Иванов Е.А., Амелютин Е.В. Разработка системы автоматической идентификации и классификации угроз безопасности в информационно-аналитической системе // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 1(51) с. 97–107

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИИ И КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ

Иванов Е.А., **[1]Амелютин Е.В.**
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail:[1] kmaw2@yandex.ru

В статье проведён анализ предметной области системы обнаружения вторжений (IDS) и определены ключевые характеристики угроз безопасности в информационно-аналитических системах. Рассмотрены методы автоматической идентификации и классификации сетевых угроз на основе анализа трафика и поведения системы.

Ключевые слова: Система обнаружения вторжений, автоматическая идентификация угроз, информационная безопасность, сетевой трафик, классификация угроз.

DEVELOPMENT OF A SYSTEM FOR AUTOMATIC IDENTIFICATION AND CLASSIFICATION OF SECURITY THREATS IN AN INFORMATION AND ANALYTICAL SYSTEM

Ivanov E.A., **[1]Amelutin E.V.**
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: [1] kmaw2@yandex.ru

The article analyzes the subject area of the intrusion detection system (IDS) and defines key characteristics of security threats in information and analytical systems. Methods of automatic identification and classification of network threats based on traffic analysis and system behavior are considered.

Keywords: Intrusion detection system, automatic threat identification, information security, network traffic, threat classification.

В условиях цифровой трансформации информационно-аналитические системы становятся основой для хранения, обработки и анализа данных в организациях. Рост объёмов информации и увеличение числа подключённых устройств повышают риски возникновения угроз безопасности. Для эффективного противодействия этим угрозам необходимы автоматизированные системы, способные своевременно обнаруживать и классифицировать возможные атаки. В данном исследовании рассматривается разработка системы обнаружения вторжений (IDS), обеспечивающей автоматическую идентификацию и классификацию угроз в информационно-аналитической системе.

Разработка системы автоматической идентификации и классификации угроз, являющаяся предметом данной работы, направлена на повышение защищенности информационно-аналитических систем (ИАС) путем автоматизации ключевых процессов

анализа и управления угрозами. Это особенно важно в условиях постоянно меняющихся угроз информационной безопасности, когда вручную управлять рисками становится всё сложнее.

Системы обнаружения вторжений (IDS) представляют собой ключевые компоненты информационной безопасности, предназначенные для мониторинга сетевого трафика и активности пользователей с целью выявления потенциальных угроз. В настоящее время на рынке существует множество IDS-решений, как коммерческих, так и открытых. Эти системы могут различаться по методам обнаружения, подходам к обработке данных и возможностям интеграции. Изучим классификацию существующих решений IDS, их особенности, а также проблемы и ограничения, с которыми сталкиваются традиционные системы. Также будет рассмотрено, как эти системы применяются в различных сферах, включая корпоративные сети, критическую инфраструктуру и IoT-системы.

Системы обнаружения вторжений (IDS) классифицируются по различным признакам, и одним из ключевых является метод обнаружения угроз. В этом контексте можно выделить три основных подхода: сигнатурный, аномальный и гибридный [1].

Сигнатурные системы работают на основе заранее определенных шаблонов или сигнатур, которые представляют собой записи о типичных признаках уже известных угроз. Такие системы эффективно выявляют атаки, зафиксированные в базе данных, например, вирусы, трояны и другие виды вторжений. Однако их главный недостаток заключается в том, что они не способны распознавать новые и неизвестные угрозы, которых нет в базе сигнатур.

В отличие от них, аномальные системы используют базовый профиль нормального поведения сети или пользователя. Если наблюдаемая активность отклоняется от этого профиля, система рассматривает такое поведение как потенциальную угрозу. Этот метод позволяет обнаруживать ранее неизвестные атаки, однако он сопровождается повышенным риском ложных срабатываний, особенно в сложных и динамичных сетевых средах, где нормальное поведение постоянно меняется.

Гибридные системы сочетают в себе элементы сигнатурного и аномального анализа. Такой подход позволяет более эффективно выявлять как известные, так и новые угрозы, обеспечивая при этом снижение числа ложных срабатываний. Благодаря сочетанию методов гибридные IDS демонстрируют высокую гибкость и точность, что делает их универсальными для различных сценариев обеспечения безопасности.

Таким образом, выбор метода обнаружения в IDS зависит от требований к точности, скорости реакции и способности адаптироваться к новым видам угроз.

Системы обнаружения вторжений (IDS) также классифицируются по месту их внедрения. В зависимости от уровня, на котором осуществляется мониторинг, можно выделить сетевые, хостовые и гибридные решения [2].

Сетевые IDS (NIDS) устанавливаются на уровне сети и занимаются анализом сетевого трафика, проходящего через точки подключения. Такие системы особенно эффективны для мониторинга взаимодействий между различными узлами сети. Они позволяют оперативно выявлять угрозы и атаки, происходящие на уровне передачи данных, что делает их важным инструментом для защиты сетевой инфраструктуры.

Хостовые IDS (HIDS), в свою очередь, размещаются непосредственно на конечных устройствах, таких как серверы или рабочие станции. Эти системы анализируют журналы событий, выполняемые процессы и другие данные, связанные с активностью на конкретном

устройстве. Хостовые IDS способны обнаруживать подозрительные действия, например, изменения в файловой системе или попытки несанкционированного доступа к конфиденциальной информации. Они играют важную роль в дополнении к сетевым IDS, так как могут выявлять атаки, которые остаются незамеченными на уровне сети.

Гибридные IDS объединяют функции как сетевых, так и хостовых систем, предоставляя комплексный подход к обеспечению безопасности. Такое сочетание позволяет достигнуть более полного покрытия и обеспечивать защиту как на уровне сети, так и на уровне конечных устройств. Гибридные решения эффективно выявляют широкий спектр угроз и атак, благодаря чему обеспечивается повышенная надежность и точность системы безопасности.

На рынке информационной безопасности представлено множество коммерческих систем IDS, каждая из которых разрабатывается с учётом конкретных потребностей и масштабов применения. Одним из примеров является **Cisco Secure Network Analytics** (ранее известная как Stealthwatch). Эта система специализируется на анализе сетевого трафика и использует технологии машинного обучения и поведенческого анализа для выявления аномальных паттернов. Благодаря высокой степени автоматизации и интуитивно понятному интерфейсу, решения Cisco особенно эффективны для крупных корпоративных сетей и объектов критической инфраструктуры.

Ещё одним широко применяемым решением является **McAfee Network Security Platform (NSP)**. Эта система использует комбинацию сигнатурных и аномальных методов для анализа сетевого трафика и обнаружения угроз. NSP востребована в крупных организациях, где требуется защита как от известных, так и от новых, неизвестных атак.

Кроме того, **Intrusion Detection Systems от Symantec (Broadcom)** представляют собой комплексные решения для обнаружения и предотвращения вторжений в корпоративных и облачных сетях. Эти системы обеспечивают анализ и блокировку атак на различных уровнях, применяя как сигнатурный анализ, так и технологии машинного обучения. Такой подход позволяет эффективно защищать информационные ресурсы от широкого спектра угроз и атак [7].

Основными преимуществами коммерческих решений являются высокое качество поддержки, гарантии работы и предоставление множества функциональных возможностей, включая интеграцию с другими средствами безопасности. Однако они обладают рядом ограничений, таких как высокая стоимость, сложности с кастомизацией под специфические задачи и закрытый исходный код, что ограничивает возможности для индивидуальной настройки под уникальные требования.

В дополнение к коммерческим решениям, на рынке также доступны открытые IDS-системы, которые приобретают всё большую популярность благодаря своей доступности и гибкости для адаптации под различные потребности. Одной из самых известных и распространённых систем является **Snort**. Этот инструмент поддерживает как сигнатурный, так и аномальный методы обнаружения, предоставляя пользователям возможность модифицировать систему под конкретные задачи. Snort является бесплатным и имеет открытый исходный код, что облегчает интеграцию с различными средствами мониторинга и управления безопасностью.

Другой значимой системой является **Suricata** — высокопроизводительная IDS/IPS-система с открытым исходным кодом. Suricata поддерживает многозадачность и способна

обрабатывать значительные объёмы трафика в реальном времени. Благодаря сочетанию сигнатурного и аномального анализа, а также поддержке различных сетевых протоколов, Suricata является гибким инструментом для множества сценариев применения.

Также заслуживает внимания система **Zeek**, ранее известная как Bro. Эта IDS ориентирована на глубокий сетевой анализ и использует уникальные подходы к мониторингу трафика. Zeek выявляет угрозы, анализируя сетевые паттерны и поведение сети, что позволяет эффективно обнаруживать аномалии. Дополнительным преимуществом является возможность интеграции Zeek с другими системами безопасности, что расширяет её функциональные возможности и повышает эффективность защиты [14].

Открытые решения позволяют использовать широкий спектр инструментов для настройки и оптимизации системы под специфические нужды организации. Преимущества таких решений включают низкую стоимость, возможность кастомизации и активное сообщество разработчиков. Однако у них также есть свои ограничения, такие как высокая сложность настройки и недостаток официальной технической поддержки.

Системы обнаружения вторжений (IDS) должны быть способны выявлять широкий спектр угроз, как внешних, так и внутренних. Эти угрозы могут варьироваться от традиционных атак, таких как взлом и DDoS-атаки, до более сложных и скрытых угроз, таких как инсайдерские атаки. Важно понять, как различные типы угроз могут быть обнаружены с помощью различных методов анализа, включая сигнатурный, аномальный и поведенческий подходы [6].

Система IDS должна эффективно работать с различными видами угроз, обеспечивая комплексную защиту сети и информационных ресурсов. Среди наиболее распространённых внешних угроз выделяются DDoS-атаки [12], которые представляют собой массовые атаки на сеть с использованием множества скомпрометированных устройств для создания большого объема трафика, направленного на целевой сервер или сервис. Цель таких атак заключается в перегрузке ресурсов системы, что приводит к отказу в обслуживании и недоступности сервиса для легитимных пользователей.

Также распространены попытки несанкционированного доступа [3], которые могут включать эксплуатацию уязвимостей в программном обеспечении, подбор паролей, внедрение вредоносного кода и другие методы, направленные на получение доступа к защищённым ресурсам. Эти действия могут привести к компрометации данных и нарушению целостности системы.

Особую опасность представляют атаки с использованием фишинга и социальной инженерии. Такие угрозы нацелены на обман пользователей с целью получения конфиденциальной информации, например, логинов, паролей или данных банковских карт. Злоумышленники создают поддельные сайты и сообщения, имитирующие доверенные источники, чтобы вызвать у жертвы чувство доверия и заставить её раскрыть важные данные.

Ещё одной серьёзной угрозой являются вредоносные программы [8], такие как вирусы, трояны и шпионское ПО. Эти программы могут использоваться для создания скрытых каналов доступа (бэкдоров), кражи данных и нарушения нормального функционирования системы. Они наносят значительный ущерб безопасности, внедряясь в инфраструктуру и выполняя деструктивные действия. Эффективное выявление и нейтрализация таких угроз являются важными задачами IDS для обеспечения устойчивости системы безопасности.

Внутренние угрозы также представляют собой значительный риск для безопасности информационных систем. Одним из самых опасных типов внутренних угроз являются инсайдерские угрозы [10], которые исходят от сотрудников организации, имеющих доступ к защищенным данным и системам. Эти сотрудники могут злоупотреблять своими привилегиями для выполнения вредоносных действий, таких как кража данных, саботаж или несанкционированный доступ к критической информации. Инсайдеры могут быть мотивированы личными или финансовыми интересами, что делает их угрозой, которую сложно предсказать и предотвратить с помощью стандартных методов безопасности.

Еще одной внутренней угрозой являются ошибки конфигурации и недостаточная настройка систем [5]. Эти уязвимости могут возникать из-за человеческого фактора, неправильного управления системами или несоответствия безопасности установленным стандартам. Если настройки системы сделаны неаккуратно или с ошибками, они могут стать дверью для злоумышленников, которые смогут использовать эти уязвимости для проникновения в сеть или нарушении работы системы.

Для обнаружения внутренних угроз существует несколько методов, каждый из которых имеет свои особенности и ограничения. Сигнатурный метод обнаружения эффективно защищает от известных угроз, однако он не способен обнаружить новые, неизвестные атаки, что является его основным ограничением. Аномальный метод, в свою очередь, может привести к высокому количеству ложных срабатываний, так как любой отклоняющийся от нормы трафик может восприниматься как атака. Поведенческий метод требует постоянного мониторинга и анализа больших объемов данных, что может быть трудно реализуемо в реальном времени, особенно в сложных и динамичных средах. [13] Поэтому при проектировании системы IDS важно учитывать все эти ограничения и выбирать наиболее подходящие методы для эффективной защиты от как внешних, так и внутренних угроз.

Таким образом, сочетание этих методов в одной системе IDS позволяет более эффективно обнаруживать как известные, так и новые угрозы, а также минимизировать количество ложных срабатываний.

Хотя системы обнаружения вторжений играют ключевую роль в защите информационных систем, они не лишены ряда ограничений, которые могут затруднить их внедрение и эффективность: Высокие затраты на внедрение и поддержку — коммерческие решения, как правило, требуют значительных финансовых вложений, а их обслуживание может быть связано с дополнительными затратами на обновление и настройку. Сложность настройки и использования — многие решения требуют глубокой настройки и профессиональных навыков для правильной интеграции с существующими системами безопасности. Это может стать барьером для организаций с ограниченными ресурсами. Высокая частота ложных срабатываний — системы, использующие аномальный анализ, могут давать много ложных срабатываний, что требует дополнительной настройки и мониторинга, чтобы избежать перезагрузки команды безопасности. Закрытые исходные коды — коммерческие IDS часто имеют закрытый исходный код, что ограничивает возможности их модификации и адаптации под специфические нужды компании.

Эти ограничения подчеркивают необходимость разработки отечественных IDS, ориентированных на локальные условия, которые обеспечивают высокую гибкость в настройке и эффективное реагирование на угрозы в специфических условиях.

В рамках данного исследования рассмотрены современные методы и алгоритмы для анализа угроз, включая методы машинного обучения, анализ сетевого трафика и поведенческий анализ.

В рамках данного исследования рассмотрены современные методы и алгоритмы, используемые для анализа угроз в системах безопасности. Одним из ключевых подходов является применение методов машинного обучения для классификации угроз. В частности, используются алгоритмы, такие как деревья решений, случайный лес, методы опорных векторов (SVM) [11], а также глубокие нейронные сети. Эти методы позволяют создавать модели, которые могут обучаться на исторических данных, улучшая точность предсказаний и адаптируясь к новым, ранее не встречавшимся угрозам.

Также важным методом является анализ сетевого трафика, который включает использование заранее определенных правил для выявления аномалий на основе базового профиля сети. Этот подход позволяет отслеживать отклонения от нормального поведения, что помогает своевременно обнаруживать потенциальные угрозы и предотвращать атаки.

Поведенческий анализ, в свою очередь, ориентирован на изучение паттернов действий пользователей и процессов. Он помогает выявлять отклонения, которые могут свидетельствовать о том, что в системе происходят атаки или другие злонамеренные действия. Такой подход позволяет своевременно обнаружить угрозы, которые не могут быть выявлены с помощью традиционных методов, основанных на сигнатурах.

Для обеспечения высокой точности классификации угроз в разработанной системе используется комбинация перечисленных методов. Это позволяет учитывать и статистические, и поведенческие особенности угроз, что повышает надежность системы.

Архитектура системы, разработанная на основе UML-моделей, включает несколько ключевых компонентов, каждый из которых выполняет свою роль в обеспечении безопасности и анализа угроз. Данные для обучения модели берутся из файла logs.csv, который содержит набор метрик, собранных за определенный период времени, включая как нормальный трафик, так и потенциальные угрозы. Этот файл формируется на основе журналов сетевого трафика, которые могут быть выгружены из систем мониторинга, таких как IDS/IPS (Intrusion Detection/Prevention Systems) или файлы *.pcap, используемые для анализа сетевых пакетов. На этапе сбора данных система захватывает и агрегирует информацию из различных источников, таких как сетевой трафик, системные логи и события безопасности. Для реализации этого процесса были использованы специализированные библиотеки и фреймворки: **Flask**, **Pandas, Scikit-learn, Joblib, Matplotlib**, **SQLite** и инструменты, включая libpcap и tcpdump для мониторинга сетевого трафика, а также Logstash для обработки логов. Гибкость настройки позволяет системе работать как в режиме реального времени, отслеживая текущую активность, так и в пакетном режиме для обработки архивных данных.

На следующем этапе происходит обработка собранных данных. Этот процесс включает фильтрацию для удаления дублирующейся и нерелевантной информации, а также нормализацию, которая приводит данные к единому формату. Подготовленные данные проходят этап агрегации и выделения ключевых признаков, необходимых для дальнейшего анализа. Такой подход гарантирует высокое качество данных и повышает точность идентификации угроз на следующих этапах обработки.

На уровне анализа система применяет современные алгоритмы машинного обучения и методы детектирования аномалий. Были реализованы как классические алгоритмы классификации, такие как случайный лес, метод опорных векторов и k-ближайших соседей, так и нейронные сети для более сложных сценариев. Эти алгоритмы позволяют системе распознавать известные типы угроз и выявлять аномальное поведение, что помогает идентифицировать новые или модифицированные атаки. Благодаря возможности автоматического обучения на новых данных, система адаптируется к изменениям сетевого трафика и эволюции киберугроз.

Для удобного взаимодействия с системой был разработан интуитивно понятный веб-интерфейс. Он предоставляет пользователю визуализацию результатов анализа в форме интерактивных графиков, таблиц и дашбордов. Через интерфейс можно управлять параметрами системы, настраивать уровни критичности угроз и создавать отчеты на основе результатов анализа. Веб-приложение разработано с использованием современных технологий, таких как React и Bootstrap, что обеспечивает стабильность и адаптивность интерфейса для работы на различных устройствах.

Тестирование системы проводилось на реальных сценариях эксплуатации, включающих моделирование различных типов атак. В ходе испытаний были воспроизведены DDoS-атаки, попытки фишинга и эксплуатации уязвимостей. Результаты тестов подтвердили высокую точность классификации угроз и стабильность системы при обработке больших объемов данных. Система успешно распознает как известные угрозы, так и новые виды атак благодаря механизмам анализа аномалий. Гибкая и масштабируемая архитектура позволяет легко интегрировать разработку с существующими информационно-аналитическими платформами и расширять её функционал по мере необходимости.

В ближайшие годы можно ожидать развитие новых технологий в области ИТ-безопасности, таких как использование квантовых вычислений для усиленной защиты данных или внедрение систем защиты, основанных на блокчейн-технологиях. Это создаст новые возможности для улучшения существующих систем IDS и разработки более мощных и надежных инструментов защиты.

Внедрение системы автоматической идентификации и классификации угроз позволяет значительно снизить риски кибератак, что ведет к сокращению финансовых потерь и трудозатрат, связанных с устранением последствий инцидентов ИБ. Дополнительным преимуществом является снижение зависимости от внешних поставщиков и повышение информационной независимости компании. Экономические расчеты показали, что использование IDS помогает существенно сократить затраты на предотвращение угроз и повысить общую безопасность организации.

Созданная система представляет собой надежное и доступное решение для отечественных компаний, позволяя повысить уровень защиты информационно-аналитических систем, сократить время реакции на инциденты и минимизировать ущерб от кибератак.

После внедрения системы автоматической идентификации и классификации угроз значительное внимание стоит уделить ее поддержке и развитию, поскольку динамично изменяющиеся угрозы требуют постоянной адаптации системы к новым реалиям. Важнейшей частью является регулярное обновление базы данных угроз, совершенствование алгоритмов

машинного обучения и улучшение механизмов обнаружения аномалий. Это позволит системе оставаться эффективной и актуальной на протяжении длительного времени.

Кроме того, стоит отметить, что система IDS, как и любая другая компонент информационной безопасности, должна интегрироваться в общую экосистему защиты, что требует тесного взаимодействия с другими системами безопасности, такими как системы управления инцидентами (SIEM) [9], антивирусные решения и системы управления доступом. Эффективная интеграция IDS с этими системами позволит не только оперативно реагировать на инциденты, но и проводить глубокий анализ причин и последствий атак.

Важным аспектом является обучение персонала, работающего с системой. Даже самая продвинутая система IDS не будет эффективной без квалифицированного реагирования на предупреждения и инциденты. Специалисты, использующие систему, должны быть обучены правильной интерпретации результатов анализа и принятия своевременных мер для минимизации ущерба. Это также способствует повышению общей осведомленности сотрудников о текущих угрозах и улучшению процессов реагирования на инциденты.

Еще одной важной стороной внедрения системы является обеспечение ее масштабируемости. В современных организациях, работающих с большими объемами данных, необходимо гарантировать, что система будет справляться с увеличивающимся потоком информации, не теряя в эффективности. Масштабируемость должна учитывать не только количество данных, но и сложность анализа, которая будет возрастать по мере увеличения числа угроз и новых типов атак.

Для повышения устойчивости системы к современным угрозам и увеличения ее гибкости в будущем предполагается дальнейшая разработка и внедрение более сложных моделей на основе нейронных сетей, что позволит адаптироваться к новым типам атак без необходимости полной переработки алгоритмов. В частности, методики глубокого обучения (deep learning) [4] могут значительно улучшить точность обнаружения и классификации угроз, особенно в тех случаях, когда необходимо работать с большими объемами данных и сложно выявляемыми аномалиями.

Системы автоматической идентификации и классификации угроз могут также интегрироваться с различными облачными сервисами и платформами. В условиях быстро развивающихся технологий облачные решения становятся все более востребованными, и возможность интеграции IDS с облачной инфраструктурой будет играть важную роль в обеспечении безопасности гибридных и облачных ИАС. Это также обеспечит высокую доступность системы и минимизацию рисков, связанных с потерей данных или отказом оборудования.

Наконец, нельзя забывать о важности создания гибкой политики безопасности, которая будет учитывать особенности работы каждой отдельной организации. Успешная реализация системы IDS зависит от того, насколько она будет интегрирована в существующую инфраструктуру и насколько пользователи смогут адаптировать ее под свои специфические потребности. Это требует наличия функций кастомизации, включая настройку пороговых значений для тревог и настройку алгоритмов на основе специфики работы предприятия.

Заключение

В данной статье был проведен всесторонний анализ проблем безопасности информационно-аналитических систем и рассмотрены основные подходы к разработке системы автоматической идентификации и классификации угроз безопасности. Было показано, что угрозы информационной безопасности могут быть разнообразными, включая как внешние, так и внутренние атаки, а также ошибки конфигурации и человеческий фактор. Важно отметить, что традиционные методы обнаружения угроз, такие как сигнатурный анализ, не всегда способны эффективно противостоять новым, неизвестным угрозам, что подчеркивает необходимость в комплексных решениях, использующих аномальные и поведенческие методы.

Одной из ключевых задач в разработке системы IDS является способность эффективно классифицировать и анализировать угрозы, обнаруженные в информационной системе, чтобы предотвратить или минимизировать их последствия. В статье подробно рассмотрены различные методы анализа сетевого трафика, основанные на машинном обучении, а также применение нейросетевых технологий для прогнозирования угроз и выявления аномального поведения в реальном времени.

Для эффективной защиты информационных систем от внешних и внутренних угроз требуется не только использование специализированных программных решений, таких как IDS, но и внедрение организационных и правовых мер. Правильная настройка и постоянное совершенствование системы безопасности могут значительно повысить уровень защиты данных и предотвратить возможные инциденты.

Разработка системы автоматической идентификации и классификации угроз, как показано в статье, может значительно улучшить мониторинг и защиту информационно-аналитических систем, обеспечивая защиту как от традиционных, так и от более сложных атак. Внедрение таких решений требует глубокого анализа существующих угроз, использования современных технологий анализа данных и постоянного обновления системы для защиты от новых типов угроз.

Список литературы

1. Николаева М.О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации // Журнал: Мониторинг. Образование. Безопасность. – 2023. – С. 51-57.
2. Чапис М.А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере // Журнал: НАУКОСФЕРА – 2024. – С. 551-557
3. Добродеев А.Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности. // Журнал: Труды ЦНИИС. Санкт-петербургский филиал – 2020. – С. 50-78
4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. - 2nd Edition. - No Starch Press, 2013.
5. Kshetri, N. Cybersecurity and International Relations: An Introduction. – 2020. – Т. 8. – No. 3. – pp. 11-18.
6. Northcutt, S., & Novak, J. Network Intrusion Detection. – 3rd Edition. – New Riders, 2003.

7. Debar, H., Dacier, M., & Scuteri, M. A survey of intrusion detection systems. – Computer Networks. – 1999. – T. 31. – No. 8. –pp. 1007-1021.
8. Sommer, R., & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. – 2010. – ACM Transactions on Information and System Security. – T. 13. – No. 3. – p. 6.
9. Ziegler, K., & Huitema, C. "Application of Machine Learning in Intrusion Detection Systems." – IEEE Communications Surveys & Tutorials. – 2022. – T. 24. – No. 1. – pp. 58-72.
10. Chabaud, F., & Ren, L. Behavioral Anomaly Detection for Intrusion Prevention Systems. – Springer, 2021.
11. Bace, R. Network Intrusion Detection. – 2nd Edition. – Sams Publishing, 2000.
12. Zhang, Z., & Zeng, X. A Survey of Intrusion Detection Systems Using Data Mining Techniques. – Journal of Network and Computer Applications. – 2022. – T. 133. – pp. 118-126.
13. Li, X., & Wang, W. A Review of Signature-Based Intrusion Detection Systems. – Journal of Computer Science and Technology. – 2021. – T. 36. – p. 101-113.
14. Breiman, L. Random Forests. – Machine Learning. – 2001. – T. 45. – p. 5-32.

References

1. Nikolaeva M.O. Information security: a modern picture of the problem of information security and information protection // Journal: Monitoring. Education. Safety. – 2023. – pp. 51-57.
2. Chapis M.A. Information security of the state as a legal procedure for ensuring national security in the information sphere // Journal: NAUKOSPHERE – 2024. – pp. 551-557
3. Dobrodeev A.Yu. Information security indicators as a characteristic (measure) of the compliance of communication networks and organizations with information security requirements. // Journal: Proceedings of the Central Research Institute. St. Petersburg branch – 2020. – pp. 50-78
4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. - 2nd Edition. - No Starch Press, 2013.
5. Kshetri, N. Cybersecurity and International Relations: An Introduction. – 2020. – T. 8. – No. 3. – pp. 11-18.
6. Northcutt, S., & Novak, J. Network Intrusion Detection. – 3rd Edition. – New Riders, 2003.
7. Debar, H., Dacier, M., & Scuteri, M. A survey of intrusion detection systems. – Computer Networks. – 1999. – T. 31. – No. 8. – pp. 1007-1021.
8. Sommer, R., & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. – 2010. – ACM Transactions on Information and System Security. – T. 13. – No. 3. – p. 6.
9. Ziegler, K., & Huitema, C. "Application of Machine Learning in Intrusion Detection Systems." – IEEE Communications Surveys & Tutorials. – 2022. – T. 24. – No. 1. – pp. 58-72.
10. Chabaud, F., & Ren, L. Behavioral Anomaly Detection for Intrusion Prevention Systems. – Springer, 2021.
11. Bace, R. Network Intrusion Detection. – 2nd Edition. – Sams Publishing, 2000.

12. Zhang, Z., & Zeng, X. A Survey of Intrusion Detection Systems Using Data Mining Techniques. – Journal of Network and Computer Applications. – 2022. – Т. 133. – pp. 118-126.
13. Li, X., & Wang, W. A Review of Signature-Based Intrusion Detection Systems. – Journal of Computer Science and Technology. – 2021. – Т. 36. – pp. 101-113.
14. Breiman, L. Random Forests. – Machine Learning. – 2001. – Т. 45. – pp. 5-32.