ЭКОНОМИКА ДАННЫХ: СЕТИ И СИСТЕМЫ СВЯЗИ

Проектирование защищенной сетевой инфраструктуры предприятия: от архитектуры до программно-аппаратных средств защиты

С.С. Соколов, Государственный университет морского и речного флота (ГУМРФ) им. адмирала С.О. Макарова, ректор, профессор, д.т.н.; sokolovss@gumrf.ru
О.С. Лаута, ГУМРФ им. адмирала С.О. Макарова, профессор, д.т.н.; laos-82@yandex.ru
М.В. Митрофанов, Национальный исследовательский университет ИТМО, доцент, д.т.н.; vonafortim@yandex.ru
А.С. Куракин, ООО «Специальный Технологический Центр», начальник направления, к.т.н.; nirt@mail.ru
Н.Н. Крамской, ООО «Специальный Технологический Центр», заместитель директора по разработке специальных средств - генеральный конструктор систем и комплексов криптографической защиты информации; kram.com@mail.ru

УДК 004.056.5 DOI: 10.34832/ELSV.2026.78.4.001

Аннотация. *В статье предложен комплексный подход к проектированию защищенной сетевой инфраструктуры предприятия, базирующийся на принципах Security by Design, который предполагает интеграцию требований безопасности на всех этапах жизненного цикла системы – от физического размещения оборудования до настройки прикладного программного обеспечения. В рамках исследования разработана референсная архитектура, включающая сегментацию сети на уровне L3, использование бастион-серверов для администрирования, централизованную систему управления доступом, отключение неиспользуемых сервисов и строгую фильтрацию трафика. Экспериментальная верификация на стенде продемонстрировала, что предложенная архитектура эффективно блокирует попытки горизонтального перемещения внутри сети, повышает устойчивость к DDoS-атакам и обеспечивает обнаружение 95% инцидентов в течение первых 5 минут.*

Ключевые слова: *защищенная сетевая инфраструктура, информационная безопасность, сетевая архитектура, киберугрозы, межсетевое экранирование, защита от DDoS-атак, управление доступом (IAM), резервное копирование.*

Для цитирования: *Соколов, С.С. Проектирование защищенной сетевой инфраструктуры предприятия: от архитектуры до программно-аппаратных средств защиты / С.С. Соколов, О.С. Лаута, М.В. Митрофанов и др. // Электросвязь. – 2026. – № 4. – С. 2-14.*

ВВЕДЕНИЕ

Современные киберугрозы, включающие распределенные атаки на отказ в обслуживании (DDoS-атаки), целенаправленные вторжения в корпоративные сети и эксплуатация уязвимостей программного обеспечения (ПО), представляют большой риск для информационной безопасности (ИБ) предприятий любого масштаба. Статистические данные демонстрируют устойчивый рост количества успешных кибератак, причем в центре внимания злоумышленников оказываются как крупные финансово-технологические компании, так и небольшие организации, использующие ограниченное количество серверов. Анализ инцидентов ИБ показывает, что значительная доля успешных атак обусловлена не столько техническим превосходством злоумышленников, сколько фундаментальными недостатками архитектурного проектирования защищенных систем, когда меры безопасности внедряются постфактум, после развертывания основной инфраструктуры. Данная ситуация актуализирует необходимость разработки комплексного подхода к проектированию сетевой инфраструктуры предприятия, в которой требования ИБ интегрированы на всех уровнях – от физического размещения оборудования до конфигурирования прикладных сервисов [1–5].

Рассматривая существующую практику построения корпоративных информационных систем, необходимо выделить ряд противоречий, препятствующих достижению требуемого уровня защищенности (рис. 1). Первое противоречие заключается в дихотомии между необходимостью обеспечения публичного доступа к сервисам предприятия и требованиями изоляции внутренних ресурсов от внешних угроз. Традиционный подход предполагает размещение всех серверов с прямым доступом в публичную сеть, что создает расширенную поверхность атаки и позволяет злоумышленникам проводить сканирование на предмет известных уязвимостей.

Второе противоречие связано с организацией взаимодействия между компонентами распределенной системы: связывание ресурсов на канальном уровне