УДК 34 **DOI: 10.34670/AR.2023.46.59.012**

Сравнительное исследование: обеспечение информационной безопасности серверного оборудования в соответствии с требованиями законодательства

Олифиренко Артем Алексеевич

Студент,
Саратовская государственная юридическая академия,
410056, Российская Федерация, Саратов, ул. Чернышевского, 104;
e-mail: panolifer@gmail.com

Аннотация

Данный исследовательский проект предусматривает углубленный анализ законодательных требований к информационной безопасности серверного оборудования в США, ЕС, России и Китае с целью изучения возможностей практического применения и перспектив импортозамещения в России. программа технологической неприкосновенности. В исследовании сравниваются правовые рамки, передовая практика и тематические исследования в каждой юрисдикции, выделяются сходства и различия между ними. В нем определяются уроки, которые Россия может извлечь из опыта США, ЕС и Китая, и предлагаются возможные меры по повышению информационной безопасности серверного оборудования в контексте российской программы импортозамещения и технологической неприкосновенности. Выводы этого исследования имеют практическое значение как для директивных органов, так и для организаций, действующих в исследуемых юрисдикциях. Сравнительный анализ законодательных требований и механизмов обеспечения соответствия является ценным ориентиром для директивных органов, стремящихся повысить информационную безопасность серверной инфраструктуры в пределах своих соответствующих юрисдикций. Рекомендации исследования представляют собой дорожную карту для совершенствования национальной политики в области кибербезопасности и продвижения более безопасной и устойчивой серверной инфраструктуры. Данное исследование внесло значительный вклад в понимание законодательных требований и систем соответствия требованиям информационной безопасности серверного оборудования в Соединенных Штатах, Европейском Союзе, России и Китае. Выявив общие проблемы и возможности для улучшения, исследование предоставило ценную информацию директивным органам и организациям, стремящимся повысить безопасность серверной инфраструктуры и способствовать созданию более безопасной цифровой среды.

Для цитирования в научных исследованиях

Олифиренко А.А. Сравнительное исследование: обеспечение информационной безопасности серверного оборудования в соответствии с требованиями законодательства // Вопросы российского и международного права. 2023. Том 13. № 3А. С. 112-131. DOI: 10.34670/AR.2023.46.59.012

Ключевые слова

Информационная безопасность, серверное оборудование, требования законодательства, США, ЕС, Россия, Китай, сравнительное исследование, импортозамещение.

Введение

Информационная безопасность является важнейшей задачей в эпоху цифровых технологий, когда серверное оборудование играет ключевую роль в хранении, обработке и передаче данных. Серверное оборудование является неотъемлемой частью функционирования цифровой инфраструктуры, и его уязвимость к киберугрозам создает существенные риски для бизнеса, правительств и частных лиц. Таким образом, обеспечение безопасности серверного оборудования имеет важное значение для защиты конфиденциальности, целостности и доступности данных.

Серия громких кибератак в рамках кибервойны, нацеленных на серверное оборудование, высветила потенциальное воздействие нарушений безопасности. Такие атаки могут привести к финансовым потерям, репутационному ущербу и юридическим последствиям для организаций. Более того, инциденты в сфере безопасности могут подорвать доверие общественности к цифровой инфраструктуре и иметь последствия для национальной безопасности.

Учитывая транснациональный характер Интернета, всеобъемлющая правовая база для обеспечения информационной безопасности серверного оборудования имеет решающее значение. Такая структура охватывает защиту данных и конфиденциальность, сетевую и системную безопасность, отчетность об инцидентах и реагирование на них, оценку рисков и управление ими, а также ответственность и правоприменение. Однако нынешний российский правовой ландшафт постепенно перестраивается в рамках программы импортзамещения.

Основная цель данного исследования – обеспечить всестороннее понимание законодательных требований по обеспечению информационной безопасности серверного оборудования в России, а также сравнение с Китаем, США и ЕС. Для достижения этой цели исследование направлено на решение следующих исследовательских вопросов:

1. Каковы требования информационной безопасности есть на данный момент в Российской Федерации?

Цель этого вопроса – изучить основные требования государственных регуляторов и законодательства к серверной инфраструктуре.

2. Каковы основные законодательные требования по обеспечению информационной безопасности серверного оборудования в США, ЕС, России и Китае?

Этот вопрос включает в себя анализ правовой базы в каждой юрисдикции, включая соответствующие законы, нормативные акты и директивы, которые касаются информационной безопасности серверного оборудования.

3. Как различаются законодательные требования к информационной безопасности серверного оборудования в США, ЕС, России и Китае?

Этот вопрос требует сравнительного анализа законодательных требований в каждой юрисдикции, выявления сходств и различий в их подходах к информационной безопасности.

Отвечая на эти исследовательские вопросы, исследование будет способствовать лучшему пониманию правового поля, регулирующего информационную безопасность серверного

оборудования в этих ключевых юрисдикциях, а также предоставит практическую информацию организациям, работающим в различных регионах.

Объектом исследования является правовая база России, а также Китая, США и ЕС, регулирующая информационную безопасность серверного оборудования. Предметом исследования являются конкретные законодательные требования и техническая регламентация, рамки соблюдения требований и механизмы правоприменения, связанные с информационной безопасностью в этих юрисдикциях.

Гипотеза данного исследования заключается в том, что сравнительный анализ законодательных требований к информационной безопасности серверного оборудования в США, ЕС, России и Китае выявит общие проблемы и возможности для совершенствования российского законодательства. Ожидаемым результатом является разработка руководств и рекомендаций для организаций, стремящихся обеспечить информационную безопасность серверного оборудования в соответствии с этими законодательными требованиями.

Актуальность данного исследования заключается в изучении законодательных требований к информационной безопасности серверного оборудования в четырех основных юрисдикциях, что позволяет получить представление о проблемах и возможностях для гармонизации и совершенствования. Новизной исследования является его сравнительный подход и разработка руководящих принципов и рекомендаций для организаций, работающих в нескольких регионах.

В исследовании будет использован целый ряд источников, включая:

– Первоисточники: нормативные правовые акты (законы, подзаконные акты, директивы) России, Китая, США, ЕС;
– Вторичные источники: академическая литература, правительственные отчеты и отраслевой анализ информационной безопасности и правовых рамок.
– Технические источники, данные компаний.

Методы исследования, использованные в данном исследовании, включают:

– Сравнительно-правовой анализ: сравнение законодательных требований к информационной безопасности серверного оборудования в США, ЕС, России и Китае
– Анализ документов: обзор первичных и вторичных источников, связанных с правовой базой и информационной безопасностью
– Тематические исследования: изучение конкретных случаев нарушений безопасности серверного оборудования и их правовых последствий.

Основная часть

Серверная инфраструктура относится к совокупности физических и виртуальных ресурсов, которые облегчают хранение, обработку и передачу данных внутри организации или через интернет. Серверная инфраструктура является важнейшим компонентом современных систем информационно-коммуникационных технологий, обеспечивающим функционирование цифровых сервисов и приложений в различных секторах экономики. В этой главе будет представлен обзор ключевых элементов серверной инфраструктуры, включая аппаратное обеспечение, программное обеспечение, сетевые подключения и хранилище данных.

Аппаратное обеспечение включает в себя физические компоненты серверной инфраструктуры, такие как серверные машины, устройства хранения данных и сетевое оборудование. Серверные машины – это мощные компьютеры, предназначенные для управления и обработки больших объемов данных, в то время как устройства хранения данных

(например, жесткие диски, твердотельные накопители) хранят и извлекают информацию. Сетевое оборудование, такое как коммутаторы и маршрутизаторы, облегчает обмен данными между серверами и другими устройствами в сети.

Программное обеспечение относится к программам и приложениям, которые выполняются в серверной инфраструктуре, обеспечивая управление, обработку и хранение данных. Ключевые программные компоненты включают операционные системы, системы управления базами данных и платформы виртуализации. Операционные системы, такие как Linux или Windows Server, обеспечивают основу для запуска других программных приложений. Системы управления базами данных, такие как MySQL или PostgreSQL, управляют и организуют хранение данных в серверной инфраструктуре. Платформы виртуализации позволяют нескольким виртуальным серверам работать на одном физическом сервере, оптимизируя использование ресурсов и управление ими [ЛиМАНОВА, Серезнев, 2022].

Сетевые подключения имеют решающее значение для соединения серверной инфраструктуры с другими устройствами и системами, облегчая связь и обмен данными. Сетевые подключения могут устанавливаться с использованием проводных (например, Ethernet) или беспроводных (например, Wi-Fi) технологий, в зависимости от конкретных требований серверной инфраструктуры. В дополнение к локальным сетям (LAN) внутри организации серверная инфраструктура также может быть подключена к Интернету, обеспечивая удаленный доступ и связь с другими серверами и системами [Schwartz, Solove, 2019].

Хранение данных является важным аспектом серверной инфраструктуры, поскольку оно обеспечивает доступность и целостность информации с течением времени. Данные могут храниться на различных типах устройств, таких как жесткие диски, твердотельные накопители или ленточные накопители, в зависимости от требований организации и бюджета. Хранение данных также может быть организовано с использованием различных архитектур, таких как сети хранения данных (SANS) или системы хранения данных с подключением к сети (NAS), которые предоставляют централизованные и распределенные решения для хранения данных соответственно.

Серверная инфраструктура образует основу цифровых систем, обеспечивая хранение, обработку и передачу данных в различных секторах экономики1. Учитывая его критическую роль, обеспечение информационной безопасности серверной инфраструктуры имеет первостепенное значение как для бизнеса, правительств, так и для частных лиц [Whitman, Mattord, 2020].

Нарушения безопасности в серверной инфраструктуре могут привести к значительным финансовым потерям для организаций. Эти потери могут быть вызваны различными факторами, включая кражу конфиденциальных данных, перебои в предоставлении услуг и расходы, связанные с устранением нарушений и соблюдением законодательства.

Организации, которые страдают от нарушений безопасности в своей серверной инфраструктуре, также могут столкнуться с репутационным ущербом, что приведет к потере доверия со стороны клиентов, партнеров и инвесторов. В некоторых случаях такая потеря доверия может иметь долгосрочные последствия, влияющие на рыночные позиции организации и конкурентные преимущества.

Таким образом, изучение и нормативно-правовых требований к организациям, предоставляющим в аренду серверную инфраструктуру, является наиболее важным аспектом в обеспечении информационной безопасности серверов, поскольку государство и государственные органы, прям работающие в данном направлении – разрабатывают стандарты и сертификации систем для предотвращения утечек информации и кибератак.

Российская Федерация

Рассмотрим федеральные законы и нормативные акты Российской Федерации, а также основы соблюдения требований, которыми руководствуются организации при внедрении мер информационной безопасности (в том числе объекты КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры в одной из следующих сфер: здравоохранение, наука, транспорт, связь, энергетика, банки и иные организации финансового рынка, топливно-энергетический комплекс, атомная энергия, оборона, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности).

Федеральные законы

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации»[1]: Настоящий закон устанавливает основные принципы информационной безопасности в России, включая защиту серверной инфраструктуры. Он устанавливает правовую основу для обеспечения конфиденциальности, целостности и доступности информации на серверном оборудовании.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[2]: основы сбора, обработки, хранения и передачи персональных данных в России. Закон определяет права субъектов персональных данных, обязанности контролеров и обработчиков данных, а также роль Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в надзоре за соблюдением требований. Закон имеет значительные последствия для информационной безопасности серверной инфраструктуры в России, особенно в следующих областях:

Хранение и обработка данных: Контролеры и обработчики данных обязаны применять соответствующие меры безопасности для защиты персональных данных, включая использование защищенного серверного оборудования и шифрование данных.

Проверки соответствия требованиям: Организации должны проводить регулярные проверки соответствия требованиям, чтобы убедиться, что их серверная инфраструктура соответствует законодательным требованиям, изложенным в Федеральном законе 152.

Реагирование на инциденты и уведомление: В случае утечки данных организации обязаны уведомить Роскомнадзор и, в некоторых случаях, затронутых субъектов данных, подчеркивая важность надежной защиты серверной инфраструктуры для предотвращения несанкционированного доступа или утечки данных.

Реализация Федерального закона 152 ставит перед организациями ряд задач, в том числе:

Затраты на внедрение: Обеспечение соответствия Федеральному закону 152 может быть ресурсоемким, поскольку организациям может потребоваться инвестировать в защищенную серверную инфраструктуру, технологии шифрования и обучение персонала.

Ограничения на трансграничную передачу данных: Требование локализации данных может ограничить способность многонациональных организаций передавать персональные данные через границы, что потенциально может повлиять на стратегию их серверной инфраструктуры.

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.03.2023).

[2] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2023).

3. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»[3]: Настоящий закон направлен на защиту критической информационной инфраструктуры, включая серверное оборудование, от кибератак и других угроз. Это требует, чтобы операторы критически важной информационной инфраструктуры применяли надлежащие меры безопасности, сообщали об инцидентах соответствующим органам власти (ФСБ, ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации) и регулярно проходили оценку безопасности.

Акты Президента РФ

Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю...»[4] – наделяет ФСТЭК России полномочиями в области обеспечения безопасности КИИ, в том числе функцией государственного контроля.

Указ Президента РФ от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне...»[5] – относит к гостайне информацию о мерах обеспечения безопасности КИИ и о состоянии ее защищенности от атак. ФСБ России и ФСТЭК России назначены государственными органами, наделенными полномочиями по распоряжению сведениями, отнесенными к государственной тайне.

Акты Правительства РФ

Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений»[6] – устанавливает порядок и сроки категорирования объектов КИИ.

Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[7] – определяет правила проведения плановых и внеплановых проверок в области обеспечения безопасности значимых объектов КИИ.

Постановление Правительства РФ от 8.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения

[3] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[4] Указ Президента РФ от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085».

[5] Указ Президента РФ от 2 марта 2018 г. № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203».

[6] Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

[7] Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

функционирования значимых объектов критической информационной инфраструктуры»[8] – устанавливает приоритетность категорий сетей электросвязи, которые могут использовать субъекты КИИ для обеспечения функционирования значимых объектов. Определяет обязанности оператора связи при подключении значимых объектов к сети связи общего пользования.

Ведомственные акты

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[9] – предъявляет требования по аттестации (оценке соответствия) государственных информационных систем (ГИС), в частности от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней.

Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»[10] – определяет сведения о значимом объекте КИИ, необходимые для внесения в реестр. Решение о включении в реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта КИИ. Не реже чем один раз в месяц ФСТЭК России направляет сведения из реестра в ГосСОПКА.

Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[11] – определяет форму акта по итогам проверки значимого субъекта КИИ.

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»[12] – устанавливает требования к силам обеспечения безопасности значимых объектов, программным и программно-аппаратным средствам, документам по безопасности значимых объектов, функционированию системы безопасности.

---

[8] Постановление Правительства РФ от 8 июня 2019 г. № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры».

[9] Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[10] Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

[11] Приказ Федеральной службы по техническому и экспортному контролю от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[12] Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»[13] – определяет набор сведений о результатах присвоения объекту КИИ категории значимости, который необходимо направить во ФСТЭК России. Сведения сгруппированы в девять разделов.

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[14] – устанавливает требования к обеспечению безопасности значимых объектов КИИ в ходе создания, эксплуатации и вывода их из эксплуатации, к организационным и техническим мерам защиты информации и определяет состав мер для каждой категории значимости объекта.

Приказ ФСТЭК России от 26.04.2018 № 72 «О внесении изменений в Регламент Федеральной службы по техническому и экспортному контролю, утвержденный приказом ФСТЭК России от 12 мая 2005 г. № 167»[15] - Относит обеспечение безопасности значимых объектов КИИ к нормативно-правовому регулированию вопросов ФСТЭК России.

Ответственные органы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК). ФСТЭК является ключевым регулирующим органом в области информационной безопасности в России. Она разрабатывает и обеспечивает соблюдение стандартов и руководств по защите серверного оборудования, включая требования к сертификации продуктов и систем информационной безопасности[16].

2. Федеральная служба безопасности (ФСБ, точнее Центр информационной безопасности ФСБ) обеспечивает собственную защиту конфиденциальной информации и контролирует создание системы информационной безопасности по всей стране вместе с ФСТЭК (часто авторы пишут ФСТЭК-ФСБ). Практика деятельности ФСБ выражается в организационных мерах – лицензировании, сертификации, аккредитации – и осуществлении оперативно-розыскных мероприятий в рамках киберпреступлений по 28 главе УК РФ[17].

3. Федеральная служба по надзору в сфере связи, информационных технологий и массовых

[13] Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

[14] Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[15] Приказ Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239».

[16] Федеральная служба по техническому и экспортному контролю. URL: https://fstec.ru/

[17] Федеральная служба безопасности. URL: http://www.fsb.ru/fsb.htm

коммуникаций (Роскомнадзор)[18] несет ответственность за мониторинг и обеспечение соблюдения Федерального закона № 152, который включает в себя надзор за безопасностью серверной инфраструктуры, обрабатывающей персональные данные. Ключевые функции и ответственность агентства в этой связи включают:

– Разработка и внедрение политики и руководящих принципов защиты данных
– Проведение аудитов соответствия требованиям и инспекций контролеров и обработчиков данных
– Расследование утечек данных и наложение административных санкций за несоблюдение требований
– Лицензирование и аккредитация специалистов по защите данных
– Предоставление руководств и рекомендаций организациям по передовым методам обеспечения информационной безопасности и защиты данных

Роскомнадзор проводит регулярные проверки соответствия требованиям, чтобы убедиться, что организации соблюдают требования Федерального закона 152 в отношении своей серверной инфраструктуры. Эти аудиты могут включать:

– Оценка адекватности технических и организационных мер, применяемых для защиты персональных данных
– Оценка эффективности механизмов шифрования данных и контроля доступа
– Проверка соответствия требованиям к локализации данных
– Пересмотр планов реагирования на инциденты и процедур уведомления о нарушениях

4. Министерство цифрового развития, связи и массовых коммуникаций: это министерство отвечает за разработку и реализацию национальной политики и правовое регулирование в области информационной безопасности, включая защиту серверного оборудования. Он осуществляет надзор за принятием соответствующих законов, нормативных актов и стратегий по обеспечению информационной безопасности в России[19].

В заключение следует отметить, что в России создана всеобъемлющая правовая база для обеспечения информационной безопасности серверного оборудования, включая федеральные законы и нормативные акты, а также механизмы соблюдения требований. Эти правовые инструменты играют жизненно важную роль в защите конфиденциальных данных и продвижении безопасной цифровой среды в России.

Китайская Народная Республика

Рассмотрим национальные законы и нормативные акты КНР, а также механизмы соблюдения требований, которыми руководствуются организации при внедрении мер информационной безопасности.

Национальные законы и нормативные акты

1. Закон Китайской Народной Республики о кибербезопасности (2017)[20]: Этот закон устанавливает всеобъемлющую правовую базу для обеспечения кибербезопасности в Китае, включая защиту серверного оборудования. Это требует от сетевых операторов принятия необходимых мер для обеспечения сетевой безопасности, защиты личной информации и

[18] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/

[19] Министерство цифрового развития, связи и массовых коммуникаций. URL: https://digital.gov.ru/ru

[20] Cybersecurity Law of the People's Republic of China, adopted on 7 November 2016, effective on 1 June 2017.

предотвращения кибератак.

Закон применяется к сетевым операторам и компаниям в «критических секторах». Под критическим секторам Китай грубо делит отечественные предприятия на сетевые предприятия, занимающиеся телекоммуникациями, информационными услугами, транспортировкой энергии, водоснабжением, финансовыми услугами, общественными услугами и электронными правительственными услугами. К числу наиболее спорных разделов закона относятся статьи 28, 35 и 37.

Статья 28 обязывает неопределенно определенных «сетевых операторов» (интерпретируемых как: платформы социальных сетей, разработчики приложений и другие технологические компании) сотрудничать с органами общественной безопасности, такими как Министерство общественной безопасности, и предоставлять информацию по запросу.

Статья 35 направлена на покупку иностранного программного или аппаратного обеспечения правительственными учреждениями или другими «операторами критической информационной инфраструктуры», согласно которой любое приобретенное оборудование или программное обеспечение должно быть проверено такими органами, как SCA Китая или Государственное управление криптографии, что может включать предоставление исходных кодов и других конфиденциальных проприетарных данных. информация государственным учреждениям, прокладывающая путь для кражи интеллектуальной собственности государством или ее передачи отечественным конкурентам. Особенно статья создает дополнительное бремя регулирования для иностранных технологических компаний, работающих в Китае, и косвенно создает более благоприятные конкурентные условия для отечественных конкурентов, которые, конечно же, были бы более склонны соблюдать правила.

Статья 37 устанавливает требование локализации данных, что означает, что иностранные технологические компании, такие как Microsoft, Apple и PayPal, работающие на китайском рынке, обязаны хранить данные китайских пользователей на китайских серверах в материковом Китае, чтобы предоставить китайской разведке и органам государственной безопасности более легкий доступ для перехвата данных и коммуникаций, в то время как расширение полномочий правящей Коммунистической партии Китая для учета несогласных мнений и контроля за гражданами.

Закон распространяется на все компании в Китае, которые управляют своими собственными серверами или другими сетями передачи данных. Среди прочего, ожидается, что сетевые операторы разъяснят ответственность за кибербезопасность внутри своей организации, примут технические меры для обеспечения безопасности сетевых операций, предотвращения утечки и кражи данных и будут сообщать обо всех инцидентах кибербезопасности как пользователям сети, так и ответственному отделу внедрения для этого сектора [Xu, Fan, 2020].

Закон состоит из вспомогательных разделов нормативных актов, которые устанавливают цель. Например, правила безопасности Инициативы по базовой инфраструктуре (CII) и меры по оценке безопасности трансграничной передачи персональных данных и важных данных. Однако закон еще предстоит закрепить на камне, поскольку китайские правительственные учреждения заняты определением более условных законов, чтобы лучше соответствовать закону о кибербезопасности. Включив уже существующие законы о VPN и защите данных в закон о кибербезопасности, китайское правительство усиливает свой контроль и подчеркивает, что иностранные компании должны соблюдать национальные правила.

Закон о кибербезопасности также содержит положения и определения, касающиеся юридической ответственности. За различные виды противоправного поведения закон

предусматривает большое количество наказаний, таких как штрафы, приостановление исправления, отзыв разрешений и лицензий на ведение бизнеса и другие. Соответственно, закон предоставляет органам кибербезопасности и административным органам права и руководящие принципы для судебного преследования за незаконные действия.

2. Закон Китайской Народной Республики о защите данных (2021)[21]. Этот закон устанавливает правовую основу для защиты данных и безопасности в Китае. Это требует от организаций принятия мер безопасности для защиты данных, хранящихся на серверном оборудовании, а также сообщать об инцидентах и нарушениях безопасности данных соответствующим органам власти 4.

Закон спорно требует локализации данных, собираемых иностранными и отечественными организациями о гражданах Китая. Закон запрещает экспорт данных технологическими компаниями без предварительного завершения «проверки кибербезопасности», процесс которой является расплывчатым и все еще разрабатывается. Кроме того, иностранным судебным органам запрещено запрашивать данные о китайских гражданах без предварительного получения разрешения китайских властей.

Статья 36: Компетентные органы КНР должны рассматривать запросы иностранных органов юстиции или правоохранительных органов о предоставлении данных в соответствии с соответствующими законами и договорами или соглашениями, заключенными КНР или в которых она участвовала, или в соответствии с принципом равенства и взаимности. Отечественные организации и частные лица не должны предоставлять данные, хранящиеся на материковой территории КНР, органам юстиции или правоохранительным органам зарубежных стран без одобрения компетентных органов КНР.

3. Многоуровневая схема защиты (MLPS 2.0)[22]: MLPS 2.0 – это нормативная база, которая классифицирует информационные системы, включая серверное оборудование, на различные уровни защиты в зависимости от потенциального воздействия инцидентов безопасности. Организации обязаны внедрять соответствующие меры безопасности в соответствии с назначенным им уровнем защищения6.

Рамки соблюдения требований

1. Администрация киберпространства Китая (CAC)[23]: CAC является центральным регулирующим органом, ответственным за надзор за кибербезопасностью в Китае. Он формулирует и обеспечивает соблюдение политик, стандартов и руководящих принципов кибербезопасности, в том числе связанных с защитой серверного оборудования.

2. Министерство общественной безопасности (MPS)[24]: MPS отвечает за поддержание общественной безопасности в Китае, включая кибербезопасность. Она обеспечивает соблюдение законов и нормативных актов в области информационной безопасности, проводит оценку безопасности критической информационной инфраструктуры и расследует киберпреступления с использованием серверного оборудования.

В заключение следует отметить, что Китай создал всеобъемлющую правовую базу для

[21] Data Security Law of the People's Republic of China, adopted on 10 June 2021, effective on 1 September 2021.

[22] Implementation Measures for the Multi-Level Protection Scheme, issued by the Ministry of Public Security on 29 June 2018. URL: https://www.mondaq.com/china/security/754186/mps-publishes-draft-regulations-on-cybersecurity-multilevel-protection-scheme-for-public-comment

[23] Cyberspace Administration of China. URL: http://www.cac.gov.cn/

[24] Ministry of Public Security. URL: http://www.cac.gov.cn/

обеспечения информационной безопасности серверного оборудования, включая национальные законы и нормативные акты, а также механизмы соблюдения требований. Эти правовые инструменты играют жизненно важную роль в защите конфиденциальных данных и продвижении безопасной цифровой среды в Китае.

Соединенные Штаты Америки

Правовой ландшафт в Соединенных Штатах охватывает различные федеральные законы и нормативные акты штатов, направленные на обеспечение информационной безопасности серверного оборудования.

Федеральные законы и нормативные акты

1. Федеральный закон об управлении информационной безопасностью (FISMA)[25]: FISMA обеспечивает комплексную основу для защиты федеральных информационных систем, включая серверную инфраструктуру. Закон требует от федеральных агентств внедрять программы информационной безопасности, которые соответствуют руководящим принципам и стандартам, установленным Национальным институтом стандартов и технологий (NIST).

2. Закон о переносимости и подотчетности медицинского страхования (HIPAA)[26]: HIPAA устанавливает строгие стандарты безопасности для защиты электронной защищенной медицинской информации (ePHI), хранящейся на серверном оборудовании. Охваченные организации и их деловые партнеры должны соблюдать правило безопасности HIPAA, чтобы обеспечить конфиденциальность, целостность и доступность ePHI.

3. Закон об обмене информацией о кибербезопасности (CISA)[27]: CISA поощряет обмен информацией о киберугрозах между государственным и частным секторами для повышения информационной безопасности серверного оборудования. Закон предусматривает защиту от ответственности организаций, которые делятся информацией о киберугрозах с назначенными федеральными агентствами.

Законы Штатов

1. Калифорнийский закон о защите прав потребителей (CCPA)[28]: CCPA расширяет права потребителей на неприкосновенность частной жизни и требует от компаний принятия разумных мер безопасности для защиты личной информации, хранящейся на серверном оборудовании. Закон также устанавливает строгие требования к уведомлению об утечке данных для организаций, которые страдают от инцидентов безопасности.

2. Постановление Департамента финансовых услуг Нью-Йорка (NYDFS) о кибербезопасности[29]. Это постановление обязывает финансовые учреждения, действующие в штате Нью-Йорк, разрабатывать комплексные программы кибербезопасности, включая защиту серверной инфраструктуры. Регламент требует от организаций проводить регулярные оценки рисков, внедрять надежные средства контроля безопасности и сообщать об инцидентах кибербезопасности в NYDFS.

Рамки соблюдения требований

[25] Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq.

[26] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936.

[27] Cybersecurity Information Sharing Act of 2015, Pub. L. 114-113, 129 Stat. 2242.

[28] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.

[29] New York Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies.

Система кибербезопасности NIST30: Эта добровольная система предоставляет организациям набор передовых практик, руководящих принципов и стандартов для управления рисками кибербезопасности на серверном оборудовании и снижения их. Эта платформа широко применяется в различных отраслях промышленности и служит эталоном для практики обеспечения информационной безопасности в Соединенных Штатах.

Положение государственных ведомств

1. Федеральное бюро расследований (ФБР): ФБР играет решающую роль в расследовании и судебном преследовании киберпреступлений, нацеленных на серверную инфраструктуру, включая атаки на критически важные объекты инфраструктуры и крупномасштабные утечки данных. ФБР также сотрудничает с организациями частного сектора для обмена разведданными об угрозах и предоставления рекомендаций по передовым методам обеспечения информационной безопасности[31].

2. Агентство национальной безопасности (АНБ)[32]: АНБ отвечает за защиту систем национальной безопасности, включая серверную инфраструктуру, которая поддерживает военные и разведывательные операции. Агентство разрабатывает и поддерживает криптографические стандарты и технологии для защиты конфиденциальной информации и предоставляет рекомендации по методам обеспечения информационной безопасности для федерального правительства и его подрядчиков.

3. Агентство по кибербезопасности и инфраструктурной безопасности (CISA)

CISA является основным агентством, ответственным за координацию защиты важнейших секторов национальной инфраструктуры. Агентство фокусируется на управлении рисками, предоставляя инструменты кибербезопасности, услуги реагирования на инциденты и возможности оценки федеральным правительствам, правительствам штатов, местным органам власти, племенам и территориям, а также частному сектору. Национальный центр интеграции кибербезопасности и коммуникаций CISA (NCCIC) служит центральным узлом для обмена информацией о киберугрозах, выдачи предупреждений и координации реагирования на инциденты[33].

4.Министерство торговли (DoC)

DoC вносит свой вклад в обеспечение информационной безопасности через Национальный институт стандартов и технологий (NIST), который разрабатывает стандарты, руководящие принципы и передовую практику в области кибербезопасности[34]. Одним из наиболее значительных вкладов NIST является Рамочная программа кибербезопасности, добровольная рамочная программа, которая предоставляет организациям рекомендации по управлению рисками кибербезопасности и их снижению. NIST также контролирует Национальную базу данных уязвимостей (NVD), всеобъемлющее хранилище уязвимостей в системе безопасности и связанной с ними технической информации.

5. Министерство внутренней безопасности (DHS)

DHS играет жизненно важную роль в защите критической инфраструктуры страны, как

[30] National Institute of Standards and Technology, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.

[31] Federal Bureau of Investigation, 2023. Cyber Crime. URL: https://www.fbi.gov/investigate/cyber

[32] National Security Agency, 2023. Cybersecurity. URL: https://www.nsa.gov/what-we-do/cybersecurity/

[33] CISA, 2018. Cybersecurity and Infrastructure Security Agency Act of 2018. Pub. L. 115-278.

[34] NCCIC, 2023. National Cybersecurity and Communications Integration Center.

указано в ее Национальном плане защиты инфраструктуры (NIPP). В обязанности департамента входит анализ разведывательных данных, оценка уязвимости и планирование обеспечения безопасности. DHS также тесно сотрудничает с частным сектором и международными партнерами в целях расширения обмена информацией и сотрудничества[35].

Совместно CISA, DoC и DHS формируют скоординированный подход к решению проблем и угроз информационной безопасности в Соединенных Штатах.

Разберем Отчет по оценке важнейших цепочек поставок, поддерживающих индустрию информационных и телекоммуникационных технологий США, нас интересует только пункт 4.4 Downstream Products: Routers, Switches, and Servers – 4.4 Последующие продукты: Маршрутизаторы, коммутаторы и серверы (то беж сетевое оборудование)[36].

Сетевое оборудование, такое как маршрутизаторы, коммутаторы и серверы, имеет решающее значение для передачи данных, распределения процессов обработки данных и приложений, обмена данными между устройствами и подключения сетей. Различные типы сетевого оборудования используются потребителями, предприятиями, сетевыми операторами и поставщиками услуг связи. Маршрутизаторы, коммутаторы и серверы состоят из различных компонентов, таких как материнская плата, центральный процессор (CPU), блок питания, жесткие диски, оперативная память (RAM), печатные платы и многие другие. В результате конечные продукты могут быть очень сложными, поскольку один сервер содержит от 3500 до 4000 компонентов. В то время как в Соединенных Штатах есть несколько ведущих компаний, поставляющих сетевое оборудование (например, Dell, HPE, IBM), большая часть производства сосредоточена в Азии через компании EMS, в которых доминируют тайваньские компании со штаб-квартирами (например, Foxconn, Inventec, Wistron)[37].

В заключение следует отметить, что в Соединенных Штатах существует разнообразный правовой ландшафт, включающий федеральные законы и нормативные акты штатов, механизмы соблюдения требований и участие федеральных агентств, таких как ФБР и АНБ, в обеспечении информационной безопасности серверного оборудования. Эти правовые рамки играют решающую роль в защите конфиденциальных данных и содействии созданию безопасной цифровой среды в стране.

Европейский Союз

Рассмотрим директивы и нормативные акты ЕС, национальные законы и подзаконные акты в отдельных государствах – членах ЕС, а также основы соблюдения требований, которыми руководствуются организации при внедрении мер информационной безопасности.

Директивы и нормативные акты ЕС

1. Общее положение о защите данных (GDPR)[38]: GDPR устанавливает всеобъемлющую правовую базу для защиты данных и конфиденциальности в ЕС. Это требует от организаций

[35] DHS, 2013. National Infrastructure Protection Plan. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan

[36] Assessment of the critical supply chains supporting the U.S. information and communications technology industry. URL: https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf

[37] Comments of Telecommunications Industry Association to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (TIA, November 4, 2021).

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

принятия соответствующих технических и организационных мер для обеспечения безопасности персональных данных, обрабатываемых на серверном оборудовании. GDPR также налагает строгие требования к уведомлению об утечке данных и значительные штрафы за несоблюдение.

2. Директива о сетях и информационных системах (Директива NIS)[39]: Директива NIS является первым общеевропейским законодательством по кибербезопасности. Он направлен на повышение безопасности сетевых и информационных систем, включая серверное оборудование, по всему ЕС. Государства-члены обязаны включить Директиву NIS в национальное законодательство и назначить компетентные органы для обеспечения безопасности основных сервисов и поставщиков цифровых услуг.

3. Закон о кибербезопасности: Закон о кибербезопасности устанавливает правовую основу для Европейской группы сертификации кибербезопасности (ECCG). Эта группа, состоящая из представителей государств - членов ЕС, отвечает за разработку схем сертификации кибербезопасности для продуктов, услуг и процессов ИКТ, включая серверное оборудование[40].

Национальные законы и нормативные акты в отдельных государствах - членах ЕС

1. Германия: Закон о Федеральном управлении информационной безопасности Германии (BSI) и Закон об ИТ-безопасности требуют от операторов критически важной инфраструктуры, включая поставщиков серверной инфраструктуры, внедрять минимальные стандарты безопасности и сообщать о значительных инцидентах безопасности в BSI[41].

2. Франция: Французский закон о сетевой и информационной безопасности (NIS) переносит Директиву NIS во французское законодательство, требуя от операторов основных служб и поставщиков цифровых услуг внедрять меры безопасности для защиты своей серверной инфраструктуры и сообщать об инцидентах безопасности[42].

Рамки соблюдения требований

1. Агентство Европейского союза по кибербезопасности (ENISA): ENISA поддерживает государства – члены ЕС и организации в реализации Директивы NIS, предоставляя руководящие принципы, передовой опыт и рекомендации по мерам информационной безопасности серверного оборудования[43].

2. ISO/IEC 27001:2013: Этот европейский стандарт обеспечивает системный подход к управлению конфиденциальной информацией, в том числе хранящейся на серверном оборудовании, посредством внедрения Системы управления информационной безопасностью (ISMS). Организации в ЕС часто используют сертификацию ISO/IEC 27001 для демонстрации соответствия GDPR и другим правилам информационной безопасности[44].

В своем последнем отчете ENISA (Агентство по сетевой и информационной безопасности Евросоюза – это орган ЕС, занимающийся обеспечением кибербезопасности в масштабах

[39] European Commission, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union.

[40] Regulations (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. Official Journal of the European Union.

[41] Act on the Federal Office for Information Security (BSI Act – BSIG) German law of 14 August 2009 (Federal Law Gazette I p. 2821)

[42] Décret n° 2018-384 du 23 mai 2018

[43] European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/

[44] ISO/IEC 27001:2013. International standart. URL: https://www.scanforsecurity.com/wp-content/docs/iso/ISO-IEC_27001-2013%20Requirements%20(original).pdf

Европы) выделила блок «Supply chain attacks» («Атаки на цепочки поставок»), куда входит серверная инфраструктура[45].

В заключение следует отметить, что ЕС создал надежную правовую базу для обеспечения информационной безопасности серверного оборудования, включая директивы и нормативные акты ЕС, национальные законы государств-членов и механизмы соблюдения требований. Эти правовые инструменты играют жизненно важную роль в защите конфиденциальных данных и продвижении безопасной цифровой среды по всему ЕС.

Сравнение подходов

Для выявления положительного опыта для Российской Федерации необходимо сравнить подходы каждой из рассмотренных стран.

Соединенные Штаты внедрили надежную правовую базу для обеспечения информационной безопасности серверного оборудования, включая Федеральный закон об управлении информационной безопасностью (FISMA) и руководящие принципы, изданные Национальным институтом стандартов и технологий (NIST). Подход США делает упор на управление рисками и непрерывный мониторинг с акцентом на государственно-частное партнерство и отраслевые нормативные акты.

Европейский союз принял Общее положение о защите данных (GDPR) и Директиву о сетях и информационных системах (NIS), которые в совокупности обеспечивают комплексную основу для обеспечения информационной безопасности серверного оборудования. Подход ЕС делает упор на защиту данных и неприкосновенность частной жизни, с сильными механизмами правоприменения и акцентом на сотрудничество между государствами-членами.

Правовая база России в области безопасности серверного оборудования включает ФЗ 149, 152 187 и различные ведомственные акты, изданные Федеральной службой по техническому и экспортному контролю (ФСТЭК). Российский подход делает акцент на государственном контроле и интересах национальной безопасности, уделяя особое внимание импортозамещению и технологической независимости.

Подход Китая к обеспечению безопасности серверного оборудования регулируется Законом о кибербезопасности, который устанавливает всеобъемлющие рамки информационной безопасности, подчеркивая государственный контроль, интересы национальной безопасности и технологический суверенитет. Китай также внедрил различные отраслевые нормативные акты и стандарты, уделяя особое внимание местным инновациям и развитию отечественных технологий.

Основываясь на сравнении подходов Соединенных Штатов, Европейского Союза и Китая, можно применить несколько лучших практик для повышения безопасности серверной инфраструктуры России:

Риск-ориентированный подход: Принятие риск-ориентированного подхода к информационной безопасности, как это наблюдается в США и ЕС, может обеспечить более гибкую и адаптивную основу для противодействия развивающимся киберугрозам.

Государственно-частное партнерство: Поощрение сотрудничества между правительственными учреждениями и организациями частного сектора, как это наблюдается в США, может способствовать обмену опытом и ресурсами для повышения безопасности

[45] ENISA Threat Landscape 2022. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

серверного оборудования.

Гармонизация и сотрудничество: Принятие более совместного подхода с другими странами, как это наблюдается в ЕС, может помочь России разработать общие стандарты и поделиться передовым опытом в области безопасности серверного оборудования (в нашем случае внутри БРИКС и ЕАЭС, а также Шанхайской организации сотрудничества).

Акцент на технологической независимости: Опираясь на акцент Китая на местные инновации и технологический суверенитет, Россия может продолжать заниматься импортозамещением и развитием отечественных технологий, чтобы уменьшить зависимость от иностранного серверного оборудования и повысить национальную безопасность.

Применяя риск-ориентированный подход, укрепляя государственно-частное партнерство, стремясь к гармонизации и сотрудничеству и уделяя особое внимание технологической независимости, Россия может повысить безопасность своего серверного оборудования и способствовать созданию более безопасной и устойчивой цифровой среды.

Заключение

Целью данного исследования было провести анализ законодательных требований к информационной безопасности серверного оборудования в США, ЕС, России и Китае, а также реализованные средства технической защиты серверной инфраструктуры России для изучения возможности практического применения и перспективы российской программы импортозамещения и технологической независиомстити.

Мы обнаружили, что каждая юрисдикция имеет свой уникальный подход к решению вопросов защиты данных, сетевой и системной безопасности, отчетности об инцидентах и реагирования на них, технических и организационных мер, оценки рисков и управления ими, а также ответственности и правоприменения. Несмотря на эти различия, существует несколько передовых практик и уроков, которые Россия может извлечь из опыта США, ЕС и Китая. В частности, исследование предполагает, что Россия может извлечь выгоду из:

1. Принятие всеобъемлющей правовой базы информационной безопасности, которая касается защиты данных, сетевой и системной безопасности, отчетности об инцидентах и реагирования на них, технических и организационных мер, оценки рисков, а также ответственности и правоприменения, аналогично GDPR ЕС и Директиве NIS, а также Закону Китая о кибербезопасности и Закону о защите данных.

2. Установление отраслевых правил и руководств, адаптированных к уникальным потребностям каждого сектора, примером чего могут служить HIPAA США для здравоохранения и GLBA для финансовых услуг.

4. Внедрение риск-ориентированного подхода к управлению информационной безопасностью, который получил широкое распространение в США, ЕС и Китая.

Практическое применение этих уроков и передового опыта в контексте российской программы импортозамещения и технологической неприкосновенности могло бы привести к повышению информационной безопасности серверного оборудования и укреплению общей системы кибербезопасности страны. Приняв эти меры, Россия может создать более устойчивую и безопасную цифровую среду для своих граждан и бизнеса, укрепляя доверие к информационной инфраструктуре страны.

Основной целью данного исследования была оценка законодательных требований и рамок соответствия требованиям для обеспечения информационной безопасности серверного

оборудования в Соединенных Штатах, Европейском Союзе, России и Китае. Благодаря всестороннему изучению соответствующих законов, нормативных актов и тематических исследований исследование дало ценную информацию о сильных и слабых сторонах подхода каждой юрисдикции к обеспечению безопасности серверной инфраструктуры. Кроме того, проведя сравнительный анализ, исследование выявило общие проблемы и возможности для гармонизации и улучшения информационной безопасности серверного оборудования. Таким образом, цели исследования были достигнуты.

Выводы этого исследования имеют практическое значение как для директивных органов, так и для организаций, действующих в исследуемых юрисдикциях. Сравнительный анализ законодательных требований и механизмов обеспечения соответствия является ценным ориентиром для директивных органов, стремящихся повысить информационную безопасность серверной инфраструктуры в пределах своих соответствующих юрисдикций. Рекомендации исследования, основанные на передовой международной практике и опыте, представляют собой дорожную карту для совершенствования национальной политики в области кибербезопасности и продвижения более безопасной и устойчивой серверной инфраструктуры.

Для организаций понимание законодательных требований и механизмов соблюдения требований в различных юрисдикциях имеет решающее значение для поддержания защищенной серверной инфраструктуры и сведения к минимуму риска нарушений безопасности. Следуя руководящим принципам и рекомендациям, представленным в этом исследовании, организации могут лучше защитить свое серверное оборудование и снизить вероятность кибератак и утечек данных.

Это исследование заложило основу для будущих исследований в области информационной безопасности серверного оборудования. Дальнейшее расследование могло бы быть сосредоточено на конкретных секторах или отраслях промышленности, поскольку законодательные требования и рамки соблюдения требований могут отличаться в зависимости от характера организации и типа обрабатываемых данных. Кроме того, в будущих исследованиях можно было бы изучить влияние новых технологий, таких как искусственный интеллект и квантовые вычисления, на информационную безопасность серверной инфраструктуры и правовую базу, регулирующую эту область.

Другим потенциальным направлением будущих исследований является анализ эффективности государственно-частного партнерства в повышении безопасности серверной инфраструктуры. Изучение успеха таких партнерств в различных юрисдикциях могло бы дать ценную информацию о передовой практике и стратегиях укрепления сотрудничества между государственными учреждениями и организациями частного сектора в области информационной безопасности.

В заключение следует отметить, что данное исследование внесло значительный вклад в понимание законодательных требований и систем соответствия требованиям информационной безопасности серверного оборудования в Соединенных Штатах, Европейском Союзе, России и Китае. Выявив общие проблемы и возможности для улучшения, исследование предоставило ценную информацию директивным органам и организациям, стремящимся повысить безопасность серверной инфраструктуры и способствовать созданию более безопасной цифровой среды.

Библиография

1. Лиманова Н.И., Селезнев И.А. Анализ эффективности клиент-серверной архитектуры // Бюллетень науки и практики. 2022. № 7. С. 392-396.
2. Министерство цифрового развития, связи и массовых коммуникаций. URL: https://digital.gov.ru/ru
3. Федеральная служба безопасности. URL: http://www.fsb.ru/fsb.htm
4. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/
5. Федеральная служба по техническому и экспортному контролю. URL: https://fstec.ru/
6. Assessment of the critical supply chains supporting the U.S. information and communications technology industry. URL: https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf
7. Cyberspace Administration of China. URL: http://www.cac.gov.cn/
8. DHS, 2013. National Infrastructure Protection Plan. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan
9. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/
10. Federal Bureau of Investigation, 2023. Cyber Crime. URL: https://www.fbi.gov/investigate/cyber
11. Ministry of Public Security. URL: http://www.cac.gov.cn/
12. National Security Agency, 2023. Cybersecurity. URL: https://www.nsa.gov/what-we-do/cybersecurity/
13. NCCIC, 2023. National Cybersecurity and Communications Integration Center. URL: https://us-cert.cisa.gov/nccic
14. Schwartz P.M., Solove D.J. Information Privacy Law. New York: Wolters Kluwer. 2019. 1219 p.
15. Whitman M.E., Mattord H.J. Principles of Information Security. Boston, MA: Cengage Learning. 2020. 676 p.
16. Xu L., Fan C. The Multilevel Protection Scheme 2.0: A Major Overhaul of China's Cybersecurity Regulatory Framework // International Journal of Law and Information Technology. 2020. 28 (1). P. 1-22.

Comparative study: ensuring information security of server equipment in accordance with legal requirements

Artem A. Olifirenko

Graduate Student,
Saratov State Law Academy,
410056, 104, Chernyshevskogo str., Saratov, Russian Federation;
e-mail: panolifer@gmail.com

Abstract

This research project provides an in-depth analysis of the legal requirements for information security of server equipment in the US, EU, Russia and China in order to study the possibilities of practical application and the prospects for import substitution in Russia. technological immunity program. The study compares legal frameworks, best practices and case studies in each jurisdiction, highlighting similarities and differences between them. It identifies lessons that Russia can learn from the experience of the US, the EU and China, and suggests possible measures to improve the information security of server equipment in the context of the Russian import substitution program and technological immunity. The findings of this study have practical implications for both policy makers and organizations operating in the jurisdictions under study. Comparative analysis of legal requirements and compliance mechanisms is a valuable reference for policymakers seeking to improve the information security of server infrastructure within their respective jurisdictions. The study's recommendations provide a roadmap for improving national cybersecurity policies and promoting a more secure and resilient server infrastructure. This study has made a significant contribution to understanding the legal requirements and information security compliance systems

of server hardware in the United States, the European Union, Russia and China. By identifying common challenges and opportunities for improvement, the study provided valuable insights to policymakers and organizations looking to improve the security of their server infrastructure and help create a more secure digital environment.

For citation

Olifirenko A.A. (2023) Sravnitel'noe issledovanie: obespechenie informatsionnoi bezopasnosti servernogo oborudovaniya v sootvetstvii s trebovaniyami zakonodatel'stva [Comparative study: ensuring information security of server equipment in accordance with legal requirements]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (3A), pp. 112-131. DOI: 10.34670/AR.2023.46.59.012

Keywords

Information security, server hardware, legal requirements, USA, EU, Russia, China, comparative study, import substitution.

References

1. *Assessment of the critical supply chains supporting the U.S. information and communications technology industry.* Available at: https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf [Accessed 03/03/2023]
2. *Cyberspace Administration of China.* Available at: http://www.cac.gov.cn/ [Accessed 03/03/2023]
3. *DHS, 2013. National Infrastructure Protection Plan.* Available at: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan [Accessed 03/03/2023]
4. *European Union Agency for Cybersecurity*. Available at: https://www.enisa.europa.eu/ [Accessed 03/03/2023]
5. *Federal Bureau of Investigation, 2023. Cyber Crime*. Available at: https://www.fbi.gov/investigate/cyber [Accessed 03/03/2023]
6. *Federal'naya sluzhba bezopasnosti* [Federal Security Service]. Available at: http://www.fsb.ru/fsb.htm [Accessed 03/03/2023]
7. *Federal'naya sluzhba po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii* [Federal Service for Supervision of Communications, Information Technology and Mass Communications]. Available at: https://rkn.gov.ru/ [Accessed 03/03/2023]
8. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu* [Federal Service for Technical and Export Control]. Available at: https://fstec.ru/ [Accessed 03/03/2023]
9. Limanova N.I., Seleznev I.A. (2022) Analiz effektivnosti klient-servernoi arkhitektury [Analysis of the effectiveness of client-server architecture]. *Byulleten' nauki i praktiki* [Bulletin of science and practice], 7, pp. 392-396.
10. *Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsii* [Ministry of Digital Development, Telecommunications and Mass Media]. Available at: https://digital.gov.ru/ru [Accessed 03/03/2023]
11. *Ministry of Public Security.* Available at: http://www.cac.gov.cn/ [Accessed 03/03/2023]
12. *National Security Agency, 2023. Cybersecurity.* Available at: https://www.nsa.gov/what-we-do/cybersecurity/ [Accessed 03/03/2023]
13. *NCCIC, 2023. National Cybersecurity and Communications Integration Center.* Available at: https://us-cert.cisa.gov/nccic [Accessed 03/03/2023]
14. Schwartz P.M., Solove D.J. (2019) *Information Privacy Law*. New York: Wolters Kluwer.
15. Whitman M.E., Mattord H.J. (2020) *Principles of Information Security.* Boston, MA: Cengage Learning.
16. Xu L., Fan C. (2020) The Multilevel Protection Scheme 2.0: A Major Overhaul of China's Cybersecurity Regulatory Framework. *International Journal of Law and Information Technology*, 28 (1), pp. 1-22.