УДК 343 DOI: 10.17277/pravo.2023.04.pp.464-472

На основе проведенного анализа показано, что безопасность цифровой информации непосредственно связана с безопасностью цифровой сети передачи информации. Цифровые системы передачи информации внедряются по всей России, от малого бизнеса до крупных государственных учреждений, чтобы обеспечить безопасность, эффективность и надежность связи. Говоря о безопасности цифровой информации, невозможно обойти стороной безопасность цифровой системы передачи такой информации, поскольку преступления могут быть совершены как с помощью информационной сферы, элементом которой является цифровая система. Безопасность систем передачи цифровой информации контролируется различными организациями как на национальном, так и международном уровне в зависимости от их юрисдикции и сферы деятельности. Проанализировано законодательство, регулирующее отдельные аспекты правового закрепления и научного толкования цифровой информации, способов ее передачи.

Ключевые слова: цифровой суверенитет; цифровая информация; цифровая система передачи; безопасность; преступное посягательство; владелец; должностное лицо; доступ к информации; способы защиты.

Ирина Владимировна Семёнова, *канд. юрид. наук, преподаватель, ФГКВОУ ВО «Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации», Санкт-Петербург, Россия; 9053202867@mail.ru*

ЦИФРОВОЙ СУВЕРЕНИТЕТ И БЕЗОПАСНОСТЬ – ДОМИНАНТЫ НОВОГО МИРОПОРЯДКА: УГОЛОВНО-ПРАВОВОЙ АСПЕКТ

Введение

Всемирная паутина Интернета создала предпосылки для создания всемирного единого информационного пространства – единой глобальной цифровой экосистемы. В процессе развития в данном направлении всех стран появилось недоверие, что послужило катализатором в формировании цифрового суверенитета, который позволяет государству осуществлять контроль за свой цифровой средой, включая контроль за поставками и использованием всей цепочки поставок от данных до аппаратного и программного обеспечения (ПО). Внедрение в ПО шпионских программ, отслеживающих перемещение, прослушивающих и просматривающих со стороны недружественных государств, формирует тенденцию к усилению цифрового суверенитета, начиная от критически важных цифровых компонентов, таких как компьютерные чипы, вплоть до контроля над международным потоком данных граждан. Такие события приводят к фрагментации рынков высоких технологий.

Обсуждение

Дальнейшее развитие цифровой трансформации отмечается на государственном уровне, представляет угрозу не только для информации, но и личности, общества и государства в целом[1].

Цифровой суверенитет позволяет государству выступать в качестве конечного хранителя всей цифровой информации, поступающей в страну или покидающей ее, а также управляющего всеми информационными потоками внутри страны. Формирующийся авторитарный режим построения цифрового суверенитета есть приоритет национальной безопасности, связывая свободное перемещение информации с глобальными проблемами, в том числе с глобальными проблемами в сфере безопасности, неприкосновенности частной жизни, материальном благополучии, при этом поощряя меры, направленные на защиту прав человека во имя национальных интересов, и сохраняя важные политико-экономические и идеологические основы самоопределения, несмотря на устойчивую глобальную цифровую конвергенцию.

Безопасность систем передачи цифровых данных становится все более важным вопросом в современном мире. С развитием Интернета и других цифровых технологий постоянно растет потребность в законодательстве, методах и средствах для защиты конфиденциальности и безопасности передачи данных.

Развитие цифровых систем передачи информации в Российской Федерации находится в авангарде технологического прогресса с начала 2000-х годов. Это позволило значительно повысить уровень связи между людьми и ресурсами, а также повысить безопасность как отдельных лиц, так и организаций. Цифровые системы передачи информации внедряются по всей России, от малого бизнеса до крупных государственных учреждений, чтобы обеспечить безопасность, эффективность и надежность связи.

Мир, перешедший в цифровую среду, имеет четыре отличительные черты, которым присущи гигантские размеры и объемы: запоминающие устройства, скорости поиска и распознавания данных, расстояние и скорость передачи и распространения информации и знаний [6].

Говоря о безопасности цифровой информации, невозможно обойти стороной безопасность цифровой системы передачи такой информации, поскольку «преступления могут быть совершены как с помощью информационной сферы, элементом которой является цифровая система передачи, а также сама информация может выступать объектом и предметом посягательства» [7, с. 160]. Цифровая информация – это данные, хранящиеся в электронной (цифровой) форме в том или ином виде, например, в виде текстовых документов, изображений или видео. Она может передаваться с помощью различных методов, таких как беспроводные сети, спутниковые каналы связи или оптические кабели. Цифровая информация также может храниться на физических носителях, таких как жесткие диски или флэш-накопители, usb-накопители, CD/DVD или внешние жесткие диски

[1] Об утверждении государственной программы Российской Федерации «Информационное общество»: постановление Правительства РФ от 15.04.2014 № 313 (ред. от 29.04.2023) // Собрание законодательства РФ. 05.05.2014, № 18 (часть II). Ст. 2159.

или карты памяти на персональных компьютерах или серверах, расположенных в облаке.

Методы и устройства сбора, накапливания, хранения, обработки и передачи информации представляют собой тесно взаимосвязанные информационно-телекоммуникационные технологии, в связи с этим отсутствует необходимость разделения их на отдельные категории [1, с. 52].

Помимо собственника, законного владельца такой информации, законный доступ к цифровой информации контролируется федеральными органами исполнительной власти, которые имеют право получать доступ к любым электронным данным в целях расследования или преследования в уголовных делах. Кроме того, некоторые частные компании также могут иметь доступ к определенным цифровым данным, если они получили разрешение от государственных органов для определенных целей, таких как предоставление услуг или проведение исследовательских проектов.

Не стоит забывать о цифровых правах следователя, дознавателя на доступ к цифровой системе передачи и цифровой информации, которые могут быть определены в информационной системе и закреплены на законодательном уровне, а также определен способ доступа: открытый или закрытый, независимо от принадлежности системы [5, с. 111].

Наиболее распространенный тип цифровой информации известен как двоичные данные, которые состоят из единиц (1) и нулей (0).

Развитие цифровых систем передачи информации в России имеет множество преимуществ. Эти технологии не только позволяют ускорить обмен информацией между людьми и организациями, но и обеспечивают дополнительный уровень безопасности от несанкционированного доступа к конфиденциальным данным. Кроме того, эти системы позволяют более точно отслеживать активы, что помогает сократить потери, обеспечивая надлежащее управление ресурсами и их эффективное использование. Наконец, они помогают повысить эффективность работы, позволяя автоматизировать сложные задачи, практически не требуя вмешательства человека.

Безопасность систем передачи цифровой информации контролируется различными организациями как на национальном, так и международном уровне в зависимости от их юрисдикции и сферы деятельности. На национальном уровне эти организации состоят в основном из правительственных агентств, служб, на международном уровне – из Интерпола, Всемирного банка и т.д., причем каждая организация имеет свой собственный набор правил и положений, касающихся мер безопасности, связанных с системами передачи цифровой информации. Как правило, эти организации обеспечивают безопасность с помощью методов шифрования, используемых для защиты конфиденциальных данных от несанкционированного доступа [2], а также применяя различные механизмы аутентификации [3], такие как двухфакторная аутентификация и т.д., одновременно отслеживая сетевой трафик на предмет подозрительных действий, которые могут поставить под угрозу безопасность передачи данных по сетям, использующим такие технологии.

Цифровые системы передачи информации играют важную роль в обеспечении безопасности общества от преступников, которые стремят-

ся украсть конфиденциальные данные или финансовые ресурсы у частных лиц или организаций для собственной выгоды. Эти системы позволяют государственным учреждениям и правоохранительным органам контролировать деятельность в пределах своей юрисдикции с помощью технологий наблюдения, таких как камеры видеонаблюдения или программное обеспечение для распознавания лиц, установленное на компьютерах, используемых сотрудниками сетевой инфраструктуры организации. Кроме того, использование технологии шифрования помогает защитить конфиденциальные данные от перехвата при передаче через публичные сети, такие как Интернет или спутниковые каналы связи между странами. Передача цифровой информации возможна только с помощью цифровой системы передачи данных – системы, используемой для передачи цифровой информации из одной точки в другую.

Системы передачи цифровой информации состоят из нескольких различных элементов, включая аппаратные компоненты, такие как маршрутизаторы и коммутаторы; программные приложения, такие как брандмауэры; протоколы, используемые компьютерами при взаимодействии друг с другом по сети; алгоритмы шифрования, используемые для защиты данных, передаваемых по сети; методы аутентификации, используемые для проверки личности пользователя; средства мониторинга, позволяющие отслеживать активность в сетевой инфраструктуре организации. Она может состоять из набора аппаратных и программных компонентов, которые работают вместе для передачи, хранения и приема цифровых данных. Эти компоненты включают компьютеры, модемы, терминалы, коммутаторы, кабели и другие сетевые устройства. Цифровые системы передачи данных могут включать в себя телекоммуникационные сети, системы спутниковой связи, с целью обеспечения доступа в Интернет и системы видеонаблюдения, а также распределенные базы данных, позволяющие безопасно хранить большие объемы структурированных данных; виртуальные частные сети (vpn), обеспечивающие безопасное соединение между удаленными машинами, расположенными в любой точке мира; услуги облачных вычислений, предоставляющие доступ к вычислительным мощностям по требованию через интернет-соединения.

Преступные действия направлены на осуществление атак цифровых систем передачи информации с момента их появления, чтобы получить доступ к конфиденциальным данным, принадлежащим частным лицам или организациям, без их ведома и согласия. Распространенные методы совершения преступлений включают в себя тактику социальной инженерии, например, фишинговые письма, содержащие вредоносные вложения, которые рассылаются большому количеству пользователей в надежде обманом заставить их загрузить вредоносное ПО на свой компьютер; атаки типа «отказ в обслуживании», когда несколько запросов делаются одновременно, так что сервер, на котором расположен сайт, становится перегруженным и не может обработать их все, что приводит к сбою; атаки типа «человек посередине», когда злоумышленник перехватывает сообщения, передаваемые двумя легитимными пользователями, изменяя содержимое, которым они обмениваются, и создавая видимость нормального общения между двумя сторонами. Достаточно подробно о киберпреступности: ее

виды, способы совершения и способы противостояния и особенности международного сотрудничества в этой сфере, приведены в книге [4].

Важно признать необходимость разработки безопасной системы передачи цифровой информации для предотвращения криминальных атак, описанных выше. Это включает в себя реализацию мер по обеспечению надлежащей аутентификации при предоставлении доступа к определенным областям системы, создание алгоритмов шифрования конфиденциальных данных перед их отправкой в публичные сети, установку межсетевых экранов, ограничивающих входящий трафик из неизвестных источников, регулярное обновление программных приложений для обеспечения применения последних исправлений безопасности, использование средств мониторинга для обнаружения любой подозрительной активности, происходящей в сетевой инфраструктуре.

Для безопасности в системах передачи цифровых данных всегда должны использоваться методы шифрования, чтобы защитить конфиденциальные данные, передаваемые по сетям, от несанкционированного доступа посторонних лиц. Методы шифрования включают в себя кодирование сообщений, передаваемых по сети, таким образом, что только те, кто обладает ключами, могли бы расшифровать их, что затрудняет доступ хакеров или неавторизованных пользователей. Меры безопасности также должны включать процедуры аутентификации, такие как двухфакторная аутентификация, при которой пользователям требуется не только имя пользователя, но и дополнительный код, отправляемый через текстовое сообщение, прежде чем они будут допущены в сеть. Наконец, в сетях всегда должны быть установлены брандмауэры, чтобы блокировать вредоносные атаки и при этом пропускать законный трафик.

Кроме того, наличие эффективной политики, информирующей сотрудников о потенциальных угрозах, поощряющей их сохранять бдительность и сообщать о любом подозрительном поведении, связанном с вопросами кибербезопасности, помогает минимизировать риск возникновения кибератак на территории организации. Эффективность можно повысить с помощью таких методов оптимизации, как снижение потерь пакетов, минимизация задержек, повышение пропускной способности и т.д., обеспечивая тем самым лучшую производительность в целом без ущерба для надежности. Надежность должна обеспечиваться с помощью механизмов резервирования, таких как избыточные аппаратные компоненты, программные решения, такие как кластеризация и т.д., обеспечивая тем самым бесперебойную работу, даже если один компонент выйдет из строя в силу непредвиденных обстоятельств. Кроме того, необходимо регулярно создавать резервные копии, чтобы любые потерянные/поврежденные файлы можно было быстро восстановить без ущерба для непрерывности обслуживания.

Помимо предотвращения преступной деятельности, о которой говорилось выше, наличие надежной цифровой системы передачи информации является критически важным для обеспечения общественной безопасности во время кризисов, стихийных бедствий, чрезвычайных ситуаций, происходящих на региональном и национальном уровнях. Это позволяет властям своевременно рассылать уведомления населению пострадавших рай-

онов, информируя их о том, какие шаги необходимо предпринять, чтобы оставаться в безопасности во время ситуации, а также предоставлять информацию о самой ситуации, как власти решают проблему в кратчайшие сроки, тем самым минимизирую потери, материальный ущерб, нанесенный региону, пострадавшему от инцидента, о котором говорилось ранее, важность наличия безопасного надежного способа связи между различными вовлеченными организациями нельзя недооценивать в наше время, особенно учитывая текущее состояние межконтинентального взаимодействия в современном мире, где кибератаки становятся все более частыми и изощренными с каждым годом, поэтому необходимо уделять самое пристальное внимание разработке безопасного надежного способа передачи информации в цифровом формате различными вовлеченными организациями, чтобы убедиться, что граждане страны остаются в безопасности все время, независимо от того, находится ли человек дома или заграницей.

В России к нормативной правовой базе, регулирующей использование и меры безопасности, связанные с цифровыми системами передачи информации, можно отнести Доктрину информационной безопасности Российской Федерации, которая определяет составляющую по обеспечению национальной безопасности в информационной сфере[2]; Федеральный закон № 152-ФЗ об информационных технологиях, который требует от всех пользователей, участвующих в обработке электронных документов на территории России, соблюдения определенных требований в отношении методов шифрования, используемых для защиты конфиденциальных данных от несанкционированного доступа и определяет меры технической защиты, при передаче по сети конфиденциальной личной или корпоративной информации[3]; Федеральный закон №149-ФЗ о защите от несанкционированного доступа, который обязывает всех пользователей, участвующих в обработке электронных документов на территории России, обеспечить защиту любых передаваемых конфиденциальных данных с помощью соответствующего метода шифрования; Федеральный закон № 152-ФЗ[4]; Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, определяющий принципы, на основе которых строится защита информации[5]; Приказ № 472, изданный Министерством связи и массовых коммуникаций Российской Федерации, который устанавливает дополнительные требования к аутентификации пользователей при доступе

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50. Ст. 7074.

[3] Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 01.03.2023): Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) // Собрание законодательства РФ. 31.07.2006, № 31 (1 ч.). Ст. 3448.

[4] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) // Собрание законодательства РФ. 31.07.2006, № 31 (1 ч.). Ст. 3451.

[5] Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Текст: электронный. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g (дата обращения: 01.12.2023).

к сетям с использованием компьютера, подключенного напрямую через кабельные соединения[6] и т.д., а также определяет порядок безопасного хранения паролей, чтобы не могли быть доступны третьим лицам без разрешения и др. Однако, к сожалению, в настоящее время комплексная законодательная поддержка этого вопроса недостаточна во многих областях.

Одна из основных проблем действующего законодательства заключается в том, что оно не учитывает сложности цифровых систем передачи данных. Законы часто слишком широки или расплывчаты, что затрудняет эффективную защиту пользователей от злоумышленников, которые могут попытаться использовать уязвимости в этих системах. Кроме того, эти законы часто не содержат адекватного руководства о том, как компании должны обращаться с данными пользователей и какие меры должны быть приняты для обеспечения их безопасности.

Еще одна проблема, связанная с существующей законодательной поддержкой цифровых систем передачи данных, заключается в том, что она не учитывает развитие технологий и новые угрозы, которые могут возникнуть в связи с ними. По мере развития технологий будут появляться новые угрозы, которые могут подвергнуть риску данные пользователей, если не будут должным образом учтены в законодательстве. Законы должны регулярно обновляться по мере появления новых технологий, чтобы не оставлять пользователей беззащитными. Наконец, существует недостаток правоприменения, когда речь идет о существующих законах, касающихся систем передачи цифровых данных. Без надлежащего исполнения этих законов субъекты могут чувствовать себя менее заинтересованными или мотивированными следовать им, что может привести к дальнейшим проблемам безопасности.

Заключение

В целом, несмотря на некоторые попытки обеспечить законодательную поддержку безопасности цифровых систем передачи данных, необходимо сделать гораздо больше для того, чтобы права пользователей на конфиденциальность и безопасность были действительно защищены в Интернете. Важно, чтобы законодатели признали эту необходимость и работали над созданием более комплексных правил, которые будут соответствовать развивающимся технологиям и возникающим угрозам, чтобы не оставлять пользователей уязвимыми при использовании этих услуг в Интернете. Представляется, что кибербезопасность следует отождествлять с информатизацией. Национальная безопасность не может существовать в современном мире без кибербезопасности, а без информатизации нет модернизации общества и государства. Развитие цифровой безопасности это не только вопрос суверенитета, но и контроля над информацией и людьми. Работа с общественным мнением в Интернете должна быть важнейшей задачей пропаганды и идеологической работы с обществом.

[6]Об утверждении формата электронной подписи, обязательного для реализации всеми средствами электронной подписи: Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14.09.2020 № 472. Текст: электронный. URL: http://publication.pravo.gov.ru/Document/View/0001202010290040 (дата обращения: 01.12.2023).

Список литературы

1. **Аносов А. В.** Некоторые аспекты понятийного аппарата цифровой криминологии // Цифровая трансформация системы МВД России: сб. науч. ст. по материалам Международного форума. В 2-х частях, Москва, 20 октября 2022 года. Часть 1. М., 2022. С. 48 – 55.

2. **Васильева И. Н.** Криптографические методы защиты информации: учебник и практикум для вузов. М.: Юрайт, 2023. 349 с.

3. **Викторов А. С.** Механизм аутентификации и авторизации для обеспечения безопасности периферийного сервиса // Информационно-экономические аспекты стандартизации и технического регулирования. 2018. № 5(45). С. 150 – 159.

4. **Жданов Ю. Н., Кузнецов С. К., Овчинский В. С.** Кибермафия. Мировые тенденции и международное противодействие: монография. М.: Норма, 2022. 182 с.

5. **Першин А. Н.** Цифровые права лиц, осуществляющих предварительное расследование // Вестник Университета имени О. Е. Кутафина. 2021. № 2(78). С. 108 – 115.

6. **Ракитов А. И.** Человек в оцифрованном мире // Философские науки. 2016. № 6. С. 32 – 46.

7. **Семенова И. В.** Цифровая информация как предмет посягательства преступлений в сфере компьютерной информации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2022. Т. 8, № 4. С. 158 – 165.

References

1. **Anosov A.V.** *Tsifrovaya transformatsiya sistemy MVD Rossii: sb. nauch. st. po materialam Mezhdunarodnogo foruma* [Digital transformation of the system of the Ministry of Internal Affairs of Russia: a collection of scientific articles based on materials from the International Forum], In 2 parts, Moscow, 20 Oct. 2022. Part 1, Moscow, 2022, pp. 48-55. (In Russ.)

2. **Vasil'yeva I.N.** *Kriptograficheskiye metody zashchity informatsii: uchebnik i praktikum dlya vuzov* [Cryptographic methods of information protection: textbook and workshop for universities], Moscow: Yurayt, 2023, 349 p. (In Russ.)

3. **Viktorov A.S.** [Authentication and authorization mechanism to ensure the security of peripheral services], *Informatsionno-ekonomicheskiye aspekty standartizatsii i tekhnicheskogo regulirovaniya* [Information and economic aspects of standardization and technical regulation], 2018, no. 5(45), pp. 150-159. (In Russ., abstract in Eng.)

4. **Zhdanov Yu.N., Kuznetsov S.K., Ovchinskiy B.S.** *Kibermafiya. Mirovyye tendentsii i mezhdunarodnoye protivodeystviye: monografiya* [Cybermafia. World trends and international counteraction: monograph], Moscow: Norma, 2022, 182 p. (In Russ.)

5. **Pershin A.N.** [Digital rights of persons carrying out preliminary investigation], *Vestnik Universiteta imeni O. Ye. Kutafina* [Bulletin of the O. E. Kutafin University], 2021, no. 2(78), pp. 108-115. (In Russ., abstract in Eng.)

6. **Rakitov A.I.** [Man in a digitalized world], *Filosofskiye nauki* [Philosophical Sciences], 2016, no. 6, pp. 32-46. (In Russ., abstract in Eng.)

7. **Semenova I.V.** [Digital information as a subject of encroachment of crimes in the field of computer information], *Uchenyye zapiski Krymskogo federal'nogo universiteta imeni V. I. Vernadskogo. Yuridicheskiye nauki* [Scientific notes of the Crimean Federal University named after V. I. Vernadsky. Legal sciences], 2022, vol. 8, no. 4, pp. 158-165. (In Russ., abstract in Eng.)

Digital Sovereignty and Security Dominants of the New World Order: Individual Questions. Criminal-Legal Aspect

I. V. Semenova, *Cand. Sci. (Law), Lecturer,*
St. Petersburg Military Order of Zhukov Institute
of National Guard Troops of the Russian Federation,
St. Petersburg, Russia;
9053202867@mail.ru

Based on the analysis, the author comes to the conclusion that the security of digital information is directly related to the security of the digital information transmission network. Digital information transmission systems are being implemented throughout Russia, from small businesses to large government agencies, to ensure the security, efficiency and reliability of communications. Speaking about the security of digital information, it is impossible to ignore the security of the digital transmission system of such information, since crimes can be committed both with the help of the information sphere, an element of which is the digital system The security of digital information transmission systems is controlled by various organizations both at the national and international level, depending on their jurisdiction and sphere of activity. In the article, the author analyzes the legislation regulating certain aspects of the legal consolidation and scientific interpretation of digital information, methods of its transmission.

Keywords: digital sovereignty, digital information, digital transmission system, security, criminal encroachment, owner, official, access to information, methods of protection.

Статья поступила в редакцию 01.06.2023

При цитировании использовать:

Семёнова И.В. Цифровой суверенитет и безопасность – доминанты нового миропорядка: уголовно-правовой аспект // Право: история и современность. 2023. Т. 7, № 4. С. 464 – 472. doi: 10.17277/pravo.2023.04.pp.464-472