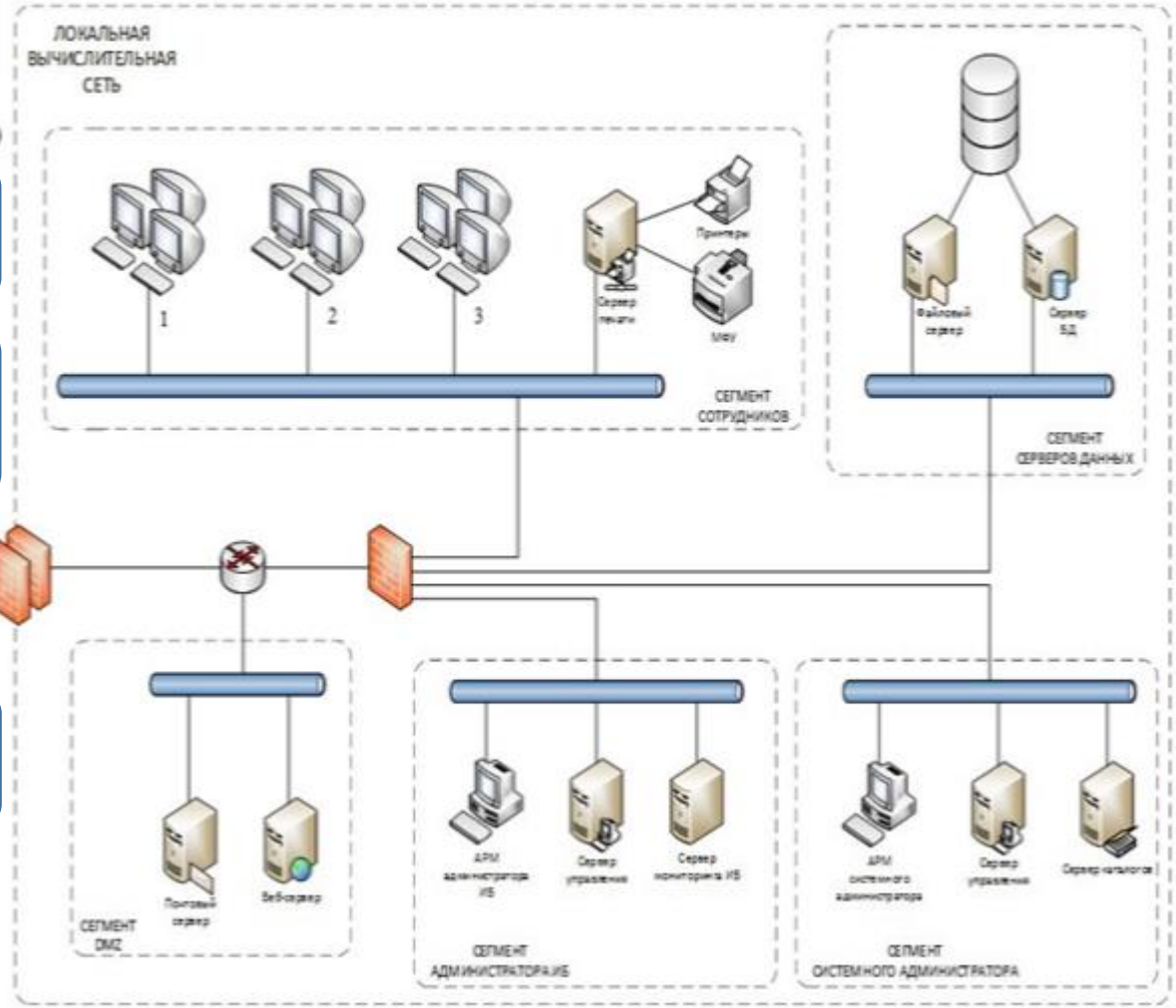
ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

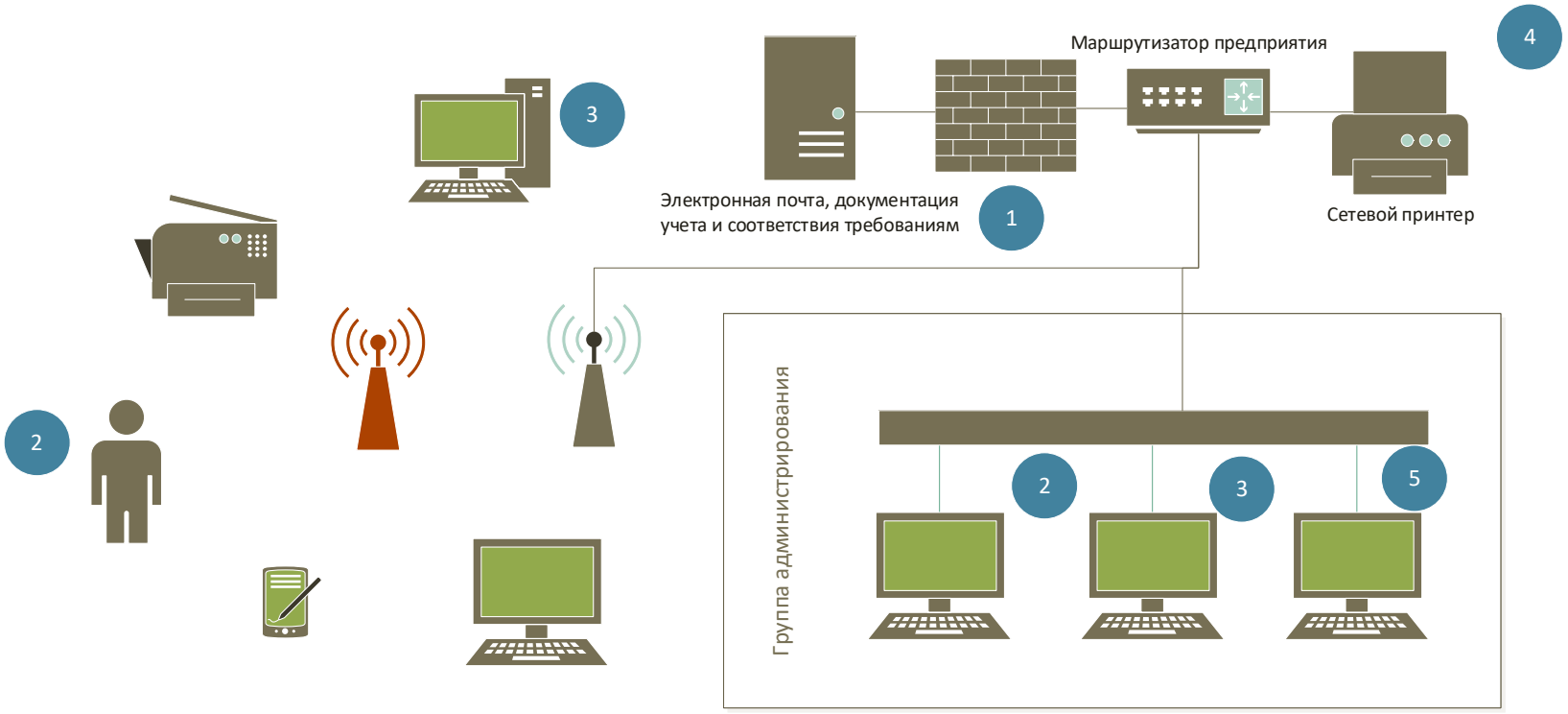
Средства и методы интеллектуального обнаружения и предотвращения вторжений

Тенденции

- Рост числа сегментов сети и количества узлов
- Рост числа типа платформ
- Рост количества виртуальных узлов и топологий (VPN, VRF, VLAN)
- Рост требований к квалификации персонала
- Рост требований к средствам защиты
- Рост количества сетевых угроз



Тенденции



1	Межсетевые экраны	5	DPL		Виртуальные машины
2	Антивирусы		Стационарные АРМ		Сетевое оборудование
3	Системы мониторинга сети (IDS/ IPS)		Мобильные АРМ		
4	СКУД		Серверы		

Проблемы традиционного подхода

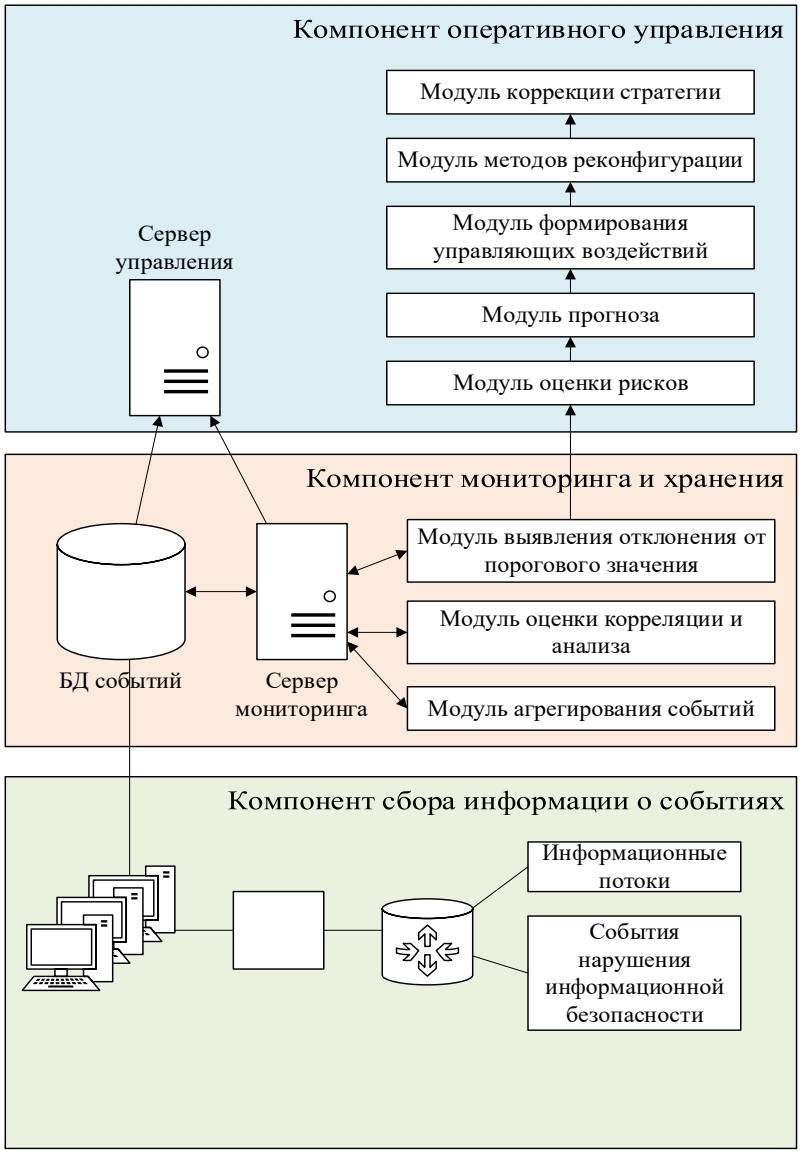
1. Настройка и контроль работы СЗИ в «ручном режиме»
2. Локальный контроль журналов и настроек хостов в сети
3. Центры управления СЗИ не консолидированы
4. Отсутствие регулярности в операций контроля работы СЗИ
5. СЗИ не сбалансированы

Архитектура систем обнаружения вторжения

Система обнаружения вторжений (Intrusion Detection System, IDS) — программное или аппаратное средство, которое автоматизируют процесс просмотра событий, и анализируют их с точки зрения безопасности.

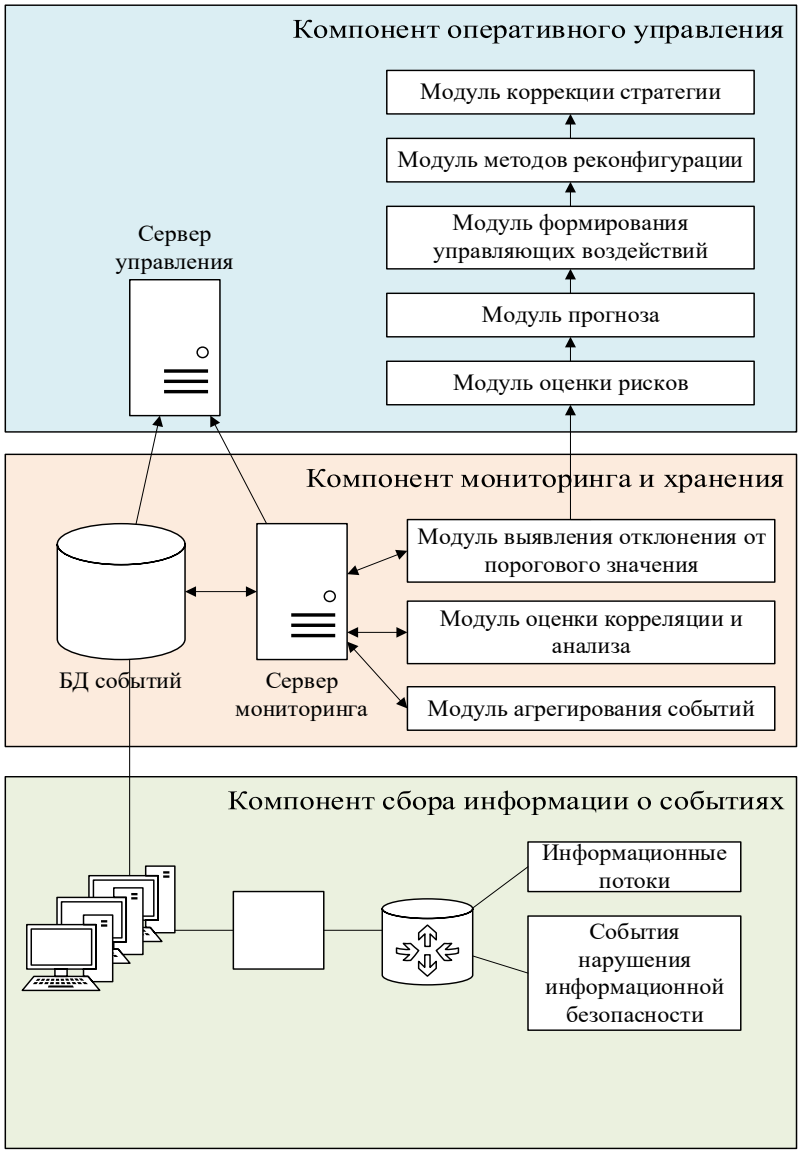
Архитектура СОВ включает:

- сенсорную подсистему
- подсистему хранения и анализа
- консоль управления



Архитектура систем обнаружения вторжения

- Сетевая СОВ используя доступ к сетевому трафику, подключаясь к шлюзу, настроенному на зеркалирование портов.
- Основанная на протоколе СОВ, представляет собой систему (либо агента), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями.
- Узловая СОВ (Host-based IDS, HIDS) — система (или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов.
- Гибридная СОВ совмещает два и более подходов к разработке СОВ

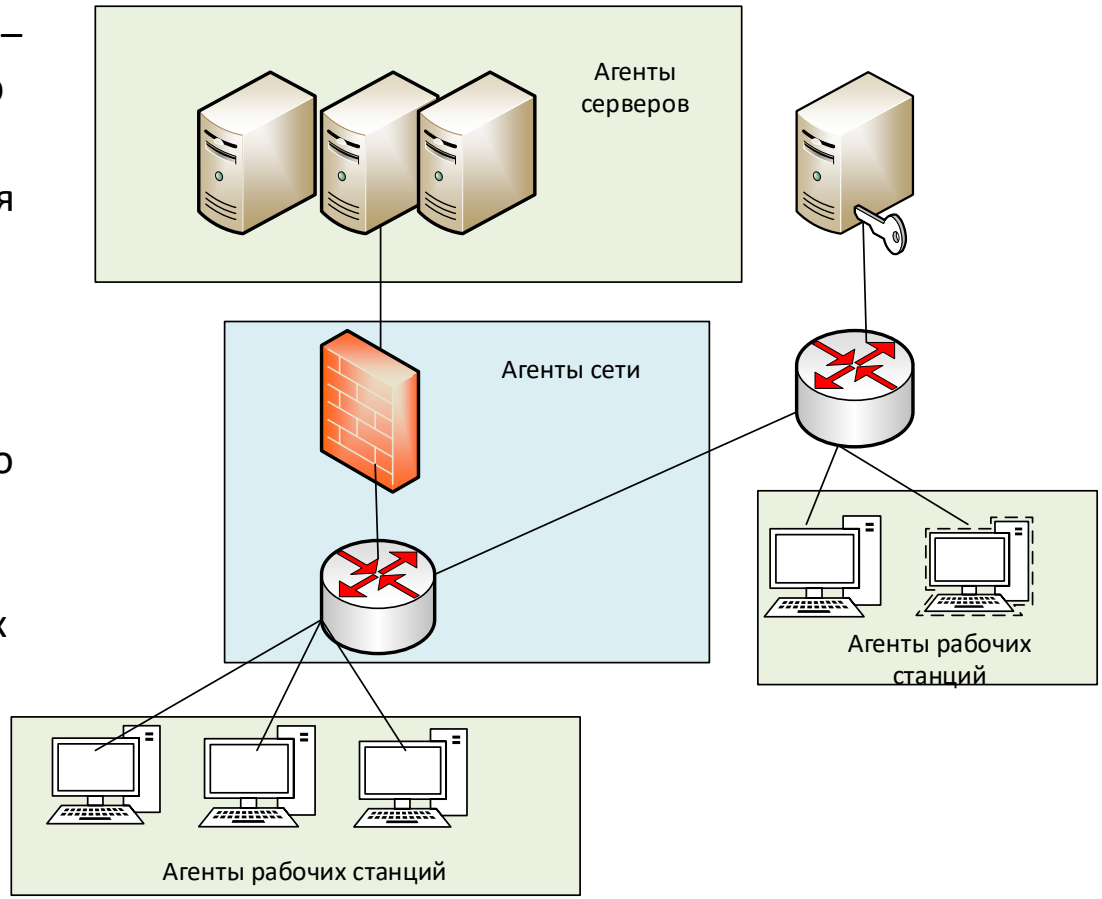


Многоагентные системы обнаружения вторжений

Многоагентную систему можно представить в виде графа G = (A,B), где A – множество агентов, B – множество ребер графа; ребро существует тогда и только тогда, когда пара агентов может связаться друг с другом, минуя других агентов.

Многоагентые системы включают в себя:

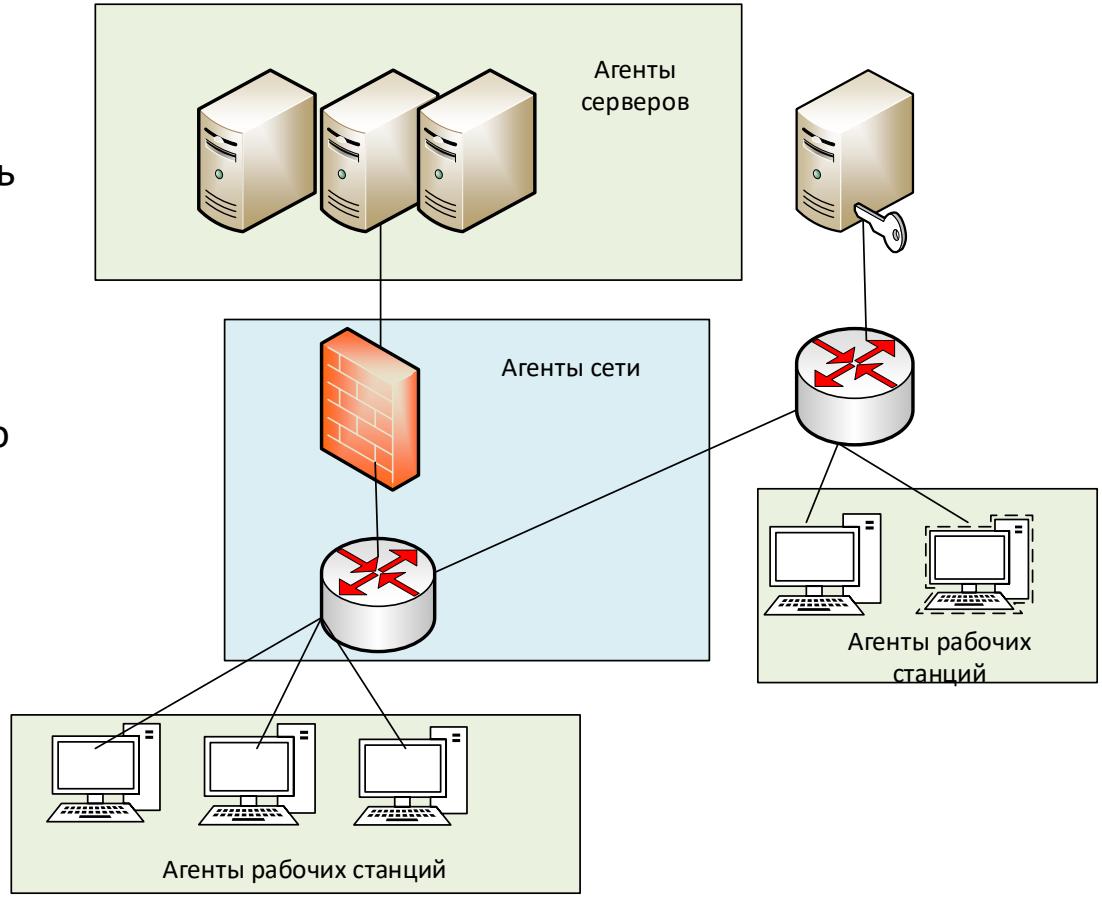
- агентов сети, анализирующих сведения о пакетах, передаваемых по сети, которые могут размещаться на сетевых устройствах (например, анализирующих сведения о событиях маршрутизаторов)
- агентов серверов, анализирующих сведения о событиях, происходящих на серверах ИС
- агентов рабочих станций, анализирующих сведения о событиях, происходящих на рабочих станциях.



Многоагентные системы обнаружения вторжений

В зависимости от того, какое событие было отнесено к одному из классов опасности, агенты СОА могут выполнять различные действия в соответствии с настройками многоагентной СОА:

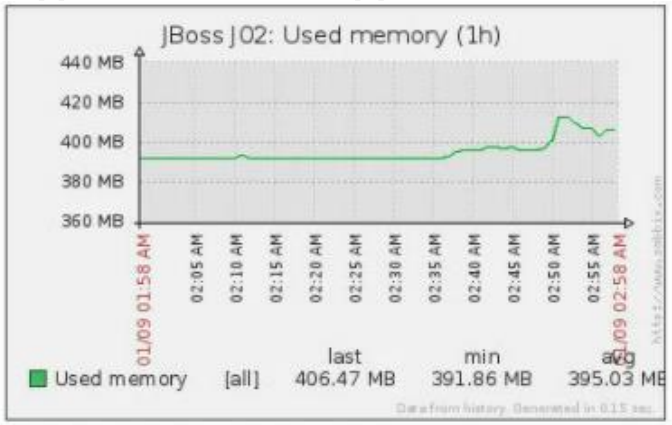
- запись события в журнал СОА
- информирование администратора о произошедшем событии
- блокирование процесса
- разрыв соединения
- прерывание процесса



Функциональные особенности

К основным функциям систем IDS относятся:
- выявление вторжений и сетевых атак;
- запись всех событий;
- поиск уязвимостей;
- прогнозирование атак;
- распознавание источника атаки;
- информирование служб ИБ об инциденте;
- формирование отчетов.

Сбор данных	Обработка	Анализ	Представление
Pull method	Нормализация	Агрегация	Визуализация
Push method	Фильтрация	Классификация	Генерация решений
	Корреляция	Корреляция	Предупреждение
	Агрегация	Анализ событий и инцидентов	Поддержка принятия решений
	Классификация	Приоритезация	
		Прогнозирование	

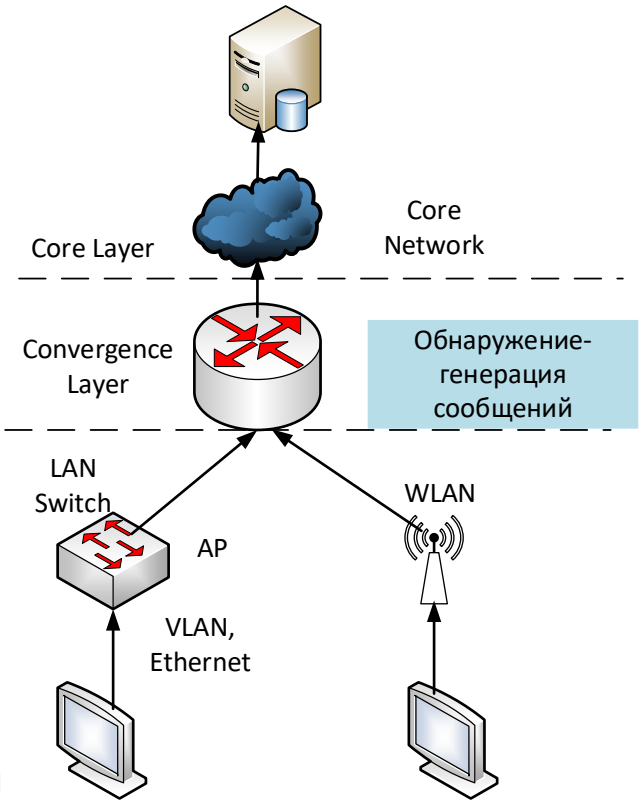


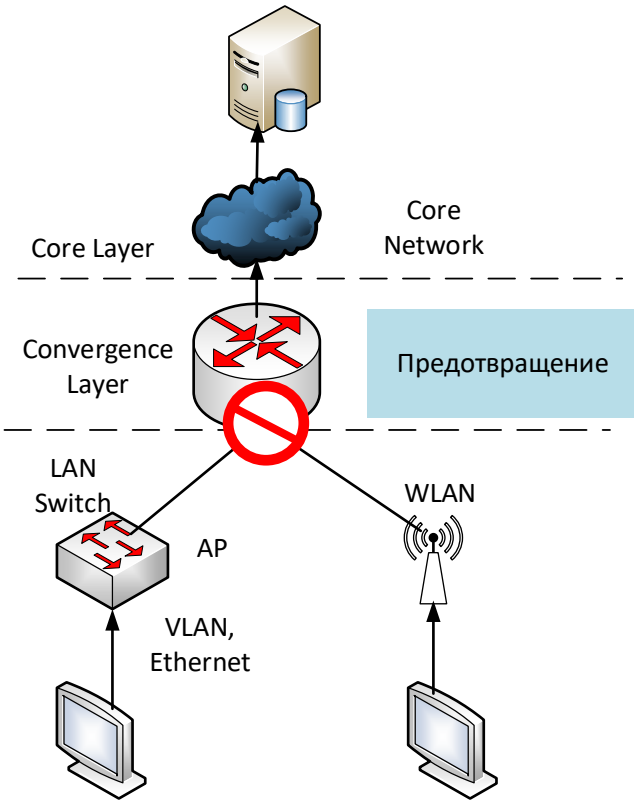
Анализ сетевой активности ↔ Анализ системной активности ↔ Анализ активности приложений ↔ Анализ активности СЗИ ↔ Анализ активности пользователей

Различия между IDS и IPS

В пассивной СОВ (IDS) при обнаружении нарушения безопасности информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются администратору системы по определенному каналу связи.

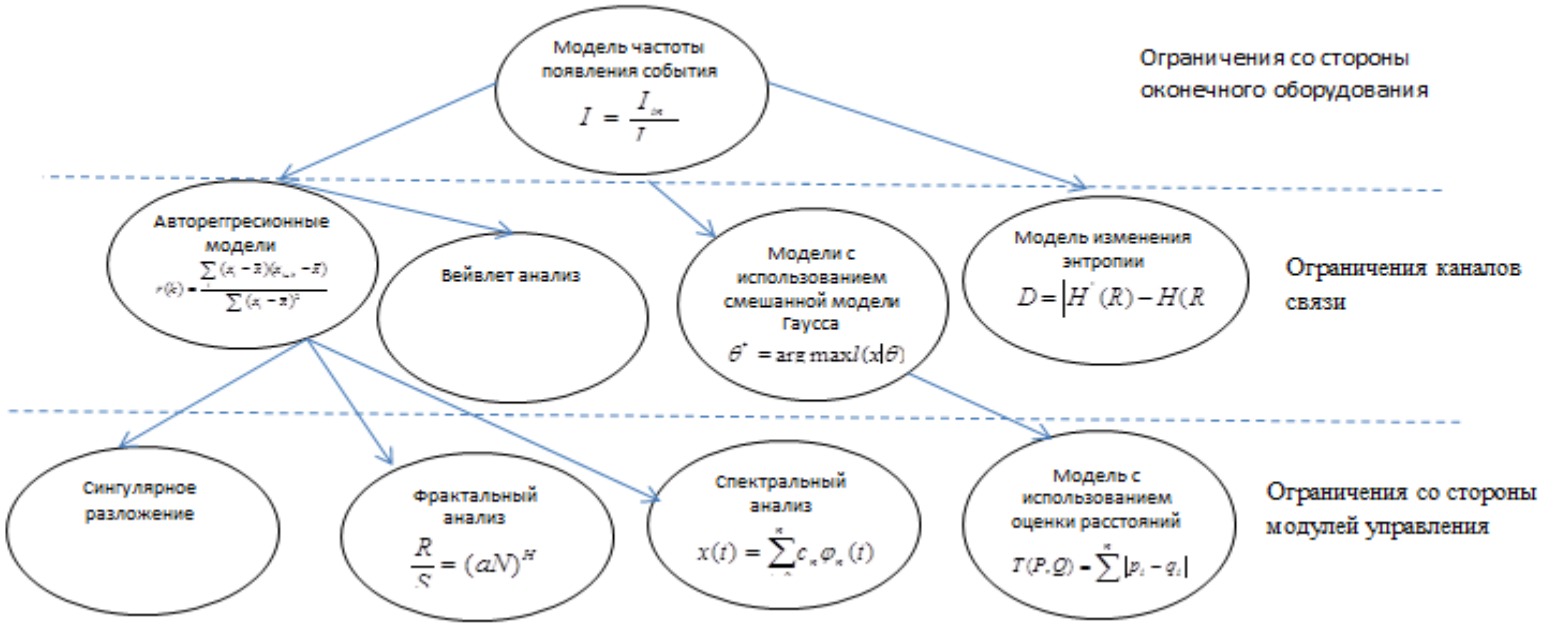
В активной системе (IPS), СОВ ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника.





Классификация систем обнаружения вторжения

Статистические методы оценки сетевого трафика

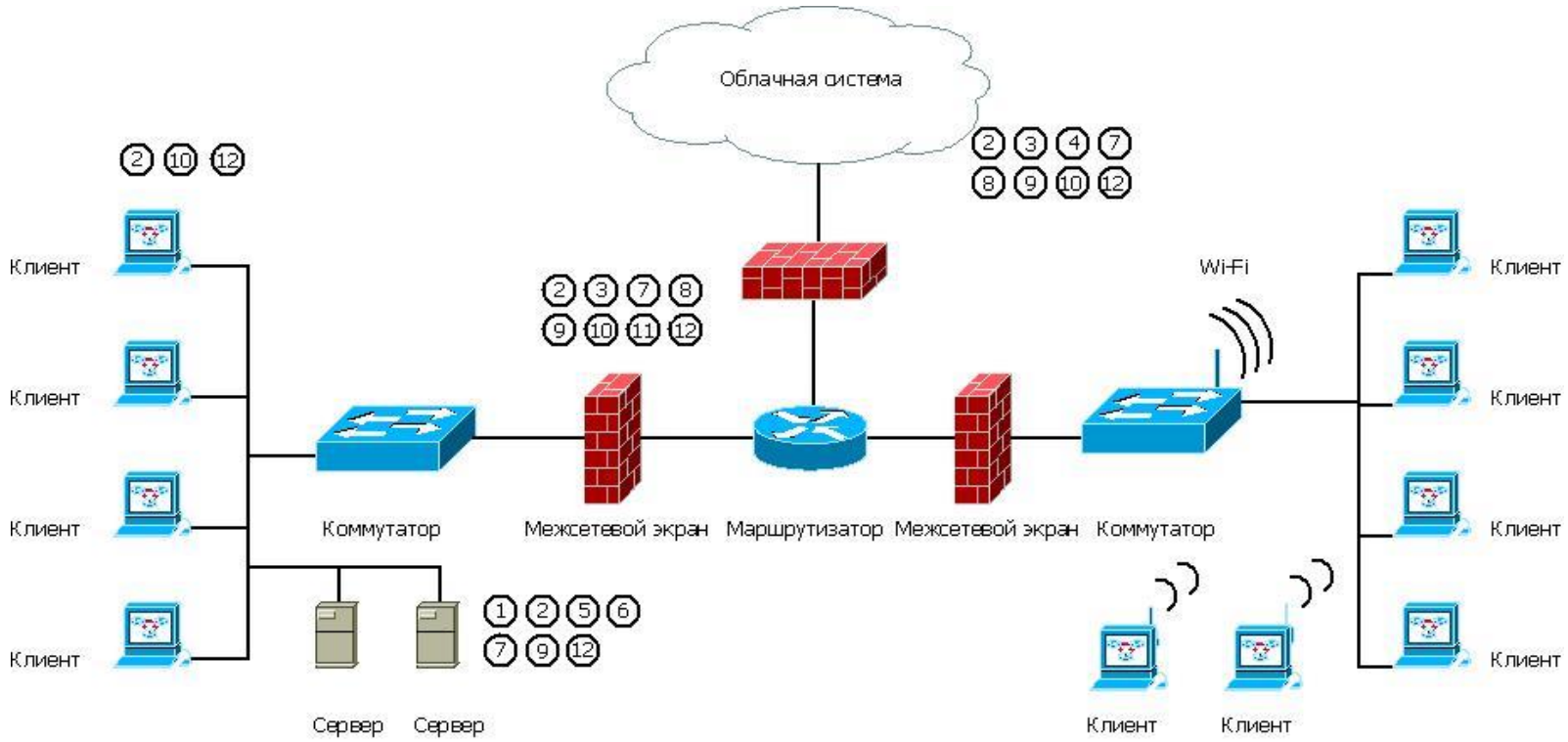


Преимущество: учет нелинейных факторов

Ограничения:

- вычислительная сложность
- избыточность полученных результатов
- трудность при адаптации
- наличии больших всплесков на фоне относительно низкого среднего уровня информационного потока
- большой объем статистических данных.

Статистические методы оценки сетевого трафика



1. вычисление коэффициентов расстояния и подобия распределений
2. модель гауссовских смесей
3. оценка характеристик входящего потока
4. вычисление разности энтропий трафика
5. вычисление разности энтропий сессий
6. вычисление разности энтропий с TCP-флагами
7. метод опорных (поворотных) точек
8. нейтрализация источника DDoS
9. расчёт частот TCP-флагов
10. вейвлет-анализ сетевого трафика
11. фрактальный анализ
12. прогнозирование трафика

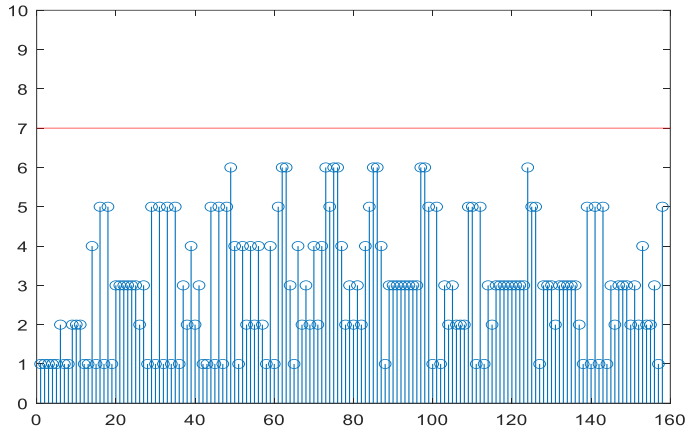
Статистические методы оценки сетевого трафика

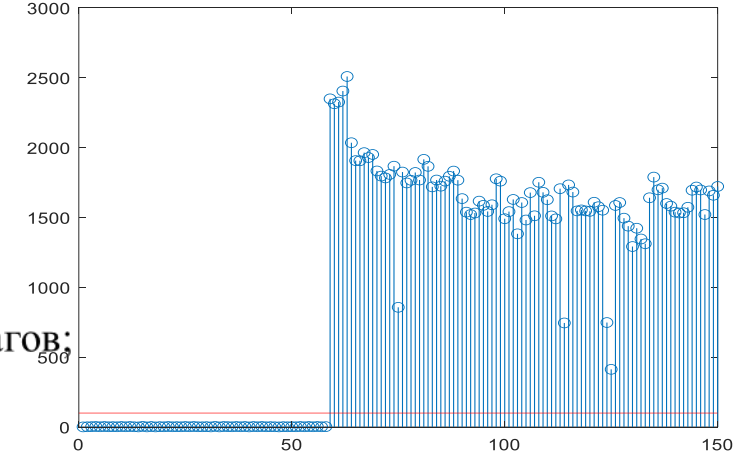
$$M = (T, X_r, Md, P),$$

где T – постоянный временной интервал,
X_r – характеристики трафика, Md – метод расчета,
P – пороговое значение

$X_r = \{src, dst, macsrc, macdst, len, tos, ttl, proto, spt, dpt, window, urg, ack, psh, rst, syn, fin, df, time\}$,
где:

- *src/dst* – ip-адрес источника/получателя;
- *macsrc/macdst* – MAC-адрес источника/получателя;
- *len* – длина пакета;
- *tos* – тип обслуживания;
- *ttl* – время жизни пакета;
- *proto* – протокол передачи;
- *spt/dpt* – порт источника/получателя;
- *window* – размер окна;
- *urg/ack/psh/rst/syn/fin/df* – наличие соответствующих флагов;
- *time* – время фиксации пакета.

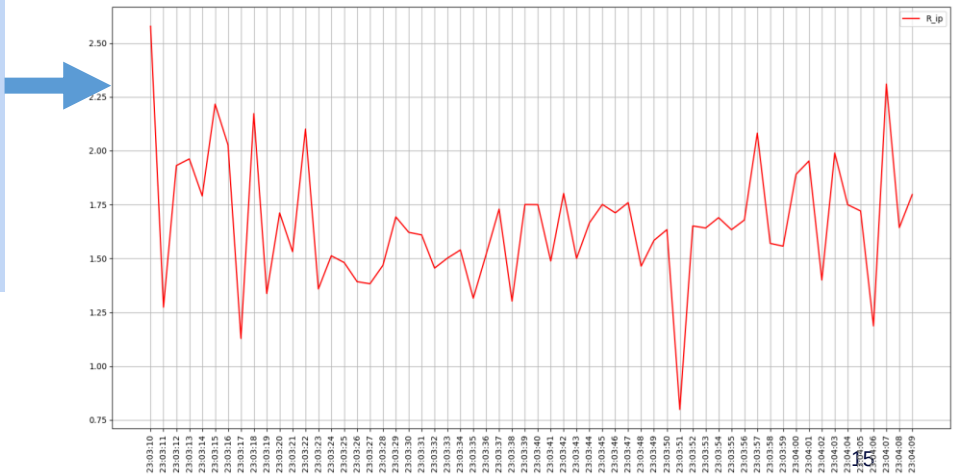




Статистические методы оценки сетевого трафика

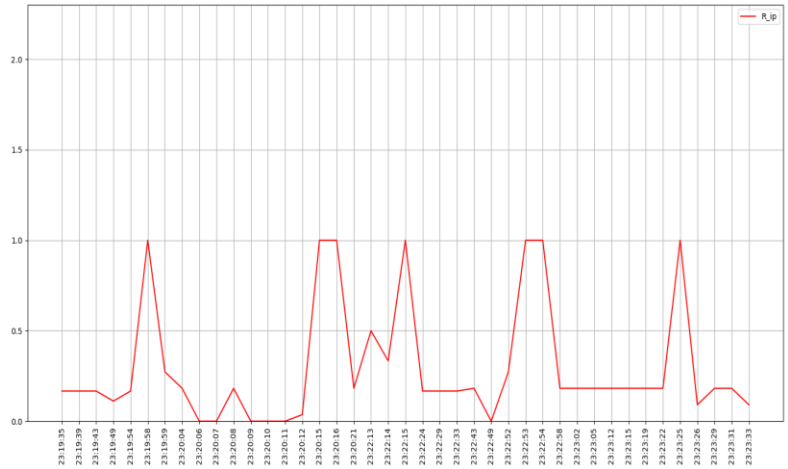
Показатели функционирования хоста				
Входящая скорость передачи данных	Наличие узла в сети	Входящая скорость передачи пакетов	Количество активных потоков	Показатель использования портов
Исходящая скорость передачи данных	Относительная частота использования протоколов	Исходящая скорость передачи пакетов	Средний размер потока	Показатель безопасности портов

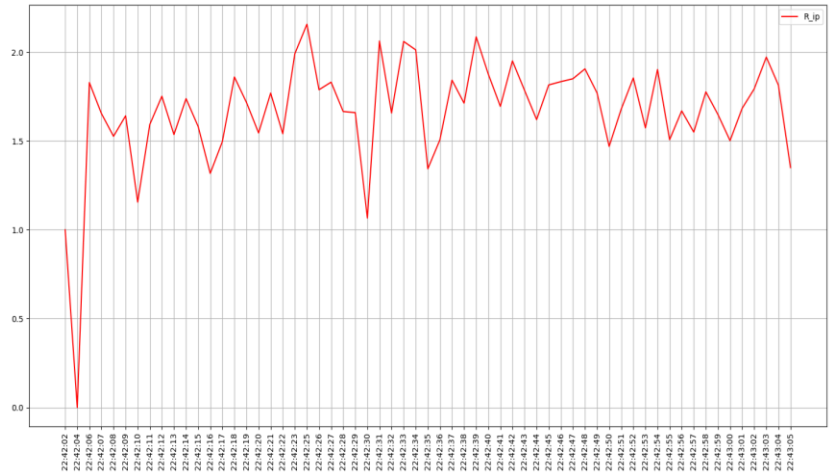
Time	R_ip	N_tcp	N_udp	N_icmp	L/N
22:42:02	1.000000	0.000000	1.0	0.0	452.000000
22:42:04	0.000000	0.000000	0.0	0.0	342.666667
22:42:06	1.828947	1.828947	0.0	0.0	184.320465
22:42:07	1.654545	1.654545	0.0	0.0	233.213230
22:42:08	1.526380	1.526380	0.0	0.0	249.328193
...	...	...	...	...	...
22:43:01	1.683549	1.683549	0.0	0.0	215.687755
22:43:02	1.793566	1.793566	0.0	0.0	235.556782
22:43:03	1.972105	1.972105	0.0	0.0	256.687799
22:43:04	1.814328	1.820851	0.0	0.0	236.546669
22:43:05	1.350482	1.350482	0.0	0.0	190.833105



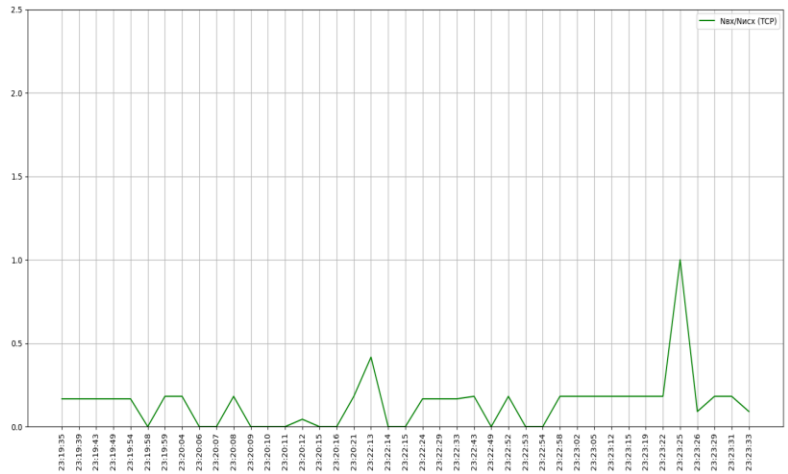
Пример обнаружения атаки HTTP-flood

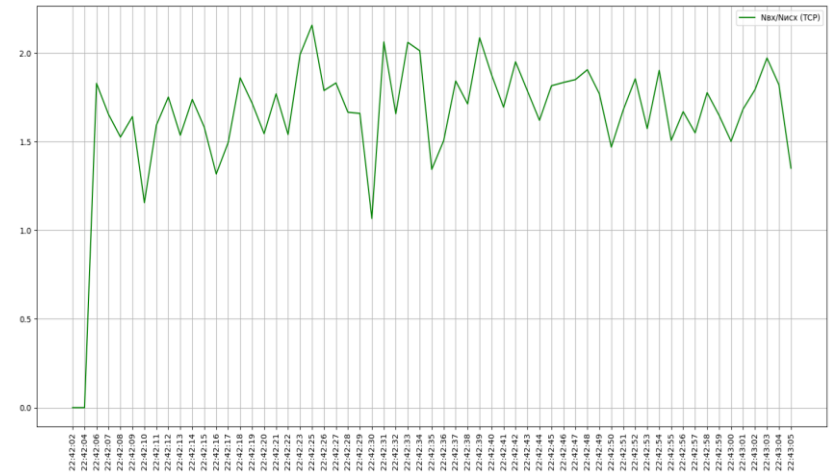
Отношение входящего и исходящего IP-трафика





Отношение количества входящих и исходящих пакетов по протоколу HTTP



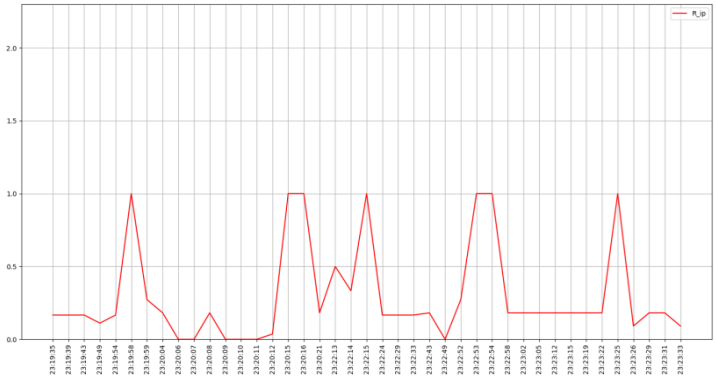


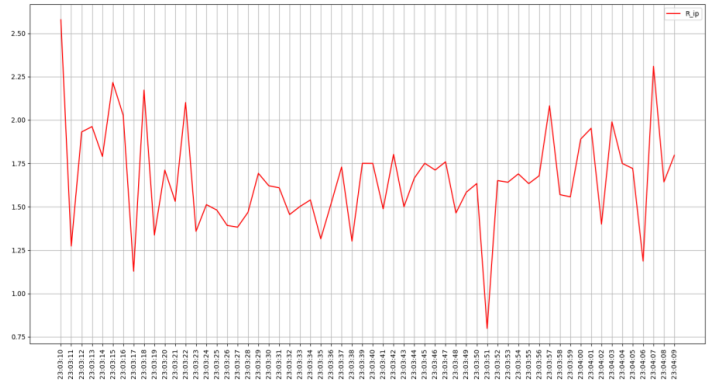
Штатное функционирование

Атака HTTP-flood

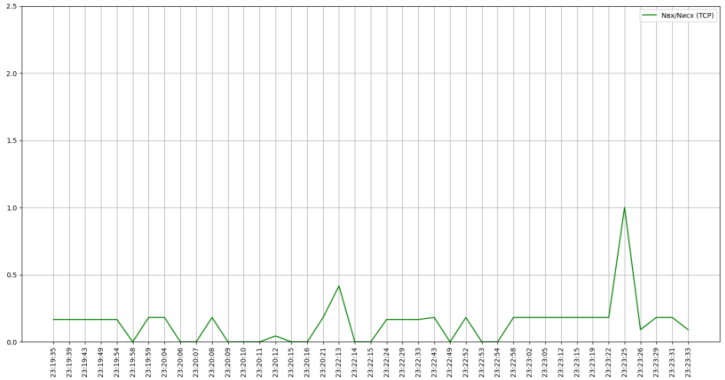
Пример обнаружения комбинированной атаки

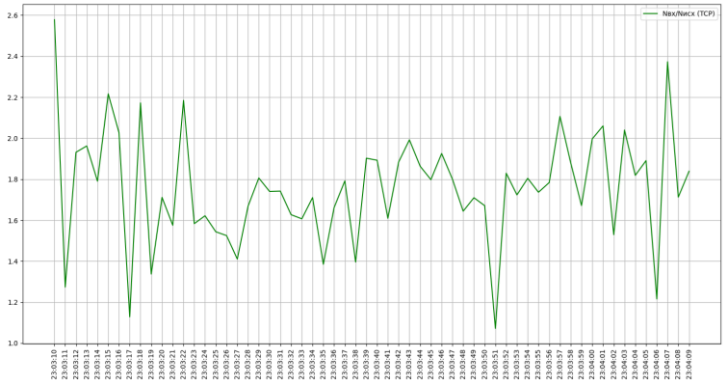
Отношение входящего и исходящего IP-трафика





Отношение количества входящих и исходящих пакетов по протоколу HTTP





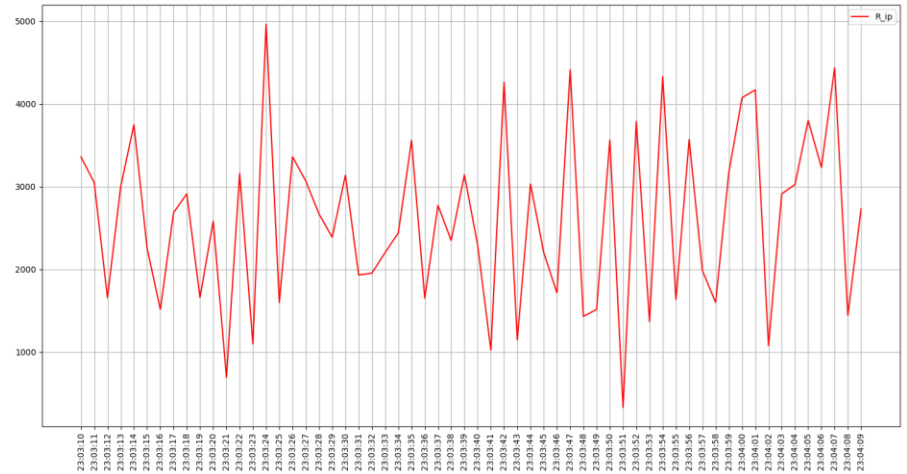
Штатное функционирование

Атака HTTP-flood

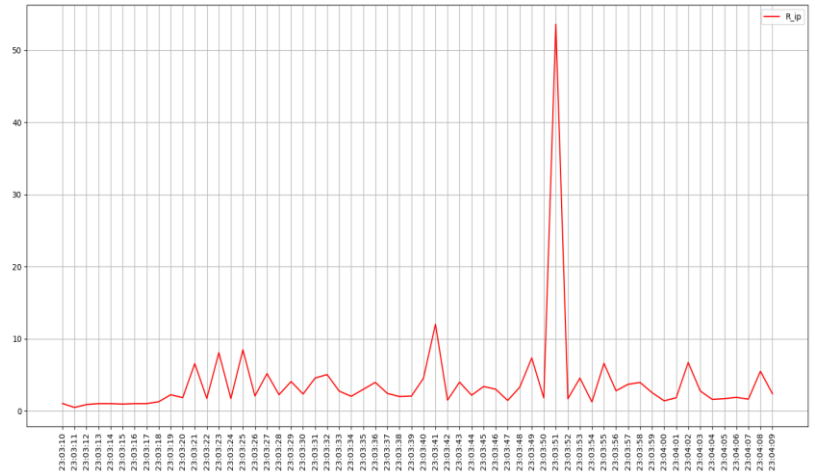
Пример обнаружения комбинированной атаки

Разделение общего трафика на потоки трафика атак SYN-flood и HTTP-flood при использовании показателей использования портов и установленных флагов в заголовке пакета

Количество IP-пакетов в секунду



HTTP-flood

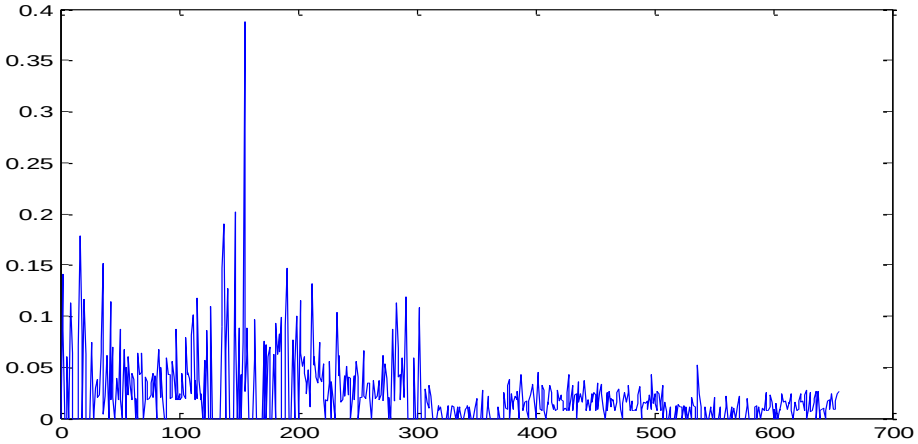


SYN-flood

Методы спектрального анализа сетевого трафика

1. Разложить случайную реализацию трафика по детерминированным ортогональным функциям.
2. Определить коэффициенты гармонического разложения.
3. Для случайного процесса разложить спектральную плотность мощности, с использованием преобразования Фурье (соотношение Винера - Хинчина).
4. Определить корреляцию процесса.

Применение спектрального анализа затруднительно в программно–аппаратных комплексах, поскольку метод имеет большую вычислительную сложность, а также избыточность полученных результатов для анализа.



Методы спектрального сингулярного разложения сетевого трафика

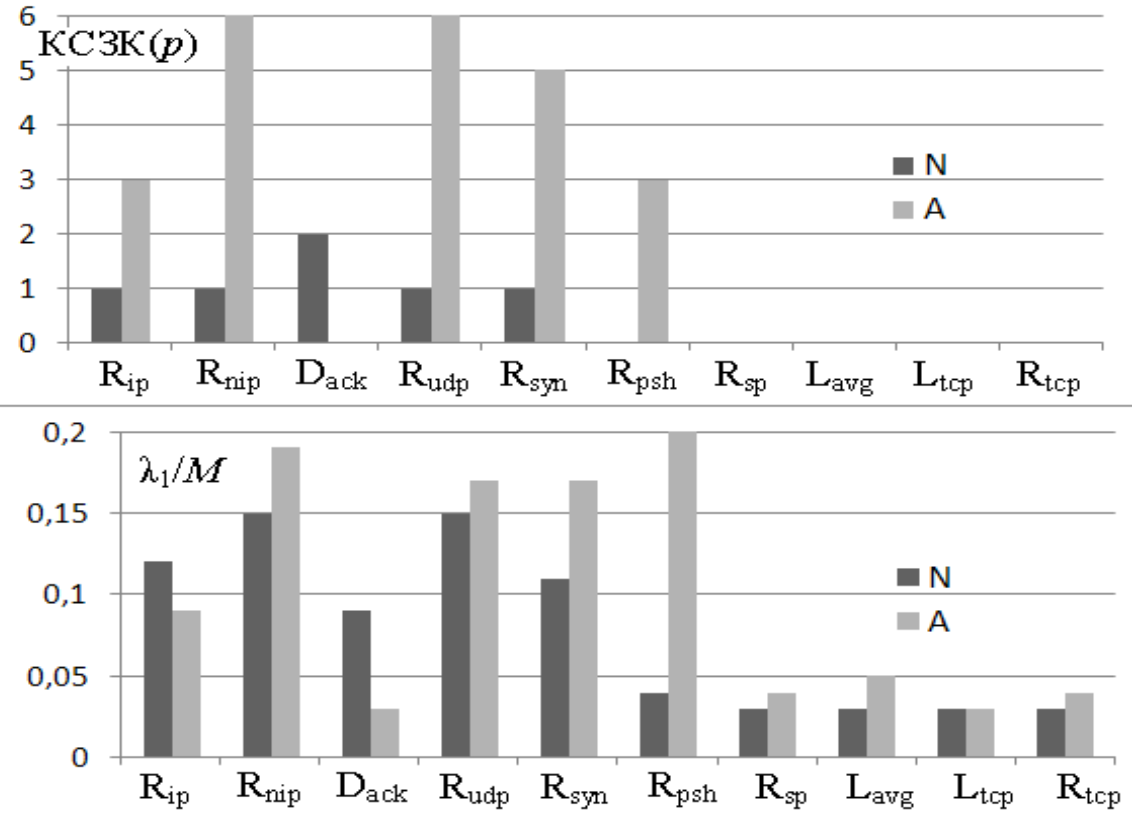
1. Методы спектрального сингулярного разложения позволяют выделить и оценить статистические характеристики сетевого трафика

2.Характеристики сетевого трафика можно разбить на две группы:

1) реагируют на атаку типа HTTP flood

2) реагируют на атаку типа UDP flood

3)все характеристики реагируют на SYN flood

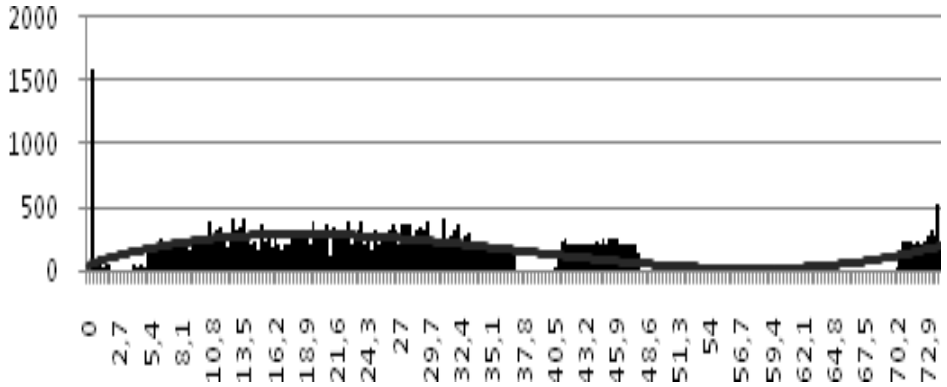


Методы, основанные на фрактальном анализе

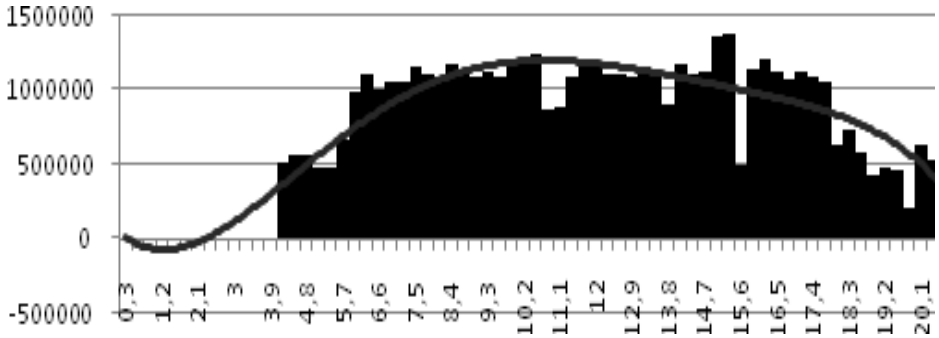
1. Для количественной оценки наличия сетевой аномальности используются R/S статистика, показатель Херста.

2. Диапазон изменений параметра Херста для сетевого трафика находится в интервале (0.5, 1). Для каждого вида атак показатель Херста меняется в зависимости от интенсивности атаки и от вида атаки.

3. Уменьшение автокорреляции, свидетельствует о нарушении стационарности процесса обработки информации.



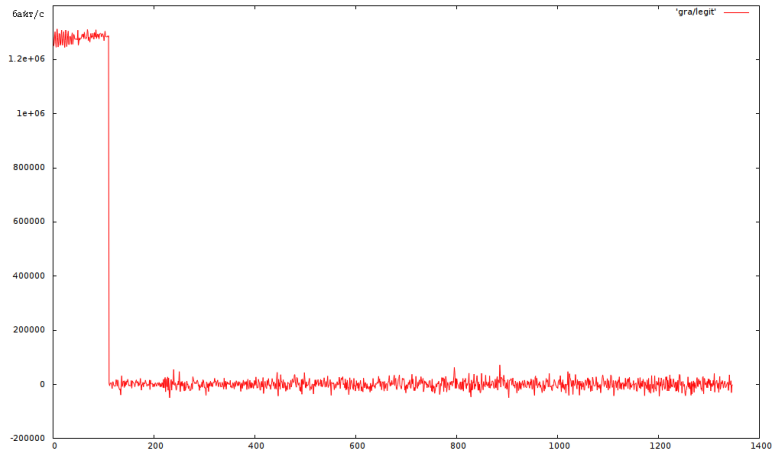
Расчет автокорреляционной функции трафика с атакой SYN flood



Расчет автокорреляционной функции трафика с атакой TCP flood

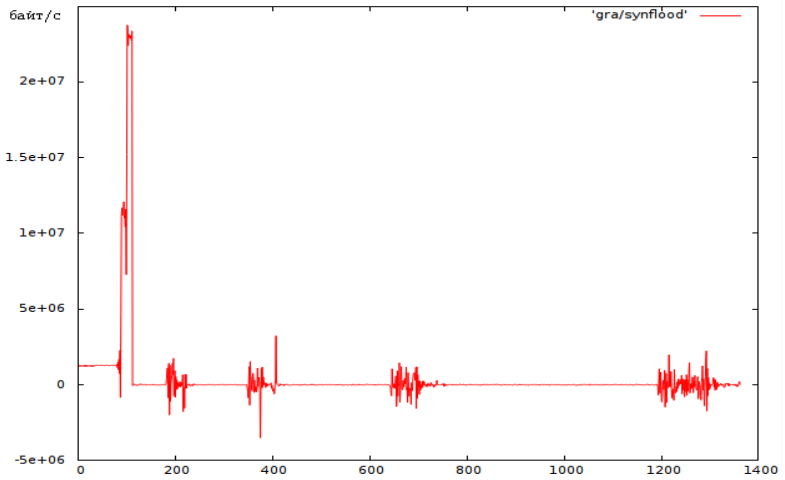
Методы, основанные на Вейвлет анализе

К основным характеристикам вейвлет анализа относя оценку аппроксимирующих и детализирующих коэффициентов, по сравнению которых можно сделать предположения о возможности идентификации аномалии сетевого трафика.



Вейвлет-разложение легитимного сетевого трафика

При атаке наблюдается увеличение отклонения средних значений от средних квадратических детализирующих коэффициентов.



Вейвлет-разложение SYN-флуд атаки

Кластерный анализ

и отображение F множества S на множество C, то есть $F: S \to C$

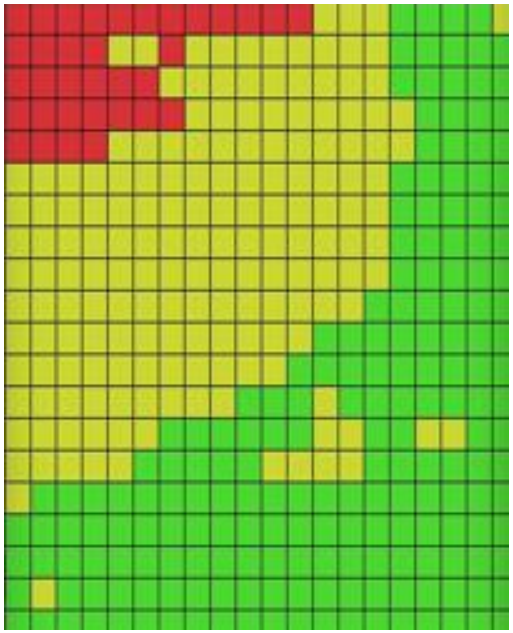
- $C = \{c_1, c_2, \dots, c_k, \dots c_M\}$,

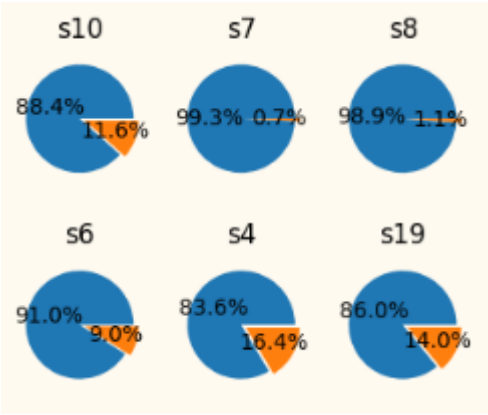
где c_k,— кластер, содержащий схожие по стилю вождения объекты из множества S:

$$c_k = \{s_i, s_j | s_i \in S \; and \; d(s_i, s_j) < h\}$$

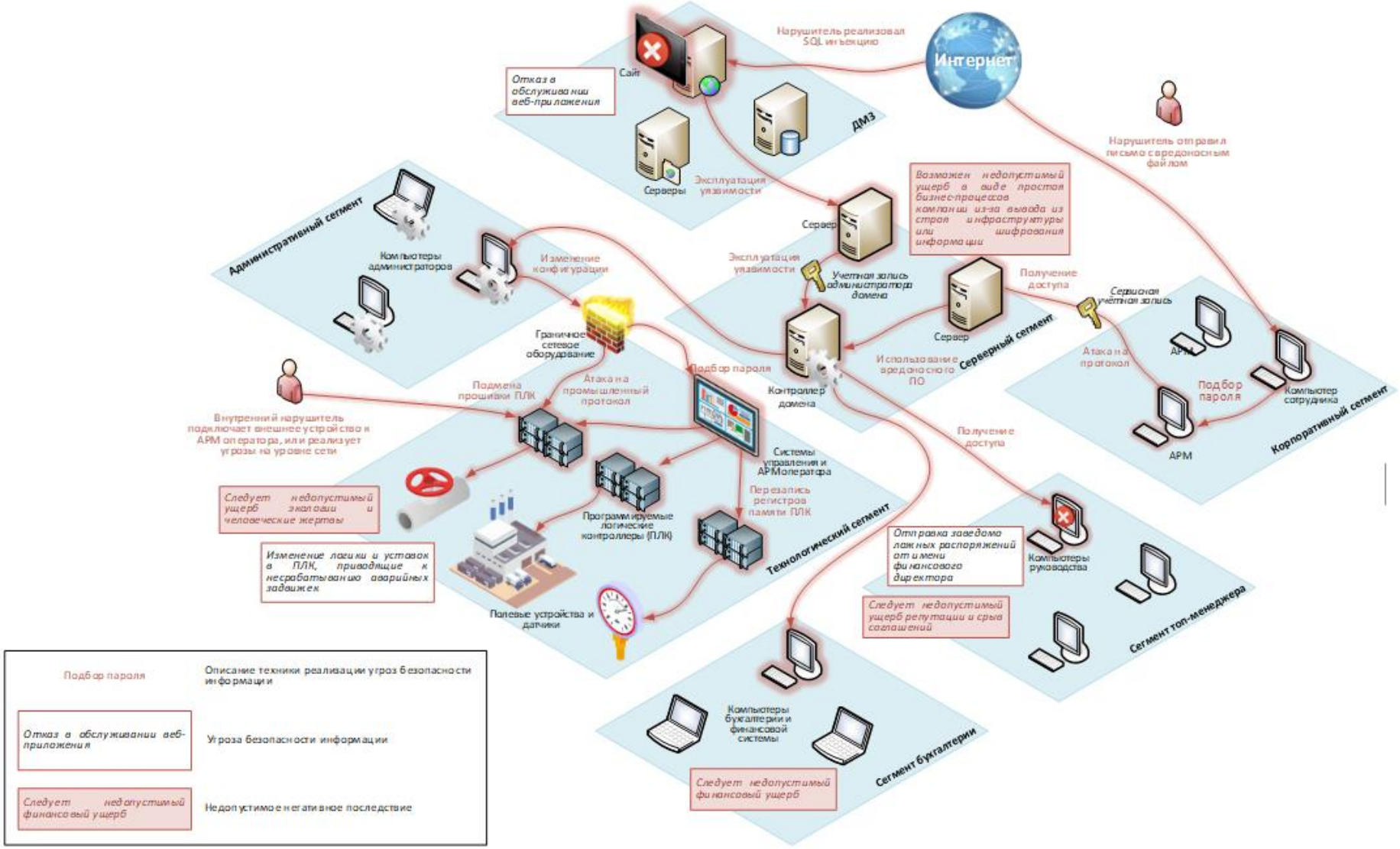
h — величина, определяющая меру близости для включения объектов в один кластер,

d_{ij} — мера близости между объектами,



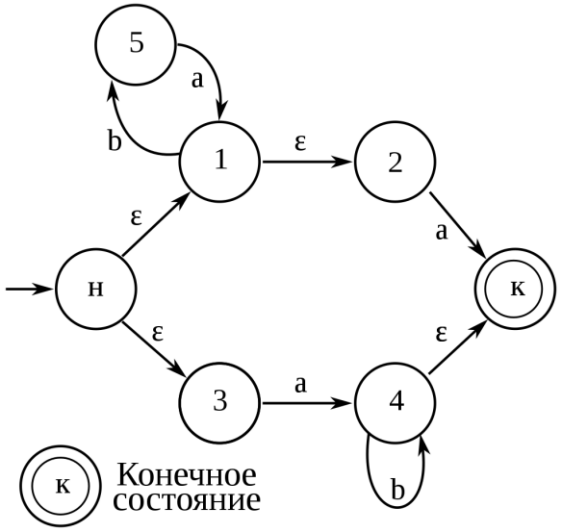


Сигнатурные методы обнаружения

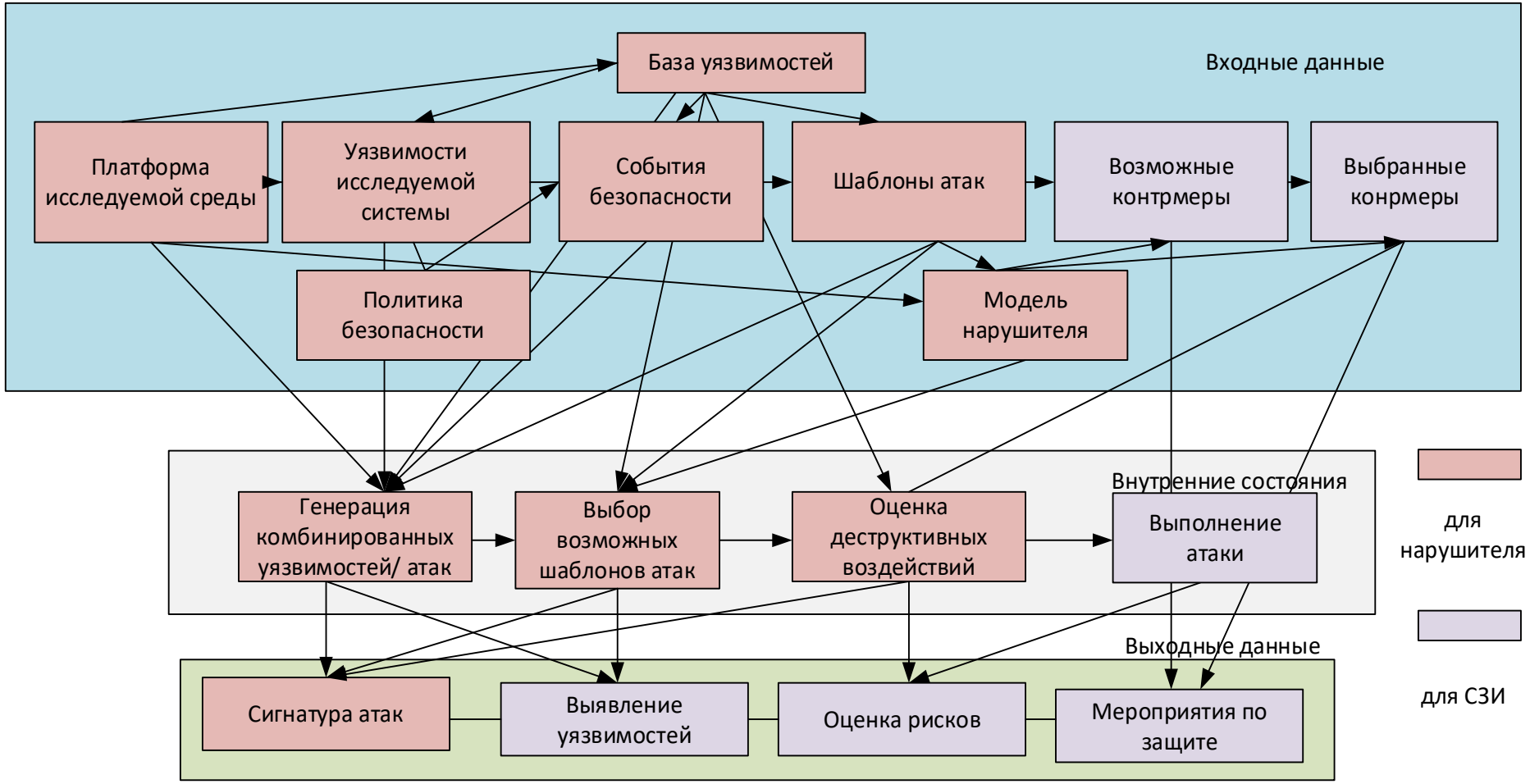


Причины использования аппарата конечных автоматов

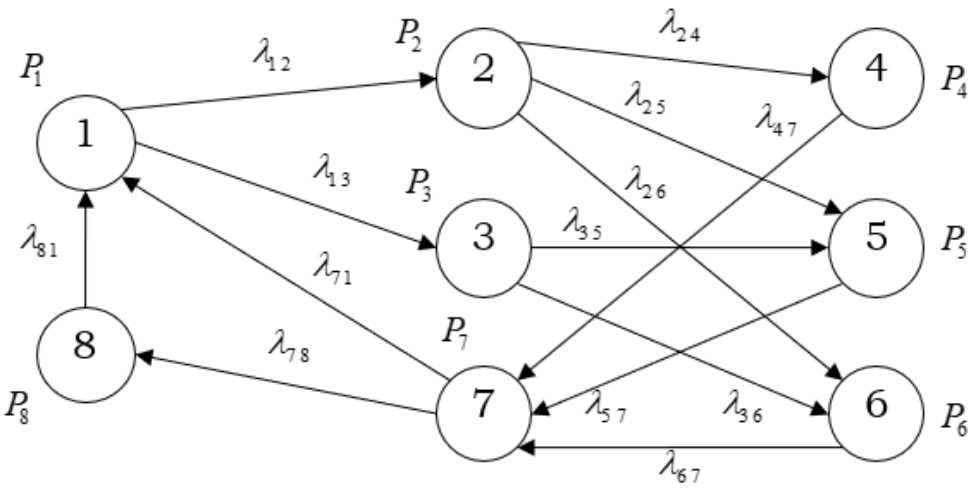
- Вычисление возможный сценариев/трасс атак
- Оценка корреляции последовательности событий
- Определение показателей защищенности
- Оценка рисков
- Определение мероприятий по защите



Конечные автоматы

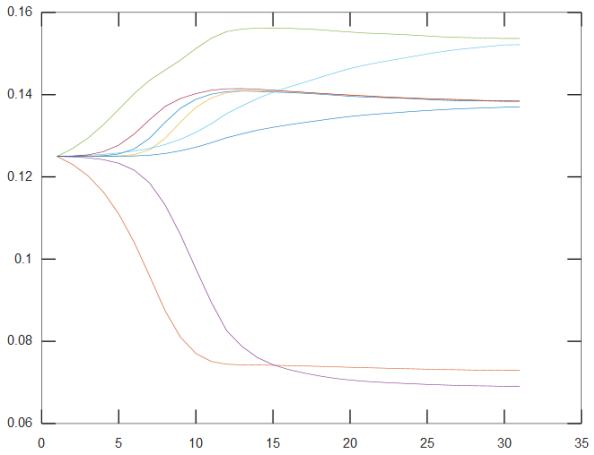


Методы обнаружения злоупотреблений



$$
\begin{cases}
\frac{dP_1}{dt} = \lambda_{71}P_7(t) + \lambda_{81}P_8(t) - \lambda_{12}P_1(t) - \lambda_{13}P_1(t) \\
\frac{dP_2}{dt} = \lambda_{12}P_1(t) - \lambda_{24}P_2(t) - \lambda_{25}P_2(t) - \lambda_{26}P_2(t) \\
\frac{dP_3}{dt} = \lambda_{13}P_1(t) - \lambda_{35}P_3(t) - \lambda_{36}P_3(t) \\
\frac{dP_4}{dt} = \lambda_{24}P_2(t) - \lambda_{47}P_4(t) \\
\frac{dP_5}{dt} = \lambda_{25}P_2(t) + \lambda_{35}P_3(t) - \lambda_{57}P_5(t) \\
\frac{dP_6}{dt} = \lambda_{26}P_2(t) + \lambda_{36}P_3(t) - \lambda_{67}P_6(t) \\
\frac{dP_7}{dt} = \lambda_{47}P_4(t) + \lambda_{57}P_5(t) + \lambda_{67}P_6(t) - \lambda_{71}P_7(t) - \lambda_{78}P_7(t) \\
\frac{dP_8}{dt} = \lambda_{78}P_7(t) - \lambda_{81}P_8(t)
\end{cases}
$$

На граф-схеме обозначены следующие состояния: 1. выбор объекта и портов для атаки; 2. отправка корректных запросов; 3. отправка некорректных запросов; 4. принятие корректных данных; 5. принятие отказа в данных; 6. отсутствие ответа; 7. анализ результатов; 8. коррекция проведения атаки



Экспертные системы

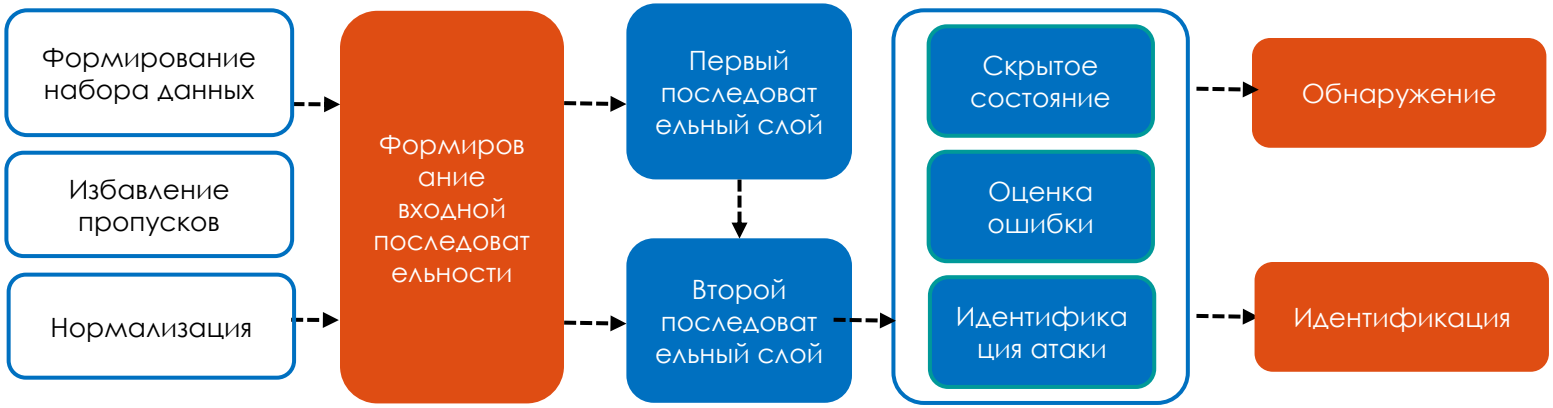
1. **Формирование экспертной группы (в** состав экспертной группы рекомендуется включать экспертов подразделения по защите информации; цифровую трансформацию; сетей связи; АСУ; обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов)).

2. **Проведение экспертной оценки.** Оценку параметров рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы).

Эксперты	Значение оцениваемого параметра (раунд 1)	Значение оцениваемого параметра (раунд 2)
Эксперт 1		
Эксперт 2		
Эксперт n		
Итоговое значение		

Метод распознавания сетевых атак

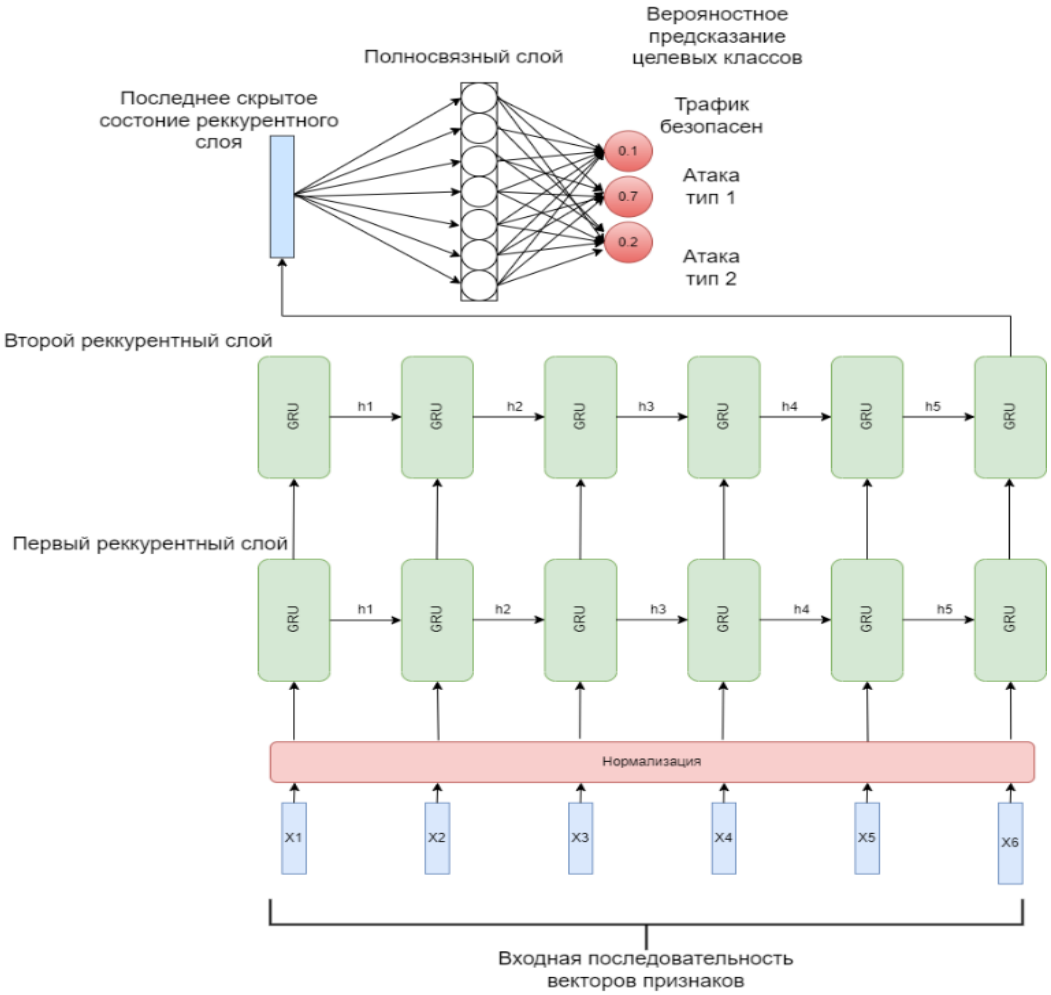
1. Формирование наборов данных, описывающих период сетевой активности для организации обучения нейронной сети и валидации результатов обучения
2. Анализ и извлечение информации из полученного набора данных для установления конечного признакового пространства, характеризующего состояние сетевой активности
3. Подготовка данных для обучения нейронной сети
4. Реализация модели нейронной сети программным способом и проведение процесса обучения
5. Проведение тестирования точности распознавания сетевых атак обученной моделью и интерпретация результата



Подготовка данных

1. Установка конечного признакового пространства
2. Обработка пропущенных значений признаков путем, замены усреднением соседних во времени значений. Удаление записей с многочисленными пропусками
3. Кодирование целевых меток распознаваемых классов в бинарный вид (one-hot представление)
4. Нормализация количественных признаков для сведения значений к единому масштабу. Данный шаг решает проблему экстремальных значений весовых коэффициентов модели
5. Разбиение наборов данных на тренировочное, валидационное и тестовое множество. Тренировочное и валидационное используется для обучения модели, тестовое для подсчета показателей качества работы модели

Модель нейронной сети на рекуррентной архитектуре GRU



$$u_t = \sigma(W_{xu} \cdot x_t + W_{hu} \cdot h_{t-1} + b_u) - update\ gate,$$

$$r = \sigma(W_{xr} \cdot x_t + W_{hr} \cdot h_{t-1} + b_r) - reset\ gate,$$

$$h'_t = tanh\big(W_{xh'} \cdot x_t + W_{hh'} \cdot (r_t \odot h_{t-1})\big),$$

$$h_t = (1 - u_t) \odot h'_t + u_t \odot h_{t-1}$$

Метрики качества распознавания обученной модели

Выбранные метрики качества для оценки модели:

$$Precision = \frac{TP}{TP + FP}$$

Характеризует количество верно классифицированных атак

$$Recall = \frac{TP}{TP + FN}$$

Характеризует количество ложных срабатываний

$$F = \frac{2 \cdot (Precision \cdot Recall)}{Precision + Recall}$$

Усреднение *Precision* и *Recall*

Интерпретация величин:

- TP (True Positive)- Истинно-позитивное срабатывание;
- TN (True Negative) - Истинно-негативное срабатывание;
- FP (False Positive)- Ложно-позитивное срабатывание;
- FN (False Negative) - Ложно-негативное срабатывание;

Практическая реализация

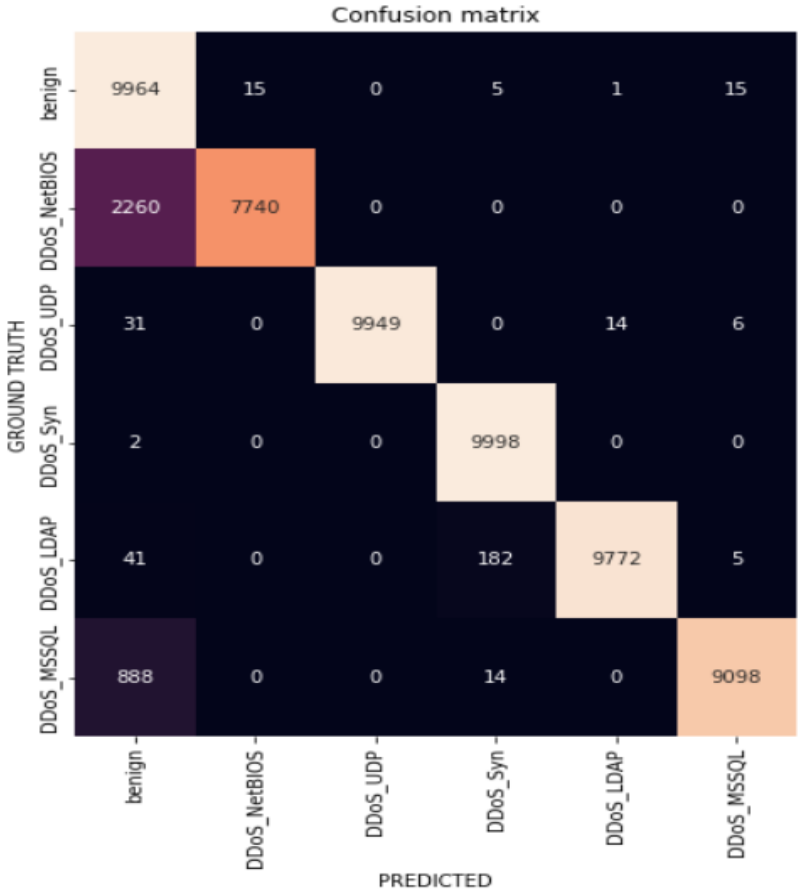
Для исследования были взяты данные Канадского университета Нью-Брунсуика CIC-DDoS-2019 (80 описательных признаков из текущего сетевого трафика).
Типы сетевых атак: DdoS MSSQL; DdoS LDAP; SYN flood; UDP flood; DdoS NetBIOS.
Реализуемая модель 5 иDdoS атаки и нормальная сетевая активность.

Имя вещественного признака	Тип данных признака	Описание
ACK Flag Count	Бинарный	Присутствие ACK сообщений
Average Packet Size	Вещественный	Средний размер пакета в входящем и исходящем трафике
Avg Bwd Segment Size	Вещественный	Средний размер сегмента, на который разделены входящие пакеты для передачи по сети
Avg Fwd Segment Size	Вещественный	Средний размер сегмента, на который разделены исходящие пакеты для передачи по сети
Bwd IAT Min	Целочисленный	Минимальное время, которое приходит после получения пакета до прибытия следующего, мс
Down/Up Ratio	Вещественный	Отношение входящего трафика к исходящему

Практическая реализация

	precision	recall	f1-score	support
benign	0.76	1.00	0.86	10000
DDoS_NetBIOS	1.00	0.77	0.87	10000
DDoS_UDP	1.00	0.99	1.00	10000
DDoS_Syn	0.98	1.00	0.99	10000
DDoS_LDAP	1.00	0.98	0.99	10000
DDoS_MSSQL	1.00	0.91	0.95	10000

- 4 из 5 выбранных атак распознаются на тестовой выборке с точностью более 90% (F1-мера);
- DDoS NetBIOS в 22,6 % принимается за безопасный трафик;
- 0.2% ложноположительных срабатываний



Матрица ошибок модели

Методы прогнозирования сетевого трафика

Ситуация 1.1 Модель ARMA применяется при стационарности ряда и отсутствии нештатных ситуаций

$$X_t = c + \sum_{i=1}^{p} a_i X_{t-i} + \sum_{i=1}^{q} b_i \varepsilon_{t-i} + \varepsilon_t$$

Ситуация 1.2 Аддитивная модель Хольта-Винтерса характеризуется при постоянстве сезонного профиля и применяется при штатной работе сети

$$\begin{cases} L_t = \alpha(Y_t - S_{t-s}) + (1-\alpha)(L_{t-1} + T_{t-1}) \\ T_t = \beta(L_t - L_{t-1}) + (1-\beta)T_{t-1} \\ S_t = \gamma(Y_t L_t) + (1-\gamma)S_{t-s} \\ \hat{Y}_{t+p} = L_t + pT_t + S_{t-s+(p \bmod s)} \end{cases},$$

$$\Delta^d X_t = c + \varepsilon_t + \sum_{i=1}^{p} \alpha_i \Delta^d X_{t-1} + \sum_{i=1}^{q} \beta_i \varepsilon_{t-i}$$

Ситуация 2 Первая мультипликативная модель Хольта-Винтерса применяется, если параметры прогнозирования стабильны на малых горизонтах прогноза:

$$\begin{cases} L_t = \dfrac{\alpha Y_t}{S_{t-s}} + (1-\alpha)(L_{t-1} + T_{t-1}) \\ T_t = \beta(L_t - L_{t-1}) + (1-\beta)T_{t-1} \\ S_t = \dfrac{\gamma Y_t}{L_t} + (1-\gamma)S_{t-s} \\ \hat{Y}_{t+p} = (L_t + pT_t)S_{t-s+(p \bmod s)} \end{cases}$$

t – последний известный момент времени, от которого строится прогноз; p – интервал времени, на который строится прогноз; $1 \le p \le h$, где h – горизонт прогнозирования; $\hat{Y}_{t+p}$ – значение прогноза в момент времени t; L_t – уровень; T_t – тренд; S_t – периодическая компонента; s – величина периода.

Ситуация 3: Модель Тейла-Вейджа используется при необходимости осуществить краткосрочное прогнозирование для быстрой реакции на атаку:

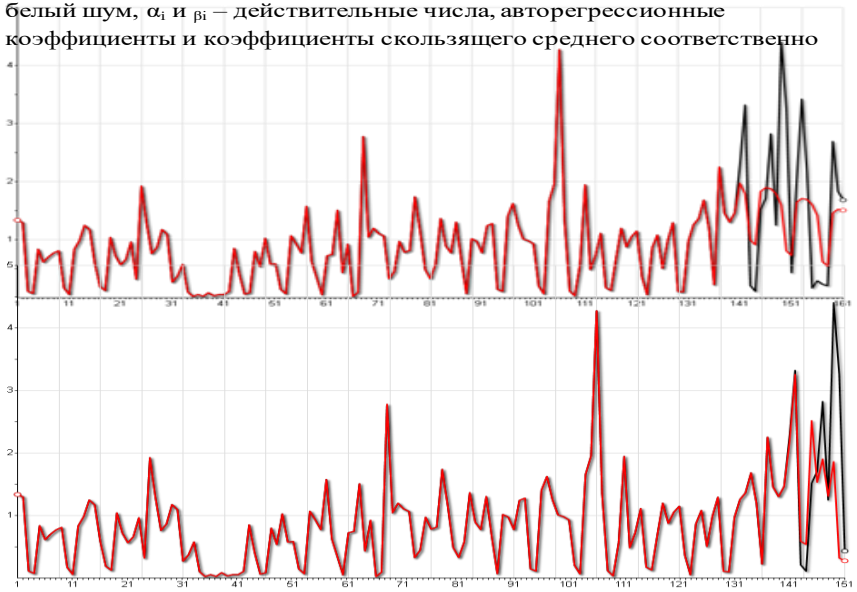
$$\begin{cases} L_t = \alpha(Y_t - S_{t-s}) + (1-\alpha)(L_{t-1} + T_{t-1}) \\ T_t = \beta(L_t - L_{t-1}) + (1-\beta)T_{t-1} \\ S_t = \gamma(Y_t - L_t) + (1-\gamma)S_{t-s} \\ \hat{Y}_{t+p} = L_t + pT_t S_{t-s+(p \bmod s)} \end{cases}$$

Ситуация 4. Модель ARIMA(p, q) используется, при необходимо достич заданной точности прогноза:

$$\Delta^d X_t = c + \sum_{i=1}^{p} a_i \Delta^d X_{t-i} + \sum_{i=1}^{q} b_i \varepsilon_{t-i} + \varepsilon_t$$

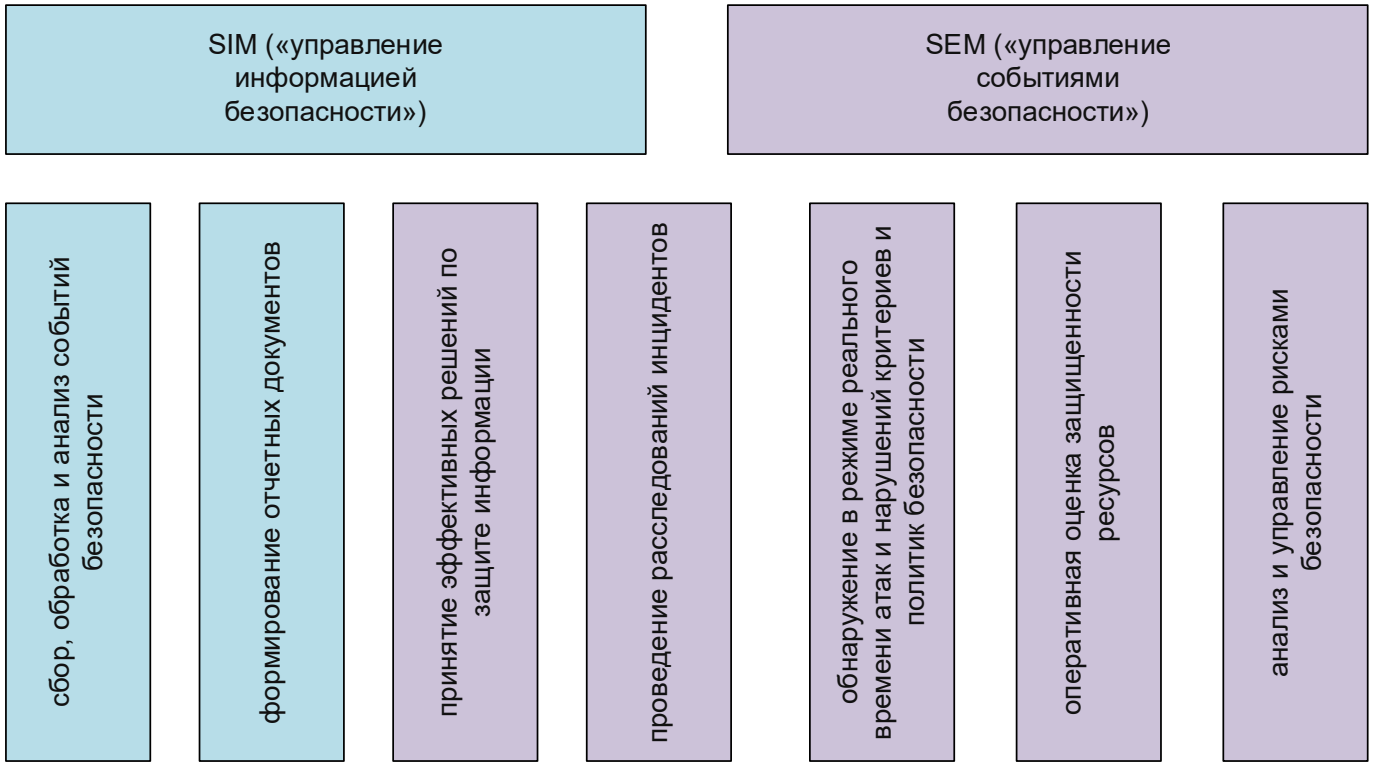
$$\Delta X_t = X_{t+1} - X_t$$
$$\Delta^d X_t = \Delta^{d-1} X_{t+1} - \Delta^{d-1} X_t ,$$

где p и q— целые числа, задающие порядок модели c – константа, ε_t – белый шум, α_i и β_i – действительные числа, авторегрессионные коэффициенты и коэффициенты скользящего среднего соответственно



SIEM

Security information and event management (сокращенно SIEM) - это программное средство, осуществляющее анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.



Отличия SIEM от IDS

IDS

Задачи СОВ:
- обнаружение вторжений (атак)

Основные методы работы СОВ:
- сбор и анализ сетевого трафика
- преимущественно сигнатурный подход для
- обнаружения вторжений

Основные принципы работы СОВ:
- ограниченное использование внешних источников событий
- горизонтальная модель событий
- отсутствует анализ топологии, и сопоставление её модели с внешними требованиями

SIEM

Задачи SIEM:
- контроль выполнения АС требований нормативных документов и регламентов
- оперативное обнаружение и мониторинг инцидентов

Основные методы работы SIEM:
- сбор, нормализация и анализ событий
- сопоставление информации о топологии АС и конфигурации её компонентов с требованиями регламентов

Основные принципы работы SIEM:
- широкое использование внешних источников информации (методы как пассивного, так и
- активного анализа)
- древовидная модель событий, корреляция новых высокоуровневых событий на основе правил из более простых событий
- обработка данных за большие периоды времени

Преимущества

Предоставляет
Высокоуровневую информацию о событии и общем состоянии защищенности АС

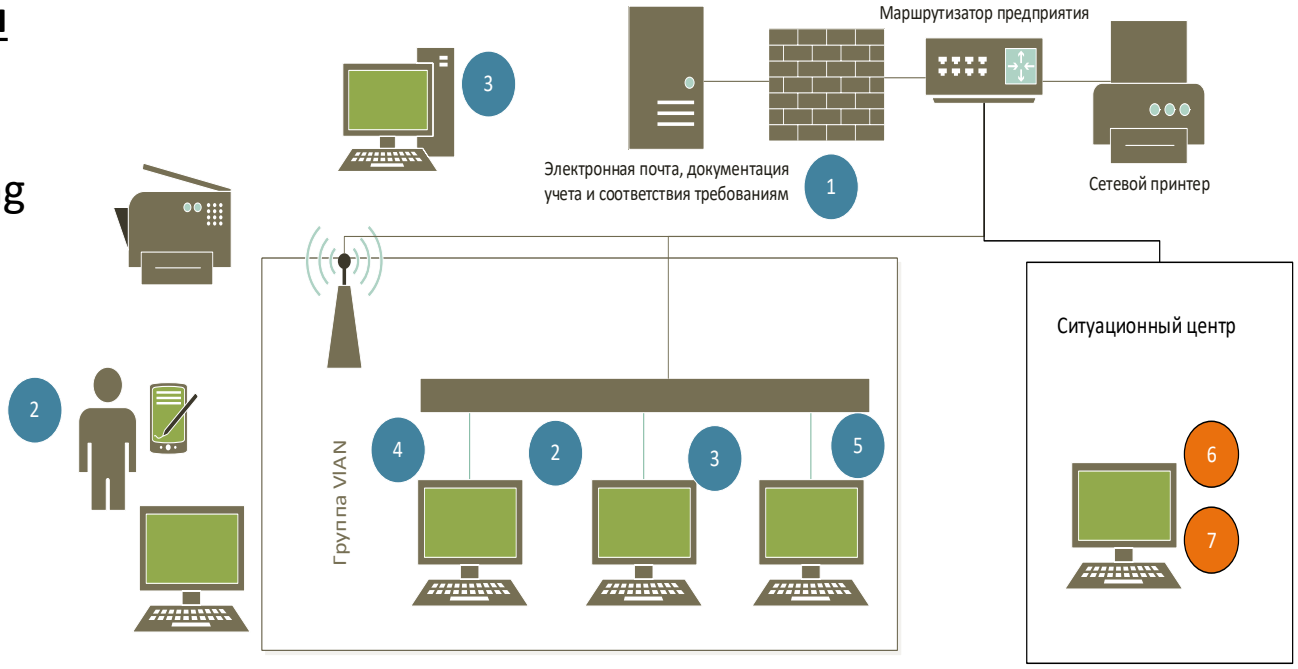
Выявляет инциденты на
основе корреляции данных из нескольких источников (интеграция СЗИ разных производителей)

Оценка соответствия АС
- требованиям стандартов и регламентов

Архитектура SIEM

Основные протоколы сбора информации:

- Syslog and Syslog-ng
- SNMPv2 and SNMPv3
- Opsec
- HTTP, HTTPS
- SQL, ODBC
- WMI, WBEM (CIM)
- FTP
- SSH
- Rsync
- Samba
- OPSEC, CPMI



1 Сенсоры на межсетевых экранах
2 Сенсоры на антивирусном ПО
3 Системы мониторинга сети (IDS/IPS)
4 Сенсоры DLP
5 Сенсоры крипошлюза
Сетевое оборудование
АРМ
Серверы
6 Консоль управления
7 Сетевое оборудование

SNMP

SNMP (Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

Задачи:

- Управление конфигурацией (Configuration Management)
- Обработка ошибок (Fault Management)
- Анализ производительности и надёжности (Performance management)
- Управление безопасностью (Security Management)
- Учёт работы (Accounting Management)

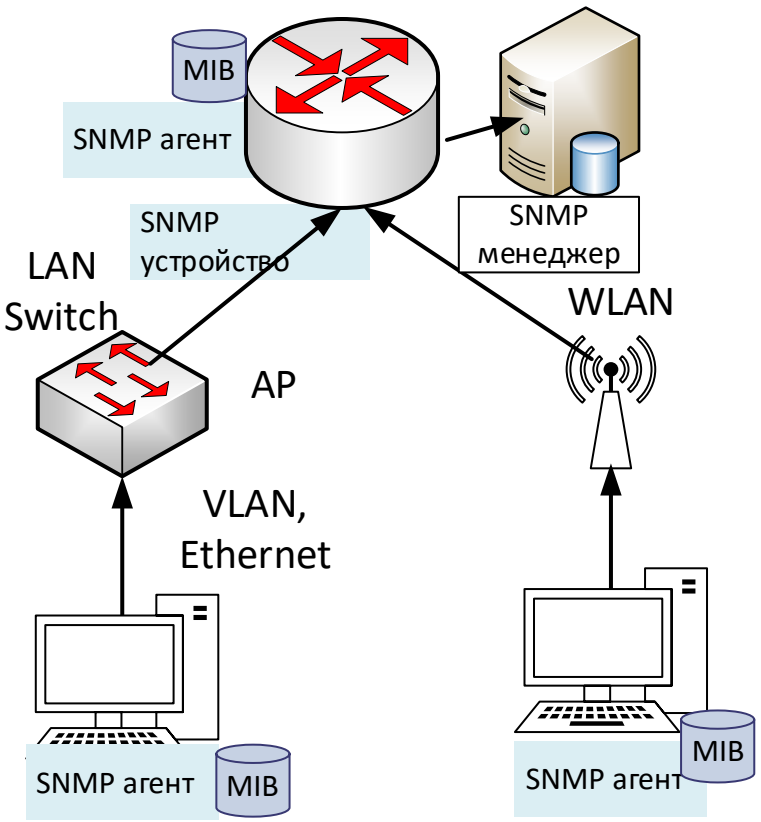
Архитектура SNMP

Управляемое устройство — элемент сети который разрешает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе.

Агент- программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства. Агент обслуживает базу управляющей информации и отвечает на запросы менеджера SNMP.

Менеджер — это программное обеспечение, установленное на рабочей станции управления, наблюдающее за сетевыми устройствами и управляющее ими. В любой управляемой сети может быть один и более менеджеров.

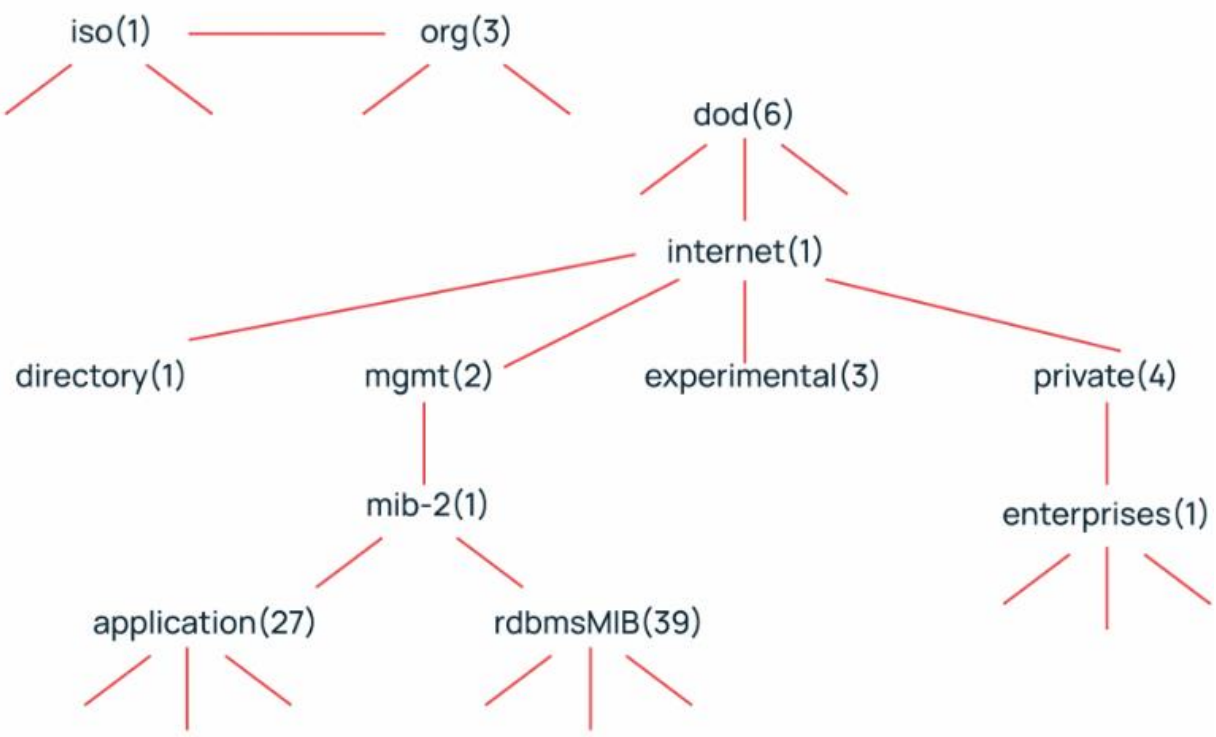
База управляющей информации — это совокупность иерархически организованной информации, доступ к которой осуществляется посредством протокола управления сетью.



База управляющей информации SNMP

Базы управляющей информации описывают структуру управляющей информации устройств и состоят из управляемых объектов (переменных).

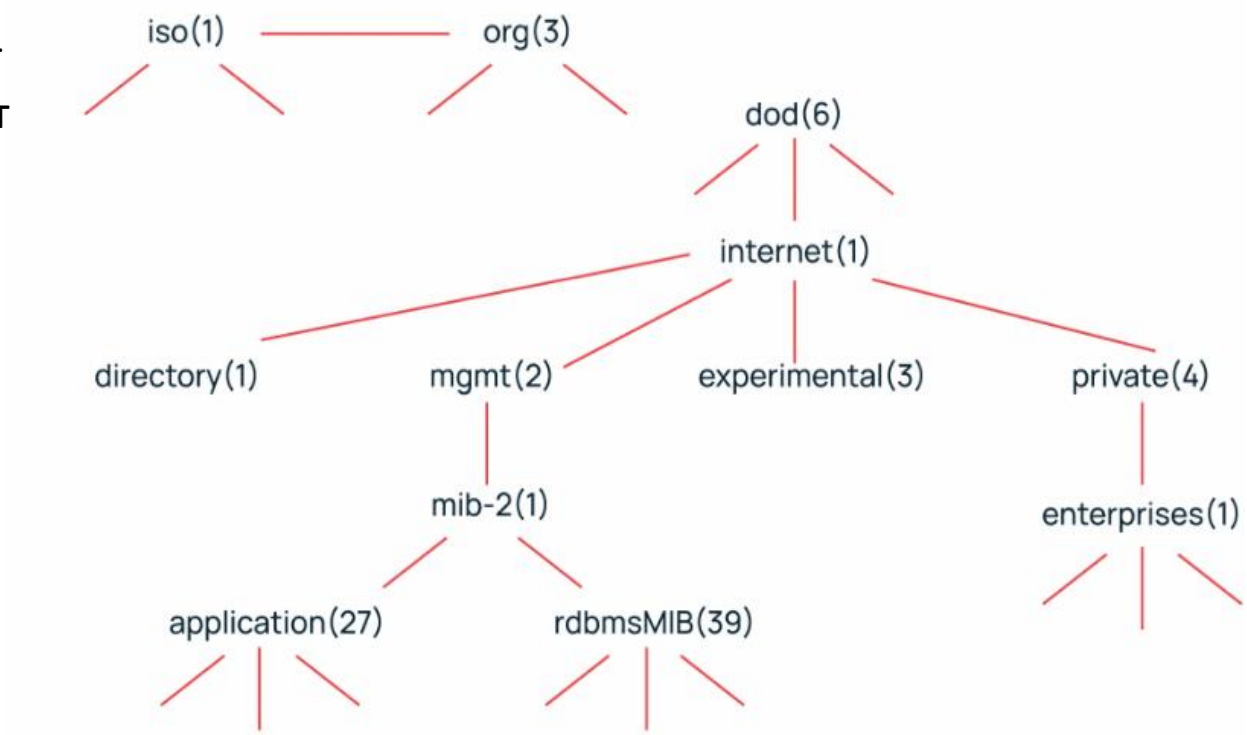
Идентификаторы ID верхних уровней отданы организациям, контролирующим стандартизацию, а идентификаторы нижних уровней определяются самими организациями.



Каждая ветвь дерева OID нумеруется целыми числами слева направо, начиная с единицы разделенных точкой, записанных слева направо и включает полный путь от корня до управляемого объекта.

База управляющей информации SNMP

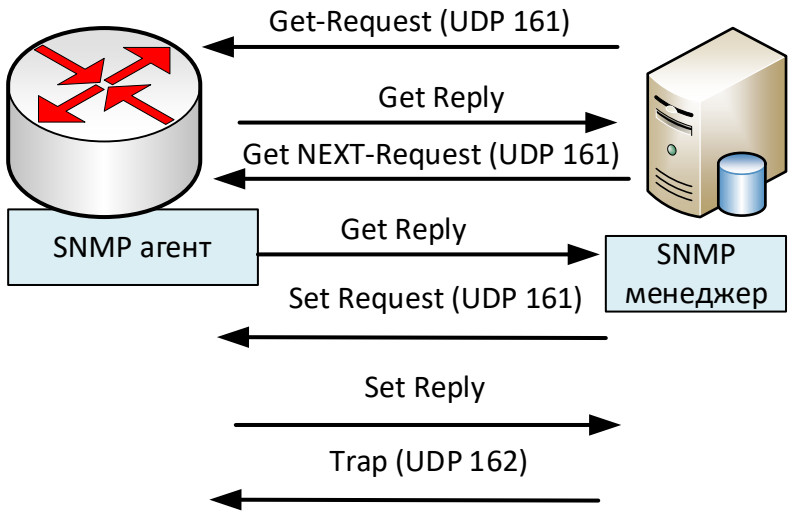
Обращение к управляемым объектам MIB происходит посредством идентификаторов объекта (Object IDentifier, OID) по уникальному идентификатору в пространстве имен OID, отвечающих за определенную ветку дерева OID и контролируемой агентством IANA. (1.3.6.1.2.1.1-эквивалентное имя: iso.org.dod.internet.mgmt.mib-2.system).



Архитектура SNMP

Протокол SNMP предусматривает передачу между менеджером и агентом по UDP.

- Get-Request — запрос значений одного или нескольких объектов
- Get-Next-Request — Запрос от менеджера к объекту для обнаружения доступных переменных и их значений.
- Set-Request — запрос на изменение значения одного или нескольких объектов
- Get(Set)-Reply — получение ответа от агента
- Trap (ловушка) используется для асинхронного сообщения о событии, происходящем на управляемом сетевом устройстве.
- GetBulk- позволяет менеджеру получить несколько переменных за один запрос.



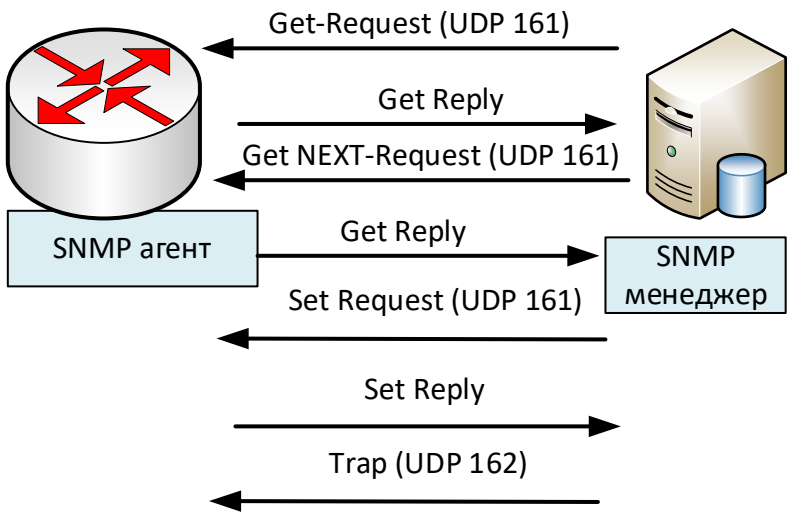
Архитектура SNMP

Типичные запросы

- входящий/исходящий трафик на интерфейсе, ошибки
- загрузка процессора
- время работы
- температура и другие OIDы, поддерживаемые производителем оборудования

Для хостов

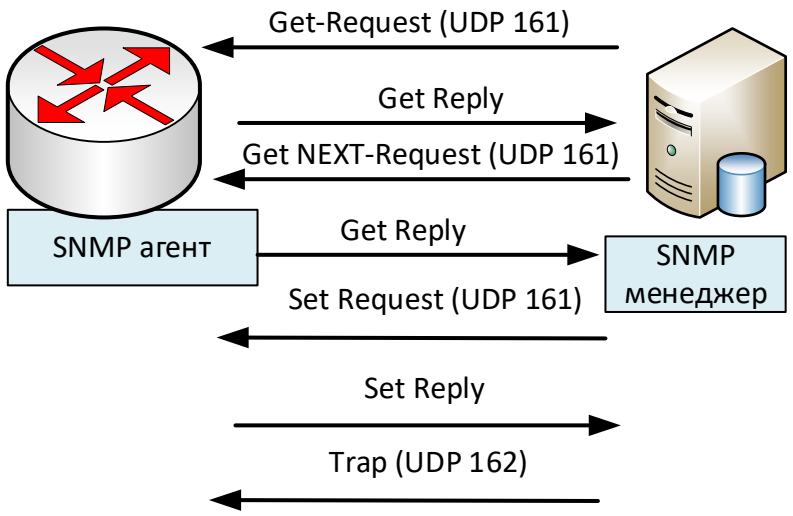
- свободное место на диске
- установленное программное обеспечение
- список активных процессов



Архитектура SNMP

В SNMP есть два типа ловушек: Trap и Inform. Отличия между ними в том, что после получения Inform менеджер подтверждает получение ловушки.

0 — **coldStart** — холодный запуск устройства
1 — **warmStart** — горячий запуск устройства
2 — **linkDown** — отключение интерфейса
3 — **linkUp** — включение интерфейса
4 — **authenticationFailure** —сообщение с неверной строкой сообщества
5 — **egpNeighborLoss** — потрея связи по EGP
6 — **entrpriseSpecific** —событие, характерное для производителя данного устройства.



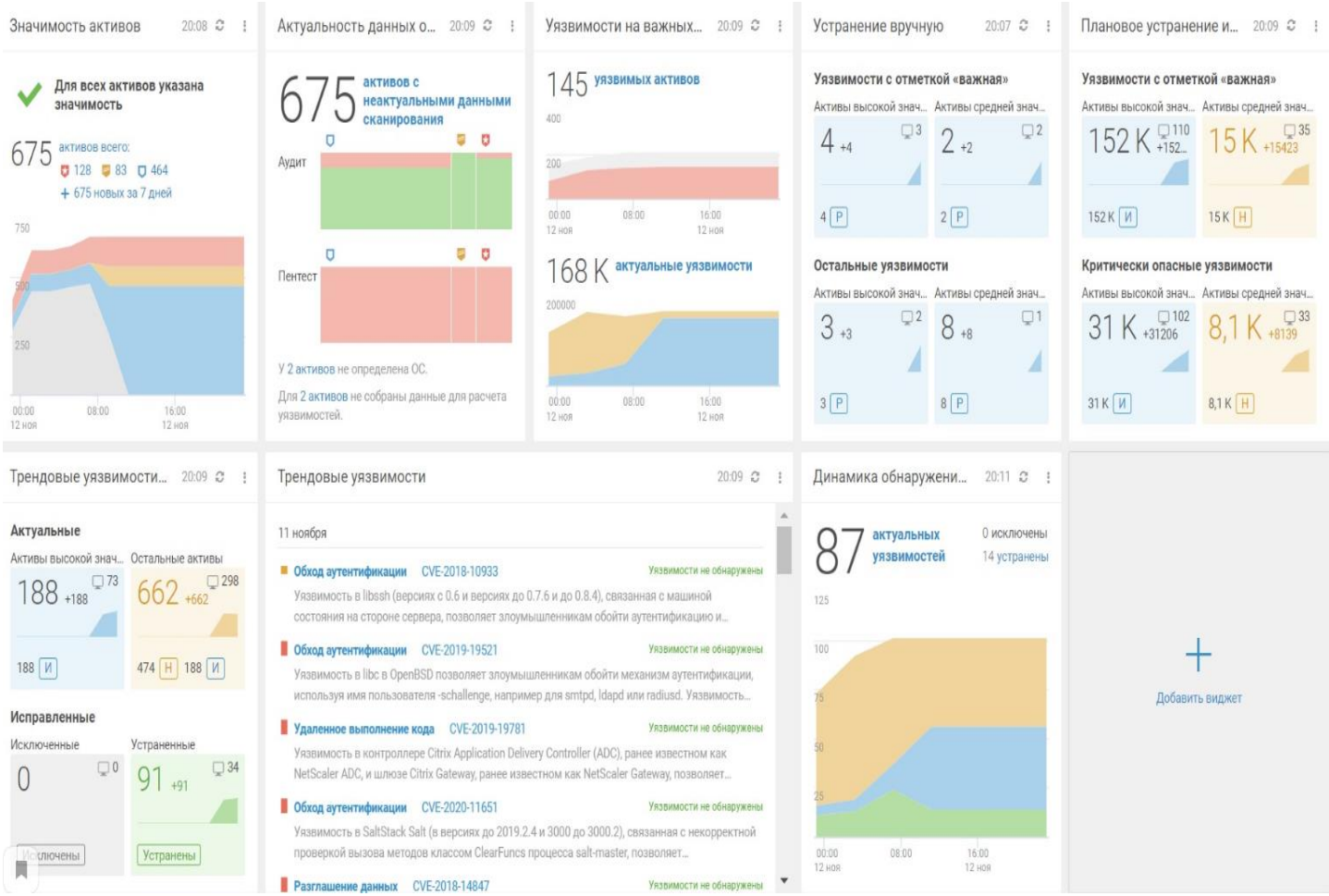
Безопасность SNMPv3

В стандарте определены сущности-агенты и сущности-менеджеры, которое выполняют четыре основные функции:

- диспетчеризация (система управления входящим и исходящим трафиком)
- обработка сообщений
- функция безопасности (аутентификация, шифрование, контроль целостности)
- функция контроль доступа (управляет службами аутентификации для контроля доступа к MIB)

Визуализация

- Автоматический анализ
- Мониторинг доступности активов и наличия ресурсов
- Оперативный контроль
- Поисковые возможности
- Анализ рисков
- Анализ и оценка соответствия требованиям



Программно-конфигурируемые сети

Программно-конфигурируемые сети (Software Defined Networking/SDN) – это разделение *контура передачи данных* и *контура управления данными*, позволяющее осуществлять программное управление контуром передачи данных, которое может быть физически или логически отделено от аппаратных коммутаторов и маршрутизаторов.

Задачи:

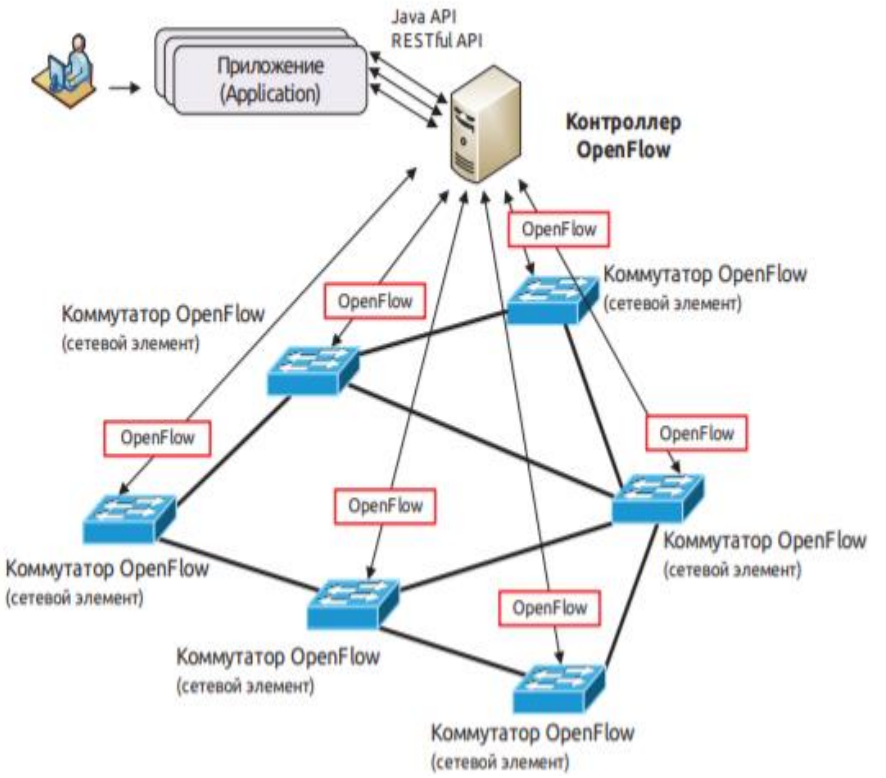
1.Физически разделить контур управления сетевым оборудованием от контура управления передачей данных.
2. Перейти от управления отдельными экземплярами сетевого оборудования к управлению сетью в целом – логически централизованное управление.
3. Создать открытый программно-управляемый интерфейс между сетевыми приложениями и транспортной сетью.

Архитектура программно-конфигурируемые сети

Инфраструктурный уровень, на котором функционируют сетевые коммутаторы и каналы передачи данных

Уровень управления — набор программных средств, физически отделённых от инфраструктурного уровня, обеспечивающий реализацию механизмов управления устройствами инфраструктурного уровня

Уровень сетевых приложений — набор SDN-приложений, взаимодействующих с SDN-контроллером через программный протокол (API) для сбора, анализа, развёртывания и управления сетевой инфраструктурой на уровне приложений.



Программно-конфигурируемые сети

Базовые подходы:
Open SDN реализуется на базе протокола OpenFlow, в которой предусмотрено полное удаление плоскости контроля
SDN via API- сохранении плоскости контроля на сетевых элементах.
SDN via Overlay- поверх физической сети строятся виртуальные каналы типа «точка-точка»

Нормативно-правовое обеспечение

Приказ ФСБ РФ от 6 мая 2019 года N 196. Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Приказ ФСТЭК России от 11 февраля 2013 г. N 17

ФСТЭК. Информационное письмо «Об утверждении требований к системам обнаружения вторжений»