DOI 10.37882/2223-2966.2023.7-2.04

# СОВРЕМЕННОЕ СОСТОЯНИЕ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ МЕТОДОВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## CURRENT STATUS AND DIRECTIONS FOR IMPROVING METHODS FOR DETECTING INFORMATION SECURITY INCIDENTS

***M. Valeev***

*Summary*: The article proposes to consider the issues of unauthorized access to protected information in a local area network, the development of attack methods and the current state of intrusion detection systems at the network level. The paper considers the features of using the SIEM information security event collection and correlation system and the need to improve information protection methods. In this paper, the author presents an analysis of the main advantages and disadvantages of systems for preventing possible information security incidents and fulfilling state requirements in the field of protecting critical information infrastructure. In the course of the study, methods for detecting intrusions in the corporate segment of an information system are presented, models of a network and host intrusion detection system are presented. By classifying information security events received from various systems, it is possible to draw a conclusion about the state of the entire protected object in real time.

*Keywords*: intrusion detection system, information security, unauthorized access, information security software, SIEM systems methodology, source of information security events, behavioral analysis.

***Валеев Михаил Владимирович***
*Аспирант, Финансовый университет при Правительстве Российской Федерации*
*waleew.miha@hotmail.com*

*Аннотация*. В статье предлагается рассмотреть вопросы несанкционированного доступа к защищаемой информации в локально-вычислительной сети, развития способов проведения атак и современного состояния систем обнаружения вторжений на сетевом уровне. В работе рассмотрены особенности использования системы сбора и корреляции событий информационной безопасности SIEM и необходимость совершенствования методов защиты информации. В настоящей работе автором представлен анализ по основным преимуществам и недостаткам систем предотвращения возможных инцидентов информационной безопасности и выполнения требований государства в области защиты критической информационной инфраструктуры. В ходе исследования приведены методики обнаружения вторжений в корпоративный сегмент информационной системы, представлены модели сетевой и хостовой системы обнаружения вторжений. Классифицируя события информационной безопасности, полученные из различных систем, возможно сделать вывод о состоянии всего объекта защиты в режиме реального времени.

*Ключевые слова*: система обнаружения вторжений, защита информации, несанкционированный доступ, программные средства защиты информации, SIEM-системы методика, источник событий информационной безопасности, поведенческий анализ.

## Введение

В эпоху цифровой трансформации и массового использования информационных технологий, организации сталкиваются с угрозами, которые могут нанести им значительный ущерб [1]. Кибератаки, утечки данных, вредоносные программы — все это лишь некоторые примеры инцидентов информационной безопасности, которые могут привести к серьезным финансовым и репутационным потерям. Поэтому понимание и эффективное управление рисками информационной безопасности становятся важнейшими задачами для организаций всех масштабов и отраслей.

За последние годы уровень угроз информационной безопасности значительно возрос, причем это касается как общественных, так и частных компаний. Насколько массовым стало явление нарушения ИБ, свидетельствует поразительная статистика, демонстрирующая, что инциденты информационной безопасности происходят в среднем 2–3 раза в месяц в сфере бизнеса, что приводит к огромным финансовым потерям [2]. Именно поэтому ежегодно компании вкладывают миллиарды рублей в системы защиты информации и встроенные программные средства, чтобы улучшать методы выявления инцидентов информационной безопасности и предотвращать их возникновение.

Одним из методов предотвращения инцидентов информационной безопасности является инвестиция в системы защиты информации. Некоторые существенные улучшения, полученные сейчас в этой области, связаны с использованием новейших технологий, таких как искусственный интеллект, блокчейн и машинное обучение. С их помощью можно определить новые угрозы, понимать, какие уязвимости стоит закрыть, и реагировать на инциденты быстрее, чем раньше [3].

Безусловным преимуществом новых систем являются их возможности по самообучению. С помощью машинного обучения, системы могут обновляться без участия оператора, что повышает скорость обучения

и делает их более эффективными в противодействии новым угрозам. С использованием блокчейн-технологий исключается возможность манипуляции данными, а искусственный интеллект может предотвращать атаки в режиме реального времени.

Однако, несмотря на значительный прогресс в этой области, необходимо учитывать, что методы выявления инцидентов информационной безопасности все еще являются очень сложными и могут быть неэффективными. Во-первых, многие компании не имеют запасных копий данных или планов аварийной эвакуации, что может привести к большим потерям в случае успешной атаки. Во-вторых, компании должны обеспечить наиболее важные с точки зрения информационной безопасности данные максимальной защитой, чтобы предотвратить утечку конфиденциальной информации.

Также значительное значение имеет эффективное обучение сотрудников компании в области информационной безопасности. Большинство атак происходят из-за ошибок персонала, поэтому обучение управляемому поведению в информационной системе и обучение безопасности в Интернете являются очень важными компонентами как для обеспечения защиты компании, так и для персональной безопасности.

Все большее количество организаций сталкивается с инцидентами информационной безопасности, что приводит к значительным материальным и репутационным потерям. Для защиты информации от киберугроз необходимо использование современных методов и технологий, чтобы обнаруживать и предотвращать возможные нарушения безопасности [5]. В данной статье рассматривается современное состояние и направления совершенствования методов выявления инцидентов информационной безопасности. В настоящее время существует несколько основных методов выявления инцидентов информационной безопасности:

— системы обнаружения вторжений (IDS);
— системы обнаружения аномалий (ADS);
— системы управления событиями безопасности (SIEM).

Системы обнаружения вторжений — это программные продукты, которые контролируют сетевой трафик и обнаруживают вторжения в систему. Они осуществляют анализ трафика на наличие признаков опасного поведения и выдают предупреждающие сообщения руководству. Системы обнаружения аномалий используются для обнаружения нестандартных и аномальных действий пользователей, которые могут являться признаками нарушения безопасности. Также они способны распознавать новые вирусы и использовать алгоритмы машинного обучения для определения подозрительных узлов сети. Системы управления событиями безопасности — это инструменты, которые собирают и анализируют данные из различных источников, таких как логи истории пользовательских действий, системные события и базы данных угроз. Они имеют возможность отслеживать события и создавать отчеты о произошедшем инциденте.

Несмотря на то, что перечисленные методы являются эффективными для выявления инцидентов информационной безопасности, они имеют свои ограничения [6]. Например, IDS и ADS могут давать ложноположительные и ложноотрицательные результаты, а SIEM не может обрабатывать большие объемы данных в режиме реального времени. Эти недостатки подталкивают к совершенствованию методов выявления инцидентов информационной безопасности.

Направления совершенствования методов выявления инцидентов информационной безопасности:

— применение машинного обучения;
— использование анализа больших данных;
— развитие технологий интеллектуальной защиты.

Говоря о применении машинного обучения, то это направление развития систем IDS и ADS, чтобы они могли с большей точностью определять наличие угроз. Методы машинного обучения, такие как нейронные сети и алгоритмы классификации, могут улучшить точность определения угроз и снизить число ложноположительных и ложноотрицательных результатов [7]. При использовании анализа больших данных мы говорим о новом направлении совершенствования методов SIEM, что в свою очередь позволяет сократить время обработки большого объема информации, а также увеличить точность определения угроз [8]. Технологии, такие как Hadoop и Apache Spark, могут быть использованы для обработки больших объемов данных в режиме реального времени. Ну и, наконец-то, говоря о развитии технологий интеллектуальной защиты мы имеем в виду такое направление развития методов защиты информации, которое позволяет создавать автоматические защитные механизмы. Использование таких технологий как когнитивные вычисления и нейронные сети могут нам помочь в повышении уровня безопасности информации [9].

Вышеописанные методы выявления инцидентов информационной безопасности являются эффективными средствами защиты информации. Однако, недостатки таких методов побуждают специалистов в области информационной безопасности к поиску новых решений и развитию уже существующих технологий. Таким образом, совершенствование методов выявления инцидентов информационной безопасности должно быть актуальным направлением развития ИТ-индустрии в ближайшие годы.

## Материалы и методы

В настоящее время, когда информационные технологии позволяют обмениваться данными между компьютерами по всему миру, кибербезопасность становится одной из наиболее важных задач. В этой связи, системы обнаружения вторжений (СОВ) являются неотъемлемой частью комплекса мероприятий по обеспечению безопасности информации.

СОВ предназначены для мониторинга системы и обнаружения любых попыток несанкционированного доступа. Эти системы работают на принципе обнаружения аномалий, то есть атак, отличающихся от нормального поведения пользователя. Также СОВ могут обнаруживать вирусы, трояны и другие вредоносные программы.

Существует два основных типа СОВ: сетевые и хост-ориентированные. Сетевые СОВ мониторят сетевой трафик и обнаруживают аномалии на уровне соединения, транспортном и прикладном уровнях. Хост-ориентированные СОВ работают внутри операционной системы и мониторят поведение процессов, файловой системы, реестра и других компонент системы.

Для обнаружения аномальных событий в сетевом трафике, существует несколько методов, таких как: анализ подписей, статистический анализ, анализ поведения и другие. Анализ подписей заключается в поиске в трафике заранее известных сигнатур известных вирусов и других угроз. Статистический анализ основан на сравнении статистических данных трафика с заранее определенными параметрами нормальной деятельности сети. Анализ поведения заключается в построении профилей поведения пользователя и обнаружении несоответствия с этими профилями.

Хост-ориентированные СОВ используются для мониторинга процессов и действий внутри операционной системы. Это позволяет обнаруживать такие вещи, как изменение файловой системы, реестра и поведение процессов, что может указывать на наличие вредоносного кода в системе. В хост-ориентированных СОВ используются методы анализа поведения процессов, анализа сигнатур и анализа поведения файловой системы и реестра.

Одним из главных достоинств СОВ является их способность к интеграции с другими системами безопасности, таких как межсетевые экраны, антивирусные программы и т.д. Это позволяет строить комплексную систему защиты информации от множества угроз.

Однако, несмотря на все предпринятые меры, системы обнаружения вторжений не являются идеальными и могут давать ложные срабатывания. Также, если злоумышленник обладает достаточной квалификацией и использует новейшие методы атаки, то СОВ могут быть бесполезными.

Системы обнаружения аномалий (англ. anomaly detection systems) — это программные инструменты, предназначенные для выявления аномальных поведенческих паттернов в данных. Под аномалией понимается отклонение от нормального или ожидаемого поведения системы или предмета, что может указывать на наличие проблемы, ошибки или нарушения безопасности [10].

Применение систем обнаружения аномалий может быть широким и разнообразным. Например, такие системы могут использоваться для защиты корпоративных сетей и информационных систем от кибератак, защиты банковских транзакций от мошеннической деятельности, определения машинных отказов и проблем в производственных цепочках, контроля за безопасностью систем управления транспортными потоками и т.д.

Системы обнаружения аномалий основаны на анализе больших объемов данных, что позволяет выявлять скрытые корреляции и зависимости между переменными. Для этого могут применяться различные методы анализа данных, такие как статистический анализ, машинное обучение, искусственные нейронные сети и др.

Важными характеристиками систем обнаружения аномалий являются скорость и точность выявления аномалий. Системы должны быть быстрыми и эффективными, чтобы в режиме реального времени обрабатывать большие объемы данных и оперативно предупреждать о возможных проблемах. Точность выявления аномалий также имеет большое значение, чтобы избежать ложных срабатываний и неправильных диагностик.

Системы обнаружения аномалий могут использоваться как самостоятельные инструменты, так и в комплексе с другими технологиями [11]. Например, можно комбинировать системы обнаружения аномалий с системами мониторинга, чтобы обеспечить комплексный контроль за работой системы. Также можно использовать системы обнаружения аномалий для обнаружения новых угроз и вредоносных программ, а затем передавать информацию в системы защиты и блокирования.

В заключении можно сказать, что системы обнаружения аномалий — это важный инструмент для обеспечения безопасности и эффективности работы различных систем и предметов. Благодаря применению таких систем можно оперативно выявлять проблемы и предотвращать их нарушения, что является особенно важным в контексте современных технологических рисков и угроз.

Системы управления событиями безопасности (SIEM) — это комплексы программных и аппаратных средств, которые служат для обеспечения безопасности объектов. SIEM позволяют оперативно обнаруживать проблемы и реагировать на них, предупреждая открытие возможных угроз [12].

SIEM могут быть реализованы как на уровне государственных объектов, так и на уровне предприятий и организаций. Они являются необходимыми для обеспечения безопасности крупных объектов, таких как аэропорты, железные дороги, общественный транспорт, учреждения здравоохранения и т.д.

Системы управления событиями безопасности включают в себя набор мер по предотвращению и управлению последствиями различных угроз. Они предоставляются в виде комплекса программных средств, которые позволяют оперативно реагировать на возможные угрозы. Это могут быть следующие проблемы:

— угрозы кибербезопасности — хакерские атаки, сбои в работе сетевого оборудования, утечки конфиденциальных данных и т.д.;
— угрозы природных катастроф — наводнения, землетрясения, тайфуны, наводнения и т.д.;
— угрозы преступности — грабежи, нападения на персонал организации, мошенничество и т.д.;
— угрозы здоровью и безопасности — пожары, взрывы, аварии, террористические акты и т.д.
— SIEM состоит из следующих компонентов:
— датчики — средства, которые считывают информацию об изменении окружающей среды, данные о температуре, влажности, освещенности и т.д.;
— контроллеры — устройства, которые анализируют полученную информацию и принимают решение о том, какую меру необходимо принять в зависимости от ситуации;
— коммуникационные модули — устройства, которые обеспечивают связь между датчиками, контроллерами и другими устройствами системы;
— программное обеспечение — комплекс программ, которые обрабатывают и анализируют данные, полученные от датчиков и контроллеров.
— SIEM можно подавать несколько видов:
— локальные SIEM — предназначены для охраны отдельных зданий и территорий организаций;
— зональные SIEM — решают задачи обеспечения безопасности крупных территорий, таких как аэропорты, гостиницы, крупные промышленные объекты и т.д.;
— глобальные SIEM — служат для обеспечения безопасности национальных объектов и территорий, таких как государственные границы, ядерные электростанции и т.д.

SIEM имеет множество преимуществ. Во-первых, они позволяют оперативно реагировать на возникающие проблемы и устранять их в их самом раннем состоянии. Во-вторых, они повышают уровень безопасности объектов и сокращают риски потери имущества и возможных угроз жизни людей. В-третьих, SIEM дают возможность улучшить эффективность работы организации и повысить уровень ее производительности.

Таким образом, системы управления событиями безопасности являются неотъемлемой частью обеспечения безопасности крупных объектов и территорий. Они обеспечивают быстрое реагирование на возникающие проблемы и помогают снизить риски потерь и угроз жизни.

С ростом онлайн-активности и использования цифровых технологий, проблема информационной безопасности (ИБ) становится все более актуальной. Активное использование технологий ведет к росту количества информации, которую нужно обрабатывать и защищать. Один из важных аспектов ИБ — это выявление инцидентов безопасности. Зачастую несанкционированные действия могут произойти без заметных признаков, поэтому для обнаружения инцидентов применяются различные методы и алгоритмы, в том числе и машинное обучение.

Машинное обучение (Machine learning) — это подход, который позволяет компьютерной системе научиться решать задачи путем анализа и обработки данных без явного программирования. С помощью машинного обучения можно совершенствовать методы выявления инцидентов ИБ, увеличивая точность и скорость обнаружения [13].

Одним из основных подходов машинного обучения является обучение с учителем (Supervised learning). При таком подходе учатся распознавать различные виды данных, используя предварительно размеченные образцы (метки). Примером этого является классификация текстов, поправок на изображениях и многое другое. В задаче ИБ, можно использовать обучение с учителем с целью определения типов инцидентов, анализа вредоносного поведения и классификации типов сетевой атаки.

Другим подходом машинного обучения является обучение без учителя (Unsupervised learning). В данном случае, система получает данные на вход без каких-либо меток и самостоятельно выявляет закономерности и шаблоны в них. Этот подход может быть использован для анализа сетевой активности и выявления потенциально вредоносного поведения [14]. К примеру, можно использовать метод кластеризации, при котором данные разбиваются на определенное количество групп в зависимости от характеристик. Это позволит определить необычное поведение в сети и заблаговременно предотвратить возможную атаку.

Еще одним интересным подходом машинного обучения является обучение с подкреплением (Reinforcement learning). В данном случае, система обучается на основе наград и наказаний за выполнение или не выполнение определенных действий. Этот подход может быть использован для обучения системы быстрому реагированию на определенные инциденты безопасности.

Применение машинного обучения в ИБ также позволяет автоматизировать процессы обнаружения аномальной сетевой активности. Такие системы называются системами обнаружения вторжений (Intrusion detection system или IDS). Они используют различные методы машинного обучения для автоматического обнаружения вредоносного поведения в сети. IDS может быть ориентирован на различные типы вредоносных действий в сети, например, на атаки типа «человек по середине» и другие. Системы машинного обучения позволяют сократить время и уменьшить возможность ошибок в процессе анализа сетевой активности, что существенно повышает защиту от инцидентов ИБ.

Машинное обучение является мощным инструментом для выявления инцидентов ИБ. С его помощью можно совершенствовать методы анализа сетевой активности, классификации типов атак и выявления аномального поведения в сети. Благодаря машинному обучению, системы защиты от ИБ становятся более точными и быстрыми, что позволяет существенно повысить уровень безопасности информации. Однако, необходимо помнить, что машинное обучение не является универсальным решением для защиты от ИБ и должно использоваться в сочетании с другими методами защиты.

В настоящее время информационная безопасность (ИБ) является приоритетной задачей для многих организаций. Многие компании инвестируют большие деньги в ИБ, но не всегда эти инвестиции дают желаемый эффект. Одной из причин этого является то, что угрозы ИБ меняются очень быстро. Поэтому необходимо совершенствовать методы выявления инцидентов ИБ, используя современные инструменты.

Анализ больших данных (Big Data) — это один из таких инструментов. Он позволяет собирать связанные с ИБ данные из разных источников, например, журналов безопасности, данные о доступе к системам, а также данные, полученные из социальных сетей. С помощью анализа больших данных можно выявлять скрытые связи между различными событиями в компьютерных системах, чтобы быстро выявлять угрозы безопасности [15].

Преимущества использования анализа больших данных для выявления инцидентов ИБ:

— выявление проблем, не обнаруживаемых при обычном мониторинге событий;
— снижение времени отклика на угрозы ИБ;
— создание новых методов защиты данных на основе сведений, полученных из анализа больших данных;
— повышение эффективности работы экспертов по безопасности путем сокращения времени, затрачиваемого на ручной анализ данных.

В заключение стоит отметить, что использование анализа больших данных в ИБ — это неотъемлемый элемент многих систем защиты. Технологии успешно применяются в кибербезопасности благодаря своей способности отслеживать миллионы событий в режиме реального времени и результативно обнаруживать угрозы безопасности. Таким образом, использование анализа больших данных в качестве средства выявления инцидентов ИБ является основой для совершенствования методов безопасности.

В настоящее время Интернет является неотъемлемой частью жизни большинства людей. В то время как он предоставляет значительное количество удобств и возможностей, он также приносит множество угроз для безопасности. Криминальные элементы используют Интернет как инструмент для совершения преступлений, включая взломы, кражи личных данных и попытки мошенничества.

В свете этих угроз, цифровая безопасность становится все более важной. Компании и организации должны использовать эффективные методы защиты данных и выявления инцидентов ИБ, чтобы предотвратить утечки информации и минимизировать потенциальный ущерб. Развитие технологий интеллектуальной защиты — один из ключевых инструментов для совершенствования методов выявления инцидентов ИБ.

Одним из основных преимуществ интеллектуальной защиты является способность автоматически обнаруживать и предотвращать атаки ИБ [16]. Технологии, такие как машинное обучение и искусственный интеллект, могут отслеживать действия злоумышленников и выявлять подозрительную активность на ранней стадии, что позволяет быстро реагировать на потенциальную угрозу.

Кроме того, интеллектуальная защита может помочь в анализе больших данных, связанных с безопасностью. Технологии анализа данных позволяют собирать, обрабатывать и интерпретировать большие объемы данных, связанных с безопасностью, чтобы выявлять скрытые угрозы и предсказывать вероятные направления атаки. Это позволяет компаниям принимать точные и обоснованные решения для улучшения своей защиты.

Интеллектуальная защита также может повысить уровень управления информационной безопасностью

внутри компаний. Она позволяет автоматизировать процессы, связанные с безопасностью данных, такие как мониторинг, анализ и реагирование на события ИБ. Это упрощает процесс управления рисками и взаимодействия с акционерами.

Наконец, интеллектуальная защита может быть использована для создания адаптивных защитных механизмов. Она позволяет компаниям использовать быстрое обнаружение и анализ данных для адаптации к новым угрозам ИБ. Например, алгоритмы машинного обучения могут обновляться на основе опыта и обучаться распознавать новые виды атак, которые бывают уникальными для конкретных ситуаций.

В итоге, развитие технологий интеллектуальной защиты имеет огромный потенциал для совершенствования методов выявления инцидентов ИБ. Использование этих технологий позволяет компаниям и организациям защищать свои данные и минимизировать потенциальный ущерб, причиняемый атаками ИБ.

SIEM-системы (Security Information and Event Management) являются основными инструментами для мониторинга и анализа безопасности информации в современных организациях. Они обеспечивают сбор, корреляцию и анализ информации о событиях безопасности в режиме реального времени, позволяя выявлять угрозы и принимать соответствующие меры [17]. Однако, как и любые технологии, SIEM-системы имеют свои сильные и слабые стороны. Ниже приведен SWOT-анализ современных SIEM-систем.

Сильные стороны:
— широкий диапазон определения угроз: современные SIEM-системы могут обнаруживать и анализировать различные типы угроз, такие как вирусы, хакерские атаки, DDoS-атаки и фишинг;
— развитые и гибкие функции аналитики: современные SIEM-системы обеспечивают широкий набор инструментов для анализа событий безопасности, включая машинное обучение, искусственный интеллект и множество других методов;
— возможности адаптации: SIEM-системы позволяют быстро изменять наборы правил и запросов для улучшения работы системы на основе опыта анализа предыдущих угроз;
— эффективное управление угрозами: современные SIEM-системы позволяют реагировать на угрозы в режиме реального времени, обеспечивая защиту от многих угроз без интервенции операторов.

Слабые стороны:
— высокие затраты на внедрение: SIEM-системы являются дорогостоящими решениями, которые могут требовать значительных инвестиций для их внедрения и поддержания;
— требования к производительности: SIEM-системы требуют высокой скорости обработки и анализа информации о безопасности, поэтому для их использования необходимы мощные сервера и коммуникационные сети;
— сложность управления: SIEM-системы могут сохранять большие объемы данных, что может привести к серьезным проблемам управления ресурсами, конфигурации и обслуживания;
— подверженность ложным срабатываниям: SIEM-системы могут быть склонны к ложным срабатываниям и могут требовать значительных ресурсов для анализа и принятия решений в подобных случаях.

Возможности:
— разработка новых функций: SIEM-системы с каждым годом усовершенствуются, поэтому есть возможность разработки новых функций, таких как распознавание и анализ угроз на основе блокчейн-технологии;
— использование облака: Облачные решения могут быть использованы для ускорения и упрощения процессов SIEM-анализа, уменьшения затрат на обслуживание, а также для придания более высокой мобильности и доступности;
— развитие стандартов безопасности: вместе с развитием новых типов угроз, разрабатывается и новые стандарты безопасности, что дает возможность расширения функционалов и возможностей SIEM-систем.

Угрозы:
— возможность нарушения безопасности: SIEM-системы могут также стать объектом нападения злоумышленников и кибермафии, как и любые другие решения, которые работают с данным;
— большое количество данных: увеличение количества данных, хранящихся в SIEM-системах, также может стать причиной проблем безопасности информации;
— ограниченный человеческий ресурс: человеческий ресурс, нужный для обработки аналитики, может оказаться недостаточным для обнаружения и решения конкретных угроз в реальном времени.

В целом, можно заключить, что SIEM-системы могут обеспечивать высокий уровень безопасности и защиты данных в организации, но также могут столкнуться с проблемами затрат, управления и аналитики, особенно при работе с большим объемом данных [18]. Однако, возможности разработки новых функций и внедрения облачных решений могут привести к новым возможностям для улучшения работы SIEM-систем.

Таблица 1.

SWOT-анализ основных SIEM-систем

| SWOT-анализ | Сильные стороны | Слабые стороны | Возможности | Угрозы |
|---|---|---|---|---|
| Внутренние факторы | 1. Контроль доступа к системам<br>2. Автоматическое определение и реагирование на подозрительные действия<br>3. Интеграция с другими системами безопасности | 1. Ресурсоемкость<br>2. Высокая стоимость<br>3. Сложность настройки | 1. Разработка новых функций и алгоритмов<br>2. Заключение партнерских соглашений с производителями других систем безопасности | 1. Атаки со стороны злоумышленников<br>2. Регуляторные изменения |
| Внешние факторы | 1. Широкий выбор поставщиков SIEM-систем<br>2. Удобство интеграции с другими системами безопасности<br>3. Широкий спектр индустрий, в которых используются SIEM-системы | 1. Необходимость частых обновлений<br>2. Ограничения на использование при решении определенных задач | 1. Рост спроса на SIEM-системы на мировом рынке<br>2. Прирост количества цифровых угроз | 1. Возможность перспективного сотрудничества с другими системами безопасности<br>2. Усиление конкуренции на рынке SIEM-систем |

Основные выводы в виде SWOT-анализа по современным SIEM-систем представлены в таблице 1.

По вышеприведенному анализу необходимо внести изменения для совершенствования методов обнаружения вторжений на сетевом уровне при использовании SIEM-систем [19]:

— расширить возможности сбора данных: добавление новых источников и форматов данных;
— расширить аналитические возможности: добавление новых методов анализа и машинного обучения для обнаружения угроз;
— улучшить скорость обработки и анализа данных: оптимизация алгоритмов обработки и повышение производительности оборудования;
— улучшить пользовательский интерфейс: облегчить навигацию, упростить настройку, улучшить отображение результатов;
— произвести интеграцию с другими системами безопасности: улучшение совместимости и интеграции с другими системами защиты для повышения эффективности работы;
— улучшение системы обучения и повышения квалификации пользователей: улучшение качества обучения пользователей и повышение их квалификации в области информационной безопасности;
— улучшение системы мониторинга и управления угрозами: улучшение возможностей мониторинга и быстрого реагирования на угрозы;
— разработка улучшенных моделей безопасности: разработка и внедрение новых моделей безопасности для эффективного выявления угроз и защиты информации.

ЛИТЕРАТУРА


1. Домбровская, Л.А. Современные подходы к защите информации, методы, средства и инструменты защиты / Л.А. Домбровская, Н.А. Яковлева, Р.Е. Стахно. — Электрон. текстовые дан. — Режим доступа: https://www.3minut.ru (дата обращения: 18.06.2023). — Загл. с экрана.
2. Кияев, В.И. Безопасность информационных систем / В.И. Кияев, О.Н. Граничин. — М.: Открытый Университет «ИНТУИТ», 2016. — 192 с.
3. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / В.В. Баранов, М.А. Коцыняк, О.С. Лаута, В.М. Московченко // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. — 2017. — Т. 11, № 2. — С. 11–15.
4. Российская Федерация. Законы. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». — Доступ из справ.-правовой системы «КонсультантПлюс».
5. Современные системы защиты информации от НСД // Компания «Инфозащита». — Электрон. текстовые дан. — Режим доступа: http://itprotect.ru (дата обращения: 10.06.2023). — Загл. с экрана.
6. Ежгуров В.Н., Юмашева Е.С., Бач М.А. Проблемы внедрения системы обнаружения вторжения и устранения компьютерных атак // Материалы конференции ГНИИ «Нацразвитие», Санкт -Петербург, январь, 2018. С. 19–27.
7. Сироткин Д.В., Рекунков И.С., Лазунин К.А., Ильин К.В. Технические аспекты создания системы защиты информационного пространства // Информационные войны. 2017. № 3 (43). С. 84 — 88. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ = IT Security, Том 26, № 1 (2019).
8. Столяров В. Безопасность критической информационной инфраструктуры как она есть // Системный администратор. 2018. № 1–2 (182–183). С. 10–14.
9. Бринк Х., Ричардс Д., Феверолф М. Машинное обучение. СПб.: «Питер», 2017. 336 с.
10. Самсонова В.Г., Кулинич Р.С. Сравнительный анализ систем управления информационной безопасностью и событиями безопасности // Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно -технической конференции / под. ред. В.А. Матвеева — М.: МГТУ им. Н.Э. Баумана, 2016. С. 248–253.

11. Кожевникова И.С. Анализ методов обнаружения аномалий для обнаружения сканирования портов // Молодой ученый. — 2017. — № 14. — С. 31–34. URL https://moluch.ru/archive/148/41829/ (дата обращения: 10.06.2023).
12. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 3(22). С. 84–100.
13. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1(24). С. 21–40.
14. Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН. 2018. № 2 (57). С. 211–240.
15. Василишин Н.С., Ушаков И.А, Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Аллея науки. 2018. № 6(22). С. 1012–1021.
16. Котенко И.В., Кулешов А.А., Ушаков И.А. Система сбора, хранения и обработки информации и событий безопасности на основе средств elastic stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.
17. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в siem-системах. Часть 1 // Труды СПИИРАН. 2016. № 4 (47). С. 5–27.
18. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в siem-системах. Часть 2 // Труды СПИИРАН. 2016. № 6 (49). С. 208–225.
19. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.


Журнал «Современная наука: актуальные проблемы теории и практики»