Дата поступления рукописи в редакцию: 10.10.2026 г. DOI: 10.24412/2782-3830-2026-11-34-42
Дата принятия рукописи в печать: 12.11.2026 г.

ТРОФИМОВ Максим Сергеевич,
кандидат юридических наук, доцент, доцент кафедры административного и финансового права Федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет», ORCID 0000-0001-8584-6563, e-mail: sim-pai@mail.ru,

ПИСКОВАТСКИЙ Данил Александрович,
ассистент кафедры уголовного права и процесса Федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет», ORCID 0009-0007-4313-2264, e-mail: mr.piskovatskia@mail.ru

УГОЛОВНО-ПРАВОВАЯ ПОЛИТИКА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ: ДОКТРИНАЛЬНЫЙ ПОДХОД

Аннотация. *Цифровизация общественных отношений превратила информационное пространство в новую арену геополитического противостояния, вынуждая государства переопределять границы своего суверенитета. В статье рассматриваются доктринальные основы уголовно-правовой политики России как инструмента обеспечения информационного суверенитета. Цель исследования — проанализировать, как концептуальные установки государства преломляются в конкретных нормах уголовного закона, формируя правовую основу цифрового суверенитета. Результаты показывают, что уголовно-правовая политика России в этой области прошла качественную трансформацию: от фрагментарного регулирования компьютерных преступлений конца XX в. к формированию целостной стратегической доктрины защиты государственного суверенитета в информационной сфере. Вместе с тем реализация этой политики сталкивается с системным кризисом правоприменения, обусловленным отсутствием рыночного эквивалента цифровых данных и субъективностью оценки «крупного ущерба». Сравнительный анализ китайского, американского и европейского подходов к цифровому суверенитету показывает, что Россия движется в русле глобального тренда на суверенизацию информационного пространства, сохраняя при этом гибридную модель, сочетающую открытость с защитой критических национальных интересов. Авторы приходят к выводу, что современная уголовно-правовая политика выступает не просто как совокупность запретов, а как сложный инструмент геополитического и государственного управления, где уголовное право служит финальным аргументом государства в борьбе за контроль над своим информационным пространством.*

Исследование выполнено за счет гранта Российского научного фонда № 25-28-01643 «Информационный суверенитет (суверенитет в информационной сфере): российский и зарубежный опыт правового регулирования и обеспечения», https://rscf.ru/project/25-28-01643/

Ключевые слова: *информационный суверенитет, уголовно-правовая политика, цифровизация, киберугрозы, доктринальный анализ, публичный интерес, экстерриториальность, сравнительно-правовое исследование.*

Для цитирования: *Трофимов М. С., Писковатский Д. А. Уголовно-правовая политика как инструмент обеспечения информационного суверенитета Российской Федерации: доктринальный подход // Российский научный вестник. 2026. № 11. С. 34–42.*

TROFIMOV Maksim Sergeevich,
Candidate of Law, Associate Professor, associate Professor, Department of administrative and financial law North Caucasus Federal University (Stavropol)

PISKOVATSKII Danil Alexandrovich,
Assistant of the Department of Criminal Law and Procedure
North Caucasus Federal University (Stavropol)

CRIMINAL LAW POLICY AS A TOOL FOR ENSURING THE INFORMATION SOVEREIGNTY OF THE RUSSIAN FEDERATION: DOCTRINAL APPROACH

Annotation. *Digitalization of social relations has turned the information space into a new arena of geopolitical confrontation, forcing states to redefine the boundaries of their sovereignty. The article examines the doctrinal foundations of Russia's criminal law policy as an instrument for ensuring information sovereignty. The purpose of the study is to analyze how the state's conceptual guidelines are refracted in specific norms of criminal law, forming the legal basis of digital sovereignty. The results show that Russia's criminal law policy in this area has undergone a qualitative transformation: from fragmented regulation of computer crimes in the late 20th century to the formation of an integral strategic doctrine for protecting state sovereignty in the information sphere. At the same time, the implementation of this policy faces a systemic crisis of law enforcement, caused by the absence of a market equivalent for digital data and the subjectivity of assessing "major damage." A comparative analysis of the Chinese, American, and European approaches to digital sovereignty shows that Russia is moving in line with the global trend toward the sovereignization of the information space, while preserving a hybrid model that combines openness with the protection of critical national interests. The authors conclude that contemporary criminal law policy acts not merely as a set of prohibitions but as a complex instrument of geopolitical and state governance, where criminal law serves as the state's final argument in the struggle for control over its information space.*

Key words: *information sovereignty, cybercrime, computer crimes, information and telecommunications networks, Chapter 28 of the Criminal Code of the Russian Federation.*

For citation: *Trofimov M. S., Piskovatskii D. A. Criminal law policy as a tool for ensuring the information sovereignty of the Russian Federation: doctrinal approach. Russian scientific bulletin. 2026;(11):34–42. (In Russ.).*

The research was carried out at the expense of a grant Russian Science Foundation № 25-28-01643 «Information sovereignty (sovereignty in the information sphere): Russian and foreign experience in legal regulation and support», https://rscf.ru/en/project/25-28-01643/

В отличие от классической уголовно-правовой доктрины, сфокусированной на охране конкретных общественных отношений (жизнь, собственность и т.д.), информационная доктрина оперирует категориями нематериального характера: данными, алгоритмами, трафиком и т.д., формирование этих основ происходит на стыке теории национальной безопасности, международного публичного права и науки уголовного права.

Концептуальный уровень доктрины уголовно-правовой политики в информационной сфере базируется на переосмыслении классического понятия государственного суверенитета применительно к цифровой реальности. Если традиционный Вестфальский суверенитет защищал территорию, население и аппарат управления от внешнего военного или дипломатического вмешательства, то информационный суверенитет защищает цифровую проекцию государства. [10, с.18] На этом уровне уголовное право выступает не просто как карательный инструмент, а как средство разграничения границ национального цифрового пространства.

В классической теории права граница – это линия на карте, государственная граница выступает особым объектом, требующим специального правового режима, который включает правила пересечения границы, режим приграничных территорий и порядок их использования, так это понятие раскрывает Р.М. Самигуллин, но в информационную эпоху концептуально признается существование «невидимой границы» проходящая через цифровые просторы. [12, с.98] Например, точки обмена трафиком и сервера DNS (доменная система имен) рассматриваются как стратегические объекты, контроль над которыми эквивалентен контролю над таможенными переходами, уголовная политика направлена на защиту этих узлов от перехвата управления извне, отсюда был принят Федеральный закон № 90-ФЗ от 1 мая 2019 г., который в народе получил название «Закон о суверенном интернете [16].

Концепция подразумевает создание автономного контура управления сетями связи внутри страны. С точки зрения уголовного права, любое

несанкционированное вмешательство в работу точек обмена трафиком или систем централизованного мониторинга посягает не только на инфраструктуру связи, но непосредственно на государственный суверенитет, что может быть квалифицированно как совершение диверсии (ст. 281 Уголовного Кодекса РФ [17]).

Проблема концептуального уровня доктрины уголовно-правовой политики заключается в ограниченной досягаемости национального уголовного закона. Суверенитет абсолютен внутри страны, но виртуальное пространство трансграничное по своей природе. Решение может быть разное, например, привлечение к уголовной ответственности своих граждан (и постоянно проживающих в РФ лиц) за деяния, совершенные за рубежом, если они направлены против интересов РФ.

Реализация уголовно-правовой политики в информационной сфере сталкивается с рядом фундаментальных барьеров технико-юридического характера [5].

Так, проблема оценки размера ущерба в Интернете является одной из самых острых и дискуссионных в современной российской уголовно-правовой доктрине. Традиционный инструментарий материального права, оперирующий понятиями «стоимость имущества», «реальный ущерб» и «упущенная выгода» сталкивается с объектами, которые не имеют физической формы или рыночной цены – данными, доступностью сервисов и конфиденциальностью. В отличие от кражи автомобиля, где цена определяется рынком, стоимость базы персональных данных или иных цифровых данных субъективна.

Проблема отсутствия рыночного эквивалента данных, это фундаментальный кризис квалификации преступлений в Интернете, возникающий при попытке применить классические нормы уголовного права к нематериальным активам. Для квалификации преступления по признаку «крупный ущерб» (примечание к ст. 272 УК РФ – сумма свыше 1 млн. руб.) правоприменитель вынужден конвертирование мегабайты в информации в рубли. Поскольку судья не понимает природы цифрового актива, он полностью делегирует оценку эксперту. Эксперт сам выбирает методику (строки кода, затраченные часы, сметная стоимость сервера). Оспорить такие выводы адвокату практически невозможно без привлечения еще более дорогостоящего специалиста, которого суд часто отказывается приобщать. Суть проблемы в том, что у данных часто нет универсального, объективно измеримого рыночного эквивалента – той самой цены, которая сложилась бы на открытом рынке в условиях конкуренции. А без такого эквивалента сложно решать ряд практических задач, а именно оценивать ущерб в судебных спорах [8].

Анализ судебной практики показывает, что проблема отсутствия рыночного эквивалента данных является одной из самых сложных для правоприменителя. Метод затраты на восстановление является наиболее распространенным способом преодоления порога крупного ущерба (свыше 1 млн. рублей по примечанию к ст. 272 УК РФ), суды принимают расчеты, основанные не на стоимости самой информации, а на стоимости услуг по ее возвращению или защиты.

Для устранения доктринального и правоприменительного тупика, связанного с отсутствием рыночной цены данных, необходимы конкретные точечные изменения в законодательство. Например, уйти от зависимости «миллион рублей за данные» к формализованной оценке вреда, дополнить ст. 272 УК РФ примечанием 3 следующим положением: «При отсутствии рыночного эквивалента компьютерной информации или невозможности установить точный материальный ущерб, под «крупным ущербом» понимается сумма затрат на восстановление целостности и доступности информационной системы, подтвержденная финансово-экономической экспертизой, но не менее одного миллиона рублей. При этом затраты на оплату труда штатных сотрудников по устранению последствий инцидента включаются в расчет только при наличии приказа о привлечении к сверхурочной работе». Этот механизм превратил бы оценку ущерба из произвольного акта воли правоприменителя в строгую процедуру проверки документально подтвержденных документов.

Нельзя обойти вниманием и нормативно-идеологический уровень формирования уголовной политики. Он представляет собой механизм перевода абстрактных политических установок и доктринальных концепций на язык конкретных юридических запретов, это стадия, где государственная воля обретает форму диспозиций и санкций статей Уголовного кодекса РФ. В контексте обеспечения информационного суверенитета этот процесс характеризуется высокой скоростью реагирования, законодатель часто использует уголовный закон как инструмент «быстрого решения» для купирования внезапно возникающих угроз. [4, с.37] В основе формирования уголовно-правовой политики России в информационной сфере лежит иерархическая система нормативно-правовых актов стратегического планирования и фундаментальных политико-правовых идей, эти документы формируют в целом ratio legis (цель закона), которым руководствуется сегодня законодатель при криминализации деяний.

Важнейшим правовым актом определяющий вектор развития всей правовой системы России сегодня является Стратегия национальной

безопасности РФ, утвержденная Указом Президента РФ от 02.07.20201 г. № 400 [18]. Стратегия определяет недопустимость вмешательства во внутренние дела РФ, идея защиты государственного суверенитета трансформируется в уголовное преследование за сотрудничество с нежелательными организациями – ст. 284.1 и дискредитация использования ВС РФ – ст. 280.3 УК РФ, сеть же интернет рассматривается как основной канал такого вмешательства. Стратегия ставит задачу достижения технологического суверенитета, это также выливается в уголовную политику, а именно к выделению критической информационной инфраструктуры в особый объект охраны – ст. 274.1 УК РФ.

Стратегическая цель государственной информационной политики состоит в поступательной трансформации страны в демократическое информационное общество и ее эффективной интеграции в глобальное информационное пространство. [14, с.40] Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 05.12.2016 г. № 646, является дорожной картой для законодателя. Если Стратегия национальной безопасности говорит об идеях, то Доктрина перечисляет конкретные угрозы, которые должны быть нейтрализованы уголовным правом [19]. Так, например, угроза деструктивного информационно-психологического воздействия трансформировалась в появление составов о фейках (ст. 207.1–207.3 УК РФ), а идея заключается в том, что ложная информация сама по себе является оружием массового поражения, подрывающим общественную безопасность.

Угроза монополизации рынка ИТ-услуг иностранными государствами привела к доктрине локализации данных. И хотя само нарушение закона «О персональных данных» чаще влечет административную ответственность, систематическое неисполнение требований или утечки баз данных могут становиться основанием для уголовных дел по ст. 272 УК РФ (неправомерный доступ) или ст. 137 УК РФ (нарушение неприкосновенности частной жизни) [20]. Технико-юридический уровень доктрины отражает то, как законодатель формирует нормы закона и определяет объект преступления – те общественные отношения, ценности и блага, которые охраняются уголовным законом и на которые посягает преступник. [1, с.10] Глава 28 УК РФ (ст. 272–274) изначально рассматривалась как дополнение к главе о защите собственности. Неправомерный доступ квалифицировался по аналогии с кражей или уничтожением имущества. Объектом преступления являлось право собственности владельца сервера или ЭВМ, а также нормальная работа конкретных аппаратно-программных комплексов. Данная концепция не позволяла адекватно оценить вред от взлома государственного реестра, если при этом не было похищено имущество физических лиц. Преступник, который просто смотрел данные или временно блокировал работу сайта без вымогательства денег, часто оставался вне зоны действия жестких санкций [15].

С развитием социальных сетей, облачных технологий и появлением Интернета у всех граждан, фокус сместился. Компьютер перестал быть самоцелью, он стал средой передачи данных. Уголовная политика начала защищать информацию как таковую, независимо от носителя. Появление составов-трансформеров, это введение ответственности за клевету в сети (ст. 128.1 УК РФ), нарушение тайны переписки (ст. 138 УК РФ) именно с использованием информационно-телекоммуникационных сетей [21]. Объектом преступления выступает уже конфиденциальность, целостность и доступность информации. Охраняемыми стали режимы секретности - государственная тайна, коммерческая тайна, персональные данные. Эти концептуальные решения превратили интернет из места совершения преступления в способ, повышающий общественную опасность любого деяния (от мошенничества до сбыта наркотиков).

Современный этап развития уголовно-правовой политики характеризуется радикальным расширением объекта охраны, информация больше не рассматривается как пассивный ресурс, она стала оружием, а инфраструктура ее передачи – элементом национальной обороны. Изменения понимания объекта неизбежно повлекло за собой изменение юридической техники. Почти все современные цифровые составы являются бланкетными (отсылающими к другим законам). Чтобы понять суть преступления по ст. 274.1 УК РФ, необходимо изучить Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [22], это делает уголовное право «зависимым» от технического регулирования.

Эволюция объекта преступления на технико-юридическом уровне – это постоянный диалог права и технологий, право не может игнорировать новые реалии, но и не может технически переносить технические термины в юриспруденцию, отсюда вытекает задача – найти баланс, адекватно отразить суть новых угроз, четко определить объект охраны и при этом сохранить юридическую определенность норм, чтоб правоприменитель мог конкретно квалифицировать деяние. [3, с.255]

Системообразующие принципы современной уголовно-правовой политики в информационной сфере

На основе произведенного анализа, можно сформировать основные принципы, лежащие в

основе российской модели. Принципы формирования современной уголовно-правовой политики в цифровой сфере, это руководящие идеи, которые определяют логику законодателя при создании новых концепций и назначений наказаний за деяния, совершенные с использованием информационно-телекомукационных технология, как говорилось ранее, в отличие от классической уголовной политики, ориентированной на физический мир, информационная политика вынуждена учитывать специфику среды регулирования, это анонимность, трансграничность, скорость распространения информации и сложность доказывания. Принципы выстроены по степени убывания их концептуальной значимости для государства. Вышестоящий принцип определяет границы применения нижестоящего. Они работают в связке, образуя замкнутый цикл обеспечения суверенитета.

Принцип приоритета защиты публичного интереса над частным является стратегическим фундаментом современной российской уголовно-правовой-политики, он означает, что посягательство на цифровые активы государства квалифицируется как более опасное деяние, нежели аналогичное по материальному ущербу посягательство на имущество частного лица. Он стоит во главе угла, так как обосновывает саму необходимость вмешательства уголовного в цифровую среду ради целей, выходящий за рамки охраны жизни отдельного человека Доктринальное содержание принципа трактует, что традиционно уголовное право строилось вокруг защиты блага, имеющего физическую или экономическую форму, в цифровую эпоху акценты сместились, публичный интерес теперь защищается через охрану трех ключевых сущностей:

устойчивость процессов государственного управления, где информация рассматривается не как товар, а как инструмент власти;

общественная безопасность (когнитивный уровень), защита ментального состояния населения от пропаганды;

технологический суверенитет, независимость критических систем от иностранных решений. [13, с.152]

Принцип технологического реализма, это прагматичный подход к формированию уголовной политики, под которым государство признает объективные ограничения своих возможностей по прямому контролю над интернетом в целом. Признание государством своей технологической уязвимости перед децентрализованными сетями. Технологический реализм исходит из того, что анонимность интернета, использование VPN, прокси серверов носит трансграничный характер, что делает невозможным задержание каждого хакера или автора деструктивного поста традиционными методами. Суть принципа заключается в смещении вектора репрессии с конечного пользователя на инфраструктуру и посредников, которые обеспечивают его присутствие в сети. Если государство не может заблокировать поток зашифрованного трафика через определенный протокол, оно вводит уголовную ответственность за финансирование разработки таких инструментов или за оказание услуг по обеспечению анонимности преступникам. [2, с.277] Этот принцип позволяет государству защищать национальный сегмент сети, не обладая монополией на все мировые технологии.

Альтернативной принципу технологического реализма выступает принцип нейтральности и правовой определенности. Как подчеркивает Крыжан В.А., суть данного принципа заключается в том, что государство признает свою техническую слабость перед информационными угрозами и теперь закон должен регулировать суть отношений, например саму сделку, а не форму или инструмент с помощью которого это делается. [6, с.82] Реализуя данный принцип, государство вместо блокировки ресурсов выходит к развитию института гражданско-правовой ответственности пользователей. Если пользователь совершает преступление, государство должно использовать сложные технико-следственные действия для его идентификации, а не требовать выдачи ключей шифрования. Согласно принципу, технологии должны развивать свободно, а право догонять их точечно, квалифицируя уже совершенные деяния, а не пытаясь предугадать технические пути обхода.

Принцип криминализации намерения - самый радикальный принцип. Представляет собой отказ от классического постулата уголовного права – нет наказания без совершения деяния. Но в условиях информационного суверенитета государство исходит из того, что цифровые угрозы развиваются слишком быстро, а их последствия могут быть необратимыми, поэтому закон должен наказывать не только за наступивший вред, но и за само создание условий для этого вреда или наличие умысла на его причинение. [11, с.34] Реализация данного принципа наиболее ярко выражена в статьях, где отсутствие реального материального ущерба не является препятствием для возбуждения уголовного дела. Например, криминализация создания инструментов, согласно ст. 273 УК РФ преступлением признается сам факт написания кода вируса, трояна или программы для подбора паролей. Правоприменителю не надо доказывать, что программа была кем-то запущена, украдены ли средства или уничтожены данные, ответственность уже предусматривается

при создании. Логика законодателя здесь понятна, поскольку скорость распространения софта мгновенна, ждать наступление последствий нельзя. Само существование такого инструмента в сети уже представляет общественную опасность. В силу ч. 2 ст. 30 УК РФ, уголовная ответственность наступает за приготовление только к тяжким и особо тяжким преступлениям. В информационной среде круг таких деяний расширяется, поиск наемных хакеров для атаки на государственные реестры или приготовление оборудования для шпионской деятельности квалифицируется как приготовление задолго до момента самого удара по инфраструктуре. Принцип криминализации позволяет государству действовать на опережение, здесь уголовное законодательство берет на себя роль иммунной системы, она пытается индентифицировать вирус или опасный код на стадии создания. Однако обратной стороной такой эффективности является неизбежное привлечение к ответственности за несовершенные деяния.

Принцип универсализации цифрового пространства, как обстоятельства опасности, является доктринальным положением, согласно которому информационно-телекоммуникационная сеть «Интернет» рассматривается не просто как техническое средство связи или место совершения преступления, а как фактор, имманентно повышающий общественную опасность любого деяния. В рамках этого принципа использование сети Интернет признается законодателем качественным признаком, который переводит деяние на более высокий уровень тяжести, это проявляется через два основных механизма: закрепление интернета в качестве квалифицирующего признака и признание его обстоятельством, отягчающим наказание. [2, с.278]

Принцип альтернативный принципу универсальности интернета выдвинули В.Н. Перекрестов и А.А. Дехер. По их мнению, интернет – это лишь среда коммуникации, такая же, как бумага или улица. [9, с.65] Признание его обстоятельством, отягчающим наказание, по мнению авторов необоснованно, так как охват аудитории может быть меньше, чем предполагалось. Реализуется данный принцип через отказ от автоматического учета использования сети как отягчающего признака, переход к оценке реального масштаба последствий. Если ложная новость осталась внутри закрытого чата на 5 человек, она не представляет общественной опасности, даже если формально распространена через интернет. Квалификация должна зависеть от психологического воздействия на конкретную группу лиц, а не от факта прохождения пакета данных.

Принцип экстерриториальности национальной юрисдикции в контексте защиты информационного суверенитета, подразумевает, что государство сохраняет уголовно-правовой контроль над своими гражданами и постоянно проживающим на его территории иными лицами независимо от того, где физически они находятся в момент совершения деяния. Классическое уголовное право базируется на территориальном принципе, где закон действует там, где находится территория государства, однако информация не имеет физических границ. Пост в социальной сети, написанный пользователем, сидящим в кафе, например в Стамбуле, мгновенно отображается на смартфонах пользователей внутри России и влияет на общественное мнение так же, как если бы он был написан в соседнем подъезде.

Реализация этого принципа опирается на положения статьи 12 УК РФ, граждане РФ, совершившие преступление вне пределов России, подлежат уголовной ответственности, если совершенное ими деяние признано преступлением в государстве, на территории которого оно было совершено, и если они не были за его осуждены в иностранном государстве. [7, с.365]

Иностранные граждане и лица без гражданства, не проживающие постоянно в РФ, также могут быть привлечены к ответственности, если преступление направлено против интересов Российской Федерации либо гражданина РФ. Принцип экстерриториальности превратил информационное пространство в единое поле боя, где нет нейтральных территорий. Для российской уголовной политики физическая граница перестала быть препятствием. Любое высказывание или действие в сети оценивается исключительно по критерию потенциального вреда интересам государства, а паспорт гражданина РФ рассматривается как постоянная юридическая связь, исключающая возможность ухода от ответственности путем смены географической локации.

Заключение

Уголовно-правовая политика Российской Федерации в сфере обеспечения информационного суверенитета прошла качественную трансформацию. Она эволюционировала от фрагментарного регулирования компьютерных преступлений конца XX в. до формирования целостной стратегической доктрины защиты национального цифрового контура.

Современная уголовная политика представляет собой не просто совокупность запретов, а сложный инструмент геополитического и государственного управления, где уголовное право выступает финальным аргументом государства в борьбе за контроль над своим информационным пространством. В технико-юридическом аспекте это привело к фундаментальному сдвигу объекта охраны: от защиты стоимости компьютера и про-

граммного обеспечения законодатель перешел к защите информационных процессов и самой способности государства функционировать в условиях гибридных угроз. Принципы формирования современной уголовной политики — технологический реализм, приоритет публичного интереса над частным, проактивность и экстерриториальность — свидетельствуют о том, что государство осознало асимметрию цифровых вызовов. Поскольку техническое подавление внешних посягательств невозможно на сто процентов, репрессивный аппарат концентрируется на контроле инфраструктуры внутри страны и привлечении к ответственности внутренних субъектов, создающих условия для реализации угроз.

Очевидна объективная необходимость пересмотра категориального аппарата уголовного права применительно к цифровым объектам посягательства. Классическая триада «предмет – объект – вред» утрачивает свою объяснительную силу в условиях, когда информация не обладает физической формой и рыночной ценой. Для преодоления правоприменительного кризиса требуется переход от стоимостной модели оценки ущерба к функционально-восстановительной, где ключевым критерием становится не размер материальных потерь, а степень нарушения устойчивости государственных информационных систем и социально значимых сервисов. Такой подход позволит согласовать уголовно-правовую охрану с реальной природой цифровых угроз и устранить произвол в квалификации.

Принцип экстерриториальности, активно внедряемый в правоприменительную практику, вступает в объективное противоречие с фундаментальным принципом законности и территориальной определенности юрисдикции. В условиях отсутствия международных согласованных механизмов привлечения к ответственности иностранных субъектов за информационные посягательства российское уголовное законодательство вынуждено компенсировать этот пробел через расширение оснований для заочного осуждения и использования института «гражданской ипотеки» (например, требования локализации данных). Однако такая стратегия, будучи политически оправданной в текущей геополитической обстановке, создает риски необоснованного расширения судейского усмотрения и подрыва принципа правовой определенности. Дальнейшая эволюция уголовной политики должна быть направлена на выработку внутренних критериев пропорциональности и соразмерности репрессии, а также на поиск форм международного сотрудничества, пусть и ограниченного, для предотвращения цифрового вакуума правовой ответственности.

Совокупность обозначенных выводов позволяет утверждать, что российская уголовно-правовая политика обеспечения информационного суверенитета находится на этапе активного доктринального оформления, и ее эффективность в долгосрочной перспективе будет определяться способностью законодателя и правоприменителя гармонизировать императивы безопасности с фундаментальными правовыми принципами, сохраняя при этом адаптивность к стремительно меняющейся технологической среде.

Список литературы:

[1] Баранова М.В., Купцова О.Б. Технико-юридическая культура как базовая основа эффективного функционирования системы властных и невластных начал современного российского права // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2021. – № 3 (55). – С. 8–16. – DOI: 10.36511/2078-5356-2021-3-8-16..

[2] Голубенко Н.Р. Перспективы развития уголовного права в контексте цифровых технологий // Молодой ученый. – 2025. – № 49 (600). – С. 277–279. – URL: https://moluch.ru/archive/600/130926 (дата обращения: 04.07.2026).

[3] Долгиева М.М. Цифровой объект преступления // Вестник Томского государственного университета. – 2022. – № 483. – С. 253–260. – DOI: 10.17223/15617793/483/27..

[4] Егоров А.В. Правовая идеология и трансформация современных правовых систем // Вестник Московского университета. Серия 11. Право. – 2025. – № 2. – С. 35–49. – DOI: 10.55959/MSU0130-0113-11-66-2-2..

[5] Коптева Н.П. Регулирование индустрии больших данных: применим ли опыт Китая для России // Молодой ученый. – 2022. – № 47.1 (442.1). – С. 45–47. – URL: https://moluch.ru/archive/442/96758 (дата обращения: 14.07.2026).

[6] Крыжан В.А. О содержании принципа правовой определенности // Пермский юридический альманах. – 2018. – № 1. – С. 81–88.

[7] Кузнецов В.В. Принцип гражданства как экстерриториальный принцип действия уголовного кодекса РФ в пространстве // Вопросы российской юстиции. – 2025. – № 36. – С. 364–375.

[8] Матвеев И.В. Взаимовлияние цифровых технологий и уголовного права // Закон и право. – 2024. – № 7. – С. 179–182. – DOI: 10.24412/2073-3313-2024-7-179-182..

[9] Перекрестов В.Н., Дехерт А.А. Использование сети Интернет как обстоятельство, отягчающее наказание: цивилизационная трансформация или предрассудки прошлого? // Legal Concept = Правовая парадигма. – 2023. – Т. 22, № 1. – С. 63–69. – DOI: 10.15688/lc.jvolsu.2023.1.9..

[10] Петрова Г.В. Государственный суверене-

нитет и его охрана как международно-правовая ценность в повышении эффективности сотрудничества и коллективной безопасности стран СНГ // Международное сотрудничество евразийских государств: политика, экономика, право. – 2016. – № 2 (7). – С. 14–23.

[11] Русскевич Е.А. О криминализации обеспечения функционирования цифровой инфраструктуры киберпреступности // Научные исследования преступления и наказания. – 2026. – № 2 (6). – С. 32–39.

[12] Самигуллин Р.М. Конституционно-правовой режим государственной границы // Аграрное и земельное право. – 2024. – № 11 (239). – С. 95–97. – DOI: 10.47643/1815-1329_2024_11_95..

[13] Тарасов А.А. Об относительности границ публичного и частного интересов в уголовном процессе // Правовое государство: теория и практика. – 2025. – № 1 (79). – С. 152–163. – DOI: 10.33184/pravgos-2025.1.17..

[14] Трофимов М.С., Проводина О.А., Пископатский Д.А. Государственная политика Российской Федерации в сфере информации и информатизации: нормативно-правовой подход // Российский научный вестник. – 2025. – № 12. – С. 34–43. – DOI: 10.24412/2782-3830-2025-12-34-43..

[15] Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. – 2019. – № 1. – С. 29–35. – DOI: 10.19073/2306-1340-2019-16-1-29-35..

[16] Федеральный закон «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации» от 01.05.2019 № 90-ФЗ (последняя редакция) // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_323815/ (дата обращения: 07.07.2026).

[17] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 10.06.2026, с изм. от 29.06.2026) // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 07.07.2026).

[18] Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения 11.07.2026).

[19] Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения 11.07.2026).

[20] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 09.07.2026).

[21] Федеральный закон "О внесении изменения в статью 128.1 Уголовного кодекса Российской Федерации" от 30.12.2020 № 538-ФЗ (последняя редакция) // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_372713/ (дата обращения: 10.07.2026).

[22] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // СПС «КонсультантПлюс» / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (29.08.2026).

References:

[1] Baranova M.V., Kuptsova O.B. Technical and legal culture as the basic basis for the effective functioning of the system of power and non-power principles of modern Russian law // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. – 2021. – № 3 (55). - S. 8-16. – DOI: 10.36511/2078-5356-2021-3-8-16..

[2] Golubenko N.R. Prospects for the development of criminal law in the context of digital technologies // Young scientist. – 2025. – № 49 (600). - S. 277-279. - URL: https://moluch.ru/archive/600/130926 (access date: 04.07.2026).

[3] Dolgieva M.M. Digital object of crime // Bulletin of Tomsk State University. – 2022. – № 483. - S. 253-260. – DOI: 10.17223/15617793/483/27..

[4] Egorov A.V. Legal ideology and transformation of modern legal systems // Bulletin of Moscow University. Series 11. Right. – 2025. – № 2. - S. 35-49. – DOI: 10.55959/MSU0130-0113-11-66-2-2..

[5] Kopteva N.P. Regulation of the big data industry: is China's experience applicable to Russia // Young scientist. – 2022. – № 47.1 (442.1). - S. 45-47. - URL: https://moluch.ru/archive/442/96758 (access date: 14.07.2026).

[6] Kryzhan V.A. On the content of the principle of legal certainty // Perm Legal Almanac. – 2018. – № 1. - S. 81-88.

[7] Kuznetsov V.V. The principle of citizenship as an extraterritorial principle of the criminal code of the Russian Federation in space // Issues of Russian justice. – 2025. – № 36. - S. 364-375.

[8] Matveev I.V. Mutual influence of digital technologies and criminal law // Law and law. – 2024. – № 7. - S. 179-182. – DOI: 10.24412/2073-3313-2024-7-179-182..

[9] Crossroads VN, Dehert A.A. Use of the Internet as a circumstance aggravating punishment: civilizational transformation or prejudices of the past? // Legal Concept = Legal paradigm. – 2023. - T. 22, NO. 1. - S. 63-69. – DOI: 10.15688/lc.jvolsu.2023.1.9..

[10] Petrova G.V. State sovereignty and its protection as an international legal value in increasing the effectiveness of cooperation and collective security of the CIS countries // International cooperation of Eurasian states: politics, economy, law. – 2016. – № 2 (7). - S. 14-23.

[11] Russkevich E.A. On the criminalization of ensuring the functioning of the digital infrastructure of cybercrime // Scientific research of crime and punishment. – 2026. – № 2 (6). - S. 32-39.

[12] Samigullin R.M. Constitutional and legal regime of the state border // Agrarian and land law. – 2024. – № 11 (239). - S. 95-97. – DOI: 10.47643/1815-1329_2024_11_95..

[13] Tarasov A.A. On the relativity of the boundaries of public and private interests in criminal proceedings // Rule of law: theory and practice. – 2025. – № 1 (79). - S. 152-163. – DOI: 10.33184/pravgos-2025.1.17..

[14] Trofimov M.S., Provodina O.A., Piskovatsky D.A. State policy of the Russian Federation in the field of information and informatization: regulatory approach // Russian Scientific Bulletin. – 2025. – № 12. - S. 34-43. – DOI: 10.24412/2782-3830-2025-12-34-43..

[15] Churilov A.Yu. Principles of the General Regulation of the European Union on the Protection of Personal Data (GDPR): Problems and Prospects of Implementation // Siberian Legal Review. – 2019. – № 1. - S. 29-35. – DOI: 10.19073/2306-1340-2019-16-1-29-35..

[16] Federal Law "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection" dated 01.05.2019 No. 90-FZ (latest edition) // SPS "ConsultantPlus" / URL: https://www.consultant.ru/document/cons_doc_LAW_323815/ (date of reference: 07.07.2026).

[17] Criminal Code of the Russian Federation dated 13.06.1996 No. 63-FZ (as amended on 10.06.2026, as amended on 29.06.2026) // SPS ConsultantPlus / URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed on: 07.07.2026).

[18] Decree of the President of the Russian Federation of 02.07.2021 No. 400 "On the National Security Strategy of the Russian Federation" // SPS ConsultantPlus URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (date of appeal 11.07.2026).

[19] Decree of the President of the Russian Federation of 05.12.2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation" // SPS ConsultantPlus" / URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (date of request 11.07.2026).

[20] Federal Law "On Personal Data" dated 27.07.2006 No. 152-FZ (latest edition) // SPS ConsultantPlus URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (date of reference: 09.07.2026).

[21] Federal Law "On Amending Article 128.1 of the Criminal Code of the Russian Federation" dated 30.12.2020 No. 538-FZ (latest edition) // SPS "ConsultantPlus / URL: https://www.consultant.ru/document/cons_doc_LAW_372713/ (date of reference: 10.07.2026).

[22] Federal Law "On Security of Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 No. 187-FZ // SPS "ConsultantPlus / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (29.08.2026).