Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 3. – С. 488–493.

УДК: 343

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

Семёнова И. В.

Санкт–Петербургский ордена Жукова институт войск национальной гвардии

Безопасность цифровой информации непосредственно связана с безопасностью цифровой сети передачи информации. В России активно внедряются цифровые технологии для обмена данными в предприятиях различного масштаба и госорганах, что способствует улучшению связи и её защиты. Вопросы защиты таких систем от киберпреступлений регулируются национальными и международными институтами, в зависимости от их компетенции и области действия. В статье автором анализируется 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.

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 цифровой среды, включая контроль поставок и использования всей цепочки поставок от данных до аппаратного и программного обеспечения. Внедрение в ПО технические устройства шпионских программ недружественными государствами, позволяющие отслеживать перемещение, прослушивать и просматривать деятельность наших граждан, формирует тенденцию к усилению цифрового суверенитета, начиная от критически важных цифровых компонентов, таких как компьютерные чипы вплоть до контроля над международным потоком данных граждан. Эти события приводят к фрагментации рынков высоких технологий. Дальнейшее развитие цифровой трансформации, отмечается на государственном уровне, представляет угрозу не только для информации, но и личности, обществу и государству 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 также является приоритетом национальной безопасности, связывая свободное перемещение информации с глобальными проблемами, в том числе с проблемами в сфере безопасности, неприкосновенности частной жизни, материального благополучия. 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.

В сфере цифровых коммуникаций в современности актуализируется вопрос защиты информации. Расширение сети Интернет и прогресс в области цифровых инноваций усиливают потребности в правовых нормах и технологических решениях

для обеспечения приватности и надежности обмена данными. С начала XXI в. Россия активно применяет последние достижения в области цифровой коммуникации. Этот процесс способствовал усилению взаимодействия между гражданами и улучшению уровня защиты данных для частных и корпоративных пользователей. Распространение цифровых технологий охватывает различные секторы страны, способствуя повышению эффективности и надежности информационного обмена.

В цифровом пространстве существуют 4 основных характеристики, которые отличаются внушительными масштабами и объемами: это возможности хранения информации, быстрота её поиска и идентификации, а также дистанция и скорость, с которой данные и знания передаются и распространяются [2]. Обсуждая защиту данных в интернете, нельзя игнорировать безопасность сетевых каналов, ведь преступления могут быть осуществлены с использованием информационных технологий или же сама информация может стать целью атаки [3, с. 160]. Инструменты и системы для сбора данных, их хранения, обработки и распространения настолько взаимозависимы, что их разделение на разные классы не требуется. Они объединены в единый комплекс инфо- и телекоммуникационных технологий [4, с. 52].

Не только владелец информации может распоряжаться ею. Государственные структуры, в рамках своих полномочий, также имеют доступ к электронным данным для следственных действий в рамках уголовного расследования. Определенные частные организации могут получить право работать с такими данными после одобрения со стороны властей для выполнения услуг или научных работ. Необходимо помнить, что закон может устанавливать особые полномочия для сотрудников правоохранительных органов, касающиеся входа в электронные сети и работы с информацией в них. Правила доступа к подобным системам, будь то открытый или ограниченный доступ, должны быть четко прописаны и закреплены на уровне законодательства [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.

Цифровое шифрование и технологические средства мониторинга, такие как видеокамеры и распознавание лиц, ключевые для защиты от хакеров и преступников. Они помогают правоохранителям следить за порядком в своей юрисдикции. Шифрование данных обеспечивает их безопасность при передаче по Интернету и другим сетям. Эти системы защиты необходимы для передачи информации на расстояние.

В защите своих цифровых данных заинтересованы различные организации. Такая задача ставится перед специализирующимися на этом ведомствами, а первоначальными вопросами безопасности – Интерпол и Всемирный банк, разрабатывая стандарты и правила предотвращения неавторизованного доступа к информации, применяя при этом систему шифрования [6], в том числе применяя механизмы аутентификации [7, с. 15].

Системы передачи цифровой информации состоят из различных элементов, включая аппаратные компоненты, протоколы, алгоритмы и методы аутентификации, средства мониторинга активности в сетевой инфраструктуре. Они могут состоять из набора аппаратных и программных компонентов, работающие синхронно и служат для передачи, хранения и приема цифровых данных. Эти элементы состоят из компьютеров, модемов, терминалов, коммутаторов, кабелей и других сетевых устройств. Цифровые технологии включают в себя различные сети, в том числе спутниковую связь, для подключения к сети, системы камер наблюдения. Также к ним относятся децентрализованные хранилища для защищенного сохранения данных, VPN для надежного взаимодействия между компьютерами на расстоянии; облачные сервисы, предлагающие мощности для обработки информации через интернет. Преступные действия направлены на осуществление атак на цифровые системы передачи информации существуют с момента появления последних, цель которых заключается в получении доступа к конфиденциальным данным, без ведома и согласия собственника. 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, при этом создавая видимость нормального общения между двумя сторонами.

В работе авторов Ю. Н. Жданова, С. К. Кузнецова и В. С. Овчинского анализируются типы киберпреступлений, методы их осуществления, а также меры борьбы с ними. Отдельное внимание уделено аспектам международного взаимодействия в борьбе с киберпреступностью [8]. Представляется, что важность разработки защищенной системы для пересылки цифровой информации, остается актуальной по настоящее время. Превентивными мерами по защите информации являются проверка подлинности пользователей, шифрование данных перед их передачей в интернет, установка фаерволов для фильтрации входящего трафика, обновление ПО для исправления уязвимостей и наблюдение за сетью на предмет необычных действий.

Методы шифрования включают в себя кодирование сообщений, передаваемых по сети, таким образом, чтобы только те, кто обладает ключами, могли расшифровать их, что способствует затруднению доступ хакеров или неавторизованных пользователей к ним. Меры безопасности также могут 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. В сетях всегда должны быть установлены брандмауэры, чтобы блокировать вредоносные атаки, но при этом пропускать законный трафик. Кроме того, наличие эффективной политики, информирующей сотрудников о потенциальных угрозах в организациях, убеждать сотрудников быть бдительными и уведомлять о подозрительных действиях в области IT-безопасности. Улучшение работы сети достигается за счет оптимизации передачи данных, уменьшения задержек и увеличения пропускной способности. Для

получения бесперебойной работы необходимо установить запасные системы и ПО для автоматического переключения при сбоях, при этом систематически обновлять резервные копии, чтобы в случае потери данных обеспечить быстрое восстановление сервиса. Помимо предотвращения преступной деятельности, о которой говорилось выше, наличие надежной цифровой системы передачи информации является важным для обеспечения общественной безопасности во время кризисов, стихийных бедствий, чрезвычайных ситуаций.

Наличие качественно работающей системы позволит при наступлении форс-мажорных обстоятельств, своевременно разослать уведомления населению пострадавших районов, информируя их о том, какие шаги необходимо предпринять, чтобы оставаться в безопасности вовремя ситуации, а также предоставлять информацию о самой ситуации, тем самым минимизирую потери, материальный ущерб, нанесенный региону, пострадавшему от инцидента. Важность наличия надежного способа связи между 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.

В связи с этим необходимо уделять пристальное внимание разработке безопасного надежного способа передачи информации в цифровом формате организациями, чтобы убедиться, что граждане страны остаются в безопасности все время, независимо от территориально нахождения человека. К нормативной правовой базе, регулирующей использование и меры безопасности, связанные с цифровыми системами передачи информации, отнесем Доктрину информационной безопасности РФ, которая определяет составляющую по обеспечению национальной безопасности в информационной сфере [9]; ФЗ № 152-ФЗ об информационных технологиях, определяющий пользователям, участвующих в обработке электронных документов, соблюдения определенных требований в отношении возможностей шифрования, используемые для защиты информации, и определяет меры технической защиты, при передаче по сети конфиденциальной личной или корпоративной информации [10].

ФЗ №149-ФЗ о защите от несанкционированного доступа, который обязывает всех пользователей, участвующих в обработке электронных документов на территории РФ. Применение алгоритмов криптографии для надежной передачи данных, предписывается законом ФЗ №152, устанавливает основные принципы обеспечения безопасности информационных систем и компьютерного оборудования от неавторизированных действий. Закон, определяющий принципы, на основе которых строится защита цифровой информации [12]. Приказ №472 Минсвязи и массовых коммуникаций РФ, устанавливающий дополнительные требования к аутентификации пользователей при доступе к сетям с использованием компьютера, подключенного напрямую через кабельные соединения [13], в т.ч. определяя порядок безопасного хранения паролей, чтобы не могли быть доступны третьи лица без разрешения и другие, но, настоящее время законодательное регулирование этого вопроса, недостаточна во многих областях. Основная сложность регулирования связана с неспособностью законов адекватно регулировать тонкости работы цифровых коммуникаций. Нередко законодательные акты нечетки и обобщенные, что мешает защите пользователей от атак киберпреступников, эксплуатирующих системные уязвимости. К тому же, законы редко определяют алгоритм действий компаниям по обработке и защите персональных данных клиентов.

Существующее правовое регулирование в сфере цифровой передачи информации не в полной мере может адекватно отражать технологический прогресс и возникающие в связи с этим новые виды рисков для пользователей. Необходима своевременная адаптация законов так, чтобы они предвосхищали потенциальные угрозы, связанные с инновациями в области ИТ. Законы должны регулярно обновляться по мере появления новых технологий. Есть и пробелы, существующие в системе правоприменения, когда речь идет о существующих законах, касающихся систем передачи данных. Без надлежащего исполнения этих законов субъекты могут чувствовать себя менее заинтересованными или мотивированными следовать им, что может привести к дальнейшим проблемам безопасности. В целом, несмотря на некоторые попытки обеспечить законодательную поддержку безопасности цифровых систем передачи данных, необходимо сделать гораздо больше для того, чтобы конфиденциальность и безопасность были действительно защищены в сети. Важно, чтобы законодатели признали эту необходимость и работали над созданием более комплексные правила, которые будут соответствовать развивающимся технологиям и возникающим угрозам, чтобы не оставлять пользователей уязвимыми при использовании этих услуг в Интернете.

Представляется, что цифровую безопасность следует отождествлять с информатизацией. Национальная безопасность не может существовать 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 сети должна быть важнейшей задачей пропаганды и идеологической работы с обществом.

Список литературы:

1. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 29.04.2023) «Об утверждении государственной программы Российской Федерации "Информационное общество"» // Собрание законодательства РФ.2014. № 18 (часть II), ст. 2159.
2. Ракитов А.И. Человек в оцифрованном мире/А.И. Ракитов// Философские науки. 2016. № 6.С.32-46.
3. 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.
4. Аносов А. В. Некоторые аспекты понятийного аппарата цифровой криминологии / А. В. Аносов // Цифровая трансформация системы МВД России: Сборник научных статей по материалам Международного форума. В 2-х частях, Москва, 20 октября 2022 года / под редакцией И.Г. Чистобородова. Том Часть 1. – Москва: Академия управления МВД Российской Федерации, –2022. – С. 48-55.
5. Першин А. Н. Цифровые права лиц, осуществляющих предварительное расследование // Вестник Университета имени О. Е. Кутафина. – 2021. – №2 (78). – С 108-115.
6. Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Москва: Издательство Юрайт, 2023. –349 с.
7. Викторов А. С. Механизм аутентификации и авторизации для обеспечения безопасности периферийного сервиса // Информационно-экономические аспекты стандартизации и технического регулирования. – 2018. – № 5(45). – С. 15.
8. Жданов Ю. Н. Кибермафия. Мировые тенденции и международное противодействие: монография / Ю. Н. Жданов, С. К. Кузнецов, В. С. Овчинский; вступ. Ст. О. В. Храмова. – М.: Норма, 2022. – 182 с.
9. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» //Собрание законодательства Российской Федерации. 2016. г. № 50 ст. 7074.
10. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // Собр.законодательства РФ. 2006. № 31 (1 ч.), ст. 3448.
11. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (1 ч.), ст. 3451.
12. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. // URL.: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g.

13. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14.09.2020 № 472 «Об утверждении Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи» // URL.: http://publication.pravo.gov.ru/Document/View/0001202010290040.

Semenova I.V. Digital sovereignty and security dominants of the new world order: individual questions. Criminal-legal aspect // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 3. – P. 488–493.

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.

Spisok literatury:

1. Postanovlenie Pravitel`stva RF ot 15.04.2014 № 313 (red. ot 29.04.2023) «Ob utverzhdenii gosudarstvennoj programmy` Rossijskoj Federacii "Informacionnoe obshhestvo"» // Sobranie zakonodatel`stva RF.2014. № 18 (chast` II), st. 2159.
2. Rakitov A. I. Chelovek v ocifrovannom mire/A.I. Rakitov // Filosofskie nauki. – 2016. – № 6. – S. 32-46.
3. Semenova I. V. Cifrovaya informaciya kak predmet posyagatel`stva prestuplenij v sfere komp`yuternoj informacii // Ucheny`e zapiski Kry`mskogo federal`nogo universiteta imeni V.I. Vernadskogo. Yuridicheskie nauki. – 2022. – T. 8, № 4. – S. 158-165.
4. Anosov A. V. Nekotory`e aspekty` ponyatijnogo apparata cifrovoj kriminologii // Cifrovaya transformaciya sistemy` MVD Rossii: Sbornik nauchnyx statej po materialam Mezhdunarodnogo foruma. V 2-x ch., M., 20.10.2022 / pod red. I.G. Chistoborodova. T. 1. – M.: Akademiya upravleniya MVD RF, 2022. – S. 48-55.
5. Pershin A. N. Cifrovy`e prava licz, osushhestvlyayushhix predvaritel`noe rassledovanie // Vestnik Universiteta imeni O. E. Kutafina. 2021. №2 (78). – S 108-115.
6. Vasil`eva I. N. Kriptograficheskie metody` zashhity` informacii: uchebnik i praktikum dlya vuzov / I. N. Vasil`eva. Moskva: Izdatel`stvo Yurajt, 2023. 349 s.
7. Viktorov A. S. Mexanizm autentifikacii i avtorizacii dlya obespecheniya bezopasnosti periferijnogo servisa/Informacionno-e`konomicheskie aspekty standartizacii i texnicheskogo regulirovaniya. 2018.№5(45).S. 15.
8. Zhdanov Yu. N. Kibermafiya. Mirovy`e tendencii i mezhdunarodnoe protivodejstvie: monografiya / Yu. N. Zhdanov, S. K. Kuzneczov, B. S. Ovchinskij; vstu. Stat. O. V. Xramova. Moskva: Norma, 2022. – 182 s.
9. Ukaz Prezidenta RF ot 5 dekabrya 2016 g. № 646 «Ob utverzhdenii Doktriny` informacionnoj bezopasnosti Rossijskoj Federacii» //Sobranie zakonodatel`stva Rossijskoj Federacii. 2016. g. № 50 st. 7074.
10. Federal`ny`j zakon ot 27.07.2006 № 149-FZ (red. ot 29.12.2022) «Ob informacii, informacionny`x texnologiyax i o zashhite informacii» // Sobranie zakonodatel`stva RF. 2006. № 31 (1 ch.), st. 3448.
11. Federal`ny`j zakon ot 27.07.2006 № 152-FZ (red. ot 06.02.2023) «O personal`ny`x danny`x» // Sobranie zakonodatel`stva RF. 2006. № 31 (1 ch.), st. 3451.
12. Rukovodyashhij dokument. Reshenie predsedatelya Gostexkomissii Rossii ot 30 marta 1992 g. // URL.: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g.
13. Prikaz Ministerstva cifrovogo razvitiya, svyazi i massovy`x kommunikacij Rossijskoj Federacii ot 14.09.2020 № 472 «Ob utverzhdenii Formata e`lektronnoj podpisi, obyazatel`nogo dlya realizacii vsemi sredstvami e`lektronnoj podpisi» // URL.: http://publication.pravo.gov.ru/Document/View/0001202010290040.
.