Охотин Данил Александрович, студент,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко», г. Краснодар

Енин Дмитрий Николаевич, студент
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко»г. Краснодар

Хечиев Наран Валерьевич, студент,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко». г. Краснодар

Акишин Андрей Владимирович, Доцент,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко».г. Краснодар

Панкратова Марина Николаевна,
младший научный сотрудник,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко».г. Краснодар

СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДПРИЯТИЯХ И ОРГАНИЗАЦИЯХ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ВОЗНИКНОВЕНИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В статье рассматривается классификация систем поддержки принятия решений (СППР) для подразделений информационной безопасности в российских предприятиях и организациях. Их функциональные возможности и роль в противодействии современным киберугрозам. Предложены перспективы развития данного направления с учетом специфики российской практики.

Ключевые слова: Орган защиты информации, защита информации, система поддержки принятия решения, информационная безопасность.

Термины и определения:

Орган защиты информации – подразделение, выполняющее функции, направленные на защиту информацию.

Защита информации (ЗИ) – совокупность правовых, организационных и технических мер, направленных на предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения; соблюдения конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации [1].

Система поддержки принятия решений (СППР) – компьютерная автоматизированная система, целью которой является помощь людям, принимающим решения в сложных условиях для полного и объективного анализа предметной деятельности [2].

Угроза информационной безопасности – это совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере [3].

Введение. В условиях возрастающей зависимости организаций от информационных технологий, проблема обеспечения информационной безопасности приобретает критическую

значимость. В настоящее время наблюдается экспоненциальный рост как количества, так и сложности киберугроз, что ставит под вопрос эффективность существующих автоматизированных систем защиты. Несмотря на широкое распространение автоматизированных средств, их ограниченная адаптивность и недостаточная гибкость в ситуациях, требующих контекстного анализа и принятия нетривиальных решений, создают серьезные вызовы для специалистов по информационной безопасности. В этой связи, особое внимание заслуживают системы поддержки принятия решений (СППР), которые предоставляют возможность комбинировать аналитические возможности компьютерных систем с экспертным знанием и интуицией человека. СППР, ориентированные на сферу информационной безопасности, способны оперативно обрабатывать большой объем разнородных данных, выявлять сложные взаимосвязи и предоставлять варианты действий для эффективного реагирования на возникающие угрозы, минимизируя риски и предотвращая потенциальный ущерб. Таким образом, изучение и разработка СППР для подразделений информационной безопасности (ИБ) в российских предприятиях и организациях является актуальной и перспективной задачей, обусловленной необходимостью повышения устойчивости к современным киберугрозам [4].

Классификация СППР, ориентированных на информационную безопасность:

1. СППР для мониторинга и обнаружения угроз:

Функция: Обнаружение аномалий в сетевом трафике, подозрительной активности на хостах, вторжений и других угроз.

Примеры: Системы на основе машинного обучения для анализа лог-файлов и сетевых пакетов, системы обнаружения вторжений (СОВ) [5].

2. СППР для анализа рисков и уязвимостей:

Функция: Оценка вероятности реализации угроз, анализ уязвимостей программного обеспечения и инфраструктуры, выбор мер защиты.

Примеры: Системы, использующие методы формальной верификации, моделирование сценариев атак, базы данных уязвимостей [6].

3. СППР для реагирования на инциденты:

Функция: Автоматизация процессов реагирования на инциденты, предоставление вариантов действий для устранения последствий, организация совместной работы специалистов.

Примеры: Системы оркестрации и автоматизации безопасности (SOAR), платформы управления инцидентами.

Перспективы развития СППР для подразделений ИБ в Российской Федерации:

1. Интеграция передовых технологий ИИ и машинного обучения:

Описание: Дальнейшее развитие СППР будет тесно связано с применением передовых методов искусственного интеллекта (ИИ) и машинного обучения (МО). Эти технологии позволят автоматизировать многие процессы, включая анализ данных, обнаружение аномалий, прогнозирование угроз и реагирование на инциденты.

Содержание:

Углубленное обучение (Deep Learning): Использование нейронных сетей для анализа сложных паттернов и выявления угроз, которые могут быть незаметны для традиционных методов. Это включает в себя работу с большими данными (Big Data) для обнаружения сложных кибератак.

Обучение с подкреплением (Reinforcement Learning): Разработка систем, которые могут самостоятельно учиться принимать оптимальные решения в динамической среде, адаптируясь к изменяющимся условиям киберугроз.

Автоматизация анализа угроз: Использование МО для автоматической классификации, выбора и анализа угроз, что сократит время реагирования и повысит эффективность работы специалистов ИБ.

Прогнозирование кибератак: Применение методов машинного обучения для прогнозирования потенциальных атак на основе анализа исторических данных и текущих тенденций.

Примеры: Системы поведенческого анализа, способные обнаруживать аномальную активность пользователей, и интеллектуальные системы анализа лог-файлов.

Перспектива: Повышение эффективности и скорости работы СППР, а также уменьшение зависимости от человеческого фактора в рутинных операциях.

2. Развитие адаптивных и контекстно-ориентированных СППР:

Описание: Будущие СППР будут более адаптивными, способными учитывать специфические особенности каждой организации и текущую ситуацию в киберпространстве. Это потребует разработки контекстно-ориентированных систем, которые могут динамически адаптироваться к изменяющимся условиям.

Содержание:

Учет отраслевой специфики: Разработка СППР, учитывающих особенности и требования различных отраслей (финансы, здравоохранение, энергетика и т.д.).

Адаптация к инфраструктуре: Способность СППР интегрироваться с существующей инфраструктурой организации, включая различные операционные системы, сетевое оборудование и облачные сервисы.

Учет текущей ситуации: Возможность динамически адаптировать стратегии защиты на основе анализа текущих киберугроз и выявленных уязвимостей.

Персонализация: Разработка систем, способных предоставлять индивидуализированные рекомендации для конкретных пользователей и ролей.

Перспектива: Повышение эффективности СППР за счет более точного соответствия их функционала специфическим требованиям организации.

3. Интеграция СППР с другими системами и инструментами:

Описание: Будущие СППР будут не изолированными решениями, а частью интегрированной экосистемы безопасности. Это подразумевает их взаимодействие с другими инструментами, такими как SIEM, SOAR, Threat Intelligence и т.д.

Содержание:

Обмен данными: Создание платформ для обмена данными и информацией об угрозах между различными системами.

Автоматизация рабочих процессов: Интеграция СППР с системами автоматизации для ускорения реагирования на инциденты.

Централизованное управление: Разработка платформ для централизованного управления всеми компонентами системы безопасности.

Перспектива: Создание комплексной и интегрированной системы безопасности, обеспечивающей более эффективное управление и защиту информационных активов.

4. Улучшение пользовательского опыта (UX) и доступности:

Описание: Будущие СППР будут более удобными и интуитивно понятными для пользователей, независимо от их уровня технических знаний. Это потребует разработки интерфейсов, ориентированных на пользователя, и упрощения процессов использования системы.

Содержание:

Визуализация данных: Использование интерактивных дашбордов и визуальных инструментов для представления информации о состоянии безопасности.

Интуитивные интерфейсы: Разработка пользовательских интерфейсов, понятных и простых в использовании, что снизит порог входа для новых пользователей.

Мобильный доступ: Предоставление мобильного доступа к СППР, что позволит специалистам ИБ оперативно реагировать на инциденты из любого места.

Перспектива: Повышение эффективности работы специалистов ИБ за счет удобства использования систем и более быстрого доступа к необходимой информации [8].

5. Развитие отечественных решений и импортозамещение:

Описание: В условиях геополитической нестабильности и усиления киберугроз, важным направлением является развитие отечественных решений в области СППР, что обеспечит технологическую независимость и безопасность.

Содержание:

Поддержка отечественных разработчиков: Стимулирование создания отечественных технологий и решений в области ИБ.

Импортозамещение: Снижение зависимости от зарубежных технологий и продуктов за счет развития отечественных аналогов.

Создание стандартов: Разработка стандартов и методик для оценки и сертификации отечественных решений.

Перспектива: Обеспечение технологической независимости и безопасности, а также развитие отечественной IT-индустрии.

Вывод

1.Анализ существующих и перспективных направлений развития СППР для подразделений информационной безопасности в Российской Федерации указывает на отсутствие универсального «лучшего» решения. Оптимальный выбор зависит от конкретных потребностей организации и имеющихся ресурсов. Тем не менее, системы, интегрирующие возможности машинного обучения для анализа больших данных и автоматизации реагирования на инциденты (SOAR-платформы), представляются наиболее эффективными в настоящий момент. Эти системы позволяют своевременно обнаруживать аномалии, анализировать риски и автоматизировать рутинные задачи, высвобождая время специалистов для решения более сложных проблем.

2.Наиболее перспективным направлением для развития СППР в РФ видится создание комплексных, адаптивных и контекстно-ориентированных систем, основанных на передовых методах искусственного интеллекта (ИИ) и машинного обучения (МО). Такие системы должны обладать способностью:

- **Самообучаться и адаптироваться** к новым видам угроз и изменяющимся условиям информационной среды.
- **Интегрироваться с различными источниками данных** и инструментами обеспечения безопасности (SIEM, SOAR, Threat Intelligence).
- **Обеспечивать прозрачность принятия решений**, позволяя специалистам ИБ контролировать процесс и интерпретировать результаты анализа.
- **Учитывать специфику отрасли и нормативные требования Российской Федерации.**
- **Быть разработаны с использованием преимущественно отечественных технологий**, способствуя импортозамещению и обеспечению технологического суверенитета.

Развитие в этом направлении потребует совместных усилий со стороны научных организаций, разработчиков ПО и самих подразделений ИБ, а также государственной поддержки, направленной на стимулирование инноваций и внедрение передовых технологий. Только комплексный подход позволит создать надежные и эффективные СППР, способные противостоять современным и будущим киберугрозам в России.”

Список литературы:

1. Сизоненко А.Б., Алиманов П.Е. Модель организационно-штатного обеспечения подразделений защиты информации / Вестник Воронежского института МВД России 2020 г.
2. Стародубцев А.А. Система поддержки принятия решений / Актуальные проблемы авиации и космонавтики 2016 г.
3. Доктрина информационной безопасности, утвержденная Указом Президента РФ от 5 декабря 2016 года №646.
4. Карташов Г. П. Классификация систем поддержки принятия решений для использования в системе управления событиями и информацией о безопасности / Г. П. Карташов, Е. К. Корбин. – Текст: непосредственный // Молодой ученый. – 2023. – № 37 (484). – С. 9-11. –
5. Татарникова Т.М., Богданов П.Ю. Обнаружение атак в сетях интернета вещей методами машинного обучения / Информационно-управляющие системы 2021 г.
6. Федоренко С.Н. Технологии упрвления данными при проектировании сиситемы педдержки приятия решений / Вестник Сыктывкарского университета. Серия 1. Математика. Механика. Информатика 2020 г.
7. Васильченко А.Д. Система поддержки принятия решений для обеспечения информационной безопасности в облачной среде / Шаг в науку 2020 г.
8. Аннаева А.Р., Бабылова Б.Ч., Батыров Ы.Б., Довлетгелдиев С.Д. Применение принципов адаптивного веб-дизайна для улучшения пользовательского опыта / Символ науки 2023 г.