4. Обучение на нерепрезентативных данных. Если модель обучается на данных, которые не отражают всю разнообразность ситуаций или популяций, она может выдавать неточные или смещенные результаты.

5. Подготовка специалистов. Внедрение ИИ в науку и образование требует подготовки кадров, способных эффективно использовать и внедрять технологии ИИ [3]. Это вызывает необходимость в развитии соответствующих образовательных программ.

6. Безопасность данных. Обработка больших объемов данных требует высокого уровня безопасности, чтобы предотвратить утечки данных, манипуляции или несанкционированный доступ.

7. Финансовые затраты. Разработка и внедрение технологий ИИ может требовать значительных финансовых ресурсов, что может быть вызовом для некоторых учебных и научных учреждений.

В заключение можно отметить, что применение искусственного интеллекта в науке и образовании актуально и перспективно, поскольку оно не только улучшает процессы исследований, но и трансформирует методы обучения, делая их более эффективными и доступными. Необходимо учитывать этические аспекты и продолжать развивать ИИ с учетом потребностей образования и научных исследований для достижения более устойчивого и разностороннего прогресса.

Список литературы

1. Коровникова Н.А. Искусственный интеллект в современном образовательном пространстве: проблемы и перспективы // Социальные новации и социальные науки. 2021. № 2 (4). С. 98-113.

2. Ендовицкий Д.А., Гайдар К.М. Университетская наука и образование в контексте искусственного интеллекта // Высшее образование в России. 2021. № 6. С. 121-131.

3. Соколов Н.В., Виноградский В.Г. Искусственный интеллект в образовании: анализ, перспективы и риски в РФ // Проблемы современного педагогического образования. 2022. № 76-2. С. 166-169.

4. Аширалиева М.А., Мыратлыев Б. Искусственный интеллект в современной науке // Вестник науки. 2023. № 6 (63). С. 869-872.

5. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2016. 578 с.

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ КЛАССИФИКАЦИИ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Андрияхов Я.В.

ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Москва, e-mail: yarik-and@mail.ru

В современном цифровом мире проблематика в области информационной безопасности и управления событиями становится всё более сложной и разнообразной. Одной из ключевых трудностей является рост объёмов данных, требующих анализа для выявления угроз. Это ставит под угрозу эффективность традиционных систем безопасности, так как они зачастую не справляются с новым масштабом задач, приводя к пропуску важных инцидентов. С увеличением сложности кибератак требуется более глубокий анализ данных, что выходит за рамки возможностей стандартных автоматизированных систем и создаёт дополнительную нагрузку на специалистов, отвлекая их от более важных задач [8, с. 51-52].

В статье рассмотрены предложения по реализации продвинутых систем обработки естественного языка, таких как крупномасштабные языковые модели (LLM), которые могут быть использованы в рамках функционала SIEM-систем (Security Information and Event Management). SIEM-системы представляют собой комплексные системы, предназначенные для сбора, агрегации и анализа данных о событиях безопасности из множества источников. Они обеспечивают нормализацию данных, обнаружение аномалий, генерацию оповещений и предоставляют инструменты для визуализации и отчетности, что является важным элементом в стратегии обеспечения информационной безопасности.

LLM-модели, обученные на больших объёмах текстовых данных, обладают способностью к глубокому пониманию и интерпретации естественного языка, что позволяет им создавать осмысленные тексты, анализировать данные и поддерживать процессы принятия решений. В контексте SIEM-системы, LLM-модели обеспечивают эффективную обработку больших объемов данных, выявлять сложные угрозы и автоматизировать рутинные задачи, тем самым ускоряя обнаружение инцидентов и снижая нагрузку на специалистов [7, с. 59]. Это значительно повышает эффективность систем управления информационной безопасностью и помогает организациям адаптироваться к постоянно меняющемуся ландшафту кибербезопасности.

Нейросетевые технологии в решении задач автоматизации процессов классификации и реагирования на инциденты информационной безопасности

Наличие SIEM-системы в инфраструктуре автоматизирует процесс обработки событий. Автоматизация достигается при помощи алгоритмов нормализации и корреляции событий. События внутри SIEM-системы проходят следующую цепочку обработки (рис 1).

Модуль приема событий принимает события для дальнейшей обработки, а также добавляет метку со временем поступления события в SIEM.

Модуль нормализации событий реализует процедуру приведения необработанных событий к нормализованному виду в соответствии с заданными для источника и типа событиями правилами нормализации.

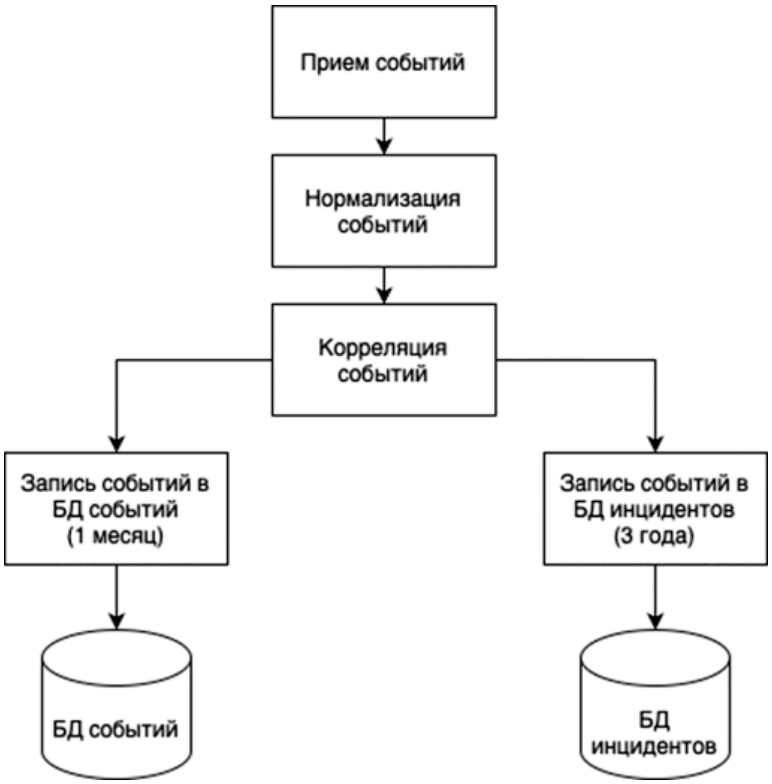

Рис. 1. Схема обработки событий информационной безопасности

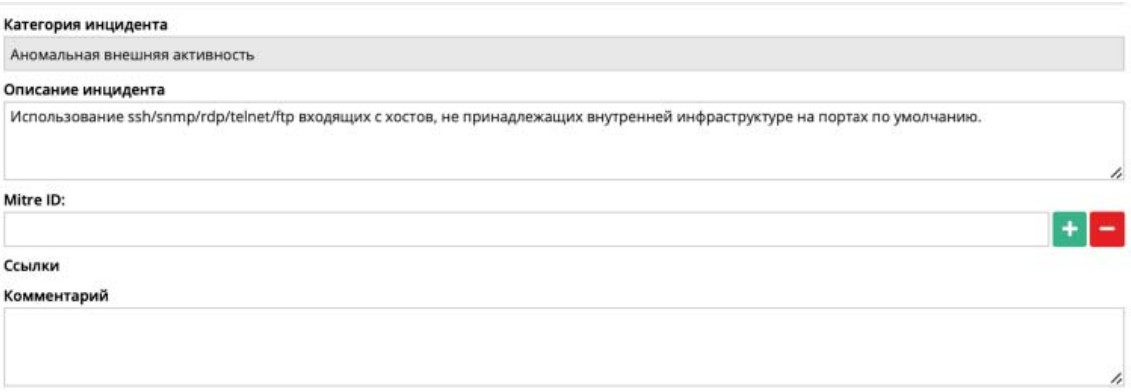

Рис. 2. Карточка инцидента

Модуль корреляции событий реализует анализ нормализованных событий согласно корреляционным правилам на наличие заданных цепочек взаимосвязей.

После обработки данными модулями события записываются в “БД событий” для их хранения (В нашем случае в течении месяца). Если какие-то события вызвали инцидент, то информация о них дублируется в “БД инцидентов” на долгосрочный период (В нашем примере в течение 3 лет) [1, с. 71].

Правила корреляции могут дополнительно обогащать информацию следующими типами данных: описание инцидента, информацию из перечня уязвимостей CVE. Карточка инцидента, представленная на рисунке 2, включает следующее описание инцидента в SIEM-системе: Категорию инцидента, информацию об инциденте, MITRE ID – уникальный идентификатор инцидента, соответствующий базе знаний MITRE ATT&CK (общедоступная база знаний действия нарушителя), а также комментарий к данному инциденту [8].

В представленном описании не в полной мере содержаться сведения для достоверной идентификации и приоритизации инцидента. Все эти данные добавляются на этапе создания правила корреляции и скорее относятся к зара-

нее заготовленному шаблону, а не к произошедшему инциденту. Для дальнейшей обработки инцидента обязательно наличие высококвалифицированного специалиста первой линии. Этапы обработки инцидента при такой схеме представлены на рисунке 3 [5].

К основным задачам сотрудников первой линии (L1) относятся: категоризация, приоритизация и анализ событий ИБ. Данные шаги, как правило, занимают значительное время и практически не автоматизированы в типовой SIEM-системе, в том числе не обеспечивают необходимую степень достоверности [2, с. 3–7].

В свою очередь LLM-модели могут обеспечивать адекватное описание исходя из конкретных событий, которые вызвали инциденты, и давать комплексное описание, а также проводить приоритизацию, исходя из более глубоко анализа. С использованием LLM-моделей анализ событий реализуется следующим образом.

В SIEM-системе формируется запрос по API-интерфейсу к LLM-модели о возникшем инциденте ИБ (рис 4).

На основе LLM-модели производится анализ полученных событий, используя алгоритмы обработки естественного языка, результатом чего является построение аналитических цепочек, соответствующих следующим возможным инцидентам: вирусным атакам, несанкционированному доступу, техническим сбоям и т.д.

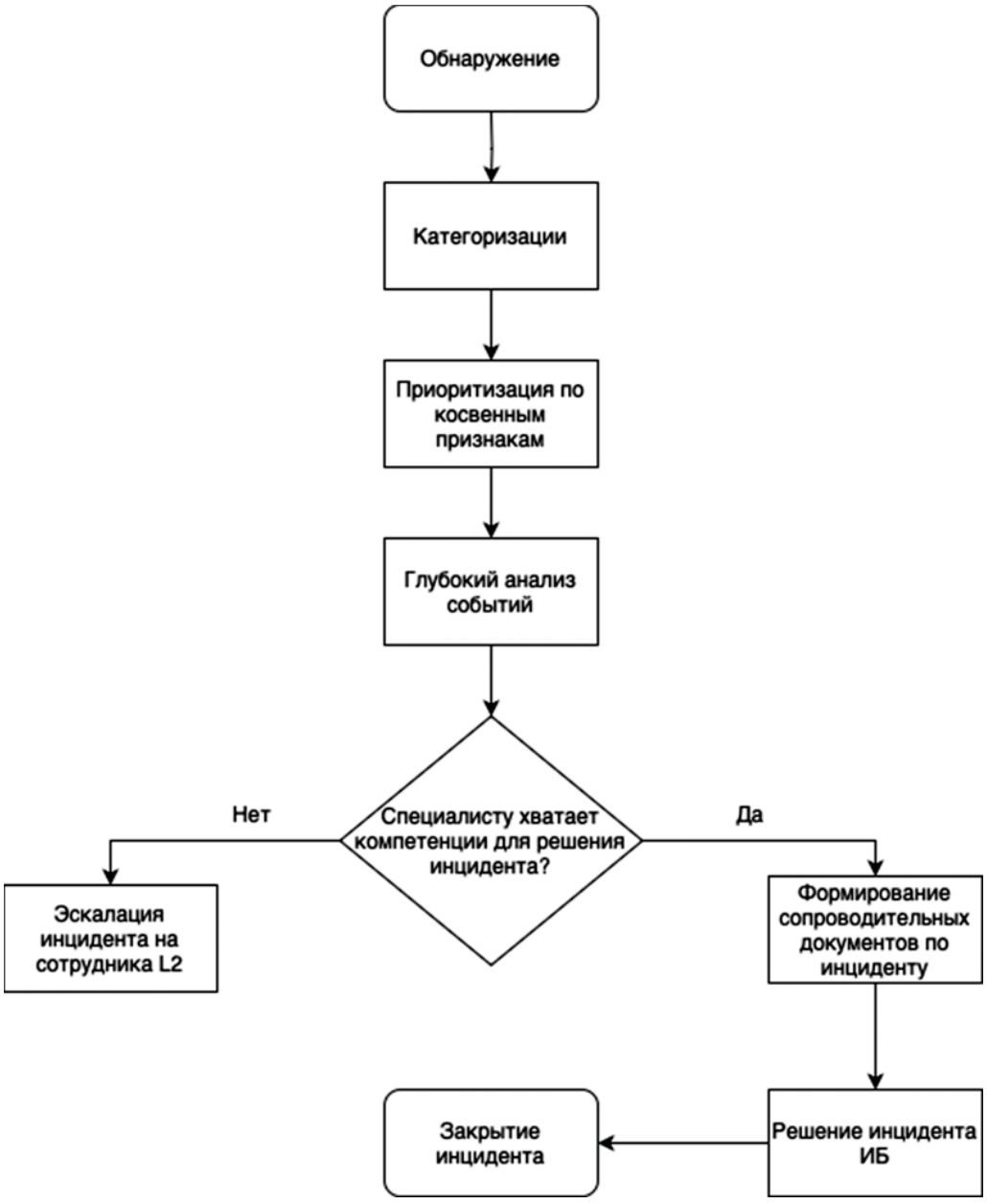

Рис. 3. Этапы обработки инцидента на первой линии

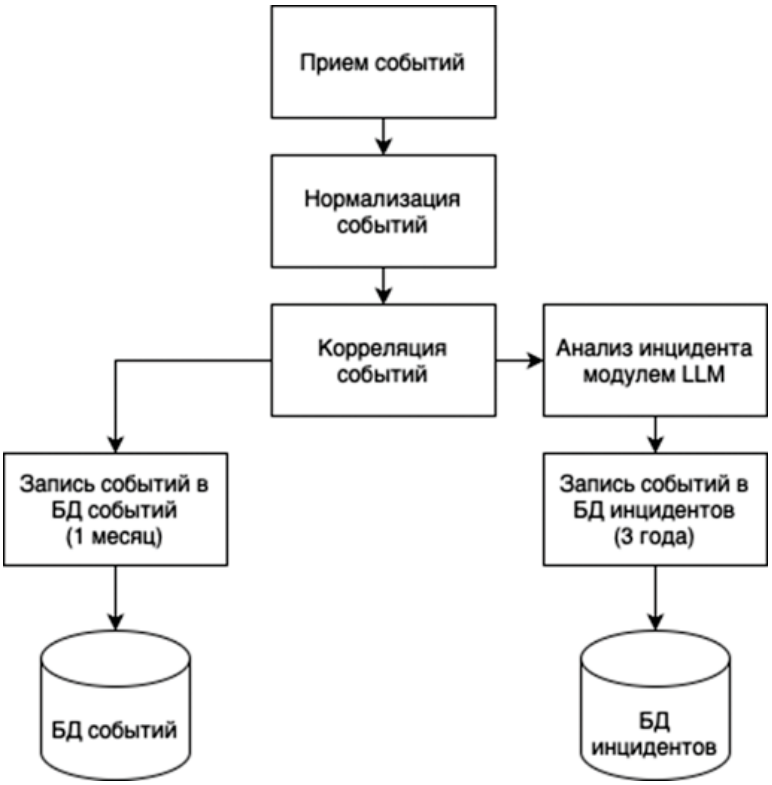

Рис. 4. Схема обработки событий информационной безопасности с использованием LLM-модели

В результате использования крупномасштабных языковых моделей в обработке инцидентов информационной безопасности, достигается более глубокий анализ каждого события и категоризация инцидентов. Это включает учет контекста, истории событий и их потенциального влияния на организацию, а также анализ поведенческих шаблонов, сравнение с известными угрозами и оценку вероятности ложных тревог. Такой подход позволяет более точно приоритизировать события, опираясь на уровень риска, влияние на бизнес-процессы и потенциальную угрозу для ключевых активов организации. [3, с 234-236].

Кроме того, использование LLM-моделей облегчает процесс подготовки подробных описаний каждого инцидента, включая контекст, вероятные причины и предложения по дальнейшим действиям. Эти описания обеспечивают специалистам первого уровня (L1) более оперативную обработку и глубокое понимание проблем, что способствует эффективному и оперативному реагированию. В дополнение, LLM-модели могут предоставлять рекомендации по реагированию на инциденты, основанные на лучших практиках и анализе предыдущих событий, что значительно ускоряет процесс принятия решений и повышает качество управления инцидентами. Таким образом, интеграция LLM-моделей в системы управления инцидентами позволяет повысить общую эффективность и точность процессов в области информационной безопасности [4].

Проанализируем инцидент: “Infotecs IDS: Попытка эксплуатации уязвимости ETERNALBLUE.” Описание которого представлена на рисунке 5.

На представленном рисунке демонстрируются результаты, полученные на основе крупномасштабной языковой модели. На основе анализа событий, были получены уточненные детали инцидента при помощи крупномасштабной языковой модели, превосходящие общее описание «Удаленного выполнения кода». С помощью LLM-модели были выявлены более конкретные и точные сведения о происходящих событиях. Кроме того, с использованием этой модели были разработаны специфические рекомендации по решению проблемы, связанной с конкретным IP-адресом, что демонстрирует её эффективность в предоставлении направленных и практических советов для ответа на инцидент. Результаты, показанные на рисунке 6, демонстрируют, как будет проходить расследование инцидента для инженера первой линии, исходя из полученных данных.

Данная интеграция позволяет существенно сократить время необходимое на обработку инцидентов, а также снизить нагрузку на специалистов второй линии за счет снижения необходимых компетенций для специалистов первой линии.

Категория инцидента

Удаленное выполнение кода

Описание инцидента

Категория инцидента: Атака на сетевые службы
Приоритет инцидента: Критический

Описание инцидента:
В системе Infotecs IDS зарегистрирована попытка эксплуатации уязвимости ETERNALBLUE на IP-адресе 172.16.0.9. Инцидент был создан после обнаружения 45 событий, связанных с данной попыткой эксплуатации.

Шаги по решению для специалиста L1:
1. Проверить бэкапы и целостность данных на сервере с IP-адресом 172.16.0.9.
2. Изолировать сервер с IP-адресом 172.16.0.9 от остальной сети и пропустить его через анализатор трафика для дальнейшего обнаружения аномалий.
3. Провести анализ журналов безопасности и событий на сервере с IP-адресом 172.16.0.9 для выявления следов атаки и определения действий злоумышленников.
4. Обновить все системы и программное обеспечение на сервере с IP-адресом 172.16.0.9 до последней версии, установить необходимые патчи и обновления безопасности.
5. Проверить сетевые настройки сервера и наличие открытых портов, связанных с эксплуатацией уязвимости ETERNALBLUE. Закрыть ненужные порты.
6. Провести аудит системы безопасности, включая системы антивирусной защиты, брандмауэры и механизмы обнаружения вторжений.
7. Рассмотреть возможность применения дополнительных мер безопасности, таких как внедрение двухфакторной аутентификации, использование белых списков и ограничение прав доступа.
8. Следить за дальнейшими событиями и активностью на сервере с IP-адресом 172.16.0.9 и реагировать на любую подозрительную активность.

Рис. 5. Сгенерированное описание в карточке инцидента

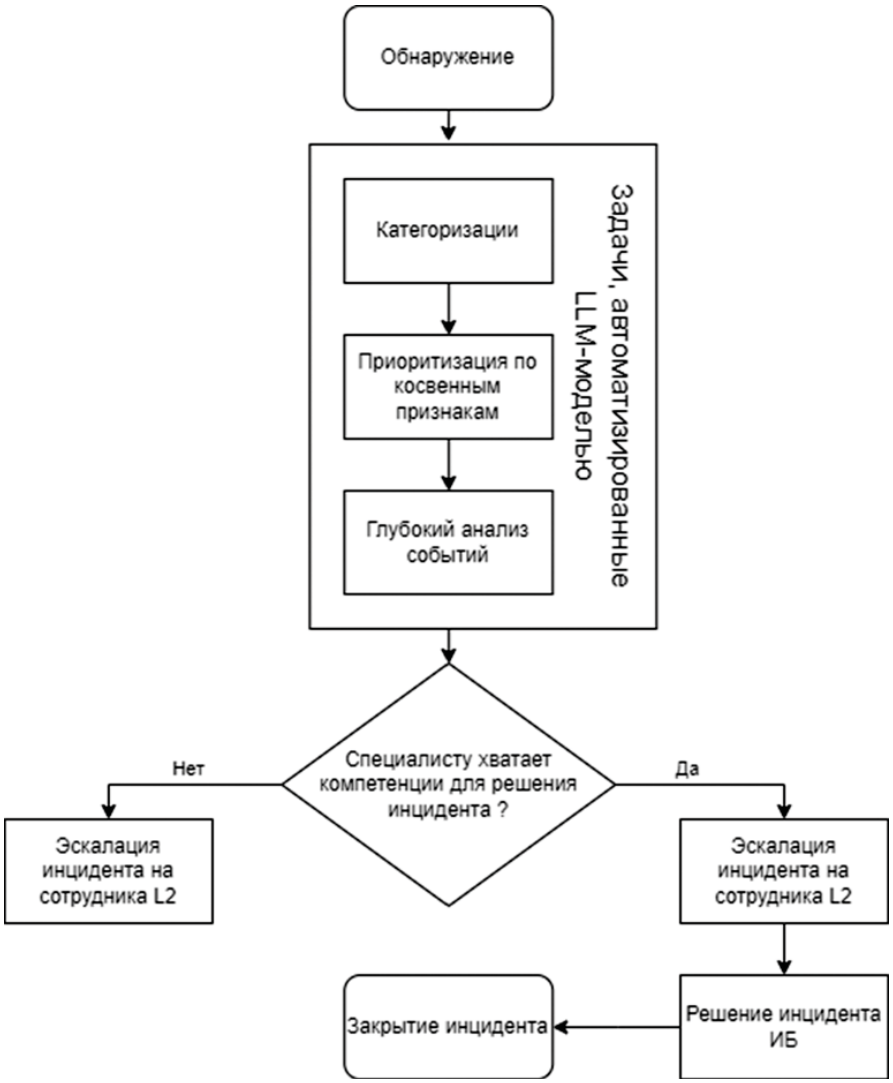

Рис. 6. Схема автоматизации обработки инцидентов

Исходя из рисунка можно сделать вывод, что осуществляется автоматизация следующих процессов: категоризация инцидентов, приоритизация инцидента, глубокий анализ событий информационной безопасности. Был реализован пилотный проект по внедрению LLM-модели в организацию, в результате которого были получены следующие результаты:

Среднее время решения инцидентов снизилось с 145 минут до 126 минут для специалистов первой линии.

Среднее количество ошибок LLM-модели в первую неделю составило около 4 ошибок на 10 инцидентов. Через месяц уровень выдачи ложных результатов анализа снизился до 2 ошибок на 10 инцидентов.

Приоритизация, инцидентов полученная в ходе анализа, полностью соответствует требованиям отдела информационной безопасности организации.

Количество инцидентов, закрытых аналитиками первой линии, увеличилось на 9%. Таким образом, обеспечено снижение поток инцидентов эскалированных на аналитиков второй линии.

Заключение

LLM-модель значительно расширяет возможности SIEM-систем, обеспечивая более глубокий анализ данных и более точное обнаружение угроз. Интеграция LLM-моделей в SIEM-системы позволяет автоматизировать многие процессы, связанные с обработкой и анализом больших объемов данных, что повышает эффективность системы безопасности. Однако стоит использовать локальные LLM-модели для обеспечения конфиденциальности данных, производить непрерывное обучение и адаптацию этих моделей к изменяющимся условиям кибербезопасности.

Данная интеграция позволяет существенно сократить время, необходимое на обработку инцидентов, а также снизить нагрузку на специалистов второй линии за счет снижения необходимых компетенций для специалистов первой линии.

Список источников

1. Сизов В.А. Киров А.Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. 2020. №24. С. 69-79.

2. Клюев С.Г., Трунов Е.Е. Проблемы обучения глубоких нейронных сетей для обнаружения угроз нарушения безопасности в сетях с динамической топологией // моделирование, оптимизация и информационные технологии. 2021. № 32. DOI: 10.26102/2310-6018/2021.32.1.012.

3. Аверкин А.Н., Афанасьев С.Д., Микрюков А.А., Паджев В.В., Райков А.Н., Хохлов Ю.Е., Храмцовская Н.А. Стандартизация работы с большими данными: международные и национальные стандарты // Информационное общество. 2021. № 4-5. С. 220-258.

4. Сизов В.А., Киров А.Д. Метод двухэтапной нечеткой кластеризации инцидентов кибербезопасности для субъектов экономической деятельности // Прикладная информатика. 2023. Т. 18, № 5(107). С. 77-90. DOI: 10.37791/2687-0649-2023-18-5-77-90.

5. Очередько А.Р., Герасименко В.С., Путято М.М., Макарян А.С. Исследование SIEM-систем на основе анализа механизмов выявления кибератак // Вестник Адыгейского государственного университета. 2020. № 59. С. 25-31.

6. Микрюков А.А., Бабаш А.В., Сизов В.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий. Открытое образование. 2019. Т. 23, № 1. С. 57-63.

7. Микрюков А.А., Усцелемов В.Н. Гибридная модель оценки рисков в информационных системах // Прикладная информатика. 2014. № 1 (49). С. 50-55.

8. Корпоративные SIEM ловят всего 24% техник MITRE ATT&CK! На кой они тогда нужны? // SecurityLab. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/353009.php (дата обращения: 20.10.2023).

ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ ТОЧЕК ДОСТУПА ДЛЯ WI-FI: МАКСИМИЗАЦИЯ ПОКРЫТИЯ И КАЧЕСТВА СИГНАЛА

Артушян О.А., Аветисян Т.В.

Колледж Воронежского института высоких технологий, Воронеж, e-mail: vtatyana_avetisyan@mail.ru

В наши дни тяжело представить, что в какой-то современной организации или в здании не будет Wi-Fi. В современное время во всем обществе стремительными темпами увеличивается потребность в беспроводной сети Wi-Fi, используя в качестве среды передачи данных радиоканал, что никак не потребует присутствия специализированных проводных соединений клиентов с сетью. Технология беспроводных сетей считается более комфортной в обстоятельствах, требующих мобильность, несложность сборки устройства и применения ее на практике. Обычно Wi-Fi применяется для локальной сети устройств и для обеспечения высокоскоростного доступа в интернет. Беспроводная сеть дает возможность людям устанавливать и получать доступ к приложениям и информации без применения проводов, а это гарантирует свободу в перемещении и использовать приложения, которые пребывают в других местах.

Для того, чтобы обеспечить надежное и стабильное подключение к Wi-Fi, необходимо правильно разместить точки доступа в пространстве. Разберемся, какие факторы влияют на эффективность работы Wi-Fi, как выбрать место для размещения точек доступа и каким образом оптимизировать сеть для достижения максимальной производительности.

Рекомендации по размещению устройств точек доступа в помещение могут включать следующие советы [1, 2]:

1. Избегайте установки точек доступа в металлических или бетонных стенах, так как это может ухудшить качество сигнала (рисунок 1).

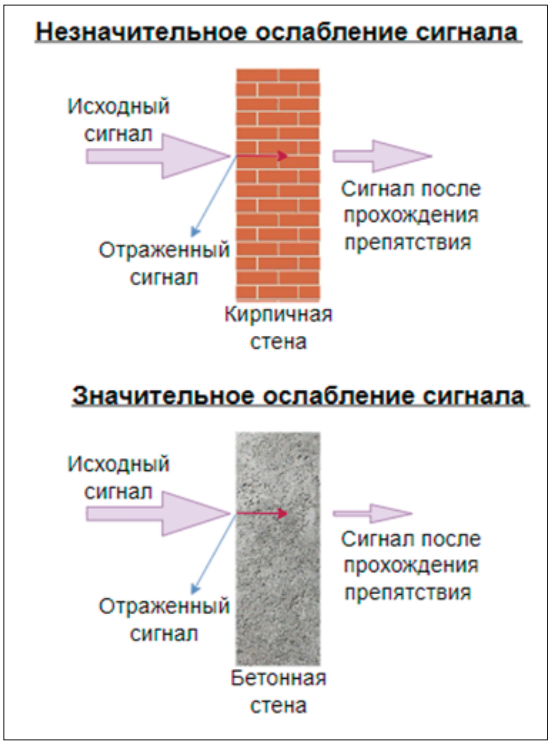

Рис. 1. Сигнал после прохождения препятствия

2. Размещайте точки доступа на высоте около 2 метров от пола, чтобы избежать пересечения сигнала с мебелью и препятствиями на пути. Общепринятая рекомендация – расстояние между точками доступа должно быть не более 15-20 метров в помещении с нормальной степенью загрузки. Однако, если пользователи находятся на большом расстоянии от точки доступа или на пути могут появиться препятствия, такие как стены и двери, то расстояние может быть уменьшено до 7-10 метров (рисунок 2).

3. Размещайте точки доступа в центре офиса для максимального покрытия зоны сигналом.