Программная инженерия

Москва
2026

Лекция № 4. Инциденты

Основы кибербезопасности

Белявский Д.А.

Уведомление об инцидентах

Определяется метод уведомлений

Определяется порядок эскалации

Критичность	Высокая	Средняя	Низкая	Незначительная
Уведомляемые лица в организации	Руководство организации + Владелец ИС/актива	Руководство организации + Владелец ИС/актива	Владелец ИС/актива (при необходимости расследования)	Владелец ИС/актива (при необходимости расследования)
Время на оповещение	15 минут	15 минут	30 минут	В течение рабочего дня
Метод оповещения	Электронная почта + SMS + звонок	Электронная почта + SMS	Электронная почта + телеграм	Электронная почта

Оценка последствий инцидентов

Отчет с подробным описанием ситуации и событий, которые привели к инциденту

Анализ экономических и других видов **потерь** от данного инцидента

Анализ рисков, которые появились при инциденте, или, которые были упущены при раннем анализе

Определяем (составляем) план по устранению уязвимостей и недостатков в ИС, которые были обнаружены (**корректирующие действия**)

Управление инцидентами

Управление инцидентами – регулярный процесс, направленный на сокращение влияния инцидентов на информационную безопасность

Эффективность кибербезопасности

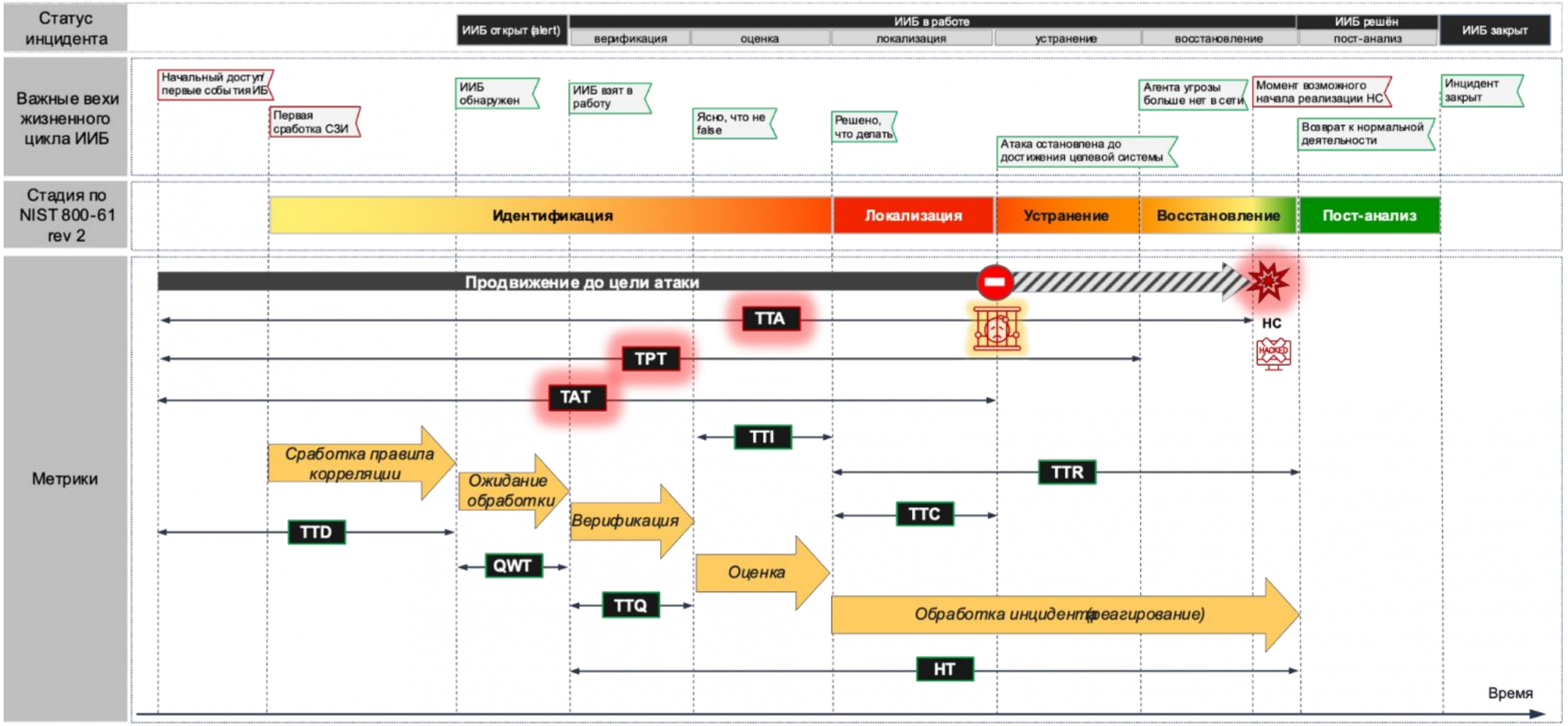
Вводятся метрики для измерения эффективности кибербезопасности с точки зрения управления инцидентами

TTD (time-to-detect)	TTR (time-to-respond)
Время обнаружения инцидента	Время реагирования на инцидент

Основное правило кибербезопасности:

БЫСТРО обнаруживаем и БЫСТРО реагируем!

Различные метрики в кибербезопасности




Журналы (логи)

Linux: журналы ОС

Общие журналы ОС

- `/var/log/syslog`
- `/var/log/messages`

Журналы аутентификации

- `/var/log/auth.log`
- `/var/log/secure`

Журналы ядра ОС

- `/var/log/kern.log`

Журналы загрузки ОС

- `/var/log/dmesg`

Команда просмотра журналов

- `journalctl`

```
journalctl -xe
journalctl -u apache
journalctl --since "1 hour ago"
```

Linux: журналы прикладного ПО

Журналы веб-сервера
- `/var/log/apache2/`
- `/var/log/nginx/`

Журналы СУБД
- `/var/log/mysql/`
- `/var/log/postgresql/`

Журналы почтового сервера
- `/var/log/mail.log`
- `/var/log/mail.err`

При анализе инцидентов в Linux обращают внимание на:
- **нетипичное время активности**
- **неизвестные IP-адреса** в auth.log, прикладных журналах
- **ошибки сегментации** в системных журналах (попытку эксплуатации уязвимостей)
- **новые события**, которых ранее на наблюдалось

Windows: журналы ОС

Общие журналы ОС

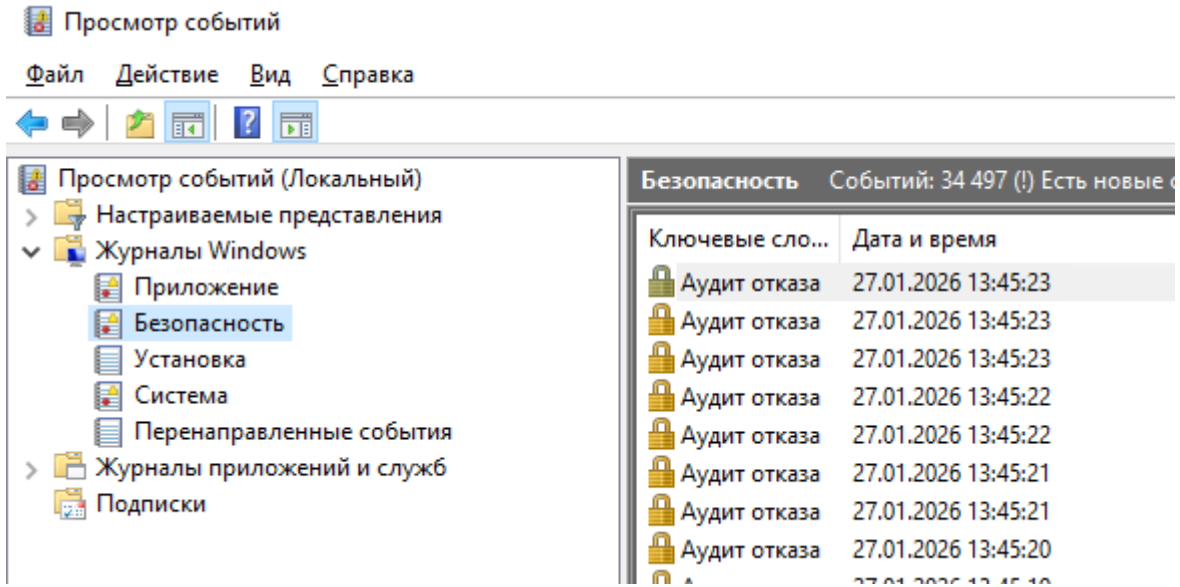
- Система
- Установка

Журналы безопасности

- Безопасность

Журналы прикладного ПО

- Приложение
- Собственные места хранения журналов



Windows: событий и утилиты

Событие	Значение	Что искать
4624	Успешный вход	Кто и когда зашел на сервер.
4625	Ошибка входа	Попытки подбора пароля (Brute-force).
4648	Вход с явными учетными данными	Попытки использовать «запустить как администратор» (подозрительно для админов).
4720	Создание пользователя	Несанкционированное создание новой «учетки».
1102	Журнал аудита очищен	Кто-то пытается замести следы (очень критично).

Sysinternals

https://learn.microsoft.com/en-us/sysinternals/

Автоматизированные средства сбора событий

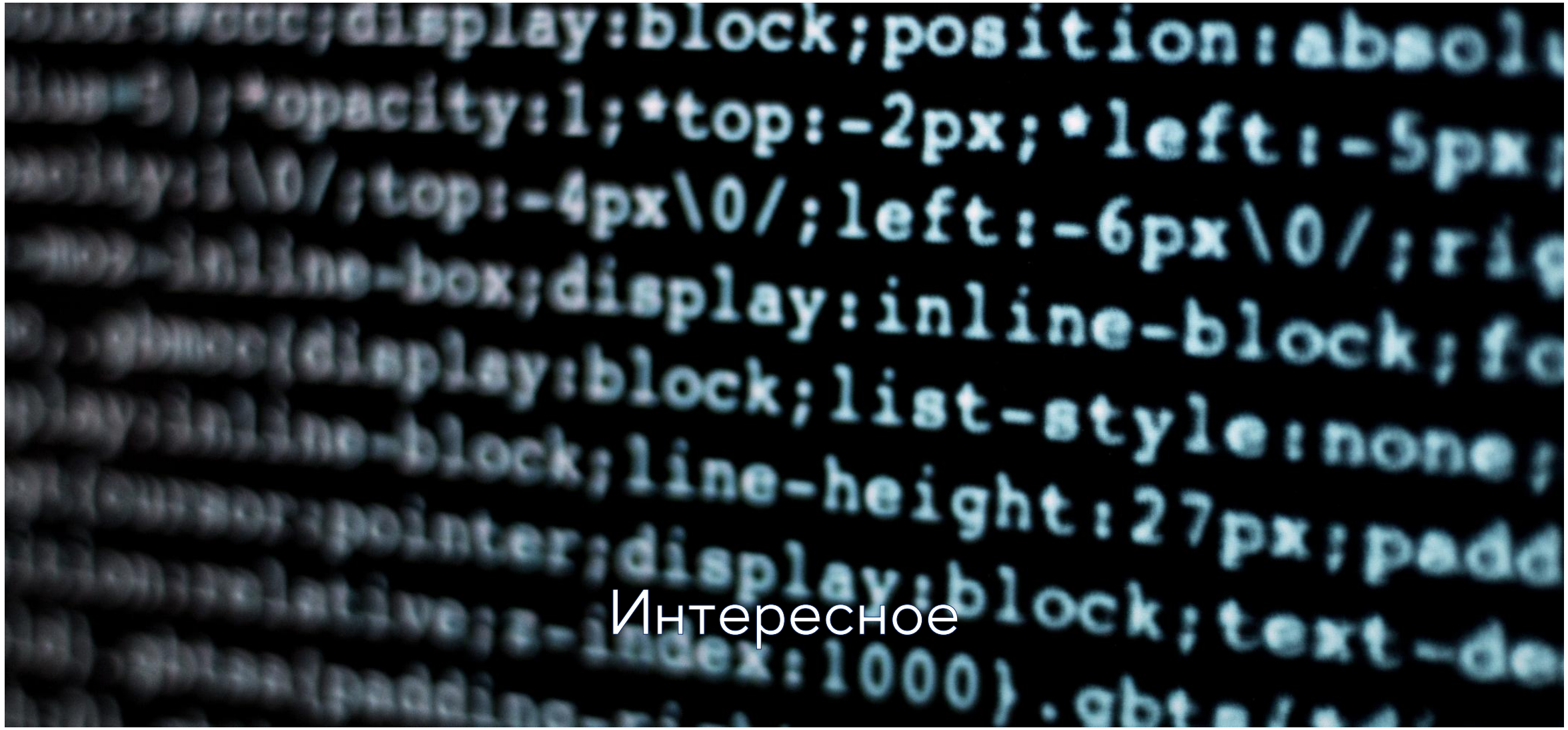
SIEM – Система сбора событий и выявления инцидентов информационной безопасности

wazuh.

Бесплатная с открытым исходным кодом.
Хорошо для обучения!

Kaspersky
Unified Monitoring
and Analysis Platform

MaxPatrol SIEM


display:block;position:
opacity:1;*top:-2px;*left:-5px
top:-4px\0/;left:-6px\0/;
inline-box;display:inline-block;
display:block;list-style:none;
inline-block;line-height:27px;
pointer;display:block;
index:1000)

Интересное

Bug bounty

STANDOFF 365

bugbounty.standoff365.com

BI.ZONE

bugbounty.bi.zone

Bug bounty

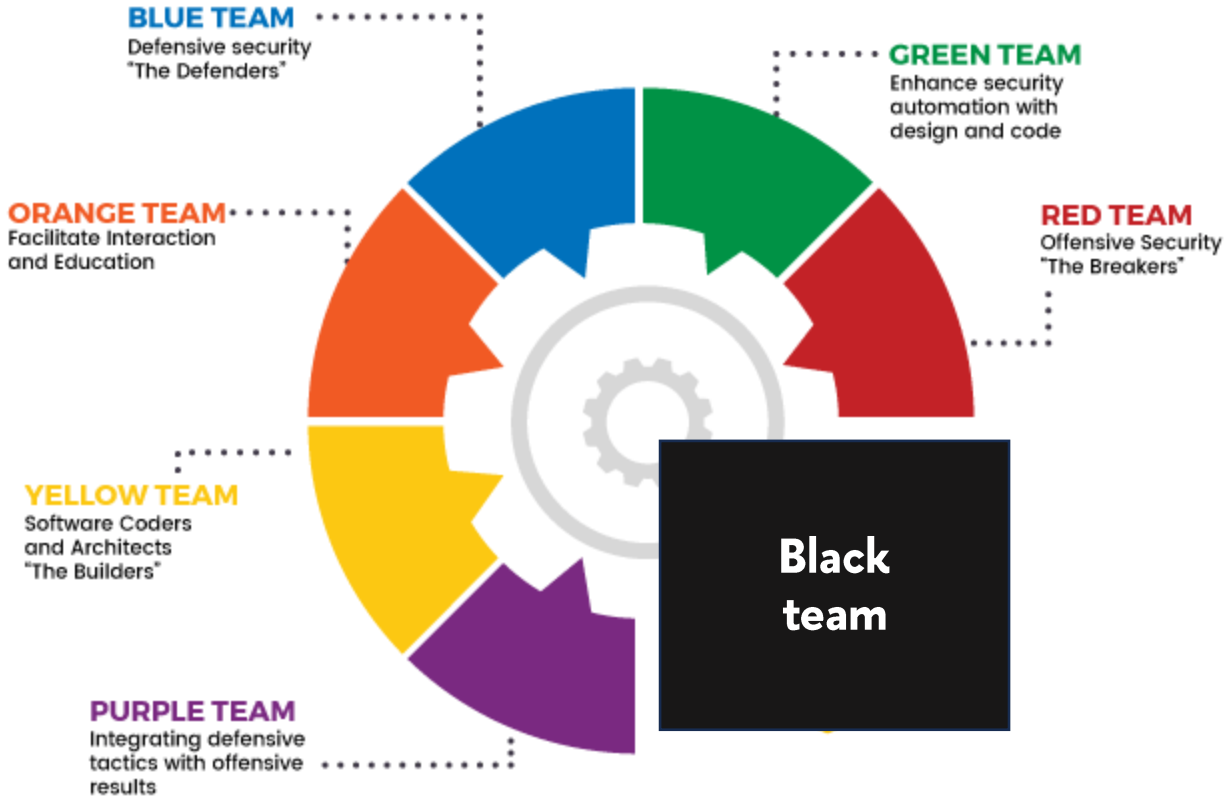
hackerone

hackerone.com/directory/programs

Методы поиска уязвимостей и предотвращения инцидентов

Penetration testing (PenTest)
Тестирование на проникновение

APT (Advanced Persistent Threat)



Что будет на семинаре № 4?

- Обсуждение по прошедшим темам лекций
- Обсуждение результатов тестов
- Контрольная работа по инцидентам


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •