### Защита информации от утечки по технический каналам

Выполнил студент группы: ПР-20-1 Мошко А.В

Проверил преподаватель:

Сошенко Е.Н

#### Содержание

- 1. Введение
- 2. Определение понятия «Технические каналы»
- 3. Анализ угроз
- 4. Основные методы утечки информации
- 5. Классификация информации и оценка её степени конфиденциальности
- 6. Контроль доступс
- 7. Шифрование данных
- 8. Обновление ПО и применение патчей
- 9. Обучение сотрудников
- 10. Аудит информационной безопасности
- 11. Установка брандмауэров и антивирусного программного обеспечения
- 12. Мониторинг и обнаружение
- Заключение

#### 1. Введение

- Утечка информации стала одной из наиболее серьёзных угроз для компаний и организаций в информационном цифромов мире.
- - В настоящее время технические каналы являются одним из основных способов утечки информации (например, через сеть, устройства хранения данных и коммуникационные средства).

## 2. Определение понятия «Технические каналы»

 Технические каналы – это средства передачи информации, которые используются в современных технических системах, таких как компьютеры, сети, мобильные устройства и т.д.

### 3. Анализ угроз

• Первым шагом в защите информации от утечки по техническим каналам является анализ угроз. Необходимо идентифицировать потенциальные уязвимости и слабые места в системе передачи информации. Это включает в себя оценку рисков и возможных каналов утечки, а также определение основных угроз, таких как прослушивание, перехват и восстановление

# 4. Основные методы утечки информации

- Подслушивание и перехват данных по сети или при передаче.
- Взлом системы и доступ к защищенным данным.
- Уязвимости программного обеспечения и операционной системы.
- - Кража устройств хранения данных.

- 5. Классификация информации и оценка её степени конфиденциальности
- Важно классифицировать информацию по степени конфиденциальности (например, общедоступная, коммерческая, конфиденциальная, секретная) и провести анализ её уязвимостей.

#### 6. Контроль доступа

 Один из наиболее эффективных способов защиты от утечки информации по техническим каналам – это установка контроля доступа. Это включает в себя управление правами доступа к системе, физическую безопасность помещений и контроль доступа к серверам и сетям. Также важно регулярно обновлять пароли и ограничивать доступ к информации определённым группам пользователей.

#### 7. Шифрование данных

 Для защиты информации от утечки необходимо применять современные методы шифрования данных. Это позволяет обезопасить информацию от несанкционированного доступа и предотвратить возможность расшифровки данных в случае их перехвата.

# 8. Обновление ПО и применение патчей

 Регулярное обновление и применение патчей помогает закрыть уязвимости и предотвратить потенциальные утечки информации.

### 9. Обучение сотрудников

 Организация обучающих программ по безопасности информации для всех сотрудников, чтобы иметь хорошее понимание угроз и методов их предотвращения.

## 10. Аудит информационной безопасности

 Регулярное проведение аудита информации безопасности позволяет выявить и устранить уязвимости и слабые места в системе

## 11. Установка брандмауэров и антивирусного ПО

 Установка и настройка брандмауэров и антивирусного программного обеспечения помогает обнаружить и блокировать попытки несанкционированного доступа или передачи информации

# 12. Мониторинг и обнаружение

• Осуществление постоянного мониторинга и обнаружения аномалий в системе передачи информации может рано обнаружить попытки утечки. Использование специализированных программного и аппаратного обеспечения позволяет обнаруживать необычную активность и принимать меры по её пресечению.

#### Заключение

- Утечка информации через технические каналы является серьёзной угрозой для организации.
- Применение мер по защите информации от утечки по техническим каналам является важной задачей, которая требует комплексного подхода и регулярного обновления.