Уязвимость нулевого дня

Основы информационной безопасности

Улитина М.М.

16 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Улитина Мария Максимовна
- студентка
- Российский университет дружбы народов

Вводная часть

Цель работы

Целью данного доклада является изучение информации об уязвимости нулевого дня, рисках данной уязвимости и способах её предотвращения.

Введение

Специалисты сферы информационной безопасности ежедневно сталкиваются с различными типами уязвимостей и угроз. Одной из основных задач в данной области является обнаружение потенциальных угроз безопасности и стабильности быстрее злоумышленников для предотвращения утечек данных и других негативных последствий.

Основная часть

Основные понятия

- Уязвимость нулевого дня
- Эксплойт нулевого дня

Обнаружение уязвимости нулевого дня

1. Использование существующих баз вредоносных программ. Уже описанные поведения и паттерны могут послужить справочным материалом для обнаружения уязвимостей.
2. Поиск признаков взаимодействия вредоносных программ и возможностей их работы.
3. Применение ИИ и машинного обучения.

Опасность уязвимостей нулевого дня

Атакам нулевого дня подвержены следующие объекты:

1. Операционные системы
2. Браузеры
3. Приложения
4. Интернет вещей
5. Аппаратное обеспечение и прошивка

Защита от атак нулевого дня

1. Обновление программ и операционных систем.
2. Использование только необходимого ПО.
3. Использование сетевого экрана.
4. Обучение персонала.
5. Использование комплексного антивирусного ПО.

Выводы

Выводы

В данном докладе я рассмотрела основные аспекты уязвимостей нулевого дня, а также способы их предотвращения.