УДК 004.4

Крузина Алина Алексеевна, *магистрант,*

ФГБОУ ВО «МИРЭА - Российский технологический университет».

ОБЗОР ПРИМЕНЕНИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В КИБЕРБЕЗОПАСНОСТИ

В статье рассмотрены современные системы поддержки принятия решений (СППР) в области кибербезопасности, их роль в выявлении и предотвращении киберугроз. Проведен обзор существующих российских решений и основных методов, используемых в СППР, включая машинное обучение и интеллектуальный анализ данных. Обсуждаются направления развития таких систем, в частности применение предиктивного анализа и искусственного интеллекта для повышения эффективности защиты информационных систем. Сделан вывод о необходимости дальнейшего совершенствования СППР для более проактивного и комплексного обеспечения безопасности.

Ключевые слова: система поддержки принятия решений, кибербезопасность, интеллектуальный анализ данных, прогнозирование угроз, информационная безопасность, защита данных.

The article reviews modern decision support systems (DSS) in cybersecurity and their role in detecting and preventing cyber threats. It provides an overview of existing Russian solutions and key methods used in DSS, including machine learning and intelligent data analysis. Development trends such as predictive analysis and artificial intelligence are discussed to improve information system protection. The conclusion highlights the need for further improvement of DSS for more proactive and comprehensive security.

Key words: decision support systems, cybersecurity, intelligent data analysis, threat prediction, information security, data protection.

Введение

В 2024 году наблюдается значительный рост количества и сложности киберугроз. Согласно данным аналитического отчета компании BI.ZONE за первое полугодие 2024 года, было зафиксировано увеличение количества киберинцидентов на 40% по сравнению с аналогичным периодом прошлого года. Большинство киберинцидентов было зафиксировано в промышленности (38%), IT-отрасли (27%) и финансовой сфере (15%) [1].

В условиях увеличения числа киберинцидентов возрастает необходимость в эффективных инструментах для их предотвращения и минимизации последствий. Системы поддержки принятия решений (СППР) в кибербезопасности становятся ключевыми компонентами в обеспечении защиты информационных систем, позволяя не только реагировать на инциденты, но и предсказывать их развитие, оценивать риски и предлагать оптимальные меры реагирования.

Литературный обзор

Актуальность использования систем поддержки принятия решений (СППР) в кибербезопасности обусловлена необходимостью оперативной обработки больших объёмов разнородных данных, выявления инцидентов и выбора адекватных мер реагирования. СППР позволяют автоматизировать аналитическую составляющую работы специалистов, формируя на основе формальных моделей и алгоритмов рекомендации по минимизации угроз и последствий кибератак.

В работе Кожухиной А. В. и Бурнаковой А. А. [2] рассматривается применение методов поддержки принятия решений в целях обеспечения информационной безопасности. Авторы акцентируют внимание на необходимости автоматизации и формализации выбора защитных мероприятий, особенно в условиях усложняющейся информационной инфраструктуры. В качестве одного из подходов анализируется метод анализа иерархий,

позволяющий учитывать множество критериев при выборе оптимальных решений по предотвращению утечек данных. Такой подход способствует более обоснованному и структурированному принятию решений в области ИБ.

Интерес к интеллектуальным методам в СППР демонстрируют Авдошин и соавторы [3], рассматривающие применение алгоритмов машинного обучения в задачах кибербезопасности. Приведены примеры построения моделей классификации и обнаружения аномалий на основе поведенческого анализа, в том числе с использованием нейросетевых архитектур. Это подтверждает тенденцию перехода от классических СППР к интеллектуализированным системам с возможностями самонастройки и адаптации.

Полтавцева и Печенкин [4] в своей работе акцентируют внимание на внедрении методов интеллектуального анализа данных в СППР, предназначенные для поддержки процесса тестирования на проникновение. Разработка использует принципы машинного обучения для автоматизации этапов анализа уязвимостей и построения оптимальных сценариев атак, что снижает нагрузку на экспертов и ускоряет цикл оценки защищённости.

Таким образом, проведённый анализ отечественных исследований демонстрирует, что в российской научной среде активно ведётся работа над развитием СППР в сфере кибербезопасности. Преобладают подходы, основанные на машинном обучении, моделировании угроз и оценке рисков. Однако остаётся значительный потенциал для расширения проактивных функций таких систем, включая прогнозирование последствий атак, моделирование цифровых двойников инфраструктуры и автоматическую адаптацию защитных стратегий — что на данный момент в исследованиях представлено фрагментарно и требует дальнейшего развития.

Определение и классификация СППР

Система поддержки принятия решений (СППР) — это компьютерная автоматизированная система, предназначенная для помощи лицам,

принимающим решения, в условиях неопределенности и сложности, путем предоставления необходимой информации и аналитических инструментов [5].

Существует множество подходов к классификации СППР. Рассмотрим наиболее распространенные:

По взаимодействию с пользователем:

- **Пассивные**: предоставляют информацию, но не предлагают конкретных решений.
- **Активные**: предлагают конкретные решения на основе анализа данных.
- **Кооперативные**: взаимодействуют с пользователем в процессе выработки решения.

По концептуальному подходу:

- **Управляемые сообщениями (Communication-Driven DSS)**: поддерживают коммуникацию между участниками процесса принятия решений.
- **Управляемые данными (Data-Driven DSS)**: фокусируются на анализе больших объемов данных.
- **Управляемые документами (Document-Driven DSS)**: работают с неструктурированной информацией.
- **Управляемые знаниями (Knowledge-Driven DSS)**: используют базы знаний и правила для выработки решений.
- **Управляемые моделями (Model-Driven DSS)**: опираются на математические и статистические модели

По техническому уровню:

- **Корпоративные СППР**: интегрированы в инфраструктуру предприятия и обслуживают множество пользователей.
- **Настольные СППР**: предназначены для индивидуального использования.

По сфере применения:

- **Общесистемные**: используются в крупных организациях с большими объемами данных.
- **Функциональные**: ориентированы на поддержку решений в конкретных функциях управления.

Анализ существующих классификаций систем поддержки принятия решений показывает их многообразие и комплексность, что отражает широкий спектр подходов и задач, решаемых данными системами.

Существующие СППР в кибербезопасности

На российском рынке представлены несколько решений, содержащих элементы СППР:

Security Vision: интеграционная платформа класса SOAR, поддерживающая автоматизацию процессов обработки инцидентов, содержит преднастроенные сценарии реагирования и модуль выработки рекомендаций на основе экспертных правил [6].

R-Vision TIP: платформа для сбора и анализа данных об угрозах с функциями корреляции и приоритизации инцидентов, поддерживающая принятие решений в области кибербезопасности [7].

F6 Threat Intelligence: система анализа угроз, предоставляющая контекстную информацию по индикаторам компрометации и обоснованные рекомендации, использует методы приоритизации и классификации угроз на основе контекста инфраструктуры [8].

Современные решения в области кибербезопасности, такие как платформы SIEM, SOAR и TIP, обладают широкими возможностями для мониторинга, корреляции событий и автоматизации реагирования, а также включают базовые функции поддержки принятия решений на основе анализа данных и экспертных правил. Они эффективно собирают и обрабатывают разнородную информацию, что помогает специалистам своевременно выявлять и устранять инциденты безопасности. Однако возможности проактивного прогнозирования последствий

кибератак и моделирования сценариев их развития в этих системах пока реализованы весьма ограниченно и не обеспечивают комплексного упреждающего анализа.

Направления развития СППР в киберезопасности

Для повышения эффективности защиты информационных систем в условиях постоянно меняющегося ландшафта киберугроз требуется целенаправленное развитие систем поддержки принятия решений, обеспечивающих предиктивные и адаптивные возможности. Прежде всего, СППР должны ориентироваться на проактивный анализ потенциальных угроз, позволяя прогнозировать последствия кибератак до их реализации. Такой подход требует системной интеграции с широким спектром источников данных — от результатов внутренней инвентаризации активов до внешней разведки угроз (threat intelligence), что обеспечивает формирование целостной и актуальной картины состояния информационной безопасности предприятия.

Важным направлением эволюции СППР становится внедрение методов машинного обучения и искусственного интеллекта. Эти технологии позволяют автоматизировать обнаружение аномалий в поведении пользователей и систем, предсказывать возможные инциденты и вырабатывать предложения по реагированию на них в режиме реального времени. Кроме того, современные ИС нуждаются в системах, обладающих высокой адаптивностью и масштабируемостью. Это означает, что СППР должны эффективно функционировать как в условиях локальной инфраструктуры, так и в распределённых средах, таких как облачные и гибридные решения, а также иметь возможность подстраиваться под динамику развития бизнес-процессов и инфраструктуры.

Развитие систем в указанном направлении обеспечит не только своевременное реагирование на инциденты информационной безопасности, но и позволит существенно повысить уровень превентивной защиты. В результате снижается потенциальный ущерб от атак, повышается устойчивость

информационной системы к внешним и внутренним угрозам, а также оптимизируются ресурсы, затрачиваемые на обработку инцидентов.

Заключение

Системы поддержки принятия решений играют ключевую роль в обеспечении кибербезопасности, позволяя анализировать угрозы, прогнозировать развитие инцидентов и вырабатывать оптимальные меры реагирования. Несмотря на наличие ряда решений на российском рынке, существует необходимость в разработке более продвинутых СППР, способных проводить проактивный анализ и предсказывать последствия потенциальных атак. Интеграция таких систем в инфраструктуру информационной безопасности позволит повысить устойчивость организаций к киберугрозам и обеспечить более эффективную защиту информационных ресурсов.

Использованные источники

1. Киберинциденты в 2024: что показал отчет BiZone? // SecurityLab URL: https://www.securitylab.ru/news/550454.php (дата обращения: 15.05.2025).

2. Кожухина А.В., Бурнакова А.А. Обеспечение информационной безопасности с помощью применения методов принятия решений // Молодой ученый. - 2022. - №49. - С. 8-12.

3. Авдошин С.М., Лазаренко А.В., Чичилева Н.И., Наумов П.А., Ключарев П.Г. Примеры использования машинного обучения в кибербезопасности // Труды Института системного программирования РАН. - 2019. - №31(5). - С. 191-202.

4. Полтавцева М.А. Печенкин А.И. Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение // Проблемы информационной безопасности. Компьютерные системы. - 2017. - №3. - С. 62-69.

5. Карташов Г.П., Корбин Е.К. Классификация систем поддержки принятия решений для использования в системе управления событиями и информацией о безопасности // Молодой ученый. - 2023. - №37. - С. 9-10.

6. SOAR // Security Vision URL: https://www.securityvision.ru/products/soar/ (дата обращения: 15.05.2025).

7. R-Vision TIP // R-Vision URL: https://rvision.ru/products/tip (дата обращения: 15.05.2025).

8. Threat Intelligence // F6 URL: https://www.f6.ru/products/threat-intelligence/ (дата обращения: 15.05.2025).

kruzina.alina@gmail.com