Дата поступления рукописи в редакцию: 19.06.2026 г. DOI: 10.24412/2782-3830-2026-7-317-325
Дата принятия рукописи в печать: 13.07.2026 г.

КУЛЕШОВ Дмитрий Алексеевич,
аспирант, Федеральное Государственное Автономное Образовательное Учреждение Высшего Образования «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)», Кафедра информационного права и цифровых технологий, ORCID 0009-0003-7589-9751, SPIN-код 1405-4650, AuthorID 1119258, УДК 34.096, e-mail: dima.kuleshoff@gmail.com

УГРОЗА «HARVEST NOW, DECRYPT LATER» И ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ РАЗВИТИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Аннотация. *Цель настоящей статьи заключается в теоретической квалификации угрозы «harvest now, decrypt later» (HNDL) в качестве самостоятельного юридически значимого сценария угрозы с отложенной реализацией вредоносных последствий, в систематизации правовых пробелов российского регулирования, обусловленных данной угрозой, в правовом осмыслении технических категорий «горизонт криптоустойчивости» и «криптографическая адаптивность» в качестве самостоятельных правовых категорий российского законодательства, а также в формулировании предложений по совершенствованию законодательства о персональных данных, критической информационной инфраструктуре и информационной безопасности. В результате исследования установлено, что действующее российское законодательство содержит пять структурно различных пробелов применительно к угрозе HNDL: темпоральный, квалификационный, пробел моделирования угроз, стандартизационный и доктринально-политический. Сравнительно-правовой анализ показал, что европейская модель реагирования опирается на динамический стандарт технологической состоятельности мер защиты, американская — на прямые законодательные предписания и техническую стандартизацию NIST; российская система в части постквантовых угроз лишена сопоставимого нормативного содержания. Предложена системная модель устранения выявленных пробелов, основанная на категориях горизонта криптоустойчивости и криптографической адаптивности.*

Ключевые слова: *квантовые угрозы; персональные данные; постквантовая криптография; информационная безопасность; правовые пробелы; квантовый компьютер.*

KULESHOV Dmitrii Alekseevich,
PhD Student, Federal State Autonomous Educational Institution of Higher Education "Kutafin Moscow State Law University (MSAL)", Department of Information Law and Digital Technologies

THE «HARVEST NOW, DECRYPT LATER» THREAT AND LEGAL MECHANISMS FOR PERSONAL DATA PROTECTION IN THE ERA OF QUANTUM COMPUTING

Annotation. *This article aims to provide a theoretical legal qualification of the «harvest now, decrypt later» (HNDL) threat as an independent legally significant threat scenario involving the deferred manifestation of harmful consequences; to systematise the legal gaps in Russian regulation arising from this threat; to conceptualise the technical notions of the «cryptographic resilience horizon» and «cryptographic adaptability» as distinct legal categories of Russian law; and to formulate proposals for improving legislation on personal data, critical information infrastructure, and information security. The study establishes that current Russian legislation contains five structurally distinct gaps in relation to the HNDL threat: a temporal gap, a qualification gap, a threat-modelling gap, a standardisation gap, and a doctrinal-policy gap. The comparative legal analysis demonstrates that*

the European response model relies on a dynamic standard of technological adequacy of protective measures, whereas the American model is based on direct legislative mandates and NIST technical standardisation; by contrast, the Russian system lacks comparable normative content in relation to post-quantum threats. The article proposes a systemic model for eliminating the identified gaps based on the categories of the cryptographic resilience horizon and cryptographic adaptability.

Key words*: quantum threats; personal data; post-quantum cryptography; information security; legal gaps; quantum computer.*

Введение

Право традиционно реагирует на угрозы после реализации вреда. Угроза «harvest now, decrypt later» (далее — HNDL) разрушает эту логику. Злоумышленник перехватывает зашифрованные данные, не имея возможности их прочитать, и сохраняет их в расчёте на то, что квантовый компьютер в обозримой перспективе позволит вскрыть любой из существующих ассиметричных криптографических алгоритмов [Mosca, 2018: 38–39]. Квантовый компьютер принципиально отличается от обычного не мощностью, а природой вычислений, основанной на квантовых эффектах: он способен решать математические задачи, на вычислительной трудоёмкости которых десятилетиями строилась устойчивость криптографии [Mascelli, Rodden, 2025: 4–5].

В экспертном и регуляторном дискурсе используется термин Q-Day как обозначение момента утраты адекватности существующих криптографических стандартов [Scanlon, Zweifel-Keegan, 2026: 1].

HNDL характеризуется темпоральным разрывом между перехватом и причинением вреда. Материальные последствия проявляются спустя годы или десятилетия после первичного сбора данных [Abdikhakimov, 2026: 2]. И даже полноценный переход на постквантовую криптографию не устраняет ретроспективный риск, он защищает будущие коммуникации, но не данные, уже перехваченные сегодня.

Применительно к российскому праву возникают вопросы, на которые действующее законодательство не даёт ответа. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (далее - 152-ФЗ) использует категорию необходимых и достаточных мер защиты информации, не определяя временной горизонт их достаточности. Возникает вопрос об обязанности операторов учитывать предсказуемые технологические изменения при выборе криптографических средств и о квалификации перехвата зашифрованных данных как самостоятельного нарушения при последующей расшифровке.

Актуальность исследования обусловлена развитием квантовых вычислений [Aggarwal K. et al., 2024: 627-629], институционализацией постквантового перехода в ЕС и США [Scanlon, Zweifel-Keegan, 2026: 3], а также отсутствием в российском законодательстве механизмов учёта HNDL при оценке достаточности мер защиты персональных данных.

Цель статьи состоит в квалификации HNDL как угрозы с отложенной реализацией последствий, выявлении пробелов российского регулирования и предложении модели их устранения.

Методологическую основу составляют формально-юридический анализ законодательства о персональных данных, сравнительно-правовой анализ зарубежных регуляторных решений в сфере постквантовой криптографии и междисциплинарное сопоставление правовых положений с данными технической литературы о квантовой архитектуре и криптографической уязвимости.

Техническая природа угрозы HNDL: правовое значение

Современная инфраструктура защищённой передачи данных основана на сочетании асимметрической и симметрической криптографии: первая преимущественно используется для установления ключей, аутентификации и электронной подписи, вторая для шифрования основного объёма передаваемых данных. Её надёжность связана с особенностями ряда математических задач, решение которых требует значительных вычислительных ресурсов и времени даже при использовании высокопроизводительных систем. Указанная вычислительная сложность выступает гарантией защиты.

Однако, алгоритм П. Шора показал, что при наличии квантового компьютера указанные задачи решаются за несопоставимо малое время [Shor, 1997: 1484]. Это подтверждают и официальные материалы Министерства обороны США, где отмечается способность квантового компьютера компрометировать широко применяемые алгоритмы шифрования, используемые для установления соединений и создания цифровых подписей [18].

HNDL изменяет временную структуру угрозы: технологическая предпосылка нарушения формируется в момент передачи данных, а последствия проявляются позднее.

Для правового анализа существенны три свойства HNDL. Во-первых, при HNDL на момент перехвата данные остаются математически защи-

щёнными, однако их криптографическая устойчивость ограничена во времени [Mascelli, Rodden, 2025: 16].

Во-вторых, невидимость для оператора. HNDL не предполагает активного вмешательства в систему. Перехват трафика возможен без изменения функционирования инфраструктуры, вследствие чего оператор не имеет технической возможности обнаружить такой перехват. Недетектируемость осложняет оценку предсказуемости риска и ставит вопрос о стандарте должной осмотрительности при отсутствии фиксируемых индикаторов.

В-третьих, вероятностный характер будущего вреда. Точный момент появления квантового компьютера нужной мощности неизвестен [19]. Однако угроза основана на устойчивом научном прогрессе и государственных программах разработки [European Commission, 2022: 3, 23]. Для права это означает следующее: если оператор хранит данные, которые должны оставаться конфиденциальными в течение 20–30 лет, он не может игнорировать эту угрозу, ссылаясь лишь на то, что квантовый компьютер ещё не создан. Критерий достаточности мер защиты не может быть привязан исключительно к сегодняшнему состоянию технологий.

Правовая оценка угрозы HNDL в российском праве должна опираться на конструкцию публично-правовой обязанности оператора по обеспечению безопасности персональных данных. В соответствии со статьёй 19 Федерального закона № 152-ФЗ «О персональных данных» (далее - 152-ФЗ) оператор принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения. Поскольку при HNDL на момент перехвата содержание данных не раскрывается, возникает расхождение между техническим фактом копирования зашифрованного массива и юридической конструкцией доступа, ориентированной на ознакомление с содержанием персональных данных.

Обязанность оператора конкретизируется в Постановлении Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», которое предусматривает обеспечение безопасности посредством нейтрализации актуальных угроз. Под актуальными угрозами понимается совокупность условий и факторов, создающих опасность несанкционированного доступа и иных неправомерных действий (пункт 6).

Тип угроз и уровень защищённости определяются с учётом оценки возможного вреда (пункты 7–10). Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ред. от 14.05.2020) устанавливает состав организационных и технических мер защиты и связывает их с результатами идентификации актуальных угроз.

Российская модель защиты персональных данных ориентирована на нейтрализацию актуальных угроз и формальное соответствие установленным требованиям. Поэтому использование допустимых и сертифицированных средств защиты, даже при их потенциальной будущей уязвимости, не образует самостоятельного нарушения без предварительного нормативного закрепления обязанности учитывать долгосрочный горизонт криптостойкости.

Право Европейского союза формирует иную конструкцию реагирования на постквантовые риски, чем российская система. Различие заключается в разграничении моделей, ориентированных на формализованные угрозы, и моделей, основанных на оценке вероятности и тяжести будущих рисков [Backman, 2023: 90]. И если российское регулирование обеспечения информационной безопасности преимущественно выстроено по первой логике [Терещенко, 2018: 149], то европейское регулирование следует второй модели, опираясь на изменяемый стандарт мер защиты, встроенный в нормы о защите данных и кибербезопасности.

Регламент (ЕС) 2016/679 (GDPR) закрепляет в статьях 25 и 32 обязанность применять технические и организационные меры с учетом состояния технологий.

Особое значение имеет пункт 26 преамбулы GDPR, предусматривающий учет всех средств, которые могут быть разумно использованы с учетом технологического развития при оценке идентифицируемости. Тем самым временной фактор включается в сам механизм правовой оценки. Потенциальная возможность раскрытия сведений в будущем не выводится за пределы анализа лишь потому, что соответствующие вычислительные мощности еще не получили широкого распространения.

В научной литературе высказывается позиция, согласно которой постквантовые алгоритмы должны рассматриваться как часть развивающегося стандарта должной осмотрительности в сфере защиты данных [Bruno, Spano, 2021: 7]. Из такой интерпретации следует, что применение криптографии, уязвимой к прогнозируемым квантовым атакам, способно быть квалифицировано как несоответствие требованию state of the art в отношении сведений с длительным сроком конфиденциальности.

Директива (ЕС) 2022/2555 закрепляет обязательность мер управления киберрисками для широкого круга субъектов. Конструкция директивы опирается на оценку как актуальных, так и потенциальных угроз. Органы управления субъектов обязаны утверждать меры управления киберрисками и контролировать их исполнение, а государства-члены должны предусмотреть возможность привлечения руководства к ответственности за нарушение соответствующих обязанностей.

Хотя текст директивы прямо не упоминает квантовые сценарии, стратегия HNDL укладывается в категорию предсказуемого технологического риска. Следовательно, ее учет возможен в рамках существующих требований к управлению киберрисками без специальной поправки к директиве.

Переход к институциональному признанию проявился в дорожной карте подготовленной Рабочей группой ЕС по постквантовой криптографии в рамках Группы сотрудничества NIS и опубликованной Европейской комиссией в 2025 году. В документе прямо обозначена проблема ретроспективной дешифровки и установлен ориентир завершения миграции на постквантовую криптографию к 2035 году [EU PQC Workstream, 2025: 2–3, 7].

Европейская модель характеризуется изменяемым стандартом технологической состоятельности мер защиты, институционализированным управлением киберрисками и программным планированием перехода к постквантовой криптографии. В отличие от российской системы, где временная проекция обязанности по обеспечению безопасности прямо не закреплена, право Европейского союза уже содержит нормативные механизмы, позволяющие оценивать бездействие по модернизации криптографической защиты как возможное несоответствие требованиям state of the art и риск-ориентированного управления безопасностью.

Американская система выстроена иначе, чем европейская. Переход к постквантовой криптографии закреплен не через интерпретацию общих принципов, а посредством прямых предписаний федерального уровня.

Федеральный закон H.R. 7535 Quantum Computing Cybersecurity Preparedness Act (Pub. L. 117-260) и последующие федеральные управленческие документы закрепили обязанность агентств провести инвентаризацию криптографических зависимостей [20], выделить данные с длительным сроком конфиденциальности и подготовить планы перехода на алгоритмы, утверждённые NIST [21]. В 2024 году NIST утвердил стандарты FIPS 203, 204 и 205, определившие техническое содержание постквантового перехода. Американская модель тем самым образует трёхуровневую конструкцию: законодательное предписание Конгресса, управленческую координацию исполнительной власти и техническую стандартизацию NIST.

Распространение данной модели на частный сектор осуществляется преимущественно опосредованно через требования к подрядчикам, условия федеральных контрактов и стандарты. В результате квантовый риск получает в федеральном секторе статус фактора, требующего обязательной организационной и технической подготовки.

Сопоставление ЕС и США позволяет выделить две модели превентивного учёта постквантовых рисков: динамическую, основанную на стандарте state of the art, и директивно-стандартизационную, основанную на прямом предписании и стандартах NIST.

Таблица 1. Сравнительная характеристика правовых режимов постквантовой защиты данных

Критерий	Российская Федерация	Европейский союз	США
Нормативное упоминание постквантовой криптографии	Отсутствует в 152-ФЗ и 187-ФЗ	Прямого упоминания в GDPR нет; выводится из «state of the art» (ст. 25, 32 GDPR); признана в EU PQC Roadmap	Прямое признание в Quantum Computing Cybersecurity Preparedness Act
Правовая модель оценки технологического риска	Реактивная; ориентирована на актуальные угрозы (БДУ ФСТЭК)	Динамическая; учитывает технологическое развитие (Recital 26 GDPR); риск-ориентированная модель NIS2	Программно-превентивная; стратегическое признание HNDL (NSM-10)

Обязанность перехода к PQC	Не установлена	Прямой обязанности нет; может выводиться из «state of the art» и risk management	Установлена для федеральных агентств (Pub. L. 117-260)
Техническая стандартизация	Отсутствует	Рекомендации ENISA; EU PQC Roadmap; требования CRA к обновляемости и безопасности продуктов, косвенно поддерживающие криптографическую адаптивность.	Обязательные стандарты NIST FIPS 203/204/205
Юридическое признание угрозы HNDL	Не закреплено	Признана на уровне институтов ЕС (Roadmap)	Прямо отражена в стратегических документах (NSM-10)
Ответственность за бездействие	Специально не предусмотрена применительно к квантовому риску	Общая санкция ст. 83 GDPR (до 4% мирового оборота) потенциально применима при квалификации надзорным органом применяемой криптографии как несоответствующей критерию «state of the art»; специальной санкции за непереход на ПКК не установлено	Контроль исполнения предписаний Pub. L. 117-260 и OMB M-23-02; специальная санкция за непереход законом прямо не установлена

Систематизация правовых пробелов и модель их устранения

В юридической науке пробел понимается как отсутствие нормативного предписания, необходимого для регулирования общественных отношений, объективно требующих правовой регламентации [Горбачева, 2022: 39–40]. В сфере информационной безопасности возникновение таких пробелов обусловлено асимметрией темпов технологического развития и закрепления механизмов реагирования [Семенов, 2022: 94–95]. Исходя из этого, анализ российского регулирования позволяет выделить пять взаимосвязанных пробелов: темпоральный, квалификационный, пробел моделирования угроз, стандартизационный и доктринально-политический.

Темпоральный пробел состоит в том, что статья 19 152-ФЗ и подзаконные акты ФСТЭК не требуют учитывать срок необходимой конфиденциальности данных и риск будущей утраты криптографической стойкости. Надлежащая защита оценивается через соответствие текущим требованиям, а не через способность применяемых средств сохранять конфиденциальность информации в долгосрочной перспективе [Орлова, 2025: 495].

Для устранения данного дефекта целесообразно закрепить две взаимосвязанные категории: «горизонт криптоустойчивости» и «криптографическая адаптивность». Близкие технические понятия уже используются в зарубежной регуляторной и технической практике: cryptographic agility обозначает способность системы к замене криптографических примитивов, а data security lifetime — период, в течение которого сведения сохраняют конфиденциальную ценность. Однако эти категории обычно остаются в технико-организационной плоскости и сами по себе не формируют юридически значимых обязанностей, критериев надзорной оценки и последствий несоответствия. Предлагаемые понятия отличаются именно правовой природой: они должны выступать нормативными критериями достаточности мер защиты.

Под горизонтом криптоустойчивости следует понимать период, в течение которого применяемые средства криптографической защиты обязаны обеспечивать конфиденциальность обрабатываемых сведений с учётом прогнозируемой динамики вычислительных возможностей. Криптографическая адаптивность, в свою очередь, означает свойство информационной системы, позволяющее заменить криптографические алгоритмы и средства защиты без изменения функциональной архитектуры прикладного программного обеспечения.

Эти категории целесообразно закрепить в статье 3 152-ФЗ, а статью 19 дополнить обязанностью оценивать соответствие применяемых средств защиты горизонту криптоустойчивости и обеспечивать криптографическую адаптивность систем, обрабатывающих данные с длительным сроком необходимой конфиденциальности. Детализация порядка оценки, требований к адаптив-

ности и сроков постквантового перехода должна быть отнесена к компетенции Правительства Российской Федерации по представлению ФСБ России и ФСТЭК России.

Квалификационный пробел заключается в отсутствии в российском праве механизмов правовой оценки использования криптографических средств, которые формально соответствуют установленным требованиям, но объективно утрачивают устойчивость в среднесрочной технологической перспективе. Проблема в том, что контроль в сфере защиты персональных данных ориентирован преимущественно на проверку соблюдения установленных требований, а не на оценку фактической устойчивости применяемых технических решений [Полякова, Камалова, 2022: 115–116]. Оператор считается исполнившим возложенные на него обязанности, если применяет допустимые и сертифицированные средства защиты. При этом привлечение к ответственности возможно лишь после предварительного нормативного закрепления соответствующей обязанности, что вытекает из принципа правовой определённости [Савельев, 2015: 55–58].

Устранение данного пробела требует поэтапной модели регулирования. На первом этапе на уровне подзаконного акта следует закрепить обязанность оператора при формировании модели угроз и технического задания определять горизонт криптоустойчивости обрабатываемых сведений, сопоставлять его с характеристиками применяемых алгоритмов и проводить инвентаризацию криптографических зависимостей системы. На втором этапе статью 23 Закона № 152-ФЗ можно дополнить положением, позволяющим Роскомнадзору учитывать при осуществлении контроля заключения ФСБ России и ФСТЭК России о соответствии применяемых средств защиты установленному горизонту криптоустойчивости. Такая конструкция позволит сформировать контрольный механизм без немедленного ужесточения ответственности и чрезмерного регуляторного давления.

Пробел моделирования угроз выражается в отсутствии HNDL в Банке данных угроз безопасности информации ФСТЭК России как самостоятельного сценария. Отсутствие данной угроз не исключает её самостоятельного выявления оператором, однако лишает данный сценарий формализованного статуса и единообразного методического отражения, что затрудняет его систематический учёт при разработке моделей угроз.

Для устранения пробела Банк данных угроз ФСТЭК следует дополнить позицией, описывающей риск перехвата зашифрованных сведений с расчётом на их последующую расшифровку при появлении достаточных квантовых вычислительных ресурсов. Одновременно Методика оценки угроз безопасности информации должна быть дополнена разделом об угрозах с отложенной реализацией, предусматривающим инвентаризацию криптографических зависимостей, классификацию сведений по сроку необходимой конфиденциальности и проверку соответствия применяемых алгоритмов установленному горизонту криптоустойчивости. Такие изменения не расширяют контрольные полномочия ФСТЭК, а корректируют исходную модель угроз с учётом современного уровня технологического развития.

Стандартизационный пробел состоит в отсутствии нормативно оформленного механизма перехода к постквантовой криптографии. Действующая система обязательных требований опирается на признанные средства защиты и формально закреплённые перечни мер, однако не содержит критериев криптографической адаптивности, требований к плановой миграции алгоритмов и сроков завершения постквантовой стандартизации. В связи с этим целесообразно установить предельный срок разработки национального стандарта постквантовых алгоритмов в рамках деятельности ТК26, например не позднее 2027 года. Требования к криптографической адаптивности информационных систем целесообразно закрепить в документах ФСТЭК России, регулирующих моделирование угроз и архитектуру защиты, а требования к замене и применению средств криптографической защиты следует закрепить в документах ФСБ России.

Особое значение постквантовая миграция имеет для объектов критической информационной инфраструктуры первой и второй категорий. Для таких объектов целесообразно ввести обязанность разработки дорожной карты криптографической миграции, содержащей перечень уязвимых компонентов системы, сроки их замены и порядок перехода на устойчивые к квантовым атакам средства защиты. Данный инструмент позволит обеспечить управляемый переход без немедленного введения запретительных мер и соответствует зарубежной практике поэтапной постквантовой миграции.

Доктринально-политический пробел выражается в отсутствии квантовых угроз в стратегических документах информационной безопасности. Его устранение требует не декларативного упоминания HNDL, а закрепления долгосрочной криптографической устойчивости государственных информационных систем и объектов критической инфраструктуры как стратегической цели, а также создания межведомственного механизма постквантовой миграции с участием ФСБ России, ФСТЭК России, Минцифры России, Росатома как ответственной организации по направлению квантовых вычислений и ОАО «РЖД» как ответственной организации по направлению кванто-

вых коммуникаций. Без определения ответственного центра координации постквантовый переход сохранит фрагментарный характер, что особенно существенно с учётом отмечаемой в научной литературе разнородности источников регулирования информационной безопасности [Яковлева, 2021: 74–75].

Выводы.

1. Угроза HNDL представляет собой самостоятельный юридически значимый сценарий, при котором неправомерное копирование зашифрованных данных и окончательная реализация вреда в форме раскрытия их содержания разделены продолжительным временным интервалом.
2. Российское регулирование не содержит целостного механизма учёта HNDL: отсутствуют обязанность учитывать срок необходимой конфиденциальности, критерии оценки алгоритмов с ограниченным горизонтом устойчивости, формализация HNDL в БДУ ФСТЭК, нормативный ориентир постквантовой стандартизации и доктринальное закрепление квантовых рисков.
3. Сравнительное исследование демонстрирует различие двух зарубежных моделей реагирования на постквантовые риски. Европейский режим опирается на изменяемый стандарт технологической состоятельности мер защиты. Американская система использует механизм, основанный на прямых предписаниях федерального уровня и централизованной технической стандартизации. Российская модель ближе к американской, но пока не содержит сопоставимого нормативного наполнения.
4. Категории горизонта криптоустойчивости и криптографической адаптивности позволяют перевести технические параметры постквантового перехода в юридические критерии мер защиты и выступают нормативным содержанием принципа гибридной квантово-безопасной миграции в публично-правовом регулировании квантовых коммуникаций.
5. Устранение выявленных пробелов требует поэтапного сочетания законодательных изменений, обновления методических документов ФСТЭК и ФСБ, завершения постквантовой стандартизации и включения квантовых рисков в стратегическое планирование информационной безопасности.

Список литературы:

[1] Абдихакимов И. Проблема стратегии «перехватить сейчас — расшифровать позже» (HNDL) для международно-правового режима ответственности государств в квантовую эпоху // Elita Law Journal. 2026. № 1 (4). С. 1–12.

[2] Аггарвал К. и др. Квантовые вычисления: навигация по будущему вычислений, вызовы и технологические прорывы // Quantum Reports. 2024. Т. 6. № 4. С. 627–663. DOI: 10.3390/quantum6040039.

[3] Бакман С. Риск-ориентированная и угрозо-ориентированная кибербезопасность: пример ЕС // Европейская безопасность. 2023. Т. 32. № 1. С. 85–103. DOI: 10.1080/09662839.2022.2069464.

[4] Бруно Л., Спано И. Постквантовое шифрование и регулирование приватности: успевает ли закон за технологиями? [Электронный ресурс] // European Journal of Privacy Law & Technologies. 2021. № 1. URL: https://ssrn.com/abstract=3920272 (дата обращения: 05.03.2026).

[5] Горбачева С. В. Теоретические аспекты понятия законодательных пробелов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 39–46. DOI: 10.36511/2078-5356-2022-4-39-46.

[6] Европейская комиссия. Флагманская программа Европейского союза в области квантовых технологий: основные достижения в 2018–2021 гг. [Электронный ресурс]. Брюссель: Европейская комиссия, 2022. 36 с. URL: https://digital-strategy.ec.europa.eu/en/library/eus-quantum-technologies-flagship (дата обращения: 15.04.2026).

[7] Маскелли Дж., Родден М. «Собери сейчас — расшифруй потом»: анализ постквантовой криптографии и рисков конфиденциальности данных для сетей распределенных реестров // Finance and Economics Discussion Series. 2025. № 2025-093. Вашингтон: Совет управляющих Федеральной резервной системы, 2025. URL: https://doi.org/10.17016/FEDS.2025.093 (дата обращения: 05.03.2026).

[8] Моска М. Кибербезопасность в эпоху квантовых компьютеров: будем ли мы готовы? // IEEE Security & Privacy. 2018. № 5. С. 38–41.

[9] Орлова К. С. Практика применения законодательства о персональных данных в Российской Федерации: анализ организационных практик, нарушений и правоприменительной деятельности // Вестник науки. 2025. Т. 1. № 12 (93). С. 490–499.

[10] Полякова Т. А., Камалова Г. Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2. С. 112–121. DOI: 10.33184/pravgos-2022.2.12.

[11] Рабочая группа ЕС по постквантовой криптографии. Согласованная дорожная карта перехода к постквантовой криптографии. Часть

1. Версия 1.1 [Электронный ресурс]. Группа сотрудничества NIS, 2025. 17 с. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (дата обращения: 15.06.2026).

[12] Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

[13] Семенов Е. Ю. Совершенствование правовых и организационных аспектов защиты персональных данных в Российской Федерации // Закон и право. 2022. № 1. С. 94–96. DOI: 10.24412/2073-3313-2022-1-94-96.

[14] Сканлон И., Цвайфель-Киган К. Квантовый контекст: право в сфере кибербезопасности после Q-Day [Электронный ресурс] // IAPP. 29 янв. 2026. URL: https://iapp.org/news/a/a-quantum-of-context-cybersecurity-law-after-q-day (дата обращения: 05.03.2026).

[15] Терещенко Л. К. Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161. DOI: 10.17323/2072-8166.2018.4.142.161.

[16] Шор П. Полиномиальные алгоритмы для факторизации целых чисел и вычисления дискретных логарифмов на квантовом компьютере // SIAM Journal on Computing. 1997. Т. 26. № 5. С. 1484–1509.

[17] Яковлева А. В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. Т. 11. № 4. С. 70–81. DOI: 10.33693/2223-0092-2021-11-4-70-81.

[18] United States Department of Defense (2021) Quantum computing and quantum information science: Frequently asked questions. Washington, DC: U.S. Department of Defense. Available at: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (Accessed: 11 March 2026)

[19] United States Department of Defense (2021) Quantum computing and quantum information science: Frequently asked questions. Washington, DC: U.S. Department of Defense. Available at: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (Accessed: 11 March 2026)

[20] Presman, D. (2024) The U.S. Government's Transition to Post-Quantum Cryptography (PQC). Presentation at the 5th PQC Standardization Conference, 10 April 2024. National Institute of Standards and Technology (NIST). Available at: https://csrc.nist.gov/csrc/media/Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf (Accessed: 11 March 2026).

[21] Moody, D. et al. (2024) Transition to Post-Quantum Cryptography Standards. NIST IR 8547. National Institute of Standards and Technology, pp. 20–22. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf (Accessed: 11 March 2026).

References:

[1] Abdikhakimov I. The problem of the "intercept now - decipher later" (HNDL) strategy for the international legal regime of state responsibility in the quantum era//Elita Law Journal. 2026. № 1 (4). S. 1-12.

[2] Aggarwal K, et al. Quantum Computing: Navigating the Future of Computing, Challenges and Technological Breakthroughs//Quantum Reports. 2024. T. 6. № 4. S. 627-663. DOI: 10.3390/quantum6040039.

[3] Buckman S. Risk-oriented and threat-oriented cybersecurity: an example of the EU//European security. 2023. T. 32. № 1. S. 85-103. DOI: 10.1080/09662839.2022.2069464.

[4] Bruno L, Spano I. Post-quantum encryption and privacy regulation: Is the law keeping pace with technology? [Электронный ресурс] // European Journal of Privacy Law & Technologies. 2021. № 1. URL: https://ssrn.com/abstract=3920272 (access date: 05.03.2026).

[5] Gorbacheva S.V. Theoretical aspects of the concept of legislative gaps//Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2022. № 4 (60). S. 39-46. DOI: 10.36511/2078-5356-2022-4-39-46.

[6] European Commission. European Union flagship quantum technology programme: Major achievements in 2018-2021 [Electronic resource]. Brussels: European Commission, 2022. 36 c. URL: https://digital-strategy.ec.europa.eu/en/library/eus-quantum-technologies-flagship (дата обращения: 15.04.2026).

[7] Maschelli J, Rodden M. "Collect Now - Decipher Later": An Analysis of Post-Quantum Cryptography and Data Privacy Risks for Distributed Ledger Networks//Finance and Economics Discussion Series. 2025. № 2025-093. Washington: Federal Reserve Board of Governors, 2025. URL: https://doi.org/10.17016/FEDS.2025.093 (access date: 05.03.2026).

[8] Mosca M. Cybersecurity in the Age of Quantum Computers: Will We Be Ready ?//IEEE Security & Privacy. 2018. № 5. S. 38-41.

[9] Orlova K. S. Practice of applying legislation on personal data in the Russian Federation: analysis of organizational practices, violations and law enforcement activities//Bulletin of Science. 2025. VOL. 1. № 12 (93). S. 490-499.

[10] Polyakova T. A., Kamalova G. G. New vectors for the development of the system of legal sup-

port of information security as one of the priorities of national security (on the 30th anniversary of the adoption of the Law of the Russian Federation “On Security”)//The rule of law: theory and practice. 2022. № 2. S. 112-121. DOI: 10.33184/pravgos-2022.2.12.

[11] EU Working Party on Post-Quantum Cryptography. Agreed roadmap for the transition to post-quantum cryptography. Part 1. Version 1.1 [Electronic Resource]. NIS Collaboration Group, 2025. 17 c. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (дата обращения: 15.06.2026).

[12] Savelyev A. I. Problems of the application of legislation on personal data in the era of “Big Data “//Law. Journal of the Higher School of Economics. 2015. № 1. S. 43-66.

[13] Semenov E. Yu. Improvement of legal and organizational aspects of personal data protection in the Russian Federation//Law and Law. 2022. № 1. S. 94-96. DOI: 10.24412/2073-3313-2022-1-94-96.

[14] Scanlon I, Zweifel-Keegan K. Quantum context: cybersecurity law after Q-Day [Electronic Resource]//IAPP. 29 Jan 2026. URL: https://iapp.org/
news/a/a-quantum-of-context-cybersecurity-law-after-q-day (дата обращения: 05.03.2026).

[15] Tereshchenko L.K. State control in the field of personal data protection//Law. Journal of the Higher School of Economics. 2018. № 4. S. 142-161. DOI: 10.17323/2072-8166.2018.4.142.161.

[16] Shore P. Polynomial algorithms for integer factorization and computing discrete logarithms on a quantum computer//SIAM Journal on Computing. 1997. T. 26. № 5. S. 1484-1509.

[17] Yakovleva A. V. Cybersecurity and its legal regulation (foreign and Russian experience)// Socio-political sciences. 2021. T. 11. № 4. S. 70-81. DOI: 10.33693/2223-0092-2021-11-4-70-81.

[18] United States Department of Defense (2021) Quantum computing and quantum information science: Frequently asked questions. Washington, DC: U.S. Department of Defense. Available at: https://media.defense.gov/2021/
Aug/04/2002821837/-1/-1/1/Quantum_
FAQs_20210804.PDF (Accessed: 11 March 2026)

[19] United States Department of Defense (2021) Quantum computing and quantum information science: Frequently asked questions. Washington, DC: U.S. Department of Defense. Available at: https://media.defense.gov/2021/
Aug/04/2002821837/-1/-1/1/Quantum_
FAQs_20210804.PDF (Accessed: 11 March 2026)

[20] Presman, D. (2024) The U.S. Government’s Transition to Post-Quantum Cryptography (PQC). Presentation at the 5th PQC Standardization Conference, 10 April 2024. National Institute of Standards and Technology (NIST). Available at: https://csrc.nist.gov/csrc/media/
Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf (Accessed: 11 March 2026).

[21] Moody, D. et al. (2024) Transition to Post-Quantum Cryptography Standards. NIST IR 8547. National Institute of Standards and Technology, pp. 20–22. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
(Accessed: 11 March 2026).



www.law-books.ru

Юридическое издательство **«ЮРКОМПАНИ»** издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.