DOI: 10.58168/MIST2026_282-289
УДК 303.732.4

# О ПРИМЕНЕНИИ МЕТОДОВ СИСТЕМНОГО АНАЛИЗА В ПРОЕКТИРОВАНИИ И РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.С. Кравченко[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. О применении системного анализа в разработке безопасного программного обеспечения. Детализирован алгоритм анализа угроз с раскрытием применения методов системного анализа. Приведен пример декомпозиции системы на составляющие элементы и идентификация возможных угроз безопасности информационных ресурсов

Ключевые слова: Системный анализ, декомпозиция, SWOT-анализ, «What if»-модели.

# ON THE APPLICATION OF SYSTEM ANALYSIS METHODS IN THE DESIGN AND DEVELOPMENT OF SECURE SOFTWARE

A.S. Kravchenko[1]

[1] Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. On the application of system analysis 41in the development of secure software. The algorithm of threat analysis is detailed, with the application of system analysis methods. An example of system decomposition into constituent elements and identification of possible threats to the security of information resources is given.

Keywords: System analysis, decomposition, SWOT analysis, «What if» models.

## Введение

Среди всех практических приложений системного анализа к разработке безопасного программного обеспечения можно выделить три наиболее значимых:

© Кравченко А. С., 2026

1. Выявление угроз и рисков безопасности информационных ресурсов: Выявление потенциальных угроз и уязвимостей информационных систем при проектировании позволяет заранее обеспечить внедрение мер купирования угроз и снижения рисков.

2. Аспект структурирования требований к безопасности обработки информационных ресурсов: Аппарат теории системного анализа позволяет сформировать определенные и однозначные функциональные и нефункциональные требований к безопасности информационных ресурсов, разрабатываемого продукта. Что способствует согласованности целей проекта и редуцированию ошибок проектирования.

3. Решение задач оценки эффективности разрабатываемых решений: Включение в набор используемых средств методов моделирования и тестирования дает возможность вырабатывать оценку эффективности реализованных мер обеспечения безопасности информационных ресурсов, раннее обнаружение слабых мест способствует повышению качества конечного продукта.

Далее приведем описание процесса выявления угроз и рисков безопасности информационных ресурсов и выявим возможности применения аппарата системного анализа для решения этой задачи.

Следует показать, что на этапе выявления угроз и рисков безопасности информационных ресурсов аппарат системного анализа применяется для изучения внешних и внутренних факторов возникновения угроз для информационных ресурсов разрабатываемого программного обеспечения. Цель процесса состоит в идентификации потенциальных уязвимостей информационной системы [1].

В свою очередь, процесс выявления угроз и рисков безопасности информационных ресурсов можно разделить на следующие этапы:

1. **Идентификация компонентов и ресурсов:** Локализация и идентификация свойств ключевых компонентов системы, нуждающихся в обеспечении безопасности, необходима идентификация и описание конфиденциальных данных и описание с ними связанных процессов, фиксация номенклатуры программного и аппаратного обеспечения.

2. **Анализ угроз безопасности информационных ресурсов системы:** Составление номенклатуры вероятных видов атак на информационную систему, оценка их последствий. Включая как анализ известных типов атак, так и их комбинаций.

3. **Оценка рисков:** Расчет вероятности реализации угрозы безопасности и ущерба, связанного с ее реализацией. Например, рассчитывается вероятность утечки персональных данных или потери важной информации.

4. **Формулирование рекомендаций:** На основании результатов анализа формируются рекомендации по устранению выявленных угроз и снижению уровня риска.

Таким образом, системный анализ на данном этапе обеспечивает основу для принятия обоснованных решений относительно необходимых защитных мер и механизмов контроля, повышая общую защищенность программного обеспечения.

**Детализировать алгоритм анализа угроз с раскрытием применения методов системного анализа можно, например, следующим образом.**

А**нализ угроз** предполагает детальное исследование потенциально опасных ситуаций и условий, угрожающих безопасности разрабатываемого программного обеспечения [2].

**Шаг 1: Сбор и классификация информации о компонентах системы**

Цель: Определить элементы и компоненты системы, подлежащие защите. (Приём системного анализа: Декомпозиция)

**Декомпозируем систему на составляющие элементы**. Разделяем систему на модули, сервисы, базы данных, интерфейсы взаимодействия и др., определяя наиболее важные активы.

Классифицируем каждый элемент согласно уровню критичности (важности):

- Высокоприоритетные элементы (конфиденциальные данные, коммерческие тайны)
- Средней важности элементы (функциональные возможности, инфраструктура)
- Низкоприоритетные элементы (лог-файлы, вспомогательные инструменты)

**Шаг 2: Идентификация возможных угроз**

Цель: Составить полный перечень угроз для каждого элемента системы. (Приём системного анализа: SWOT-анализ (Strengths, Weaknesses, Opportunities, Threats))

Для каждого классифицированного элемента используем методику SWOT-анализа, выделяя возможные угрозы (Threats). Среди примеров угроз:

- Уязвимости конфигурации сервера (переполнение буферов, некорректные настройки)
- Атаки типа «Отказ в обслуживании» (DoS/DDoS)
- Инъекции SQL-кода
- Фишинговые атаки
- Нарушение целостности данных
- Утечка конфиденциальной информации [3,4].

**Шаг 3: Моделирование сценариев атаки**

Цель: Создать реалистичные модели атак, направленных против системы. (Приём системного анализа: Имитация («What if»-модели)).

Применяется техника построения моделей гипотетических атак («Что произойдет, если…?»). Для каждого вида угроз создаётся сценарий возможного инцидента:

- Если злоумышленники получат доступ к базам данных?
- Что произойдёт при успешной инъекции вредоносного скрипта?
- Какова реакция системы на массированную DDoS-атаку?

**Шаг 4: Ранжирование угроз по степени опасности**

Цель: Установить приоритет угроз для дальнейшей обработки. (Приём системного анализа: Методология оценки рисков (матрица вероятностей и последствий)).

Каждую угрозу оцениваем по двум параметрам:

- Вероятность реализации угрозы (низкая/средняя/высокая)
- Последствия реализации угрозы (невысокие/умеренные/катастрофические)

Строится матрица рисков, позволяющая определить приоритеты для устранения угроз.

**Шаг 5: Формирование стратегии реагирования**

Цель: Предложить конкретные методы и механизмы противодействия угрозам. (Приём системного анализа: Морфологический синтез.)

Исходя из ранжированных угроз, выбираются соответствующие защитные мероприятия:

- Использование технологий шифрования данных
- Настройка двухфакторной аутентификации
- Регулярное обновление патчей и исправлений
- Мониторинг аномалий поведения сети
- Создание резервных копий и восстановление данных

Таблица 1 – Итоговая таблица угроз и мероприятий

| № | Угроза | Уровень риска | Рекомендуемые контрмеры |
|---|---|---|---|
| 1 | Перехват сетевого трафика | Средний | TLS-шифрование |
| 2 | Атакующие SQL-инъекции | Высокий | Проверка вводимых данных |
| 3 | Утрата данных вследствие сбоев | Высший | Резервное копирование |
| 4 | Незаконный доступ сотрудников | Средний | Контроль прав доступа |

Рассмотрим пример, раскрывающий первый шаг алгоритма, применимо к программному средству, реализующему доступ к системе управления технологическим процессом с мобильного устройства.

Первый шаг: Сбор и классификация информации о компонентах системы

Цель первого шага заключается в определении всех элементов системы, которые подлежат защите, и классификации их по уровню значимости и критичности. Этот шаг необходим для последующего фокусирования внимания на важнейших аспектах безопасности и правильного распределения ресурсов.

Для успешного выполнения данного шага используются приемы системного анализа, среди которых ключевой является декомпозиция, то есть разделение сложной системы на отдельные подсистемы и компоненты, позволяющие ясно увидеть структуру и взаимосвязи.

Этап 1: Детализация структуры системы

Мы рассматриваем систему управления технологическим процессом (СУТП), доступной через мобильное приложение. Она состоит из следующих основных компонент:

1. Сервер СУТП

Обеспечивает управление оборудованием и мониторинг технологических процессов.

Содержит базу данных с важными производственными показателями и конфигурациями оборудования.

2. Мобильное приложение

– Предоставляет интерфейс для оператора (или инженера), позволяющий управлять системой и получать уведомления о состоянии производства.

– Передаёт команды серверу и получает обратно информацию о статусе оборудования.

3. Каналы связи

– Интернет-канал между мобильным устройством и сервером СУТП.

– Локальная сеть предприятия, связанная с серверами и промышленным оборудованием.

4. Пользовательские аккаунты

– Учётные записи операторов и инженеров, обладающие различными правами доступа.

5. Аппаратное оборудование

– Серверы СУТП, промышленные контроллеры, датчики и исполнительные механизмы, взаимодействующие с системой.

Этап 2: Классификация элементов системы по значимости

Следующим этапом является присвоение каждому элементу определённого уровня значимости исходя из его роли в обеспечении безопасности технологического процесса. Примем для рассмотрения три уровня классификации значимости:

Высокий – элементы, нарушение безопасности в которых влечет серьезный ущерб (потеря производительности, угроза персоналу, финансовые убытки);

Средний – элементы, нарушение безопасности в которых влечет к ущербу, но не оказывает существенного влияния на производство;

Низкий – элементы, нарушение безопасности в которых несущественно и последствия легко восстановимы.

Таблица 2 – Уровни значимости

| **Компоненты** | **Значимость** |
|---|---|
| База данных производственного состояния | Высокая |
| Пользовательские учётные записи | Средняя |
| Протокол передачи данных (интернет-каналы) | Высокая |
| Интерфейс мобильного приложения | Средняя |
| Аппаратное оборудование (серверы) | Высокая |
| Внешнее ПО на мобильном устройстве | Низкая |

**Заключение**

Таким образом, применив приёмы системного анализа (декомпозиция, SWOT-анализ, имитация, оценка рисков и морфологический синтез), мы можем

эффективно проанализировать угрозы и предложить комплекс эффективных защитных мер для минимизации рисков в рамках разрабатываемого программного обеспечения.

По завершении первого шага мы получаем чёткое представление о структуре системы и уровнях значимости отдельных её частей. Эти знания позволят нам сосредоточить внимание на наиболее важных компонентах, подвергнуть их тщательному анализу угроз и принять эффективные меры по обеспечению информационной безопасности.

## Список литературы

1. Рябев, В. И. Системный анализ информационной модели голографической визуализации данных / В. И. Рябев, С. Л. Сахаров, А. Ю. Павлов // Моделирование систем и процессов. – 2025. – Т. 18, № 1. – С. 78-84. – DOI 10.12737/2219-0767-2025-78-84. – EDN GBXSOC.

2. Огнева, К. Н. Перспективы внедрения технологий искусственного интеллекта в системы обеспечения информационной безопасности / К. Н. Огнева, А. С. Кравченко // Молодежь и XXI век - 2024 : Сборник научных статей 13-й Международной молодежной научной конференции. В 3-х томах, Курск, 15–16 февраля 2024 года. – Курск: ЗАО "Университетская книга", 2024. – С. 413-415. – EDN TQDQUK.

3. Анализ методик автоматизированной оценки угроз и рисков информационной безопасности информационно-телекоммуникационных систем / Ю. В. Скоредова, Е. В. Гречишников, А. С. Кравченко, О. В. Ланкин // Вестник Воронежского института ФСИН России. – 2017. – № 3. – С. 128-133. – EDN YRBEBE.

4. Безопасная разработка и уязвимости программного кода. – URL: https://habr.com/ru/company/otus/blog/658319.

## References

1. Ryabev, V. I. Sistemnii analiz informatsionnoi modeli golograficheskoi vizualizatsii dannikh / V. I. Ryabev, S. L. Sakharov, A. Yu. Pavlov // Modelirovanie sistem i protsessov. – 2025. – T. 18, № 1. – S. 78-84. – DOI 10.12737/2219-0767-2025-78-84. – EDN GBXSOC.

2. Ogneva, K. N. Perspektivi vnedreniya tekhnologii iskusstvennogo intellekta v sistemi obespecheniya informatsionnoi bezopasnosti / K. N. Ogneva, A. S.

Kravchenko // Molodezh i XXI vek - 2024 : Sbornik nauchnikh statei 13-i Mezhdunarodnoi molodezhnoi nauchnoi konferentsii. V 3-kh tomakh, Kursk, 15–16 fevralya 2024 goda. – Kursk: ZAO "Universitetskaya kniga", 2024. – S. 413-415. – EDN TQDQUK.

3. Analiz metodik avtomatizirovannoi otsenki ugroz i riskov informatsionnoi bezopasnosti informatsionno-telekommunikatsionnikh sistem / Yu. V. Skoredova, Ye. V. Grechishnikov, A. S. Kravchenko, O. V. Lankin // Vestnik Voronezhskogo instituta FSIN Rossii. – 2017. – № 3. – S. 128-133. – EDN YRBEBE.

4. Bezopasnaya razrabotka i uyazvimosti programmnogo koda. – URL: https://habr.com/ru/company/otus/blog/658319.