1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**Курсовая работа**

1. «**Сравнительный анализ методов построения СОВ**»
2. по дисциплине «Методы безопасности компьютерных систем»
3. **Выполнил:**
4. студент гр. 4851001/90002 Судаков Д.И.

<*подпись*>

**Проверил:**

1. Старший преподаватель Т. Д. Овасапян

<*подпись*>

1. Санкт-Петербург
2. 2021
3. **Содержание**

Введение…………………………………………………………………….3

1. Исследование по теме……………………………………………………...4
2. Различия IDS/IPS…..……………………………………………………….6
3. Методы построения СОВ…………………………………………………..6
   1. Глубокое обучение……………………………………………………..6
   2. Быстрое обучение и оптимизация “Swarm”………………………….8
   3. Контроллер reCAPTCHA………………………………………………9
   4. Гибридная оптимизация……………………………………………….12
   5. Адаптивная СОВ………………………………………………………..14
4. Сравнительный анализ методов построения СОВ..………………………19

Заключение…………………………………………………………………..21

Список источников………………………………………………………….22

Введение

Системы обнаружения вторжений (Intrusion Detection System) — это совокупность программных и/или аппаратных средств, служащих для выявления фактов несанкционированного доступа в компьютер или компьютерную сеть, а также предотвращения неавторизованного управления ими.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)[1].

*Актуальность разработки систем обнаружения вторжений:*  
В настоящее время все больше предприятий так или иначе задумываются о сохранности информации и бесперебойной работе своих информационных систем. На рынке систем обнаружения атак представлено множество решений. Системы обладают различным функционалом, предлагают различные методы борьбы с атаками. Также наряду с коммерческими программными продуктами на рынке можно встретить и бесплатные версии систем обнаружения вторжений, которые доступны широкому потребителю[2].

*Цель* данной работы заключается в объективной оценке различных методов построения систем обнаружения и предотвращения вторжений путем проведения сравнительного анализа на основе научной литературы и научных статей на английском языке.

Выделим следующие *задачи,* необходимые для достижения поставленной цели:

- провести краткое исследование СОВ на основе научной статьи из международного журнала технологических исследований и управления

- выделить различия между системами обнаружения вторжений и системами предотвращения вторжений

- выделить основные методы построения систем обнаружения вторжений

- сформулировать преимущества и недостатки изучаемых методов построения СОВ

- провести анализ методов построения СОВ

- сделать выводы на основании проведенного анализа

- провести сравнительный анализ изученных методов построения СОВ

- подвести итоги и сделать выводы на основании проделанной работы

1. Исследование по теме

*Статья «Исследование СОВ»* из международного журнала технологических исследований и управления:

[A Survey on Intrusion Detection System(IDS)](http://www.ijtrm.com/PublishedPaper/5Vol/Issue7/2018IJTRM7201815907-0b85b8a6-2929-4b4a-995c-1aa15c78c79819620.pdf)[3]

Материалы данной статьи более широко раскрывают понятия IPS и IDS. В первую очередь речь идёт о структуре и принципе работы СОВ в базовом её представлении.

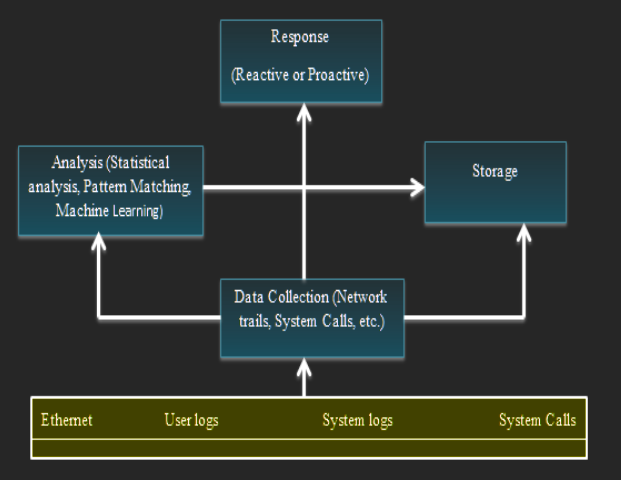
Системы предотвращения обнаружения вторжений пытаются обнаруживать вторжения в операционные системы (другие защищаемые объекты) и реагировать на них. Большинство IDS представлены набором компонентов, определяющих общую модель. В статье рассматриваются такие компоненты как Data Collection (Сбор данных), Storge (Хранилище), Analysis (Анализ) и Response (Реакция). Data Collection отвечает за предоставление системе информации, необходимой для принятия решения о том, является ли конкретное действие навязчивым или нет. Этот компонент собирает журналы пользователей, системные журналы, системные вызовы и т.д. для остальных компонентов IDS. Этот модуль очень важен, потому что без него другие модули не смогут функционировать. Storage хранит все данные системы как до их обработки, так и после. Response, в свою очередь, формирует, если это необходимо, команды для защищаемого объекта, которые по существу являются реакцией СОВ на активность в системе (Рисунок 1).

Рисунок 1 – Базовая модель IDS

Также в статье приводится классификация СОВ по исполнению. Речь идёт о сетевых, хостовых и распределенных IDS, однако, как известно существует множество иных вариантов исполнения, например, достаточно популярны гибридные IDS, также встречаются протокольные, узловые, сигнатурные, корреляционные и другие.

1. Различия IDS и IPS

СОВ в англоязычной литературе разделяют на IDS(Intrusion Detection System) и IPS(Intrusion Prevention Systems), ниже приведена статья, раскрывающая причину такого разделения.

*Статья о различиях IDS и IPS:*

[Comparing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) | Engineering Education (EngEd) Program | Section](https://www.section.io/engineering-education/comparing-intrusion-detection-systems-ids-and-intrusion-prevention-systems-ips/)[4]

Изучив информацию, приведенную в данной статье можно сделать вывод о том, что IDS целесообразно применять вместе с IPS, так как они выполняют две тесно связанные функции защиты от вредоносного трафика: IDS распознаёт угрозу, а IPS гарантирует её блокирование и невозможность доставки вредоносных пакетов на защищенный объект. Так большинство современных разработчиков объединяют эти две технологические системы в одно решение.

1. Методы построения СОВ

Существует множество различных методов построения СОВ, ниже приведены статьи, раскрывающие некоторые из них.

3.1 Глубокое обучения для СОВ: [Deep Learning Approach for Intelligent Intrusion Detection System | IEEE Journals & Magazine[5].](https://ieeexplore.ieee.org/abstract/document/8681044) В данной статье рассматривается возможность модернизации СОВ путём внедрения в компонент Analysis глубокой нейронной сети и её обучения. Автор статьи иллюстрирует основные принципы данной идеи на собственном проекте, включающем разработку СОВ с глубоким обучением. В приведенном примере в качестве вычислительной модели используется нейронная сеть с глубоким обучением, построенная на основе подхода ANN (искусственная нейронная сеть), позволяющего включить искусственный интеллект в предложенную модель, поскольку на нее влияют характеристики биологических нейронных сетей. Тип нейронной сети прямого распространения (FFN) представляет собой ориентированный граф, используемый для передачи различной системной информации по ребрам от одного узла к другому без формирования цикла. Модель данного типа в приведенном примере представлена многослойным персептроном (MLP), имеющим три и более слоёв с одним входным слоем, несколькими скрытыми слоями и одним выходным слоем. Стоит отметить, что каждый слой имеет множество нейронов (единиц) в математической нотации. Количество скрытых слоев выбирается методом выбора гиперпараметров. Информация преобразуется из одного слоя в другой в прямом направлении, при этом нейроны в каждом слое полностью связаны. Вычисление каждого скрытого слоя математически определяется как , где , , , – объем входных данных. В общих чертах для многих скрытых слоёв MLP формулируется следующим образом: . Такой способ наложения скрытых слоёв и называется глубокой нейронной сетью.

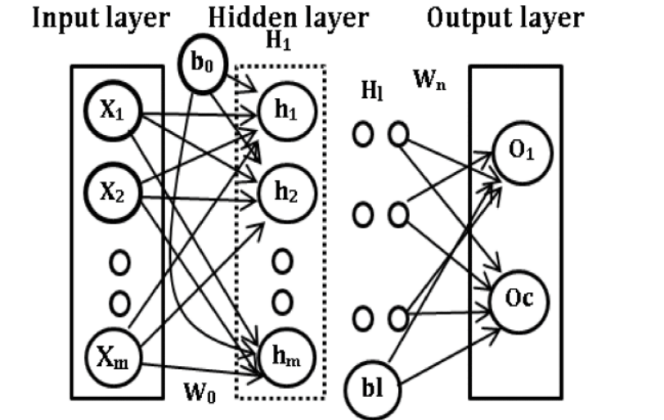


Рисунок 2 – Глубокая нейронная сеть

Подводя итоги по данному методу, необходимо обозначить тот факт, что его уникальность заключается в моделировании многослойности при построении нейронной сети. Внедрение такой модернизации влечет как преимущества, так и недостатки. В качестве преимуществ можно выделить повышенную надежность и отказоустойчивость, в качестве недостатков – увеличение со временем числа ложных срабатываний.

3.2 Быстрое обучение и оптимизация “Swarm” алгоритма. [A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization | IEEE Journals & Magazine | IEEE Xplore](https://ieeexplore.ieee.org/abstract/document/8326489)[6]. В данной статье поставлен акцент на алгоритме оптимизации «роя частиц» (Swarm). Оптимизация роя частиц (PSO) - это метод параллельных эволюционных вычислений, разработанный Мишрой и Сенгуптой . Протокол был разработан на основе метафоры социального поведения. На производительность алгоритма PSO сильно влияют включенные параметры и настройка, часто называемые компромиссом между разведкой и разработкой: исследование описывает способность оценивать различные области в проблемном пространстве, чтобы попытаться определить хороший оптимум, предпочтительно глобальный.

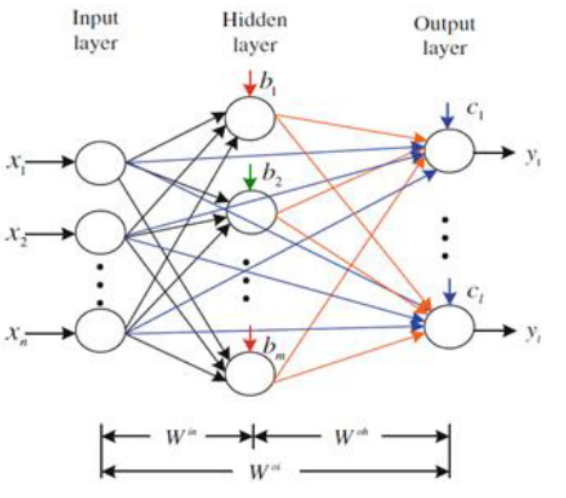
Эксплуатация описывает способность сосредоточить поиск в непосредственной близости от многообещающего потенциального решения, чтобы эффективно и быстро найти оптимальное. Несмотря на недавние исследовательские усилия, выбор параметров алгоритма остается в значительной степени эмпирическим.  Сеть быстрого обучения (FLN), предложенная Sahu *et al.,* представляет собой параллельное соединение SLFN и трехуровневой FNN, которая уже была упомянута в ранее.  FLN – искусственная нейронная сеть, которая представляет собой двойную параллельную прямую нейронную сеть (DPFNN), демонстрируется ниже с использованием аналитического подхода, а именно методов наименьших квадратов, как показано на рисунке 3.

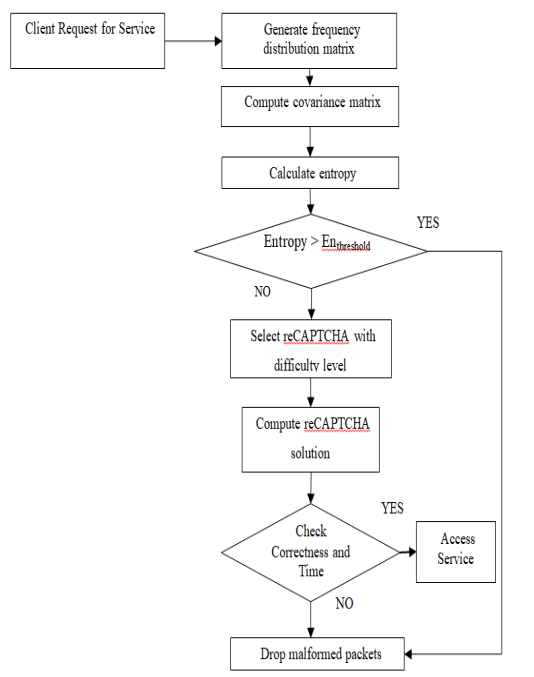
Рисунок 3 – Структура FLN

Анализируя материалы данной статьи, делаем вывод о том, что использование метода быстрого обучения и алгоритма оптимизации Swarm является наиболее перспективным решением проблемы возникновения ошибочно верных и ложных срабатываний, поскольку обучение реализовано на реальных примерах. Из недостатков можно выделить сложность реализации и высокую степень зависимости от настроек и включенных параметров, выбор которых по прежнему осуществляется эмпирически.

3.3 Использование контроллера reCAPTCHA для СОВ. [Intrusion Prevention System with reCAPTCHA controller using IBM | IEEE Journals & Magazine](https://ieeexplore.ieee.org/abstract/document/8859299)[7]. В данной статье рассматривается решение, подразумевающее использование системного контроллера reCAPTCHA, фильтрующего трафик с помощью проверок целостности на стороне источника. Автор дает следующее определение такому контроллеру: reCAPTCHA – это механизм ответа на вызов, который может блокировать трафик генерируемый ботом, не реагируя при этом на трафик, генерируемый реальными пользователями.

В некоторых атаках задействованы вредоносные узлы, которые участвуют в минимальном количестве взаимодействий, избегая тем самым лишнего времени простоя, задерживаясь с частичными запросами и ответами. Такие атаки потребляют ресурсы защищаемого объекта и замедляют работу приложений, что в конечном итоге приводит к невозможности обработки сообщений. Данный тип атак именуют «low and slow», поскольку сравнительно небольшое количество злоумышленников может принять участие в DDoS-атаке незаметно и медленно, без какого-либо значительного потребления полосы пропускания в сети. В наши дни они стали обычным явлением. Для реализации предложенного метода контроллера reCAPTCHA настройка правил является основным этапом для ограничения неавторизованного доступа в сети.

Поведение пользователей анализируется на предмет обнаружения вредоносных узлов. Поведение пользователя представлено количеством запросов на доступ к ресурсам, которое определяется по матрице частот порядка . Здесь, N обозначает количество запросов, а  *dw* – окно обнаружения. Каждая запись в матрице обозначается Fij для определения частоты соответствия правил входящим пакетам в каждом окне обнаружения. Согласно теории информации, метрическая энтропия - это мера неопределенности и случайности, связанная с переменной (случайной). Она измеряет информацию, содержащуюся в срезе данных. Энтропию наблюдений можно рассчитать как раз из ковариационной матрицы. Порог энтропии же определяется распределением энтропии. Здесь мы также можем рассмотреть записи в то время, когда DDoS-атака произошла в прошлом. Теперь эту систему можно использовать для обнаружения вредоносных программ путем сравнения текущей энтропии с пороговой энтропией. Для реализации этой техники контроллера reCAPTCHA используются различные параметры моделирования.

 Рисунок 4 – Блок-схема алгоритма использования контроллера reCAPTCHA

Резюмируя приводимые в статье рассуждения об использовании контроллера reCAPTCHA, мы с уверенностью можем заявить о том, что предлагаемый контроллер не смотря на имеющиеся недостатки в силу новизны является крайне эффективным с точки зрения безопасности и производительности, что подтверждается обширными экспериментами, проиллюстрированными в статье. Основными недостатками данного метода являются недостаточная изученность в силу новизны и ограниченная область применения, так как защита реализуется с целью обнаружения и предотвращения вторжений со стороны ботов, а значит против злоумышленников, лично осуществляющих вторжения данный метод бесполезен. Помимо прочего в наши дни существуют методы обхода reCAPTCHA, такие как использование аудиоверсии с машинным преобразованием голоса в текст и последующим получением доступа, а также удаленное решение специальным работником через различные сервисы.

3.4 Использование гибридной оптимизации данных на основе машинного обучения для СОВ. [Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms (hindawi.com)](https://www.hindawi.com/journals/scn/2019/7130868/)[8]. В данной статье предлагается оптимизировать данные, с которыми работает любая СОВ. Реализация данной идеи основывается на применении гибридной оптимизации.

В сети нормальное поведение пользователей - это нечто большее, чем аномальное поведение, что делает распределение данных о нормальном и аномальном поведении несбалансированным. Чтобы повысить эффективность обнаружения IDS, в статье предлагается гибридный метод оптимизации данных, основанный на множественных алгоритмах машинного обучения. Метод оптимизации данных состоит из двух частей: выборки данных и выбора признаков. В рассматриваемом решении метод обнаружения выбросов iForest используется для выборки данных, GA используется для оптимизации коэффициента выборки в глобальном масштабе, а эффективность классификации RF по выборочным данным кандидатов используется в качестве индикатора оценки. Целью выборки данных является поиск оптимального набора обучающих данных и уменьшение дисбаланса набора данных. Что касается выбора характеристик, в статье метод интеграции GA с RF используется для выбора функций. Подобно выборке данных, GA используется в качестве стратегии поиска для определения подмножества функций-кандидатов, а эффективность классификации RF служит индикатором оценки подмножества функций-кандидатов. Цель выбора функций - найти лучшее подмножество функций, которое может максимизировать производительность обнаружения. После выбора оптимального набора обучающих данных и оптимального подмножества признаков они будут приняты на этапе обучения классификатора, который использует алгоритм RF. Весь процесс показан на рисунке 5.

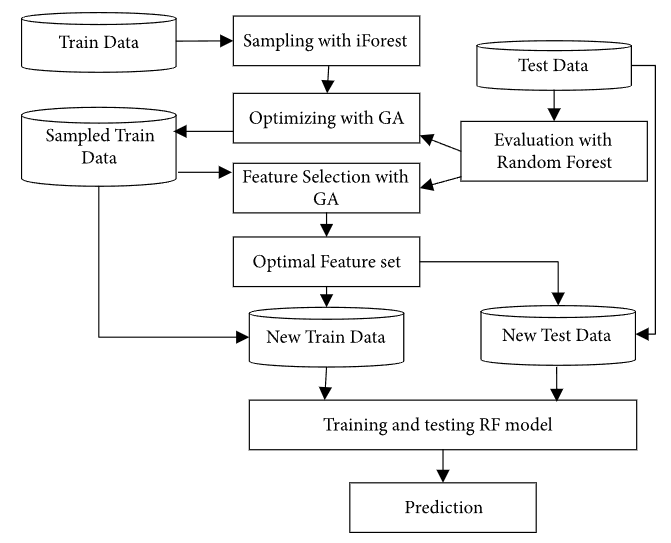


Рисунок 5 – Процесс гибридной оптимизации данных

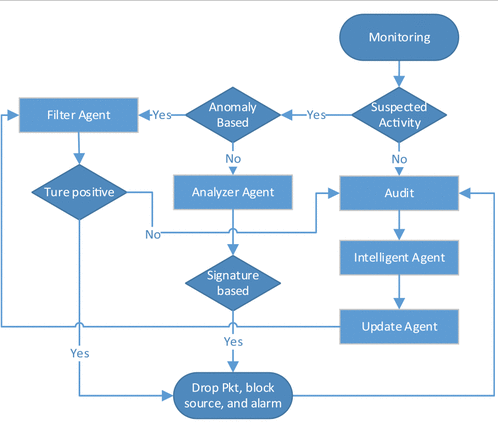
Подводя итоги по данной статье, можно сделать вывод о том, что RF-классификатор является наиболее сильным классификатором среди остальных, а гибридная оптимизация позволяет значительно повысить как производительность, так и эффективность СОВ. Следовательно, объединенный эффект гибридной оптимизации и RF-классификатора делает предложенное решение одним из лучших по всем основным параметрам, особенно при обнаружении аномального поведения с небольшим количеством записей, например, Dos атак, несанкционированного анализа системы, бэкдора и червей. Тем не менее, есть улучшения, на которых можно сосредоточиться, например, большие временные затраты на этапе оптимизации данных и поддержка онлайн-обработки.

3.5 Построение адаптивной СОВ. [An adaptive intrusion detection and prevention system for Internet of Things - Sheikh Tahir Bakhsh, Saleh Alghamdi, Rayan A Alsemmeari, Syed Raheel Hassan, 2019 (sagepub.com)](https://journals.sagepub.com/doi/full/10.1177/1550147719888109)[9]. В данной статье речь и идет о построении адаптивной системе обнаружения и предотвращения вторжений для интернета вещей.

Предлагаемый IDPIoT основан на агентской технологии для поддержки мобильности, жесткости и самозапуска атрибутов. Из-за ограничений Интернета вещей предлагаемое решение реализуется посередине между устройствами Интернета вещей и маршрутизатором, который можно установить в шлюз. Предлагаемый IDPIoT представляет собой гибридное решение, поскольку оно основано на неправильном использовании и аномалиях. Экземпляр агента предотвращения, отправленный для предотвращения на устройствах IoT в случае атаки или вторжения, чтобы изолировать IoT от защищенной сети, пока она не будет вылечена. [Рисунок](https://journals.sagepub.com/doi/full/10.1177/1550147719888109) 6 показывает, что агент монитора отвечает за получение пакета из сети и передачу его агенту-детектору, где агент-детектор отвечает за обнаружение любой подозрительной активности и затем передает его анализатору или фильтру на основе активности подозрения (аномалии или на основе подписи).


                        фигура
                    Рисунок 6 – Системные взаимодействия

Агент-анализатор работает в активном (в реальном времени) и пассивном режимах, он отвечает за проверку пакета и решает, является ли он нормальным пакетом или угрозой, на основе двух подходов: на основе сигнатур или на основе аномалий. Если он решает, что это нормальный пакет или поведение, то он проходит через агент фильтрации. Агент фильтрации решает, является ли он ложноположительным или истинно-положительным; если он ложноположительный, тревога не генерируется; если истинно положительный, будет сгенерирован сигнал тревоги, и агент предотвращения предпримет действия. Если есть подозрительное вторжение или угроза, срабатывает сигнал тревоги для пользователя с правами администратора, пакет отбрасывается, а источник пакета блокируется агентом предотвращения. Менеджер предотвращения несет ответственность за действия по защите устройств IoT, в случае диспетчера предотвращения DoS, он отправляет экземпляр в целевой IoT, чтобы сбросить соединение или пакет злоумышленника. Интеллектуальный агент - это то место, где агент может учиться у агента аудита в течение срока службы системы и может оказывать поддержку позже для предотвращения или обновления анализатора и агентов фильтрации. Агент обновления данных отвечает за обновление правил и политик фильтров и анализаторов, а также обновляется интеллектуальным агентом. Агент аудита - это то место, где все действия и события регистрируются в этом агенте. Генератор отчетов может создавать периодические отчеты системы в зависимости от конфигурации пользователя. В предлагаемом решении программное обеспечение устанавливается на оборудование для обнаружения вторжений и подключается к маршрутизатору и устройствам IoT для управления трафиком и обеспечения мониторинга всей связи между IoT и Интернетом. Это посредник между маршрутизатором и подключением IoT-устройств, разрешенным только от IDS. Таким образом, агент может путешествовать, чтобы выполнить профилактику устройств IoT и изолировать их от сети, чтобы предотвратить вторжение или атаки. Агент также может быть установлен на каждом устройстве IoT, поскольку он может работать асинхронно. Пользователи могут получить доступ к IoT через облако, промежуточное программное обеспечение может быть установлено в облаке. [Рисунок](https://journals.sagepub.com/doi/full/10.1177/1550147719888109) 7 показывает системный компонент Radius/NAP, который является сервером/службой удаленных пользователей с телефонным подключением. Защита доступа к сети может использоваться для аутентификации устройств IoT. Межсетевой экран для добавления дополнительного уровня защиты может быть интегрирован с предлагаемой системой. Система обнаружения и предотвращения вторжений основана на гибридном методе обнаружения. IPSec – это набор защищенных сетевых протоколов, который аутентифицирует и шифрует пакеты данных, отправляемые по сети Интернет-протокола, для защиты и шифрования связи между IoT и конечным пользователем.

 Рисунок 7 – Диаграмма деятельности системы

В предлагаемом решении два возможных сценария показаны на [рисунке 8.](https://journals.sagepub.com/doi/full/10.1177/1550147719888109) Во-первых, злоумышленник может попытаться вмешаться в беспроводную сеть, чтобы атаковать устройства Интернета вещей или сеть или выдать себя за другое лицо. Таким образом, в этом решении мы реализуем RADIUS для аутентификации подключенных устройств к беспроводной сети, чтобы гарантировать, что к сети подключены только легитимные устройства. Во-вторых, злоумышленник может попытаться выдать себя за устройство IoT, используя SIM-карту модуля идентификации абонента для подключения через абонентов сотовой связи к сети. Таким образом, наша система способна обнаруживать такое вторжение и действовать для предотвращения этого злоумышленника, отбрасывая пакеты злоумышленников и блокируя источник пакета. Таким образом, это может помочь в построении доверия между сервисом и сетью на основе сетей 5G, как показано на [Рисунке 9](https://journals.sagepub.com/doi/full/10.1177/1550147719888109). Кроме того, его можно интегрировать с брандмауэром, чтобы он мог обновлять правила и политики брандмауэра.

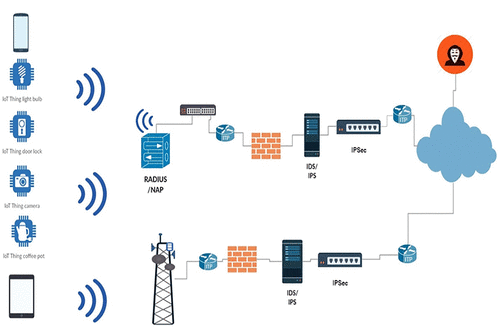


Рисунок 8 – Развертывание системы

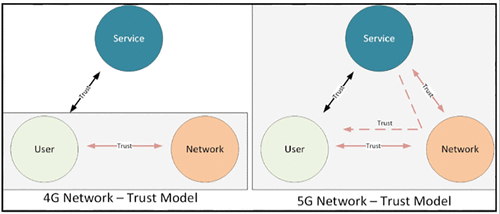


Рисунок 9 – Сетевое доверие

Анализируя материалы данной статьи, делаем вывод о том, что данный метод имеет огромные перспективы в силу чрезвычайной актуальности и эффективности решения, достигаемой обеспечением защиты от атак в реальном времени и предоставлением возможности изолировать серверы. Необходимость реализации и оценки данного метода в реальных системах, помимо прочего, обуславливается возможностью защитить связь между сервисами и сетью 5G, а также возможностью укрепить доверие между ними. Огромным недостатком данного метода, очевидно, является отсутствие прототипов, испытанных на реальных системах, так как данный факт поражает вероятность опровержения теоретической эффективности предложенного решения.

1. Сравнительный анализ методов построения СОВ

Сравнивать приведенные в работе методы построения систем обнаружения/предотвращения вторжений довольно трудно, так как каждый из них изначально еще на стадии разработке должен соответствовать задачам, которые ставятся разработчикам в ТЗ. Очевидно, что часто эти задачи противоречат друг другу, однако также часто они пересекаются. Последними случаями мы и воспользуемся для достижения объективности сравнительного анализа.

Прежде всего стоит отметить, что все методы имеют огромный потенциал в сфере компьютерной безопасности, однако в ходе работы выяснилось, что универсальных и безотказных решений попросту не существует. Так, например, реализация глубокого обучения при построении СОВ чревата ошибками, связанными с ложными срабатываниями, поэтому в случаях, когда такие ошибки недопустимы или крайне нежелательны, разумным решением будет реализация быстрого обучения.

В случаях, когда основной задачей СОВ является борьба с Dos атаками и другим негативным влиянием ботов на защищаемый объект, наиболее подходящим решением будет применение контроллера reCAPTCHA. В противном случае, когда необходима защита от реальных пользователей, намеренных оказать негативное воздействие на защищаемый объект, данный метод абсолютно бесполезен, следовательно, стоит выбирать иной путь решения данной задачи.

Для обнаружения аномального поведения с небольшим количеством записей лучшим решением можно считать использование гибридной оптимизации данных на основе машинного обучения. В случаях, когда количество записей значительно больше, чем способны данные системы стоит обратить внимание на построение адаптивной СОВ. Однако прежде, чем приступить к реализации, стоит оценить риски нужно учесть тот факт, что данное решение не было до конца изучено и не имеет фактического подтверждения своей эффективности в силу отсутствия проведенных испытаний на реальных системах.

*В заключение*, изучив приведенные в работы статьи, можно сделать вывод о том, что СОВ может иметь несколько возможных исполнений: сетевая, протокольная, узловая, гибридная, сигнатурная, корреляционная и другие. Исполнение СОВ является наиболее значимым критерием при сравнении методов построения СОВ, так как от этого зависит направленность, совместимость, отказоустойчивость и другие важнейшие свойства СОВ, однако существуют и другие критерии, такие как, например, метод определения атак, наличие активного режима и кроссплатформенность. Среди рассмотренных методов построения СОВ наиболее популярным исполнением оказалось построение гибридной системы. Подводя итоги проведенного сравнительного анализа методов построения СОВ, делаем вывод о том, что прежде всего при выборе решения необходимо учитывать задачи, которые СОВ должна решать. Стоит также отметить, что почти все современные решения требуют доработки и более глубокого изучения для достижения наибольшей эффективности. При этом одни имеют больший потенциал для модернизации, другие – меньший; и за какое решение браться – решать уже ученым и разработчикам.

**Список источников**

[1]: Ш. А. Акбарова, А. А. Ганиев. — Молодой ученый, 2017.

[2]: М. О. Максудов, И. Е. Дорошенко, А. С. Грехов, Д. Г. Макарова – Актуальность разработки СОВ, 2020.

[3]: [A Survey on Intrusion Detection System(IDS)](http://www.ijtrm.com/PublishedPaper/5Vol/Issue7/2018IJTRM7201815907-0b85b8a6-2929-4b4a-995c-1aa15c78c79819620.pdf) | Department of Computer Science & Engineering SKSITS – Priyanka Alekar, 2018

[4]: [Comparing Intrusion Detection Systems (IDS1) and Intrusion Prevention Systems (IPS) | Engineering Education Program – [Eric Kahuha](https://www.section.io/engineering-education/authors/eric-kahuha/), 2020](https://www.section.io/engineering-education/comparing-intrusion-detection-systems-ids-and-intrusion-prevention-systems-ips/)

[5]: [Deep Learning Approach for Intelligent Intrusion Detection System | IEEE Journals & Magazine](https://ieeexplore.ieee.org/abstract/document/8681044) – [R. Vinayakumar](https://ieeexplore.ieee.org/author/37086229174), [Mamoun Alazab](https://ieeexplore.ieee.org/author/37601552300), [K. P. Soman](https://ieeexplore.ieee.org/author/37296443000), [Prabaharan Poornachandran](https://ieeexplore.ieee.org/author/37085564830), [Ameer Al-Nemrat, 2019](https://ieeexplore.ieee.org/author/37085539337)

[6]: [A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization | IEEE Journals & Magazine | IEEE Xplore](https://ieeexplore.ieee.org/abstract/document/8326489) – [Mohammed Hasan Ali](https://ieeexplore.ieee.org/author/37086366504), [Bahaa Abbas Dawood Al Mohammed](https://ieeexplore.ieee.org/author/37086365954), 2018

[7]: [Intrusion Prevention System with reCAPTCHA controller using IBM | IEEE Journals & Magazine - [M. Poongodi](https://ieeexplore.ieee.org/author/37087084862), [V. Vijayakumar](https://ieeexplore.ieee.org/author/37086454377), [Fadi Al-Turjman](https://ieeexplore.ieee.org/author/38273345000), [Mounir Hamdi](https://ieeexplore.ieee.org/author/37272053300), [Maode Ma](https://ieeexplore.ieee.org/author/37280212000)](https://ieeexplore.ieee.org/abstract/document/8859299), 2019

[8]: [Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms – Mamoun Alazab, 2019](https://www.hindawi.com/journals/scn/2019/7130868/)

[9]: [An adaptive intrusion detection and prevention system for Internet of Things - Sheikh Tahir Bakhsh, Saleh Alghamdi, Rayan A Alsemmeari, Syed Raheel Hassan, 2019](https://journals.sagepub.com/doi/full/10.1177/1550147719888109).