Студент: Ихкайма Гайдаа Группа: 241-352

Место прохождения практики: Московский Политех, кафедра

Информационная безопасность

Отчет принят с оценкой \_\_\_ Дата \_\_\_\_\_\_\_\_

Руководитель практики: Кесель Сергей Александрович

# Изучение потенциальных угроз безопасности для корпоративной сети

Современные корпоративные сети сталкиваются с рядом угроз, которые могут повлиять на их устойчивость и безопасность. К основным угрозам относятся:

- DDoS-атаки — направлены на перегрузку серверов и отказ в обслуживании.

- Фишинг — обманный способ получения конфиденциальной информации через поддельные письма или сайты.

- Компрометация учетных записей — получение злоумышленником доступа к корпоративным аккаунтам с целью кражи данных или дальнейших атак.

# Описание процессов разработки и внедрения политики мониторинга событий безопасности

Политика мониторинга событий безопасности разрабатывается для выявления и отслеживания подозрительной активности. Основные этапы:

1. Определение критичных для мониторинга систем и данных.

2. Настройка систем сбора и анализа логов (например, SIEM-систем).

3. Установка порогов и сигнатур для определения аномалий.

4. Обучение персонала работе с системой мониторинга.

5. Постоянное обновление правил мониторинга на основе новых угроз.

# Проектирование процесса реагирования на инциденты

Процесс реагирования должен включать следующие этапы:

1. Классификация инцидентов — по уровню критичности (низкий, средний, высокий).

2. Оповещение ответственных лиц — через автоматические уведомления и внутренние регламенты.

3. Анализ воздействия — оценка ущерба и возможных последствий для бизнеса.

4. Восстановление — возврат систем к рабочему состоянию, устранение уязвимостей.

# Разработка схемы документооборота для инцидентов безопасности

Для обеспечения прозрачности и эффективности реагирования необходимо внедрить следующую схему документооборота:

- Регистрация инцидента в журнале безопасности.

- Уведомление пользователя о произошедшем и возможных последствиях.

- Подготовка технического отчета по инциденту.

- Документирование действий по восстановлению.

- Отчет о восстановлении доступа и принятии мер по предотвращению повтора.

Вывод

В условиях стремительного развития технологий и увеличения количества киберугроз обеспечение информационной безопасности корпоративных сетей приобретает первостепенное значение. Анализ потенциальных угроз, таких как DDoS-атаки, фишинг и компрометация учетных записей, позволяет своевременно выявлять риски и минимизировать ущерб. Эффективная политика мониторинга, грамотно организованный процесс реагирования на инциденты и налаженный документооборот — это ключевые элементы, обеспечивающие защиту информационных ресурсов организации. Комплексный подход к безопасности позволяет повысить устойчивость корпоративной инфраструктуры и защитить интересы как компании, так и её пользователей.