



А.Е. Сарбасов

*Алматинская академия Министерства внутренних дел Республики Казахстан имени М. Есбұлатова,
г. Алматы, Республика Казахстан*

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Аннотация. Настоящее исследование посвящено актуальной проблеме уголовно-правового регулирования нарушений правил эксплуатации информационных систем в условиях стремительной цифровизации общества и расширения сферы применения информационно-коммуникационных технологий. Рост зависимости государства, бизнеса и граждан от цифровой инфраструктуры сопровождается увеличением числа правонарушений, связанных с обработкой, хранением, передачей и защитой компьютерной информации. В работе представлен комплексный анализ законодательных подходов к криминализации противоправных деяний в указанной сфере на примере Республики Казахстан и зарубежных государств. Особое внимание уделено сравнительно-правовому исследованию уголовно-правовых норм, предусматривающих ответственность за нарушение правил эксплуатации информационных систем, несанкционированный доступ к информации, а также иные посяательства на информационную безопасность. Детально рассматриваются развитие и современное состояние законодательства Республики Казахстан, выявляются пробелы правового регулирования и анализируется зарубежный опыт с целью выработки предложений по совершенствованию национального уголовного законодательства.

Ключевые слова: информационная безопасность; киберпреступность; уголовная ответственность; уголовное законодательство; цифровизация; нарушение правил эксплуатации; компьютерная информация; криминализация; программное обеспечение; защита информации.

А.Е. Сарбасов

*Қазақстан Республикасы Ішкі істер министрлігінің М. Есбұлатов атындағы Алматы академиясы,
Алматы қ., Қазақстан Республикасы*

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ЗАҢНАМАНЫ ЖЕТІЛДІРУ МӘСЕЛЕСІ ТУРАЛЫ

Аннотация. Осы зерттеу қоғамның қарқынды цифрлануы және ақпараттық-коммуникациялық технологияларды қолдану аясының кеңеюі жағдайында ақпараттандыру объектілерін пайдалану қағидаларын бұзуды қылмыстық-құқықтық реттеудің өзекті мәселесіне арналған. Мемлекеттің, бизнестің және азаматтардың цифрлық инфрақұрылымға тәуелділігінің артуы компьютерлік ақпаратты өңдеуге, сақтауға, беруге және қорғауға байланысты құқық бұзушылықтар санының өсуімен қатар жүруде. Жұмыста Қазақстан Республикасы мен шет мемлекеттердің мысалында аталған саладағы құқыққа қайшы іс-әрекеттерді криминализациялауға қатысты заңнамалық тәсілдерге кешенді талдау жүргізіледі. Ақпараттандыру объектілерін пайдалану қағидаларын бұзғаны, ақпаратқа құқыққа сыйымсыз қол жеткізгені, сондай-ақ ақпараттық қауіпсіздікке өзге де қол сұғушылықтар жасағаны үшін жауаптылықты көздейтін қылмыстық-құқықтық нормаларды салыстырмалы-құқықтық зерттеуге ерекше назар аударылады. Қазақстан Республикасы заңнамасының дамуы мен қазіргі жай-күйі егжей-тегжейлі қарастырылып, құқықтық реттеудегі олқылықтар анықталады және ұлттық қылмыстық заңнаманы жетілдіру жөнінде ұсыныстар әзірлеу мақсатында шетелдік тәжірибе талданады.

Түйінді сөздер: ақпараттық қауіпсіздік; киберқылмыстылық; қылмыстық жауаптылық; қылмыстық заңнама; цифрландыру; пайдалану қағидаларын бұзу; компьютерлік ақпарат; криминализация; бағдарламалық қамтылым; ақпаратты қорғау.



A.E. Sarbassov

*The Almaty Academy of the Ministry of internal Affairs of the Republic of Kazakhstan named after M. Yesbulatov,
Almaty, the Republic of Kazakhstan*

ON THE ISSUE OF IMPROVING CRIMINAL LEGISLATION IN THE FIELD OF INFORMATIZATION AND COMMUNICATIONS

Abstract. This study is devoted to the urgent issue of criminal law regulation of violations of the rules for the operation of information systems in the context of the rapid digitalization of society and the expanding use of information and communication technologies. The growing dependence of the state, business, and citizens on digital infrastructure is accompanied by an increase in the number of offenses related to the processing, storage, transmission, and protection of computer information. The paper presents a comprehensive analysis of legislative approaches to the criminalization of unlawful acts in this area, using the Republic of Kazakhstan and foreign states as examples. Particular attention is paid to a comparative legal study of criminal law provisions establishing liability for violations of the rules for the operation of information systems, unauthorized access to information, and other infringements on information security. The development and current state of the legislation of the Republic of Kazakhstan are examined in detail, gaps in legal regulation are identified, and foreign experience is analyzed in order to develop proposals for improving national criminal legislation.

Keywords: information security; cybercrime; criminal liability; criminal legislation; digitalization; violation of operating rules; computer information; criminalization; software; information protection.

Введение. В условиях стремительной цифровизации общественных отношений информационные системы (далее – ИС) становятся неотъемлемой частью деятельности государства, бизнеса и граждан.

Развитие современных цифровых технологий способствовало оптимизации процессов предоставления государственных услуг, обеспечению удаленного доступа к финансовым операциям, обработке персональных данных и функционированию критически важных инфраструктур. Параллельно с расширением цифрового пространства наблюдается увеличение числа преступлений и правонарушений, связанных с нарушением правил эксплуатации ИС.

Согласно данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан (далее – РК), в 2025 году было зарегистрировано 215 уголовных правонарушений в сфере информатизации и связи. Этот показатель демонстрирует существенный рост по сравнению с 2024 годом, когда было зафиксировано 38 аналогичных деяний, что составляет увеличение на 465,8%¹.

Данная динамика свидетельствует о возрастающей общественной опасности нарушений в сфере информатизации и наглядно подтверждает острую необходимость совершенствования уголовно-правовых механизмов их предупреждения.

Как отмечают зарубежные авторы, последствия киберинцидентов выходят за рамки финансовых убытков одной организации и затрагивают общественные интересы, в связи с чем требуется усиление правовых механизмов защиты цифровой инфраструктуры, так как исследуемая область знаний рассматривает кибербезопасность не только как техническую, но и как социально-правовую ответственность организаций [1].

Несмотря на наличие исследований, посвященных киберпреступности, несанкционированному доступу к информации и использованию вредоносного программного обеспечения, вопросы уголовной ответственности за нарушение правил эксплуатации ИС разработаны недостаточно. В законодательстве РК отсутствует самостоятельная норма, предусматривающая ответственность за такие деяния, тогда как в ряде зарубежных государств соответствующие составы уже закреплены.

¹ Отчет №1-М «О зарегистрированных уголовных правонарушениях» // Правовая статистика [Электронный ресурс]. – Режим доступа: <https://qamqor.gov.kz/crimestat/statistics>.



Нарушения правил информационной безопасности нередко совершаются лицами, имеющими законный доступ к системам, а нарушение внутренних правил эксплуатации остается одной из наиболее сложных форм цифровых правонарушений для правовой квалификации, что демонстрирует особую роль поведения лиц, имеющих легитимный доступ к информационным ресурсам [2].

Научная новизна исследования заключается в выявлении пробела в уголовном законодательстве РК и обосновании необходимости введения самостоятельной нормы, устанавливающей ответственность за нарушение правил эксплуатации ИС с учетом зарубежного опыта.

Исследовательский вопрос сформулирован следующим образом: в какой мере действующая модель уголовно-правовой охраны информационных систем в Республике Казахстан позволяет реагировать на общественно опасные нарушения правил их эксплуатации лицами, имеющими правомерный доступ, и какие элементы зарубежных моделей могут быть использованы для устранения выявленного пробела без избыточной криминализации? Для ответа на данный вопрос последовательно сопоставляются объект правовой охраны, субъект деяния, характер нарушения, обязательность наступления последствий, форма вины и способы дифференциации ответственности.

Вместе с тем вопрос о самостоятельной уголовной ответственности именно за нарушение правил эксплуатации ИС правомерным пользователем при наступлении общественно опасных последствий остается недостаточно разработанным. Указанное обстоятельство обуславливает наличие исследовательского пробела, на восполнение которого направлена настоящая работа.

Материалы и методы. Исследование выполнено в рамках формально-юридического и сравнительно-правового подходов. На первом этапе были определены нормы законодательства РК, регулирующие ответственность за нарушения в сфере информатизации и эксплуатации ИС. На втором этапе отобраны зарубежные правовые порядки, в которых предусмотрены специальные составы, позволяющие сопоставить различные модели криминализации. На третьем этапе нормы сравнивались по единым критериям: объект правовой охраны; специальный или общий субъект; характер запрещенного деяния; обязательность наступления общественно опасных последствий; форма вины; критерии дифференциации ответственности и санкций.

Сравнительно-правовой метод применялся для сопоставления элементов составов правонарушений и преступлений. Формально-юридический метод использовался при анализе статей 207, 210 УК РК, статьи 641 Кодекса об административных правонарушениях РК (далее – КоАП РК) и сопоставимых зарубежных норм. Системный и логико-юридический методы позволили выявить их взаимосвязи и обосновать наличие нормативного пробела.

Нормативную основу исследования составили законодательство Казахстана, Узбекистана, России, Беларуси и Украины, а также положения права Европейского союза. Выбор указанных государств обусловлен наличием сопоставимых норм об ответственности за нарушения правил эксплуатации информационных систем и различиями в подходах к ее дифференциации.

Результаты. Законодательная система РК в сфере информационной безопасности представляет собой многоуровневый комплекс нормативных актов, направленных на защиту цифровых активов и противодействие киберугрозам.

Ключевым актом, определяющим информационную безопасность как элемент национальной безопасности РК, является Закон «О национальной безопасности Республики Казахстан». Его положения конкретизируются «Едиными требованиями в области информационно-коммуникационных технологий и информационной безопасности», устанавливающими обязательные требования для государственных органов и организаций с государственным участием.



Наряду с этим, существенное значение имеет Закон «О персональных данных и их защите», который подробно регламентирует порядок обработки конфиденциальной информации о физических лицах. Данный закон определяет условия получения информированного согласия от субъектов персональных данных, устанавливает ограничения на сроки хранения такой информации и возлагает на операторов обязанность по применению сертифицированных средств защиты.

Особое внимание также уделяется процедурам уведомления уполномоченного органа о выявленных фактах нарушений, что формирует основу для механизма оперативного реагирования на возникающие инциденты².

По состоянию на сегодняшний день ситуация в сфере защиты персональных данных стала одним из ключевых факторов социальной обеспокоенности в Казахстане, влияющих на эффективность обеспечения информационной безопасности государства. Особенно это стало заметно на фоне событий последних лет, когда практически ежеквартально в медиапространстве стали говорить об утечках конфиденциальных данных казахстанцев [3].

Уголовное законодательство РК предусматривает ответственность за несанкционированный доступ, незаконное присвоение, уничтожение и изменение информации, нарушение функционирования ИС, кибермошенничество, а также создание, распространение и использование вредоносного программного обеспечения.

В связи с этим перед наукой и правоприменительной практикой стоит задача объяснить особенности современной киберпреступности, спрогнозировать ее уровни с целью создания эффективного инструментария поиска и обработки различных информационных данных [4].

Административное регулирование в сфере информационной безопасности осуществляется статьями 637-641 КоАП РК. В частности, статья 641 устанавливает ответственность за нарушение правил эксплуатации ИС, возлагая ее в т.ч. на субъектов, специально уполномоченных обеспечивать безопасность³.

Примечательно, что в законодательстве ряда стран аналогичные нарушения квалифицируются как уголовные преступления, однако мера ответственности за них варьируется.

Осознавая глобальный масштаб киберугроз, государства, в том числе Узбекистан, активно разрабатывают специализированное законодательство. Ядром уголовно-правового реагирования Республики Узбекистан (далее – РУз) на нарушения в цифровой сфере с 1994 года является статья о нарушении правил информатизации (первоначально ст. 174 Уголовного кодекса (далее – УК), ныне ст. 278¹ УК РУз). Ее включение демонстрирует прогрессивность и своевременность подхода законодателя. Эта норма, устанавливающая уголовную ответственность за причинение существенного вреда из-за несоблюдения правил создания и эксплуатации ИС, легла в основу главы о компьютерных преступлениях (2007 г.), расширившей перечень криминализированных деяний. Параллельно, для менее опасных проступков, в Кодекс об административной ответственности введена статья 155. Внесенные в 2024 году дополнения в уголовное законодательство (ст.ст. 278⁸-278⁹), касающиеся противоправных деяний в сфере криптовалютных технологий, свидетельствуют о формировании сбалансированной модели. Данная модель включает в себя как репрессивные и превентивные меры, так и нормы, ориентированные на защиту национального цифрового суверенитета⁴.

Одним из направлений реформирования признается применение опыта стран с более

² О защите персональных данных и их защите: закон Республики Казахстан от 21 мая 2013 г. № 94-V [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm>.

³ Об административных правонарушениях: кодекс Республики Казахстан от 5 июля 2014 г. № 235-V ЗРК [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000235>.

⁴ Уголовный кодекс Республики Узбекистан: от 22 сент. 1994 г. № 2012-XII [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=30421110.



развитой системой права в сфере информатизации, что включает введение уголовной ответственности за системные нарушения правил эксплуатации ИС и установление критериев «крупного ущерба» с учетом затрат на восстановление данных и упущенной выгоды.

Уголовное законодательство Российской Федерации (далее – РФ) четко выделяет ответственность за нарушение установленных правил эксплуатации и доступа в сфере компьютерной информации и сетей. Общая норма (ст. 274 УК РФ) предусматривает наказание за такие нарушения, повлекшие крупный ущерб или тяжкие последствия. При этом для наиболее важных объектов критической информационной инфраструктуры (далее – КИИ) введена отдельная, значительно более строгая норма (ст. 274.1 УК РФ). Она специально предусматривает уголовную ответственность за нарушение правил эксплуатации и доступа к системам КИИ, повлекшее причинение вреда, устанавливая за это максимально суровые наказания вплоть до 10 лет лишения свободы⁵.

Уголовное законодательство Республики Беларусь (далее – РБ) устанавливает ответственность за нарушение правил эксплуатации компьютерных систем и сетей (ст. 355 УК РБ). Данная норма предусматривает наказание за причинение существенного вреда в виде ущерба информационной безопасности, финансовых потерь или сбоев в работе систем, при этом санкция предусматривает штраф, исправительные работы или ограничение свободы до двух лет. В случае тяжких последствий применяется квалифицированный состав с наказанием до семи лет лишения свободы. Особенностью является ограниченный круг субъектов – лица, имеющие правомерный доступ к системам (администраторы, ИТ-специалисты), что отражает принцип повышенной ответственности и дифференциации наказаний⁶.

Таким образом, конструкция статьи 355 УК РБ демонстрирует сбалансированный подход к криминализации рассматриваемых деяний, сочетая превентивную функцию уголовного закона с требованием соразмерности наказания степени общественной опасности содеянного.

Статьи 362 и 363 УК Украины имеют свои определенные особенности в установлении уголовной ответственности за правонарушения в сфере компьютерной информации и эксплуатации ИС. Данные нормы демонстрируют относительно менее строгий подход законодателя в отношении лиц, обладающих правом доступа к информации или ответственных за эксплуатацию систем, нежели уголовное законодательство ряда зарубежных стран.

Статья 362 УК Украины предусматривает ответственность за несанкционированное воздействие на компьютерную информацию лицом, имеющим к ней правомерный доступ. Часть 1 охватывает модификацию, уничтожение или блокирование информации и предусматривает штраф либо исправительные работы до двух лет без лишения свободы. Часть 2 устанавливает ответственность за неправомерный перехват или копирование информации, повлекшие ее утечку, с возможностью лишения свободы до трех лет и дополнительного лишения права занимать определенные должности или заниматься определенной деятельностью. При наличии квалифицирующих признаков, включая повторность, совершение деяния группой лиц по предварительному сговору или причинение значительного ущерба, наказание ужесточается до лишения свободы на срок от трех до шести лет.

Статья 363 УК Украины предусматривает ответственность за нарушение правил эксплуатации компьютерных систем, сетей электросвязи или защиты обрабатываемой в них информации, если деяние совершено лицом, ответственным за эксплуатацию, и повлекло существенный вред. Особенностью данной нормы является отсутствие такого наказания за данные деяния, как лишение свободы даже при наступлении существенного вреда. В качестве

⁵ Уголовный кодекс Российской Федерации: от 13 июня 1996 г. № 63-ФЗ (ред. от 04.08.2026 г.) [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/.

⁶ Уголовный кодекс Республики Беларусь: от 09 июня 1999 г. № 275-З [Электронный ресурс]. – Режим доступа: <https://pravo.by/document/?guid=3871&p0=hk9900275>.



наказания предусмотрены штраф, пробационный надзор или ограничение свободы до трех лет с возможным лишением права занимать определенные должности или заниматься определенной деятельностью. Состав правонарушения является материальным, поскольку обязательным условием ответственности выступает наступление существенного вреда. Такой подход свидетельствует о менее строгой уголовно-правовой реакции по сравнению с нарушениями правил безопасности в иных критических сферах⁷.

На основе Директивы (ЕС) 2018/1972 (Европейский кодекс электронных коммуникаций) государства-члены обязаны установить эффективные механизмы ответственности за несоблюдение требований безопасности, включая принудительные меры и санкции. Директива прямо требует от государств-членов создать национальные правовые механизмы, обеспечивающие соблюдение правил безопасности.

Это включает:

1. Наделение компетентных органов широкими надзорными и принудительными полномочиями (проверки, предписания, запрос информации, обязательные аудиты, расследования).

2. Обязательное введение мер ответственности (административные или иные санкции) для операторов, которые:

- не принимают надлежащих технических и организационных мер безопасности;
- не уведомляют своевременно о значительных инцидентах;
- не информируют пользователей о существенных угрозах;
- не выполняют законные предписания компетентных органов⁸.

Таким образом, Директива не просто устанавливает правила безопасности, но императивно обязывает государства-члены обеспечить их соблюдение через национальные системы принуждения и ответственности. Конкретная форма санкций определяется национальным законодательством.

Сравнительный анализ показал, что во всех рассмотренных правовых системах охраняются безопасность информации и информационных систем, а субъектом нарушения правил эксплуатации, как правило, выступает лицо, имеющее правомерный доступ к системе или ответственное за ее эксплуатацию. Уголовная ответственность преимущественно связывается с наступлением существенного вреда или иных тяжких последствий. Казахская модель отличается отсутствием самостоятельного уголовно-правового состава за нарушение правил эксплуатации информационных систем.

Обсуждение. Основное различие заключается в характере юридической реакции на последствия нарушения. Поэтому криминализация таких деяний должна предусматривать ответственность не за формальное нарушение правил, а за нарушение, совершенное специальным субъектом и повлекшее общественно опасные последствия.

В условиях конкурентного рынка коммерческие организации нередко отдают приоритет скорости вывода цифровых продуктов на рынок и снижению издержек, откладывая внедрение комплексных мер кибербезопасности на поздние этапы разработки. Исследователи указывают, что недостаточная определенность механизмов юридической ответственности за уязвимости ИС фактически снижает мотивацию субъектов цифрового рынка к реализации принципа «*security by design*», что, в свою очередь, способствует росту числа цифровых инцидентов и нарушений информационной безопасности [5].

⁷ Уголовный кодекс Украины: от 05 апр. 2001 г. № 2341-III [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=30418109&pos=3336;-57#pos=3336;-57.

⁸ Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02018L1972-20181217>.



Высокий уровень цифровизации упрощает получение гражданами услуг, позволяя им избегать сложных и длительных бюрократических процедур, но предполагаемый массированный сбор данных, в том числе персонального характера, в совокупности с недостаточным контролем за сбором и обработкой такой информации способствует многочисленным утечкам данных [6].

Анализ показывает, что правовое регулирование подобных правонарушений зависит от страны. В РК сегодня особенно значим перенос повседневности в цифровое пространство. Гарантировать безопасность в этой области – прямая задача специально назначенных уполномоченных лиц и ведомств.

Ответственность субъектов за нарушения информационной безопасности играет ключевую роль в правовом регулировании ИТ-сферы. Хотя за несоблюдение требований по защите данных предусмотрена дисциплинарная, гражданская и административная ответственность, действующее законодательство не устанавливает уголовного наказания за такие нарушения.

В научной литературе подчеркивается, что стремительное развитие цифровых технологий сопровождается пропорциональным ростом киберугроз, что объективно требует совершенствования нормативно-правовой базы в сфере кибербезопасности. В частности, в исследовании зарубежных авторов отмечается, что увеличение масштабов цифровых рисков обуславливает необходимость модернизации уголовного законодательства, а также разработки новых механизмов юридической ответственности за противоправные деяния в цифровой среде [7].

В научной литературе отсутствует единый подход к пределам уголовно-правового вмешательства в цифровой сфере. Исследователи подчеркивают необходимость правовой определенности и четкого установления признаков криминализируемого деяния [8], а казахстанские авторы — адаптации зарубежного опыта к национальному законодательству [9]. Полученные результаты соответствуют этим подходам: уголовная ответственность связывается со специальным субъектом и наступлением юридически значимых последствий. Однако стоит отметить, что хотя законодательство РК предусматривает различные меры ответственности за нарушения в информационной сфере, УК РК не содержит отдельной статьи, предусматривающей ответственность именно за несоблюдение правил информатизации. Отсутствие прямой нормы частично компенсируется иными положениями УК.

Статья 207 УК РК нацелена на умышленные деяния, приведшие к сбою работы ИС. Отягчающими обстоятельствами являются нарушения на критической инфраструктуре, группой лиц или с тяжкими последствиями. Объектом преступления является защита общественных отношений в сфере безопасности ИС (целостность, конфиденциальность) и интересов владельцев.

Статья 210 УК РК фокусируется на создании или изменении вредоносного ПО, предназначенного для незаконного воздействия на данные или работу систем или устройств. Особо выделяются случаи злоупотребления служебным положением для доступа к критическим ресурсам.

Административная ответственность за несоблюдение единых требований в сфере информационно-коммуникационных технологий (далее – ИКТ) и информационной безопасности РК прямо установлена законодательством РК. В частности, пункт 2 части 1 статьи 641 КоАП РК предусматривает санкции за нарушение обязательных стандартов и правил, утвержденных в области ИКТ и защиты информации. Единые требования представляют собой нормативно закреплённый комплекс мер и правил, направленных на обеспечение безопасности, совместимости и надежности ИС и инфраструктуры на национальном уровне. Таким образом, любое отступление субъектов от предписанных данных требований при осуществлении



деятельности, связанной с ИКТ или обработкой информации, является самостоятельным составом административного правонарушения по указанной статье, независимо от наступления вредных последствий.

Заключение. Учитывая вышеуказанное, хотелось бы отметить, что отечественное законодательство нуждается в доработке в части установления уголовной ответственности за нарушения законодательства сфере информатизации.

Статья 641 КоАП РК предусматривает ответственность за нарушение обязательных требований, однако не охватывает случаи причинения существенного общественно опасного вреда. Зарубежный опыт показывает, что разграничение административной и уголовной ответственности основывается прежде всего на тяжести последствий и особенностях субъекта. Поэтому криминализация таких деяний должна учитывать их общественную опасность, правовую определенность и соразмерность. С учетом выявленного пробела в правовом регулировании целесообразно инкорпорировать часть 1 пункта 2 статьи 641 КоАП РК в УК, сформулировав ее в следующей редакции: *«Нарушение правил эксплуатации информационных систем или сетей лицом, имеющим доступ к данной системе или сети, если это повлекло по неосторожности уничтожение, блокирование либо модификацию компьютерной информации, – относится к категории преступлений небольшой тяжести».*

Состав данной статьи должен быть материальным, с квалифицирующим признаком в виде крупного или особо крупного ущерба. Под ущербом следует понимать не только прямые потери, но и упущенную выгоду, расходы на восстановление систем и данных, а также затраты на внедрение нового программного обеспечения. Введение нормы в УК РК (в виде статьи 207-1 УК РК) обеспечит восполнение пробела в уголовно-правовой охране информационной безопасности и будет соответствовать международным тенденциям развития законодательства в условиях цифровизации.

Список использованной литературы:

1. Khan, W.N. Is Cybersecurity a Social Responsibility? / W.N. Khan, J.K. Lee, S. Liu // Information Systems Frontiers. – 2025. – Vol. 27. – Pp. 1367-1391.
2. Balagopal, N. Exploring the factors influencing information security policy compliance and violations: A systematic literature review / N. Balagopal, S.K. Mathew // Computers & Security. – 2024. – Vol. 147. – 104062.
3. Ерболатов, Е.Е. Проблемы и перспективы правового регулирования обработки биометрических данных / Е.Е. Ерболатов, С.К. Жетписов // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 4 (34). – С. 26-36.
4. Smith, G.J.D. The challenges of doing criminology in the big data era: towards a digital and data-driven approach / G.J.D. Smith // British Journal of Criminology. – 2017. – Vol. 57. Iss. 2. – Pp. 259-274.
5. Kianpour, M. More than malware: unmasking the hidden risk of cybersecurity regulations / M. Kianpour, S. Raza // Int. Cybersecur. Law Rev. – 2024. – № 5. – Pp. 169-212.
6. Амиров, А.М. Состояние и перспективы применения цифровых технологий в борьбе с преступностью / А.М. Амиров, А.В. Сырбу // «Хабаршы-Вестник» Карагандинской академии МВД РК им. Б. Бейсенова. – 2025. – № 1 (87). – С. 278-284.
7. E. Ok, J. Aria, D. Jose, C. Diego. The Impact of Cybersecurity Laws on Legal Procedures and Case Law. – 2025 [Электронный ресурс] – Режим доступа: https://ru.scribd.com/document/950227063/bymostaphar2?utm_source=chatgpt.com.
8. Ауешова, Б.Т. Comparative analysis of the legislative experience of the Republic of Kazakhstan and foreign countries in the field of criminal law protection of information security / Б.Т. Ауешова, А.А. Утенова, Г.К. Изтурганова // Вестник Института законодательства и правовой информации Республики Казахстан. – 2025. – № 1 (80). – С. 135-146.
9. Qin, X. Three Important Issues in the Legislation of Cyber Data Crime / X. Qin // Journal of Beijing Institute of Technology (Social Sciences Edition). – 2024. – Vol. 26, No. 1. – Pp. 140-147.



References:

1. Khan, W.N. Is Cybersecurity a Social Responsibility? / W.N. Khan, J.K. Lee, S. Liu // Information Systems Frontiers. – 2025. – Vol. 27. – Pp. 1367-1391.
2. Balagopal, N. Exploring the factors influencing information security policy compliance and violations: A systematic literature review / N. Balagopal, S.K. Mathew // Computers & Security. – 2024. – Vol. 147. – 104062.
3. Erbolatov, E.E. Problemy i perspektivy pravovogo regulirovaniya obrabotki biometricheskikh dannyh / E.E. Erbolatov, S.K. Zhetpisov // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 4 (34). – S. 26-36.
4. Smith, G.J.D. The challenges of doing criminology in the big data era: towards a digital and data-driven approach / G.J.D. Smith // British Journal of Criminology. – 2017. – Vol. 57. Iss. 2. – Pp. 259-274.
5. Kianpour, M. More than malware: unmasking the hidden risk of cybersecurity regulations / M. Kianpour, S. Raza // Int. Cybersecur. Law Rev. – 2024. – № 5. – Pp. 169-212.
6. Amirov, A.M. Sostojanie i perspektivy primeneniya cifrovyyh tehnologij v bor'be s prestupnost'ju / A.M. Amirov, A.V. Syrbu // «Habarshy-Vestnik» Karagandinskoy akademii MVD RK im. B. Bejsenova. – 2025. – № 1 (87). – S. 278-284.
7. E. Ok, J. Aria, D. Jose, C. Diego. The Impact of Cybersecurity Laws on Legal Procedures and Case Law. – 2025 [Elektronnyj resurs] – Rezhim dostupa: https://ru.scribd.com/document/950227063/bymostaphar2?utm_source=chatgpt.com (data obrashheniya: 27.08.2026).
8. Aueshova, B.T. Comparative analysis of the legislative experience of the Republic of Kazakhstan and foreign countries in the field of criminal law protection of information security / B.T. Aueshova, A.A. Utenova, G.K. Izturganova // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazakhstan. – 2025. – № 1 (80). – S. 135-146.
9. Qin, X. Three Important Issues in the Legislation of Cyber Data Crime / X. Qin // Journal of Beijing Institute of Technology (Social Sciences Edition). – 2024. – Vol. 26, No. 1. – Pp. 140-147.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Алихан Ержанұлы Сарбасов – М. Есболатов атындағы Қазақстан Республикасы Ішкі істер министрлігі Алматы академиясының қылмыстық құқық және криминология кафедрасының оқушысы, ұлттық қауіпсіздік және әскери істер магистрі, e-mail: alihosarbas@gmail.com, orcid.org/0009-0008-4725-4776.

Сарбасов Алихан Ержанович – преподаватель кафедры уголовного права и криминологии Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, магистр национальной безопасности и военного дела, e-mail: alihosarbas@gmail.com, orcid.org/0009-0008-4725-4776.

Sarbassov Alikhan Erzhanovich – Lecturer at the Department of Criminal Law and Criminology at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Yesbulatov, Master of National Security and Military Affairs, e-mail: alihosarbas@gmail.com, orcid.org/0009-0008-4725-4776.