УДК 004.056.5

Ю.С. Корякина, jk169@list.ru
Институт машиноведения автоматики и геомеханики НАН КР
М.Э. Эсенбекова, meerimaesenbekova@gmail.com
Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР ПОДХОДОВ РЕАЛИЗАЦИИ ПОДСИСТЕМ ЗАЩИТЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В СОСТАВЕ SOC

Современные корпоративные сети сталкиваются с растущими угрозами кибератак, что требует применения передовых технологий защиты. В данной работе проведен аналитический обзор методов реализации подсистем обнаружения и предотвращения вторжений (IDS/IPS) в составе центров мониторинга безопасности (SOC). Рассмотрены теоретические аспекты работы сетевых и хостовых решений (NIDS, HIDS, NIPS, HIPS), а также методы анализа поведения сети (NBA). Проанализированы современные подходы к интеграции технологий Suricata, Zeek и Security Onion, их функциональные возможности, принципы работы и сравнительная эффективность. Особое внимание уделено вопросам корреляции событий, минимизации ложных срабатываний, взаимодействия с SIEM-системами и автоматизации реагирования на инциденты. В работе рассмотрены преимущества и недостатки различных технологий, а также предложена схема комплексного подхода к обеспечению безопасности корпоративных сетей. В заключение сформулированы рекомендации по выбору оптимальных решений для построения устойчивой системы защиты, способной эффективно противодействовать современным угрозам.

Ключевые слова: SOC, IDS, IPS, информационная безопасность, NIDS, HIDS, NIPS, HIPS, NBA, корреляция событий, сигнатурный анализ, поведенческий анализ, автоматическое предотвращение атак, SIEM, SOAR.

Введение

В условиях стремительной цифровой трансформации и роста угроз ИБ актуальность разработки современных методов реализации подсистем защиты обнаружения и предотвращения вторжений для центров мониторинга безопасности (SOC) приобретает особое значение. Современные организации сталкиваются с динамично меняющейся средой, где злоумышленники постоянно совершенствуют свои методики, используя автоматизированные инструменты и эксплуатируя уязвимости в критически важных программных решениях. Объектом исследования являются методы и технологии обеспечения безопасности корпоративных сетей в рамках SOC. Предметом исследования являются методы обнаружения и предотвращения сетевых атак с использованием систем IDS/IPS в составе SOC. В работе особое внимание уделяется разработке и интеграции подсистемы IDS/IPS, анализу методов детектирования угроз ИБ, а также механизму автоматического предотвращения атак. Рассматриваются вопросы корреляции событий, минимизации ложных срабатываний, взаимодействия IDS/IPS с SIEM-системами и влияние предложенного решения на эффективность защиты.

По данным Лаборатории Касперского, в первом полугодии 2024 года зафиксирован кратный рост атак на сферы телекоммуникаций и строительства, что свидетельствует о том, что ключевые отрасли инфраструктуры становятся приоритетными целями для киберпреступников. Такой рост атак отражает не только увеличение количества инцидентов, но и их возрастающую сложность, поскольку злоумышленники применяют новые методы обхода традиционных систем защиты. [1]

Отчет ICS CERT за второй квартал 2024 года демонстрирует, что в промышленном секторе происходят регулярные инциденты, направленные на вывод из строя производственных систем или кражу технологической информации, что может привести к

значительным экономическим потерям и подрыву доверия к инфраструктурной безопасности предприятий. [2]

Особенно тревожной является информация о том, что каждая четвертая компания в мире столкнулась с APT-угрозами в 2024 году. APT-атаки, отличающиеся многоступенчатостью и длительностью, представляют особую сложность для традиционных систем защиты, так как требуют комплексного анализа и корреляции данных. Атаки такого типа направлены на кражу конфиденциальной информации, включая персональные данные, коммерческие тайны и финансовые сведения, что подрывает не только репутацию, но и конкурентоспособность организаций. Наряду с этим возрастает число DDoS-атак, направленных на перегрузку сетевых ресурсов, что приводит к временному нарушению работы сервисов и снижению доступности корпоративных систем. Такие атаки существенно влияют на оперативную деятельность организаций и требуют эффективного обнаружения и реагирования в режиме реального времени. [3]

По данным глобальной сети центров очистки трафика, всего системы StormWall в 2024 году предотвратили 6,6 млн DDoS-атак по всему миру. Средняя продолжительность атаки составила 23 минуты. Количество инцидентов с продолжительностью больше 1 часа увеличилось на 120%. При этом средняя мощность атак выросла на 53%. Самая мощная DDoS-атака, предотвращенная StormWall в 2024 году, достигала 1,6 Тбит/с. Из всего количества DDoS-атак, предотвращенных StormWall, 59% были направлены на прикладной уровень модели OSI, а точнее — на протокол HTTP. [4] На рисунке 1 представлена статистика DDoS-атак StormWall.

Квартал	Количество предотвращённых DDoS-атак	Рост за квартал
1 кв. 2024	1,2 млн	-
2 кв. 2024	1,4 млн	16,7 %
3 кв. 2024	1,7 млн	21,4 %
4 кв. 2024	2,3 млн	35,3 %

Рисунок 1 — Статистика DDoS-атак StormWall

Считается, что традиционные решения IPS/IDS, развернутые на различных платформах, обладают рядом недостатков, существенно влияющих на их эффективность, а именно:

1. Большое количество аппаратных ресурсов.
2. Большое количество программных ресурсов.
3. Существенных финансовых затрат.
4. Отсутствие одного интерфейса, что приводит к фрагментации процессов мониторинга и анализа угроз, что усложняет оперативное реагирование на инциденты.
5. Ограничения в функциональных возможностях.
6. Не имеют автономности и зависят от других компонентов SOC, а именно от SIEM и SOAR систем.

Поэтому для обеспечения надежной защиты корпоративных сетей необходим комплексный подход, объединяющий возможности различных систем мониторинга и анализа угроз в единую интегрированную платформу.

Основа IPS/IDS, принцип работы

IDS (Intrusion Detection System) — это система обнаружения вторжений, а IPS (Intrusion Prevention System) — система предотвращения вторжений. Они настолько близки и похожи, что обычно упоминаются в связке друг с другом. Кроме того, ранее IDS было отдельным инструментом, но позднее вошло в состав IPS. Если сравнивать их с традиционными решениями информационной безопасности, то IDS/IPS способны добиться более высокого уровня сетевой защиты. [5] IDS представляет собой пассивную систему, которая сканирует трафик и сообщает об угрозах. IDS никоим образом не изменяет сетевые пакеты, тогда как IPS предотвращает доставку пакета в зависимости от содержимого пакета, подобно тому, как межсетевой экран предотвращает трафик по IP-адресу. IPS – это средство безопасности для предотвращения сетевых угроз. Система исследует сетевой трафик, потоки для предотвращения эксплойтов, злонамеренных действий с целевым приложением или службой. Все для того, чтобы злоумышленники не смогли прервать работу компании и получить контроль над приложением или конечной точкой.[6]

IDS функционируют в режиме мониторинга и анализа сетевого трафика или активности хостов. Они сравнивают поступающие данные с известными шаблонами атак (сигнатурами) или выявляют аномальное поведение, после чего уведомляют администраторов о подозрительной активности. Однако IDS не могут блокировать атаки самостоятельно. IPS работают аналогично IDS, но с ключевым отличием – они не только обнаруживают угрозы, но и принимают активные меры по их блокировке. IPS могут автоматически фильтровать вредоносный трафик, разрывать соединения и предотвращать выполнение вредоносного кода, действуя в режиме реального времени.

Принцип работы IPS/IDS можно описать следующим образом:

1. Мониторинг трафика: Система получает копии сетевых пакетов или анализирует журналы событий, чтобы отслеживать деятельность в сети или на хостах.
2. Анализ данных:
   - Сигнатурный анализ: сравнивает данные с базой известных шаблонов атак (например, SQL-инъекций, DDoS-атак).
   - Анализ аномалий: оценивает, соответствует ли поведение сети или хоста нормальным параметрам. Аномалии могут быть вызваны необычными пиками трафика или подозрительными действиями.
3. Обнаружение угроз: если найдена угроза, IDS создает уведомление (алерт), а IPS немедленно принимает меры.
4. Реакция на угрозу:
   - Для IDS: Система записывает событие и уведомляет администратора.
   - Для IPS: Система автоматически блокирует вредоносный трафик или действия (например, завершает соединение или запрещает доступ к ресурсу).

IPS/IDS часто интегрируются в межсетевые экраны (firewalls) и работают на уровне сетевого трафика или хостов для обеспечения максимальной безопасности.

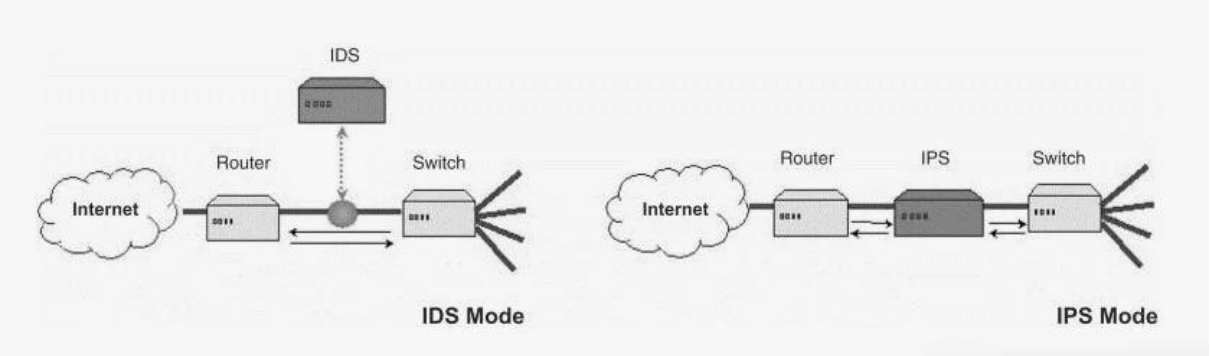

Рисунок 2 — Схема работы IPS/IDS

На рисунке 2 представлены две схемы, иллюстрирующие работу систем IDS и IPS в сетевой инфраструктуре:

1. IDS Mode (слева):
   - В этой конфигурации система IDS расположена параллельно сетевому трафику.
   - Роутер передает трафик к коммутатору, и система IDS получает копию трафика через механизм зеркалирования портов (Port Mirroring или SPAN).
   - IDS анализирует трафик, но не вмешивается в процесс его передачи.
   - Если обнаружена угроза, IDS генерирует уведомление для администратора, но не блокирует угрозу самостоятельно.
2. IPS Mode (справа):
   - Здесь система IPS расположена непосредственно в пути сетевого трафика между роутером и коммутатором.
   - IPS анализирует трафик в режиме реального времени.
   - При обнаружении угрозы IPS может заблокировать вредоносные пакеты, прервать соединение или применить другие защитные меры.
   - Таким образом, IPS активно участвует в защите сети, предотвращая потенциальные атаки.

Ключевое различие между двумя режимами заключается в том, что IDS работает в режиме мониторинга (пассивно), тогда как IPS действует в режиме вмешательства (активно).

Аналитический обзор существующих мер для реализации поставленных задач

На сегодняшний день существует широкий спектр методов и технологий для создания подсистем обнаружения и предотвращения вторжений (IDS/IPS), которые интегрируются в инфраструктуру SOC (Security Operations Center) для обеспечения комплексной информационной безопасности. Эти меры направлены на эффективное выявление угроз, минимизацию ложных срабатываний и автоматизацию реагирования.

На рисунке 3 представлены основные методы обнаружения вторжений, которые классифицируются по их функциональным возможностям.

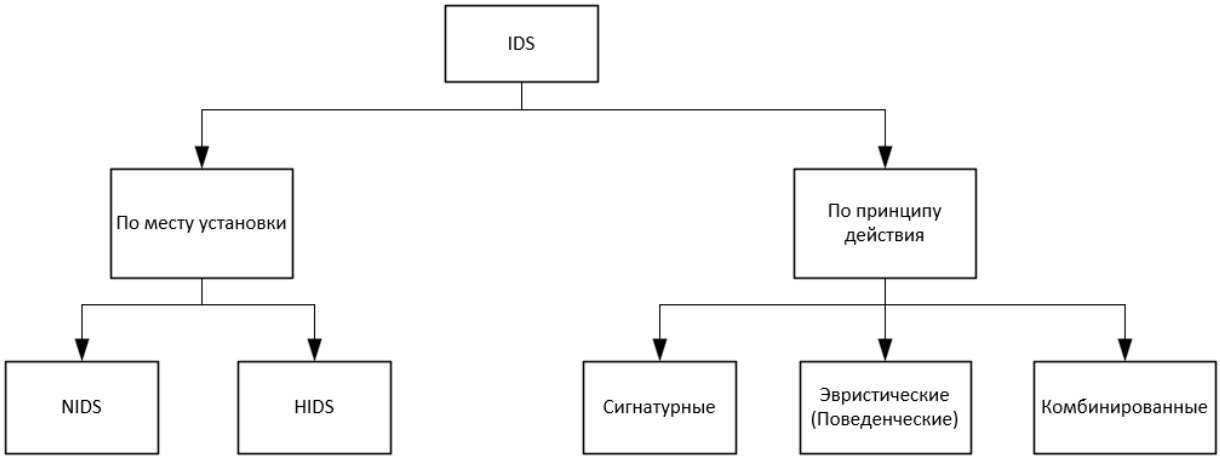

Рисунок 3 — Систематизация методов обнаружения вторжений (IDS)

Системы IDS различаются по месту установки и по принципу действия. В зависимости от места расположения IDS делятся на *сетевые* (network-based IDS, NIDS) и *хостовые* (host-based, HIDS). [7] IDS уровня сети (NIDS) используют сенсоры, являющиеся отдельными компьютерами с установленным на них специальным программным обеспечением либо специальными выделенными устройствами (appliance). Каждый сенсор имеет сетевую карту (NIC – network interface card), работающую в режиме прослушивания сети (promiscuous mode). Обычные сетевые карты получают только сетевые пакеты, адресованные этой сетевой карте, широковещательные (broadcast) и много адресные (multicast) пакеты. Драйвер сетевой карты копирует данные из передающей среды и отправляет его стеку сетевых протоколов для обработки. Если сетевая карта находится в режиме прослушивания, драйвер сетевой карты захватывает весь трафик, делает копии всех пакетов, а затем передает одну копию в стек TCP, а вторую копию – анализатору для поиска определенных шаблонов (сигнатур). NIDS контролирует сетевой трафик и не может увидеть действия, происходящие внутри отдельного компьютера. Для отслеживания таких действий следует использовать IDS уровня хоста. [8] IDS уровня хоста (HIDS) может быть установлена на отдельные рабочие станции и/или серверы для выявления нежелательных или аномальных действий. HIDS обычно используются для обеспечения уверенности, что пользователи не удаляют системные файлы, не изменяют важные настройки или подвергают систему риску иными способами. Так, если NIDS понимает и контролирует сетевой трафик, средства HIDS ограничиваются только самим компьютером. HIDS не понимает и не отслеживает сетевой трафик, а NIDS не контролирует действия внутри системы. Каждое из этих средств имеет свои задачи и выполняет их своими способами. В большинстве сред системы HIDS устанавливаются только на критичные серверы, а не на каждый компьютер в сети, поскольку это могло бы вызвать существенное повышение нагрузки на компьютеры и на администраторов. [8]

HIDS и NIDS могут быть одного из следующих типов:

- Сигнатурные (signature based).
- Поведенческие или эвристические (heuristic-based).
- Комбинированные.

1) **Сигнатурные методы.** Сигнатурные методы обнаружения вторжений на основе сигнатур обычно используются в системах обнаружения вторжений, в которых содержатся сигнатуры (шаблоны) типовых атак, созданные на основе заголовков или содержимого сетевых пакетов. Большое количество сигнатур делает этот метод более затратным с точки зрения стоимости вычислений. Для решения этого ограничения был предложен метод, сочетающий новый метод анализа данных с традиционным сопоставлением с сигнатурами. Главным преимуществом этого подхода является увеличение

производительности сигнатурного метода и уменьшение ложных срабатываний, поскольку поиск идет только в определенных частях пакетов. [9] При сигнатурном методе система анализирует сетевые пакеты или логи. Далее полученные данные проверяются на соответствие известным шаблонам атак. Если обнаружена совпадающая сигнатура, IDS фиксирует инцидент и отправляет администратору или в SOC. На рисунке 4 представлен сигнатурный метод обнаружения вторжений.

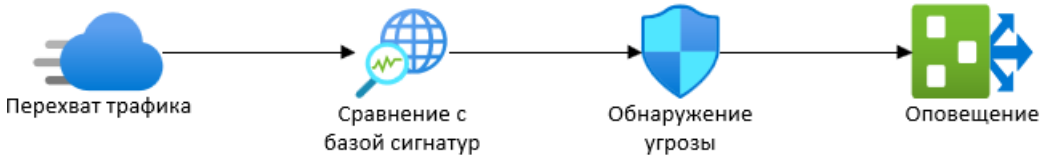

Рисунок 4 — Сигнатурный метод обнаружения вторжений

Преимущества сигнатурного метода: эффективное определение атак на ИС. отсутствие больного числа ложных срабатываний, надежное определение использования конкретного инструментального средства или метода атаки, возможность наиболее точно задать параметры сигнатуры.

Недостатки сигнатурного метода: необходимость обновлять базы сигнатур для обнаружения новых атак; невозможность выявления атак, не описанных в экспертной системе; невозможность выявить атаки, отличающиеся от сигнатурного описания, либо без описания.

2) Поведенческие методы. Поведенческие методы основаны не на моделях информационных атак. а на моделях «нормального» функционирования ИС. Принцип работы любого из этих методов состоит в обнаружении расхождений между текущим режимом работы информационной системы и режима работы, который является эталонным для этой ИС. Любое несоответствие рассматривается как вторжение или аномалия. Сложностью данного принципа является создание точной эталонной модели «нормального» режима информационной системы. [9]

Рисунок 5 — Сигнатурный метод обнаружения вторжений

На рисунке 5 представлен сигнатурный метод обнаружения вторжений, который сопровождается этапами, описанными далее. Система мониторинга сетевого трафика и действий пользователей собирает данные. Далее строится нормальная модель поведения (на основе машинного обучения или эвристики) и выявляются отклонения от норм (высокая активность, необычные запросы, новые соединения). Если зафиксировано подозрительное поведение, система помечает его как возможную атак. В конце отправка уведомлений, регистрация или передача данных в IPS для блокировки.

Преимущества поведенческого метода: определение атаки без знания конкретных деталей (сигнатуры): детекторы аномалии могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур атак. высокая чувствительность к изменениям состоянии ИС.

Недостатки поведенческого метода: ложные сигналы при непредсказуемом поведении пользователей; ложные срабатывания при непредсказуемой сетевой активности; временные затраты на этапе обучения системы.

У каждого принципа есть свои методы, построенные на основе этих принципов. *Сигнатурные методы:* Метод контекстного поиска состоит в обнаружении в исходной информации определенного набора символов. Например, для обнаружения атак на веб-сервера под Unix подобные ОС, направленной на получение несанкционированного доступа к фиалу паролей, производится поиск последовательности символов " */e c/pa " в заголовке запроса HTTP.

Методы анализа состояния основаны на формирования сигнатур атак в виде последовательности переходов информационной системы из одного состояния в другое. наборы таких событии задается параметрами сигнатур атак.

Поведенческие методы (методы обнаружения аномалии): Методы, основанные на статистических моделях, определяют статистические показатели, характеризующиеся параметрами регулярного поведения системы. Если с течением времени есть некоторое отклонение этих параметров от заданных значении, то фиксируется обнаружение атаки. [9]

3) Комбинированные методы: Метод продукционных правил позволяют описать модели для атак на естественном языке с высоким уровнем абстракции. Экспертные системы, использующие эти методы, состоят из двух баз данных: факты и правила. Факты являются входными данными из информационной системы. а правила алгоритмы для логических решении о факте нападения на основе входящего набора фактов. Полученная система правил должна описывать характеристики атак, которые должна обнаружить система обнаружения вторжения. [9]

База правил. С помощью экспертной системы можно точно определить взаимодействие между узлами ИС, которое всегда осуществляется в соответствии с определенными протоколами. Если в процессе обмена информацией между узлами появляется неизвестная команда или нестандартное значение одного из параметров, можно считать это признаком атаки.

Метод имитации поведения биологических систем не использует алгоритмы моделей, основанных на биологических объектах, таких как генетические алгоритмы и искусственные нейтронные сети (ИНС). Методы, основанные на биологических моделях, считаются наиболее перспективным в первую очередь из-за их адаптации и саморазвития.

На этапе вторжения можно обнаруживать атаку как сигнатурным, так и поведенческим методом. Любое вторжение характеризуется определенными особенностями, которые, с одной стороны, могут быть представлены в виде сигнатур, а с другой, как своего рода отклонение от эталонного поведения информационной системы. Наиболее эффективное сочетание обоих методов одновременно, при этом для получения необходимых входных данных применить любые (сетевые либо узловые) датчики. [9]

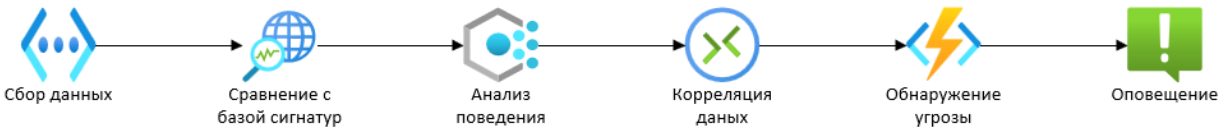

Рисунок 6 — Комбинированный метод обнаружения вторжения

На рисунке 6 представлен комбинированный метод обнаружения вторжений, который сопровождается этапами: сбор данных – анализ сетевого трафика, журналов, активности пользователей; проверка по сигнатурам – сравнение с базой известных атак (SQLi, XSS, DDoS и др.); анализ поведения – выявление аномалий (нестандартные запросы, подозрительные соединения); корреляция данных – объединение результатов методов для точного обнаружения; обнаружение внешней угрозы – фильтрация ложных устройств и проявление слабого воздействия; оповещение – передача в IPS для блокировки.

В таблице 1 представлены преимущества и недостатки методов обнаружения вторжений.

Таблица 1 — Сравнительный анализ

Методы обнаружения вторжений (IDS)	**Преимущества**	**Недостатки**
NIDS (Network-based IDS)	- Отслеживает трафик всей сети, позволяя выявлять широкомасштабные атаки - Менее нагружает конечные устройства, так как анализ ведется на сетевом уровне - Централизованное управление и настройка правил - Может анализировать несколько сегментов сети одновременно	- Не видит зашифрованный трафик (например, HTTPS) или трафик внутри зашифрованных VPN-туннелей - При высоких скоростях сети может возникать проблема с производительностью - Сложность корректной настройки фильтров и правил обнаружения
HIDS (Host-based IDS)	- Глубокий анализ активности на конкретном устройстве (системные вызовы, логи, изменения файлов) - Точная диагностика инцидентов (можно определить, какие именно процессы были скомпрометированы) - Возможность обнаружения атак, не видимых на сетевом уровне	- Нагрузка на систему, так как анализ ведется локально на хосте - Не защищает всю сеть в целом, а только конкретный узел - Сложнее централизованно управлять большим количеством хостов - Требует регулярного обновления политик и правил
Сигнатурные (Signature-based)	- Высокая точность при обнаружении известных угроз - Быстрое срабатывание при совпадении с сигнатурами - Относительно простая реализация и настройка (использование готовых баз правил)	- Не выявляет новые, ранее неизвестные атаки (0-day) - Требует регулярного обновления сигнатур - Может генерировать ложные срабатывания при неверных или слишком общих правилах
Эвристические (Поведенческие)	- Способны обнаруживать новые и неизвестные атаки (0-day), анализируя аномалии и поведение - Менее зависят от базы сигнатур, применяют статистические и поведенческие методы - Позволяют выявлять	- Возможны ложные срабатывания из-за неправильной или недостаточной настройки базовой модели поведения - Требуют значительных вычислительных ресурсов - Более сложная реализация и поддержка,

	сложные, многовекторные атаки	чем у сигнатурных систем
Комбинированные (Signature + Heuristic)	- Сочетают преимущества сигнатурного и поведенческого подходов - Высокая точность при обнаружении известных угроз + способность выявлять новые атаки - Гибкость настройки и адаптации к разным сценариям	- Более высокая сложность конфигурации и сопровождения - Повышенная нагрузка на ресурсы (анализ ведется сразу несколькими методами) - При неправильной настройке возрастает риск ложных срабатываний

Таким образом, IDS у нас может предупреждать о вредоносной активности, но зачастую задача стоит предотвратить вредоносную активность на ранней стадии. В этом может помочь IPS. Методы ее работы относятся к своевременным (превентивным) и проактивным, в отличие от IDS, выполняющей детективные функции. [2] Подобно сетевым IDS (network IDS, NIDS) и IDS на хосте (host IDS, HIDS) существуют сетевые IPS (NIPS) и IPS на хосте (HIPS). Решения NIPS анализируют трафик, прежде чем пропустить его в сеть или подсеть. Решения HIPS анализируют пакеты перед тем, как они поступают в компьютер. [9] Возможность предотвращения атак реализована за счет того, что сетевая IPS, как правило, встраивается «в разрыв» сети и пропускает через себя весь трафик, а также имеет внешний интерфейс, на который приходит трафик и внутренний интерфейс, который пропускает трафик далее, если он признается безопасным. Существует также возможность работы с копией трафика в режиме мониторинга, но тогда мы теряем основной функционал данной системы. [9]

На рисунке 7 представлены основные методы обнаружения вторжений, которые классифицируются по их функциональным возможностям.

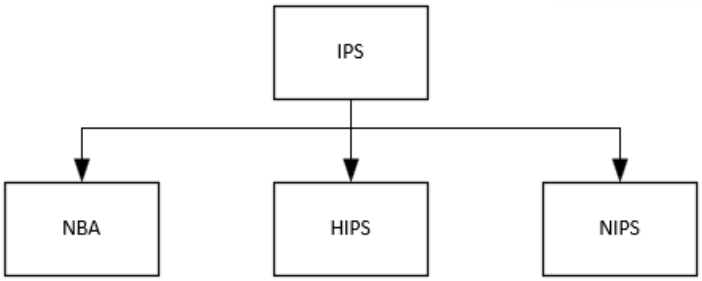

Рисунок 7 — Классификация методов предотвращения вторжений (IPS)

На сегодняшний день существуют два класса IPS - NIPS (Network based Intrusion Prevention System — сетевые системы противодействия вторжениям) и HIPS (Host based Intrusion Prevention System — системы противодействия вторжениям для защиты хост-компьютеров). [10] Глобально IPS можно разделить на те, которые анализируют трафик и сравнивают с известными сигнатурами, и те, которые на основе анализа протоколов ищут нелегитимный трафик, основываясь на базе знаний о найденных ранее уязвимостях. За счет второго класса обеспечивается защита от неизвестного типа атак. Что касается методов реагирования на атаки, то их накопилось большое количество, но из основных можно выделить следующие: блокирование соединения с помощью TCP-пакета с RST-флагом или посредством межсетевого экрана, перенастройка коммуникационного оборудования, а также

блокирование записей пользователей или конкретного хоста в инфраструктуре. [7] Но, кроме двух известных методов, имеется и 3 подход — анализатор поведения сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS- атаки.

• Сетевые IPS (Network-based Intrusion Prevention, NIPS): отслеживают трафик компьютерной сети и блокируют подозрительные потоки данных. NIPS работает, будучи установленным в сетевой трафик или через зеркальные порты. Он выполняет глубокую проверку пакетов (DPI) для анализа данных в реальном времени. Система включает в себя ключевые компоненты, такие как захват пакетов, декодеры протоколов, механизмы сопоставления сигнатур, эвристики, алгоритмы обнаружения аномалий и проверку состояния. Первым шагом является захват пакетов, где он получает необработанные пакеты из сетевого интерфейса. Далее я продолжу описывать, как каждый компонент вносит свой вклад в процесс обнаружения и предотвращения. NIPS перехватывает и анализирует сетевой трафик на лету, захватывая пакеты и выполняя глубокую проверку пакетов (DPI). Она собирает фрагментированные пакеты, проверяет полезную нагрузку и декодирует протоколы, такие как TCP, UDP и SSL/TLS. Обнаружение на основе сигнатур сравнивает пакеты с известными шаблонами атак, в то время как обнаружение аномалий ищет отклонения трафика. Проверка с отслеживанием состояния обеспечивает целостность протокола. NIPS использует аппаратное ускорение для повышения эффективности и интегрируется с SIEM для централизованного ведения журнала событий. Она может блокировать угрозы в режиме реального времени и использует машинное обучение для адаптации и улучшения обнаружения с течением времени.

На рисунке 8 представлена сетевая система предотвращения вторжений.

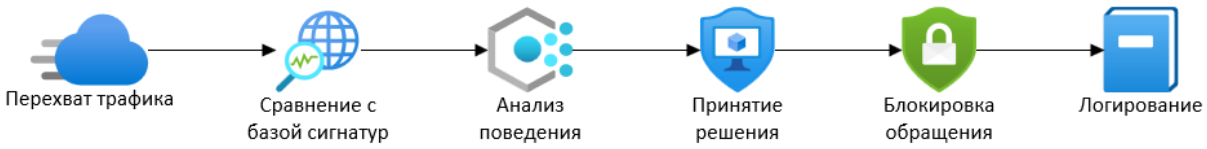

Рисунок 8 — Сетевая система предотвращения вторжений

NIPS применяет многослойный подход для обнаружения атак на разных уровнях сетевого трафика. Это включает в себя анализ трафика приложений, таких как SQL-инъекции и XSS, а также сетевые атаки, такие как DoS и аномалии протоколов. Система использует правила для обнаружения атак с регулярными обновлениями. В режиме встроенной системы процесс включает захват, обработку, анализ и принятие решений о действиях.

• Хостовые IPS (Host-based Intrusion Prevention, HIPS): резидентные программы, обнаруживающие подозрительную активность на компьютере. HIPS работает, будучи установленным непосредственно на конечном устройстве, и интегрируется с операционной системой для мониторинга всех системных событий. Он выполняет глубокий анализ событий (Deep Inspection of Events) для анализа действий в реальном времени. [11] Система включает в себя ключевые компоненты, такие как захват событий, декодеры системных вызовов, механизмы сопоставления сигнатур, эвристический анализ, алгоритмы обнаружения аномалий и проверку целостности системы. Первым шагом является захват событий, где HIPS регистрирует все обращения к системным ресурсам, файловой системе, реестру и сетевым интерфейсам. Далее рассмотрим, как каждый компонент вносит свой вклад в процесс обнаружения и предотвращения угроз.

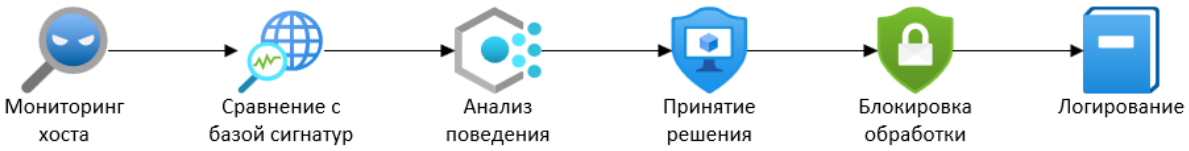

Рисунок 9 — Хостовая система предотвращения вторжений

HIPS перехватывает и анализирует системные события в реальном времени, фиксируя действия процессов, изменения файлов, обращения к критически важным компонентам системы и системные вызовы. Система собирает информацию о действиях приложений и операционной системы, декодирует вызовы и преобразует их в понятный формат для дальнейшего анализа. Обнаружение на основе сигнатур сравнивает эти события с известными шаблонами атак, тогда как эвристический анализ выявляет отклонения в поведении приложений, которые могут указывать на новые, ранее не зарегистрированные угрозы. Контроль целостности и отслеживание состояния помогают убедиться, что системные файлы и настройки не были изменены злоумышленниками.

HIPS использует следующие ключевые компоненты:

- Захват событий: Получение необработанных системных вызовов, изменений файлов, действий приложений и сетевых операций.
- Декодеры системных вызовов: Преобразование низкоуровневых данных операционной системы в структурированную информацию.
- Механизмы сопоставления сигнатур: Сравнение событий с базой данных известных угроз и шаблонов атак.
- Эвристический анализ: Применение алгоритмов для обнаружения аномального поведения, даже если конкретная угроза еще не зарегистрирована.
- Алгоритмы обнаружения аномалий: Поиск отклонений от нормального поведения системы, что может свидетельствовать о попытках компрометации.
- Проверка целостности и состояния: Контроль изменений в критически важных системных файлах и настройках для выявления несанкционированных изменений.

HIPS интегрируется с централизованными системами логирования (например, SIEM) для ведения подробного журнала событий, что позволяет администраторам оперативно получать уведомления и анализировать инциденты. Система может блокировать или ограничивать подозрительные процессы в режиме реального времени, применять методы машинного обучения для адаптации к новым угрозам и постоянно обновлять свои базы сигнатур и эвристические модели.

Применяя многослойный подход, HIPS анализирует события на различных уровнях операционной системы – от действий отдельных приложений до низкоуровневых системных вызовов. Это позволяет обнаруживать как попытки изменения системных файлов и вмешательства в работу служб, так и атаки на уровне приложений, такие как эксплойты или несанкционированное изменение конфигурации. В активном режиме HIPS может немедленно блокировать вредоносные процессы, а в режиме мониторинга – лишь регистрировать события для последующего анализа, что позволяет снизить риск ложных срабатываний.

Таким образом, HIPS представляет собой комплексное решение для защиты конечного устройства, где каждая составляющая, от захвата событий до анализа и принятия решения, играет свою роль в своевременном обнаружении и предотвращении угроз.

- Анализатор поведения сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS- атаки. NBA работает, установленный через зеркальные порты или inline, для анализа сетевого трафика в реальном времени. Он осуществляет глубокий анализ пакетов (DPI) и обнаруживает аномалии, сравнивая поведение текущего трафика с установленными базовыми моделями. Система включает следующие ключевые компоненты:

- Захват пакетов – получение необработанных пакетов с сетевого интерфейса, включая сбор фрагментированных данных.
- Декодеры протоколов – распознавание и восстановление протоколов (TCP, UDP, ICMP, HTTP, SSL/TLS и др.).
- Нормализация трафика – приведение данных к единому формату для корректного анализа.
- Механизмы сопоставления сигнатур – сравнение пакетов с известными шаблонами атак.
- Эвристический анализ и алгоритмы обнаружения аномалий – выявление отклонений от нормы с помощью машинного обучения и статистических методов.
- Проверка с отслеживанием состояния – контроль целостности сессий и протоколов.

На рисунке 10 представлен анализатор поведения сети. Первым шагом происходит захват пакетов с сетевого интерфейса, после чего трафик агрегируется, декодируется и нормализуется. Далее система применяет алгоритмы для выявления аномальных паттернов, что позволяет обнаруживать атаки типа DDoS, сканирование портов, ботнет-активность, SQL-инъекции и XSS. Интеграция с SIEM обеспечивает централизованное ведение журнала событий и корреляцию инцидентов. В inline-режиме NBA может блокировать подозрительный трафик, а в пассивном режиме – только мониторить сетевую активность.

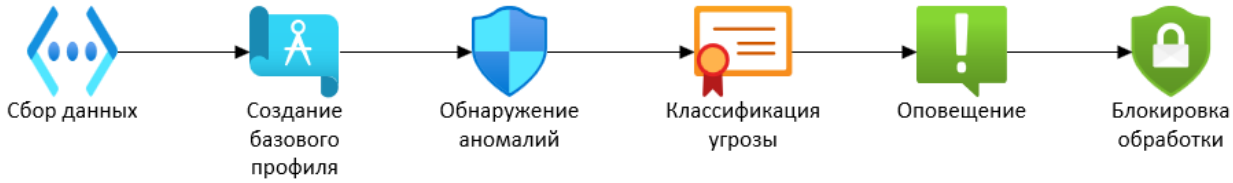

Рисунок 10 — Анализатор поведения сети

В таблице 2 представлены преимущества и недостатки методов предотвращения обнаружения.

Таблица 2 — Сравнительный анализ

Методы предотвращения вторжений (IPS)	**Преимущества**	**Недостатки**
NIPS (Сетевые IPS)	- Анализ трафика в реальном времени с помощью DPI- Inline -блокировка угроз - Декодирование протоколов (TCP, UDP, SSL/TLS и др.) - Интеграция с SIEM для централизованного ведения журнала	- Высокая ресурсоемкость - Возможны ложные срабатывания - Сложность настройки - Потенциальное увеличение задержек в сети
HIPS (Хостовые IPS)	- Локальная защита конечного устройства - Многоуровневый анализ (сигнатурный, поведенческий, эвристический) - Детальное логирование событий - Гибкая настройка политик безопасности	- Высокая нагрузка на систему - Риск ложных тревог - Сложность конфигурации - Необходимость регулярных обновлений баз данных

NBA (Анализатор поведения сети)	- Глубокий анализ поведения сети в реальном времени - Обнаружение аномалий и неизвестных угроз - DPI и декодирование протоколов - Централизованное логирование через SIEM - Гибкая настройка порогов аномалий	- Возможны ложные срабатывания при неправильной настройке - Требует обучения базовым моделям трафика - Высокая вычислительная нагрузка при обработке больших объемов данных - Сложность интеграции в инфраструктуру

Проведенный анализ различных методов обнаружения и предотвращения вторжений показал, что каждая система имеет свои технические особенности и ограничения. Из этого следует, что:

IDS (система обнаружения вторжений):

- NIDS (Network-based IDS) – анализирует весь сетевой трафик и обнаруживает атаки до их проникновения в систему.
- HIDS (Host-based IDS) – мониторит активность на уровне операционной системы и файловой структуры серверов и рабочих станций.
- Комбинированный метод (сигнатурный + поведенческий анализ) – позволяет обнаруживать как известные, так и новые угрозы.

IPS (система предотвращения вторжений):

- NIPS (Network-based IPS) – предотвращает вторжения, блокируя вредоносные пакеты на сетевом уровне.
- HIPS (Host-based IPS) – защищает серверы и рабочие станции от эксплойтов и вредоносных процессов.
- NBA (Network Behavior Analysis) – анализирует аномальное поведение в сети и выявляет сложные угрозы (ботнеты, APT, скрытые атаки).

Таким образом, после рассмотрения всех факторов, следует выделить платформы, использующие данные методы:

- Cisco Firepower – включает NIPS, NBA и HIPS.
- Darktrace – мощная NBA-система на основе ИИ.
- Suricata – IDS/IPS, анализ пакетов и сетевых атак (NIDS/NIPS).
- Snort – IDS/IPS, мониторинг трафика и предотвращение атак (NIDS/NIPS).
- OSSEC – HIDS, мониторинг целостности файлов и журналов, предотвращение атак.
- Zeek – NIDS, анализ сетевого трафика и обнаружение инцидентов.

Каждая из этих платформ так или иначе решает поставленные задачи, но при этом затрачивает дополнительно: аппаратные, программные и денежные ресурсы; не имеет одного интерфейса, что доставляет неудобство при использовании; не имеет автономности и зависит от других компонентов SOC, а именно от SIEM и SOAR систем. Но чтобы решить эти проблемы, предлагается использовать комплексный подход.

Таблица 3 — Решение поставленных задач

Поставленные задачи:	**Решение:**
Предотвращение несанкционированного изменения данных о событиях и атаках	Логи и события сохраняются в защищtнном хранилище с применением методов хеширования и цифровых подписей для подтверждения их целостности
Защита алгоритмов детекции от	Настройки и алгоритмы детекции в

внешнего вмешательства	Suricata и Zeek защищены через строгие механизмы контроля доступа (например, RBAC) и мониторинг всех изменений
Обеспечение безопасности передачи и хранения данных	Все данные о событиях шифруются, а доступ к ним строго контролируется. Логи могут быть защищены через хранение в зашифрованных базах данных или на защищенных серверах.
Конфиденциальность и целостность данных при интеграции с другими системами	Взаимодействие с другими системами безопасности, такими как SIEM или SOAR, осуществляется через защищенные каналы связи (например, VPN или HTTPS), чтобы исключить утечку или компрометацию данных
Реагирование на угрозы в реальном времени	Система на базе Suricata и Zeek позволяет выявлять угрозы в реальном времени с минимальной задержкой. Это обеспечивается быстрым анализом пакетов и аномалий, а также возможностью автоматического реагирования (например, блокировка трафика)

Комплексный подход решает поставленные задачи, которые представлены в таблице 3. Благодаря такому подходу решаются не только поставленные задачи, но и перекрываются все недостатки, упомянутые ранее при использовании всех компонентов по отдельности, а именно:

- Автономная система, позволяющая работать без поддержки SIEM/SOAR;
- Использование IPS/IDS;
- Использование меньшего количества аппаратных ресурсов;
- Использование меньшего количества программных ресурсов;
- Оптимизация;
- Гибкость в интеграции с SOC;
- Платформы имеют бесплатные решения.

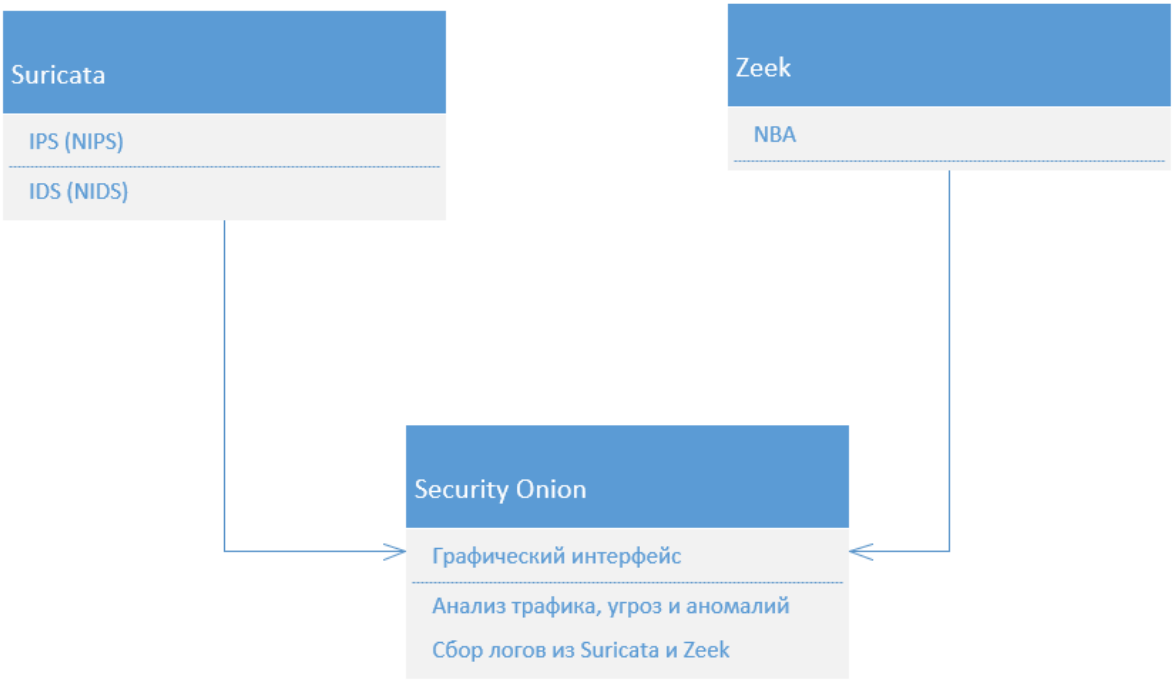

Рисунок 11 — Комплексный подход IPS/IDS

На рисунке 11 представлен комплексный подход IPS/IDS. Система на базе Security Onion**,** Suricata **и** Zeek является комплексным решением для мониторинга и защиты сети в реальном времени. Она сочетает в себе возможности IDS/IPS, анализа поведения и сетевого трафика для обнаружения угроз и атак. Эти компоненты работают совместно для того, чтобы обеспечить всестороннюю защиту.

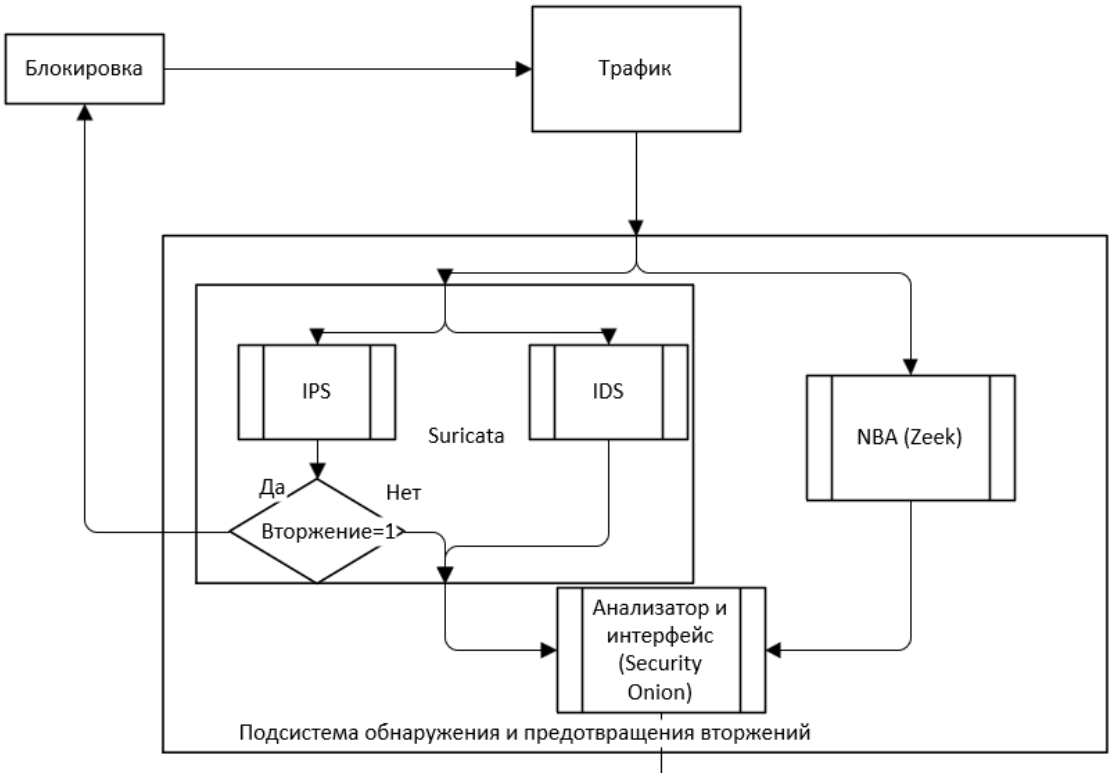

Рисунок 12 — Архитектура комплексного подхода IPS/IDS

На рисунке 12 представлена архитектура комплексного подхода IPS/IDS. На **первом этапе** идет сбор данных о трафике: Suricata просматривает пакеты данных и использует сигнатуры угроз, чтобы идентифицировать известные атаки. Она также может работать в режиме IPS, чтобы блокировать трафик, если обнаружены угрозы. Zeek анализирует трафик на более высоком уровне, чем Suricata. Вместо того чтобы только искать сигнатуры атак, он пытается выявить аномалии в поведении сети. Например: если в сети появляются необычные запросы на разрешение DNS или аномально много попыток подключения к внутренним серверам, Zeek будет генерировать события для дальнейшего анализа. На **втором этапе** идет обработка и хранение логов. Все данные о сетевых событиях, которые собираются Suricata и Zeek, сохраняются в Security Onion. На **третьем этапе** реакция на угрозы: в случае обнаружения угроз, система может сгенерировать уведомления для администраторов безопасности или автоматически предпринять шаги по устранению угрозы: Suricata может заблокировать вредоносный трафик в режиме IPS. Zeek может отслеживать аномальные события и, если настроено, передавать эти события в другие системы для реакции. В случае обнаружения угроз в реальном времени, например, в результате DDoS-атаки или подозрительного поведения на DNS, система может изолировать атакующие устройства или применить политику ограничения доступа. На **четвертом этапе** идет защита и безопасность данных. Важно также защитить сами данные о сетевых событиях. Шифрование логов и трафика на уровне передачи данных (например, через SSL/TLS) помогает предотвратить утечку данных. Целостность данных контролируется через хеширование. Логи и события могут подписываться цифровыми подписями, чтобы гарантировать, что они не были изменены. Защищенные каналы передачи используются для передачи данных между компонентами системы, что исключает их компрометацию.

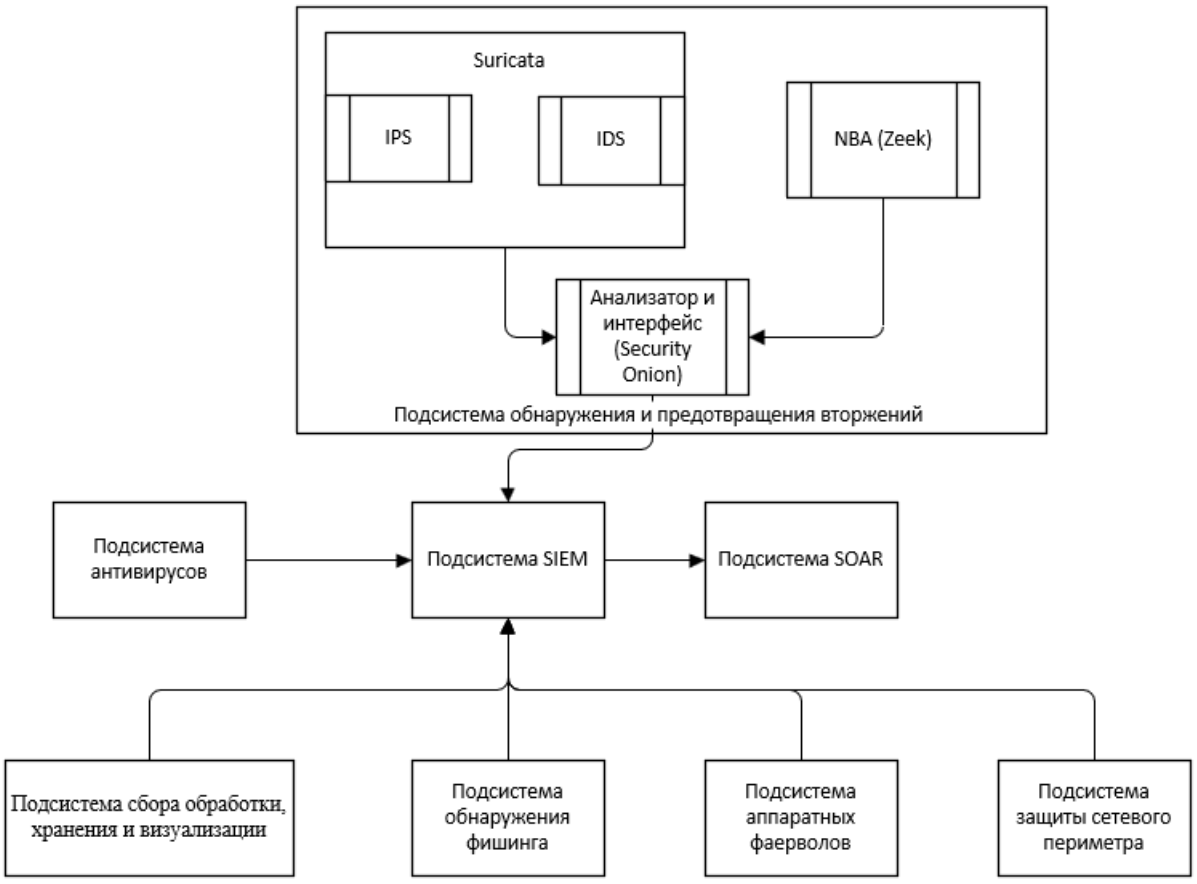

Рисунок 13 — Взаимодействие подсистемы IPS/IDS с SOC

На рисунке 13 представлено взаимодействие подсистемы IPS/IDS с SOC. А именно NBA анализирует поведение трафика (странные запросы, необычные порты, аномальные DNS-запросы). Если находит аномалию, отправляет ее в Security Onion → SIEM → SOAR. Не блокирует трафик, а просто сообщает о подозрительном. Suricata проверяет пакеты по сигнатурам атак (например, SQL-инъекции, DDoS, сканирование портов). Если обнаружена угроза, отправляет событие в Security Onion → SIEM → SOAR. Если атака подтверждена, IPS блокирует ее сразу**.** Параллельно передает данные в Security Onion → SIEM → SOAR для расследования. Если Zeek нашел аномалию, то это не значит, что атака подтверждена. Дальше анализ идет через SIEM → SOAR. Но если Suricata (IDS) нашла атаку**,** то в режиме IPS она сразу заблокирует ее.

Защита клиентских сетей с помощью комплексного подхода IPS/IDS:

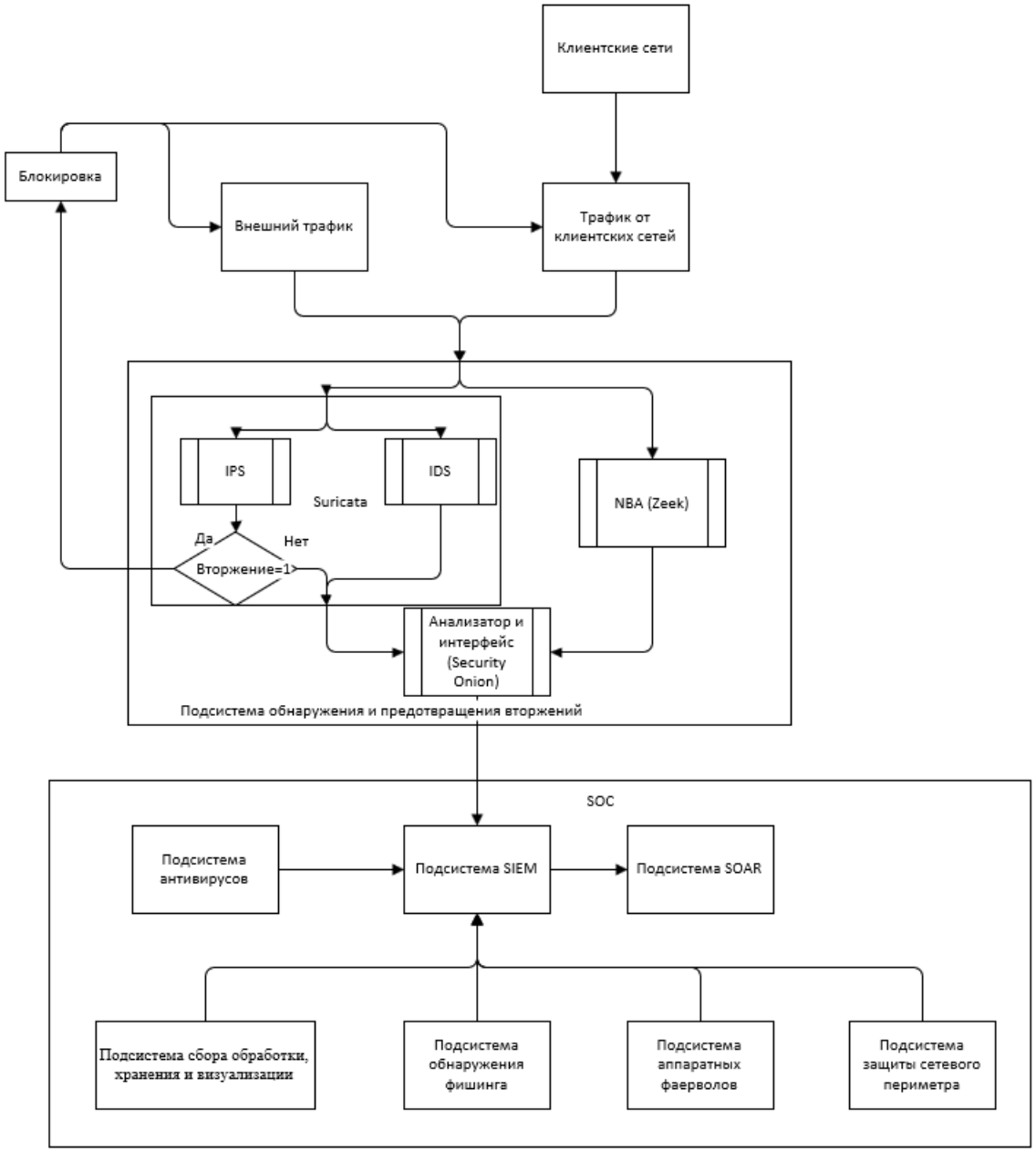

Рисунок 14 — Защита клиентских сетей

На рисунке 14 представлена защита клиентских сетей в рамках **SOC (Security Operations Center)**. Она включает в себя несколько подсистем, совместно работающих, отслеживающих и предотвращающих вторжения.

1. Клиентские сети — источник трафика, который поступает в систему SOC. Трафик от клиентских сетей направляется в SOC для анализа и фильтрации.

2. Клиентский трафик проходит через систему обнаружения и предотвращения вторжений. Она включает: IDS и IPS — реализованы на основе Suricata. IDS анализирует трафик и выявляет потенциальные угрозы. IPS может блокировать лицензионные пакеты. NBA анализирует сетевой трафик и выявляет аномальное поведение. В случае обнаружения угрозы информация направляется в Security Onion, который обеспечивает интерфейс для анализа инцидентов.

3. Вредоносный трафик может быть заблокирован системой IPS. Внешний трафик также анализируется на предмет угрозы.

4. SOC получает данные от систем обнаружения вторжений и передает их в другие подсистемы для обработки: SIEM (Информация о безопасности и управление событиями) – собирает и анализирует события безопасности и SOAR (Security Orchestration, Automation and Response) – автоматизирует реагирование на угрозу.

Дополнительные преимущества SOC:

- Антивирусная защита.
- Систему обнаружения рыбалки.
- Аппаратные файрволлы.
- Защита периметра сети.

Эти компоненты работают совместно, обеспечивая всестороннюю защиту клиентских сетей. В этом контексте предлагаемая в данной работе подсистема IPS/IDS, основанная на интеграции технологий Suricata, Zeek и Security Onion, эффективно решает поставленные задачи. Объединяя возможности обнаружения, анализа и предотвращения угроз, данное решение не только оптимизирует затраты на инфраструктуру, но и обеспечивает единый интерфейс для мониторинга, что значительно повышает уровень защиты корпоративных сетей. Комплексный подход, включающий анализ аномалий, корреляцию событий и оперативное реагирование, позволяет минимизировать потенциальный ущерб и повысить устойчивость информационных систем перед современными угрозами ИБ.

Таким образом, учитывая масштаб и разнообразие современных угроз ИБ, а также ограничения традиционных систем IPS/IDS, актуальность разработки и внедрения интегрированной подсистемы обнаружения и предотвращения вторжений является бесспорной. Комплексный подход к защите, позволяющий объединить все необходимые инструменты в единую платформу, является ключом к обеспечению безопасности корпоративных сетей в условиях постоянно эволюционирующей среды.

Заключение

В заключение можно обозначить, что для эффективного выявления и предотвращения сетевых атак используются различные системы сетевой безопасности, каждая из которых обладает своими преимуществами в зависимости от задачи. Среди наиболее мощных решений выделяются IDS/IPS-системы, такие как Suricata, и системы анализа сетевого поведения (NBA), например, Zeek, объединенные в единую платформу Security Onion.

Suricata, работая в режиме IDS и IPS, обеспечивает детектирование атак на основе сигнатурного анализа и предотвращение угроз в реальном времени. В то же время Zeek фокусируется на поведенческом анализе трафика, выявляя аномалии и подозрительные шаблоны взаимодействий, которые могут указывать на скрытые атаки. Такое сочетание позволяет обнаруживать как известные угрозы, так и новые атаки, ранее не включенные в базы сигнатур.

Security Onion интегрирует эти инструменты, обеспечивая централизованный сбор, хранение и анализ событий безопасности. Использование Elasticsearch, Logstash и Kibana позволяет визуализировать угрозы, выявлять закономерности и оперативно реагировать на инциденты. Благодаря встроенным механизмам шифрования и защиты логов система предотвращает несанкционированное изменение данных, обеспечивая их целостность и конфиденциальность.

Таким образом, комбинация Security Onion, Suricata и Zeek создает эффективное и экономичное решение для защиты сетей, не требующее дополнительных SIEM- и SOAR-систем. Этот подход обеспечивает оперативное реагирование на угрозы, минимальные задержки при анализе атак и надежную защиту данных, что делает его оптимальным выбором для построения современной системы кибербезопасности.

Литература

1. https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva (дата обращения 01.15.2025).
2. https://ics-cert.kaspersky.ru/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/ (дата обращения 01.20.2025).
3. https://www.kaspersky.ru/about/press-releases/v-nachale-2024-goda-v-apt-atakah-po-vsemu-miru-chashe-vsego-ispolzovalis-uyazvimosti-v-instrumentah-udalyonnogo-dostupa-i-winrar (дата обращения 01.25.2025).
4. https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet#:~:text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B%20StormWall%20%D0%B2%202024,%D0%BC%D0%BE%D1%89%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%B0%D1%82%D0%B0%D0%BA%20%D0%B2%D1%8B%D1%80%D0%BE%D1%81%D0%BB%D0%B0%20%D0%BD%D0%B0%2053%25. (дата обращения 01.30.2025).
5. https://www.cloud4y.ru/blog/ips-and-ids-what-is-it/ (дата обращения 02.05.2025).
6. https://cloudnetworks.ru/inf-bezopasnost/ids-ips/#:~:text=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%BE%D0%B1%D0%BD%D0%B0%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%B2%D1%82%D0%BE%D1%80%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9%20(IDS)%20%D0%BF%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D1%8F%D0%B5%D1%82,%D0%BF%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B0%D0%B5%D1%82%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%20%D0%BF%D0%BE%20IP%2D%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D1%83. (дата обращения 02.10.2025).
7. https://habr.com/ru/companies/otus/articles/479584/ (дата обращения 02.15.2025).
8. https://studfile.net/preview/6211055/page:19/#46 (дата обращения 02.20.2025).
9. https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy/viewer (дата обращения 02.25.2025).
10. https://lib.itsec.ru/articles2/Oborandteh/tehnologii-hips (дата обращения 02.30.2025).
11. https://www.osp.ru/winitpro/2006/04/2578870#:~:text=%D0%A0%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%20NIPS%20%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B8%D1%80%D1%83%D1%8E%D1%82%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%2C%20%D0%BF%D1%80%D0%B5%D0%B6%D0%B4%D0%B5,%D0%BC%D0%BE%D0%B3%D1%83%D1%82%20%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D1%87%D0%B0%D1%82%D1%8C%D1%81%D1%8F%20%D0%BF%D0%BE%20%D1%82%D0%B8%D0%BF%D1%83%20%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B0. (дата обращения 03.15.2025).