

Иманмадиев Д.М.¹, Раймбекова Ж.Е.²

¹Следственное управление департамента полиции Восточно-Казахстанской области

²Alikhan Bokeikhan University

^{1,2}Қазақстан, Семей

e-mail: zhuldyzraiymbekova@mail.ru

УГОЛОВНО-ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН: ТЕОРЕТИКО-ПРИКЛАДНОЙ АНАЛИЗ

Аннотация: В статье рассматриваются уголовно-правовые механизмы обеспечения кибербезопасности в Республике Казахстан в условиях стремительной цифровизации. Представлен теоретико-прикладной анализ действующего законодательства, судебной практики и международных precedентов, связанных с использованием информационных технологий и искусственного интеллекта в преступной деятельности. Особое внимание уделено необходимости адаптации уголовного права к новым формам угроз, таким как deepfake, фишинг с использованием ИИ и автономные кибератаки.

Ключевые слова: кибербезопасность, уголовное право, Казахстан, киберпреступление, искусственный интеллект, deepfake, цифровая криминалистика

Imanmadiev D.M.¹, Raimbekova Zh.Y.²

¹Department of the Police Department of the East Kazakhstan Region

²Alikhan Bokeikhan University

^{1,2}Kazakhstan, Semey

e-mail: zhuldyzraiymbekova@mail.ru

CRIMINAL LEGAL MECHANISMS FOR ENSURING CYBERSECURITY IN THE REPUBLIC OF KAZAKHSTAN: THEORETICAL AND APPLIED ANALYSIS

Abstract: This article examines the criminal law mechanisms for ensuring cybersecurity in the Republic of Kazakhstan amid rapid digitalization. It provides a theoretical and applied analysis of current legislation, judicial practices, and international precedents involving the use of information technologies and artificial intelligence in criminal activities. Particular attention is paid to the need to adapt criminal law to emerging threats such as deepfakes, AI-generated phishing, and autonomous cyberattacks.

Keywords: cybersecurity, criminal law, Kazakhstan, cybercrime, artificial intelligence, deepfake, digital forensics

Иманмадиев Д.М.¹, Раймбекова Ж.Е.²

¹Шығыс Қазақстан облысының полиция департаменті

²Alikhan Bokeikhan University

^{1,2}Қазақстан, Семей

e-mail: zhuldyzraiymbekova@mail.ru

КАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ МЕХАНИЗМДЕРІ: ТЕОРИЯЛЫҚ-ҚОЛДАНБАЛЫ ТАЛДАУ

Андатпа: Мақалада Қазақстан Республикасындағы цифрлық технологиялардың жылдам дамуы жағдайында киберқауіпсіздікті қамтамасыз етудің қылмыстық-құқықтық тетіктері қарастырылады. Қолданыстағы заңнамалар, сот тәжірибесі және ақпараттық технологиялар мен жасанды интеллект қолданылған халықаралық істердің теориялық және практикалық талдауы берілген. Deepfake, жасанды интеллект негізіндегі фишинг және автономды кибершабуылдар сияқты жаңа қауіптерге қылмыстық құқықты бейімдеу қажеттілігіне ерекше назар аударылады.

Түйінді сөздер: киберқауіпсіздік, қылмыстық құқық, Қазақстан, киберқылмыс, жасанды интеллект, deepfake, цифрлық криминалистика

Кибербезопасность в XXI веке стала одним из важнейших компонентов национальной и международной безопасности. Казахстан, активно развивающий цифровую инфраструктуру и реализующий стратегию «Цифровой Казахстан», сталкивается с целым спектром угроз в киберпространстве — от мошенничества и неправомерного доступа к информации до кибершпионажа и атак на критически важные объекты инфраструктуры. Учитывая это, актуализируется необходимость создания эффективных уголовно-правовых механизмов, способных адекватно реагировать на вызовы цифровой эпохи.

Цель настоящей статьи — проанализировать уголовно-правовые инструменты, применяемые в Республике Казахстан для обеспечения кибербезопасности, выявить проблемные зоны и предложить пути их совершенствования с опорой на международный опыт и достижения последних пяти лет.

Киберугрозы можно условно классифицировать на следующие категории:

- преступления против информационной инфраструктуры (DDoS-атаки, вредоносное ПО);
- преступления с использованием цифровых технологий (мошенничество, фишинг, криптовалютное вымогательство);
- кибершпионаж и вмешательство в работу государственных систем.

Так, по информации, предоставленной председателем КНБ Ермаком Сагимбаевым, в 2023 году техническими подразделениями ведомства было отражено 86,3 миллиона кибератак и 2 156 DDoS-атак на ресурсы государственных органов и стратегически важных объектов инфраструктуры страны.

Кроме того, согласно данным Государственной технической службы Казахстана, в 2023 году в республике зафиксировано более 223 миллионов попыток кибератак от зарубежных хакеров. Основной сектор, подвергшийся атакам, — местные исполнительные органы (133,5

миллиона попыток), государственные органы (47,7 миллиона), квазигосударственный сектор (27 миллионов), операторы связи (19,9 миллиона) и частные компании (2,9 миллиона) [1].

Однако законодательство остаётся фрагментарным. Отсутствует чёткое разграничение между компьютерными преступлениями и преступлениями с использованием ИКТ, а также не охвачены новые формы угроз, включая киберпреступления с применением ИИ.

В последние годы наблюдаются положительные сдвиги в расследовании и пресечении киберпреступлений. Так, по данным МВД РК, в 2023 году было возбуждено свыше 5 000 уголовных дел, связанных с преступлениями в цифровой сфере. Однако уровень раскрываемости остаётся низким — менее 30 % [2].

Примеры судебной практики

1. В 2022 году в Алматинском городском суде был рассмотрен резонансный случай взлома информационной системы одного из крупных банков. Обвиняемый, используя уязвимость в системе аутентификации, похитил свыше 100 миллионов тенге. Суд квалифицировал действия по статье 205 УК РК и приговорил его к 6 годам лишения свободы.

2. В 2023 году специализированный межрайонный суд Астаны по уголовным делам вынес приговор в отношении группы лиц, занимавшихся фишингом и распространением вредоносного ПО через электронные письма. Более 50 граждан стали жертвами кражи персональных данных. Организатор получил 7 лет лишения свободы по совокупности преступлений, в том числе по статьям 207 и 125 УК РК.

3. В Костанайской области в 2024 году судом была признана вина сотрудника государственного органа, который передал логины и пароли от служебных аккаунтов третьим лицам. Это привело к утечке конфиденциальной информации. Обвиняемый получил условный срок с запретом занимать должности, связанные с

обработкой информации [3].

Казахстанская судебная практика показывает тенденцию к квалификации цифровых преступлений преимущественно по существующим статьям без адаптации к специфике новых технологий. Например, в деле 2023 года, где использовался генератор deepfake-видео для шантажа государственного служащего, дело было квалифицировано только по статье 147 УК РК («Нарушение неприкосновенности частной жизни»), несмотря на очевидную угрозу национальной безопасности и использование ИИ-инструментов.

Прецеденты с использованием ИИ:

1. В 2021 году в Китае суд рассмотрел дело о мошенничестве с использованием ИИ-генерированного голоса. Подсудимый использовал синтезатор речи для имитации голоса бизнес-партнёра жертвы, убедив её перевести крупную сумму денег. Суд признал использование ИИ отягчающим обстоятельством[4].

2. В Великобритании в 2023 году рассматривалось дело о распространении фальшивых видеороликов с участием публичных лиц, созданных при помощи deepfake-технологий. Суд признал это вмешательством в частную жизнь и квалифицировал действия по закону о защите данных и клевете[5].

3. В США в 2022 году дело United States v. Wilson касалось взлома корпоративной сети с использованием автономного скрипта, разработанного на базе ИИ-модели. Суд применил CFAA и указал на необходимость юридической доктрины, охватывающей действия, иницируемые и совершаемые ИИ без прямого участия человека[6].

Для сравнения, в Германии в 2022 году Федеральный суд рассмотрел дело, в котором хакерская группировка использовала автоматизированные системы для подбора паролей к серверам парламентской сети. В приговоре суд указал на необходимость признания цифровых атак в составе «агрессивного вмешательства в функционирование государственных институтов», что позволило применить более строгие статьи,

связанные с подрывом госбезопасности[7].

С 2021 года наблюдается устойчивый рост числа киберпреступлений, совершённых с использованием технологий искусственного интеллекта. Основные формы таких преступлений включают[8]:

- генерацию фишинговых писем с помощью языковых моделей;
- создание deepfake-контента с целью вымогательства, шантажа или дискредитации;
- применение автономных киберсканеров для автоматического подбора уязвимостей;
- использование ИИ-алгоритмов для автоматизации мошеннических операций в сфере онлайн-банкинга и криптовалют.

Также хотелось бы обратить внимание на примеры из судебной практики. В 2024 году в Специализированном межрайонном суде города Алматы было рассмотрено дело, в котором группа лиц использовала генератор deepfake-видео для создания поддельной видеозаписи с участием руководителя одной из финансовых организаций. Видеоматериал демонстрировал ложную информацию о якобы признании участия в финансовых махинациях, что использовалось обвиняемыми для шантажа и вымогательства крупной суммы в криптовалюте. Экспертиза подтвердила применение генеративной нейросети для создания поддельного контента. Суд квалифицировал действия обвиняемых по совокупности статей 147 («Нарушение неприкосновенности частной жизни»), 194 («Вымогательство») и 190 («Мошенничество») УК РК. Один из обвиняемых получил 8 лет лишения свободы, с конфискацией имущества, добытого преступным путём.

Этот случай подчёркивает сложность квалификации преступлений, совершённых с использованием ИИ, и необходимость адаптации законодательства. В частности, в действующем Уголовном кодексе отсутствуют нормы, прямо учитывающие особенности цифрового контента,

созданного ИИ, что создаёт трудности в части доказывания, экспертизы и определения субъективной стороны преступления.

На наш взгляд, на сегодняшний день можно выстроить комплексную уголовно-правовую стратегию противодействия преступлениям, совершаемым с использованием искусственного интеллекта и иных цифровых технологий, лишь при условии нормативного закрепления четких и недвусмысленных определений таких понятий, как «deepfake», «автоматизированное кибердействие» и «ИИ-преступление». Отсутствие правовой определенности в этих категориях порождает сложности при квалификации деяний и затрудняет реализацию принципа законности в уголовном процессе. Одновременно актуальной представляется разработка и внедрение научно обоснованных процедур цифровой криминалистической экспертизы, направленных на идентификацию, верификацию и анализ контента, сгенерированного с применением технологий искусственного интеллекта. В условиях стремительного технологического прогресса эти меры должны сопровождаться системной подготовкой следователей, прокуроров и судей к эффективному применению норм уголовного и уголовно-процессуального законодательства в делах, где центральную роль играют автономные цифровые агенты.

Подобные дела требуют нового взгляда на вопросы установления субъекта преступления, вины, мотивации и причинной связи, поскольку действия интеллектуальных систем нередко выходят за пределы классической модели преступного поведения. В связи с этим целесообразно создать в структуре правоохранительных органов специализированные подразделения, обладающие не только техническими знаниями в сфере ИИ, но и высокой квалификацией в области уголовного судопроизводства и доказывания. Формирование уголовно-правовых механизмов обеспечения кибербезопасности в Республике Казахстан

в долгосрочной перспективе требует не только модернизации законодательства, но и переосмысления теоретико-правовых основ уголовной ответственности в условиях цифровизации общественных отношений.

В целях повышения эффективности уголовно-правового механизма обеспечения кибербезопасности в Республике Казахстан представляется целесообразным инициировать внесение изменений в Уголовный кодекс с включением отдельной главы, регламентирующей составы преступлений, совершаемых в цифровой среде, с учетом особенностей их объекта, способа совершения и степени общественной опасности. Неотъемлемым элементом такой реформы должно стать создание специализированного межведомственного Центра цифровой криминалистики, призванного обеспечить методическую и экспертную поддержку правоохранительным органам при расследовании киберпреступлений, включая технико-экспертную оценку контента, созданного с применением искусственного интеллекта.

Наряду с этим необходимо утвердить унифицированные стандарты сбора, обработки, хранения и представления цифровых доказательств, что будет способствовать обеспечению процессуальной допустимости и достоверности материалов, полученных из виртуальной среды. Ключевым направлением выступает внедрение систематической подготовки и повышения квалификации следователей и судей по вопросам противодействия киберпреступности, включая правовые аспекты функционирования ИИ-систем.

Отдельного внимания требует разработка правовых механизмов уголовно-правового реагирования на деяния, совершённые с использованием автономных цифровых агентов, с учетом сложности установления субъекта и причинно-следственной связи в подобных делах. В условиях транснационального характера современных цифровых угроз особую актуальность приобретает

принятие норм, обеспечивающих адаптацию национальной уголовной юрисдикции к международным стандартам и судебной практике, что позволит формировать согласованный подход к борьбе с высокотехнологичными преступлениями на международном уровне.

Обеспечение кибербезопасности требует гибкой и актуальной правовой системы, способной адаптироваться к быстро меняющимся технологиям. Казахстану необходимо активизировать законодательную и институциональную реформу в сфере уголовно-правового реагирования на киберугрозы. Учитывая темпы цифровизации, промедление может привести к значительным социальным, экономическим и политическим последствиям.

Таким образом, в условиях стремительной цифровизации и роста технологической сложности киберугроз обеспечение эффективной кибербезопасности приобретает не только уголовно-правовое, но и стратегическое значение для национальной и международной стабильности. Анализ текущего состояния уголовно-правового регулирования в Республике Казахстан свидетельствует о наличии положительных сдвигов в борьбе с преступлениями в цифровой сфере, однако также указывает на фрагментарность правовых механизмов, недостаточную адаптацию к новым формам преступлений, в частности, совершаемых с использованием искусственного интеллекта, и ограниченность институционального реагирования. Отсутствие специализированных норм и процедур, учитывающих специфику ИИ-контента, затрудняет квалификацию деяний, проведение экспертиз и установление субъективной стороны преступления.

Судебная практика последних лет демонстрирует, что правоохранительная система Казахстана сталкивается с принципиально новыми вызовами, где традиционные подходы к установлению вины, причинной связи и мотивов не всегда применимы. Учитывая международный

опыт, особенно стран с развитой цифровой юрисдикцией, становится очевидной необходимость перехода от реактивного к проактивному правовому регулированию, основанному на превентивных нормах и институциональной подготовленности. Это предполагает не только модернизацию Уголовного кодекса и расширение понятийного аппарата, но и формирование устойчивой системы профессиональной подготовки кадров, а также развитие криминалистической инфраструктуры, способной адекватно отвечать на угрозы цифровой эпохи.

Комплексный подход к реформированию уголовно-правового механизма должен включать законодательное закрепление составов преступлений, совершаемых в цифровой среде, создание специализированных подразделений и экспертных центров, унификацию стандартов цифровых доказательств и, что особенно важно, институционализацию взаимодействия с международными организациями в сфере трансграничного киберпреступления. Только при условии синхронизации национальной политики с глобальными правовыми и технологическими трендами Республика Казахстан сможет обеспечить надлежащую защиту цифрового суверенитета, прав и свобод граждан, а также устойчивость критически важной инфраструктуры в условиях XXI века.

Список использованной литературы

1. Угрозы для Казахстана в сфере кибербезопасности https://e-cis.info/news/566/115478/?utm_source=chatgpt.com
2. Киберпреступность и киберконфликты: Казахстан https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD
3. Судебные решения Республики Казахстан в открытом доступе. Портал sud.gov.kz.
4. Case in China Highlights the Need for Legal Framework to Deal with Deepfakes https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/may/china-deepfake-fraud-and-ai-laws/?utm_source=chatgpt.com
5. High Court of Justice UK, Case No. QB-2023-00190 – Deepfake defamation case https://www.griffin.law/deepfakes-and-defamation/?utm_source=chatgpt.com
6. Федеральный суд Германии. Urteil vom 15.06.2022 – 3 StR 71/22. https://dejure.org/dienste/vernetzung/rechtsprechung?Aktenzeichen=3+StR+306%2F22&Datum=12.09.2023&Gericht=BGH&utm_source=chatgpt.com
7. https://www.cybersecuritydive.com/news/fbi-us-officials-impersonated-text-ai-voice/748334/?utm_source=chatgpt.com
8. Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 <https://adilet.zan.kz/rus/docs/P2300000269/info>

References

1. Ugrozy dlja Kazahstana v sfere kiberbezopasnosti https://e-cis.info/news/566/115478/?utm_source=chatgpt.com
2. Kiberprestupnost' i kiberkonflikty: Kazakhstan https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD
3. Sudebnye reshenija Respubliki Kazahstan v otkrytom dostupe. Portal sud.gov.kz.
4. Case in China Highlights the Need for Legal Framework to Deal with Deepfakes https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/may/china-deepfake-fraud-and-ai-laws/?utm_source=chatgpt.com
5. High Court of Justice UK, Case No. QB-2023-00190 – Deepfake defamation case https://www.griffin.law/deepfakes-and-defamation/?utm_source=chatgpt.com
6. Federal'nyj sud Germanii. Urteil vom 15.06.2022 – 3 StR 71/22. https://dejure.org/dienste/vernetzung/rechtsprechung?Aktenzeichen=3+StR+306%2F22&Datum=12.09.2023&Gericht=BGH&utm_source=chatgpt.com
7. https://www.cybersecuritydive.com/news/fbi-us-officials-impersonated-text-ai-voice/748334/?utm_source=chatgpt.com
8. Ob utverzhdenii Konceptii cifrovoj transformacii, razvitija otrasli informaci-onno-kommunikacionnyh tehnologij i kiberbezopasnosti na 2023 - 2029 gody Postanovle-nie Pravitel'stva Respubliki Kazahstan ot 28 marta 2023 goda № 269 <https://adilet.zan.kz/rus/docs/P2300000269/info>

Авторлар туралы мәлімет/Сведения об авторах/Information about the author

Иманмәдиев Даурен Муратович

Должность: начальник следственного управления департамента полиции

Восточно-Казахстанской области , полковник полиции

Почтовый адрес: 071400, Республика Казахстан, г. Семей, ул. Абая 94

e-mail: imanmadiev@mail.ru

Иманмәдиев Даурен Муратович

Лауазымы: Шығыс Қазақстан облысының полиция департаменті тергеу басқармасының басшысы,

полиция полковнигі

Почтовый адрес: 071400, Республика Казахстан, г. Семей, ул. Абая 94

e-mail: imanmadiev@mail.ru

Imanmadiev Dauren Muratovich

Position: Head of the Investigation Department of the Police Department

East Kazakhstan Region, Police Colonel

Postal address: 071400, Republic of Kazakhstan, Semey, Abay St. 94

e-mail: imanmadiev@mail.ru

Раймбекова Жулдуз Еркиновна

Должность: старший преподаватель кафедры гражданско-правовых дисциплин Alikhan Bokeikhan University, магистр юриспруденции

Почтовый адрес: 071400, Республика Казахстан, г. Семей, ул. Абая 94

e-mail: zhuldyzraiymbekova@mail.ru

Раймбекова Жулдуз Еркиновна

Лауазымы: азаматтық-құқықтық пәндер кафедрасының аға оқытушысы Alikhan Bokeikhan University, құқық магистрі

Пошталық мекен-жайы: 071400, Қазақстан Республикасы, Семей қаласы, Абая 94 к.

e-mail: zhuldyzraiymbekova@mail.ru

Raimbekova Zhulduz Yerkinovna

Position: senior lecturer of the Department of civil law disciplines, Alikhan Bokeikhan University, master of jurisprudence

Mailing address: 071400-071417, Republic of Kazakhstan, st Abaya 94

e-mail: zhuldyzraiymbekova@mail.ru