Стратегическое управление информационной безопасностью: методологический фреймворк перехода от реактивной к проактивной модели защиты

С.С. Соколов, Государственный университет морского и речного флота им. адмирала С.О. Макарова, ректор, профессор, д.т.н.; sokolovss@gumrf.ru
М.В. Митрофанов, Национальный исследовательский университет ИТМО, доцент, д.т.н.; vonafortim@yandex.ru
О.С. Лаута, Государственный университет морского и речного флота им. адмирала С.О. Макарова, профессор, д.т.н.; laos-82@yandex.ru
А.С. Куракин, ООО «Специальный Технологический Центр», начальник направления, к.т.н.; nirt@mail.ru
Т.П. Кныш, Государственный университет морского и речного флота им. адмирала С.О. Макарова, проректор по вопросам организации и развития образовательного процесса высшего и среднего профессионального образования, информатизации и цифровизации, доцент, к.ф.-м.н.; knyshtp@gumrf.ru

УДК 004.056.5 DOI: 10.34832/ELSV.2026.77.3.010

Аннотация. *Статья предлагает инновационный структурированный подход, который определяет стратегическое управление информационной безопасностью (методологический фреймворк). Он обеспечивает переход от реактивной модели к проактивной защите в условиях экспоненциального роста киберугроз. Разработан гибридный подход на базе инструментов стратегического менеджмента, адаптированных к информационной безопасности (GAP-анализ, моделирование As is/To be, SWOT-анализ для оценки сильных/слабых сторон и угроз, критерии SMART для конкретизации целей; Balanced Scorecard (BSC) для метрик по четырем проекциям (финансовая, клиентская, процессная, развитие); стейкхолдер-анализ для гармонизации интересов; моделирование дорожной карты трансформации). Фреймворк трансформирует информационную безопасность из центра затрат в стратегический актив и снижает риски утечек. Он обеспечивает прогнозирование атак, оптимизацию ресурсов и адаптивность к неизвестным уязвимостям. Практическая реализация включает аудит, дорожную карту проекта (roadmap) и мониторинг ключевых показателей эффективности.*

Ключевые слова: *стратегическое управление информационной безопасностью, проактивная защита, GAP-анализ, SWOT-анализ, Balanced Scorecard, SMART, стейкхолдер-анализ, киберугрозы, управление рисками, цифровая трансформация.*

Для цитирования: *Соколов, С.С. Стратегическое управление информационной безопасностью: методологический фреймворк перехода от реактивной к проактивной модели защиты / С.С. Соколов, М.В. Митрофанов, О.С. Лаута и др. // Электросвязь. – 2026. – № 3. – С. 83-88.*

ВВЕДЕНИЕ

Современное управление информационной безопасностью находится в состоянии фундаментального противоречия между объективной необходимостью проактивного стратегического планирования и доминированием реактивной операционной парадигмы. Актуальность данной проблематики подтверждается отрицательной динамикой ландшафта киберугроз: по данным RED Security SOC, за девять месяцев 2025 г. в России зафиксировано более 105 тыс. кибератак, что на 46% превышает показатели аналогичного периода предыдущего года, при этом каждая пятая атака классифицирована как критическая с потенциалом нанесения ущерба свыше 1 млн рублей. Согласно исследованию группы компаний «Солар», количество высококритичных инцидентов в 2024 г. возросло двукратно по сравнению с предшествующим годом, причем более половины успешных атак пришлись на государственный сектор. Фишинговые атаки продемонстрировали рост в 425%, согласно данным Центра мониторинга Роскомнадзора, в то время как количество DDoS-атак увеличилось на 70%. Эти показатели свидетельствуют о неспособности традиционных реактивных механизмов обеспечить адекватную защиту в условиях цифровой трансформации бизнес-процессов [1–3].

Противоречие в практике управления ИБ проявляется в концентрации ресурсов на тактических задачах ситуативной нейтрализации инцидентов, устранения уязвимостей и выполнения регуляторных предписаний, что препятствует интеграции функции безопасности в процессы создания стоимости и трансформации подразделений ИБ из центров затрат в стратегические активы организации. Исследование