ISSN: 2181-9416
2-SON, 2026

YURIST AXBOROTNOMASI

ВЕСТНИК ЮРИСТА * LAWYER HERALD

HUQUQIY, IJTIMOIY, ILMIY-AMALIY JURNAL

ISSN 2181-9416
DOI JURNAL: 10.34920/2181-9416/2026/2

YURIST AXBOROTNOMASI

2-SON

ВЕСТНИК ЮРИСТА

НОМЕР 2

LAWYER HERALD

ISSUE 2

Toshkent — 2026

СОЛИЕВА Сабрия
Эксперт-юрист в области кибербезопасности
Компания ООО «Rubicon Wireless Communication»
E-mail: sabriyasolieva@gmail.com

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ОТВЕТСТВЕННОСТИ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ УЗБЕКИСТАН

For citation (iqtibos keltirish uchun, для цитирования): СОЛИЕВА С. Уголовно-правовые аспекты ответственности за утечку персональных данных в Республике Узбекистан // Yurist axborotnomasi – Вестник юриста – Lawyer herald. № 2 (2026) С. 115-123.

2 (2026) DOI http: https://doi.org/10.34920/2181-9416/2026/2-012

АННОТАЦИЯ

В статье исследованы уголовно-правовые аспекты ответственности за утечку персональных данных в условиях цифровой среды. Установлено, что стремительное развитие информационных технологий и увеличение объёма обрабатываемых персональных данных обусловливают рост рисков их неправомерного использования и распространения. Выявлено, что действующее уголовное законодательство Республики Узбекистан не в полной мере учитывает специфику цифровых процессов обработки данных, что приводит к трудностям квалификации соответствующих деяний. Рассмотрены основные проблемы уголовно-правового регулирования, включая отсутствие самостоятельного состава преступления, размытость субъекта ответственности, а также сложности установления общественно опасных последствий, обусловленных нематериальным и отсроченным характером вреда. Оценено влияние трансграничного характера утечек персональных данных на эффективность правоприменения. Проведён критический и сравнительно-правовой анализ зарубежного опыта, позволивший выявить более детализированные и эффективные модели уголовно-правовой защиты персональных данных. Охарактеризованы ключевые направления совершенствования национального законодательства, включая необходимость введения самостоятельного состава преступления, дифференциации ответственности, а также усиления механизмов защиты прав субъектов персональных данных. Сделан вывод о необходимости модернизации уголовного законодательства с учётом современных цифровых вызовов и международной практики.

Ключевые слова: персональные данные, утечка персональных данных, уголовная ответственность, цифровая среда, защита данных, киберпреступления, правовое регулирование, информационная безопасность, квалификация преступлений, трансграничная передача данных.

SOLIYEVA Sabriya Ravshan qizi
Kiberxavfsizlik bo‘yicha yurist-ekspert
“Rubicon Wireless Communication” MChJ
E-mail: sabriyasolieva@gmail.com

O‘ZBEKISTON RESPUBLIKASIDA SHAXSGA DOIR MA’LUMOTLAR SIZIB CHIQISHI UCHUN JINOIY-HUQUQIY JAVOBGARLIK MASALALARI

ANNOTATSIYA

Ushbu ilmiy maqolada zamonaviy raqamli muhit sharoitida shaxsga doir ma’lumotlar qonunga xilof ravishda sizib chiqishi uchun javobgarlikning dolzarb jinoiy-huquqiy jihatlari atroflicha tadqiq

etilgan. Axborot texnologiyalarining jadal rivojlanishi va raqamli makonda ishlov beriladigan shaxsiy ma'lumotlar hajmining keskin ortishi ulardan maqsadsiz foydalanish xavfini oshirishi o'rnatildi. O'zbekiston Respublikasining amaldagi jinoiy qonunchiligi raqamli jarayonlarning o'ziga xos xususiyatlarini hali to'liq qamrab olmaganligi, bu esa ijtimoiy xavfli qilmishlarni huquqiy malakalashda jiddiy qiyinchiliklar tug'dirishi aniqlandi. Maqolada mustaqil jinoyat tarkibining mavjud emasligi, javobgarlik subyektining noaniqligi hamda zararli oqibatlarni aniqlashdagi murakkabliklar kabi tizimli muammolar ko'rib chiqilgan. Shuningdek, global axborot makonidagi transchegaraviy sizib chiqishlarning milliy huquqni qo'llash amaliyoti samaradorligiga ko'rsatadigan salbiy ta'sir baholandi. Rivojlangan xorijiy davlatlar tajribasini qiyosiy-huquqiy tahlil qilish natijasida shaxsga doir ma'lumotlarni himoya qilishning yanada takomillashgan modellari ma'lum bo'ldi. Milliy qonunchilikni modernizatsiya qilishning ustuvor yo'nalishlari va asosiy muntazamliklar tavsiflandi. Yakunda jinoiy qonunchilikni zamonaviy raqamli tahdidlar, kiberxavfsizlik talablari va ilg'or xalqaro standartlarni hisobga olgan holda tubdan isloh qilish zarurligi to'g'risida asoslantirilgan xulosalar bayon etilgan.

Kalit so'zlar: shaxsga doir ma'lumotlar, shaxsga doir ma'lumotlarning sizib chiqishi, jinoiy javobgarlik, raqamli muhit, ma'lumotlarni himoya qilish, kiberjinoyatlar, huquqiy tartibga solish, axborot xavfsizligi, jinoyatlarni kvalifikatsiya qilish, ma'lumotlarni transchegaraviy uzatish.

SABRIYA Soliyeva
Legal Expert in Cybersecurity
«Rubicon Wireless Communication» LLC
E-mail: sabriyasolieva@gmail.com

CRIMINAL LAW ASPECTS OF LIABILITY FOR PERSONAL DATA BREACHES IN THE REPUBLIC OF UZBEKISTAN

ANNOTATION

This article examines the criminal law aspects of liability for personal data breaches in the digital environment. It is found that the rapid development of information technologies and the increasing volume of processed personal data lead to growing risks of unlawful use and dissemination. It is established that the current criminal legislation of the Republic of Uzbekistan does not fully reflect the specifics of digital data processing, resulting in difficulties in legal qualification. The main problems are considered, including the absence of an independent corpus delicti, the ambiguity of the subject of liability, and challenges in determining socially dangerous consequences. The impact of the cross-border nature of data breaches is evaluated. Regularities are characterized through a comparative legal analysis of foreign experience, revealing more detailed and effective models of criminal law protection. Directions for improving national legislation are proposed. It is concluded that modernization of criminal law is necessary.

Keywords: personal data, personal data breach, criminal liability, digital environment, data protection, cybercrime, legal regulation, information security, crime qualification, cross-border data transfer

Утечка персональных данных представляет собой одну из наиболее острых и системных проблем как в Республике Узбекистан, так и в мировом масштабе. Стремительное развитие информационных технологий, цифровых платформ и электронных сервисов обусловило значительное увеличение объёма обрабатываемых персональных данных, что, в свою очередь, привело к росту рисков их неправомерного использования, распространения и утраты [1, B.3]

Особую сложность в сфере защиты и регулировании персональных данных представляет не только технический аспект обеспечения их безопасности, но и правовая неопределённость, связанная с механизмами контроля, надзора и выявления правонарушений. Процессы обработки данных в цифровой среде носят распределённый, многоуровневый и зачастую трансграничный характер, что существенно затрудняет установление факта противоправного

воздействия, определение круга ответственных лиц, а также последующую правовую квалификацию соответствующих деяний.

Под утечкой персональных данных следует понимать неправомерное раскрытие, распространение либо предоставление персональной информации третьим лицам без законных оснований или согласия субъекта данных, в том числе в результате нарушения требований к их обработке и защите [2]. Утечка может происходить как вследствие умышленных действий (например, незаконная передача или продажа баз данных), так и в результате неосторожности, связанной с недостаточным уровнем технической или организационной защиты информации. Между тем утечка персональных данных способна повлечь существенные негативные последствия для прав и законных интересов личности, включая вмешательство в частную жизнь, причинение материального и репутационного вреда, а также использование персональных данных для совершения мошеннических и иных преступлений [3], [4]. Несмотря на это, существующие механизмы правовой защиты, в том числе уголовно-правовые, не всегда оказываются достаточными для эффективного противодействия данным угрозам.

Действующее уголовное законодательство Республики Узбекистан не в полной мере обеспечивает эффективную правовую реакцию на утечки персональных данных в условиях цифровой среды. Несмотря на формальное наличие статьи 141-2 Уголовного Кодекса Республики Узбекистан (далее по тексту – УК РУз), её конструкция не позволяет в достаточной степени учитывать особенности современных цифровых процессов обработки информации и связанных с ними рисков.

Особую проблему представляет размытость субъекта ответственности в условиях распределённой обработки данных, а также сложность установления причинно-следственной связи между действиями конкретного лица и наступившими последствиями. Дополнительные трудности возникают при квалификации и оценке вреда, который зачастую носит нематериальный, отсроченный или потенциальный характер. С учётом проведённого сравнительно-правового анализа зарубежного опыта обоснована необходимость совершенствования уголовно-правового регулирования в данной сфере. В частности, представляется целесообразным уточнение элементов состава, включая формы вины, а также внедрение более дифференцированного подхода к ответственности с учётом характера данных и степени общественной опасности деяния.

Уголовно-правовое регулирование защиты персональных данных в Республике Узбекистан на сегодняшний день в значительной степени сосредоточено в рамках статьи 141-2 УК РУз, предусматривающей ответственность за нарушение законодательства о персональных данных [5]. Указанная норма представляет собой ключевой инструмент уголовно-правовой охраны соответствующих общественных отношений, направленных защиту персональной информации. Вместе с тем её содержание и правоприменительная практика свидетельствуют о наличии ряда концептуальных и практических проблем, обусловленных как особенностями самой конструкции состава преступления, так и стремительным развитием цифровой среды, в которой обработка и утечка персональных данных приобретают качественно новые формы [6]. В этой связи представляется необходимым проведение критического анализа статьи 141-2 УК РУз с точки зрения её способности обеспечивать эффективную уголовно-правовую защиту персональных данных, выявление существующих пробелов и противоречий, а также сопоставление национального подхода с зарубежным опытом регулирования. Такой анализ позволит сформулировать обоснованные предложения по совершенствованию действующего законодательства с учётом современных цифровых вызовов и рисков.

Статья 141-2 УК РУз закрепляет уголовную ответственность за нарушение законодательства о персональных данных, охватывая широкий перечень противоправных действий, включая незаконный сбор, хранение, использование, распространение и иные формы обработки персональных данных [5]. Формально данная норма представляет собой комплексный механизм уголовно-правовой защиты персональных данных, ориентированный на регулирование их оборота, в том числе с использованием информационных технологий. При более детальном анализе содержания данной статьи выявляется её чрезмерно широкий и в определённой степени декларативный характер. Перечень действий, указанных в диспозиции нормы, охватывает практически все возможные операции с персональными данными, что, с одной стороны, свидетельствует о стремлении законодателя обеспечить максимальную защиту соответствующих общественных отношений, однако, с другой стороны, создаёт значительные сложности для правоприменительной практики. В частности, отсутствие чёткой дифференциации между отдельными формами противоправного поведения затрудняет квалификацию деяний и разграничение уголовной и административной ответственности. Особое внимание заслуживает положение о наступлении уголовной ответственности лишь при условии предварительного применения административного взыскания. Данная конструкция фактически свидетельствует о вторичном, субсидиарном характере уголовно-правовой защиты персональных данных, при котором утечка или иное неправомерное использование персональных данных первоначально рассматривается как административное правонарушение. В условиях цифровой среды, где утечка персональных данных может повлечь существенные и зачастую необратимые последствия для прав и законных интересов личности, подобный подход вызывает обоснованные сомнения в его эффективности. Кроме того, проблемным аспектом является неопределённость в установлении общественно опасных последствий, особенно в случаях, не подпадающих под квалифицирующие признаки части второй данной статьи. Законодатель не раскрывает критерии «тяжких последствий», что создаёт риск субъективного толкования и неоднородности судебной практики. При этом значительная часть вреда от утечек персональных данных носит нематериальный, отсроченный или потенциальный характер, что затрудняет его оценку в рамках традиционных подходов уголовного права.

В том числе особую актуальность представляет квалификация утечек персональных данных в рамках действующего Уголовного Кодекса. Несмотря на формальное закрепление ответственности за нарушение законодательства о персональных данных, правоприменительная практика сталкивается с рядом системных проблем, обусловленных особенностями цифровой среды. Прежде всего, значительные трудности возникают при установлении причинно-следственной связи между действиями виновного лица и наступившими последствиями. В условиях распределённой обработки данных, использования облачных технологий и привлечения множества субъектов (операторов, администраторов, подрядчиков) процесс обработки персональных данных приобретает сложный многоуровневый характер [6]. Это затрудняет выявление конкретного лица, действия которого привели к утечке, а также установление степени его вины. Кроме того, проблема разграничения форм вины. Утечки персональных данных могут происходить как в результате умышленных действий (например, незаконная передача или продажа баз данных), так и вследствие неосторожности, выражающейся в недостаточном обеспечении мер защиты информации. Однако на практике разграничение указанных форм вины вызывает затруднения, поскольку последствия могут быть идентичными, а доказательная база — ограниченной. Дополнительной проблемой является оценка общественно опасных последствий утечки персональных данных. В отличие от традиционных преступлений, вред в

рассматриваемых случаях зачастую носит нематериальный, отсроченный или потенциальный характер. Персональные данные могут быть использованы спустя значительное время после их утечки, что усложняет установление факта причинения вреда и его объёма.

Кроме того, необходимо обратить внимание на разграничение уголовной и административной ответственности за нарушение законодательства о персональных данных. В действующей редакции статьи 141-2 УК РУз уголовная ответственность носит субсидиарный характер и наступает лишь после применения административного взыскания, что фактически размывает границы между указанными видами ответственности. На мой взгляд подобная конструкция не соответствует современным условиям цифровой среды, в которой утечки персональных данных способны повлечь масштабные и трудноустранимые последствия уже при первом совершении деяния. В этой связи разграничение уголовной и административной ответственности должно осуществляться не формально, а на основе критериев общественной опасности. В качестве таких критериев целесообразно рассматривать: масштаб утечки персональных данных; категорию затронутой информации (включая биометрические и чувствительные данные); форму вины (умысел либо неосторожность); характер и степень последствий, включая нематериальный и потенциальный вред. При этом административная ответственность должна применяться в случаях единичных и малозначительных нарушений, не повлёкших существенного вреда, тогда как уголовная ответственность — при наличии умысла, массового распространения данных, использовании служебного положения либо создании реальной угрозы причинения вреда правам субъектов персональных данных.

Следовательно специфика цифровой среды обуславливает необходимость пересмотра традиционных подходов к квалификации преступлений, связанных с персональными данными, а также разработки более гибких и адаптированных уголовно-правовых механизмов реагирования.

В научной литературе, посвящённой вопросам уголовно-правовой защиты персональных данных, отсутствует единый подход к оценке достаточности действующего регулирования, что свидетельствует о формировании доктринальной дискуссии по данному вопросу. С одной стороны, в ряде исследований обращается внимание на недостаточную эффективность существующего механизма ответственности в Республике Узбекистан. Отмечается, что действующая система санкций не в полной мере учитывает масштаб правонарушения, характер обработки персональных данных и степень причинённого вреда, а также не обеспечивает должной дифференциации ответственности в зависимости от формы вины и последствий. Кроме того, указывается на отсутствие пропорциональности наказания, в связи с чем санкции могут не обладать достаточным сдерживающим эффектом, особенно в отношении крупных операторов персональных данных. В таких условиях ответственность может восприниматься не как превентивная мера, а как допустимый риск осуществления деятельности [7]. С другой стороны, высказывается позиция, согласно которой действующее уголовно-правовое регулирование обладает достаточным потенциалом за счёт своего комплексного характера. Подчёркивается, что персональные данные охраняются не изолированно, а в системе взаимосвязанных объектов уголовно-правовой защиты, включающих информационную безопасность, права личности и общественную безопасность [8]. Однако, на мой взгляд признание достаточности существующего регулирования не учитывает масштабность и трансграничный характер утечек персональных данных, их высокую латентность, а также возможность многократного использования информации после её незаконного распространения. В свою очередь, сосредоточение исключительно на усилении санкций без изменения конструкции уголовно-правовой нормы не позволяет устранить проблемы квалификации и доказательства.

Анализ зарубежного законодательства позволяет выявить иные, более системные подходы к уголовно-правовой охране персональных данных [4] [9]. В Японии уголовно-правовая защита персональных данных осуществляется, в том числе, на основе Закона «О защите личной информации» 2003 года. Особенностью данного подхода является институциональное разделение: в рамках одного нормативного акта детально определяется правовой статус персональных данных (статья 2), а также устанавливаются основания и меры уголовной ответственности (раздел VIII, статьи 176-185) [3] [10]. Подобная конструкция позволяет обеспечить более чёткую взаимосвязь между определением объекта правовой охраны и санкциями за его нарушение. В отличие от более абстрактных формулировок, характерных для уголовного законодательства ряда стран, японская модель демонстрирует высокий уровень нормативной определённости, что способствует единообразию правоприменительной практики и снижает риск произвольного толкования.

В свою очередь, в Южной Кореи уголовно-правовая охрана персональных данных реализуется в рамках Закона «О защите персональной информации» 2011 года (Personal Information Protection Act – PIPA) [11], который считается одним из наиболее строгих в мире. В отличие от японского подхода, корейская модель характеризуется не только детальной регламентацией обязанностей операторов персональных данных, но и широким перечнем конкретизированных составов правонарушений. В частности, уголовно наказуемыми признаются такие деяния, как незаконное получение персональных данных, их разглашение в процессе исполнения служебных обязанностей, а также непринятие мер по их удалению по истечении установленного срока хранения [3].

Существенным отличием корейской модели является также наличие дополнительных механизмов воздействия, направленных на усиление превентивной функции уголовного права. Так, наряду с традиционными видами наказаний (лишение свободы и штраф), законодатель предусматривает возможность конфискации или взыскания прибыли, полученной в результате незаконного использования персональных данных. Данный подход отражает признание экономической ценности персональных и направлен на устранение финансовой заинтересованности в совершении соответствующих правонарушений.

Интерес представляет также подход Российской Федерации к уголовно-правовой защите персональных данных, который, в отличие от Республики Узбекистан, характеризуется более детализированным и дифференцированным регулированием. В частности, уголовная ответственность за незаконные действия с персональными данными закреплена в специальной норме – статье 272.1 Уголовного кодекса Российской Федерации [12]. Анализ содержания данной статьи позволяет отметить, что российский законодатель выделяет самостоятельный состав преступления, непосредственно связанный с незаконным оборотом персональных данных. В отличие от более обобщённой конструкции статьи 141-2 УК РУз, норма Уголовного Кодекса Российской Федерации детально разграничивает формы противоправного поведения, включая незаконный сбор, хранение, использование и распространение персональных данных, полученных незаконным путём. Существенным преимуществом российской модели является градация ответственности в зависимости от характера и степени общественной опасности деяния. Так, законодатель выделяет квалифицирующие признаки, связанные с обработкой данных особых категорий (например, биометрических или данных несовершеннолетних), наличием корыстной заинтересованности, причинением крупного ущерба, использованием служебного положения, а также совершением деяния группой лиц [13]. Более того, отдельно предусматривается ответственность за трансграничную передачу персональных данных, что отражает современный характер цифровых угроз.

Особого внимания заслуживает также криминализация создания и функционирования информационных ресурсов, предназначенных для незаконного оборота персональных данных. Данная норма демонстрирует переход от реактивного к превентивному подходу уголовно-правовой защиты, направленного на пресечение инфраструктуры, обеспечивающей распространение незаконных баз данных. Вместе с тем, несмотря на более высокий уровень нормативной детализации, российская модель не лишена дискуссионных аспектов. В частности, остаётся актуальной проблема установления причинно-следственной связи между действиями виновного лица и наступившими последствиями, а также вопросы разграничения уголовной и административной ответственности.

Кроме того, широкая диспозиция статьи может порождать риск избыточной криминализации при отсутствии чётких критериев оценки общественной опасности деяния [14]. Тем не менее, в сравнении с законодательством Республики Узбекистан, российский подход представляется более адаптированным к условиям цифровой среды, поскольку предусматривает самостоятельную уголовно-правовую оценку незаконного оборота персональных данных, учитывает разнообразие форм противоправного поведения и вводит дополнительные механизмы ответственности, включая квалифицирующие признаки и специальные составы.

Проведённый анализ статьи 141-2 УК РУз, а также сравнительное исследование зарубежного опыта позволяют сформулировать ряд конкретных предложений, направленных на повышение эффективности уголовно-правовой защиты персональных данных в условиях цифровой среды. Во-первых, необходимо выделить утечку персональных данных в качестве самостоятельного состава преступления, с закреплением в диспозиции нормы чёткого определения утечки как неправомерного раскрытия, распространения либо предоставления персональной информации третьим лицам без законных оснований. Это позволит устранить существующую неопределённость и повысить качество квалификации соответствующих деяний: ***«незаконное раскрытие, распространение либо предоставление персональных данных третьим лицам без согласия субъекта данных или иных законных оснований, совершённое с использованием информационных технологий, — наказывается…».*** Во-вторых, необходимо закрепить дифференцированный подход к ответственности в зависимости от категории персональных данных. В частности, следует предусмотреть повышенную ответственность за незаконные действия с биометрическими данными, данными несовершеннолетних, а также иными чувствительными категориями информации. В-третьих, необходимо введение квалифицирующих признаков, в том числе связанных с трансграничной передачей персональных данных, совершением деяния с использованием служебного положения, извлечением имущественной выгоды, а также характером и объёмом распространённых данных. Указанные признаки позволят устранить существующие сложности квалификации, дифференцировать ответственность и обеспечить единообразие правоприменительной практики. Возможная формулировка квалифицированного состава: ***«то же деяние, совершённое:***

а) в отношении биометрических данных;

б) с использованием служебного положения;

в) с целью извлечения имущественной выгоды;

г) путём трансграничной передачи персональных данных;

д) повлёкшее тяжкие последствия, — наказывается…».

В-четвертых, необходимо нормативное закрепление критериев оценки общественно опасных последствий утечки персональных данных, включая признание нематериального, отсроченного и потенциального вреда в качестве значимых последствий. Это позволит

устранить существующие сложности в доказывании и обеспечит единообразие правоприменительной практики. В частности, к числу таких последствий целесообразно отнести: ***«причинение вреда неприкосновенности частной жизни; создание угрозы использования персональных данных для совершения мошеннических и иных преступлений; распространение персональных данных неограниченному кругу лиц; причинение репутационного или имущественного вреда, в том числе в потенциальной форме».*** В-пятых, следует рассмотреть возможность введения уголовной ответственности за создание, администрирование и использование информационных ресурсов, предназначенных для незаконного оборота персональных данных, включая базы данных и цифровые платформы. Данная мера позволит перейти от реактивного к превентивному подходу в противодействии утечкам персональных данных. В частности, под такими ресурсами могут пониматься интернет-сайты, телеграм-каналы, базы данных, маркетплейсы или иные цифровые платформы, используемые для систематического хранения, распространения или продажи персональных данных без законных оснований. Представляется возможным закрепление следующей диспозиции: ***«создание, администрирование либо использование информационных ресурсов, заведомо предназначенных для незаконного сбора, хранения, распространения или иного оборота персональных данных, — наказывается…». При этом квалифицирующими признаками могут выступать: совершение деяния группой лиц; извлечение имущественной выгоды; массовый характер распространения персональных данных.*** Закрепление подобной нормы позволит пресекать не только последствия утечек, но и функционирование инфраструктуры, обеспечивающей незаконный оборот персональных данных, что соответствует современным тенденциям развития киберпреступности. В-шестых, целесообразно определить признаки субъекта преступления, включая закрепление ответственности не только физических лиц, но и должностных лиц организаций, осуществляющих обработку персональных данных, с учётом их роли в обеспечении безопасности информации. В частности, к числу таких лиц могут относиться руководители организаций, компаний, администраторы информационных систем, сотрудники, ответственные за обработку и защиту персональных данных, а также иные лица, на которых возложены соответствующие обязанности. В этой связи целесообразно закрепление положения о том, что уголовная ответственность наступает в случае невыполнения или ненадлежащего выполнения обязанностей по обеспечению безопасности персональных данных, если это повлекло их утечку либо создало реальную угрозу наступления таких последствий. Предлагается следующая формулировка диспозиции: ***«нарушение установленных требований по обеспечению безопасности персональных данных лицом, обязанным соблюдать такие требования в силу занимаемой должности или выполняемых функций, повлёкшее их незаконное раскрытие, распространение либо предоставление третьим лицам, — наказывается…»***. Закрепление подобной нормы позволит устранить неопределённость в распределении ответственности между участниками обработки персональных данных и повысить уровень защищённости информации в организациях.

Таким образом, предложенные изменения направлены на формирование более чёткой, дифференцированной и адаптированной к цифровой среде системы уголовно-правовой защиты персональных данных, обеспечивающей эффективное противодействие современным угрозам.

Представленные предложения по совершенствованию Уголовного кодекса Республики Узбекистан направлены на устранение выявленных пробелов и повышение эффективности уголовно-правовой защиты персональных данных. Следует отметить, что предлагаемые изменения основаны не только на теоретическом анализе, но и на выявленных в

правоприменительной практике проблемах, включая сложности квалификации, неоднородность судебной практики и недостаточную эффективность действующих механизмов ответственности. В этой связи их реализация позволит обеспечить не формальное, а содержательное усиление уголовно-правовой защиты персональных данных.

В этой связи, дальнейшее развитие уголовного законодательства в сфере защиты персональных данных должно осуществляться с учётом международного опыта, технологических изменений и необходимости обеспечения баланса между интересами государства, общества и личности, что является ключевым условием формирования эффективной и устойчивой системы правового регулирования в цифровую эпоху.

СНОСКИ/ IQTIBOSLAR/REFERENCES:

1. Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных // Автореферат диссертации на соискание ученой степени кандидата юридических наук — 2017г.— Текст: непосредственный.

2. Утечка персональных данных. — Текст: электронный // URL: https://academy-of-capital.ru/blog/utechka-personalnykh-dannykh/ (дата обращения: 31.03.2026)

3. Волкова А. Ю. Современное состояние уголовно-правовой охраны персональных данных: зарубежный опыт. — Текст: электронный // URL: https://legascom.ru/notes/10615-sovremennoe-sostoyanie-ugolovno-pravovoj-okhrany-personalnykh-dannykh-zarubezhnyj-opyt-volkova-a-yu (дата обращения: 22.03.2026).

4. Утечка персональных данных. — Текст: электронный // сайт «Лаборатория Касперского» // URL: https://www.kaspersky.ru/resource-center/definitions/data-breach (дата обращения: 28.03.2026).

5. Уголовный Кодекс Республики Узбекистан. — Текст: официальный // URL: https://lex.uz/docs/111457 (дата обращения: 20.03.2026).

6. К задаче выявления утечек персональных данных: классификация через атрибутивный анализ. — Текст: электронный // URL: https://www.researchgate.net/publication/400489110_K_zadace_vyavlenia_utecek_personalnyh_dannyh_klassifikacia_cerez_atributivnyj_analiz_On_the_problem_of_detecting_personal_data_breaches_classification_through_attribute-based_analysis (дата обращения: 1.04.2026)

7. Азимжонов Д. Д. Правовые механизмы защиты персональных данных в условиях цифровых угроз Республики Узбекистан // CENTRAL ASIAN JOURNAL OF ACADEMIC RESEARCH. — 2025. — Текст: непосредственный.

8. Бахадирова И. И. Особенности защиты персональных данных в уголовном праве Республики Узбекистан // Сборник материалов международной научной конференции «Zamonaviy dunyoda ijtimoiy fanlar: nazariy va amaliy izlanishlar». — Текст: непосредственный. — DOI: https://doi.org/10.5281/zenodo.18547931.

9. Прокопенко А. Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? — Текст: электронный // URL: https://cyberleninka.ru/article/n/borba-s-utechkami-personalnyh-dannyh-pomozhet-li-uzhestochenie-otvetstvennosti/viewer (дата обращения: 26.03.2026).

10. Уголовный Кодекс Японии. — Текст: перевод// URL: Уголовный кодекс Японии | Россия: Библиотека Пашкова (дата обращения: 20.03.2026).

11. Уголовный Кодекс Южной Кореи. — Текст: перевод // URL: Уголовный кодекс Республики Корея 형법 (дата обращения: 21.03.2026).

12. Уголовный Кодекс Российской Федерации. — Текст: официальный // URL: «Уголовный кодекс Российской Федерации» (УК РФ) от 13.06.1996 N 63-ФЗ (последняя редакция) \ КонсультантПлюс (дата обращения: 21.03.2026).

13. Ужесточение ответственности за утечку персональных данных в 2025 году. — Текст: электронный // URL: https://ideco.ru/uzhestvochenie_otvetstvennosti_za_utechku_personalnykh_dannykh_v_2025_godu (дата обращения: 22.03.2026).

14. Вагидов А. Н., Болдырева А. А. Кибербезопасность: юридическая ответственность за утечку данных. — Текст: электронный // URL: https://cyberleninka.ru/article/n/kiberbezopasnost-yuridicheskaya-otvetstvennost-za-utechku-dannyh/viewer (дата обращения: 27.03.2026).

YURIST AXBOROTNOMASI

2-SON

ВЕСТНИК ЮРИСТА

НОМЕР 2

LAWYER HERALD

ISSUE 2

ISSN 2181-9416

DOI JURNAL: 10.34920/2181-9416/2026/2

2026-YIL