Известия СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 4. С. 30–41
LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 4. P. 30–41

УДК 004.056 Обзорная статья

https://doi.org/10.32603/2071-8985-2024-17-4-30-41

Обзор систем обнаружения вторжений

М. Аль-Тамими[1]✉, М. Б. Хассан[1], А. А. Пазников[1], М. Н. Аль-Хайкани[1], Е. Б. Альбадрави[2]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия

[2] Васит университет, Васит, Ирак

✉ almokhalad44@gmail.com

Аннотация. В эпоху цифровых технологий возрастающая зависимость от взаимосвязанных систем вызывает нарастающую тревогу в области кибербезопасности. Данная статья обращается к актуальной необходимости улучшения средств безопасности с применением систем обнаружения вторжений, подчеркивая их важную роль в анализе системных журналов и потока данных для выявления и предотвращения злонамеренных атак. Системы обнаружения вторжений (СОВ) играют ключевую роль в укреплении сетей от потенциальных угроз, обеспечивая фундаментальный уровень защиты для персональных данных, приложений и бизнес-транзакций. В статье рассматриваются механизмы функционирования систем обнаружения вторжений, их классификации, алгоритмы, а также их преимущества и недостатки. Обсуждаются общие цели, общие структуры сигнатурных систем обнаружения вторжений, аномалии и гибридные системы обнаружения вторжений. Заключительный раздел объединяет основные результаты, формулируя всесторонние выводы о сложном пейзаже систем обнаружения вторжений.

Ключевые слова: система обнаружения вторжений, сигнатурное обнаружение, обнаружение аномалий, гибридная система обнаружения вторжений

Для цитирования: Обзор систем обнаружения вторжений / М. Аль-Тамими, М. Б. Хассан, А. А. Пазников, М. Н. Аль-Хайкани, Е. Б. Альбадрави // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 4. С. 30–41. doi: 10.32603/2071-8985-2024-17-4-30-41.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Review article

Review of Intrusion Detection Systems

M. Al-Tameemi[1]✉, M. B. Hassan[1], A. A. Paznikov[1], M. N. Al-Khaykanee[1], E. B. Albadrawi[2]

[1] Saint Petersburg Electrotechnical University, Saint Petersburg, Russia

[2] Wasit University, Wasit, Iraq

✉ almokhalad44@gmail.com

Abstract. In the modern digital era, the escalating dependence on interconnected systems raises growing concerns in the field of cybersecurity. This article addresses the pressing need to enhance security measures using Intrusion Detection Systems (IDS), emphasizing their role in the analysis of system logs and data streams to detect and prevent malicious attacks. Intrusion Detection Systems play a crucial role in fortifying networks against potential threats, providing a fundamental level of protection for personal data, applications, and business transactions. The article explores the mechanisms of operation of Intrusion Detection Systems, their classifications, algorithms, as well as their advantages and disadvantages. Structured sequentially, the article commences with an introduction, followed by discussions on the common goals, general structure, signature-based intrusion detection systems, anomaly detection systems, and hybrid intrusion detection systems. The concluding section consolidates the key findings, formulating comprehensive conclusions about the intricate landscape of intrusion detection systems.

Keywords: intrusion detection system, signature-based detection, anomaly detection, hybrid intrusion detection system

For citation: Review of Intrusion Detection Systems / M. Al-Tameemi, M. B. Hassan, A. A. Paznikov, M. N. Al-Khaykanee, E. B. Albadrawi // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 4. P. 30–41. doi: 10.32603/2071-8985-2024-17-4-30-41.

Conflict of interest. The authors declare no conflicts of interest.

Введение. Современный цифровой ландшафт характеризуется увеличивающейся взаимосвязью, вызывая значительные опасения из-за растущей зависимости от компьютерной и сетевой взаимосвязи в различных аспектах повседневной жизни. Это стало причиной повышенного внимания к защите сетей и систем. Неотложность улучшения мер безопасности и систематической документации кибератак сопровождается тщательным анализом для разработки решений против внешних угроз, вторжений и сложных уязвимостей, подчеркивается нарастающей распространенностью вычислительных устройств. Эти устройства играют важную роль в различных аспектах ежедневного существования. Основная цель использования систем обнаружения вторжений (СОВ) заключается в анализе и аудите системных журналов, данных, передаваемых в сети, и мониторинге других соответствующих источников данных. Эта усиливающаяся деятельность направлена на выявление и предотвращение злонамеренных атак на сеть, а также на предотвращение несанкционированного доступа к чувствительным данным. Достижение этой цели включает в себя корреляцию поведения системы с записями истории атак и накопленным опытом. Через тщательное изучение поведения данных механизмы обнаружения вторжений могут принимать обоснованные решения относительно наличия атаки на сеть и последующих действий для защиты целостности данных. Значение систем обнаружения вторжений сложно недооценить, поскольку их внедрение играет ключевую роль в укреплении сетей против потенциальных угроз. Они выступают в качестве краеугольного камня в создании безопасной среды для таких элементов, как персональные данные, приложения, бизнес-транзакции и личные файлы. Эти системы не только предоставляют фундаментальные и проактивные меры против потенциальных сетевых угроз, но также добавляют дополнительный уровень защиты, дополняя традиционные протоколы безопасности, такие как брандмауэры и антивирусные решения. СОВ обладают принципиальным преимуществом в своей способности выявлять как известные, так и неизвестные угрозы. Системы обнаружения на основе сигнатур основываются на анализе прошлых атак, сохраняя их шаблоны в базах данных для сравнения с поступающими данными с целью выявления и категоризации известных угроз. В отличие от этого, методы обнаружения на основе аномалий работают на основе анализа поведения, выявляя отклонения от установленных норм сетевого поведения для обнаружения новых и ранее неизвестных атак. Необходимо признать, что хакеры постоянно вырабатывают новые методологии для эксплуатации уязвимостей в сетях, избегая традиционных средств безопасности. Расширенные угрозы, нулевые дни и внутренние угрозы представляют серьезные вызовы для безопасности сети. Крепкие решения систем обнаружения вторжений, обладающие передовыми возможностями в анализе, непрерывном мониторинге и машинном обучении, неотъемлемы для выявления, предотвращения и смягчения таких видов деятельностей с целью свести их вред к минимуму. Создание архива исторических атак, сопровождаемого их уникальными шаблонами, играет ключевую роль в выявлении аналогичных угроз в последующем. Этот процесс способствует классификации этих угроз как вредоносных данных, что особенно полезно для систем обнаружения на основе сигнатур. Напротив, обнаружение на основе аномалий включает в себя изучение несоответствий или отклонений от обычного потока данных в сети, что позволяет выявлять тонкие и невидимые атаки.

Цель применения систем обнаружения вторжений. Внедрение систем обнаружения вторжений служит общей цели усиления возможностей систем информационной безопасности (СИБ). Эти системы охватывают как аппаратные устройства, так и интегрированные программные компоненты, плавно встроенные в протоколы управления информацией и данными, а также соответствие требованиям по безопасности. Открытие только что внедренной в Интернет системы вводит уязвимость, подвергая ее множеству потенциальных атак. В этом контексте становится

неотложной необходимость укрепления системы против разнообразных угроз, с которыми она может столкнуться.

Любая попытка компрометации системы, получения несанкционированного доступа к конфиденциальной информации или захвата активов с использованием интрузивных методов традиционно категоризируется как вторжение [1]. Увеличение использования коммуникационных систем и передача информации и данных как по локальным, так и по глобальным сетям Интернета сопровождается увеличением уязвимостей к вторжениям. Необходимость защиты от несанкционированного доступа превратилась в современную императивную задачу, учитывая растущую зависимость от взаимосвязанных сетей и компьютерных систем. Следовательно, стало неотъемлемым сотрудничество между коммерческим и академическим секторами для разработки решений, направленных на смягчение этих проблем в области безопасности. Критическим определителем безопасности устройства в сетях служит эффективность системы для обнаружения атак и ее реакция на новые угрозы. Таким образом, система, характеризующаяся высокой эффективностью обнаружения угроз и коротким временем реакции, считается прочной и безопасной [2]. Одним из основных требований для обеспечения безопасности служит уверенность в том, что данные доступны исключительно авторизованным лицам. В этом контексте надежность предполагает обеспечение целостности данных и информации, защищая их от вмешательства, несанкционированного доступа и вредоносных атак. Более того, надежная система безопасности должна включать в себя безопасное предоставление неличной и конфиденциальной информации пользователям. В этом аспекте СОВ играют ключевую роль, активно мониторируя и защищая данные и информацию в системе.

СОВ представляют собой мощный механизм защиты от разнообразных попыток вторжения, различных модальностей атак, несанкционированных проникновений и имеют особое значение для укрепления систем против различного спектра угроз. Совместная интеграция систем обнаружения вторжений с устройствами безопасности – такими, как брандмауэры, на компьютерных системах особенно заметна при повышении общей безопасности.

Заметным ограничением, присущим брандмауэрам, служит их неспособность функционировать автономно. В частности, брандмауэры не обладают «врожденной» способностью выявлять конкретные атаки в сетях и противостоять им, включая атаки отказа в обслуживании, распределенные атаки отказа в обслуживании и другие их разновидности [3]. Увеличение использования и неотложная необходимость в развитии сетей тесно связаны. Рост использования сетей коррелирует с увеличением частоты атак, что подчеркивает необходимость усиления систем, посвященных обеспечению защиты и безопасности информации. Это требует параллельного развития механизмов обнаружения вторжений для реагирования на нарастающий уровень угроз.

СОВ несут на себе ответственность за обеспечение безопасности частных сетей посредством анализа трафика, направляемого к Интернету и от него, в соответствии с предопределенными политиками или правилами, эффективно выступая преградой между частной сетью и Интернетом [4]. Брандмауэры могут представляться в различных формах, начиная от автономных компьютерных систем до отдельных сетей с несколькими вспомогательными устройствами или службами, работающими на маршрутизаторах и серверах. Обычно классифицируются как брандмауэры на уровне приложения и брандмауэры с фильтрацией пакетов [5]; последние используют предопределенные правила для определения разрешения или запрета сетевого трафика, входящего в сеть или выходящего из нее. СОВ систематически накапливают и анализируют данные из различных локаций в компьютере или сети с целью выявления потенциальных нарушений безопасности. Стратегическое внедрение СОВ совместно с другими средствами безопасности вносит значительный вклад в создание устойчивой инфраструктуры обороны от развивающихся угроз в области компьютерных наук и информационной безопасности.

В общем контексте СОВ охватывает основные компоненты (рис. 1):

– *датчики* (*Sensors*): роль датчиков в составе СОВ заключается в активном мониторинге и сборе данных о трафике в сети и деятельности системы. Датчики функционируют как первая линия обороны, непрерывно отслеживая и выявляя потенциальные инциденты безопасности [6];

– *аналитический движок* (*Analysis Engine*): анализирует данные, собранные датчиками, используя предопределенные правила или поведенческие шаблоны для выявления аномальной или вредоносной активности [7];

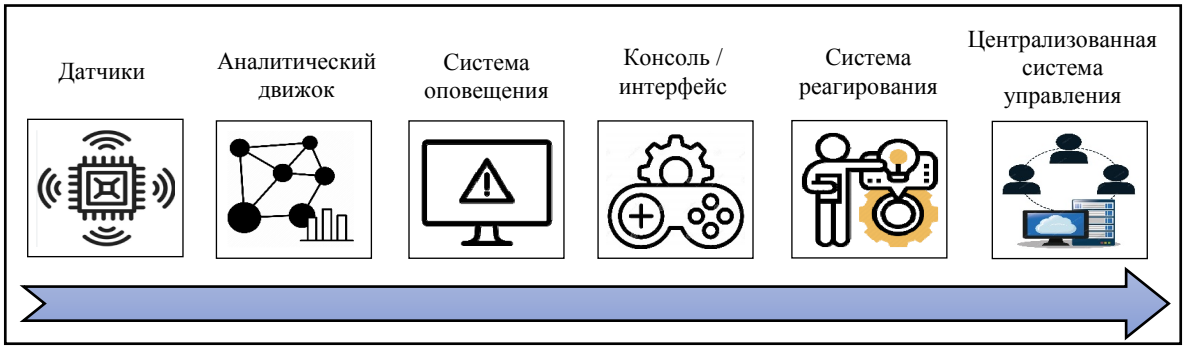

Рис. 1. Основные компоненты системы обнаружения вторжений
Fig. 1. Key components of the intrusion detection system

– *система оповещения* (*Alerting System*): когда аналитический движок выявляет подозрительную активность или потенциальные угрозы безопасности, система оповещения выдает предупреждения или сообщения. Оповещения играют ключевую роль в оперативном уведомлении руководителей по безопасности, позволяя им быстро реагировать для смягчения рисков и расследования инцидента [8];

– *консоль*/*интерфейс* (*Console*/*Interface*): консоль или управляющий интерфейс, служит пользовательским интерфейсом для аналитиков по безопасности и администраторов, предоставляя платформу для взаимодействия с системой обнаружения вторжений;

– *система реагирования* (*Response System*): предпринимает заранее определенные действия в ответ на выявленные инциденты безопасности. Эти действия могут включать в себя блокирование вредоносного трафика, изоляцию скомпрометированных систем или генерацию оповещений. Этот компонент должен обладать динамичной и адаптивной системой безопасности, тем самым улучшая общую устойчивость системы или сети [9];

– *централизованная система управления* (*Centralized Management System*): надзирает и координирует операции нескольких компонентов СОВ. Эта централизация облегчает управление возможностями обнаружения вторжений и их мониторинг, обеспечивая унифицированную и согласованную стратегию безопасности [10].

В области обнаружения вторжений выделяются три основные классификации СОВ: на основе сигнатур, на основе аномалий и гибридные.

Системы обнаружения вторжений на основе сигнатур. СОВ на основе сигнатур функционируют, анализируя сетевой трафик, активно ищут заранее установленные шаблоны или сигнатуры с целью выявления потенциальных атак. Термин «сигнатура», также известный как «правила», служит фундаментальным определением для атаки. По сути, для каждой распознанной атаки в базе данных СОВ на основе сигнатур архивируется шаблон, или сигнатура. Затем сетевая активность сравнивается с этими сохраненными сигнатурами в рамках процесса обнаружения. В случае выявления совпадения срабатывает сигнализация. Множество сигнатур генерируется через итеративное выполнение известного эксплойта, где процесс включает в себя мониторинг данных при их передвижении по сети и выявление характерного шаблона, который постоянно повторяется при каждом выполнении эксплойта. Эта методология эффективно гарантирует последовательное соответствие сигнатуры попыткам конкретного эксплойта. Хотя не существует универсально принятого определения, точно указывающего, что представляет собой сигнатура атаки, в нее обычно включены несколько компонентов, предназначенных для уникальной характеризации атаки. Оптимальная сигнатура характеризуется простотой и эффективностью выявления целевой атаки. Простота сигнатуры улучшает удобство поиска совпадения в потоке данных, особенно в контексте сетевых пакетов. В отличие от этого сложные сигнатуры могут создавать значительную нагрузку на обработку. Для спектра известных атак существуют различные типы сигнатур. Они охватывают сигнатуры, описывающие характеристики отдельной IP-опции – до тех, которые определяют полезную нагрузку атаки, при этом некоторые сигнатуры интегрируют оба аспекта. Многие СОВ на основе сигнатур поддерживают сопоставление шаблонов с использованием регулярных выражений при формулировании сигнатур. Затем система обнаружения вторжений на основе сигнатур сравнива-

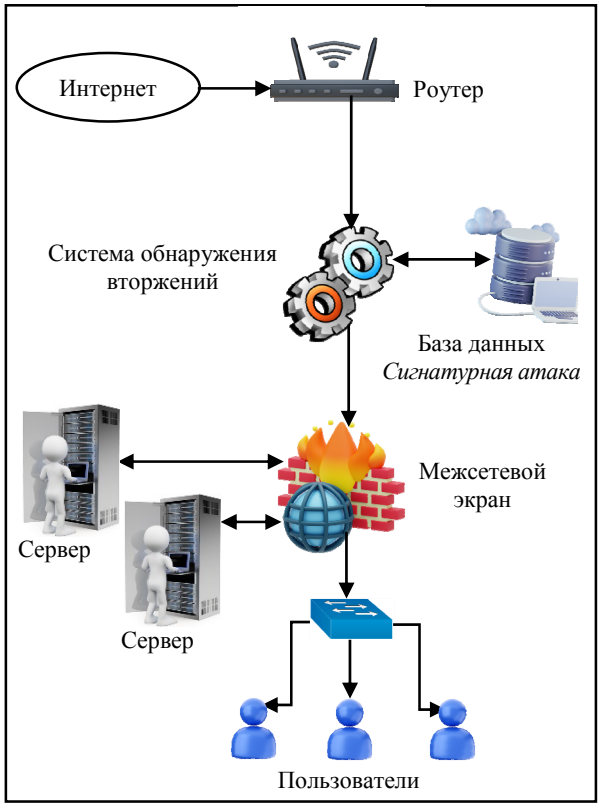

Рис. 2. Системы обнаружения вторжений на основе сигнатур
Fig. 2. Intrusion detection systems based on signatures

ет сетевую активность с сигнатурами, хранящимися в ее базе данных, определяя, соответствует ли она известной атаке, как показано на рис. 2. Важно подчеркнуть, что СОВ на основе сигнатур выявляют исключительно известные атаки [1], и их способность идентифицировать новые атаки, отсутствующие в базе данных, ограничена.

Табл. 1 предоставляет всестороннее резюме сильных и слабых сторон каждой СОВ на основе сигнатур, включая информацию о разработчике/компании, ключевых особенностях и поддерживаемых протоколах. Важно подчеркнуть, что эффективность СОВ зависит от различных факторов, включая стратегии развертывания, настройки конфигурации и конкретные сценарии использования.

В таблице содержится сравнительный анализ различных систем обнаружения вторжений на основе сигнатур, детализируя основную информацию, включая данные о разработчике/компании, особенности, поддержку протоколов, а также преимущества и недостатки. Этот краткий обзор служит ценным ресурсом для понимания уникальных характеристик и факторов, которые следует учитывать при выборе СОВ на основе сигнатур.

Системы обнаружения вторжений на основе аномалий. В области компьютерных наук и информационной безопасности СОВ на основе аномалий функционируют, следя за операциями системы и классифицируя их как типичные или аномальные. Эти системы обладают способно-

Табл. 1. Системы обнаружения вторжений на основе сигнатур
Tab. 1. Signature-based intrusion detection systems

Наименование СОВ	Разработчик/ компания	Основные характеристики	Поддержка протоколов	Преимущества	Недостатки
Snort [11]	Cisco	Открытый исходный код, основанный на правилах; анализ протоколов	TCP/IP, UDP, ICMP, IP	Широко используется; обширный набор правил; активная поддержка сообщества	Однопоточная; может оказать влияние на производительность в сетях с высоким трафиком
Suricata[12]	OISF	Открытый исходный код, многопоточный, высокопроизводительный	TCP/IP, UDP, ICMP, IP	Высокая производительность; поддержка новейших протоколов	Сложность конфигурации для некоторых пользователей
Bro/Zeek[13]	Corelight	Открытый исходный код; анализ сетевого трафика	TCP/IP, UDP, ICMP, IP	Основное внимание уделяется видимости сети; расширяемый фреймворк	Кривая обучения, может потребоваться установка дополнительных плагинов для определенных функций
Sourcefire[14]	Cisco	Основанный на правилах; обнаружение аномалий; интеграция	TCP/IP, UDP, ICMP, IP	Интегрирована с экосистемой безопасности «Cisco»	Собственноручный, потенциальные финансовые последствия
YARA[15]	Virus Total	Сопоставление по шаблонам; поддержка пользовательских правил	N/A (основано на файлах, не на сети)	Высокая настраиваемость; эффективность при обнаружении на основе файлов	Не предназначено для мониторинга сети в реальном времени

стью распознавать как компьютерные, так и сетевые вторжения, а также случаи неправомерного использования. Процесс классификации разработан для выявления любой формы неправомерного использования, отклоняющейся от типичной работы системы, используя эвристику или правила вместо заранее определенных шаблонов или сигнатур (*Истории атак*, рис. 3). В отличие от систем, полагающихся исключительно на сигнатуры и ограниченных выявлением атак, для которых заранее установлена сигнатура [16], в процессе обнаружения аномалий применяются статистические методы.

Анализируют сетевой трафик в двух наборах данных. Первый набор данных, полученный из наблюдений в реальном времени, устанавливает текущие сетевые профили, в то время как второй набор данных включает в себя предварительно обученные статистические профили. Сравнение этих двух профилей используется для вычисления балла аномалии, который служит представлением степени необычности для конкретной активности. Напротив, стратегия на основе знаний играет ключевую роль в СОВ. Этот подход включает в себя присвоение меток входным данным на основе набора правил, охватывающих два различных этапа. Во-первых, различные классы и сетевые активности выявляются во входных обучающих данных.

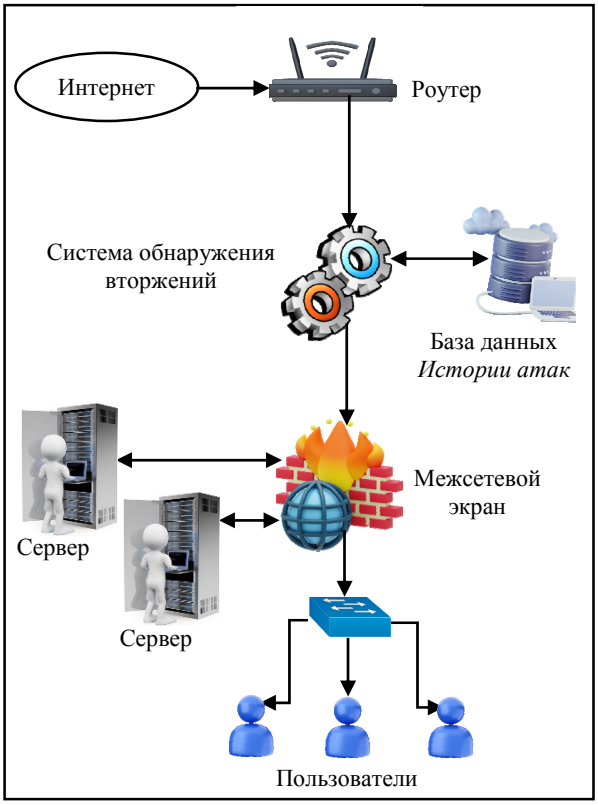

Рис. 3. Системы обнаружения вторжений на основе аномалий
Fig. 3. Anomaly-based intrusion detection systems

Затем ряд событий классификации производится на основе рутинных действий [17], [18].

Табл. 2. Системы обнаружения вторжений на основе аномалий
Tab. 2. Anomaly-based intrusion detection systems

Наименование СОВ	Разработчик/ компания	Основные характеристики	Поддержка протоколов	Преимущества	Недостатки
Snort (режим аномалий) [19]	Cisco	Открытый исходный код, поддерживает режим обнаружения аномалий	TCP/IP, UDP, ICMP, IP	Широко используется, поддерживает как режим сигнатурного, так и режим обнаружения аномалий	Ограниченные возможности базового обнаружения аномалий, может потребоваться использование дополнительных инструментов для глубокого анализа
Bro/Zeek (Фреймворк аномалий) [20]	Corelight	Открытый исходный код, анализ сетевого трафика с обнаружением аномалий	TCP/IP, UDP, ICMP, IP	Акцент на видимости сети, расширяемый фреймворк	Крутая кривая обучения, может потребоваться установка дополнительных плагинов для определенных функций
Темный след (Dark trace) [21]	Darktrace	Машинное обучение, обнаружение аномалий на основе искусственного интеллекта	N/A (проприетарный сетевой протокол)	Возможности самообучения, обнаружение угроз в реальном времени	Проприетарный, возможные проблемы с прозрачностью и объяснимостью
McAfee Network Security [22]	McAfee	Обнаружение на основе аномалий, интеграция с экосистемой McAfee	TCP/IP, UDP, ICMP, IP	Интеграция с более широкой системой безопасности, настраиваемость	Проприетарный, возможные проблемы с прозрачностью и объяснимостью
Splunk Enterprise Security [23]	Splunk	Обнаружение аномалий, корреляция и анализ	Поддерживает различные источники данных	Интеграция с более широкой системой безопасности, настраиваемость	Сложности в конфигурации и процессы, требующие значительных ресурсов

Система обнаружения аномалий подробно рассматривается в последующих подразделах:

1. Контролируемое обнаружение аномалий: строится система, способная независимо различать необычные и нормальные записи.

2. Наблюдаемое обнаружение аномалий: цель системы этого типа – разработать другие модели с использованием нормальных данных.

3. Полунаблюдаемое обнаружение аномалий: нацелена на построение модели на основе аномальных данных, что затрудняет выявление всех аномальных случаев. Используются сложные и ненаблюдаемые алгоритмы для обнаружения новых аномальных случаев. Эти методики могут быть применены к любой системе без необходимости модификаций. Требуется набор данных с метками.

В общем, базой работы СОВ на основе аномалий служит изучение сетевого трафика данных и отправка предупреждения в случае отклонения данных от нормального уровня. Сетевой трафик данных изучается с использованием заранее определенных правил.

Табл. 2 предоставляет всесторонний анализ сильных и слабых сторон каждой СОВ на основе аномалий, детализируя информацию о разработчике/компании, ключевых особенностях и поддержке протоколов.

Гибридные системы обнаружения вторжений (рис. 4) представляют собой продвинутый подход с целью использования преимуществ различных методов обнаружения вторжений в областях компьютерных наук и информационной безопасности. Эти системы обычно объединяют компоненты обнаружения вторжений на основе сигнатур с более сложными методами, например обнаружением аномалий на основе поведения. В одном модуле выявляются вредоносные и нормальные шаблоны или мониторятся отклонения от установленного нормального поведенческого профиля сети. Другой модуль использует сигнатуры для выявления известных атак. В отношении обнаружения атак гибридные системы часто интегрируют механизмы обнаружения аномалий, которые анализируют поведение системы и сети для выявления неожиданных активностей, включая изменения в трафике, необычные доступы или неприемлемые шаблоны коммуникации. Однако эти техники требуют дополнительных энергетических и ресурсных затрат. Хотя гибридные системы обнаружения вторжений обычно не рекомендуются для сетей с ограниченными ресурсами, в этой области ведется активное исследование. В исследовании [23] представлена модель гибридной системы обнаружения вторжений, которая организует узлы-датчики в шестиугольные регионы, аналогичные сотовым сетям. Каждый регион контролируется кластерным узлом, и эти узлы мониторятся региональными узлами. Базовая станция наблюдает за всеми региональными узлами, и их иерархическая структура организована в виде дерева. Сигнатуры атак передаются от базовой станции к листовому узлу, где они хранятся для обнаружения атак.

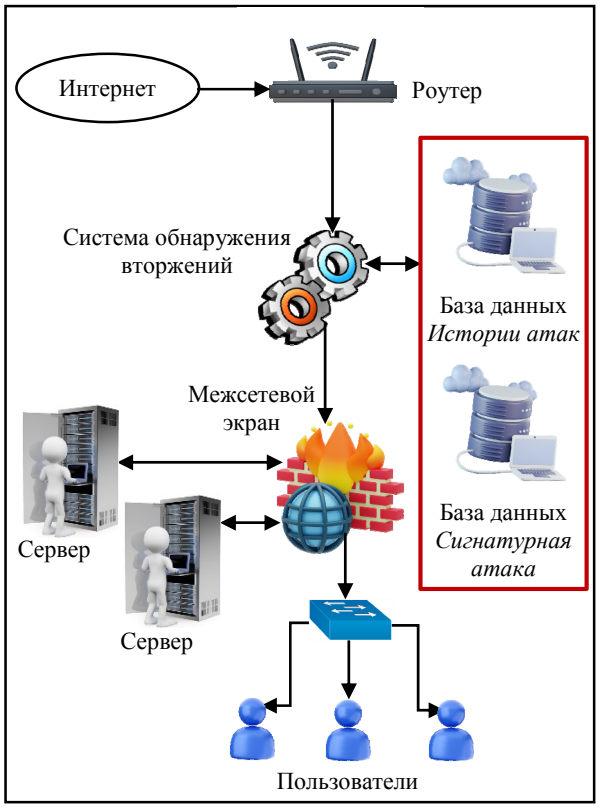

Рис. 4. Гибридные системы обнаружения вторжений
Fig. 4. Hybrid intrusion detection systems

Предопределенные параметры для нормального и аномального поведения встроены в механизм, и процесс обнаружения аномалий включает оценку отклонений от установленных параметров. Однако авторы не раскрыли уровень обнаружения и ложных срабатываний предложенной техники, и определить, какие уязвимости безопасности идентифицируются через эту конкретную систему, по-прежнему сложно. Несмотря на эти трудности, такой подход проявляет высокую точность в выявлении угроз безопасности на сетевом уровне – таких, как черви и ловушки.

В [24] представлена альтернативная гибридная система обнаружения вторжений, использующая обнаружение недопустимого использования и метод опорных векторов (SVM). SVM обучается с применением метода распределенного обучения, способного различать безобидные и вредоносные шаблоны. Эта система обнаружения вторжений специально предназначена для кластерных сетей сенсоров, где каждый узел мониторит соседние. Авторы утверждают высокий уровень обнаружения при меньшем количестве ложных срабатываний, хотя точные типы атак, на которые они ссылаются, не указаны.

В [25] представлена система обнаружения вторжений, использующая анализ потока и переходы состояний для обнаружения атак типа син-флуд, хотя ее реализацию и тестирование еще предстоит провести. Кроме того, [24] представляет гибридную систему обнаружения вторжений, основанную на кластеризации, где кластерный руководитель отвечает за обнаружение вторжений, с основной концепцией снижения энергопотребления.

В исследовании [26] предложена усовершенствованная система обнаружения вторжений, включающая три модуля: принятие решений, обнаружение на основе сигнатур и обнаружение на основе аномалий. В системе используется нейронная сеть с обратным распространением, обученная различать безвредные и вредоносные пакеты. Кроме того, в [24] представлена новая иерархическая гибридная система обнаружения вторжений, предназначенная для обнаружения атак на маршрутизацию. Гибридные системы обнаружения вторжений направлены на повышение эффективности и точности обнаружения, объединяя преимущества различных подходов. Этот комплексный подход способствует укреплению безопасности компьютерных систем перед все более разнообразным спектром угроз.

Табл. 3 предоставляет сравнительный анализ основных гибридных систем обнаружения вторжений, включая Security Onion, Alien Vault USM и Cisco Firepower. В ней указаны основные характеристики, поддерживаемые протоколы, преимущества и недостатки каждой системы. Например, Security Onion предлагает унифицированную платформу с несколькими движками, но требует времени для изучения. Alien Vault USM предоставляет возможности централизованного управления, хотя может потребовать лицензионных затрат. Cisco Firepower интегрируется беспрепятственно с обширной экосистемой, но является собственностью «Cisco» и может иметь потенциальные затраты. Этот лаконичный обзор облегчает лучшее понимание сильных сторон и соображений, связанных с каждой системой СОВ.

Заключение. В заключение можно сказать, что гибридные системы обнаружения вторжений обладают умеренной и высокой производительностью и временем реакции, при этом у них низкий и умеренный процент ошибок и высокий уровень обнаружения новых атак. Их применение становится все более распространенным в различных областях. Аномалийные системы обнаружения вторжений демонстрируют умеренную и высокую производительность и время реакции, а также низкий и умеренный процент ошибок, что делает их подходящими для отраслевых приложений. Системы обнаружения вторжений с сигнатурой обеспечивают быстрое время реакции, низкое потребление ресурсов и высокую простоту

Табл. 3. Системы обнаружения вторжений на основе аномалий
Tab. 3. Anomaly-based intrusion detection systems

СОВ	Разработчик/ Компания	Ключевые функции	Поддержка протоколов	Преимущества	Недостатки
Security Onion [27]	Security Onion	Интегрирует Snort, Suricata и OSSEC	TCP/IP, UDP, ICMP, IP	Единая платформа, несколько механизмов обнаружения	Кривая обучения, потенциальное использование ресурсов
Alien Vault USM [28]	Alien Vault	Унифицированное управление безопасностью с использованием различных методов обнаружения	TCP/IP, UDP, ICMP, IP	Централизованное управление, корреляция между несколькими источниками данных	Стоимость лицензирования, потенциально сложная настройка
Cisco Firepower [29]	Cisco	Интегрирует Snort для сигнатур и Firepower Threat Defense для обнаружения угроз на основе аномалий	TCP/IP, UDP, ICMP, IP	Интегрированная экосистема безопасности, комплексное обнаружение угроз	Собственность, потенциальные финансовые последствия

использования, но их способность обнаруживать новые атаки может быть ниже. Они широко применяются, но могут быть менее гибкими. Все три типа обновляемы, и легкость их использования зависит от конкретных настроек и требований конфигурации.

Список литературы

1. Abdulhammed R., Faezipour M., Elleithy K. M. Network Intrusion detection using hardware techniques: A review // IEEE Long Island Systems, Appl. and Technol. Conf. (LISAT). Farmingdale, NY, USA: IEEE, 2016. P. 1–7.

2. Khan Sh., Alrajeh N., Loo J. Kok-Keong. Secure route selection in wireless mesh networks // Comp. Networks. 2012. Vol. 56(2). P. 491–503. doi: 10.1016/j.comnet.2011.07.005.

3. Khan Sh., Loo J. Kok-Keong, Ziauddin Z. Framework for intrusion detection in IEEE 802.11 wireless mesh networks // The Intern. Arab J. of Inform. Technol. 2010. Vol. 7(4). P. 435–440. doi: 10.1016/j.jcss.2014.12.012.

4. Abbas S. H., Naser W. A. Kh., Kadhim A. A. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) // Global J. of Engin. and Technol. Advances. 2023. Vol. 14(02). P. 155–158.

5. Djenouri Dj., Khellad L., Badache N. A survey of security issues of mobile ad hoc and sensor networks // IEEE Communications Surveys & Tutorials. 2005. Vol. 7(4). P. 2–28. doi: 10.1109/COMST.2005.1593277.

6. Ioannou Ch., Vassiliou V., Sergiou Ch. An intrusion detection system for wireless sensor networks / 24th Intern. Conf. on Telecommunications (ICT). Limassol, Cyprus: IEEE, 2017. P. 1–5. doi: 10.1109/ICT.2017.7998271.

7. Bul'ajoul W., James A. E., Pannu M. Improving network intrusion detection system performance through quality of service configuration and parallel technology // J. of Comp. and System Sci. 2015. Vol. 81(6). P. 981–999. doi: 10.1016/j.jcss.2014.12.012.

8. Suwailem A. I. A., Al-Akhras M. T., Ghany K. K. A. Evaluating Snort alerts as a classification features set // Conf. Appl. of Artificial Intelligence in Engin. Singapore: Springer, 2021. P. 801–812.

9. Response option for attacks detected by intrusion detection system / Sh. Anwar, J. M. Zain, M. F. Zolkipli, Z. Inayat, A. N. Jabir, J. B. Odili // 4th Intern. Conf. on Software Engin. and Comp. Systems (ICSECS). Kuantan, Malaysia: IEEE, 2015. P. 195–200. doi: 10.1109/ICSECS.2015.7333109.

10. Segura G. A. N., Chorti A., Margi C. B. Centralized and distributed intrusion detection for resource-constrained wireless SDN networks // IEEE Internet of Things J. 2021. Vol. 9(10). P. 7746–7758. doi: 10.1109/JIOT.2021.3114270.

11. Noor F. Design & implementation of Layered signature based intrusion detection system using snort. PhD diss., Daffodil Intern. University, 2019. P. 27–34. URL: https://www.academia.edu/40759818/DESIGN_and_IMPLEMENTATION_OF_LAYERED_SIGNATURE_BASED_INTRUSION_DETECTION_SYSTEM_USING_SNORT (дата обращения 15.11.2023).

12. Bada G., Nabare W., Quansah D. Comparative analysis of the performance of network intrusion detection systems: snort suricata and bro intrusion detection systems in perspective // Intern. J. of Comp. Appl. 2020. Vol. 176(40). P. 39–44.

13. Waleed A., Jamali A. F., Masood A. Which open-source IDS? Snort, Suricata or Zeek // Comp. Networks. 2022. Vol. 213(1). P. 109–116. doi: 10.1016/j.comnet.2022.109116.

14. Stepanov A., Belov V. M. Comparative analysis of intrusion detection systems Snort and Suricata // Progress through Innovations: XIth Intern. Acad. and Research Conf. of Graduate and Postgraduate Students (GSRC). Новосибирск: Новосиб. гос. техн. ун-т, 2023. P. 9–10.

15. Lockett A. Assessing the effectiveness of YARA rules for signature-based malware detection and classification // Comp. Sci.: Cryptography and Security. 2021. doi: 10.48550/arXiv.2111.13910.

16. Roosta T., Shieh Sh. W., Sastry Sh. Taxonomy of security attacks in sensor networks // 1st IEEE Intern. Conf. on System Integration and Reliability Improvements. Hanoi, Vietnam: IEEE, 2006. P. 529–536.

17. Alrajeh N. A., Khan Sh., Shams B. Intrusion detection systems in wireless sensor networks: A review // Intern. J. of Distributed Sensor Networks. 2013. Vol. 9(5). P. 167575. doi: 10.1155/2013/167575.

18. Li Y, Parker L. E. Intruder detection using a wireless sensor network with an intelligent mobile robot response // IEEE SoutheastCon. Huntsville, AL, USA: IEEE, 2008. P. 37–42. doi: 10.1109/SECON.2008.4494250.

19. Intrusion detection using anomaly detection algorithm and snort / C. Yinka-Banjo, P. Alli, S. Misra, J. Oluranti, R. Ahuja // Illumination of Artificial Intelligence in Cybersecurity and Forensics. Cham: Springer Intern. Publishing. 2022. P. 45–70. doi: 10.1007/978-3-030-93453-8_3.

20. Roshandel S. Performance analysis of a graph-based anomaly detector and the Zeek intrusion detection system. 2022. P. 12–24. URL: http://hdl.handle.net/1828/13956 (дата обращения 15.11.2023).

21. Deployment of next generation intrusion detection systems against internal threats in a medium-sized enterprise / F. Piconese, A. Hakkala, S. Virtanen, B. Crispo // Master of Sci. in Technol. thesis, University Turku. 2020. P. 41–45. URL: https://www.utupub.fi/bitstream/handle/10024/150736/Piconese_Filippo_Thesis.pdf?sequence=1 (дата обращения 15.11.2023).

22. Atefi K., Hashim H., Kassim M. Anomaly analysis for the classification purpose of intrusion detection system with K-nearest neighbors and deep neural network // IEEE 7th Conf. on Systems, Process and Control (ICSPC). Melaka, Malaysia: IEEE, 2019. P. 269–274. doi: 10.1109/ICSPC47137.2019.9068081.

23. Integration of Splunk Enterprise SIEM for DDoS attack detection in IoT / M. Hristov, M. Nenova, G. Iliev, D. Avresky // IEEE 20th Intern. Symp. on Network Comp. and Appl. (NCA). Boston, MA, USA: IEEE, 2021. P. 1–5. doi: 10.1109/NCA53618.2021.9685977.

24. Yan K. Q., Wang S. C., Liu C. W. A hybrid intrusion detection system of cluster-based wireless sensor networks // Proc. of the Intern. Multiconf. of Engineers and Comp. Scientists (IMECS). Hong Kong, 2009. Vol. 1. P. 411–416.

25. Bhatnagar R., Shankar U. The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network // Intern. J. of Comp. Sci. and Engin. Survey. 2012. Vol. 3(2). P. 31 doi: 10.5121/ijcses.2012.3204.

26. Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network / K. Q. Yan, S. C. Wang, S. S. Wang, C. W. Liu // 3rd Intern. Conf. on Comp. Sci. and Inform. Technol. Chengdu, China: IEEE, 2010. Vol. 1. P. 114–118. doi: 10.1109/ICCSIT.2010.5563886.

27. Heenan R., Moradpoor N. Introduction to security onion. 2016. URL: https://www.napier.ac.uk/-/media/worktribe/output-461935/introduction-to-security-onion.ashx (дата обращения 15.11.2023).

28. Zeinali S. M. Analysis of security information and event management (SIEM) evasion and detection methods // Master Thesis. Tallinn University of Technol., 2016. 65 p. URL: https://mendillo.info/seguridad/tesis/Morteza.pdf (дата обращения 15.11.2023).

29. Trisolino A. Analysis of security configuration for IDS/IPS. Doct. diss., Politecnico di Torino. 2023. 92 p. URL: https://webthesis.biblio.polito.it/secure/29003/1/tesi.pdf (дата обращения 15.11.2023).

Информация об авторах

Аль-Тамими Мохалад – аспирант кафедры информационной безопасности СПбГЭТУ «ЛЭТИ».
E-mail: almokhalad44@gmail.com
https://orcid.org/0009-0005-5316-1689

Хассан Мубарек Барре – аспирант кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: moubarekbarrehassan@gmail.com
https://orcid.org/0009-0007-2744-5666

Пазников Алексей Александрович – канд. техн. наук, доцент кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: apaznikov@gmail.com
https://orcid.org/0000-0002-3735-6882

Аль-Хайкани Муджтаба Назар – аспирант кафедры информационных систем СПбГЭТУ «ЛЭТИ».
E-mail: mujtabatoby2b@gmail.com
https://orcid.org/0009-0004-6791-1973

Альбадрави Елаф – магистрант, Университет Васит, ул. Корниш, Васит, Ирак, 32.50108949375925, 45.838482868944446.
E-mail: Leccit2@uowasit.edu.iq
https://orcid.org/0009-0001-9560-1006

Вклад авторов:

Аль-Тамими Мохалад М. М. – системы обнаружения вторжений на основе сигнатур, системы обнаружения вторжений на основе аномалий, гибридные системы обнаружения вторжений.

Хассан М. Б. – цель применения систем обнаружения вторжений, системы обнаружения вторжений на основе сигнатур.

Пазников А. А. – руководство научной работой, аннотация, заключение.

Аль-Хайкани М. Н. – рис. 1–4.

Альбадрави Е. Б. – табл. 1–3.

References

1. Abdulhammed R., Faezipour M., Elleithy K. M. Network Intrusion detection using hardware techniques: A review // IEEE Long Island Systems, Appl. and Technol. Conf. (LISAT). Farmingdale, NY, USA: IEEE, 2016. P. 1–7.

2. Khan Sh., Alrajeh N., Loo J. Kok-Keong. Secure route selection in wireless mesh networks // Comp. Networks. 2012. Vol. 56(2). P. 491–503. doi: 10.1016/j.comnet.2011.07.005.

3. Khan Sh., Loo J. Kok-Keong, Ziauddin Z. Framework for intrusion detection in IEEE 802.11 wireless mesh networks // The Intern. Arab J. of Inform. Technol. 2010. Vol. 7(4). P. 435–440. doi: 10.1016/j.jcss.2014.12.012.

4. Abbas S. H., Naser W. A. Kh., Kadhim A. A. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) // Global J. of Engin. and Technol. Advances. 2023. Vol. 14(02). P. 155–158.

5. Djenouri Dj., Khellad, Lyes, Badache N. A survey of security issues of mobile ad hoc and sensor networks // IEEE Communications Surveys & Tutorials. 2005. Vol. 7(4). P. 2–28. doi: 10.1109/COMST.2005.1593277.

6. Ioannou Ch., Vassiliou V., Sergiou Ch. An intrusion detection system for wireless sensor networks / 24th Intern. Conf. on Telecommunications (ICT). Limassol, Cyprus: IEEE, 2017. P. 1–5. doi: 10.1109/ICT.2017.7998271.

7. Bul'ajoul W., James A. E., Pannu M. Improving network intrusion detection system performance through quality of service configuration and parallel technology // J. of Comp. and System Sci. 2015. Vol. 81(6). P. 981–999. doi: 10.1016/j.jcss.2014.12.012.

8. Suwailem A. I. A., Al-Akhras M. T., Ghany K. K. A. Evaluating snort alerts as a classification features set // Conf. Appl. of Artificial Intelligence in Engin. Singapore: Springer, 2021. P. 801–812.

9. Response option for attacks detected by intrusion detection system / Sh. Anwar, J. M. Zain, M. F. Zolkipli, Z. Inayat, A. N. Jabir, J. B. Odili // 4th Intern. Conf. on Software Engin. and Comp. Systems (ICSECS). Kuantan, Malaysia: IEEE, 2015. P. 195–200. doi: 10.1109/ICSECS.2015.7333109.

10. Segura G. A. N., Chorti A., Margi C. B. Centralized and distributed intrusion detection for resource-constrained wireless SDN networks // IEEE Internet of Things J. 2021. Vol. 9(10). P. 7746–7758. doi: 10.1109/JIOT.2021.3114270.

11. Noor F. Design & implementation of Layered signature based intrusion detection system using snort. PhD diss., Daffodil Intern. University, 2019. P. 27–34. URL: https://www.academia.edu/40759818/DESIGN_and_IMPLEMENTATION_OF_LAYERED_SIGNATURE_BASED_INTRUSION_DETECTION_SYSTEM_USING_SNORT (data obrashhenija 15.11.2023).

12. Bada G., Nabare W., Quansah D. Comparative analysis of the performance of network intrusion detection systems: snort suricata and bro intrusion detection systems in perspective // Intern. J. of Comp. Appl. 2020. Vol. 176(40). P. 39–44.

13. Waleed A., Jamali A. F., Masood A. Which open-source IDS? Snort, Suricata or Zeek // Comp. Networks. 2022. Vol. 213(1). P. 109–116. doi: 10.1016/j.comnet.2022.109116.

14. Stepanov A., Belov V. M. Comparative analysis of intrusion detection systems Snort and Suricata // Progress Through Innovations: XIth Intern. Acad. and Research Conf. of Graduate and Postgraduate Students (GSRC). Novosibirsk: Novosib. gos. tehn. un-t, 2023. P. 9–10.

15. Lockett A. Assessing the effectiveness of YARA rules for signature-based malware detection and classification // Comp. Sci.: Cryptography and Security. 2021. doi: 10.48550/arXiv.2111.13910.

16. Roosta T., Shieh Sh. W., Sastry Sh. Taxonomy of security attacks in sensor networks // 1st IEEE Intern. Conf. on System Integration and Reliability Improvements. Hanoi, Vietnam: IEEE, 2006. P. 529–536.

17. Alrajeh N. A., Khan Sh., Shams B. Intrusion detection systems in wireless sensor networks: A review // Intern. J. of Distributed Sensor Networks. 2013. Vol. 9(5). P. 167575. doi: 10.1155/2013/167575.

18. Li Y, Parker L. E. Intruder detection using a wireless sensor network with an intelligent mobile robot response // IEEE SoutheastCon. Huntsville, AL, USA: IEEE, 2008. P. 37–42. doi: 10.1109/SECON.2008.4494250.

19. Intrusion detection using anomaly detection algorithm and snort / C. Yinka-Banjo, P. Alli, S. Misra, J. Oluranti, R. Ahuja // Illumination of Artificial Intelligence in Cybersecurity and Forensics. Cham: Springer Intern. Publishing. 2022. P. 45–70. doi: 10.1007/978-3-030-93453-8_3.

20. Roshandel S. Performance analysis of a graph-based anomaly detector and the Zeek intrusion detection system. 2022. P. 12–24. URL: http://hdl.handle.net/1828/13956 (дата обращения 15.11.2023).

21. Deployment of next generation intrusion detection systems against internal threats in a medium-sized enterprise / Piconese F., Hakkala A., Virtanen S., Crispo B. // Master of Sci. in Technol. thesis, University Turku. 2020. P. 41–45. URL: https://www.utupub.fi/bitstream/handle/10024/150736/Piconese_Filippo_Thesis.pdf?sequence=1 (data obrashhenija 15.11.2023).

22. Atefi K., Hashim H., Kassim M. Anomaly analysis for the classification purpose of intrusion detection system with K-nearest neighbors and deep neural network // IEEE 7th Conf. on Systems, Process and Control (ICSPC). Melaka, Malaysia: IEEE, 2019. P. 269–274. doi: 10.1109/ICSPC47137.2019.9068081.

23. Integration of Splunk Enterprise SIEM for DDoS attack detection in IoT / M. Hristov, M. Nenova, G. Iliev, D. Avresky // IEEE 20th Intern. Symp. on Network Comp. and Appl. (NCA). Boston, MA, USA: IEEE, 2021. P. 1–5. doi: 10.1109/NCA53618.2021.9685977.

24. Yan K. Q., Wang S. C., Liu C. W. A hybrid intrusion detection system of cluster-based wireless sensor networks // Proc. of the Intern. Multiconf. of Engineers and Comp. Scientists (IMECS). Hong Kong, 2009. Vol. 1. P. 411–416.

25. Bhatnagar R., Shankar U. The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network // Intern. J. of Comp. Sci. and Engin. Survey. 2012. Vol. 3(2). P. 31 doi: 10.5121/ijcses.2012.3204.

26. Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network / K. Q. Yan, S. C. Wang, S. S. Wang, C. W. Liu // 3rd Intern. Conf. on Comp. Sci. and Inform. Technol. Chengdu, China: IEEE, 2010. Vol. 1. P. 114–118. doi: 10.1109/ICCSIT.2010.5563886.

27. Heenan R., Moradpoor N. Introduction to security onion. 2016. URL: https://www.napier.ac.uk/-/media/worktribe/output-461935/introduction-to-security-onion.ashx (дата обращения 15.11.2023).

28. Zeinali S. M. Analysis of security information and event management (SIEM) evasion and detection methods // Master Thesis. Tallinn University of Technol., 2016. 65 p. URL: https://mendillo.info/seguridad/tesis/Morteza.pdf (data obrashhenija 15.11.2023).

29. Trisolino A. Analysis of security configuration for IDS/IPS. Doct. diss., Politecnico di Torino. 2023. 92 p. URL: https://webthesis.biblio.polito.it/secure/29003/1/tesi.pdf (data obrashhenija 15.11.2023).

Information about the authors

Mokhalad Al-Tameemi – postgraduate student of the Department of Information Security Saint Petersburg Electrotechnical University.
E-mail: almokhalad44@gmail.com
https://orcid.org/0009-0005-5316-1689

Moubarek Barre Hassan – postgraduate student of the Department of Computer Technology of Saint Petersburg Electrotechnical University.
E-mail: moubarekbarrehassan@gmail.com
https://orcid.org/0009-0007-2744-5666

Alexey A. Paznikov – Cand. Sci. (Eng.), Associate Professor of the Department of Computer Technology Saint Petersburg Electrotechnical University.
E-mail: apaznikov@gmail.com
https://orcid.org/0000-0002-3735-6882

Mujtaba Al-Khaykanee – postgraduate student of the Department of Information Systems of Saint Petersburg Electrotechnical University.
E-mail: mujtabatoby2b@gmail.com
https://orcid.org/0009-0004-6791-1973

Elaf Albadrawi – master's degree, Wasit University, Kornish St., Wasit, Iraq, 32.50108949375925, 45.838482868944446.
E-mail: Leccit2@uowasit.edu.iq
https://orcid.org/0009-0001-9560-1006

Author contribution statement:

Al-Tameemi M. M. – Signature-Based Intrusion Detection Systems, Anomaly-Based Intrusion Detection Systems, Hybrid Intrusion Detection Systems.

Hassan M. B. – Purpose of Intrusion Detection Systems, Signature-based Intrusion Detection Systems.

Paznikov A. A. – Research supervision, Abstract, Conclusions.

AL-khaykanee M. N. – Fig. 1–4

Albadrawi E. B. – Tab. 1–4.

Статья поступила в редакцию 11.01.2024; принята к публикации после рецензирования 27.02.2024; опубликована онлайн 23.04.2024.

Submitted 11.01.2024; accepted 27.02.2024; published online 23.04.2024.