

Дата поступления рукописи в редакцию: 11.03.2026 г.
Дата принятия рукописи в печать: 03.04.2026 г.

DOI: 10.24412/2076-1503-2026-3-88-94

ЧУКРЕЕВ Вадим Андреевич,
доктор юридических наук, доцент,
заместитель прокурора Свердловской области,
г. Екатеринбург, Российская Федерация,
e-mail: chukreevva@mail.ru

КРИМИНАЛЬНАЯ ЭКСПЛУАТАЦИЯ БИОЛОГИЧЕСКОЙ И СОЦИАЛЬНОЙ СУЩНОСТИ ЧЕЛОВЕКА: УГОЛОВНО-ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье исследуются теоретические и практические проблемы уголовно-правовой защиты человека как единства биологической и социальной сущности. Обосновывается необходимость четкого разграничения указанных сущностей в уголовном праве для адекватной квалификации общественно опасных деяний. Анализируются формы криминальной эксплуатации человека, включая новые виды — использование биометрических персональных данных и создание дипфейков. Рассматриваются последние изменения уголовного законодательства (ст. 272.1 УК РФ), актуальные проблемы правоприменения и перспективы его дальнейшего совершенствования с учетом зарубежного опыта и требований технологической безопасности.

Ключевые слова: биологическая сущность человека, социальная сущность человека, криминальная эксплуатация, персональные данные, биометрические данные, дипфейки, автоматизированная обработка, уголовная ответственность.

CHUKREEV Vadim Andreevich,
Doctor of Law, Associate Professor,
Deputy Prosecutor of the Sverdlovsk Region,
Yekaterinburg, Russian Federation

CRIMINAL EXPLOITATION OF THE BIOLOGICAL AND SOCIAL ESSENCE OF MAN: CRIMINAL LAW PROBLEMS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF DIGITALIZATION

Annotation. The article examines the theoretical and practical problems of criminal legal protection of a person as a unity of biological and social essence. The necessity of a clear differentiation of these entities in criminal law for an adequate qualification of socially dangerous acts is substantiated. The forms of criminal human exploitation are analyzed, including new types — the use of biometric personal data and the creation of deepfakes. Recent changes in criminal legislation are being considered (art. 272.1 of the Criminal Code of the Russian Federation), current problems of law enforcement and prospects for its further improvement, taking into account foreign experience and technological safety requirements.

Key words: human biological essence, human social essence, criminal exploitation, personal data, biometric data, deepfakes, automated processing, criminal liability.

Современный этап развития общества характеризуется глубокой трансформацией представлений о человеке как объекте правовой охраны. Уголовное право должно четко выделять, какие именно сущности — биологические или социальные — защищаются в той или иной норме, и достаточно ли последней

для защиты биологической или социальной сущности личности. Отсюда вытекает необходимость четкого определения и разграничения биологической и социальной сущностей человека. К сожалению, представители различных отраслей юридической науки чаще изучают соотношение понятий «личность», «человек», «индивидуум» и «гражданин»

нин», не акцентируя внимания на важности и значении биологической и социальной сущностей человека. Между тем именно это разграничение приобретает ключевое значение в условиях, когда анатомическая структура, физиологические свойства, биометрические данные человека становятся предметом самостоятельных посягательств. Важно поднять проблему уголовно-правовой и криминологической защиты понятия «человек», в котором воплощено неразрывное единство различных сторон его существа: социальной, биологической и новой — технической, поскольку под воздействием внешней информации происходит формирование ранее неизвестных интересов и целей людей в обществе. Цель настоящего исследования — на основе анализа доктринальных подходов, законодательства и правоприменительной практики разработать концептуальные основы уголовно-правовой охраны биологической и социальной сущности человека, а также сформулировать предложения по совершенствованию уголовного закона в части защиты персональных и биометрических данных.

Человека как биологическое существо, его природные, приобретенные качества или свойства, навыки можно эксплуатировать (использовать) совершенно различными способами. Эксплуатация человека обладает повышенной опасностью, высоколатентна и очень доходна. Можно согласиться с мнением В.И. Коваленко, что «криминальная эксплуатация человека осуществляется в следующих формах: эксплуатация человека как целостной личности (социотипа), его социально и психологически обусловленных индивидуальных личностных качеств, физических, сексуальных, интеллектуальных свойств, умений, трудовых навыков (услуг); эксплуатация биологических свойств, физиологических функций организма человека (биотипа) в сфере трансплантационных, репродуктивных технологий, в ходе которой последний эксплуатируется как представитель биологического вида (человек)» [1]. Указанная классификация носит очень общий характер и не включает в себя ряд иных противоправных видов эксплуатации, например, эксплуатацию человека для извлечения гамет или использование биометрических персональных данных человека для противоправных целей. Статья 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» «биометрическими персональными данными признает сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные)» [2].

В этой связи следует говорить о таких называвшихся выше видах эксплуатации человека, как 1) эксплуатация (использование) человека как лично-

сти (его навыков, способностей, умений), 2) эксплуатация (использование) анатомической структуры или физиологических свойств человека и 3) эксплуатация биометрических персональных данных человека.

Развитие искусственного интеллекта, в том числе создание с его помощью «фиктивных» видео, звукозаписей, изображений с использованием биометрических персональных данных создает правовые пробелы в уголовном законодательстве по защите и охране основных прав человека. Существует и другие проблемы в уголовно-правовой науке, связанных с защитой персональных данных и использования биометрических персональных данных человека.

Во-первых, угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных при автоматизированной обработке биометрических персональных данных на устройстве клиента-физического лица в целях идентификации и (или) аутентификации физического лица в случае выполнения условий, установленных в частях 18.18 и 18.20 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378, зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620.

Во-вторых, угрозы безопасности, актуальные при сборе биометрических персональных данных, их передаче в осуществляющие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц информационные системы организаций финансового рынка, указанных в части 10 статьи 14.1 Федерального закона № 149-ФЗ, в целях идентификации и (или) аутентификации физического лица в случае выполнения условий, установленных в частях 18.18 и 18.20 статьи 14.1 Федерального закона № 149-ФЗ. В-третьих, угрозы безопасности, актуальные при обработке (за исключением сбора), в том числе хранении, био-

метрических персональных данных и информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее - информация о степени соответствия) в информационной системе организации финансового рынка в целях аутентификации физического лица в случае выполнения условий, установленных частью 18.18 статьи 14.1 Федерального закона N 149-ФЗ. В-четвертых, угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, нарушения конфиденциальности (компрометации) биометрических персональных данных при обработке (за исключением сбора), в том числе хранении, биометрических персональных данных и информации о степени соответствия в информационной системе организации финансового рынка в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18.20 статьи 14.1 Федерального закона N 149-ФЗ, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 «Состава и содержания организационных и технических мер».

В-пятых, угрозы безопасности, актуальные при передаче биометрических персональных данных и информации о степени их соответствия в информационную систему организации финансового рынка в целях аутентификации и (или) идентификации физического лица в случае выполнения условий, установленных частями 18.18 и 18.20 статьи 14.1 Федерального закона N 149-ФЗ.

В-шестых, угроза безопасности, актуальная при взаимодействии организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка в целях аутентификации физического лица в соответствии с частью 18.24 статьи 14.1 Федерального закона N 149-ФЗ – угроза нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 «Состава и содержания организационных и технических мер» [3].

Можно прогнозировать, что подобные угрозы могут возникнуть при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах иных организаций. К сожалению, в УК РФ пока нет статей, которые предусматривали бы наказа-

ние за нарушения в сфере оборота персональных данных. Наиболее близкие статьи УК РФ – это ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 272 «Неправомерный доступ к компьютерной информации».

Уголовный закон только в ч. 2 ст. 173.2 предусматривает ответственность за незаконный оборот именно персональных данных: использование персональных данных, полученных незаконным путем, если эти деяния совершены для внесения в единый государственный реестр юридических лиц сведений о подставном лице. В этой связи возникает необходимость совершенствования уголовного-правового механизма охраны персональных данных, в том числе разработку специальной уголовно-правовой нормы об ответственности за совершение общественно опасных деяний, нарушающих требования законодательства о персональных данных гражданина. В этой связи возникает ряд задач, связанных с определением общественной опасности такого деяния, которая была бы достаточна для криминализации. Такая задача решается путем осуществления сопоставительного анализа действующих норм об административной ответственности за неправомерные действия с персональными данными, а также моделированием негативных последствий, которые могут наступить в результате совершения таких правонарушений.

Действующее российское законодательство предусматривает различные виды юридической ответственности за нарушение правил обращения персональных данных. КоАП РФ содержит ряд специальных норм об ответственности для физических лиц и организаций за неправомерные действия с персональными данными граждан: ст. 13.11. Нарушение законодательства РФ в области персональных данных. Действие данной нормы распространяется на физических и юридических лиц, подлежащих ответственности за совершение нарушений действующего законодательства о персональных данных. Учитывая, что уголовная ответственность организаций действующим законодательством исключается, следует рассмотреть содержание деяний-правонарушений, ответственность за совершение которых может быть возложена на физическое лицо за утрату или иное несанкционированное распространение персональных данных, а равно – создания условий, при которых будет возможным получение персональных данных третьими, не уполномоченными на то лицами: – неправомерная обработка персональ-

ных данных (ч. 1 ст. 13.11 КоАП РФ); – обработка персональных данных, произведенная без согласия их правообладателя – субъекта персональных данных (ч. 2 ст. 13.11 КоАП РФ); – невыполнение обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных (ч. 4 ст. 13.11 КоАП РФ); – невыполнение обязанности о блокировании или уничтожении персональных данных в случае, если персональные данные были неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки (ч. 5 ст. 13.11 КоАП РФ); – невыполнение обязанности по соблюдению условий сохранности персональных данных и исключающих несанкционированный к ним доступ, если это повлекло различные «неправомерные действия» в отношении персональных данных (ч. 6 ст. 13.11 КоАП РФ). Перечисленные в ст. 13.11 КоАП РФ деяния представляют собой частные случаи нарушения установленных действующим законодательством правил обращения персональных данных граждан. Сами по себе они едва ли могут претендовать на статус преступления в виду отсутствия должной общественной опасности. Поэтому криминализация правонарушения, предметом которого являются персональные данные, возможна только в случаях наступления общественно опасных последствий в виде причинения вреда жизни и здоровью, имущественного ущерба или иных тяжких последствий. Толкование содержания ст. 13.11 КоАП РФ позволяет заключить, что лицо, допущенное в установленном законом порядке, к получению, обобщению, систематизации и иным действиям с персональными данными, может в случае нарушения нормативных требований безопасности создать угрозу для утраты и/или получения третьими неуправомоченными лицами конфиденциальной информации – персональных данных, а равно – их действительная утрата и/или распространение. Поэтому при формулировании уголовно-правовой нормы нет необходимости перечислять все возможные виды нарушений законодательства о персональных данных в качестве общественно опасного деяния – признака объективной стороны. Но все же следует понимать, что общественная опасность такого преступления формируется ввиду несанкционированной передачи или получения персональных данных третьими неуправомоченными лицами, которые, в свою очередь, получают возможность для совершения противоправных действий, направленных против прав, свобод и законных интересов граждан, интересов общества и государства.

Юридическая конструкция состава преступления, предметом которого являются персональ-

ные данные, должна предполагать наступление общественно опасных последствий, которые выступают обязательным признаком объективной стороны. Конструирование состава преступления как формального не обеспечит должного уровня общественной опасности для криминализации и сведет описываемое деяние к уровню административного правонарушения. В части видов общественно опасных последствий следует предусмотреть имущественный ущерб в размерах, сопоставимых с особо крупным размером хищений, т. е. от одного миллиона рублей. Для обеспечения высокого уровня дифференциации ответственности за совершение преступления последствия в виде причинения вреда здоровью, жизни человека, а также иные тяжкие последствия необходимо рассматривать в качестве квалифицирующих обстоятельств по отношению к признакам основного состава преступления.

Сопоставление уголовной и административной ответственности в данной сфере выявило еще одно предложение по совершенствованию института ответственности за нарушение конфиденциальности персональных данных.

Во-первых, необходимо урегулировать вопрос об ужесточении ответственности субъектов отношений по сбору, обработке, хранению и распространению персональных данных. Согласно ст. 24 Федерального закона «О персональных данных» лица, виновные в нарушении требований данного Закона, несут предусмотренную законодательством Российской Федерации административную ответственность.

КоАП РФ устанавливает административную ответственность лиц за нарушение законодательства Российской Федерации в области персональных данных (ст. 13.11), за осуществление незаконной деятельности в области защиты информации (ст. 13.13), за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14).

Отметим, что размер административного штрафа за указанные административные правонарушения весьма мал. Так, обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации, влечет наложение административного штрафа на должностных лиц – от 10 тыс. до 20 тыс. руб., а на юридических лиц – от 15 тыс. до 75 тыс. руб. (ч. 2 ст. 13.11 КоАП РФ). Разглашение

информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от 500 до 1 тыс. руб.; на должностных лиц - от 4 тыс. до 5 тыс. руб. Очевидно, что размер такой ответственности не соответствует материальным (и не только) последствиям разглашения персональных данных и информации с ограниченным доступом. Размер ответственности за нарушение правил обработки персональных данных, установленных Директивой ЕС, во много раз превышает размер штрафа, предусмотренного КоАП РФ. С мая 2018 г. в Европе действуют новые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27.04.2016, GDPR - General Data Protection Regulation). Названный Регламент имеет прямое действие в 28 странах ЕС. С его принятием утратила силу Директива о защите персональных данных 95/46/ЕС от 24.10.1995. Важной особенностью GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных, а также усиление ответственности за нарушение правил обработки персональных данных: штрафы достигают 20 млн евро (около 1,5 млрд руб.).

Отсюда очевидна необходимость изменения российского законодательства в части значительного усиления ответственности за нарушения законодательства о персональных данных. Кроме того, расширение сфер применения современных технологий значительно изменяет степень общественной опасности правонарушений, совершаемых в этих областях. Особенно это относится к распространению информации в информационно-телекоммуникационной сети Интернет. Думается, что такое существенное усиление административной ответственности операторов за неисполнение обязанности по локализации баз с персональными данными послужит снижению уровня нарушений в сфере сбора и обработки персональных данных граждан. Кроме того, необходимо рассмотреть вопрос о введении уголовной ответственности за данное деяние. Полагаем необходимым усилить ответственность операторов и за нарушение правил, установленных ч. 1 и 2 ст. 13.11 КоАП РФ. Нуждается в соответствующем изменении также и ч. 6 ст. 13.11 КоАП, устанавливающая ответственность за невыполнение оператором при обработке персональных данных обязанности по обеспечению сохранности персональных данных при хранении материальных носителей персональных данных, недопущения несанкционированного к ним доступа (в том числе

уничтожения, изменения, копирования, распространения данных). В настоящее время ч. 6 ст. 13.11 КоАП РФ предусматривает наложение административного штрафа за неисполнение обязанности по обеспечению сохранности персональных данных на должностных лиц от 4 тыс. до 10 тыс. руб. Для юридических лиц максимальный размер штрафа составляет всего 50 тыс. руб. Несомненно, что такой мизерный размер штрафа не может препятствовать действиям по незаконному доступу к персональным данным, их копированию и распространению. С учетом того что основными обладателями персональных данных являются кредитные организации (банки, МФО), понятна необходимость существенного усиления ответственности операторов за нарушение законодательства о персональных данных.

Многие авторы сходятся во мнении о том, что за незаконные действия с персональными данными необходимо установить уголовную ответственность, но при этом предлагают различные варианты в части и вариантов квалификации указанных общественно опасных деяний по уже действующим уголовно-правовым нормам, и видов криминализируемых действий. Так, А.Ю. Волкова, ссылаясь на отдельные вступившие в законную силу приговоры, обосновывает необходимость квалификации незаконных действий с персональными данными граждан по ст. 137 или 272 УК РФ [4]. С.И. Гутник обосновал необходимость корректировки положений ст. 137 и 183 УК РФ, которые должны применяться в случае «распространения» сведений, которые являются персональными данными. Он указывает, что уголовная ответственность в таких случаях будет возможной, если лицо-правообладатель не давало разрешения на распространения своих персональных данных, а лицо-правонарушитель совершает запрещенные действующим законодательством действия с персональными данными. Аналогичные действия, по мнению автора, не образуют состава преступления, предусмотренного ст. 272 УК РФ [5]. А.А. Шутова приводит доводы о том, что при совершении незаконных действий с персональными (но не регистрационными) данными, которые включаются в объем банковской тайны, нарушаются три самостоятельных, но взаимосвязанных друг с другом объекта уголовно-правовой охраны: отношения собственности, отношения в сфере охраны компьютерной информации и информационно-экономические отношения. Исходя из этого, автор полагает, что совершение указанных выше действий образует идеальную совокупность преступлений, предусмотренных ст. 158, 183 и 272 УК РФ [6].

Стоит отметить, что первые два предложения могут относиться и к совершению преступле-

ний в отношении несовершеннолетних, однако предложения А.А. Шутовой уже к ним отнести затруднительно. Б.Н. Кадников полагает, что обеспечение прав и законных интересов граждан в части сохранности и правомерности пользования их персональными данными должно осуществляться в соответствии со специальной нормой Особенной части УК РФ. Общая уголовно-правовая норма (ст. 137 УК РФ) не охватывает перечисленные действия, а равно предусматривает чрезмерно мягкие меры ответственности в сравнении с общественной опасностью незаконных действий – нарушения правил обращения с персональными данными граждан. Поэтому в условиях обеспечения надлежащей охраны персональных данных граждан необходима более емкая дифференциация уголовной ответственности по увеличению степени строгости наказаний, предусмотренных ст. 137 УК РФ, а также введение специальной уголовно-правовой нормы об ответственности за нарушение правил обращения с персональными данными – конфиденциальной информацией. Но, указывая на необходимость введения специальной нормы, автор не предлагает ее содержания и точно не указывает место ее предполагаемого нахождения, исходя из родового объекта общественно опасного посягательства [7]. Аналогичной позиции придерживается Е.В. Хохлова. Не предлагая конкретного описания диспозиции и санкции специальной уголовно-правовой нормы, она предлагает аргументацию «социально-правового и криминологического» содержания в пользу введения такой нормы в отечественный уголовный закон. Общественная опасность деяний, связанных с нарушением правового режима использования персональных данных, обусловлена высокой ценностью нарушаемых прав и свобод – жизнь, личная/семейная тайна, честь, достоинство, собственность, а также особенностями современных отношений, в которых ключевую роль стала играть глобальная компьютеризированность, виртуализация [8]. И.Н. Мосечкин также указывает на необходимость установления специальной нормой уголовной ответственности за посягательства на персональные данные, которые выражаются в их незаконном получении, хранении, обработке, сбыте и использовании. Данные общественно опасные действия указывают на принципиально новое преступление, которое автор предлагает именовать «кражей личности», но не раскрывает юридических особенностей и предполагаемых признаков его состава [9].

Некоторые авторы небезосновательно полагают, что использование в нормах уголовного закона конструкции «похищение личности» нежелательно, т. к. в таком случае человек приравнивается к предмету гражданско-правовых отноше-

ний. Хищение и иные незаконные действия с персональными данными следует рассматривать в качестве преступления, ответственность за которое предусмотрено отдельной нормой из гл. 19 УК РФ. Авторы также предлагают рабочий вариант диспозиции этой уголовно-правовой нормы: «Незаконное получение цифровых идентификационных данных. Получение цифровых идентификационных данных путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом...». Правда, здесь же делается оговорка, что данное преступление следует квалифицировать по совокупности со статьями иных глав УК РФ в зависимости от посягательства на объект уголовно-правовой охраны. Кроме того, к данной уголовно-правовой норме необходимо по аналогии статьи 137 УК РФ также выделить квалифицирующий состав относительно незаконного получения цифровых идентификационных данных несовершеннолетних. Кроме того, предлагаемое решение нельзя считать окончательным, т. к. во всех случаях совершения преступления, предметом которых являются персональные данные, по мнению авторов, всегда будет требовать дополнительной квалификации и установления идеальной совокупности [10].

Проведенное исследование позволяет сформулировать следующие основные выводы и предложения.

1. Теоретическое значение разграничения биологической и социальной сущности человека. В условиях цифровизации и развития биотехнологий уголовное право должно четко определять, какая именно сущность человека — биологическая, социальная или информационная (техническая) — выступает объектом охраны в конкретной норме. Это необходимо для адекватной квалификации деяний и конструирования составов преступлений, отражающих специфику причиняемого вреда.

2. Классификация форм криминальной эксплуатации человека. Обосновано выделение трех форм эксплуатации: эксплуатация человека как личности (социальная сущность); эксплуатация анатомической структуры и физиологических свойств (биологическая сущность); эксплуатация биометрических персональных данных (информационная сущность). Последняя форма является новой и требует специального уголовно-правового регулирования.

3. Оценка изменений уголовного законодательства. Введение ст. 272.1 УК РФ является значительным шагом вперед в деле уголовно-правовой охраны персональных данных. Однако практика применения выявила определенные сложности, связанные с необходимостью доказывания

незаконности получения исходных данных и отграничения от административных правонарушений.

4. Значение сравнительно-правового анализа. Зарубежный опыт демонстрирует разнообразие подходов к защите персональных и биометрических данных. Российское законодательство должно развиваться с учетом лучших практик, сохраняя баланс между эффективностью уголовно-правовой охраны и соблюдением принципов гуманизма и справедливости. В конечном счете, речь идет о формировании целостной системы уголовно-правовой и криминологической безопасности человека как единства биологической, социальной и информационной сущности. Только такой комплексный подход способен обеспечить надежную защиту прав и свобод личности в условиях цифровой трансформации общества.

Список литературы:

- [1] Коваленко В.И. Криминальная эксплуатация человека: понятие, виды, проблемы правовой регламентации // Право и образование. 2014. № 2. С. 90-99.
- [2] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.
- [3] Официальный сайт Банка России. URL: <http://www.cbr.ru/> (дата обращения: 13.01.2026).
- [4] Волкова А. Ю. Персональные данные как объект уголовно-правовой охраны / А. Ю. Волкова // Уголовное право: стратегия развития в XXI веке. – 2023. № 3. С. 132-137.
- [5] Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. ... канд. юрид. наук / С. И. Гутник. – Красноярск, 2017. 241 с.
- [6] Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты : дис. ... канд. юрид. наук / А. А. Шутова. Н. Новгород, 2017. 264 с.
- [7] Кадников Б. Н. Уголовно-правовая охрана конституционного права граждан на неприкосновенность частной жизни : автореф. дис. ... канд. юрид. наук / Б. Н. Кадников. М., 2008. 27 с.
- [8] Хохлова Е.В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными / Е. В. Хохлова // Вестник Тверского государственного университета. Серия «Право». 2022. № 3. С. 141-148.
- [9] Мосечкин И. Н. Направления совершенствования уголовно-правовых средств обеспечения защиты персональных данных / И. Н. Мосечкин // Научные исследования в современном мире. Теория и практика. Сборник избранных статей Всероссийской (национальной) научно-практической конференции (Санкт-Петербург, 10 января 2022). – СПб.: ГНИИ «Нацразвитие». 2022. С. 200-202.
- [10] Зварыгин В. Е. Похищение «цифровой личности»: проблемы квалификации / В. Е. Зварыгин, А. М. Ахатова // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 148-157.

References:

- [1] Kovalenko V.I. Criminal exploitation of a person: concept, types, problems of legal regulation // Law and Education. 2014. No. 2. pp. 90-99.
- [2] Federal Law "On Personal Data" of July 27, 2006 N 152-FZ // Collected Legislation of the Russian Federation. 2006. No. 31 (Part 1). Art. 3451.
- [3] Official website of the Bank of Russia. URL: <http://www.cbr.ru/> (date of access: January 13, 2026).
- [4] Volkova A. Yu. Personal data as an object of criminal law protection / A. Yu. Volkova // Criminal Law: Development Strategy in the 21st Century. - 2023. No. 3. pp. 132-137.
- [5] Gutnik S. I. Criminal-legal characteristics of criminal attacks against personal data: diss. ... Cand. Sciences (Law) / S. I. Gutnik. - Krasnoyarsk, 2017. 241 p.
- [6] Shutova A. A. Criminal-legal counteraction to information crimes in the sphere of economic activity: theoretical and applied aspects: diss. ... Cand. Sciences (Law) / A. A. Shutova. N. Novgorod, 2017. 264 p.
- [7] Kadnikov B. N. Criminal-legal protection of the constitutional right of citizens to privacy: author's abstract. diss. ... Cand. Sciences (Law) / B. N. Kadnikov. Moscow, 2008. 27 p.
- [8] Khokhlova E.V. Social Determination of Criminal Liability for Crimes Related to Personal Data / E. V. Khokhlova // Bulletin of Tver State University. Series "Law". 2022. No. 3. pp. 141-148.
- [9] Mosechkin I. N. Directions for Improving Criminal-Law Means of Ensuring the Protection of Personal Data / I. N. Mosechkin // Scientific Research in the Modern World. Theory and Practice. Collection of Selected Articles of the All-Russian (National) Scientific and Practical Conference (St. Petersburg, January 10, 2022). - St. Petersburg: State Research Institute "NatSrazvitie". 2022. pp. 200-202.
- [10] Zvarygin V. E. Theft of a "Digital Identity": Problems of Qualification / V. E. Zvarygin, A. M. Akhatova // Criminal Law: Development Strategy in the 21st Century. 2023. No. 3. P. 148-157.

