Мешков Егор Олегович, Студент
Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

Енин Николай Николаевич
заместитель начальника кафедры КВВУ
Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

Жила Дмитрий Георгиевич, слушатель
Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

Пономарев Василий Юрьевич, слушатель
Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

ОБОСНОВАНИЕ ВЫБОРА ОПТИМАЛЬНОГО НАБОРА МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. В статье рассматривается проблема выбора оптимального набора мер защиты информации для объектов критической информационной инфраструктуры (КИИ). Предлагается методика структурно-уровневого анализа, развивающая принцип эшелонированной защиты с учетом требований ФЗ №187-ФЗ и нормативных документов ФСТЭК. Методика систематизирует обязательные и компенсирующие меры, обосновывает приоритеты распределения ресурсов. На примере объекта КИИ второй категории значимости (АСУ энергосетью) демонстрируется практическое применение подхода

Ключевые слова: Критическая информационная инфраструктура, информационная безопасность, многоуровневая модель защиты, оптимальный набор мер

Объектом КИИ является совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, которые обеспечивают функционирование важнейших сфер экономики и государственной безопасности. В соответствии с Федеральным законом №187-ФЗ субъекты КИИ обязаны обеспечивать защиту важных объектов от целевых компьютерных атак [1].

Зачастую на практике выбор мер защиты часто осуществляется либо формально – как простое перечисление требований регулятора, либо на основе субъективных предпочтений специалистов. Это приводит к несбалансированности системы защиты, когда отдельные направления получают избыточное обеспечение, в то время как другие остаются уязвимыми.

Гипотеза исследования состоит в том, что применение структурно-уровневой модели для анализа обязательных мер защиты позволяет выявить системные ошибки и обосновать выбор оптимального набора мер.

Существующий нормативный подход, определяющий базовые требования в соответствии с категорией значимости объекта, необходим, но недостаточен для формирования эффективной системы защиты.

Предлагаемая архитектурная модель развивает принцип эшелонированной защиты с учетом специфики объектов КИИ и требований российского регулятора. Модель включает пять уровней защиты.

Уровень 1 включает периметр и физическую безопасность: контроль физического доступа к объектам КИИ, защиту кабельных линий и инженерной инфраструктуры, системы видеонаблюдения и охранной сигнализации.

Уровень 2 представляет сетевую инфраструктуру: сегментацию сетей и управление сетевыми потоками, межсетевые экраны и системы обнаружения/предотвращения вторжений, защиту каналов связи и сетевых протоколов.

Уровень 3 программно-аппаратные комплексы: антивирусная защита, средства мониторинга и логирования безопасности, модули доверенной загрузки.

Уровень 4 защиты приложений и данных: контроль доступа к приложениям и базам данных, шифрование и защиту конфиденциальной информации, контроль целостности и резервное копирование.

Уровень 5 политики безопасности и администрирования: управление инцидентами информационной безопасности, мониторинг и аудит событий безопасности, обучение и повышение осведомленности персонала.

Методика структурно-уровневого анализа включает следующие этапы: формирование исходного набора мер в соответствии с категорией значимости объекта КИИ; распределение мер по уровням архитектурной модели; анализ сбалансированности; выявление "зон риска" – уровней с недостаточным покрытием или отсутствием дополнительных решений; обоснование выбора дополнительных мер через анализ воздействия на выявленные "уязвимые зоны" и парирование идентифицированных угроз.

Рассмотрим применение предложенной методики для условного объекта КИИ, отнесенного ко 2-й категории значимости (автоматизированной системы управления электрической сетью).

Базовый набор мер защиты формируется из 17 типов организационных и технических мер, предусмотренных Разделом III Приказа ФСТЭК России №239 [2].

Сформированные меры были распределены по пяти уровням архитектурной модели защиты в таблице 1.

Таблица 1

Распределение мер защиты по уровням архитектурной модели

Уровень защиты	**Количество мер**	**Применяемые меры защиты**
Уровень 1: Физическая безопасность	1	Система контроля и управления доступом
Уровень 2: Сетевая инфраструктура	2	Межсетевые экраны, сегментация сетевой инфраструктуры
Уровень 3: Программно-аппаратные комплексы	2	Модули доверенной загрузки, антивирусная защита
Уровень 4: Приложения и данные	1	Резервное копирование данных
Уровень 5: Процессы управления безопасностью	2	Мониторинг событий информационной безопасности, информирование и обучение персонала

На основе предложенной методики был проведён анализ сбалансированности распределения мер защиты по уровням архитектурной модели. Результаты анализа представлены в таблице 2.

Таблица 2

Результаты анализа сбалансированности системы защиты

Уровень защиты	**Оценка сбалансированности**	**Выявленные риски**
Уровень 1: Физическая безопасность	Недостаточно	Отсутствие системы разграничения доступа к оборудованию и кабельным линиям
Уровень 2: Сетевая инфраструктура	Сбалансированно	–
Уровень 3: Программно-аппаратные комплексы	Сбалансированно	–
Уровень 4: Приложения и данные	Недостаточно	Отсутствие средств обеспечения целостности критичных данных технологического процесса
Уровень 5: Управление персоналом	Сбалансированно	–

На основе выявленных зон риска и сопоставления с актуальной моделью угроз были предложены следующие дополнительные меры:

Для уровня 1 – внедрение системы разграничения доступа к оборудованию и кабельным линиям в соответствии с должностными обязанностями

Для уровня 4 – реализация средств криптографической защиты и контроля целостности критичных данных технологического процесса, обеспечивающих защиту от несанкционированного изменения технологического процесса [3].

Предложенная методика структурно-уровневого анализа предоставляет практический инструмент для обоснованного выбора оптимального набора мер защиты информации для объектов КИИ. Она позволяет систематизировать требования регулятора в рамках многоуровневой архитектуры, объективно выявлять дефициты в защите, связывать предлагаемые меры с конкретными угрозами и дефицитами, обосновывать решения по инвестициям в защиту перед руководством. Апробация на примере АСУ энергосети 2-й категории значимости показала эффективность подхода и практическую применимость для реальных объектов КИИ. Полученные результаты подтверждают, что структурированный анализ позволяет перейти от формального выполнения нормативных требований к созданию действительно защищенной и сбалансированной системы безопасности.

Перспективы дальнейших исследований включают разработку формальных метрик для количественной оценки сбалансированности системы защиты, адаптацию методики для специфических подсистем КИИ, а также интеграцию с банком данных угроз ФСТЭК для анализа покрытия тактик целевых атак.

Список литературы:

1. О безопасности критической информационной инфраструктуры Российской Федерации [Текст]: Федеральный закон от 26 июля 2017 г. № 187-ФЗ.

2. Федеральная служба по техническому и экспортному контролю. Приказ от 25 декабря 2017 г. № 239 [Текст]: Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

3. Бородин А. М., Енин Н. Н., Углов А. Е [и др.] Специальное программное обеспечение автоматизации контроля за событиями информационной безопасности [Текст]: свидетельство о государственной регистрации программы для ЭВМ № 2024615656; заявл. 19.03.2024; опубл. 27.03.2024.

4.Горшков Г. Д., Кошелев А. А., Акишин А. В [и др.] Угрозы безопасности беспроводных сетей, реализуемые утилитой "Aircrack-ng" // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. – 2021. – № 1 (14). – С. 149–153.

5.Охотин Д. А., Акишин А. В., Хечиев Н. В [и др.] Анализ и классификация угроз информационной безопасности на автоматизированных системах // Вектор научной мысли. – 2025. – № 1 (18). – С. 389–392.

6.Свидетельство о государственной регистрации программы для ЭВМ № 2024617023 [Текст]. Российская Федерация.