Дата поступления рукописи в редакцию: 26.10.2025 г.
Дата принятия рукописи в печать: 02.11.2025 г.
DOI: 10.24412/2782-3830-2025-10-92-103

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

ПРОВОДИНА Олеся Александровна,
старший преподаватель кафедры
административного и финансового права
Федерального государственного автономного
образовательного учреждения высшего образования
«Северо-Кавказский федеральный университет»,
e-mail: 19_lelya_91@mail.ru

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

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ В КОНТЕКСТЕ БОРЬБЫ С ПРЕСТУПНЫМИ ДЕЙСТВИЯМИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация. *В статье анализируется современное состояние уголовно-правовых норм, посвященных борьбе с преступлениями в компьютерной сфере, а также смежным нормам Уголовного кодекса РФ в контексте их роли в обеспечении правовой охраны информационного суверенитета России. Стремительный рост киберпреступности и использование информационно-телекоммуникационных сетей создают прямую угрозу информационному суверенитету Российской Федерации. Уголовное законодательство отстает от технологического развития, что затрудняет эффективную борьбу с вызовами в информационной сфере, что подтверждает стремительный рост преступлений, совершаемых с использованием информационно-телекоммуникационных сетей. Установлено, что действующее уголовное законодательство (ст.ст. 272–274.5 УК РФ) не в полной мере отражает современные реалии и требует модернизации. Легальное определение информационно-телекоммуникационных сетей устарело и не соответствует их комплексной природе. Для надежной защиты информационного суверенитета необходим комплексный подход, включающий совершенствование уголовного закона, развитие уголовно-правовой доктрины и согласованное применение норм различных отраслей права. Результаты исследования могут быть использованы для дальнейшего реформирования уголовного законодательства в данной сфере.*

Ключевые слова: *информационный суверенитет, киберпреступность, компьютерные преступления, информационно-телекоммуникационные сети, глава 28 УК РФ.*

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/

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

PROVODINA Olesya Alexandrovna,
Assistant of the 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 PROTECTION OF THE INFORMATION SOVEREIGNTY OF THE RUSSIAN FEDERATION IN THE CONTEXT OF COMBATING CRIMINAL ACTIONS IN THE INFORMATION SPHERE

Annotation. *The relevance of the study is driven by the exponential growth in the number and complexity of crimes committed using information and telecommunication networks, which pose a direct threat to the information sovereignty and national security of the Russian Federation. Current criminal legislation lags behind rapid technological advancements, necessitating in-depth scientific analysis. The aim of the article is to conduct a comprehensive analysis of the current state of criminal law protection of Russia's information sovereignty, identify systemic issues in legal regulation, and develop proposals for its improvement. The methodological framework includes formal legal analysis of the norms of the Criminal Code of the Russian Federation, comparative legal methods, examination of scientific doctrine, and generalization of judicial and investigative practices. The scientific article sequentially explores the evolution of the concept of "information sovereignty," elaborates on its modern meaning and legal safeguards. A detailed examination of the offenses under Chapter 28 of the Criminal Code of the Russian Federation (Articles 272–274.5), as well as related provisions (Article 275 of the Criminal Code – high treason), occupies a central place. A separate section systematizes key issues in criminal law protection (fragmentation of norms, outdated definitions, difficulties in evidence collection, imbalance between individual and state interests). It has been established that current legislation is not fully adequate to address modern cyber threats. The legal definition of information and telecommunication networks requires expansion. Effective protection of information sovereignty can only be achieved through a comprehensive approach combining improvements to the Criminal Code of the Russian Federation and the development of procedural and operational-investigative mechanisms. The findings and suggestions of the study can be used to further reform criminal law, improve law enforcement practices and develop departmental concepts in the field of cybersecurity.*

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

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 современной политической практике одним из наиболее употребляемых терминов является «суверенитет», под которым, как правило, понимается самостоятельность государств в принятии политических решений как в международных отношениях, так и внутри самого государства.

Несмотря на неоднозначность толкования суверенитета в политологии и юриспруденции, постоянно «умножении его смыслов» [13, с.64-78], никто не спорит с тем, что суверенитет является ключевой категорией в контексте феномена государства и государственности.

Развитие учений о государственном суверенитете в процессе естественной эволюции породило такое понятие как «информационный суверенитет», которое в настоящее время также прочно вошло в научный и политический оборот, как и собственно классическое понятие суверенитета.

Правовые аспекты государственного суверенитета в информационной сфере в российской юридической науке были затронуты в конце 1990-х гг. В.Б. Наумовым. [14] Исследование содержания суверенитета в информационной сфере и способов его защиты было связано, в первую очередь, с поиском ответов на новые вызовы: начинавшейся цифровой трансформацией России.

В российской юридической науке предлагается комплексный подход к охране информационного суверенитета, основанный на правовом регулировании и государственных механизмах контроля. Основные способы охраны информационного суверенитета, выделяемые учеными, включают следующие направления:

- применение международных принципов и разработанных в соответствии с ними российских нормативных актов, регулирующих информационное пространство и национальные интересы в информационной сфере [1];
- формирование и реализация единой государственной информационной политики, в рамках которой реализуются меры по противодействию распространению ложной и противоправной информации, развитию кибербезопасности, повышению цифровой грамотности населения, поддержке отечественных исследований и технологий для снижения зависимости от зарубежных продуктов в информационной сфере [4];
- разработка норм и принципов информационного права, регулирующих деятельность государства и общества в информационном пространстве. [6]
- контроль и фильтрация информации, государственный контроль за распространением информации в русскоязычном интернете, фильтрацию данных, постов, сайтов и другой информации, чтобы предотвратить доступ к нежелательной информации на территории России [5];
- создание системы обнаружения, предупреждения и ликвидации угроз в информационной сфере, в том числе противодействие кибератакам и информационным диверсиям. [12]

Основные способы охраны информационного суверенитета в российской юридической науке связаны с сочетанием правового регулирования, государственного контроля и государственной политики безопасности, направленных на защиту национальных интересов в информационной сфере.

В этой связи считаем необходимым рассмотреть такой аспект правовой охраны информационного суверенитета России как установление уголовно-правовой ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных сетей (ИТС) (включая сеть Интернет).

Информационно-коммуникационные технологии (ИКТ) играют ключевую роль в современном обществе, предоставляя широкие возможности для общения, бизнеса и государственного управления. Однако, наряду с преимуществами возникают новые угрозы и риски, обусловленные расширением масштабов противоправной деятельности в цифровой среде. Преступления приобретают особую опасность вследствие высокой степени анонимности, межрегионального характера действий преступников и сложности расследования дел.

Развитие ИТС значительно расширило пространство для преступлений, став новой ареной для совершения множества противоправных действий, влияющих на состояние информационной безопасности государства и его информационный суверенитет. Сегодня одним из главных вызовов для современной правоохранительной системы России является обнаружение и раскрытие преступлений, совершаемых в цифровой среде.

Легальное определение ИТС закреплено в п. 4 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» - «технологическая система, предназначенная для передачи по различным линиям связи, доступ к которой осуществляется с использованием средств вычислительной техники» [22].

Указанное определение сужает понимание важности рассматриваемых технологий и как следствие приводит к ухудшению предупредительной деятельности правоохранительных органов в информационной сфере и сфере ИКТ.

В этой связи А.С. Унукович предлагает под ИТС понимать «систему, предназначенную для осуществления обработки, передачи или хранения информации с помощью телекоммуникационных технологий, в том числе и сеть Интернет, обеспечивая связь между устройствами, позволяющие обмениваться информацией». [19] Н.В. Летелкин предлагает рассматривать ИТС как «технологическую систему, предназначенную для хранения и передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (компьютеров)». [11, с.219]

Проанализировав современную научную литературу, предлагаем свое понимание ИТС как комплекс взаимосвязанных систем, обеспечивающих передачу, обработку и хранение информации на основе цифровых технологий. Такие сети

объединяют компьютеры, серверы, устройства связи, каналы передачи данных, позволяя пользователям взаимодействовать друг с другом, получать доступ к ресурсам и сервисам, а также осуществлять коммуникацию независимо от географического положения.

Наиболее распространенным примером является Интернет, который сегодня объединяет миллионы компьютеров и мобильных устройств, обеспечивая свободный доступ к разнообразной информации и интерактивное взаимодействие между людьми.

Заместим, что в России с 2019 по 2023 гг. количество компьютерных преступлений возросло более чем в два раза (с 294,4 тыс. преступлений в 2019 г. до 677 тыс. в 2023 г.) [23]. В 2024 г. было совершено 84,8% преступлений с использованием Интернета, общая их численность составила 649,1 тысячи преступлений. Как заявил глава МВД России В. Колокольцев, жертвами незаконных действий в цифровой среде становятся все, в том числе и госструктуры, киберпреступления наносят значительный ущерб всем отраслям экономики и общества. [3]

Актуальность поднятой проблемы подтверждается и статистическими данными. Удельный вес компьютерных преступления в числе всех зарегистрированных уголовно-наказуемых деяний вырос с 14,5% в 2019 г. до 34,8% в 2023 г [24]. А в 2024 г. на преступления с использованием цифровых технологий пришлось 40% всех зарегистрированных деяний. [3]

Современная российская уголовно-правовая политика в области выявления и расследования преступлений, совершаемых с использованием ИТС свидетельствует об отставании законодателя от развития технологий. Преступлениями в сфере ИТС признаются деяния, направленные против конфиденциальности, целостности и доступности информационных ресурсов, осуществляемые посредством использования цифровых технологий и сетевых инфраструктур. [18] Значение ИТС постоянно возрастает, поскольку они обеспечивают основу для развития экономики, науки, образования, культуры и социальных отношений современного общества. Вместе с тем, именно в силу своей значимости и широкого охвата, ИТС становятся объектом повышенного внимания преступников, что создаёт необходимость принятия эффективных мер по обеспечению безопасности личности, общества и государства.

Информационный суверенитет государства подразумевает независимость и способность контролировать поток информации, проходящий внутри страны, а также защищать внутренние информационные ресурсы от внешних угроз. Однако в современную эпоху трансграничные преступления способны серьезно подрывать этот важный элемент суверенитета, оказывая негативное влияние на внутреннюю стабильность и безопасность государства.

Чтобы нейтрализовать указанные угрозы, необходима мощная государственная политика, направленная на защиту национальных интересов и развитие собственного информационного потенциала.

По нашему мнению, Россия движется к формированию общего подхода к международным (трансграничным) преступлениям. Развитие технологий позволяет рассчитывать на быстрое распознавание, например, схем мошенничества и автоматическое отслеживание источников угроз. Согласно Стратегии национальной безопасности РФ возникновение новых форм противоправных деяний, основанных на применении ИТС и высокотехнологичных инструментов, отнесено к ключевым стратегическим рискам, угрожающих безопасности государства [25].

Тут возникает проблема доступа правоохранительный органов к личным данным граждан, что вызывает активные дискуссии в обществе. Часть общества убеждена, что государство вправе следить за своими гражданами ради обеспечения безопасности. Другая его часть настаивает на приоритете индивидуальных свобод и конфиденциальности, считая, что операции по слежке ущемляют права человека. Так согласно ч.2 ст. 23 Конституции РФ, каждый гражданин имеет право на тайну переписки, телефонных переговоров, почтовых и иных сообщений [26]. Но в рамках уголовного судопроизводства, согласно ст. 13 Уголовно-процессуального кодекса РФ, ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается на основании судебного решения, поэтому следователи или иные представители правоохранительных органов могут получить доступ к перепискам и т.д [27].

Сегодня технологии зашиты информации достигли значительных успехов, что ещё больше усугубляет проблему оперативной слежки. Современное программное обеспечение позволяет создавать защищённые чаты, шифровать трафик и скрывать личность пользователей. Отсюда вывод - проблема оперативной слежки и контроля в ИТС продолжает оставаться острой темой обсуждения. Быстрое развитие технологий ставит правоохранительную систему перед сложными вопросами выбора между сохранением индивидуальной свободы и эффективностью защиты государства и общества от угроз в информационной сфере. Решением этой про-

блемы станет гармоничное сочетание правовых реформ, технологического прогресса и устойчивого роста доверия между населением и властью.

Одним из способов противодействия указанным деяниям является уголовно-правовая охрана безопасности информации, хранения, обработки и передачи данных с использованием информационных технологий. В Уголовном кодексе РФ существует глава 28 «Преступления в сфере компьютерной информации» (ст.ст. 272 – 274.5) [28].

Рассмотрим составы преступлений главы 28 УК РФ, которые в наибольшей степени соответствуют задаче уголовно-правовой охраны информационного суверенитета Российской Федерации.

Ст. 272 УК РФ – Незаконный доступ к компьютерной информации - охватывает ситуации, когда лицо получает доступ с нарушением закона к охраняемой компьютерной информации, в результате чего происходят уничтожение, блокировка, изменение или копирование этой информации. Субъектом преступления выступает физическое, вменяемое лицо, достигшее возраста 16 лет. Объективная сторона выражается в преступных действиях, состоящих в нарушениях установленного порядка доступа к информации. Доступ признается незаконным, если лицо не имело соответствующих полномочий и оснований для входа в систему или использованию ею. Санкция за данные деяния предусмотрена в виде лишения свободы на срок до двух лет, либо принудительными работами на срок до двух лет. Если деяние совершено группой лиц по предварительному сговору или организованной групп, наказание ужесточается до шести лет лишения свободы. При особо тяжких последствиях (массовые разрушения баз данных, значительное экономическое повреждение, угроза здоровью или жизни людей), максимальный срок лишения свободы достигает семи лет.

Судебная практика показывает рост числа рассматриваемых дел, особенно распространены случаи неправомерного доступа к банковским системам, сайтам государственных служб, закрытым ведомственным ресурсам и корпоративным базам.

Ст. 273 УК РФ – Создание, использование и распространение вредоносных программ - направлена на защиту информационных систем и данных от угроз, создаваемых специальными программами, предназначенными для правомерного вмешательства в функционирования компьютерных систем. По смыслу статьи, преступление заключается в создании программ, заведомо приводящих к негативным последствиям, выраженных в уничтожении, блокировки, модификации и копировании информации, так же в распространении созданных вредоносных программ другим лицами, что делает возможным массовое заражение компьютерных систем, все эти действия и образуют объективную сторону данного состава преступления.

Согласно ст. 4 Постановления Пленума Верховного суда РФ № 37 от 15.12.2022 г. под компьютерной программой понимается «совокупность данных и команд, предназначенных для функционирования ЭВМ в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения» [29].

Объектом преступления ст. 273 УК РФ выступают общественные отношения, обеспечивающие нормальное функционирование ИТС и сохранность обрабатываемой информации. Субъектом преступления является физическое лицо достигшее 16 лет, действующее осознанно и целенаправленно. Преступление является оконченным в момент создания, использования или распространения вредоносных программ, даже если реально не произошло уничтожения, блокирования или модификации данных. Субъективная сторона выражена в прямом умысле, когда лицо сознает потенциальную опасность своего поведения и желает нанести вред. При квалификации значение имеет установление факта создания или использования программы, направленной на деструктивные действия в отношении информации, для установления виновности лица, необходимо подтвердить цель автора на разрушение, нарушение работы систем или незаконное получение данных.

Применение ст. 273 УК РФ в практике осложняется трудностью фиксации момента создания вредоносной программы и установления связи между программой и последствиями. Как подчеркивают Е.Р. Россинская и И.А. Рядовский, проблема заключается в том, что вредоносные программы не нуждаются во внешнем управлении, заложенные в них функциональные возможности реализуются автономно. [16]

Ст. 274 УК РФ – Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС - направлена на предупреждение нарушений в сфере эксплуатации компьютерных систем и сетей, создающих риск для безопасности информации и нормальной работы технических средств. Предметом выступают действия, нарушающие установленные правила эксплуатации средств хранения, обработки или передачи информации, в результате которых произошла утрата, искажение или блокировка важных данных. Объектом преступления являются общественные отношения, гарантирующие целостность, доступность и

надежность данных, используемых государственными органами, предприятиями и физическими лицами. Субъектом преступления выступает специальный субъект, лицо, ответственное за соблюдение правил эксплуатации технических средств, чьи действия привели к возникновения негативного результата. Особые сложности возникают при установлении факта причинно-следственной связи между нарушением правил эксплуатации и наступлением негативных последствий. Правоохранительным органам необходимо доказать, что нарушение действительно повлияло на состояние технической работоспособности системы. Другая сложность связана с определением границы между халатностью и нарушением правил эксплуатации.

В 2024 г. в Уголовный кодекс РФ введена новая ст. 272.1, посвящённая борьбе с незаконным использованием или передачей, сбором или хранением компьютерной информации, содержащей персональные данные, а равно создание и обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения [30]. Данная статья направлена на защиту персональных данных граждан и организацию надзора за соблюдением правил обращения с ними. Преступление считается законченным в момент исполнения вышеуказанных действий, независимо от того, наступит ли реальный ущерб. Субъектом преступления является физическое, вменяемое лицо, достигшее возраста 16 лет. Субъективная сторона выражена в форме прямого умысла.

Введение в УК РФ указанной статьи вызвано необходимостью защитить граждан от возможных злоупотреблений их персональными данными, эта норма способствует созданию условий для безопасной жизнедеятельности и защищает личную жизнь каждого человека. Несмотря на достигнутый прогресс, остается много нерешенных вопросов, связанных с квалификацией таких преступлений.

Помимо составов главы 28 в УК РФ содержатся и иные составы преступлений, тоже связанные с применением ИКТ. Здесь можно вспомнить ст. 137 – Нарушение неприкосновенности частной жизни; ст. 138 – Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений и, конечно же, ст. 159.6 - Мошенничество в сфере компьютерной информации.

Еще более опасной ситуация с незаконным доступом или передачей компьютерной информации выглядит в контексте государственной измены (ст. 275 Уголовного кодекса РФ).

В 2025 г. Судебный департамент при Верховном суде РФ обнародовал официальную статистику применения ст. 275 Уголовного кодекса РФ. Так, согласно представленной информации, в 2024 г. за государственную измену было привлечено к ответственности 145 граждан (143 из них были приговорены к лишению свободы, двое к пожизненному сроку отбывания наказания), тогда как в 2023 г. по данной статье УК РФ было осуждено всего 39 человек, а в 2022 г. – 16 человек. Рост количества обвинительных приговоров за один 2024 год составил 371%, т.е. почти произошло почти четырёхкратное увеличение. [21]

Причин такого роста наверняка несколько, на налицо явное ужесточение практики уголовно-правовой охраны государственной безопасности.

Объект состава преступления ст.275 УК РФ - безопасность Российской Федерации, то есть общественные отношения, обеспечивающие состояние защищенности ее суверенитета, неприкосновенности и неделимости территории, обороноспособности. Важно понимать, что государственной изменой будет считаться как посягательство на все составляющие безопасности РФ, так и на ее отдельные слагаемые. При этом категория «безопасность» в контексте ст. 275 УК РФ толкуется неоднозначно, широко, нет единообразия в понимании механизма воздействия на безопасность при посягательствах.

Например, А.И. Рарог в качестве объекта указывал внешнюю безопасность страны, под которой понимает защищенность интересов государства от внешних угроз. [17, с.544] А.Г. Кулев под объектом ст. 275 УК РФ также подразумевал внешнюю безопасность, которая слагается из состояния защищенности, суверенитета, территориальной целостности и неприкосновенности, а также обороноспособности государства от внешних угроз. [10]

В соответствии со ст. 275 УК РФ государственная измена – это «совершенные гражданином Российской Федерации шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, переход на сторону противника либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации…» [31].

Все эти действия могут быть совершены с использованием ИТС и нести ущерб информационному суверенитету государства.

В отечественных исследованиях уголовно-правовой тематики в контексте защиты

информационной безопасности можно встретить ряд проблем ее обеспечения правового и организационно-технического характера.

М.А. Ефремова в своем диссертационном исследовании выделяет три глобальные проблемы. [8]

1. Отсутствие целостной уголовной политики в сфере противодействия преступлениям против информационной безопасности. Российское уголовное законодательство неадекватно и неполно отражает фактически сложившиеся общественные отношений, а также не способно эффективно реагировать на новые, быстро меняющиеся виды и формы преступлений в информационной сфере. Уголовно-правовые нормы недостаточно эффективны, так как они разрозненны и размещены в различных главах Уголовного кодекса РФ, а соответственно не связаны институционально и содержат юридико-технические различия.
2. В уголовно-правовом регулировании информационной безопасности не решена проблема баланса интересов личности, общества и государства. Требуется установление уголовной ответственности за деяния, которые посягают на интересы всех трех охраняемых субъектов, но при этом не нарушают права и свободы граждан в информационной сфере.
3. Отсутствие уголовной ответственности за нарушение профессиональной и служебной тайны в информационной сфере, что создает пробелы в защите конфиденциальной информации и способствует рискам инфокоммуникационной безопасности государства.

Еще одну ключевую проблему озвучил С.М. Ильясов, и она заключается в сложности применения уголовно-правовых норм к новым видам цифровых преступлений, связанных с использованием информационно-телекоммуникационных технологий, что требует развития уголовно-правовой доктрины и уточнения понятийного аппарата. [9]

На наличие масштабной проблемы указывает и Т.А. Полякова. Она пишет о необходимости модернизации и согласованности правовых актов стратегического планирования и законодательного регулирования. По ее справедливому мнению, современный правовой механизм охраны информационного суверенитета должен учитывать новые цифровые вызовы, включая искусственный интеллект, аутентификацию и идентификацию в электронном пространстве. [15]

Проблемы нормативных оснований уголовно-правовой защиты информационного суверенитета, а также проблемы выявления преступлений в ИТС остаются крайне острыми и взывают серьезное беспокойство у специалистов и общественности. Решение этих проблем требует усилий общества и государства. Комплексный подход, включающий улучшение законодательной базы и подготовку специалистов в данной сфере, способен привести к значительным успехам в формировании защищенного информационного пространства России.

Осознавая существующие проблемы в сфере уголовно-правовой охраны информационного суверенитета России на уровне Правительства РФ был предложен комплекс мер, который закреплен в утвержденной в 2024 г. в Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием ИКТ [32].

Отметим, что в Концепции закрепляются такие понятия, отсутствующие в российском законодательстве, как «информационно-коммуникационная сфера», «противоправные деяния, совершенные с использованием информационно-коммуникационных технологий», «государственная система противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий», «информационно-коммуникационные технологии», «средства государственной системы».

Под противоправными деяниями Концепция понимает «общественно опасные деяния, за которые предусмотрена уголовная либо административная ответственность, совершенные с использованием (применением) информационно-коммуникационных технологий или в сфере компьютерной информации, в том числе с использованием (применением) электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», информационной инфраструктуры, компьютерной техники, программных средств, онлайн-сервисов, средств коммуникации (в том числе средств мобильной связи, сервисов обмена мгновенными сообщениями, IP-телефонии), электронных средств платежа, операций с цифровой валютой и цифровыми финансовыми активами» [33].

Столь широкий подход однозначно указывает на масштабность проблемы, для борьбы с которой была разработана и принята Концепция.

По смыслу Концепции все противоправные деяния классифицируются по трем основным типам:

1) правонарушения и преступления в сфере компьютерной информации;
2) правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием электронных или ИТС, включая сеть «Интернет»;

3) правонарушения и преступления, при совершении которых применение ИКТ является альтернативным способом.

Распоряжением Правительства РФ от 14 августа 2025 г. №2207-р утвержден План мероприятий по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий [34].

Как указано на официальном сайте Правительства РФ, «Документ включает комплекс мер по совершенствованию законодательства, техническому противодействию злоумышленникам и повышению цифровой грамотности населения». [20] А это означает, что в период до IV квартала 2027 г. соответствующими ведомствами будут разработаны проекты правовых актов, направленные на совершенствование уголовного, уголовно-процессуального законодательства и законодательства об оперативно-розыскной деятельности в части выявления, предупреждения, раскрытия и расследования противоправных деяний в ИТС и с их использованием. Однако, в Плане речь не идет о внесении изменений и дополнений в Уголовный кодекс РФ. Вероятно, это будет сделано вне этого Плана, но в соответствии с разделом IV Концепции.

Таким образом, в результате проведенного исследования мы пришли к следующим выводам.

1. Уголовно-правовое регулирование противодействия преступлениям в компьютерной сфере (компьютерным преступлениям) в первую очередь направлено на борьбу с данным видом преступлений. Обеспечение информационной безопасности и информационного суверенитета России осуществляется постольку, поскольку нормы Уголовного кодекса РФ эффективны в сфере борьбы с компьютерными преступлениями.
2. Наименование главы 28 «Преступления в компьютерной сфере» УК РФ значительно сужает потенциал указанной главы в сфере обеспечения информационной безопасности и информационного суверенитета России. Тогда как полная защита и обеспечение информационного суверенитета может быть достигнуто только в комплексе с применением норм различных отраслей российского права.
3. Легальное ИТС, закрепленное в Федеральном законе «Об информации, информатизации и информационных технологиях», не отвечает современным реалиям развития технологий и не удовлетворяет требованиям правоприменительной практики. В этой связи предлагаем понимать по ИТС комплекс взаимосвязанных систем (компьютеры, серверы, устройства связи, каналы передачи данных), обеспечивающих передачу, обработку и хранение информации на основе цифровых технологий, позволяющих пользователям взаимодействовать друг с другом, получать доступ к ресурсам и сервисам, а также осуществлять коммуникацию независимо от географического положения.
4. Нормы Уголовного кодекса РФ (главы 28 и ряды статей других глав) не в полной мере соответствуют развитию современных ИКТ, не отражают всех особенностей их использования и применения злоумышленниками в преступных целях. Тем не менее, заложенный в них законодателем потенциал позволяет оказывать эффективное противодействие данному виду преступлений.
5. Выявленные ключевые проблемы уголовно-правовой охраны информационной безопасности и информационного суверенитета делают необходимым комплексное совершенствование уголовного законодательства и создание комплексной стратегии защиты информационного суверенитета в современных условиях цифровизации.

Список литературы:

[1] Бажина, М.А., Шахновская, И.В. Содержание и актуальные угрозы обеспечению информационного суверенитета: на примере Республики Беларусь и Российской Федерации // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. 2023. №2 (64). С.63-67

[2] Бастрыкин: Предлагаем закрепить в УК для киберпреступников новое отягчающее обстоятельство РГ.РУ. // [Электронный ресурс] / Режим доступа: URL: https://rg.ru/2025/01/14/v-uk-rf-dlia-kiberprestupnikov-propishut-novoe-otiag-chaiushchee-obstoiatelstvo.html (дата обращения 01.06.2025).

[3] В России в 2024 году IT-преступления достигли пика за последние пять лет. / ТАСС / [Электронный ресурс] /. URL: https://tass.ru/proisshestviya/22978955/ (дата обращения: 24.08.2025).

[4] Грибин, Н.П., Кохтюлина, И.Н., Седунов, Д.И., Соболев, Е.И. Информационный суверенитет: материалы научной дискуссии // Россия и мир: научный диалог. 2022. № 2 (4). С.100-131

[5] Дубинина Е.Н., Хорошавина Я.А. Информационный суверенитет Российской Федерации // Advances in law studies Том 9. 2021.№ 3. С.66-70

[6] Ефремов, А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т.63, № 1. С.47-61. https://doi.org/10.21638/spbu25.2019.103

[7] Ефремов, А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации / Дисс. д-ра юрид. наук: М., 2021. 418 с.

[8] Ефремова, М.А. Уголовно-правовая охраны информационной безопасности // Афтореф. дисс. д-ра юрид. наук. М., 2018. 59 с.

[9] Ильясов, С.М. Некоторые проблемы совершенствования нормативной правовой регламентации вопросов информационной безопасности в Российской Федерации // Юридический вестник ДГУ. 2024. Т. 49, № 1 (69). С.41-49

[10] Кулев, А.Г. Преступления против внешней безопасности государства: вопросы законодательной техники и дифференциации ответственности // Автореф. дисс. канд. юрид. наук - Самара, 2009. 21 с.

[11] Летелкин, Н.В. Об определении признаков и понятия «информационно-телекоммуникационная сеть» в отечественном уголовном законодательстве // Matters of Russian and International Law. 2018, Vol. 8, Is. 3A. С.216-221

[12] Меньшиков, П.В. Актуальные аспекты обеспечения информационного суверенитета России [Электронный ресурс] // Международные коммуникации. 2017. №5. Режим доступа: https://intcom-mgimo.ru/2017/2017-05/information-sovereignty-of-russia (дата обращения: 12.05.2025)

[13] Мусихин, Г.И. Классификация теорий суверенитета как попытка преодоления «концептуального эгоизма» // Общественные науки и современность. 2010. №1. С.64-78

[14] Наумов, В.Б. Интернет и государственный суверенитет. Стенограмма Первой всероссийской научно-практической конференции «Право и Интернет: теория и практика». 2 ноября 1999 года. С. 20-23

[15] Полякова, Т.А. Правовое обеспечение государственного суверенитета и информационная безопасность: вопросы противодействия цифровым угрозам // Вестник РПА. № 4. 2024. С.145-154

[16] Россинская, Е.Р., Рядовский, И.А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. №5. С.699-709. / [Электронный ресурс] / Режим доступа: URL: https://cyberleninka.ru/article/n/kontseptsiya-vredonosnyh-programm-kak-sposobov-sovershen-iya-kompyuternyh-prestupleniy-klassifikatsii-i-tehnologii-protivopravnogo (дата обращения: 06.06.2025).

[17] Уголовное право России. Части общая и особенная: учебник / под ред. А.И. Рарога. 4-е изд. испр. и доп. М., 2021. 1040 с.

[18] Уголовное право. Особенная часть: учебник / под ред. А. В. Наумова, А. Г. Кибальника. 6-е изд. перераб. и доп., М: Издательство Юрайт, 2024. 447 с. / [Электронный ресурс] / Режим доступа: URL: https://urait.ru/bcode/535355 (дата обращения: 24.05.2025).

[19] Унукович, А.С. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Государственная служба и кадры. 2021. №4. С. 278-280 / [Электронный ресурс] / Режим доступа: URL: https://cyberleninka.ru/article/n/ponyatie-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy (дата обращения: 03.06.2025).

[20] Утверждён план реализации концепции противодействия киберпреступности / [Электронный ресурс] / Режим доступа: URL: http://government.ru/news/55975/ (дата обращения: 24.08.2025)

[21] Число приговоров за госизмену выросло в России в 2024 году почти в 4 раза, свидетельствует Судебный департамент при Верховном суде / [Электронный ресурс] / Режим доступа: URL: https://cdep.ru/ (дата обращения 21.06.2025).

[22] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 01.04.2025) / Электронный ресурс / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 12.07.2025).

[23] Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» от 30 декабря 2024 г. № 4154-р / [Электронный ресурс] / Режим доступа: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения 24.08.2025)

[24] Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» от 30 декабря 2024 г. № 4154-р / [Электронный ресурс] / Режим доступа: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения 24.08.2025)

[25] Указ Президента РФ от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации» / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 18.05.2025).

[26] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993

с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 18.05.2025).

[27] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ (ред. от 21.04.2025) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 18.05.2025).

[28] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 12.06.2025).

[29] Постановление Пленума Верховного суда Российской Федерации № 37 от 15.12.2022 г. «некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». / [Электронный ресурс] / Режим доступа: URL: https://www.vsrf.ru/documents/own/31913/ (дата обращения 05.06.2025).

[30] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ (27.11.2024) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_491931/#dst100011 (дата обращения: 12.06.2025).

[31] Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 31.07.2025) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.08.2025).

[32] Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» от 30 декабря 2024 г. № 4154-р / [Электронный ресурс] / Режим доступа: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения 24.08.2025)

[33] Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» от 30 декабря 2024 г. № 4154-р / [Электронный ресурс] / Режим доступа: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения 24.08.2025)

[34] Распоряжение Правительства РФ от 14.08.2025 N 2207-р «Об утверждении Плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_512576/f62ee45faefd8e2a11d6d88941ac66824f848bc2/ (дата обращения: 24.08.2025)

References:

[1] Bazhina, M.A., and I.V. Shakhnovskaia. Content and actual threats to ensuring information sovereignty: on the example of the Republic of Belarus and the Russian Federation // Vestnik Polotskogo gosudarstvennogo universiteta. Seriia D. Ekonomicheskie i iuridicheskie nauki, no. 2 (64) (2023): 63–67.

[2] Bastrykin: We propose to fix a new aggravating circumstance in the Criminal Code for cybercriminals / Rossiiskaia gazeta, January 14, 2025. https://rg.ru/2025/01/14/v-uk-rf-dlia-kiberprestupnikov-propishut-novoe-otiagchaiushchee-obstoiatelstvo.html.

[3] In Russia, in 2024, IT crimes have peaked over the past five years // TASS, August 24, 2025. https://tass.ru/proisshestviya/22978955/.

[4] Gribin, N.P., I.N. Pokhtiulina, D.I. Sedunov, and E.I. Sobolev. Information sovereignty: materials of scientific discussion//Russia and the world: scientific dialogue // no. 2 (4) (2022): 100–131.

[5] Dubinina, E.N., and Ia.A. Khorashavina. Information sovereignty of the Russian Federation // Advances in Law Studies 9, no. 3 (2021): 66–70.

[6] Efremov, A.A. State sovereignty in the context of digital transformation // Pravovedenie 63, no. 1 (2019): 47–61. https://doi.org/10.21638/spbu25.2019.103.

[7] Efremov, A.A. Information and legal mechanism for ensuring state sovereignty of the Russian Federation // Doktorskaia dissertatsiia. Moskva, 2021.

[8] Efremova, M.A. Criminal law protection of information security // Avtoreferat doktorskoi dissertatsii. Moskva, 2018.

[9] Il'iasov, S.M. Some problems of improving the regulatory legal regulation of information security issues in the Russian Federation // Iuridicheskii vestnik DGU 49, no. 1 (69) (2024): 41–49.

[10] Kulev, A.G. Crimes against the external security of the state: issues of legislative technology and differentiation of responsibility // Avtoreferat kandidatskoi dissertatsii. Samara, 2009.

[11] Letelkin, N.V. On the definition of signs and the concept of “information and telecommunication network” in domestic criminal legislation // Matters of Russian and International Law 8, no. 3A (2018): 216–221.

[12] Men’shikov, P.V. Topical aspects of ensuring the information sovereignty of Russia // Mezhdunarodnye kommunikatsii, no. 5 (2017). https://int-com-mgimo.ru/2017/2017-05/information-sovereignty-of-russia.

[13] Musikhin, G.I. “ Classifying theories of sovereignty as an attempt to overcome “conceptual selfishness” // Obshchestvennye nauki i sovremennost’, no. 1 (2010): 64–78.

[14] Naumov, V.B. «Internet and state sovereignty» In Stenogramma Pervoi vserossiiskoi nauchno-prakticheskoi konferentsii “Pravo i Internet: teoriia i praktika”, 20–23. Moskva, 2 noiabria 1999 goda.

[15] Poliakova, T.A. Legal support of state sovereignty and information security: issues of countering digital threats // Vestnik RPA, no. 4 (2024): 145–154.

[16] Rossinskaia, E.R., and I.A. Riadovskoi. The concept of malware as a means of committing computer crimes: classifications and technologies of illegal use // Vserossiiskii kriminologicheskii zhurnal, no. 5 (2020): 699–709. https://cyberleninka.ru/article/n/kontseptsiya-vredonosnyh-programm-kak-sposobov-sovershe niya-kompyuternyh-prestupleniy-klassifikatsii-i-tehnologii-protivopravnogo.

[17] Rarog, A.I., ed. Criminal law of Russia. General and special parts: textbook. 4th ed. Moskva: Prospekt, 2021.

[18] Naumov, A.V., and A.G. Kibal’nik, eds. Criminal law. Special part: textbook. 6th ed. Moskva: Iurait, 2024. https://urait.ru/bcode/535355.

[19] Unukovich, A.S. The concept of crimes committed using information and telecommunication technologies // Gosudarstvennaia sluzhba i kadry, no. 4 (2021): 278–280. https://cyberleninka.ru/article/n/ponyatie-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy.

[20] Approved plan for the implementation of the concept of countering cybercrime / Pravitel’stvo Rossii. Accessed August 24, 2025. http://government.ru/news/55975/.

[21] The number of sentences for treason increased almost 4 times in Russia in 2024, according to the Judicial Department at the Supreme Court // Sudebnyi departament pri Verkhovnom sude RF. Accessed June 21, 2025. https://cdep.ru/.

[22] Federal Law “On Information, Information Technology and Information Protection” dated 27.07.2006 No. 149-FZ (ed. 01.04.2025) /Electronic resource/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (date of request 12.07.2025).

[23] Order of the Government of the Russian Federation of December 30, 2024 No. 4154-r “On approval of the Concept of the state system for countering illegal acts committed using information and communication technologies” dated December 30, 2024 No. 4154-r/[Electronic resource]/Access mode: https://www.garant.ru/products/ipo/prime/doc/411152413/ (date of appeal 24.08.2025)

[24] Order of the Government of the Russian Federation of December 30, 2024 No. 4154-r “On approval of the Concept of the state system for countering illegal acts committed using information and communication technologies” dated December 30, 2024 No. 4154-r/[Electronic resource]/Access mode: https://www.garant.ru/products/ipo/prime/doc/411152413/ (date of appeal 24.08.2025)

[25] Decree of the President of the Russian Federation of 02.07.2021 No. 400 “On the National Security Strategy of the Russian Federation “/[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (date of reference: 18.05.2025).

[26] Constitution of the Russian Federation (adopted by popular vote 12.12.1993 with amendments approved during the all-Russian vote 01.07.2020) /[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (date of appeal: 18.05.2025).

[27] Code of Criminal Procedure of the Russian Federation dated 18.12.2001 No. 174-FZ (as amended by 21.04.2025) /[Electronic resource]/ Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (date of reference: 18.05.2025).

[28] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended 21.04.2025) (with amendments and additions, entry effective from 02.05.2025) /[Electronic resource]/ Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (date of access 12.06.2025).

[29] Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 of 15.12.2022 “on certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet. “/[Electronic resource]/ Access mode: URL: https://www.vsrf.ru/documents/own/31913/ (date of appeal 05.06.2025).

[30] Federal Law “On Amendments to the Criminal Code of the Russian Federation” dated 30.11.2024 No. 421-FZ (27.11.2024) /[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_491931/#dst100011 (date of reference: 12.06.2025).

[31] Criminal Code of the Russian Federation No. 63-FZ dated 13.06.1996 (as amended on 31.07.2025) /[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed on: 20.08.2025).

[32] Order of the Government of the Russian Federation of December 30, 2024 No. 4154-r "On approval of the Concept of the state system for countering illegal acts committed using information and communication technologies" dated December 30, 2024 No. 4154-r/[Electronic resource]/Access mode: https://www.garant.ru/products/ipo/prime/doc/411152413/ (date of appeal 24.08.2025)

[33] Order of the Government of the Russian Federation of December 30, 2024 No. 4154-r "On approval of the Concept of the state system for countering illegal acts committed using information and communication technologies" dated December 30, 2024 No. 4154-r/[Electronic resource]/Access mode: https://www.garant.ru/products/ipo/prime/doc/411152413/ (date of appeal 24.08.2025)

[34] Order of the Government of the Russian Federation of 14.08.2025 No. 2207-r "On approval of the Action Plan for the implementation of the Concept of the state system for countering illegal acts committed using information and communication technologies "/[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_512576/f62ee45faefd8e2a11d6d-88941ac66824f848bc2/ (date of reference: 24.08.2025)

