УДК 004.056.5

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В УСЛОВИЯХ САНКЦИЙ: АНАЛИЗ ТРАНСФОРМАЦИИ IT-ИНФРАСТРУКТУР В ПРОЦЕССЕ ИМПОРТОЗАМЕЩЕНИЯ

Марина Николаевна Кустова
кандидат технических наук, доцент
kustova.64@mail.ru
Максим Александрович Комаров
студент
maksimkomarov878@gmail.com
Татьяна Андреевна Плаксина
студент
plaksinat781000@gmail.com
Поволжский государственный
университет телекоммуникаций и информатики
г. Самара, Россия

Аннотация. Изменения, происходящие в сфере IT-технологий за последние два года, оказали значительное влияние на цифровую среду российских организаций. Множество программных решений, на которые ранее опиралась корпоративная IT‑ инфраструктура, стало недоступным: одна часть поставщиков ушла с рынка, а другие прекратили продление лицензий или существенно ограничили техническую поддержку. В результате российским предприятиям потребовалось в ускоренном режиме выбирать функциональные аналоги, перестраивать процессы обеспечения информационной безопасности и реконструировать архитектуру информационных систем, которая ранее считалась

устойчивой. В этой связи в статье рассматриваются современные тенденции импортозамещения программных продуктов, ключевые трудности перехода на отечественные решения, а также риски и организационные последствия, связанные с модернизацией структуры информационной безопасности организаций.

Ключевые слова: информационная безопасность, организация, информационные технологии, инфраструктура, импортозамещение, санкции.

Уход значительной части зарубежных IT‑поставщиков привёл к тому, что многие организации оказались перед необходимостью оперативного поиска альтернативных решений. Практически половина российских компаний столкнулась с невозможностью продления лицензий, а треть – с отсутствием необходимого уровня техподдержки [2]. Это обстоятельство сформировало повышенный спрос на отечественные программные продукты и предопределило масштабную перестройку организационной инфраструктуры. В данных условиях организациям было необходимо заменить не только программные средства, но и адаптировать бизнес‑процессы, обновить аппаратную базу и подготовить персонал к работе с новыми технологиями [3].

Полный переход на отечественные IT-продукты пока реализован ограниченным числом организаций. Только 2-3 % компаний полностью отказались от использования иностранного программного обеспечения. Большинство предприятий осуществляют переход последовательно, стремясь минимизировать риски нарушения функционирования критически важных сервисов.

При переходе организации сталкиваются со следующими проблемами [2, 11]:

– несовместимость используемых прикладных систем с новыми отечественными платформами;

– недостаточная зрелость отдельных классов российских решений;

– отсутствие прямых функциональных аналогов, требующее разработки дополнительных инструментов или адаптационных механизмов.

Рынок средств защиты информации трансформировался: отечественные решения доминируют, а иностранные продукты используются преимущественно в случаях, когда их замена сопряжена с техническими или организационными рисками [2, 11].

За последние два года российские производители значительно активизировали выпуск новых версий DLP‑систем, межсетевых экранов, средств мониторинга, систем анализа событий безопасности и других продуктов, необходимых для создания комплексной системы защиты.

Большинство отечественных IT-разработчиков ориентируются на стандарты и требования регуляторов (ФСТЭК, ФСБ, Минцифры), что упрощает внедрение решений в государственные и критически важные информационные системы [6-10].

Среди значимых преимуществ внедрения отечественныхIT-решений в промышленные предприятия отмечают [11]:

– снижение валютных и санкционных рисков;

– оперативное получение обновлений;

– возможность адаптации решений под локальные задачи и инфраструктурные особенности.

Увеличение количества кибератак и утечек данных особенно заметно в отраслях с низким уровнем цифровой зрелости. Например, в образовательных учреждениях число утечек увеличилось почти на четверть по сравнению с предыдущим периодом [1,12].

Рынок труда испытывает дефицит квалифицированных специалистов по информационной безопасности на уровне 35-40%, что приводит к увеличению нагрузки на действующие IT-команды и снижению эффективности процессов обеспечения информационная безопасность большинства предприятий [3-4].

Расширение перечня требований для субъектов КИИ (критическая информационная инфраструктура), включая обязательную регистрацию доменных имён и сетевых адресов, усиливает административную нагрузку и требует дополнительной организационной проработки [6-10].

Перед началом IT-миграции необходимо провести всестороннюю диагностику: определить текущие зависимости, критичность систем, возможные

риски и подготовить инфраструктуру для перехода. Пилотные зоны позволяют протестировать решения без угрозы для основной среды.

Существенную роль играет подготовка сотрудников: обучение работе с отечественными IT-системами, формирование внутренних центров компетенций, привлечение SOC‑провайдеров и создание кадрового резерва.

Даже в период IT-миграции необходимо соблюдать требования регуляторов, контролировать своевременность обновлений, проводить тестирование на проникновение и поддерживать многоуровневую защиту инфраструктуры.

Многие организации применяют смешанную модель управления информационной безопасностью организаций: временно сохраняют критичные иностранные продукты, параллельно внедряя отечественные аналоги. Использование виртуализации и контейнеризации снижает риски несовместимости. Обеспечение информационной безопасности должно включать регулярные проверки, анализ инцидентов, актуализацию документации, контроль восстановления данных и постоянный ITмониторинг [12-13].

Вывод:

Импортозамещение в сфере информационной безопасности организаций – это долгосрочный и масштабный процесс, требующий системного подхода. Организации, которые проводят аудит, развивают кадровый потенциал, поэтапно модернизируют инфраструктуру и совершенствуют процессы безопасности, способны обеспечить устойчивость, технологическую независимость и высокий уровень защиты информационных систем.

Список литературы:

1. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров // Вопросы кибербезопасности. 2022. № 2. С. 27-38.

2. Догучаева С. М. Анализ современных проблем информационной безопасности в российских компаниях // Риск: ресурсы, информация, снабжение, конкуренция. 2022. № 2. С. 65-68.

3. Ефремов Н. А., Мужжавлева Т. В. Процессы информатизации экономики и информационная безопасность // Экономика и предпринимательство. 2023. № 3. С. 287–294.

4. Коноплева Л. А. Гуманитарные аспекты информационной безопасности: учеб. пособие / Министерство науки и высш. образования РФ, Урал. гос. экон. ун-т. Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2022. 162 с.

6. Проект № 162359 // Федеральный портал проектов, нормативных правовых актов – URL: https://regulation.gov.ru/projects/162359 (дата обращения: 03.12.2025)

7. Проект № 162360 // Федеральный портал проектов, нормативных правовых актов – URL: https://regulation.gov.ru/projects/162360 (дата обращения: 03.12.2025)

8. Проект № 162362 // Федеральный портал проектов, нормативных правовых актов – URL: https://regulation.gov.ru/projects/162362 (дата обращения: 03.12.2025)

9. Проект № 162381 // Федеральный портал проектов, нормативных правовых актов – URL: https://regulation.gov.ru/projects/162381 (дата обращения: 03.12.2025)

10. Проект № 162366 // Федеральный портал проектов, нормативных правовых актов – URL: https://regulation.gov.ru/projects/162366 (дата обращения: 03.12.2025)

11. Раткин Л. С. Информационная безопасность промышленных предприятий в условиях санкций на примере импортозамещения квантовых систем // Защита информации. Инсайд. 2022. № 5. С. 14–16.

12. Смирнов С. И., Киселев А. Н., Азерский В. Д. и др. Комплексная методика проведения расследования инцидента информационной безопасности // Защита информации. Инсайд. 2023. № 2. С. 14–26.

13. Федотова Г. В., Куразова Д. А. Угрозы кибербезопасности устойчивости цифровых платформ // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX междунар. науч.-практ. конф. (Екатеринбург, 2 дек. 2021 г.). Екатеринбург, 2021. С. 118–122.

UDC 004.056.5

INFORMATION SECURITY MANAGEMENT UNDER SANCTIONS: AN ANALYSIS OF THE TRANSFORMATION OF IT INFRASTRUCTURES AND IMPORT SUBSTITUTION PROCESSES

Marina N. Kustova
associate professor
kustova.64@mail.com
Maxim Al. Komarov
student
maksimkomarov878@gmail.com
Tatiana An. Plaksina
student
plaksinat781000@gmail.com
Samara State University of Telecommunications and Informatics
Samara, Russia

Annotation. Recent years have had a significant impact on the digital environment of Russian organizations. Many software solutions that previously

supported the corporate IT infrastructure have become unavailable: some vendors have withdrawn from the market, some have stopped renewing licenses or significantly limited technical support. As a result, enterprises had to choose functional analogues in an accelerated mode, rebuild information security (IS) processes and reconstruct the architecture of information systems, which was previously considered stable. The article examines import substitution trends, the key difficulties of switching to domestic solutions, as well as the risks and organizational consequences associated with the modernization of information security infrastructure.

Keywords: information security, IT, information technology, import substitution, sanctions.

Статья поступила в редакцию 25.02.2026; одобрена после рецензирования 20.03.2026; принята к публикации 31.03.2026.

The article was submitted 25.02.2026; approved after reviewing 20.03.2026; accepted for publication 31.03.2026.