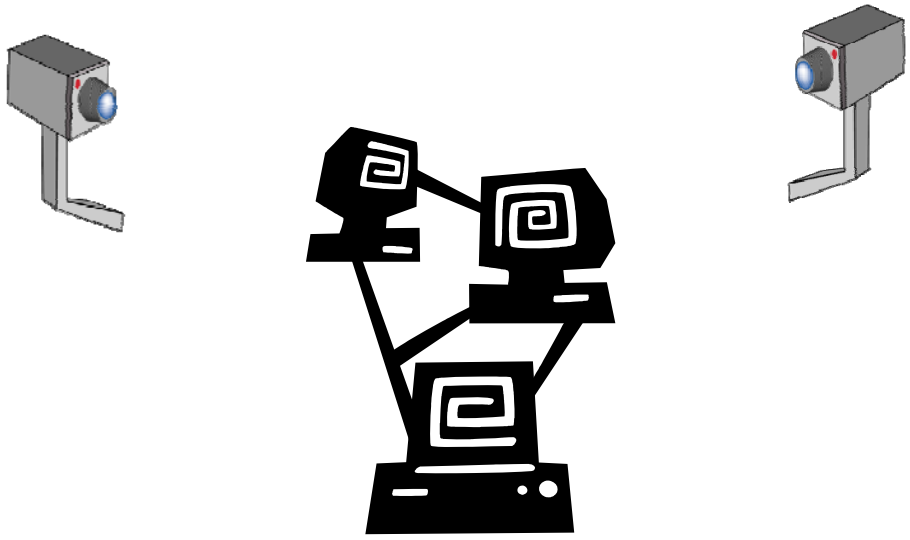
Сравнение систем обнаружения атак: методики и результаты

Лепихин Владимир,
Учебный центр «Информзащита»

Информзащита
Учебный центр

Обнаружение атак

Обнаружение вторжений (атак) – это процесс мониторинга событий, происходящих в компьютерной системе или сети с целью поиска признаков возможных инцидентов

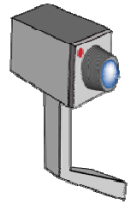


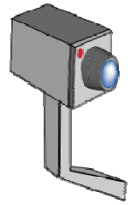
Инфраструктура обнаружения атак

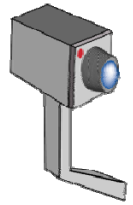
Компоненты управления (клиентская часть)

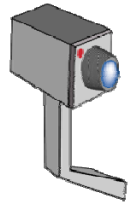
Компоненты управления (серверная часть)

Модули слежения (сенсоры)

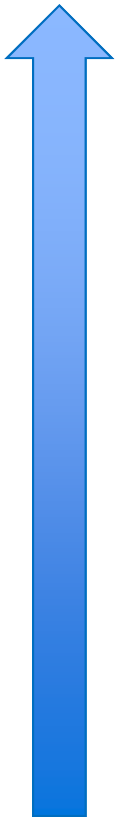








Сетевой модуль слежения (архитектура и принципы работы)



Реагирование

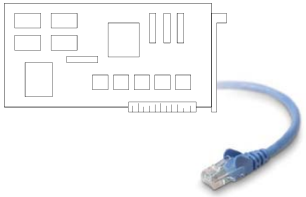
Фильтр механизмов реагирования

Поиск признаков атак

Предварительная обработка

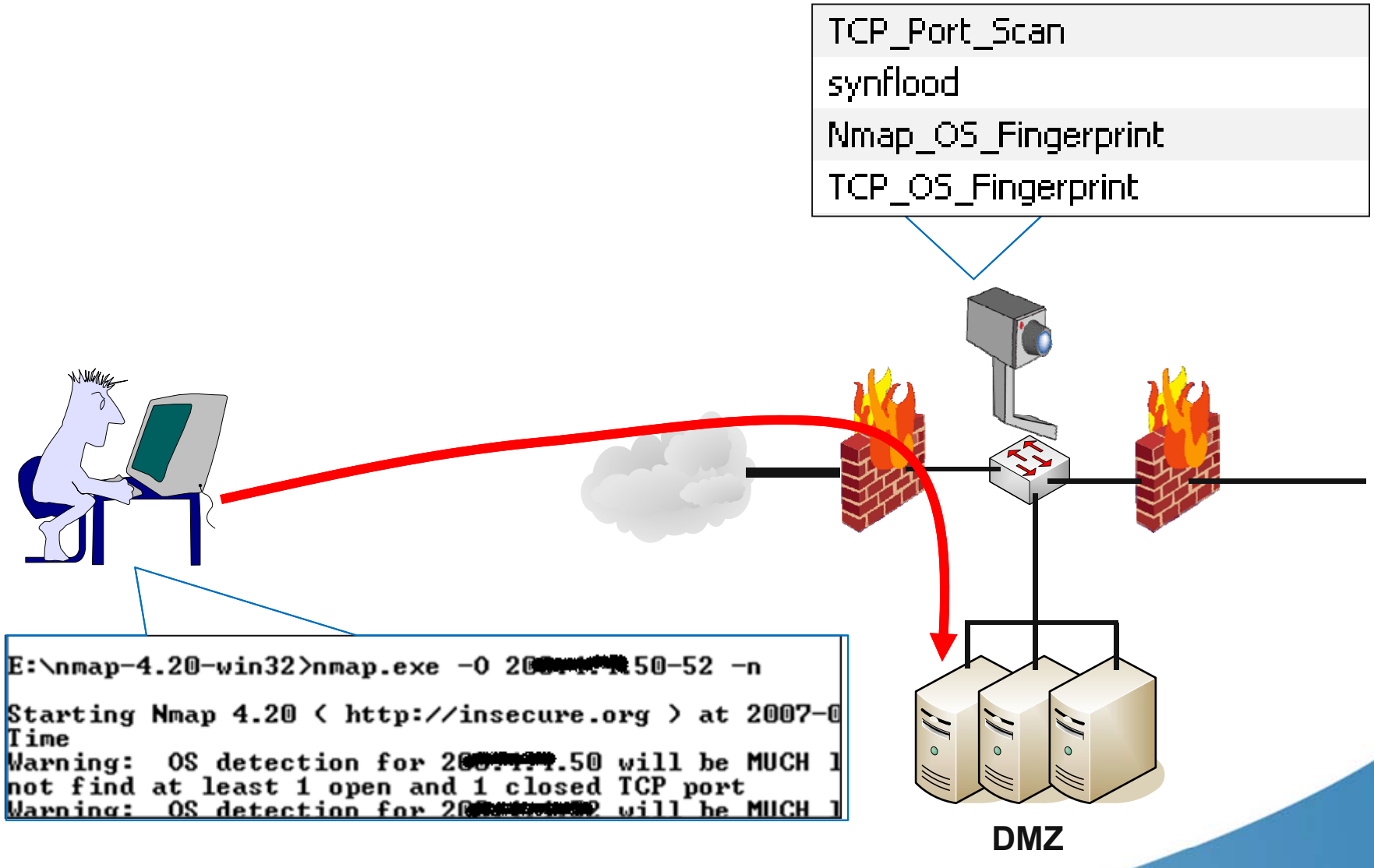
Фильтр пакетов

Захват пакетов



Информзащита
Учебный центр

«Идеальный» пример

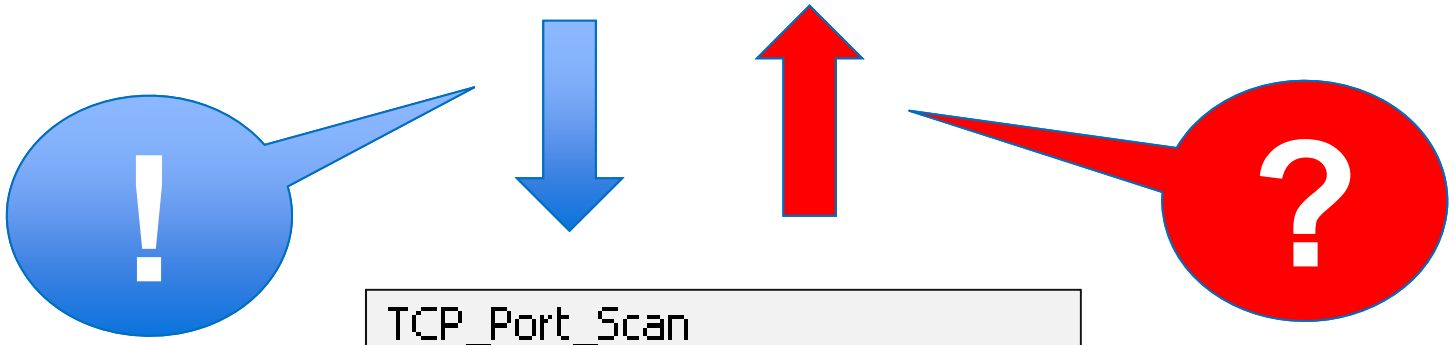


Информзащита
Учебный центр

«Реальная» задача

```
E:\nmap-4.20-win32>nmap.exe -O 20[redacted]50-52 -n

Starting Nmap 4.20 ( http://insecure.org ) at 2007-0
Time
Warning:  OS detection for 20[redacted].50 will be MUCH l
not find at least 1 open and 1 closed TCP port
Warning:  OS detection for 20[redacted] will be MUCH l
```



- TCP_Port_Scan
- synflood
- Nmap_OS_Fingerprint
- TCP_OS_Fingerprint

Информзащита
Учебный центр

Основной объект сравнения

SSL_PCT1_Overflow
Microsoft_Windows_Shell_Banner
TCP_Port_Scan
synflood
Nmap_OS_Fingerprint
TCP_OS_Fingerprint

Поиск признаков атак

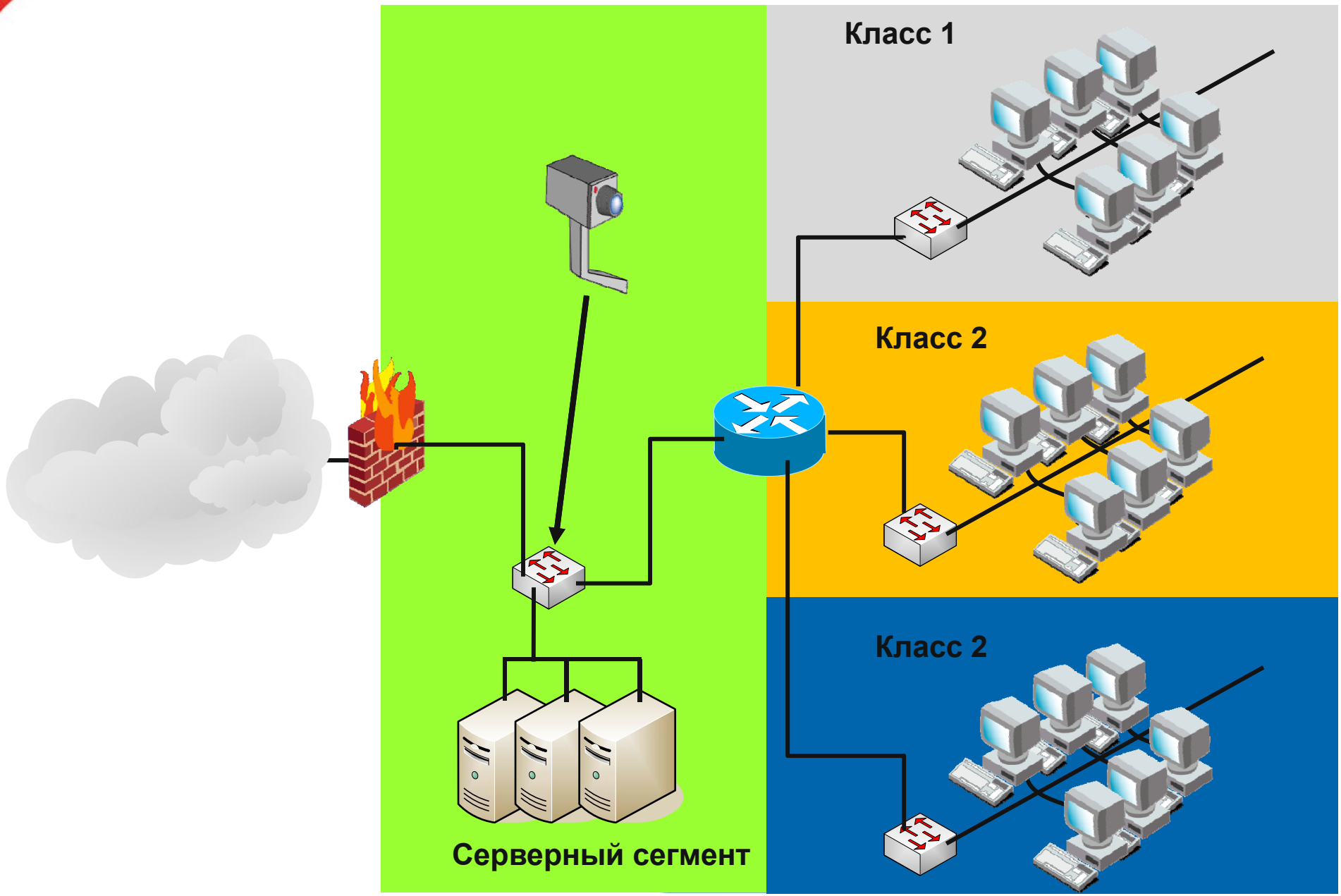
Предварительная обработка

Методика сравнения

1. Определение условий сравнения:
   a) выбор объектов мониторинга;
   b) определение задач мониторинга;
   c) построение модели нарушителя;
   d) разработка требований к настройкам систем;

2. Выбор критериев сравнения
3. Разработка системы подсчёта результирующих баллов.

Объекты мониторинга



Задачи мониторинга

1. Обнаружение атак на узлы серверного сегмента
2. Обнаружение атак на клиентские приложения
3. Выявление сбоев в работе сети
4. Наблюдение за характером трафика

Критерии сравнения

- Количество обнаруженных атак и значимых событий
- Число ложных срабатываний (False Positives)
- Количество атак, обнаруженных правильно (True Positives)
- Число пропусков (False Negatives)
- Число «правильных» пропусков (True Negatives)
- Полнота базы сигнатур (в контексте данной задачи)
- Точность работы (в контексте данной задачи)

Ложные срабатывания

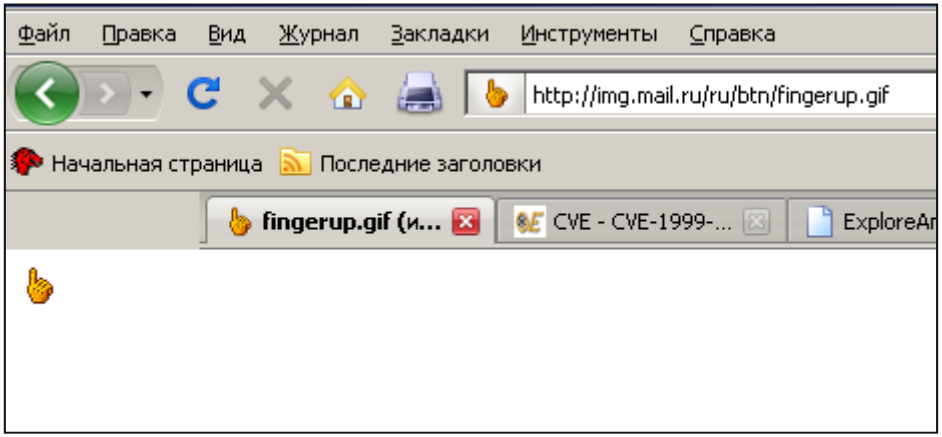
Оповещения о событиях, которых в действительно не происходило

Причины:

1. Неудачный выбор признака атаки

2. Ошибка реализации сигнатуры

Ложные срабатывания



DPort	Pr	Event Message
8080	6	WEB-CGI redirect access
8080	6	WEB-CGI finger access
8080	6	WEB-CGI redirect access

Ложные оповещения

Оповещения о событиях, которые не являются значимыми в данном конкретном случае

Причины:
1. Некорректная настройка системы
2. Особенность признака атаки

Информзащита
Учебный центр

Ложные оповещения

UPX_Packed_Executable

Description

This signature detects PE/COFF executable files that have been packed using the UPX tool. While the presence of a represent an attack, it can be considered an anomaly. The UPX tool is commonly used to pack trojans and malware, used to distribute legitimate commercial software. The file should be examined to determine if it constitutes malware.

Index of /pub/mozilla.org/firefox/releases/3.6.2/win32/ru

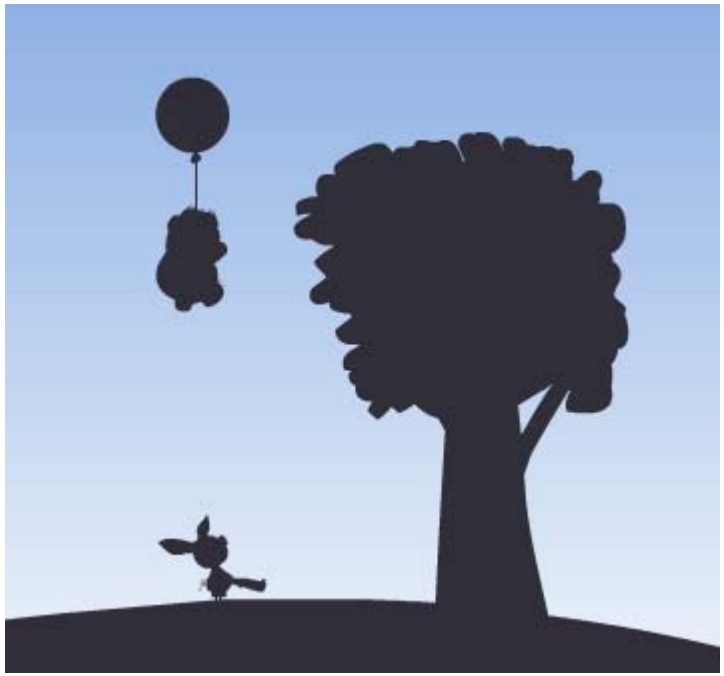
Name	Last modified	Size	Description
Parent Directory		-	
Firefox Setup 3.6.2.exe	16-Mar-2010 16:53	8.2M	
Firefox Setup 3.6.2.exe.asc	16-Mar-2010 17:02	194	

Оценка модуля слежения

По результатам мониторинга	В действительности	
	Факт атаки имел место	**Факта атаки не было**
Атака обнаружена	True Positive	False Positive
Атака не обнаружена	False Negative	True Negative

Точность обнаружения

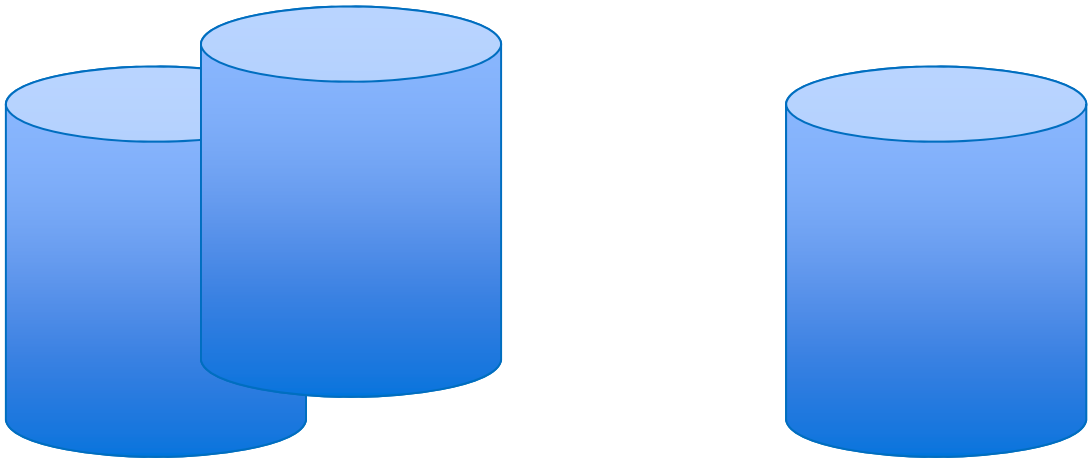
Precision= True Positive/(True Positive + False Positive)



…
— Разве я не попал? — спросил Пятачок.
— Не то чтобы совсем не попал,— сказал Пух,— но только не попал в шарик!
…

Sensitivity (полнота базы сигнатур)

Sensitivity=True Positive/(True Positive + False Negative)



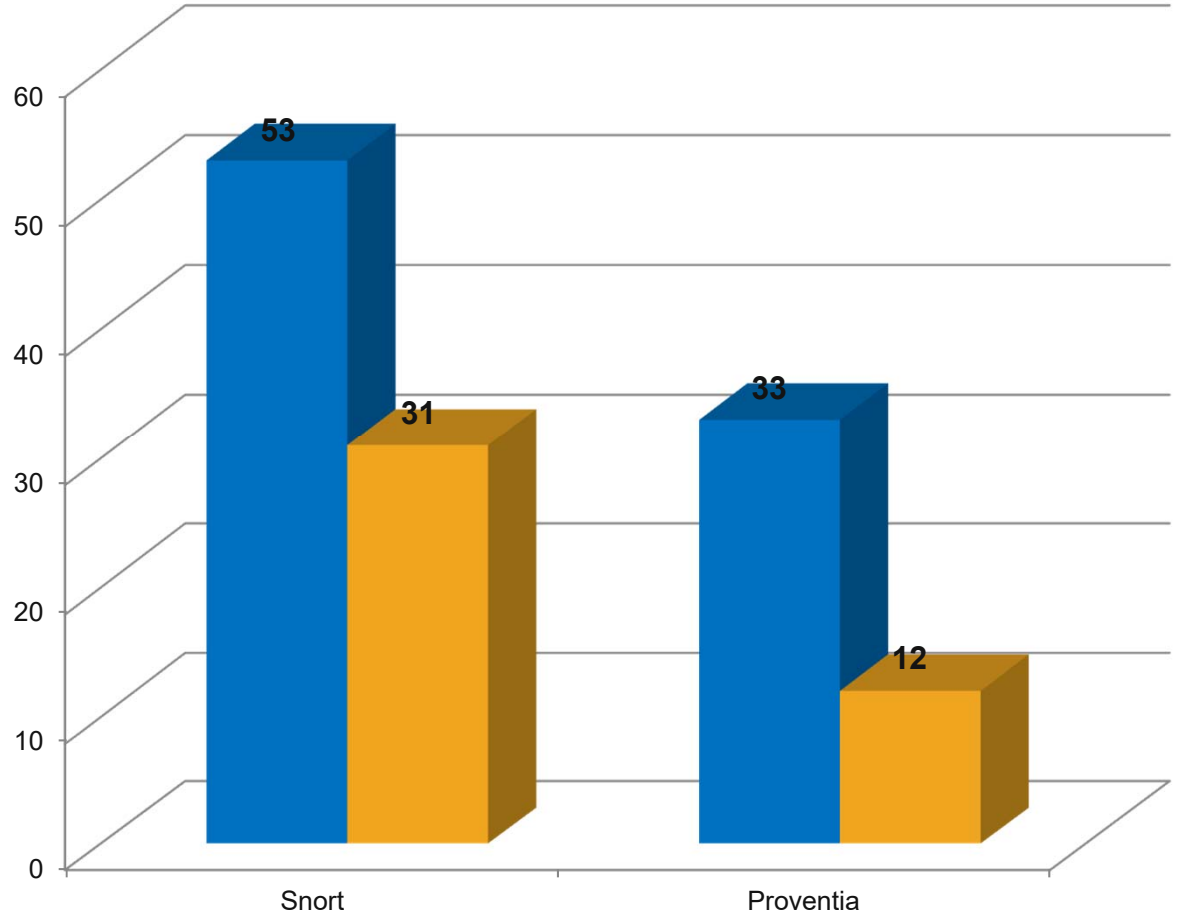
Суммарная точность работы (accuracy)

$$A=(TP+TN)/(TP+TN+FP+FN)$$

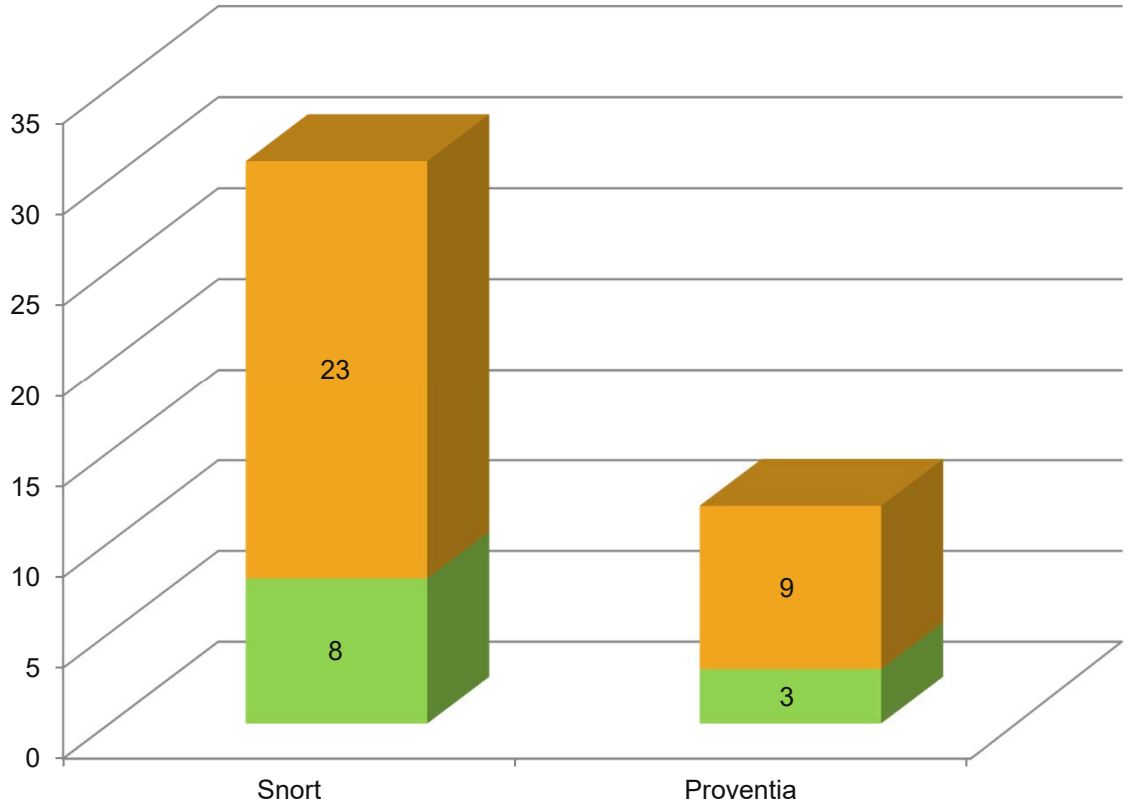
Настройка систем

- ✓ Включение всех сигнатур
- ✓Отключение событий, нормальных для условий сравнения

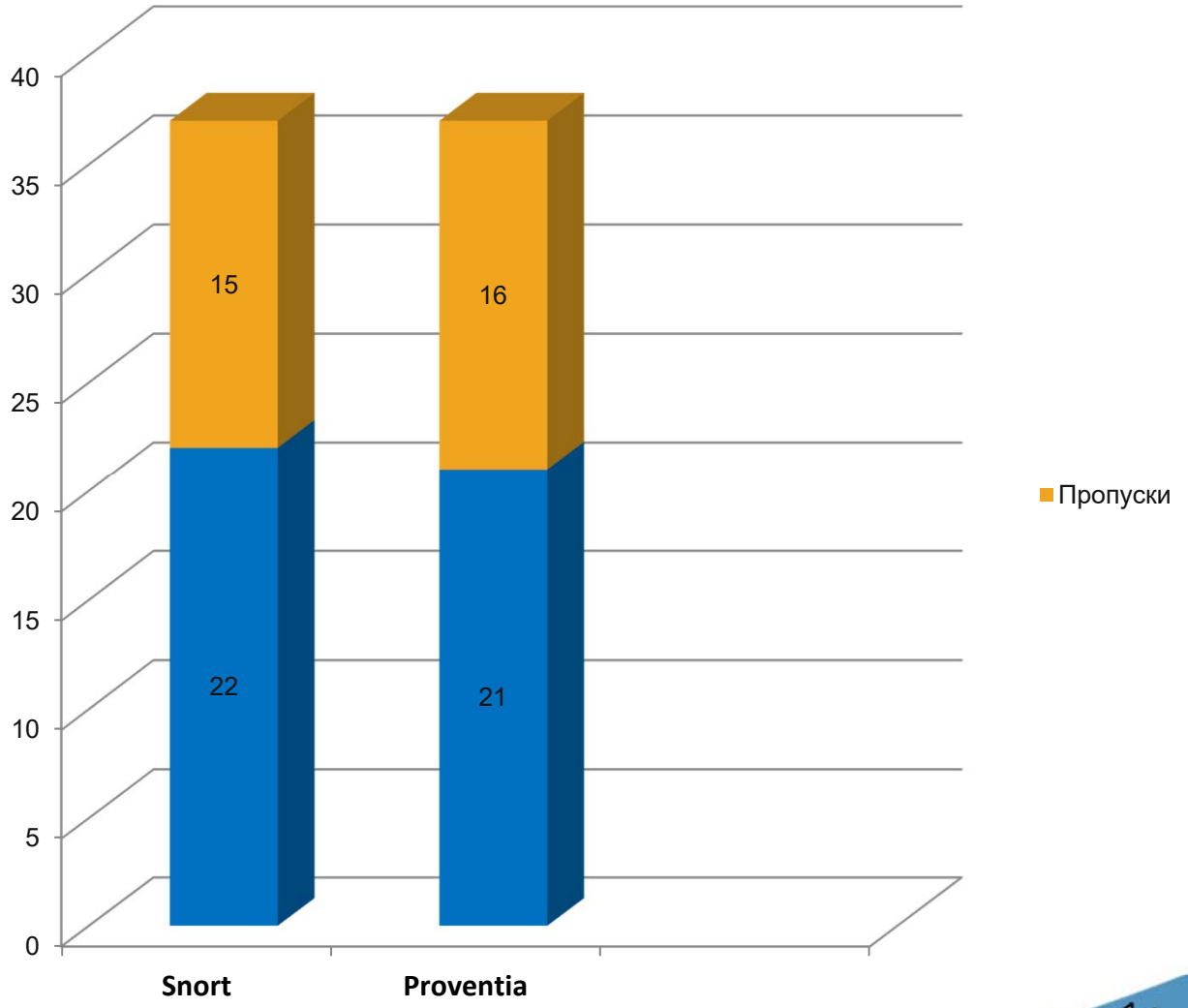
Обнаруженные события и ложные срабатывания



Ложные срабатывания и ложные оповещения



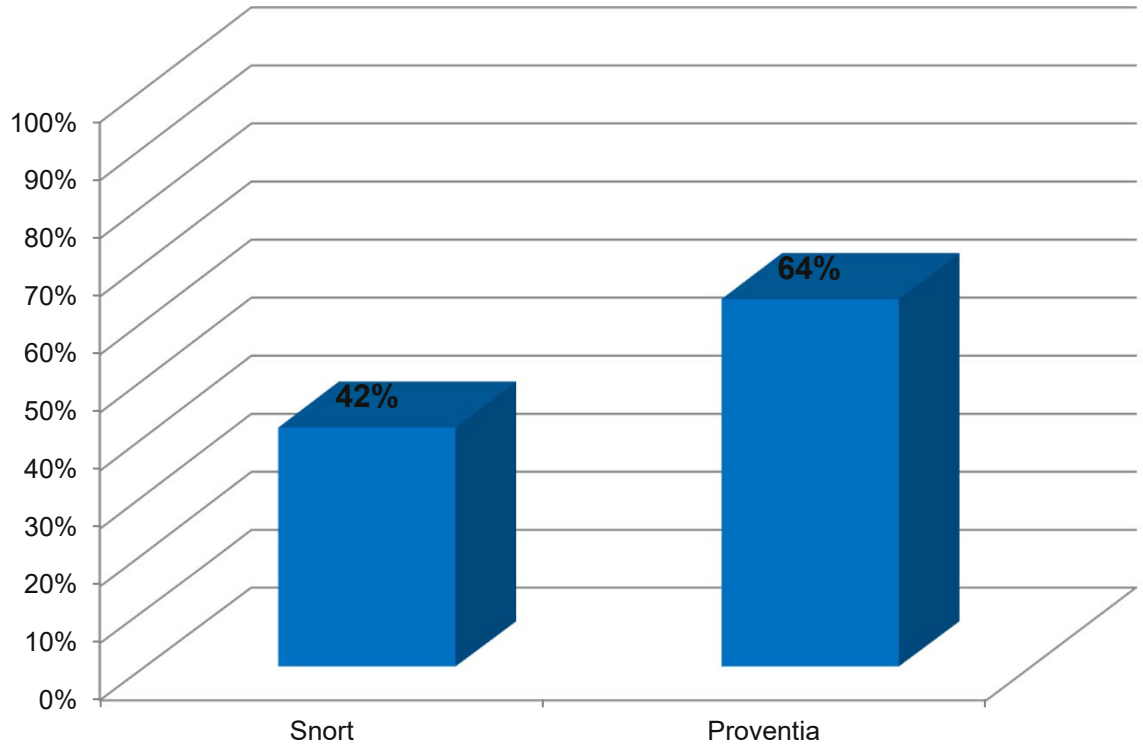
Обнаруженные события и пропуски



Информзащита
Учебный центр

Точность работы модуля обнаружения

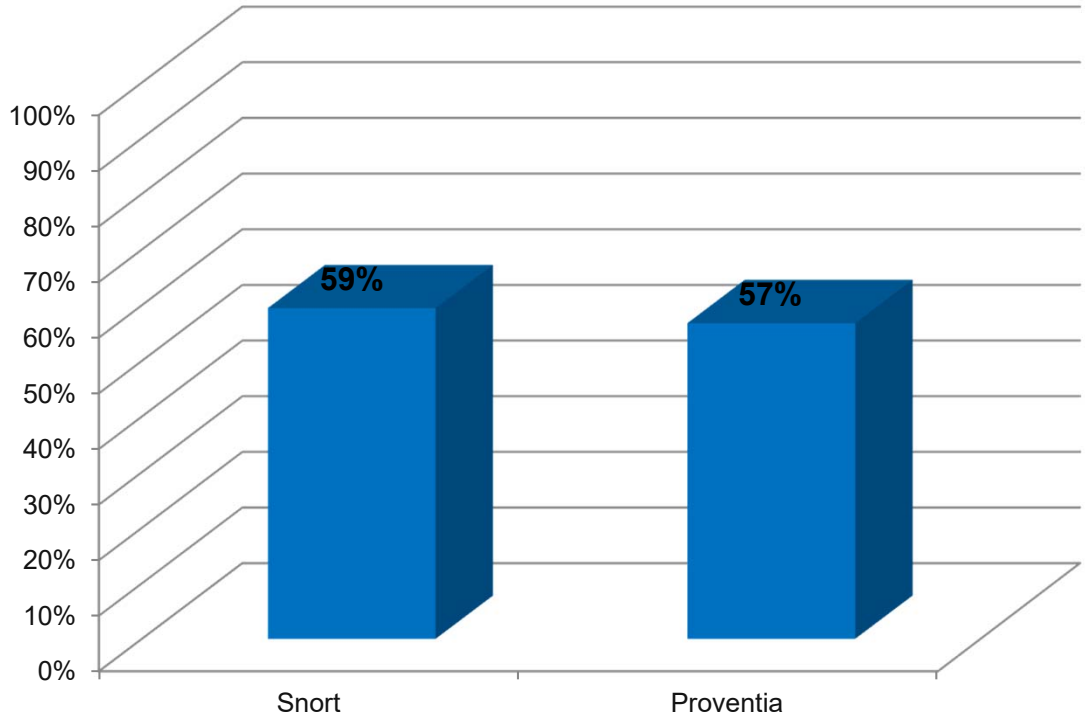
Precision=TP/(TP+FP)



Информзащита
Учебный центр

Sensitivity (полнота базы)

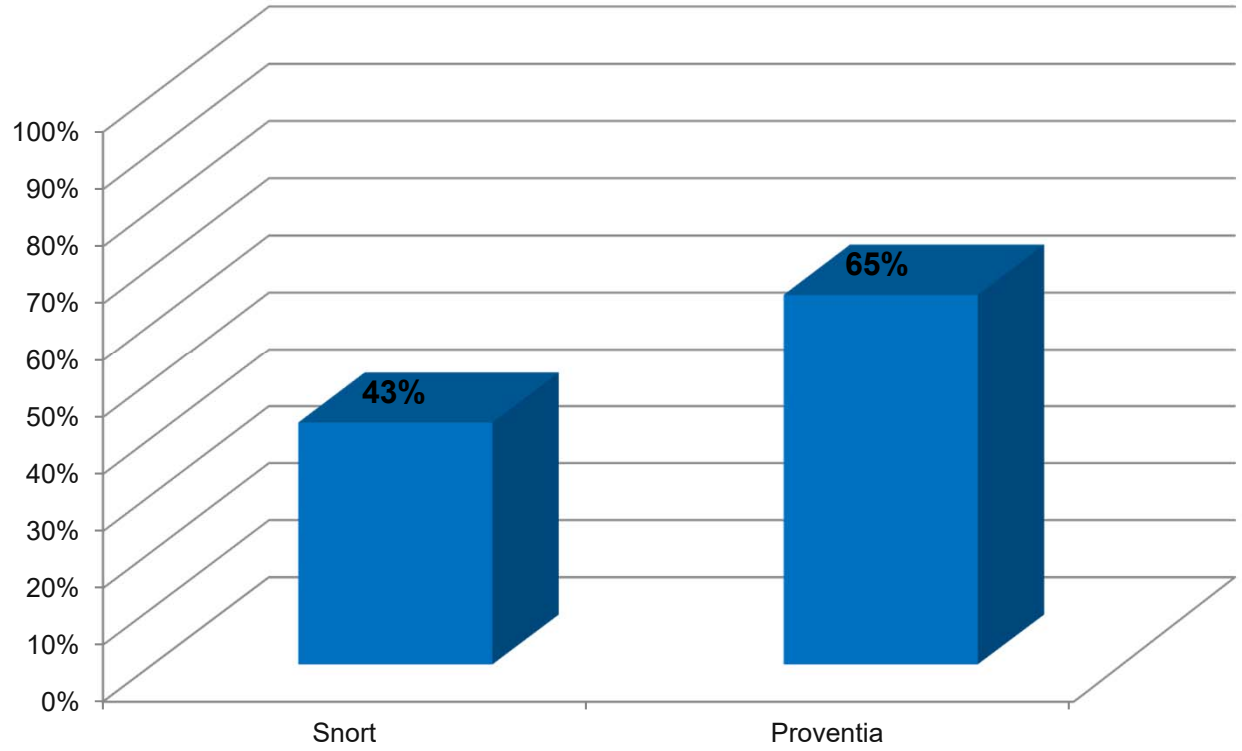
Sensitivity=TP/(TP+FN)



Информзащита
Учебный центр

Суммарная точность работы (accuracy)

A=(TP+TN)/(TP+TN+FP+FN)



Информзащита
Учебный центр

Выводы

- ✓ Обе системы имеют существенный процент ложных срабатываний
- ✓ Возникают большие сомнения относительно использования режима блокировки
- ✓ Необходима корреляция событий