

М. Д. Рублев¹✉, А. В. Шабурова¹

Совершенствование защиты объектов критической информационной инфраструктуры в организации

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: matvey.100pro@mail.ru

Аннотация. На фоне нарастающего числа киберугроз и все более сложной организации цифровых процессов в статье исследуются подходы к развитию системы защиты объектов критической информационной инфраструктуры (КИИ). В центре рассмотрения находится необходимость комплексного обеспечения безопасности, при котором организационные, технические и правовые меры не разъединяются, а соотносятся между собой. Через анализ проблем, сохраняющихся в организациях при защите КИИ, выделяются наиболее значимые уязвимости и намечаются пути их устранения. Отдельно рассматриваются внедрение современных средств защиты информации, развитие мониторинга и реагирования на инциденты, а также повышение уровня компетенций персонала. Представленные результаты ориентированы на последующее использование при разработке и совершенствовании корпоративных систем информационной безопасности.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, киберугрозы, защита информации, киберинциденты, управление рисками, SIEM-системы, цифровая безопасность

M. D. Rublyov¹✉, A. V. Shaburova¹

Improving the Protection of Critical Information Infrastructure Facilities in an Organization

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: matvey.100pro@mail.ru

Abstract. Against the backdrop of a growing number of cyber threats and the increasing complexity of digital processes, the article examines approaches to improving the protection system for critical information infrastructure facilities. The study focuses on the need for a comprehensive security framework in which organizational, technical, and legal measures are considered in conjunction rather than in isolation. By analyzing the problems that persist in organizations in the course of protecting critical information infrastructure, the paper identifies the most significant vulnerabilities and outlines directions for their elimination. Particular attention is given to the implementation of modern information protection tools, the development of incident monitoring and response systems, and the enhancement of personnel competencies. The results presented may be used in the design and further improvement of corporate information security systems.

Keywords: information security, critical information infrastructure, cyber threats, information protection, cyber incidents, risk management, SIEM systems, digital security

Введение

Сбой в работе информационной системы сегодня затрагивает не только отдельную управленческую функцию: при высокой интенсивности цифровой трансформации хозяйственной деятельности под удар попадает сама операционная основа организации. В таких условиях нарушения в цифровой среде оборачиваются заметными экономическими потерями, расстройством бизнес-процессов, а нередко и снижением доверия со стороны контрагентов. По этой причине особую значимость приобретают объекты критической информационной инфраструктуры, чья надежность связана с устойчивым состоянием не только отдельных организаций, но и целых отраслей.

Исследовательский интерес к проблематике защиты КИИ остается устойчиво высоким. Однако в имеющемся массиве работ чаще рассматриваются либо технические механизмы безопасности, либо вопросы нормативного регулирования. При таком распределении акцентов комплексное видение, в котором организационные, технологические и человеческие факторы анализируются как взаимосвязанные элементы, представлено не в полной мере.

Исследование опирается на положения теории информационной безопасности, концепции управления рисками, а также на системный и процессный подходы.

Источниковую основу составили нормативные акты, внутренние документы организаций и материалы, полученные при анализе сложившейся практики обеспечения безопасности.

В статье разрабатываются направления совершенствования защиты объектов КИИ на уровне организации. Движение к этой цели связано с выявлением ключевых угроз, рассмотрением действующих механизмов защиты и подготовкой предложений по их модернизации.

Методы и методики

Для оценки состояния системы защиты КИИ в исследовании были совмещены качественные и аналитические методы. Такое сочетание дало возможность рассматривать проблематику не фрагментарно, а с учетом нескольких уровней анализа. Системный подход задал подход, при котором информационная безопасность интерпретируется как единый механизм: изменение одного из его компонентов отражается на работе остальных, иногда не сразу, но вполне ощутимо в общей конфигурации защиты.

При сопоставлении различных подходов к построению защиты метод сравнительного анализа выявил заметное расхождение между традиционными моделями, сосредоточенными главным образом на предупреждении угроз, и более современными концепциями, где в центр выдвигаются обнаружение инцидентов и последующее реагирование. На этом фоне статические модели защиты уже не выглядят достаточными: в среде динамичных киберугроз их результативность постепенно снижается.

Результаты

В организации средства защиты работают разрозненно, уязвимость проявляется не в отсутствии отдельных технологий, а в несовпадении их действий. Именно такую картину выявил системный подход при рассмотрении защиты объектов КИИ: речь идет не о наборе самостоятельных решений, а о совокупности взаимосвязанных элементов, где результат определяется степенью их согласования [2]. В большинстве проанализированных случаев обнаруживался перекос между технической и организационной частями системы безопасности; при комплексных атаках такая несбалансированность сказывается особенно заметно.

При сравнении моделей защиты различие обнаружилось не только на уровне инструментов, но и в самой логике функционирования. Классические схемы в основном строятся вокруг предотвращения угроз через периметровую защиту. Иной тип демонстрируют современные концепции: здесь защита не замыкается на рубеже доступа, а включает непрерывный мониторинг, выявление аномалий и быстрое реагирование на инциденты [1]. Это расхождение удобно представить в виде таблицы 1.

Таблица 1 – Сравнительный анализ моделей защиты объектов КИИ

Критерий	Традиционная модель	Современная модель
Основной принцип	Предотвращение угроз	Обнаружение и реагирование
Архитектура	Периметровая	Многоуровневая
Скорость реакции	Низкая	Высокая (в реальном времени)
Учет новых угроз	Ограниченный	Адаптивный
Роль персонала	Формальная	Активная, вовлеченная
Используемые технологии	Антивирусы, межсетевые экраны	SIEM, IDS/IPS, аналитика поведения

Сопоставление показывает, что при переходе к современным моделям устойчивость информационной инфраструктуры оказывается выше. Однако в практической плоскости этот переход наталкивается на ряд ограничений, и первое из них связано с недостаточной интеграцией средств защиты. Отдельные системы продолжают функционировать изолированно, из-за чего целостная картина событий безопасности складывается с запаздыванием или не складывается вовсе; время реакции на инциденты, соответственно, возрастает. Для распределенных информационных систем подобная разобщенность становится уже не частным недостатком, а критическим ограничением [4].

Другая группа уязвимостей обнаруживается при разборе сценариев атак. Значительная их часть связана с человеческим фактором: даже при наличии технических средств защиты сотрудники нередко оказываются той точкой, через которую злоумышленники получают начальный доступ. На этом фоне формальный инструктаж выглядит недостаточным; акцент смещается в сторону практико-

ориентированной подготовки, где безопасное поведение закрепляется не декларативно, а в рабочих ситуациях [3].

Отдельно выявилась еще одна проблема: действующие механизмы защиты слабо учитывают вероятностную природу угроз. При отсутствии риск-ориентированного подхода ресурсы распределяются неравномерно. Существенные усилия направляются на прикрытие второстепенных активов, тогда как элементы инфраструктуры, действительно критичные для функционирования организации, сохраняют уязвимость [5].

Из выявленных затруднений вытекает комплекс направлений, по которым целесообразно перерабатывать защиту объектов КИИ. Речь идет о внедрении централизованных систем мониторинга и корреляции событий безопасности; о переходе к многоуровневой архитектуре с элементами адаптивного реагирования; о развитии механизмов анализа поведения пользователей и систем. К этому добавляются регулярное моделирование атак и проведение тестирования на проникновение, формирование устойчивых навыков безопасного поведения у персонала, а также применение риск-ориентированного подхода при распределении ресурсов защиты [2].

При такой конфигурации элементы системы безопасности начинают соотноситься между собой иначе: разрывы между организационными и техническими компонентами сокращаются, а сама защита оказывается более подготовленной к постоянно меняющейся угрозной среде.

Заключение

В ходе исследования выяснилось, что результативность защиты объектов критической информационной инфраструктуры связана прежде всего не с присутствием отдельных технических средств как таковых, а с тем, насколько они интегрированы и согласованы внутри единой системы. На этом фоне традиционные модели, сосредоточенные главным образом на предупреждении угроз, уже не в полной мере отвечают условиям динамичной цифровой среды.

Рассмотренные материалы указывают на необходимость смещения к современным подходам, где защита строится на непрерывном мониторинге, оперативном реагировании и риск-ориентированном управлении безопасностью. Практическая значимость проведенной работы определяется тем, что предложенные направления совершенствования применимы при модернизации систем информационной безопасности в организациях; в такой конфигурации устойчивость КИИ к актуальным киберугрозам оказывается выше.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гавдан Г. П. и др. Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2022. – Т. 29. – №. 4. – С. 53–66.
2. Евдокимова Д. А., Микрюков А. А. Актуальные задачи выявления недопустимых событий на объектах критической информационной инфраструктуры // Открытое образование. – 2024. – Т. 28. – №. 4. – С. 33–42.

3. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии // Офтальмохирургия. – 2022. – №. 4s. – С. 92–101.
4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 277 с.
5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 252 с.

© М. Д. Рублев, А. В. Шабурова, 2026