

# Лабораторная работа №6

**Тема:** Обнаружение и предотвращение вторжений в компьютерные системы. Системы защиты от вредоносного ПО и журналирования. IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems) (Windows, Linux и т. д.)

**Обнаружение и предотвращение вторжений в компьютерные системы (из курса)**

8.1. Общая характеристика систем обнаружения вторжений (IDS).

Классификация систем IDS.

8.2. Типичные механизмы обнаружения вторжений. Распространенные типы систем IDS.








8.3. Характеристики решений IDS, важные для практического применения. Смешанные системы

## Цель работы:

1. Изучение характеристик и принципа работы систем обнаружения и предотвращения вторжений. Анализ их рабочих параметров (IDS/IPS).
2. Сравнительная характеристика (в соответствии с изложенными ниже принципами) систем обнаружения или предотвращения вторжений IDS/IPS (некоторые из предлагаемого списка или другие, не вошедшие в список).
3. Изучение функциональности некоторых систем обнаружения/предотвращения вторжений (2-3 системы из предложенного списка). Проверка и указание совместимости с определенными операционными системами (Windows, Linux, iOS), если ими можно управлять с телефона или планшета.
4. Описание принципа работы систем обнаружения/предотвращения вторжений.
5. Установление классификации по степени популярности в использовании и эффективности эксплуатации перечисленных ниже SDI/SPI.

**Предлагаемый список систем обнаружения/предотвращения вторжений, предложенных для анализа:**

- [Prelude Hybrid IDS](#)
- [Sagan](#)
- [Samhain](#)
- [Snort](#)
- [Suricata](#)
- [ACARM-ng](#)
- [AIDE](#)
- [Bro NIDS](#)
- [Fail2ban](#)
- [OSSEC HIDS](#)

Free Trial?		
SolarWinds Security Event Manager		30-Day
Kismet		Free Tool
Zeek		Free Tool
Open DLP		Free Tool
Sagan		Free Tool
Suricata		Free Tool
Security Onion		Free Tool

**Примечание.** Сравнительное описание систем обнаружения/предотвращения вторжений должно быть сосредоточено на следующих принципах:

- ✓ Бесплатное программное обеспечение/лицензированное/условия использования и т. д.,
- ✓ Разнообразие операционных систем, с которыми они совместимы,
- ✓ Описание предлагаемых услуг/принцип работы,
- ✓ Преимущества/недостатки,
- ✓ Интерфейс работы/работа через команды/удобство и простота,
- ✓ Степень безопасности/риск формирования ложных сообщений/тревог,
- ✓ Степень популярности (какие категории людей ими пользуются),
- ✓ Общий аспект/удобство / простота использования инструмента,
- ✓ Другие аспекты, по которым они различаются и т. д.

**Примечание:**

1. Использовать не менее 2-3 систем обнаружения/предотвращения вторжений для их сравнительного анализа и описания.
2. Отчет должен содержать цель работы, комментарии и скриншоты процесса работы с системами обнаружения/предотвращения вторжений (проанализировано/использовано). Сравнительное описание систем обнаружения/предотвращения вторжений (проанализировано/использовано), описание принцип работы систем обнаружения/предотвращения вторжений (проанализировано).