ЭВМ на ограниченном подмножестве естественного языка[1,5 с.].

Основные принципы искусственного интеллекта включают в себя:

Машинное обучение

Машинное обучение – это метод, при котором компьютерные системы обучаются на основе данных и опыта, чтобы улучшать свою производительность и делать предсказания или принимать решения без явного программирования. Машинное обучение является одной из основных техник в области искусственного интеллекта.

Обработка естественного языка

Обработка естественного языка (Natural Language Processing, NLP) – это область искусственного интеллекта, которая занимается анализом, пониманием и генерацией естественного языка человека. Системы обработки естественного языка позволяют компьютерам взаимодействовать с людьми на естественном языке, а также анализировать и извлекать информацию из текстовых данных.

Компьютерное зрение

Компьютерное зрение – это область искусственного интеллекта, которая занимается разработкой систем и алгоритмов для анализа и

интерпретации изображений и видео. Системы компьютерного зрения позволяют компьютерам “видеть” и распознавать объекты, лица, движения и другие визуальные данные.

Робототехника

Робототехника – это область искусственного интеллекта, которая занимается разработкой и созданием роботов, способных взаимодействовать с окружающей средой и выполнять различные задачи. Роботы с искусственным интеллектом могут быть запрограммированы для выполнения сложных задач, таких как автономное движение, манипуляция объектами и взаимодействие с людьми.

Искусственный интеллект имеет широкий спектр применений и влияний на различные области жизни, включая медицину, транспорт, финансы, образование и многие другие. Развитие искусственного интеллекта представляет большой потенциал для улучшения нашей жизни и решения сложных проблем, но также вызывает вопросы и вызовы в области этики, безопасности и социального влияния.[3]

2. Специфика и области использования искусственного интеллекта

От характеристик и особенностей работы каждой конкретной системы зависят нюансы применения искусственного интеллекта. Но наряду с этим можно выделить общую особенность его применения, присущую практически каждой сфере. Это присутствие системных ошибок. Этой особенностью нельзя пренебрегать, поэтому даже при полном охвате искусственным интеллектом той или иной сферы, при его работе необходимо участие человека. Этот момент важен практически в каждой сфере, где есть необходимость принятия важных решений. Например, в медицине, где в центре внимания стоит жизнь и здоровье человека. В транспортной сфере, где существует риск аварии на дороге.

Области использования искусственного интеллекта

Несмотря на то, что искусственный интеллект используется сравнительно недавно, на сегодняшний день он нашел применение во многих областях производства и жизнедеятельности человека, даже там, где его применение еще недавно казалось просто невозможным. Рассмотрим яркие примеры его применения, которые уже имеют место сегодня и планируются в ближайшее время.

Медицина

Хорошая память и способность к переработке большого объема данных, проводя их анализ и выборку необходимой информации, явля-

ются важными характеристиками искусственного интеллекта. Именно эти характеристики способствовали его внедрению в сфере медицины. Таким образом работает система DeepMind Heals фирмы Google, система Watson фирмы IBM. Их применяют для выявления вероятности заболеваний пациентов на ранних стадиях. К ним обращаются доктора для получения рекомендаций. В России в 2017 году принято решение на внедрение системы искусственного интеллекта в медицинской сфере. На сегодняшний день работает система «Третье мнение», которая помогает докторам вырабатывать решения. Она обрабатывает снимки дна глаза и кровяных клеток, рентгеновские снимки легких, УЗИ мочевого пузыря, планируется использовать ее для обработки МРТ и компьютерных томограмм. Также работает система Botkin.AI. Она анализирует диагнозы, дает консультации, контролирует прохождение процедур, а также имеет ряд других функций. В основном используется в онкологическом направлении, но планируется расширение применения и в других сферах медицины.

Искусственный интеллект используют как доктора, так и пациенты. Широкой популярности набирает телемедицина и ее различные приложения. Используются различные способы взаимодействия, например, закрепление датчиков (например, фитнес-браслетов) на пациенте и считывание с них информации, использование опросников и выдача вероятных диагнозов, на основании ответов, а также рекомендаций лечения. Такие приложения зачастую работают с функцией распознавания речи или сообщений.

Самые распространенные приложения такого плана - это Your.MD и Ada. Они есть на сервисах Google Play и App Store.

Промышленность

В промышленном производстве быстрыми темпами автоматизируются все процессы, даже в некоторых компаниях и вовсе исключено влияние человеческого фактора. К примеру, фирма LG планирует в 2023 году запустить линию производства, где полностью все автоматизировано и управляется системой искусственного интеллекта, которым будет контролироваться абсолютно все, начиная от закупки расходных материалов, заканчивая контролем качества товаров и их отправкой конечному потребителю. Помимо этого, искусственным интеллектом будет контролироваться износ запасных частей и основных средств, а также иные важные параметры, которые будут заданы.

Сельское хозяйство

В сфере сельского хозяйства применение искусственного интеллекта вызвано необходимостью контролировать влажность и температуру воздуха и почвы, присутствие нужной концентрации удобрений, развития растений и общего ухода за ними. Например, машины уже умеют обнаружить вредные растения и удалить их, выдергивая из почвы без вреда выращиваемым растениям. Сельскохозяйственные системы умеют обнаруживать заболевания растений, доставлять необходимые медикаменты для их лечения. Это экономит расход пестицидов и гербицидов.

Транспортная сфера

В развитых странах систему искусственного интеллекта используют для регулировки движения городского транспорта и решения проблем с городскими пробками. В России, к примеру, уже используется система искусственного интеллекта, в частности для регулировки движения транспорта в городах с большой дорожной сетью и на основных магистральных дорогах. Система интеллекта использует и обрабатывает данные со светофоров, об интенсивности транспортных потоков, погодных условиях и прочих факторах, влияющих на скорость и интенсивность дорожного движения. Анализируя эти данные, система работает в оптимальном режиме и переключает светофоры в нужное время.[2]

3. Будущее ИИ

Мы считаем, то что искусственный интеллект находится на стадии развития и думаю , что он в будущем очень сильно повлияет на жизнедеятельность людей ,так как смотря на первые шаги развития его можно уже понять что искусственный интеллект это то что будет охватывать практически все области как полностью так и частично.

Искусственный интеллект перестал быть научной фантастикой и уже сейчас основательно входит в нашу жизнь. Учёные, работая над технологией, заставляют её действовать всё более похоже на настоящий мозг. Компьютеры распознают лица, прогнозируют дорожную ситуацию, предупреждают о проблемах со здоровьем.

Но несмотря на то, что мы видим впечатляющие проекты, доказывающие, что интеграция ИИ делает жизнь удобнее и безопаснее, будущее искусственного интеллекта впереди. Инженеры считают, что нынешний уровень использования ИИ даже близко не отображает весь его потенциал, а индустрия находится в зачатке.

Но есть вызовы и препятствия на пути развития искусственного интеллекта, которые нам нужно преодолеть ,чтобы он работал так скажем в совершенстве.

Ограниченность данных

Для обучения искусственного интеллекта требуются большие объемы данных. Однако, в некоторых областях, таких как медицина или космос, доступ к данным может быть ограничен из-за конфиденциальности или сложности сбора информации. Это создает препятствия для развития ИИ в этих областях.

Недостаток качественных данных

Для эффективного обучения ИИ необходимы данные высокого качества. Однако, в реальном мире данные могут быть зашумленными, неполными или содержать ошибки. Это может привести к неправильным выводам и недостаточной точности моделей ИИ.

Этические вопросы

Развитие ИИ вызывает ряд этических вопросов. Например, как обеспечить безопасность и конфиденциальность данных? Как избежать пристрастия и дискриминации в алгоритмах ИИ? Как решать этические дилеммы, возникающие при принятии решений ИИ? Решение этих вопросов является важным аспектом развития ИИ.

Недостаток прозрачности и объяснимости

Некоторые алгоритмы ИИ, такие как нейронные сети, могут быть сложными и непрозрачными. Это означает, что они могут давать точные результаты, но не объяснять, как они пришли к этим результатам. Это создает проблемы доверия и понимания для пользователей и специалистов в области ИИ.

Регулирование и нормативные вопросы

Развитие ИИ также вызывает вопросы регулирования и нормативного контроля. Какие правила и законы должны быть установлены для использования ИИ? Как обеспечить безопасность и ответственность в использовании ИИ? Решение этих вопросов требует сотрудничества между правительством, индустрией и обществом.[4].

Все эти вызовы и препятствия требуют внимания и решения для успешного развития искусственного интеллекта. Однако, с учетом активного исследования и развития в этой области, ожидается, что многие из этих проблем будут преодолены, и ИИ будет продолжать прогрессировать и преобразовывать наш мир.

Заключение

В заключение хотелось бы подчеркнуть, что искусственный интеллект уже сегодня является неотъемлемой частью нашей жизни и оказывает значительное влияние на различные сферы деятельности. С его

помощью мы сможем достичь новых высот в медицине, науке, технологиях и многих других областях.

Однако, нельзя забывать о том, что искусственный интеллект не является идеальным искусством, а лишь инструментом, который мы должны использовать со смекалкой и ответственностью. Мы должны быть бдительными в отношении этических, социальных и правовых вопросов, связанных с применением искусственного интеллекта.

Важно также обеспечить участие различных групп и общественности в процессе разработки и принятия решений по использованию искусственного интеллекта. Равноправный доступ к этим технологиям должен быть гарантирован, чтобы не допустить углубления разрыва между различными социальными слоями.

Искусственный интеллект предоставляет нам огромные возможности и вызывает множество вопросов. Совместными усилиями мы можем строить будущее, в котором искусственный интеллект будет служить интересам человечества, обеспечивая благополучие, развитие и справедливость.

Благодарю вас за внимание и интерес к теме искусственного интеллекта. Я надеюсь, что исследование помогло вам более глубоко понять и оценить значимость и потенциал этой уникальной технологии. Давайте вместе осознаем и руководствуемся принципом использования искусственного интеллекта во благо всего человечества.

Список использованных источников:

1. Боровская Е. В. Основы искусственного интеллекта : учебное пособие / Боровская Е. В., Давыдова Н. А. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 130 с.
2. https://spravochnikvs.com/oblasti_primeneniya_iskusstvennogo_intellekta
3. https://nauchniestati.ru/spravka/ii-i-budushhee-chelovechestva/#Искусственный_интеллект_определение_и_основные_принципы
4. https://nauchniestati.ru/spravka/budushhee-ii/#Будущие_возможности_и_применения_искусственного_интеллекта

УДК 349

Уксикбаева Камилла

студентка 1 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

ПОНЯТИЕ КИБЕРПРЕСТУПНОСТИ И ПУТИ БОРЬБЫ С НЕЙ

Научный руководитель:

Калимбекова А.Р.

к.ю.н., ассоциированный профессор
Высшей школы права «Әділет»
Каспийского общественного университета

Аннотация

В статье рассмотрено понятие киберпреступности и пути борьбы с ней. Автор рассматривает преступления в сфере кибертехнологии, разделив их условно на три категории; шпионаж, информационные войны и кибератаки. Также уделено внимание фишингу как методу мошенничества, при котором злоумышленники пытаются получить доступ к информации, и хакингу как процессу получения несанкционированного доступа к компьютерным системам или сетям и предлагаются методы борьбы с ними.

Ключевые слова: фишинг, хакинг, информационные войны, кибератаки, кибертехнологии, киберпреступность, безопасность, доступ к личным данным.

Уксикбаева Камилла

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 1 курс студенті,
Қазақстан Республикасы, Алматы қ.

КИБЕРҚЫЛМЫС ТҮСІНІГІ ЖӘНЕ ОНЫМЕН КҮРЕСУ ЖОЛДАРЫ

Аңдатпа

Мақалада киберқылмыс түсінігі және онымен күресу жолдары қарастырылған. Автор кибертехнологиялар саласындағы қылмыстарды қарастырып, оларды үш санатқа бөледі: тыңшылық, ақпараттық соғыс және кибершабуылдар. Сондай-ақ шабуылдаушылар ақпаратқа қол жеткізуге тырысатын алаяқтық әдісі ретінде фишингке және компьютерлік жүйелерге немесе желілерге рұқсатсыз қол жеткізу процесі ретінде бұзуға назар аударылады және олармен күресу әдістері ұсынылады.

Түйінді сөздер: фишинг, хакерлік, ақпараттық соғыс, кибершабуылдар, кибертехнологиялар, киберқылмыс, қауіпсіздік, жеке деректерге қол жеткізу.

Uksikbaeva Kamilla

1 year student of the Higher School of Law «Adilet»

Caspian Public University,

Republic of Kazakhstan, Almaty

THE CONCEPT OF CYBERCRIME AND WAYS TO COMBAT IT

Annotation

The article discusses the concept of cybercrime and ways to combat it. The author examines crimes in the field of cyber technology, dividing them into three categories: espionage, information warfare and cyber attacks. Attention is also paid to phishing as a method of fraud in which attackers try to gain access to information, and hacking as the process of gaining unauthorized access to computer systems or networks, and methods to combat them are proposed.

Key words: phishing, hacking, information warfare, cyber attacks, cyber technologies, cyber crime, security, access to personal data.

Сегодняшний мир технологичен, интернет, цифровые валюты, социальные сети, автоматизированные системы, искусственный интеллект. Все это стало важной частью нашей жизни. Новые технологии улучшают нашу жизнь, но вместе с тем, появляются и новые угрозы, такие как киберпреступность.

Что мы знаем о киберпреступности?

Преступления в сфере кибертехнологии можно поделить условно на 3 категории:

- Шпионаж
- Информационные войны
- Кибератаки

Шпионаж ведется с целью перехвата секретной информации отдельных лиц, организаций и учреждений.

В **информационных войнах** используются различные средства воздействия на поведения людей, могут быть использованы СМИ, социальные сети.

Кибератаки предполагают реальное воздействие на телекоммуникационные сети, объекты инженерной, а также транспортной инфраструктуры, информационные и др. системы.

Фишинг — это метод мошенничества, при котором злоумышленники пытаются получить доступ к чувствительной информации, такой как пароли или банковские данные, путем маскировки под доверенные организации или отправителей. Они могут использовать поддельные электронные письма, веб-сайты или сообщения, чтобы заполучить личные данные от своих жертв.

Хакинг — это процесс получения несанкционированного доступа к компьютерным системам или сетям. Хакеры, используют различные методы и техники для проникновения в защищенные системы с целью получения, изменения или уничтожения данных.

Хакеры могут использовать уязвимости в программном обеспечении, слабые пароли, социальную инженерию или другие методы, чтобы проникнуть в систему. Они могут красть личную информацию, финансовые данные, взламывать электронные почты, вредоносными программами или фишинговыми атаками.

Независимо от того, кто занимается хакингом, важно принимать меры по обеспечению безопасности, такие как использование сильных паролей, регулярное обновление программного обеспечения, ограничение доступа к системам и обучение пользователей основам безопасности в сети.

Безопасное хранение персональных данных — это важная проблема, особенно в эпоху цифровой информации. Некорректное или небезопасное хранение персональных данных может привести к утечкам информации, мошенничеству или нарушению конфиденциальности.

Неграмотность и халатное отношение населения к собственным данным, а также недостаток понимания важности конфиденциальности, являются серьезными проблемами в безопасности данных.

Некоторые распространенные проблемы в этой области включают:

1. Слабые пароли: Многие люди используют слабые пароли, такие как «123456» или «password», что делает их учетные записи уязвимыми для взлома.

2. Несанкционированное использование общедоступных сетей Wi-Fi: Люди могут подключаться к общедоступным сетям Wi-Fi без использования шифрования и без защиты своих данных, что может привести к утечке личной информации.

3. Несоответствующее пользование социальными сетями: Многие пользователи социальных сетей не осознают, какую информацию о себе они раскрывают и кому она становится доступной. Это может привести к утечке конфиденциальных данных.

4. Недостаточное обновление программного обеспечения: Некоторые пользователи не обновляют свое программное обеспечение, что оставляет системы уязвимыми для известных угроз и атак.

5. Небезопасное хранение данных: Многие люди сохраняют свои личные данные на незащищенных устройствах или облачных хранилищах без использования шифрования или других мер безопасности.

Для решения этих проблем необходимо обращать больше внимания на образование и повышение осведомленности о безопасности данных. Важно обучать людей о правильном использовании паролей, защите Wi-Fi-соединений, конфиденциальности в социальных сетях и обновлении программного обеспечения. Также необходимо повышать осведомленность о рисках утечки данных и важности сохранения конфиденциальности.

Соблюдение этих мер поможет минимизировать риски и обеспечить безопасное хранение персональных данных.

Государства и организации также должны играть активную роль в создании законодательства и политик, которые обязывают защищать персональные данные и обеспечивать конфиденциальность. Это может включать требования к организациям по обеспечению безопасности данных и наказания за нарушение конфиденциальности.

В целом, борьба с киберпреступностью и кибервойнами требует внимания и сотрудничества всех сторон: пользователей, организаций и правоохранительных органов. Образование пользователей, использование надежных паролей, обновление программного обеспечения и регулярное резервное копирование данных могут снизить риски и повысить безопасность в цифровом мире.

Общественное сознание и образование являются ключевыми факторами для решения этих проблем и обеспечения безопасного обращения с персональными данными.

УДК 347.77/78

Эльбрусжанұлы Карим,
студент 2 курса Высшей школы права «Әділет»
Каспийского общественного университета,
Республика Казахстан, г. Алматы

ПРОБЛЕМА ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ИНТЕРНЕТЕ

Научный руководитель:

Сүлейменов Н.С.

м.ю.н., сеньор-лектор

Высшей школы права «Әділет»

Каспийского общественного университета

Аннотация

Данная статья посвящена актуальной проблеме защиты интеллектуальной собственности в виртуальном пространстве. С развитием технологий и широким распространением интернета стало возможным легкое распространение и незаконное использование интеллектуальных продуктов. В работе рассматриваются основные методы нарушения авторских прав, патентов и товарных знаков в онлайн среде, а также анализируются существующие механизмы защиты прав интеллектуальной собственности, включая правовые инструменты и технологические решения. Особое внимание уделяется проблемам эффективности существующих мер и перспективам их усовершенствования. Работа представляет обзор законодательства, международных соглашений и лучших практик в области защиты интеллектуальной собственности в сети, что может быть полезным для правовых экспертов, бизнес-сообщества и исследователей, стремящихся более эффективно противостоять угрозам для инноваций и творчества в онлайн среде.

Ключевые слова: интеллектуальная собственность, плагиат и пиратство в сети, способы защиты авторский прав.

Эльбрусжанұлы Карим

Каспий қоғамдық университеті
«Әділет» Жоғары құқық мектебінің 2 курс студенті,
Қазақстан Республикасы, Алматы қ.

ИНТЕРНЕТТЕ ЗИЯТКЕРЛІК МЕНШІКТІ ҚОРҒАУ МӘСЕЛЕСІ**Аңдатпа**

Бұл мақала виртуалды кеңістіктегі зияткерлік меншікті қорғаудың өзекті мәселесіне арналған. Технологияның дамуымен және Интернеттің кең таралуымен ақылды өнімдерді оңай тарату және заңсыз пайдалану мүмкін болды. Жұмыста онлайн ортада авторлық құқықтарды, патенттерді және тауар белгілерін бұзудың негізгі әдістері қарастырылады, сондай-ақ құқықтық құралдар мен технологиялық шешімдерді қоса алғанда, зияткерлік меншік құқықтарын қорғаудың қолданыстағы тетіктері талданады. Қолданыстағы шаралардың тиімділігі проблемаларына және оларды жетілдіру перспективаларына ерекше назар аударылады. Жұмыс желідегі зияткерлік меншікті қорғаудағы заңнамаға, халықаралық келісімдерге және ең жақсы тәжірибелерге шолу жасайды, Бұл онлайн ортада инновация мен шығармашылыққа төнетін қауіптерге тиімдірек қарсы тұруға тырысатын заң сарапшылары, бизнес қауымдастықтары және зерттеушілер үшін пайдалы болуы мүмкін.

Түйінді сөздер: зияткерлік меншік, желідегі плагиат және қарақшылық, авторлық құқықты қорғау жолдары.

Elbruszhanyuly Karim

2 year student of the Higher School of Law "Adilet"
Caspian Public University,
Republic of Kazakhstan, Almaty

THE PROBLEM OF PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET**Annotation**

This article is devoted to the actual problem of intellectual property protection in the virtual space. With the development of technology and widespread use of the Internet, easy distribution and illegal use of intellectual products became possible. The paper considers the main methods of infringement of copyrights, patents and trademarks in the online

environment, and analyzes the existing mechanisms of intellectual property rights protection, including legal tools and technological solutions. Special attention is paid to the problems of effectiveness of existing measures and prospects for their improvement. The paper provides an overview of legislation, international agreements and best practices in the field of intellectual property protection online, which may be useful for legal experts, business community and researchers seeking to better address threats to innovation and creativity in the online environment.

Keywords: intellectual property, plagiarism and online piracy, ways to protect copyrights.

Интеллектуальная деятельность человека в век развития IT-технологий и Интернета имеет колоссальное значение не только для человека, но и для любого государства. Ведь защита результатов интеллектуальной деятельности человека очень значима для стабильного экономического развития государства. Сейчас, в стремительном развитии инноваций, каждый человек ощутил на себе кардинальное изменение обыденных вещей и взаимоотношений между людьми. Мы активно привыкли пользоваться электронной почтой и жестким диском для хранения информации вместо библиотек и архивов. Понятия компьютер, интернет и Wi-fi устойчиво вошли в нашу жизнь. И чем больше появляется новых открытий и инноваций в области IT-технологий, тем больше проявляется необходимость в грамотной и своевременной защите интеллектуальной собственности.

Актуальность данной темы заключается в том, что, к сожалению, защита авторских прав в сети Интернет до сих пор не имеет правового освещения в различных законах нашего государства. Необходимость в разработке и обсуждении вопросов защиты в сети Интернет, достаточно значимая тема в наше время. Серьезное внимание на эту проблему люди стали обращать сравнительно недавно, когда «всемирная паутина» стала обыденностью для человека. Цель данного исследования заключается в разработке рекомендаций по обеспечению защиты интеллектуальных прав в сети Интернет. Для достижения данной цели требуется решение следующих задач:



Определение понятия Интернета как средства доступа к всемирной интеллектуальной собственности, выявление его роли в распространении и использовании интеллектуальных результатов.



Рассмотрение основных методов обеспечения защиты авторских прав в контексте сетевого пространства, включая анализ эффективности традиционных и инновационных подходов.



Определение ряда причин, способствующих нарушениям интеллектуальных прав в онлайн-среде, анализ влияния технологических, социальных и правовых аспектов на данную проблему.

В ходе исследования этих задач будет предложен комплекс рекомендаций, направленных на повышение эффективности защиты интеллектуальных прав в сети Интернет, учитывая особенности текущего технологического и правового контекста.

Интернет - всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов; (ст 1 п44 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»)

Способы защиты авторских прав – это установленные законом правовые меры принудительного характера, исходя из которых, происходит признание нарушенных прав и впоследствии принимается мера воздействия на правонарушителя.

Эти способы представлены в Законе об АП и СП, и к ним относятся:

Статья 49. Защита авторских и смежных прав

1. Защита авторских и смежных прав осуществляется судом путем:

- 1) признания прав;
- 2) восстановления положения, существовавшего до нарушения права;
- 3) пресечения действий, нарушающих право или создающих угрозу его нарушения;
- 4) возмещения убытков, включая упущенную выгоду;
- 5) взыскания дохода, полученного нарушителем вследствие нарушения авторских и (или) смежных прав;
- 6) выплаты компенсации в сумме от ста месячных расчетных показателей до пятнадцати тысяч месячных расчетных показателей, определяемой по усмотрению суда, или в двукратном размере стоимости экземпляров произведения или в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения. Размер компенсации определяется судом вместо возмещения убытков или взыскания дохода;
- 7) принятия иных предусмотренных законодательными актами мер, связанных с защитой их прав.

Указанные в подпунктах 4), 5) и 6) настоящего пункта меры применяются по выбору правообладателя.

За один только 2016 год из незаконного оборота изъято 137,7 тысячи (в 2015 году — 229,7 тысячи) единиц контрафактной продукции, в том числе 10,1 тысячи (в 2015 году — 14,6) носителей с аудио- и 126,2 тысячи (в 2015 году — 213,6) с видеопроизведениями, 577 тысяч (в 2015 году — 840) носителей — с нелегальным программным обеспечением.

Если верить этим данным, то в действительности уровень использования пиратского софта в Казахстане находится на критически высокой отметке. Примерно такая же обстановка и в других сферах интеллектуальной собственности, где воруют все: песни, книги, фильмы.

Заметим, что сейчас государство постоянно совершенствует законодательную базу в сфере интеллектуальной собственности. Так, например, с начала 2015 года были изменены виды ответственности за нарушение авторских и смежных прав. Результатом нововведений в законодательстве стал тот факт, что нарушение авторских и (или) смежных прав предусматривает вместо административной уголовную ответственность.

Возможно, для авторов все эти цифры и нововведения как бальзам на душу, но для простых пользователей — скорее навязывание монополии и чужой воли. Да и, положив руку на сердце, какой выбор есть у честного пользователя? Вопрос далеко не риторический.[1]

Информационная сеть предоставляет обширный доступ к разнообразной информации, охватывающей политические, экономические и другие сферы. Большинство этой информации доступно в свободном использовании и может быть применено в различных контекстах. Сеть Интернет не только предоставляет возможность поиска и использования информации, но также обеспечивает механизмы для ее обмена и распространения. Пользователи могут выражать свои мысли различного характера, включая личные, коммерческие, экономические и политические взгляды. Кроме того, они могут размещать научные исследования, литературу, музыку, произведения искусства и другие объекты интеллектуальной собственности. Однако, для обеспечения правообладателя рекомендуется использовать знак копирайта для предварительного уведомления пользователя о своих правах.

Особенности и виды этой категории правонарушений:

1. Низкую правовую культуру: Некоторые пользователи считают, что размещение материалов в сети бесплатно и не нарушает авторских прав. Однако это может привести к утрате потенциальной прибыли для

автора, который не получает вознаграждение за свое произведение, так как оно уже было скачано из Интернета.

2. Проблема доказательств в суде: В случае судебных разбирательств владельцам авторских прав часто трудно доказать факт нарушения, так как нарушитель может быстро удалить доказательства. Специфика этой проблемы заключается в том, что электронные следы могут быть легко уничтожены.

3. Плагиат: Некоторые люди приписывают себе авторство за произведения, размещенные в Интернете. Владельцы интернет-ресурсов могут использовать материалы интеллектуальной собственности, «позаимствованные» у конкурентов, создавая ошибочное представление, что эти материалы являются общественным достоянием.

4. Пиратство в области программного обеспечения: Например, в США до 35% использования лицензионного программного обеспечения может сопровождаться нарушениями авторских прав, даже в условиях высокого уровня защиты прав в данной стране.

Работа в данной области требует внимания к правовым аспектам, эффективных мер предотвращения и защиты, а также разработке механизмов для борьбы с нарушениями интеллектуальной собственности в сетевом пространстве.

можно отметить, что интенсивное развитие науки и технологий становится невозможным без законодательного обеспечения прав интеллектуальной собственности. В ходе изучения определений понятия Интернета, методов защиты интеллектуальной собственности и причин нарушения этих прав, мы приходим к следующим выводам. Для эффективной защиты интеллектуальной собственности в сети Интернет необходимо:

- **Глубокое понимание и умение использовать свои права:** Правообладатели должны хорошо осведомлены о своих правах и способах их применения в сетевом пространстве. Это включает в себя знание механизмов защиты и использование правовых инструментов.

- **Наличие квалифицированных специалистов:** Важно иметь в распоряжении квалифицированных юристов и специалистов, способных оказывать правовую поддержку авторам и правообладателям. Это может эффективно реагировать на нарушения и защищать интересы.

- **Разумное использование ресурсов в сети:** Правообладатели должны осознавать, что уровень пиратства в определенных регионах может быть высоким. Иногда целесообразно ограничивать публикацию своих работ в сети, чтобы минимизировать риски несанкционированного использования.

● **Технические решения, позволяющие предупреждать и обнаруживать подобные правонарушения.**

Для предупреждения и обнаружения интеллектуальных правонарушений существует несколько технических решений и методов:

- Системы мониторинга и аналитики:
 - Использование специализированных систем мониторинга, которые анализируют контент в сети для выявления нарушений авторских прав.
 - Алгоритмы машинного обучения могут быть применены для обнаружения несанкционированного использования контента.
- Цифровая водяная печать:
 - Внедрение цифровой водяной печати в цифровые файлы для их идентификации.
 - Эти водяные знаки могут быть невидимыми, но обеспечивают уникальную отметку для каждого документа.
- Системы отслеживания исключений:
 - Разработка систем, способных автоматически отслеживать и регистрировать любые исключения или необычные события в использовании контента.
- Блокчейн-технологии:
 - Использование блокчейна для создания децентрализованных реестров прав на интеллектуальную собственность.
 - Защита прав и возможность отслеживать историю изменений владения правами.
- Технологии распознавания изображений и звука:
 - Применение систем распознавания изображений и звука для автоматического определения нарушений визуальных и звуковых материалов.
- Искусственный интеллект для анализа текста:
 - Использование алгоритмов обработки естественного языка для анализа текстов и выявления плагиата или несанкционированного использования текстовых материалов.
- Системы раннего предупреждения:
 - Разработка систем, которые могут предупреждать об интеллектуальных правонарушениях на ранних стадиях, например, при появлении подозрительных активностей в сети.
- Системы управления доступом:

- Реализация строгих систем управления доступом к цифровым ресурсам, чтобы предотвращать несанкционированный доступ и использование контента.

Комбинирование этих технических решений может повысить эффективность предотвращения и обнаружения интеллектуальных правонарушений. Однако важно также учитывать правовые аспекты и соблюдение законов при использовании таких технологий.

С учетом этих аспектов, защита интеллектуальной собственности в сети Интернет становится более эффективной, способствуя сохранению интересов авторов и обеспечению устойчивости инновационного развития.

Международные соглашения, касающиеся защиты авторских прав в интернете, включают в себя ряд документов, которые созданы для обеспечения соблюдения авторских прав в цифровой среде. Вот несколько ключевых соглашений и организаций, связанных с защитой авторских прав в интернете:

Digital Millenium Copyright Act - это закон, обеспечивающий соблюдение авторского права в цифровую эпоху. Его приняли в 1998 году в США, и действует он, соответственно, только в американской юрисдикции. **DMCA** состоит из двух частей: первая, «защита от обхода», устанавливает ответственность за обход шифрования, а вторая, «отслеживание и уведомление», позволяет оперативно удалять нарушающий авторское право контент из сети, без необходимости тратить время и деньги на суды с нарушителем.

- **Бернская конвенция об охране литературных и художественных произведений (Бернская конвенция):**

- Это одна из основных международных конвенций, касающихся авторских прав.

- Обеспечивает минимальные стандарты защиты авторских прав и обязательства по их соблюдению для стран-участниц.

- **Всемирная организация интеллектуальной собственности (ВОИС):**

- ВОИС является специализированным агентством Организации Объединенных Наций и занимается вопросами интеллектуальной собственности, включая авторские права.

- Она разрабатывает и содействует принятию международных стандартов в области защиты авторских прав.

- **Договор по авторским правам в цифровую эпоху (WCT) и Договор по исполнителям и звукозаписям (WPPT):**

- Эти договоры, принятые ВОИС, направлены на адаптацию авторских прав к цифровой среде.

- WCT обеспечивает защиту авторских прав в цифровой среде, а WPPT касается прав исполнителей и производителей фонограмм.

- **Европейская конвенция об авторском праве в информационном обществе:**

- Принята Советом Европы и направлена на обеспечение соблюдения авторских прав в контексте информационного общества.

- **Директива Европейского союза о авторских правах в цифровом одном рынке:**

- Принята в 2019 году и направлена на адаптацию законодательства ЕС к новым реалиям цифровой среды, включая обязательства по защите авторских прав.

Важно отметить, что существуют различные национальные и региональные законы, регулирующие авторские права в интернете, и их соблюдение также является частью международных усилий по борьбе с нарушениями в сети. Опыт по защите авторских прав включает в себя сотрудничество между странами, законодательные меры, судебные процессы, а также использование технологий для обнаружения и пресечения пиратства контента.

В заключение можно отметить, что проблема защиты интеллектуальной собственности в интернете представляет собой серьезный вызов для общества, бизнеса и правоохранительных органов. Развитие цифровых технологий сопровождается увеличением случаев нарушения авторских прав, пиратства и кражи конфиденциальной информации. Отсутствие эффективной системы защиты может подорвать инновационные процессы, замедлить экономический рост и подвергнуть опасности творческий потенциал индивидов и компаний.

Решение проблемы требует комплексного подхода, включающего в себя совершенствование законодательства, укрепление технических мер безопасности, развитие международного сотрудничества и повышение уровня осведомленности общества о важности защиты интеллектуальной собственности. Только совместными усилиями государств, бизнеса и граждан можно создать устойчивую и эффективную систему защиты, способную справляться с вызовами современного цифрового мира и обеспечивать устойчивое развитие инноваций и креативности.

Список использованных источников:

1. Ст. 1 п. 44, ст. 49 Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» / <https://adilet.zan.kz>
2. В Казахстане семь из 10 граждан занимаются пиратством В современном мире понятие «пират» стало многомерным и предельно разнообразным
3. Близнац И. А., Леонтьев К. Б. Авторское право и смежные права: учеб / под. ред. И. А. Близнаца. — М.: Проспект, 2009. — С. 245—312. — 416 с. — ISBN 978-5-392-00743-1.
4. Липчик Д. Авторское право и смежные права = Droit d'auteur et droit voisins. — Пер. с фр.; Предисл. М.А. Федотова. — М.: Ладомир; Изд-во ЮНЕСКО, 2002. — С. 526—643. — 788 с. — 2000 экз. — ISBN 5-86218-395-7 UNESCO 92-3-202837-9.
5. Digital Millenium Copyright Act
6. Бернская конвенция об охране литературных и художественных произведений (Бернская конвенция)
7. Всемирная организация интеллектуальной собственности (ВОИС)
8. Европейская конвенция об авторском праве в информационном обществе
9. Директива Европейского союза о авторских правах в цифровом одном рынке