DOI: 10.34773/EU.2024.4.2

Цифровой суверенитет и безопасность в эпоху информации: вызовы и стратегии развития России*

Digital Sovereignty and Security in the Information Age: Challenges and Strategies for Russia's Development

Э. МУХАМАДИЕВА, Н. ШАБАНОВ

Мухамадиева Эльвира Фанировна, канд. экон. наук, доцент ФГБОУ «Уфимский государственный нефтяной технический университет». E-mail: teffi83@yandex.ru
Шабанов Никита Игоревич, магистрант ФГБОУ «Уфимский государственный нефтяной технический университет». E-mail: fifabatl@yandex.ru

В рамках этой статьи мы рассматриваем вопросы, которые связаны с проблемами и стратегией укрепления цифрового суверенитета на территории России. Актуальность исследования обусловлена негативными тенденциями, которые включают в себя санкционную политику недружественных стран, распространение экстремистской информации, а также рост числа утечек информации и киберугроз. Для понимания угроз необходимо определить последствия санкций и текущую деятельность, которая осуществляется правительством в рамках решения этих проблем.
***Ключевые слова**: информационная безопасность, сетевой суверенитет, отечественное программное обеспечение, цифровые технологии, защита данных, киберпреступность.*

In this article, we are considering issues that are related to the problems and strategy of strengthening digital sovereignty on the territory of Russia; the problems are associated with negative trends, which include the sanctions policy of unfriendly countries, the spread of extremist information, as well as the growth of information leaks and cyber threats. To provide threats, it is necessary to determine the consequences of sanctions and the ongoing activities that are carried out by the government as part of regulating these problems.
***Key words**: information security, network sovereignty, domestic software, digital technologies, data protection, cybercrime.*

Введение

Актуальность темы данной научной работы обуславливается все большим внедрением цифровых технологий во все сферы жизни человеческого общества, что порождает новые, еще недостаточно урегулированные законодательством правоотношения. Вместе с открытием множества возможностей внедрение цифровых технологий порождает новые проблемы и вопросы, касающиеся, например, безопасности данных пользователей Сети, увеличивающееся количество киберпреступлений, неограниченный поток информации и в целом возникновение новых, еще недостаточно урегулированных законодательством отношений.

Указанные вопросы вызывают бурные дискуссии в научных кругах. Например, общие аспекты регулирования цифровых отношений раскрывает в своих работах Е.А. Иерусалимская. Понятие свободы в социальных сетях и спорные вопросы ее рамок рассматриваются в трудах С.А. Зинченко. Аспектам безопасности персональных данных пользователей всемирной сети, а также их сохранности при использовании VPN-сервисов посвящены научные статьи Е.В. Зайнутдиновой и Е.О. Купач.

Целью данной научной работы является исследование текущего направления развития Российской Федерации в рамках повышения информационной безопасности населения и страны, достижения цифрового суверенитета. Поставлены следующие задачи:

* *Ссылка на статью*: Мухамадиева Э.Ф., Шабанов Н.И. Цифровой суверенитет и безопасность в эпоху информации: вызовы и стратегии развития России // Экономика и управление: научно-практический журнал. 2024. № 4. С. 10–15. DOI: 10.34773/EU.2024.4.2.

– изучить вопросы развития сетевого суверенитета и информационной безопасности;

– рассмотреть процесс программного импортозамещение и его внедрения в деятельность российских организаций;

– выявить слабые стороны и проблемы политики информационного суверенитета, сформулировав подходы к их устранению.

Методы

Методологическую основу исследования представляет совокупность общенаучных и частнонаучных методов изучения. В рамках данной работы была выполнены:

1. Мониторинг и оценка действующего законодательства на предмет изменения регулирования в исследуемой сфере деятельности, анализ судебной практики с целью анализа практического применения и оценки реальных случаев нарушения законодательства;

2. Сравнительный анализ, определение эффективных способов преодоления санкционной политики, связанной с программным обеспечением;

3. Анализ экспертных мнений, связанных с текущим регулированием распространения запрещенной информации, способов обхода запретов доступа к запрещенным ресурсам.

Результаты

Тенденции развития российского общества в условиях необходимости обеспечения информационной безопасности были сформулированы в Указе Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»: с одной стороны – обеспечение сетевого суверенитета, т.е. создание цифрового пространства, защищенного от влияния недружественных стран, с другой стороны – усиление позиций российского программного обеспечения (ПО) на рынке и его активное внедрение в деятельность предприятий [11].

Первое направление предполагает обеспечение информационной безопасности граждан посредством блокировки доступа к запрещенной информации, борьбы с киберпреступностью.

Второе направление – укрепление отечественного рынка информационных продуктов. В период санкций этот вопрос стоит достаточно остро. Во-первых, многие иностранные производители ПО прекратили торговые отношения с Российской Федерацией, что затрудняет использование и обслуживание иностранного программного обеспечения. Во-вторых, существует немалый риск утечки личных данных пользователей зарубежных компьютерных программ, что является особенно опасным для объектов критической информационной инфраструктуры.

На данный момент имеется тенденция к изменению законодательства в сфере регулирования информации. Так, в п. 6 ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлены запреты на распространение информации, которая содержит в себе призывы к нарушению действующего законодательства, включая пропаганду войны, ненависти и вражды [12].

Активные действия по выявлению экстремистских ресурсов в России начались в 2020 году: Генеральная прокуратура активно пресекала распространение в Интернете призывов к экстремизму, терроризму и массовым беспорядкам. Было удалено противоправное содержимое с 52 тысяч интернет-ресурсов и заблокирован доступ к 10 тысячам сайтов [1].

31 декабря 2020 г. Федеральным законом от № 511-ФЗ была введена административная ответственность за нарушение порядка ограничения доступа к информации:

1. Неограничение доступа к информации, когда это требуется законом, а равно неудаление такой информации влечет за собой штраф до 4 млн рублей.

2. Неограничение доступа к ресурсам с экстремистской и порнографической информацией, а также информацией о способах изготовления наркотиков, равно как и неудаление такой информации, влечет штраф до 8 млн рублей.

Однако, несмотря на принятые в Российской Федерации меры по ограничению доступа к запрещенной информации в сети Интернет, многие пользователи продолжают находить лазейки для пользования запрещенными информационными ресурсами.

Одной из таких лазеек являются VPN-сервисы. Для ограничения их использования законодателем были приняты изменения в КоАП, предусматривающие штраф для провайдера в случае, если им не были предприняты меры по блокировке доступа к серверу, указанному Роскомнадзором.

Для пользователей ответственности за использование VPN-сервисов нет, но для сокращения их использования Правительство РФ приняло Постановление № 1905 от 14 ноября 2023 года, которое наделяет Роскомнадзор правом ограничивать рекламу VPN-сервисов. Новый приказ Роскомнадзора позволяет блокировать сайты, которые:

– содержат информацию о способах обхода блокировок;

– побуждают использовать эти способы, перечисляя получаемые преимущества;

– объясняют, как получить доступ к запрещенным ресурсам;

– содержат предложения для установки или приобретения данного сервиса [8].

Федеральный закон «О персональных данных» обеспечивает конфиденциальность и защиту персональных данных, в том числе в цифровой среде. Персональные данные являются ценным ресурсом в бизнесе и часто подвергаются кибератакам и утечкам [13].

В марте 2023 года произошла утечка персональных данных сотрудников и студентов Высшей школы экономики (ВШЭ). Несмотря на своевременное расследование утечки, Роскомнадзор был уведомлен, и суд оштрафовал ВШЭ на 60 тысяч рублей за нарушение ч. 1 ст. 13.11 КоАП РФ[9].

В кейсе, связанном с сервисом «Яндекс. Еда», в Сеть попали данные более чем 58 тысяч человек. Эти данные включали в себя номера телефонов, карт, адреса, данные о заказах, включая адреса [2].

Законодатель устанавливает правовой режим использования персональных данных через их определение и ограничения для операторов данных (ст. 3, 10, 11, 18, 18.1, 19 Федерального закона «О персональных данных» № 152-ФЗ).

Нарушение законодательства о персональных данных влечет административную ответственность по статье 13.11 КоАП РФ. Статья 13.14 КоАП РФ применяется, когда данные разглашаются лицом, имеющим к ним доступ по служебным или профессиональным обязанностям, что часто приводит к утечкам данных [14].

Уголовная ответственность наступает за более тяжкие деяния, когда разглашение данных причиняет вред имущественным или личным правам субъекта, например, осуществляется рассылка личных сообщений или публикация фото и видео гражданина. Часто такие случаи связаны с размещением информации в Интернете [4].

Стоит дополнительно отметить, что за нарушение, связанное с утечкой данных, также предусмотрена и гражданская ответственность, но судебные прецеденты по таким делам случаются реже, а также суммы компенсаций являются незначительными, например, по вышеупомянутому делу сервиса «Яндекс.Еда» моральная компенсация составила 5000 рублей на человека. Это снижает мотивацию компаний к внедрению мер для предотвращения утечек в будущем, так как внедрение систем обходится значительно дороже, чем выплата компенсаций, и вопрос о защите пострадавших от неправомерного использования данных остается открытым.

Этой проблемой активно занимается Роскомнадзор, который инициировал принятие регламента, устанавливающего обязательный порядок осведомления министерства в случае, если оператор допустил утечку информации.

Также Роскомнадзор установил правила оценки вреда, который нанесён субъектам утечки [8].

С конца 2023 года Россия находится под санкциями Евросоюза, которые направлены на ограничение доступа к программному обеспечению. Органы власти и российские компании

попали под запрет на продажу, покупку и иные способы предоставления ПО в сферах управления предприятием, промышленного проектирования и производства.

Такая ситуация на международном рынке, а также угрозы утечек персональных данных привели к необходимости внедрения альтернативы иностранному программному обеспечению [10].

Постановление Правительства Российской Федерации от 18 ноября 2020 года № 1867 требует установки российских приложений на технически сложные устройства. Компании с государственной долей участия обязаны перейти на отечественное программное обеспечение [7]. Согласно методическим рекомендациям Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, опубликованным 12 января 2024 года, это должно произойти к 2025 году для операционных систем, офисных пакетов и антивирусов, а к 2026 году — для систем управления базами данных [6].

Кроме того, в Госдуму был внесен законопроект № 47571-7, согласно которому правительство и Центральный банк России получат право определять объекты критической информационной инфраструктуры, которые обязаны будут перейти на отечественное программное обеспечение и радиоэлектронные изделия. Документ доступен в электронной базе Госдумы.

Согласно проекту, правительство и регулятор определят порядок и сроки перехода, а также требования к программному обеспечению, базам данных и радиоэлектронным изделиям, используемым на важных объектах критической информационной инфраструктуры, включая телекоммуникационное оборудование. При условии принятия закона он вступит в силу с 1 марта 2025 года.

С апреля 2022 года в России, согласно указу президента, действует запрет на покупку иностранного ПО для предприятий, которые используют критически важную информацию. Этот документ также вводит понятие «доверенного программно-аппаратного комплекса» (ПАК), соответствующего определенным критериям. Согласно постановлению, с 1 сентября 2024 года запрещается приобретение и использование недоверенных ПАК, за исключением случаев, когда Минпромторг подтверждает отсутствие российских аналогов. Переход на доверенные ПАК должен завершиться к 1 января 2030 года.

В июле 2023 года участники АНО «Вычислительная техника» обратились к Минпромторгу с предложениями по урегулированию параллельного импорта техники. В октябре того же года замминистра промышленности и торговли Василий Шпак заявил о планах Минпромторга сократить список зарубежного оборудования, которое российские заказчики могут получать с помощью «серого» импорта.

Одним из заметных примеров российского программного обеспечения стал операционный пакет AstraLinux, разработанный компанией «НПО РусБИТех». С 2020 года он завоевал доверие крупных корпораций и государственных структур, включая Министерство обороны и ФСБ, что стало важным индикатором его надежности и безопасности.

Для офисных задач также предлагается альтернатива: «МойОфис» от ООО «Новые облачные технологии» – это полный набор инструментов для совместной работы с документами, электронной почтой и облачным хранилищем. Обладающее сертификатами соответствия и будучи допущенным к работе с документами, содержащими информацию под грифом «государственная тайна», это ПО широко используется в различных сферах деятельности.

Имеются и альтернативные отечественные варианты ПО для использования в медиа, в том числе ПО, предназначенное для решения тех же задач, что и программы экосистемы Adobe. В свою очередь, Mail.ru Group, владеющая отечественной социальной сетью VK, недавно открыла бесплатный доступ к сервисам VK WorkSpace для совместной работы сотрудников.

Обсуждение

Все этим меры, безусловны, необходимы, но не позволяют превентивно предотвращать кибератаки.

Многие пользователи считают, что VPN дает возможность безопасно и анонимно пользоваться интернет-ресурсами, которые заблокированы или ограничены на территории страны, но анализ показал, что зачастую это не так. Многие сервисы не соответствуют тому уровню безопасности, которые указаны на их сайте или в описании приложения, и могут передавать данные пользователя третьим лицам, а также получать несанкционированный доступ к файлам на устройстве, в силу чего несут риски сбора данных и слежки за пользователями. Особенно выделяются бесплатные сервисы, получение прибыли которых строится на передаче данных третьим лицам, чтобы на основе этой информации выстраивать целевую рекламу. Борьба с такими сервисами — это вопрос защиты прав граждан и национальной безопасности [5].

Кроме того, в России существуют биржи и даркнет-форумы для покупки персональных данных и обмена ими. Актуальные риски связаны с появлением облачных сервисов по хранению файлов и информации, а также ботов с искусственным интеллектом, таких как ChatGPT [3]. Эти платформы являются основной целью хакеров, так как в них содержится ценная для пользователей информация, которую хакеры могут неправомерно и недобросовестно использовать. Так, утечка с сайта OpenAI позволяет мошенникам узнать содержание запросов пользователей, в которых может содержаться анализ персональной или рабочей информации.

В данной ситуации стоит внедрить превентивные меры для сокращения возможных утечек персональных данных пользователей. Одним из таких способов может быть внедрение организационных мероприятий на предприятии, которые связаны с процессом обучения сотрудников по работе с персональными данными.

Также важен постконтроль, который включает проверку деятельности оператора на предмет нарушений, приведших к утечке данных. Правоохранительные органы, такие как Роскомнадзор, могут выявить причины утечки и разработать методы их предотвращения в будущем.

Эту проблему стоит рассматривать и с точки зрения доступного программного обеспечения.

Для успешного перехода стоит рассматривать не только дополнительные меры, которые связаны с ужесточением законодательного регулирования, но и предоставлять дополнительные льготы, например, связанные с налоговыми вычетами в случае, если компания ускоряет переход на отечественные системы.

Авторами отмечается, что при переходе на отечественное ПО уменьшается информационная зависимость отечественных организаций, особенно тех, которые имеют стратегическое значение для Российской Федерации, от стран Запада и иностранного ПО, которое может предоставлять угрозу внутреннему суверенитету. Соответствие текущим нормативным актам позволяет компании не только не получать штрафы в случае нарушения законодательства, но и иметь преимущества над своими конкурентами, обеспечивая более актуальное предложение на рынке ввиду перехода на отечественное ПО.

Заключение

Таким образом, можно сделать вывод, что Россия движется по пути информационного суверенитета, направленного на ограничение зарубежной продукции в области информационных технологий в пользу развития отечественного рынка соответствующих товаров. Указанные меры подкрепляются императивным внедрением российского ПО в государственных структурах и объектах критической информационной инфраструктуры, что позволит более эффективно реализовать доктрину информационной безопасности страны.

Литература

1. Зайнутдинова Е. В. Конфиденциальность персональных данных в ситуации киберугроз // Юридическая наука и практика. 2023. Т. 19. № 3. С. 38–46.

2. Зинченко С.А. Деятельность социальных сетей по распространению экстремизма: кейс Meta // Социальные и психологические проблемы глазами молодых – 2022: сборник материалов

XXVI Междунар. научно-практич. конф. студентов, аспирантов и молодых ученых. Сыктывкар, 2022. С. 178–180.

3. Иерусалимская Е.А., Новиков В.В. Особенности правового регулирования отношений в цифровом пространстве // Вестник магистратуры. 2022. № 9. С. 37–41.

4. Кассационное определение Седьмого кассационного суда от 10.06.2020 № 77-889/2020 [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=KSOJ007&n=10297#8w5T7GUyamcm1BAP1

5. Купач Е.О. VPN: право на информацию или инструмент нарушения законности? // Россия в XXI веке: стратегия и тактика социально-экономических, политических и правовых реформ: материалы XV Всеросс. научно-практич. конф. студентов и молодых ученых, Барнаул, 28–29 апреля 2022 г. Барнаул, 2022. С. 172–173.

6. Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием (подписано 12 января 2024 г.) / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/7342/

7. Постановление Правительства Российской Федерации от 18.11.2020 № 1867 (ред. от 26.08.2023) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_368496/

8. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/405721227/

9. Решение Тверского районного суда города Москвы от 21 марта 2022 г. по делу № 02-2473/2022 - М-1527/2022 [Электронный ресурс]. URL: https://www.garant.ru/files/6/6/1660666/reshenie-tverskogo-rayonnogo-suda-g-moskvy-ot-21-marta-2022-g-po-delu-n-02-24732022.pdf

10. Токарев М.Н., Вершинин А.Н. Импортозамещение программного обеспечения // Международный журнал гуманитарных и естественных наук. 2023. Т. 6. № 3(81). С. 156–162.

11. Указ Президента РФ от 30.03.2022 № 166 (ред. от 22.11.2023) «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_413177/

12. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/

13. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/

14. Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 01.04.2020 № 99-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_349081/