Отчёт о выполенном проекте  
«Конвергенция постквантовой криптографии в сети IP на базе АТС Асткриск»

Подготовил студент второго курса, Чичасов Денис, группа SIS-2209

1. Информационная Безопасность

**Информационная безопасность (ИБ)** — это практика защиты информации от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения. Она включает в себя защиту как физических, так и цифровых данных.

**Регулярное обновление программного обеспечения:** Большинство уязвимостей и эксплойтов находятся в устаревших версиях ПО. Регулярные обновления устраняют известные уязвимости и повышают общую безопасность системы.

**Математическое обоснование:** Предположим, что вероятность успешной атаки на систему, не обновляемую на протяжении года, составляет \( P\_{old} \). После обновления эта вероятность снижается до \( P\_{new} \), где \( P\_{new} < P\_{old} \). В долгосрочной перспективе это приводит к уменьшению общего риска: — вероятность атаки, а \( C\_i \) — затраты на устранение последствий.

**Обучение сотрудников:** Наиболее частыми причинами успешных атак являются фишинговые письма и другие методы социальной инженерии. Регулярное обучение сотрудников основам информационной безопасности, таким как обнаружение подозрительных писем, проверка источников и другие важные навыки, помогает снизить риск человеческой ошибки.

**Сегментация сети:** Подразумевает разделение сети на отдельные сегменты, ограничивая доступ к критически важным ресурсам. Это помогает ограничить распространение вредоносного ПО и делает возможным локализацию атак.

**Математическое обоснование:**

Рассмотрим сеть как граф, где вершины — это узлы, а ребра — соединения между ними. Сегментация сети приводит к тому, что граф становится разреженным, уменьшая количество возможных путей для атаки. Вероятность атаки можно представить как функцию от количества возможных путей в графе: где — количество ребер в графе.

2. Кибербезопасность

**Кибербезопасность** — это практика защиты компьютерных систем и сетей от информационных угроз, таких как кибератаки, кражи данных, вредоносное ПО и другие виды киберугроз.

**Реагирование на инциденты**: Быстрое и эффективное реагирование на инциденты помогает минимизировать ущерб от атак. Это включает в себя идентификацию угрозы, изоляцию пораженных систем, ликвидацию уязвимости и восстановление после атаки.

**Математическое обоснование**: Время реагирования напрямую связано с ущербом который можно выразить через функцию ), где — возрастающая функция. Минимизация \( T\_r \) приводит к снижению ущерба.

**Тестирование на проникновение:** **Пентесты** — это процесс симулирования атак на систему для выявления её слабых мест. Регулярное проведение пентестов позволяет своевременно выявлять и устранять уязвимости до того, как ими воспользуются злоумышленники.

**Математическое обоснование:** Вероятность успешного проникновения уменьшается после каждого пентеста, так как обнаруженные уязвимости устраняются. Это можно выразить как \( где — процент устраненных уязвимостей, а \( n \) — количество проведенных пентестов.

**Обеспечение резервного копирования:** Надежные бэкапы позволяют быстро восстановиться после атак типа ransomware. Это критично для поддержания непрерывности бизнеса и минимизации простоев.

**Математическое обоснование**: Восстановление данных с резервных копий можно описать как процесс минимизации времени простоя Если вероятность успешного восстановления данных высока, то вероятность длительного простоя низка, и

3. Криптография

**Криптография** — это наука о методах обеспечения конфиденциальности, целостности и аутентификации данных посредством шифрования. Она включает в себя шифрование, дешифрование, управление ключами и создание цифровых подписей.

Использование проверенных алгоритмов: Применение криптографических алгоритмов, таких как AES, RSA или ECC, которые были тщательно проверены и имеют открытые спецификации, минимизирует риски, связанные с уязвимостями в алгоритмах.

**Математическое обоснование**: Надежность алгоритма можно выразить через его устойчивость к атакам, которую можно описать как где \( k \) — длина ключа. Например, для AES-256 устойчивость составляет

**Управление ключами:** Безопасное хранение и управление ключами — основа надёжности всей системы. Это включает в себя процессы генерации, распределения, хранения и уничтожения ключей.

**Математическое обоснование:** Устойчивость системы определяется как \( — устойчивость алгоритма, а \( S\_{key} \) — безопасность управления ключами.

**Минимизация площади атаки:** Шифруйте только те данные, которые действительно нуждаются в защите, для минимизации рисков. Излишнее шифрование может создавать дополнительные точки атаки.

**Математическое обоснование:** Вероятность атаки \( P\_{attack} \) пропорциональна количеству данных, подвергающихся шифрованию. Уменьшениеснижает

4. Постквантовая Криптография

**Постквантовая криптография** — это область криптографии, которая разрабатывает алгоритмы, устойчивые к взлому с использованием квантовых компьютеров. Квантовые компьютеры, как предполагается, смогут взламывать многие из существующих криптографических систем, таких как RSA и ECC.

**Анализ уязвимостей:** Квантовые компьютеры используют алгоритмы, такие как алгоритм Шора, который может эффективно решать задачи факторизации и дискретного логарифма, угрожая существующим криптографическим системам. Постквантовые алгоритмы, такие как NTRU и McEliece, основаны на задачах, которые считаются устойчивыми к атакам квантовых компьютеров.

**Математическое обоснование:** Время взлома квантовым компьютером для традиционного алгоритма можно выразить как ), — сложность задачи. Постквантовые алгоритмы строятся на задачах, для которых нет известных квантовых алгоритмов с такой низкой сложностью.

**Гибридные системы:** В переходный период возможен переход на гибридные системы, использующие и классическую, и постквантовую криптографию, что позволяет постепенно интегрировать новые методы без полного отказа от существующих решений.

**Математическое обоснование:** В гибридных системах общая устойчивость ) может быть выражена как Это гарантирует, что система будет устойчива, пока оба алгоритма безопасны.

5. TLS-протокол

**Transport Layer Security (TLS**) — это криптографический протокол, обеспечивающий безопасность передачи данных в интернете. Он используется для шифрования данных, аутентификации серверов и, в некоторых случаях, клиентов.

**Обновление версий TLS:** Используйте современные версии TLS (TLS 1.2 и выше), так как старые версии уязвимы к различным атакам, таким как BEAST и CRIME.

**Математическое обоснование:** Уязвимости старых версий протоколов могут быть выражены через вероятность успеха атаки Для TLS 1.0 и 1.1 выше, чем для TLS 1.2, благодаря улучшениям в механизмах шифрования и управлении ключами.

**Совместимость с HSTS:** Использование HTTP Strict Transport Security (HSTS) помогает предотвращать атаки типа "man-in-the-middle" путем обязательного использования HTTPS и предотвращения отправки данных по незащищенным каналам.

**Математическое обоснование:** HSTS снижает вероятность успешной атаки \( P\_{attack} \) на транспортный уровень, так как она принудительно переводит все соединения на HTTPS, где используется TLS.

6. SSL-протокол

**Secure Sockets Layer (SSL)** — предшественник TLS, используемый для обеспечения безопасной передачи данных по сети. SSL протоколы устарели и больше не считаются безопасными.

**Отказ от использования SSL:** Современные системы должны отказаться от использования SSL протоколов (особенно SSL 2.0 и SSL 3.0) в пользу TLS, так как SSL протоколы содержат известные уязвимости.

**Математическое обоснование:** SSL протоколы были уязвимы к атакам, таким как POODLE и DROWN, что выражается в высокой вероятности успешного взлома для этих версий. Переключение на TLS существенно снижает

7. Теория Решеток

**Теория решеток (lattice theory)** — это область математики, изучающая дискретные решетки в n-мерном пространстве. В криптографии, задачи на решетках используются для создания алгоритмов, устойчивых к квантовым атакам.

**Применение в криптографии:** Задачи, такие как Learning With Errors (LWE) и Shortest Vector Problem (SVP), являются основой для создания постквантовых криптографических алгоритмов.

**Математическое обоснование:** Для задач на решетках сложность задач масштабируется экспоненциально с увеличением размерности решетки Например, для SVP сложность решения — константа, связанная с конкретным алгоритмом решения.

**Проблема нахождения короткого вектора:** Один из фундаментальных вопросов теории решеток — нахождение самого короткого вектора в решетке. Для этого используются алгоритмы, такие как LLL (Lenstra-Lenstra-Lovász), которые позволяют найти приближенные решения.

**Математическое обоснование:** Для решетки размерности сложность нахождения точного короткого вектора экспоненциальна: зависит от выбранного метода.

8. Программа для VoIP, Asterisk

**Asterisk** — это программное обеспечение с открытым исходным кодом для организации VoIP-телефонии. Оно позволяет создавать, управлять и контролировать VoIP-системы, а также поддерживает широкий спектр протоколов связи.

**Безопасность SIP:** Использование протокола SIP (Session Initiation Protocol) в Asterisk требует внедрения мер безопасности, таких как использование TLS для шифрования сигнализации и SRTP для шифрования медиа-потоков.

**Математическое обоснование:** Без использования шифрования атаки на VoIP могут быть успешными с вероятностью , которая возрастает с увеличением доступности незащищенных данных. Шифрование через TLS и SRTP снижает эту вероятность до где

**Натройка брандмауэра и защита от DoS-атак:** Asterisk-сервера должны быть защищены от DoS-атак и нежелательного трафика через настройку брандмауэра, ограничение количества соединений и использование механизмов выявления подозрительной активности.

**Математическое обоснование:** Вероятность успешной DoS-атаки \( P\_{DoS} \) снижается пропорционально эффективности настроек безопасности и брандмауэра. Если система способна блокировать подозрительные попытки соединения, то, где — эффективность брандмауэра.

9. Реализация TLS-протокола на языке программирования Python

Реализация TLS протокола на Python подразумевает создание или использование библиотек для обеспечения безопасной передачи данных с использованием криптографических методов.

**Использование библиотеки `ssl`:** Python предоставляет модуль `ssl`, который позволяет использовать TLS протокол для создания защищенных соединений. Эта библиотека поддерживает как клиентские, так и серверные реализации.

**Математическое обоснование:** С помощью библиотеки `ssl` можно создавать защищенные соединения, где безопасность передачи данных \( S\_{data} \) определяется как функция от используемого алгоритма шифрования и длины ключа:

**Конфигурация параметров безопасности:** Важно правильно настраивать параметры безопасности, такие как версии протоколов, шифры и управление сертификатами. Это помогает избежать использования устаревших или небезопасных конфигураций.

**Математическое обоснование:** Устойчивость соединения \( определяется выбранными шифрами и параметрами: \( где \( — безопасность выбранного алгоритма шифрования, а \( — устойчивость схемы управления ключами.

10. Определение виртуальной машины и реализация TLS-протокола

**Виртуальная машина (VM)** — это программная имитация компьютерной системы, обеспечивающая исполнение программ как на физической машине. Виртуализация позволяет запускать несколько операционных систем на одном физическом устройстве.

Изоляция виртуальных машин: Одним из ключевых аспектов безопасности в виртуальных средах является изоляция виртуальных машин друг от друга. Это предотвращает возможность атаки или доступа одной VM к данным другой VM.

**Математическое обоснование**: Изоляция достигается за счет гипервизора, который управляет распределением ресурсов и контролем доступа. Вероятность успешной атаки на изолированную VM уменьшается с увеличением эффективности гипервизора , что можно выразить как

**Реализация TLS на виртуальной машине:** TLS можно реализовать на виртуальной машине для обеспечения защищенной передачи данных между VM и внешними системами. Это требует настройки виртуальных сетевых интерфейсов и использования шифрования для всех передаваемых данных.

Математическое обоснование: Безопасность данных ), передаваемых через виртуальную сеть, зависит от TLS конфигурации и сетевой архитектуры: