УДК 004.056

Модель декомпозиции объектов критической информационной инфраструктуры для анализа угроз информационной безопасности

Decomposition model of critical information infrastructure objects for information security threat analysis

Митяков / Mityakov E.
Евгений Сергеевич
(iyao@mail.ru)
доктор экономических наук, профессор.
ФГБОУ ВО «МИРЭА – Российский технологический университет», заведующий кафедрой КБ-9 «Предметно-ориентированные информационные системы».
г. Москва

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ (ВАС им. С. М. Буденного),
профессор кафедры автоматизированных систем специального назначения.
г. Санкт-Петербург

Садовников / Sadovnikov V.
Владимир Евгеньевич
(bladimir1998@mail.ru)
ВАС им. С. М. Буденного,
младший научный сотрудник научно-исследовательского центра.
г. Санкт-Петербург

Ключевые слова: критическая информационная инфраструктура – critical information infrastructure; моделирование угроз – threat modeling; каскадные риски – cascade risks; цифровая симуляция – digital simulation; информационная безопасность – information security; управление рисками – risk management.

Предложена иерархическая модель декомпозиции объектов критической информационной инфраструктуры, содержащая пять взаимосвязанных срезов (технический, процессный, организационный, функциональный, отраслевой) для анализа каскадных угроз информационной безопасности. Модель формализует перекрестные зависимости между срезами через матрицы взаимовлияния, позволяя выявлять скрытые сценарии распространения рисков в гетерогенных системах. Практическая верификация подтвердила эффективность модели: анализ базы угроз ФСТЭК выявил, что 73 % инцидентов затрагивают более одного среза, а симуляция на примере смарт-сети энергетики продемонстрировала снижение негативных последствий от реализации угроз на 55 % после оптимизации мер защиты, направленной на нейтрализацию межсрезовых угроз.

A hierarchical decomposition model of Critical Information Infrastructure (CII) objects into five interrelated layers (technical, process, organizational, functional, sectoral) is proposed for analyzing cascade information security threats. The model formalizes cross-layer dependencies through mutual influence matrices, enabling the identification of hidden risk propagation scenarios in heterogeneous systems. Practical verification confirmed its effectiveness: analysis of the Federal Service for Technical and Export Control threat database revealed that 73 % of incidents affect more than one layer, while a simulation of a smart power grid demonstrated a 55 % reduction in the impact of realized cross-layer threats after optimizing protection measures.

Введение

Современное общество в значительной степени зависит от устойчивой работы информационных систем (ИС), сетей связи и автоматизированных систем управления (АСУ), составляющих основу критической информационной инфраструктуры (КИИ). Нарушения в функционировании этих компонентов могут привести к серьезным последствиям в социально и экономически значимых сферах. Несмотря на наличие нормативно-методической базы (Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ; Постановление Правительства РФ от 08.02.2018 № 127, рекомендации ФСТЭК России), большая часть действующих документов ориентирована преимущественно на регламентацию процедур, а не на аналитику сложных межкомпонентных взаимодействий.

Цель настоящего исследования – разработка иерархической модели декомпозиции объектов КИИ, предназначенной для анализа угроз информационной безопасности (ИБ).

Разработка модели декомпозиции объектов КИИ

В качестве методологической основы предлагаемой модели используется принцип анализа по срезам, который концептуально близок к подходам, применяемым в стандартах информационной и функциональной безопасности, таких как ISO/IEC 27001 и IEC 61508. Однако указанные стандарты, как и большинство существующих нормативных документов (включая ISO 23247, ГОСТ Р 57700.37–2021), ориентированы преимущественно на компонентный или системный уровень анализа и не предусматривают детальную формализацию перекрестных зависимостей между разнотипными компонентами инфраструктуры.

При этом в КИИ наблюдаются сложные нелинейные взаимодействия между техническими, организационными, процессными и иными элементами. Такие взаимодействия способны порождать каскадные эффекты, которые выходят за рамки линейных моделей угроз, характерных для вышеупомянутых стандартов. Предлагаемая модель вводит понятие «среза» – обобщенной структурно-функциональной единицы анализа. Использование анализа по срезам обеспечивает более гибкую и масштабируемую основу для анализа угроз в условиях гетерогенности и высокой взаимозависимости компонентов. При этом модель развивает классические подходы, осуществляя синтез технического, процессного, организационного, функционального и отраслевого срезов в единую систему.

Предлагаемая модель строится на принципе разбиения объекта КИИ на пять взаимосвязанных срезов: технический, процессный, организационный, функциональный и отраслевой. Каждый срез представляет самостоятельное основание для анализа угроз и описывает конкретные аспекты функционирования инфраструктуры.

Модель интегрирует современные подходы к декомпозиции систем и анализу угроз КИИ:

- методики оценки критичности компонентов на основе анализа рисков и последствий сбоев [1, 2];
- алгоритмы структурирования сертифицированных и неидентифицированных элементов инфраструктуры [3];
- анализ взаимозависимостей для предотвращения каскадных сбоев [4, 5];
- использование методов анализа данных для выделения ключевых узлов [6, 7];
- методы оценки уязвимостей при комбинированных сбоях [8];
- методы декомпозиции сложных систем [9–11].

На основе контент-анализа Федерального закона № 187-ФЗ и других нормативно-методических документов в сфере ИБ (включая нормативные акты, регулирующие КИИ) в рамках предлагаемой модели выделены пять срезов. Каждый срез представляет собой самостоятельное основание для исследования и позволяет детализировать описание структуры и функций объектов КИИ (таблица 1).

Для формализации каскадных зависимостей между различными аспектами функционирования объектов КИИ разработана матрица взаимовлияний срезов (таблица 2). Она отражает, каким образом нарушения в одном срезе могут провоцировать сбои в других.

Иерархическая структура модели задает архитектуру данных, необходимую для анализа угроз объектов КИИ. По аналогии с матрицей взаимосвязей (см. табл. 2) возможно построение матриц для подсрезов.

Пошаговый подход к внедрению модели представлен в таблице 3.

На основе выявленных взаимосвязей можно строить цепочки распространения угроз, отражающие, как воздействие на один элемент системы способно вызывать последствия на других уровнях.

Практическая верификация модели

С целью подтверждения эффективности и прикладной применимости разработанной модели декомпозиции объектов КИИ была проведена многоуровневая верификация. Она включает как обобщенный статистический анализ угроз из Банка данных угроз ФСТЭК (БДУ), так и детализированную проверку на конкретном объекте – цифровой интеллектуальной энергетической системе (смарт-сети). Такой подход позволяет одновременно оценить системный охват модели и ее способность формализовать развитие угроз в реальных условиях.

Таблица 1

Детализация срезов и источники угроз

Срез	Элементы декомпозиции (подсрезы)	Источники угроз (примеры)
Технический	• Физическая инфраструктура (электропитание, СКУД); • Сетевое оборудование (маршрутизаторы, каналы связи); • Информационные системы (SCADA, АСУ ТП); • ПО (ОС, прикладное ПО); • СЗИ (МЭ, IDS/IPS).	Эксплуатация уязвимостей ПО/ОС, сетевые атаки, физический саботаж
Процессный	• Идентификация угроз (мониторинг, анализ); • Оценка угроз (классификация, прогнозирование); • Принятие решений (стратегии реагирования); • Исполнение мер защиты; • Контроль и обратная связь (аудит, корректировка).	Нарушение регламентов реагирования, ошибки эскалации инцидентов
Организационный	• Уровень регуляторов (ФСТЭК, ФСБ России, Минкомсвязь России, Центральный Банк РФ); • Стратегический уровень (топ-менеджмент); • Управленческий уровень (руководители ИБ); • Оперативный уровень (SOC, администраторы).	Недостатки нормативного контроля, низкая квалификация персонала
Функциональный	• Управление (передача команд, телеметрия); • Мониторинг (выявление отклонений); • Защита (контроль доступа, шифрование); • Восстановление (резервирование, аварийное переключение); • Взаимодействие (интеграция интерфейсов).	Сбои выполнения критических функций, нарушения SLA
Отраслевой	• Межсубъектные связи: - Нейтральная (изменения не влияют на другие субъекты); - Прямая (детерминированное влияние); - Косвенная (стохастическая зависимость).	Отраслевые кибератаки (например, на объекты энергетики), специфичные регуляторные риски

Таблица 2

Матрица взаимовлияний срезов

Источники влияния / Объект влияния	Технический срез	Процессный срез	Организационный срез	Функциональный срез	Отраслевой срез
Технический срез	—	Обеспечивает технические средства для реализации процедур мониторинга и реагирования на ИБ-инциденты	Ограничивает и задает технические условия для организационных мер безопасности	Поддерживает выполнение ключевых функций защиты и восстановления	Обеспечивает соответствие технических решений отраслевым стандартам защиты информации
Процессный срез	Требует надежной технической инфраструктуры для своевременного обнаружения и реагирования на угрозы	—	Зависит от организационного контроля и координации для обеспечения эффективности процессов	Опосредует выполнение функций защиты, мониторинга и восстановления	Включает процессы, адаптированные к специфике отраслевых угроз и нормативных требований
Организационный срез	Задает требования к техническим средствам и их эксплуатации с учетом рисков ИБ	Обеспечивает управление жизненным циклом ИБ-процессов и контроль исполнения мер защиты	—	Обеспечивает ресурсное и управленческое сопровождение функций безопасности	Внедряет отраслевые регуляции и стандарты ИБ в управленческие практики
Функциональный срез	Определяет технические требования для реализации функций защиты, мониторинга и восстановления	Определяет процессы, необходимые для выполнения функций ИБ и обеспечения их согласованности	Зависит от организационной поддержки для эффективного исполнения функций	—	Функциональные задачи адаптируются под отраслевые угрозы и требования безопасности
Отраслевой срез	Определяет специфические технические меры и стандарты защиты, применимые в конкретных секторах	Формирует отраслевые требования к процессам обеспечения безопасности и реагирования на угрозы	Влияет на организационные структуры и регулирующие требования, характерные для отрасли	Определяет приоритеты и специфику функциональных мер защиты в отрасли	—

Таблица 3

Практическое применение модели: пошаговые рекомендации

Этап внедрения модели	Описание действий	Практическая цель
1. Идентификация объектов КИИ	Определить состав и границы защищаемой системы	Формирование базы компонентов и подсистем
2. Классификация по срезам	Разнести элементы инфраструктуры по пяти основным срезам	Структурировать систему для анализа
3. Сбор данных об угрозах	Привязать существующие угрозы (по УБИ) к конкретным подсрезам	Выявление точек риска и зон воздействия
4. Построение матрицы взаимовлияний	Определить зависимости между срезами и возможные каскадные эффекты	Формализовать сценарии распространения угроз
5. Цифровое моделирование	Выполнить симуляцию инцидентов	Оценка уязвимости системы в динамике
6. Разработка корректирующих мер	На основе симуляции спланировать меры по устранению слабых мест	Снижение совокупного риска
7. Интеграция в процессы ИБ	Включить модель в регламенты анализа рисков, проектирования и сертификации	Обеспечение системности управления угрозами

Таблица 4

Распределение угроз безопасности информации по срезам

Срез	Число угроз, затрагивающих срез	Примеры УБИ
Технический	172 (74 %)	УБИ-1, УБИ-4, УБИ-57
Процессный	89 (38 %)	УБИ-22, УБИ-46
Функциональный	83 (36 %)	УБИ-148, УБИ-123
Организационный	41 (18 %)	УБИ-65, УБИ-201
Отраслевой	33 (14 %)	УБИ-112, УБИ-206

Таблица 5

Матрица взаимодействия срезов

Цель / Источник	Технический срез	Процессный срез	Организационный срез	Функциональный срез	Отраслевой срез
Технический срез	—	0,44	0,21	0,52	0,17
Процессный срез	0,38	—	0,29	0,41	0,14
Организационный срез	0,22	0,39	—	0,34	0,12
Функциональный срез	0,36	0,28	0,18	—	0,20
Отраслевой срез	0,31	0,20	0,13	0,38	—

Таблица 6

Угрозы безопасности информации интеллектуальной распределенной энергетической сети

УБИ	Наименование	Срезы воздействия
183	Перехват управления автоматизированной системой управления (АСУ)	Технический срез → Процессный срез, Функциональный срез
214	Задержка реагирования центра мониторинга безопасности (SOC)	Процессный срез → Организационный срез, Функциональный срез
65	Нечеткое распределение ответственности	Организационный срез → Процессный срез, Функциональный срез
112	Выполнение запрещенных команд в отраслевой инфраструктуре	Отраслевой срез → Функциональный срез, Технический срез
148	Сбой в системе управления доступом	Функциональный срез → Технический срез, Отраслевой срез
32	Подмена сигнатур программного обеспечения прошивок	Технический срез → Функциональный срез
206	Сбой оборудования при миграции	Отраслевой срез → Технический срез
54	Недобросовестность поставщика	Организационный срез → Технический срез
53	Потеря управления правами доступа	Функциональный срез → Организационный срез
46	Нарушение аутентификации при доступе	Процессный срез → Функциональный срез

Верификация модели осуществлялась на двух уровнях:

1. Общесистемный уровень – классификация 222 угроз из БДУ ФСТЭК по пяти срезам модели.

2. Прикладной уровень – цифровое моделирование каскадного инцидента в инфраструктуре смарт-сети, включающее построение матрицы влияния и симуляцию развития угроз.

Каждая угроза из БДУ ФСТЭК была проанализирована и классифицирована по одному или нескольким срезам: техническому, процессному, организационному, функциональному и отраслевому. В результате классификации выявлено распределение, представленное в таблице 4.

Отдельно стоит отметить, что 162 угрозы (73 %) одновременно затрагивают более одного среза, что свидетельствует о наличии значительного числа каскадных рисков. Эти данные подтверждают актуальность использования межсрезового моделирования в оценке устойчивости объектов КИИ.

Для количественной оценки взаимовлияний между срезами введем коэффициент влияния (КВ):

$$\text{КВ}_{A\to B} = \frac{N_{A\cap B}}{N_A}$$

где $N_{A\cap B}$ – количество угроз, относящихся одновременно к срезам A и B; N_A – общее количество угроз в срезе A.

Полученные значения можно рассматривать как условные вероятности того, что угроза, относящаяся к одному срезу, затронет другой срез, что позволяет строить матрицы взаимного влияния между аспектами критической информационной инфраструктуры (таблица 5). На пересечении соответствующих ячеек матрицы КВ фиксируется доля угроз исходного среза (столбец «Источник»), способных вызвать инциденты в целевом срезе (строка «Цель»). Например, значение 0,52 в ячейке пересечения технического источника и функционального назначения означает, что 52 % всех угроз технического среза также затрагивают функциональный.

С целью прикладной верификации разработанной модели декомпозиции объектов критической информационной инфраструктуры была выполнена симуляция инцидента в интеллектуальной распределенной энергетической сети (смарт-сети). Анализируемый объект включал узлы SCADA, элементы управления доступом, подсистемы телеметрии, а также компоненты взаимодействия с облачными сервисами.

В рамках исследования были идентифицированы десять угроз, каждая из которых задействует один или несколько срезов модели (таблица 6). В столбце «Срезы воздействия» показано направление влияния угроз: от исходного (источника) среза к целевым срезам, которые затрагиваются данной угрозой. Такая запись позволяет анализировать межсрезовые переходы и строить матрицы влияния для оценки каскадных рисков.

Для количественной оценки межсрезовых взаимодействий угроз была построена матрица КВ, отражающая долю угроз из одного среза, способных провоцировать инциденты в другом (таблица 7).

Матрица демонстрирует, что наибольший потенциал каскадного распространения угроз имеют направления: «Процессный → Функциональный», «Функ-

Таблица 7

Матрица взаимодействия срезов распределенной энергетической сети

Цель / Источник	Технический срез	Процессный срез	Организационный срез	Функциональный срез	Отраслевой срез
Технический срез	—	0,50	0,00	1.00	0,00
Процессный срез	0,00	—	0,50	1.00	0,00
Организационный срез	0,50	0,50	—	0,50	0,00
Функциональный срез	0,50	0,00	0,50	—	0,50
Отраслевой срез	1.00	0,00	0,00	0,50	—

циональный → Технический», «Отраслевой → Функциональный».

В рамках цифровой симуляции был смоделирован сценарий инцидента, инициированного эксплуатацией уязвимости в SCADA-системе (УБИ-183). Эволюция инцидента, вызванного каскадом угроз, развивалась по следующей цепочке: УБИ-183 (технический срез) → УБИ-214 (процессный срез) → УБИ-65 (организационный срез) → УБИ-148 (функциональный срез) → УБИ-112 (отраслевой срез) → отказ элементов смарт-сети.

В ходе моделирования зафиксировано стремительное нарастание тяжести последствий в течение первых 60 минут развития инцидента. При отсутствии корректирующих мер вероятность полномасштабной реализации угрозы (отказ элементов) достигала 92 %. На основании модели были предложены следующие меры нейтрализации угроз и повышения устойчивости системы:

· Устранение уязвимости SCADA → снижение уязвимости технического среза на 65 % (к угрозе УБИ-183).

· Автоматизация реагирования SOC → повышение эффективности противодействия угрозам в процессном срезе на 50 % (к угрозе УБИ-214).

· Перераспределение зон ответственности → снижение вероятности реализации организационных угроз на 60 % (к угрозе УБИ-65).

· Централизация управления доступом → повышение устойчивости функционального среза на 40 % (к угрозам типа УБИ-148, УБИ-53, УБИ-46).

Итоговая симуляция после внедрения указанных мероприятий показала снижение вероятности реализации каскада угроз до критического отказа на 55 %, а также сокращение времени реагирования на инцидент на 28 %.

Заключение

Таким образом, в статье предложена иерархическая модель декомпозиции объектов КИИ на пять взаимосвязанных срезов – технический, процессный, организационный, функциональный и отраслевой.

Новизна модели заключается в создании формализованной основы для цифрового моделирования и количественной оценки каскадных угроз объектам КИИ через выявление и структурирование перекрестных зависимостей между ее разнородными аспектами их функционирования. Ключевым инструментом модели выступают матрицы взаимовлияния срезов, позволяющие строить и симулировать сложные сценарии распространения угроз в цифровой среде, выявляя скрытые каскадные эффекты, не улавливаемые традиционными методами изолированного анализа.

Практическая ценность модели для задач моделирования и оценки рисков подтверждена верификацией: анализ БДУ ФСТЭК количественно показал преобладание межсрезовых угроз (73 %), а цифровая симуляция на примере смарт-сети продемонстрировала возможность снижения негативных последствий от реализации угроз на 55 % после оптимизации мер защиты.

Литература

1. Щелкин, К. Е. Возможные подходы к категорированию объектов критической информационной инфраструктуры / К.Е. Щелкин, П.А. Звягинцева, В.В. Селифанов // Интерэкспо Гео-Сибирь. – 2019. – Т. 6, № 1. – С. 128–133.

2. Подход к проведению категорирования объектов критической информационной инфраструктуры / В.Н. Труфанов, С.Е. Соболев, О.А. Панина [и др.] // Информатизация и связь. – 2021. – № 6. – С. 163–170.

3. Категорирование взаимосвязанных объектов критической информационной инфраструктуры / Д.М. Маличев, Х.Х. Кучмезов, В.В. Мочалов [и др.] // Прикладная информатика. – 2022. – Т. 17, № 3 (99). – С. 105–116.

4. Grigalashvili, V. The essence of critical infrastructure in the European Union, NATO and G7 countries / V. Grigalashvili // International Journal of Innovative Technologies in Economy. – 2022. – Vol. 1, No. 37.

5. Shamsi, N. Interdependency classification: A framework for infrastructure resilience / N. Shamsi, A. Helmrich // Environmental Research: Infrastructure and Sustainability. – 2025. – Vol. 5, No. 1. – P. 015009.

6. A Feature Selection-based Approach for the Identification of Critical Components in Complex Technical Infrastructures: Application to the CERN Large Hadron Collider / P. Baraldi, A. Castellano, A. Shokry [et al.] // Reliability Engineering & System Safety. – 2020. – Vol. 201. – P. 106974.

7. Lu, X. A data-driven framework for identifying important components in complex systems / X. Lu, P. Baraldi, E. Zio // Reliability Engineering & System Safety. – 2020. – Vol. 204. – P. 107197.

8. Jцnsson, H. Identifying critical components in technical infrastructure networks / H. Jцnsson, J. Johansson, H. Tehler // Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Threat and Reliability. – 2008. – Vol. 222, Iss. 2. – P. 235–243.

9. Анализ функционирования и структурная декомпозиция информационных систем специального назначения / В.И. Сумин, Т.Е. Смоленцева, Ю.Ю. Громов, В.М. Тютюнник // Научно-техническая информация. Серия 2: Информационные процессы и системы. – 2021. – № 8. – С. 5–14.

10. Белинская, Ю. С. Декомпозиция систем и терминальное управление / Ю.С. Белинская, В.Н. Четвериков // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия Естественные науки. – 2017. – № 6 (75). – С. 103–125.

11. Захарченко, Р. И. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве / Р.И. Захарченко, И.Д. Королев // Наукоемкие технологии в космических исследованиях Земли. – 2018. – Т. 10, № 2. – С. 52–61.