Программная инженерия

Москва
2026

Лекция № 3. Инциденты

Основы кибербезопасности

Белявский Д.А.

Результаты контрольной работы

Событие → Инцидент

Событие –
факт, любое изменение
или действие

«Подозрительное»
событие

Инцидент

Сохраняем
в журналы (логи)

Инцидент ИБ – событие и/или серия событий, которые привели, приводят или могут привести с высокой долей вероятности к реализации угроз информационной безопасности (или нарушению процессов в организации)

Пример

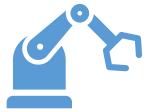
Сотрудник успешно аутентифицируется в будний день 09:00 со своего рабочего места	Событие
Сотрудник успешно аутентифицируется в будний день в 14:00 со своего рабочего места	Событие
Сотрудник неудачно аутентифицируется в субботу в 03:00 удаленно. 5 раз подряд	Подозрительное событие
Сотрудник успешно аутентифицируется в воскресенье в 19:00 удаленно с 3-й попытки (предыдущие попытки неуспешны)	Инцидент

Источники инцидентов

Пользователи/
сотрудники

Журналы
ОС и приложений

Системы сбора и
корреляции событий



Автоматизированные
проверки

Внешние и внутренние
аудиты

Внешние контрагенты
(СМИ, госорганы и пр.)

И много кто еще...

Жизненный цикл инцидента

Классификация инцидентов

По приоритету (критичности)

По ценности актива*

	Критичные активы	Актив средней критичности	Некритичный актив
Глобальный инцидент (влияет на всю организацию)	Высокая	Высокая	Высокая
Инцидент среднего масштаба (влияние на одну систему)	Высокая	Средняя	Низкая
Локальный инцидент (один сервис)	Средняя	Низкая	Незначительная

Актив с точки зрения информации

Актив - любая информация, независимо от вида её представления, имеющая ценность для организации и находящаяся в её распоряжении.

- Персональные данные
- Банковская тайна
- Коммерческая тайна
  - Стратегическая информация
  - Ноу-хау
  - Другая интеллектуальная собственность
- Профессиональная тайна
  - Адвокатская
  - Врачебная
  - Нотариальная
- Тайна связи
- Служебная тайна
- Личная и семейная тайна
- Налоговая тайна
- Гостайна

И другие виды тайн...

Активы в ИТ (и в кибербезопасности)

Стандарт
ГОСТ Р ИСО/МЭК 19770-1-2021

Классификации недостаточно, нужно подробнее

MITRE | ATT&CK®

attack.mitre.org

mitre.ptsecurity.com
(перевод на русский)

Что будет на семинаре № 3?

- Обсуждение по прошедшим темам лекций
- Обсуждение результатов контрольной работы
- Тест №2