



К.С. Лакбаев, Л.К. Аренова

Қарағандық университет Қазпотребсоюзы, г. Қарағанда, Республика Қазақстан

УГОЛОВНАЯ СТАТИСТИКА В СФЕРЕ КИБЕРПРЕСТУПНОСТИ: «БОЛЕЗНЬ РОСТА» ИЛИ СИСТЕМНАЯ ПРОБЛЕМА?

Аннотация. В данной статье рассматриваются проблемные вопросы формирования официальной уголовной статистики по группе уголовных правонарушений, объединяемых понятием «киберпреступность». Анализ их динамики за пять лет выявил ряд несоответствий, негативно отражающихся на анализе криминогенной ситуации в данной сфере. Прежде всего, это неполнота информации по некоторым уголовным правонарушениям. Также отмечается отсутствие в уголовной статистике сведений по комплексу составов, отражающих состояние оперативной обстановки по весьма актуальным направлениям, таким как кражи и наркопреступления. Аналогичная картина по разжиганию розни, публичным призывам к захвату власти и сепаратизму. Все эти уголовные правонарушения в основном готовятся и совершаются в информационной среде и с применением новых технологий. На основании изложенного предлагается дополнить официальную статистику этими важными показателями.

Ключевые слова: киберпреступность; правоохранительная деятельность; уголовная статистика; информатизация и связь; интернет; информационные технологии.

К.С. Лакбаев, Л.К. Аренова

Қазтұтынуодағы Қарағанды университеті, Қарағанды қ., Қазақстан Республикасы

«КИБЕРҚЫЛМЫСТЫЛЫҚ САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ СТАТИСТИКА: “ӨСУ ДЕРТІ” МЕ ӘЛДЕ ЖҮЙЕЛІ ПРОБЛЕМА МА?»

Аннотация. Бұл мақалада «киберқылмыстылық» ұғымымен біріктірілетін қылмыстық құқық бұзушылықтар тобы бойынша ресми қылмыстық статистиканы қалыптастырудың өзекті мәселелері қарастырылады. Олардың соңғы бес жылдағы динамикасын талдау осы саладағы криминогендік жағдайды талдауға теріс әсер ететін бірқатар қайшылықтарды анықтады. Ең алдымен, кейбір қылмыстық құқық бұзушылықтар бойынша ақпараттың толық еместігі байқалады. Сондай-ақ қылмыстық статистикада ұрлық және есірткі қылмыстары сияқты өзекті бағыттардағы жедел ахуалды сипаттайтын бірқатар құрамдар бойынша мәліметтердің жоқтығы атап өтіледі. Осындай жағдай алауыздықты қоздыру, билікті басып алуға ашық шақырулар және сепаратизм бойынша да байқалады. Аталған қылмыстық құқық бұзушылықтардың басым бөлігі негізінен ақпараттық ортада және жаңа технологияларды қолдану арқылы дайындалып, жасалады. Жүргізілген талдау негізінде ресми статистиканы осы маңызды көрсеткіштермен толықтыру ұсынылады.

Түйінді сөздер: киберқылмыстылық; құқық қорғау қызметі; қылмыстық статистика; ақпараттық технологиялар және коммуникациялар; интернет; ақпараттық технологиялар.

K.S. Lakbayev, L.K. Arenova

Karaganda university of Kazpotreboysuz, Karaganda, the Republic of Kazakhstan

CYBERCRIME STATISTICS: “GROWING PAINS” OR A SYSTEMIC PROBLEM?

Abstract. The present article analyze key impediments of collating official criminal statistics related to criminal offenses unified by the conception of “cybercrime”. A long-term analysis of their dynamics over five years exposed numerous of discrepancies that adversely affect the analysis of the criminogenic risk assessments in this area. Inter alia, this is the informational deficiency on certain infractions. Additionally, there is a lack of information in criminal statistics on a range of offenses that evince the existing conditions in crucial sectors, including larceny and drug-related violations. Analogous depiction arise with regard to promotion of hostility, public calls for the coup d'état and separatism. Aforementioned unlawful acts are primarily dedicated in the information ecosystem and utilizing new technologies. Drawing from the preceding, it is proposed to supplement official statistics with these important indicators.

Keywords: cybercrime; law enforcement; criminal statistics; information technology and communications; the



Введение. Киберпреступность является наиболее актуальной проблемой текущей криминогенной обстановки. История показывает, что преступный мир всегда пользовался последними достижениями науки: это и яды, не оставляющие в теле человека следов, ацетиленовые горелки и т.п. Настоящее время – не исключение. Криминал относительно давно освоил виртуальное пространство и новейшие достижения IT-технологий в целях реализации преступного умысла [1].

Зарубежные эксперты описывают будущую преступность лаконичным выражением: «Все можно взломать». Это означает получение доступа ко всему, что подключено к Интернету. В современном автомобиле можно нажать на тормоза или включить подушку безопасности. Определенные сервисы дают возможность подключиться к любому незащищенному устройству – веб-камере, телевизору и даже системам управления аквапарка или АЭС¹. Описание преступления в недалеком будущем может выглядеть таким образом: «Мужчина был задержан за стрельбу в свою жену, но освобожден после того, как выяснилось, что его бионическая рука была взломана»².

В то же время изучение данных официальной уголовной статистики по нашей стране позволяет сделать тревожный вывод о том, что в ней находят отражение не все опасные киберпреступления. Более того, даже та информация, которая имеется, во многом является фрагментарной, что не позволяет создать на ее основе полноценную картину реальной криминогенной ситуации в этой сфере.

Между тем в статистической информации должны содержаться сведения, характеризующие преступность; на них базируются результаты криминологических исследований [2]; она показывает, где, как, при каких условиях протекают те или другие явления, каковы их закономерности и взаимосвязи [3].

Материалы и методы. Исследование уголовной статистики по линии киберпреступности требует комплексного подхода и использования материалов из различных отраслей науки. Прежде всего, это комплекс юридических дисциплин антикриминального цикла – уголовное право и криминология, оперативно-розыскная деятельность (ОРД). Данные отрасли права формируют концептуальную базу для формирования той правовой информации, которая ложится в официальную уголовную статистику и служит основой для построения целостной картины криминогенной ситуации.

При этом использован комплексный подход, включающий элементы системно-информационного анализа, который позволяет установить причинно-следственные связи между различными составами уголовных правонарушений. Для этого также применялись общенаучные и частнонаучные методы – логико-юридический метод и метод моделирования.

Результаты, обсуждение. Определение «киберпреступность» носит в основном научный характер и охватывает весьма широкий круг криминальных деяний. Следует отметить, что в названиях различных нормативных правовых актов (как международного, так и национального характера) эта дефиниция до недавнего времени не была отражена. Например, Конвенция Совета Европы, принятая 23 ноября 2001 года в Будапеште и считавшаяся одним из основных международных документов по противодействию киберпреступности, называется «Конвенция о

¹ Будущее преступлений [Электронный ресурс] – Режим доступа: <https://cripo.com.ua/processes/?p=217471/> (дата обращения: 01.05.2026).

² Там же.



компьютерных преступлениях»³. И лишь Конвенция Организации Объединенных Наций (ООН) от 24 декабря 2024 года официально ввела данное понятие в международный правовой оборот⁴.

Тем не менее, термин «киберпреступность» достаточно давно применяется в отношении всех уголовных правонарушений, связанных с информационной сферой.

Подходя к их статистическому изучению, киберпреступления можно условно разделить на два больших блока.

Первый из них – это уголовные правонарушения, в которых непосредственным объектом посяательства являются динамично формирующиеся правоотношения в области новых информационных технологий. Как известно, в Уголовном кодексе Республики Казахстан (далее – УК РК) наиболее характерные из этих деяний объединены в специальной главе 7 «Уголовные правонарушения в сфере информатизации и связи»:

- статья 205 «Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть»;
- статья 206 «Неправомерное уничтожение или модификация информации»;
- статья 207 «Нарушение работы информационной системы или информационно-коммуникационной сети»;
- статья 208 «Неправомерное завладение информацией»;
- статья 209 «Принуждение к передаче информации»;
- статья 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов»;
- статья 211 «Неправомерное распространение электронных информационных ресурсов ограниченного доступа»;
- статья 212 «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели»;
- статья 213 «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства».

Изучение данных уголовной статистики Комитета правовой статистики и специальных учетов (далее – КПСиСУ) при Генеральной прокуратуре РК показывает рост регистрации этих уголовных правонарушений за период с 2020 по 2025 годы более чем втрое, хотя в абсолютных величинах их количество сравнительно невелико, особенно в общей криминальной массе.

Так, в 2020 году всего по данным девяти составов было зарегистрировано 62 факта, в 2021 году – 74, в 2022 году – 85, в 2023 году – 77, в 2024 году – 122, в 2025 году – 215⁵ (рис. 1).

³ Конвенция о компьютерных преступлениях: Будапешт, 23 нояб. 2001 г. [Электронный ресурс] – Режим доступа: <https://rm.coe.int/1680081580> (дата обращения: 27.03.2026).

⁴ Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям: принята резолюцией 79/243 Генеральной Ассамблеи от 24 дек. 2024 г. [Электронный ресурс] – Режим доступа: <https://www.un.org/ru/documents/assembly/resolutions/79-243> (дата обращения: 27.03.2026).

⁵ Отчет 1-М «О зарегистрированных уголовных правонарушениях» // Статистические отчеты КПСиСУ при Генеральной прокуратуре РК [Электронный ресурс] – Режим доступа: <http://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat> (дата обращения: 28.03.2026).

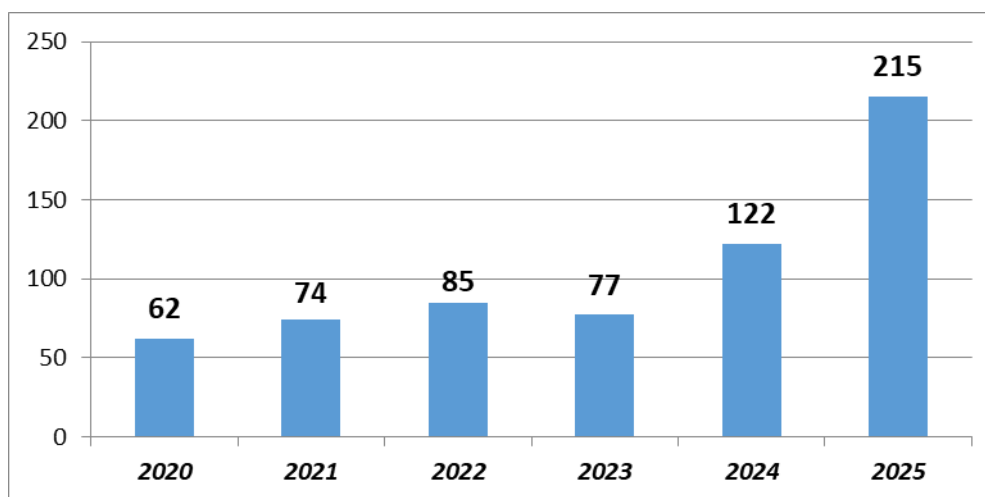


Рис. 1. Динамика регистрации уголовных правонарушений по главе 7 УК РК

В то же время реальная действительность серьезно отличается от статистических данных. Так, по итогам 2025 года АО «Государственная техническая служба» зафиксировано более 61 тыс. инцидентов в области информационной безопасности, в т.ч. с вирусами, сетевыми червями и троянами. Среди них DoS/DDoS-атаки, в т.ч. на государственные органы (11 фактов), несанкционированный доступ и модификация содержания (22 факта)⁶.

Если сравнить эту информацию с уголовной регистрацией по этим составам, то можно увидеть, что по статье 207 УК РК, регламентирующей ответственность за атаки, в 2025 году было зарегистрировано всего 4 факта из 11. И наоборот, по статьям 205 и 206 УК РК (несанкционированный доступ и модификация содержания) зарегистрировано 124 факта, т.е. в несколько раз больше, чем приводится в отчете АО «Государственная техническая служба».

При этом в июне 2025 года произошла масштабная утечка персональных данных – в открытом доступе оказалось 16,3 млн записей, содержащих фамилии, имена, индивидуальные идентификационные номера (ИИН), адреса, даты рождения, номера телефонов и другие сведения о казахстанцах [4]. В то же время, согласно данным уголовной статистики, ущерб от всех подобных фактов по статье 205 УК РК не зарегистрирован.

Следующий блок уголовных правонарушений, связанных с информационной сферой, также представляет большой интерес с точки зрения количества и качества. В него включены более привычные и традиционные составы, в т.ч. кражи и мошенничества, составляющие основную долю в общей криминогенной ситуации.

По состоянию на 31 декабря 2025 года в УК РК содержалось 34 состава, где в качестве квалифицирующего признака указывалось совершение деяния в сфере информатизации и связи, а также посредством использования сети Интернет⁷.

Вместе с тем полноценный анализ этой группы уголовных правонарушений затруднителен в связи с тем, что уголовная статистика по ним не отражает указанного квалифицирующего признака. Исключение представляет лишь интернет-мошенничества, информация по которым присутствует на портале КПСиСУ. Но даже по ним количественные показатели на несколько порядков превышают суммарное количество всех уголовных правонарушений по главе 7 УК РК.

⁶ Киберкод 2025: вызовы цифровой эпохи [Электронный ресурс] – Режим доступа: https://sts.kz/storage/media/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B4%D0%B0%D0%B9%D0%B4%D0%B6%D0%B5%D1%81%D1%82%202025_1.pdf (дата обращения: 28.03.2026).

⁷ Уголовный кодекс Республики Казахстан: от 3 июля 2014 г. № 226-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 08.10.2025).



Так, в 2020 году было совершено 15 058 фактов интернет-мошенничества, в 2021 году – 23 351, в 2022 году – 22 898, в 2023 году – 23 800, в 2024 году – 21 387, в 2025 году – 28 851⁸ (рис. 2).

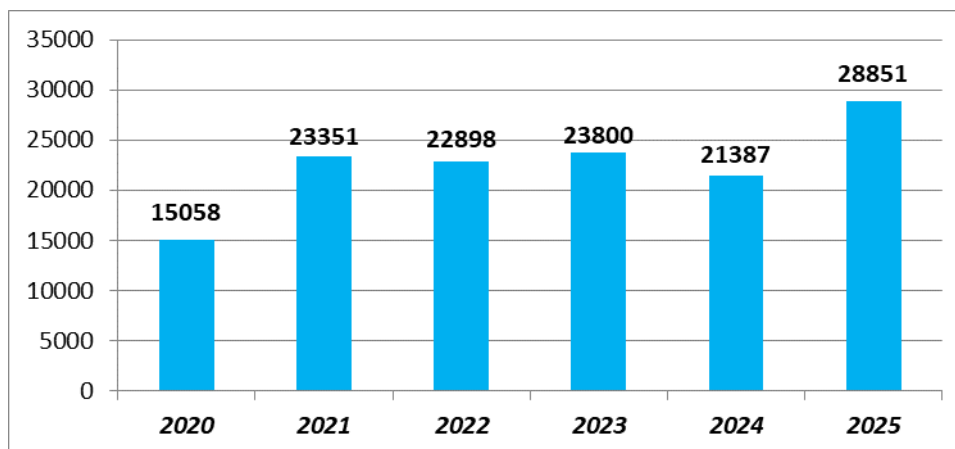


Рис. 2. Динамика интернет-мошенничеств

Понятно, что и по другим составам этого блока уголовных правонарушений значительная часть совершается или в недалеком будущем будет в значительной степени совершаться в сфере информатизации и связи, а также посредством использования сети Интернет.

В то же время объективно анализировать их динамику не представляется возможным в связи с тем, что соответствующих данных в открытой статистике не хватает. Так, в приложении PRIL 1 отчетности М-1 КПСиСУ присутствует реквизит «с использованием компьютера». Согласно ему, таким образом в 2020 году было совершено всего 6 краж из 67 254 зарегистрированных (0,00009%), в 2021 году – 12 из 57 498 (0,0002%), в 2022 году – 4 из 58 880 (0,00007%), в 2023 году – 3 из 42 639 (0,00007%), в 2024 году – 5 из 29 089 (0,0002%), в 2025 году – 6 из 23 266 (0,0006%)⁹ (рис. 3).

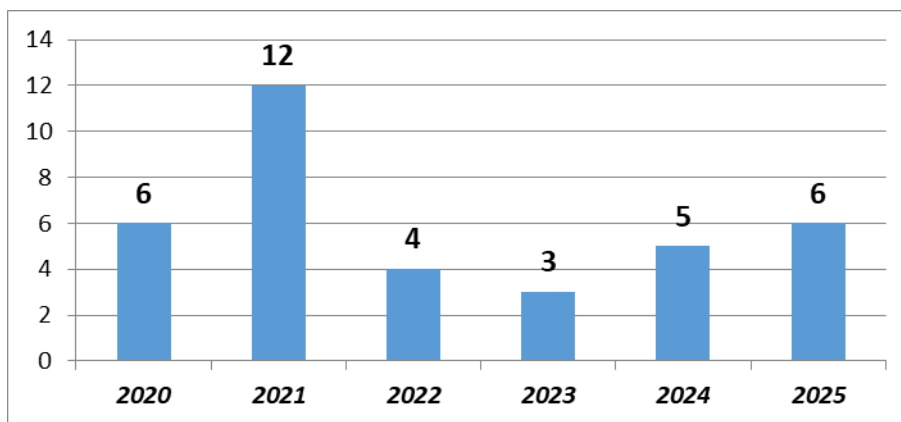


Рис. 3. Динамика регистрации краж, совершенных с использованием компьютера

⁸ Отчет 1-М «О зарегистрированных уголовных правонарушениях» КПСиСУ при Генеральной прокуратуре РК [Электронный ресурс] – Режим доступа: <https://qamqor.gov.kz/crimestat/statistics> (дата обращения: 28.03.2026).

⁹ Там же.



С учетом доли интернет-мошенничеств в общем их количестве очевидно, что такие цифры явно не отражают реальное состояние по кражам, которые также, вероятно, в значительной части совершаются с использованием новых информационных технологий.

Аналогичные вопросы возникают и по другим, более серьезным уголовным правонарушениям. Если изучить статистику в приложении PRIL 1 отчетности М-1 КПСиСУ по результатам 2022 года, то получается следующая картина.

Так, по статье 174 УК РК «Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни» было зарегистрировано 46 фактов, из них с использованием компьютера – ни одного. Аналогично обстоят дела:

- по статье 179 УК РК «Пропаганда или публичные призывы к захвату или удержанию власти либо насильственное изменение строя Республики Казахстан» (46 фактов);
- по статье 180 УК РК «Сепаратистская деятельность» (7 фактов).

Аналогичная ситуация по данному реквизиту за 2023-2025 гг.

Маловероятно, что эти весьма актуальные и опасные в настоящее время уголовные правонарушения совершались без использования информационных технологий, в т.ч. компьютеров.

Некорректность таких статистических данных еще более наглядно видна при анализе количественных показателей по статье 299-1 УК РК «Пропаганда или незаконная реклама наркотических средств, психотропных веществ или их аналогов, прекурсоров». Среди сотни ежегодно регистрируемых фактов лишь единицы значатся как совершенные с помощью компьютера. При этом общеизвестно, что практически вся пропаганда или реклама наркотиков ведется через информационные платформы.

Аналогичная проблема существует и в России, где многие ученые и практики констатируют факт, что состояние уголовно-правовой статистики из технической проблемы переросло в проблему социальную [5].

Таким образом, уголовная статистика по ряду актуальных показателей в сфере противодействия киберпреступности не является корректной, что препятствует полноценному анализу состояния криминогенной ситуации по данной линии. Следовательно, планирование каких-либо действенных управленческих мер в этой сфере изначально не может быть соответствующим.

Отсюда следует необходимость внесения корректировок в рассматриваемый реквизит «с использованием компьютера» приложения PRIL 1 отчетности М-1 КПСиСУ и сопряжения его данных с реальной информацией, фиксируемой в Едином реестре досудебных расследований (ЕРДР) по конкретным уголовным делам.

Кроме того, следует изменить название этого реквизита, т.к. оно морально устарело. В нынешних условиях значительная часть киберпреступлений совершается не только с помощью компьютеров, но и посредством телефонов и других технических устройств. К тому же, в недалеком будущем прогнозируется распространение таких уголовных правонарушений, совершаемых с использованием технологий искусственного интеллекта (ИИ) и дипфейков (deep fake). Об этом говорят многие эксперты.

Более того, отечественные ученые, указывая на некорректность уголовной статистики в этой сфере, предлагают вывести киберпреступность в отдельную категорию учета с связи ее явной спецификой [6].

Об аналогичных тенденциях говорят отечественные и зарубежные специалисты. Так, О.Ж. Жолдасов отмечает, что из-за высокой технологичности и новизны таких преступлений официальная уголовная статистика не отражает их реальные масштабы [7]. Т. Сиппи и Ф. Енок указывают на то, что уголовная статистика фиксирует состав преступления, но не метод его



совершения. Из-за отсутствия специальных статистических меток в базах данных невозможно вычленишь, какая доля преступлений совершена с применением, М. Халил говорит о критическом «внутреннем лаге» государственной статистики, которая не успевает за динамикой киберпреступности. Поэтому автор вынужден получать альтернативную картину из отчетов аналитических агентств и регуляторов, таких как Ofcom, NIST, DARPA [9].

В этой связи было бы целесообразно данный реквизит расширить и привести в соответствие с квалифицирующими признаками, обозначенными в соответствующих нормах УК РК – «совершенное в сфере информатизации и связи, а также посредством использования сети Интернет».

Заключение. Обобщая результаты изучения уголовной статистики в сфере киберпреступности, можно сделать вывод, что она пока находится на стадии становления и формирования. С одной стороны, это объяснимо новизной проблематики и традиционным отставанием правоохранительной практики от развития преступности. С другой стороны, такое несоответствие статистических данных реальной криминогенной ситуации внушает серьезные опасения, т.к. другой цифровой базы для прогнозирования перспективной правоохранительной деятельности не существует.

Соответственно, если эта база не корректна, то неадекватными будут и организационно-управленческие меры по противодействию киберпреступности.

Отсюда следует, что уголовная статистика по данной линии критически нуждается в корректировке с целью ее приближения к действительной картине оперативной обстановки.

Не хотелось бы, чтобы и в данном сегменте уголовной статистики имело под собой основание расхожее выражение о том, что существуют три вида лжи: ложь, наглая ложь и статистика [10].

Статья подготовлена в рамках реализации грантового проекта «Модернизация механизмов расследования киберпреступлений в Республике Казахстан», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан (АР 26198915).

Список использованной литературы:

1. Драпезо, Р.Г. Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» / Р.Г. Драпезо, В.Н. Шелестюков // Российский следователь. – 2018. – № 9. – С. 65-72.
2. Рогова, Е.В. Уголовно-правовая статистика и реальное состояние преступности в России / Е.В. Рогова // Глагол правосудия. – 2015. – № 2 (10). – С. 34-39.
3. Ткачев, П.Н. Статистические этюды (Опыт разработки русской уголовной статистики) / П.Н. Ткачев // Библиотека для чтения. – 1863. – № 10. – С. 1-33.
4. А. Шашкина. Уголовную ответственность за утечку данных могут ввести в Казахстане [Электронный ресурс] – Режим доступа: https://tengrinews.kz/kazakhstan_news/ugolovnuyu-otvetstvennost-massovuuyu-utechku-dannyyih-mogut-596092/ (дата обращения: 28.03.2026).
5. Гаврилов, Б.Я. Современная уголовная политика России: цифры и факты / Б.Я. Гаврилов. – М.: Проспект, 2008. – 208 с.
6. Сатбаева, А.М. Проблемы противодействия киберпреступности: опыт международного сотрудничества / А.М. Сатбаева, А.Р. Алимбетова, М.Т. Бейсенбаева // Вестник института законодательства и правовой информации Республики Казахстан. – 2024. – № 3 (78). – С. 211-221.
7. Жолдасов, О.Ж. Актуальные вопросы уголовного права в условиях развития технологий искусственного интеллекта / О.Ж. Жолдасов, Ж.А. Кегембаева // Құқық қорғау органдары академиясының Жаршысы. – 2025. – № 1 (35). – С. 157-165.
8. Sippy, T. Behind the Deepfake: 8% Create 90% Concerned / T. Sippy, F. Enock // The Alan Turing Institute [Электронный ресурс] – Режим доступа: [https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned#:~:text=First%2C%20on%20average%2C%2015%25,was%20relatively%20low%20\(8%25\)](https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned#:~:text=First%2C%20on%20average%2C%2015%25,was%20relatively%20low%20(8%25)) (дата обращения: 29.03.2026).
9. M. Khalil. Deepfake Statistics 2025: AI Fraud Data & Trends [Электронный ресурс] – Режим доступа: <https://deepstrike.io/blog/deepfake-statistics-2025> (дата обращения: 29.03.2026).



10. Huff, D. How to Lie with Statistics / D. Huff, I. Geis // W.W. Norton & Company Inc., 1954. – 144 p.

References:

1. Drapezo, R.G. Osobennosti ispol'zovaniya rezul'tatov operativno-rozysknogo meroprijatija «poluchenie komp'juternoj informacii» / R.G. Drapezo, V.N. Shelestjukov // Rossijskij sledovatel'. – 2018. – № 9. – S. 65-72.
2. Rogova, E.V. Ugolovno-pravovaja statistika i real'noe sostojanie prestupnosti v Rossii / E.V. Rogova // Glagol pravosudija. – 2015. – № 2 (10). – S. 34-39.
3. Tkachev, P.N. Statisticheskie jetjudy (Opyt razrabotki russkoj ugolovnoj statistiki) / P.N. Tkachev // Biblioteka dlja chtenija. – 1863. – № 10. – S. 1-33.
4. A. Shashkina. Ugolovnuju otvetstvennost' za utechku dannyh mogut vvesti v Kazahstane [Jelektronnyj resurs] – Rezhim dostupa: https://tengrinews.kz/kazakhstan_news/ugolovnuyu-otvetstvennost-massovuyu-utechku-dannyih-mogut-596092/ (data obrashhenija: 28.03.2026).
5. Gavrilov, B.Ja. Sovremennaja ugolovnaja politika Rossii: cifry i fakty / B.Ja. Gavrilov. – M.: Prospekt, 2008. – 208 s.
6. Satbaeva, A.M. Problemy protivodejstviya kiberprestupnosti: opyt mezhdunarodnogo sotrudnichestva / A.M. Satbaeva, A.R. Alimbetova, M.T. Bejsenbaeva // Vestnik instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. – 2024. – № 3 (78). – S. 211-221.
7. Zholdasov, O.Zh. Aktual'nye voprosy ugolovnogo prava v uslovijah razvitiya tehnologij iskusstvennogo intellekta / O.Zh. Zholdasov, Zh.A. Kegembaeva // Құқық қорғау органдары академиясының Жаршысы. – 2025. – № 1 (35). – S. 157-165.
8. Sippy, T. Behind the Deepfake: 8% Create 90% Concerned / T. Sippy, F. Enock // The Alan Turing Institute [Jelektronnyj resurs] – Rezhim dostupa: [https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned#:~:text=First%2C%20on%20average%2C%2015%25,was%20relatively%20low%20\(8%25\)](https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned#:~:text=First%2C%20on%20average%2C%2015%25,was%20relatively%20low%20(8%25)) (data obrashhenija: 29.03.2026).
9. M. Khalil. Deepfake Statistics 2025: AI Fraud Data & Trends [Jelektronnyj resurs] – Rezhim dostupa: <https://deepstrike.io/blog/deepfake-statistics-2025> (data obrashhenija: 29.03.2026).
10. Huff, D. How to Lie with Statistics / D. Huff, I. Geis // W.W. Norton & Company Inc., 1954. – 144 p.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Канат Саметулы Лакбаев – Қазтұтынуодағы Қарағанды университеті экономикалық және құқықтық зерттеулер ғылыми-зерттеу институтының бас ғылыми қызметкері, заң ғылымдарының докторы, профессор, e-mail: k.lakbaev@mail.ru.

Лакбаев Канат Саметович – главный научный сотрудник научно-исследовательского института экономических и правовых исследований Карагандинского университета Казпотребсоюза, доктор юридических наук, профессор, e-mail: k.lakbaev@mail.ru.

Lakbayev Kanat Sametovich – Chief Researcher of Research Institute of Economic and Legal Research of Karaganda University of Kazpotrebsoyuz, Doctor of Legal Sciences, Professor, e-mail: k.lakbaev@mail.ru.

Лейла Климентьевна Аренова – Қазтұтынуодағы Қарағанды университетінің экономикалық қатынастарды құқықтық реттеу кафедрасының профессоры, заң ғылымдарының кандидаты, e-mail: leila.arenova.73@inbox.ru.

Аренова Лейла Климентьевна – профессор кафедры правового регулирования экономических отношений Карагандинского университета Казпотребсоюза, кандидат юридических наук, e-mail: leila.arenova.73@inbox.ru.

Arenova Leila Klimentievna – Professor of the Department of Legal Regulation of Economic Relations at the Karaganda University of Kazpotrebsoyuz, Candidate of Law Sciences, e-mail: leila.arenova.73@inbox.ru.