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

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

Уколов Евгений Сергеевич
Слушатель, военнослужащий, Монино

Вакуленко Ирина Влдасовна, Преподавтель,
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

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

АНАЛИЗ ПРОБЛЕМ ПРИМЕНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯДЛЯ СОЗДАНИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДОЛЖНОСТНЫХ ЛИЦ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В статье анализируются основные проблемы, препятствующие эффективному применению программного обеспечения для создания систем поддержки принятия решений (СППР) в подразделениях информационной безопасности. Выявлены ключевые недостатки, и предложены направления для улучшения существующих решений, что может способствовать повышению эффективности управления информационной безопасностью.

Ключевые слова: программное обеспечение, система поддержки принятия решений, должностные лица, информационная безопасность.

Термины и определения:

1. **Программное обеспечение –** совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ [1].
2. **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].
3. **Подразделение информационной безопасности –** это структурное подразделение которое определяет уязвимость информационных систем и программного обеспечения, предотвращает утечку информации, выявляет киберугрозы и поддерживает деятельность компании в случае кибератак [3].

Введение. В современной динамичной среде киберугроз, где атаки становятся все более сложными и изощренными, принятие быстрых и обоснованных решений является критически важным для подразделений информационной безопасности (ИБ). Должностные лица, отвечающие за защиту информационных активов, сталкиваются с непрерывным потоком данных и требуют эффективных инструментов для анализа и прогнозирования рисков. Системы поддержки принятия решений (СППР) призваны удовлетворить эту потребность, однако, их разработка и внедрение сопряжены с рядом проблем. В данной статье мы проведем анализ этих проблем, исследуя технические, организационные и человеческие факторы, влияющие на эффективность СППР в сфере ИБ.

Проблемы применения программного обеспечения для создания СППР должностных лиц подразделений информационной безопасности.

1. Технические проблемы:

1.1. Сложность интеграции:

– **Описание:** Несоответствие форматов данных, протоколов и интерфейсов между СППР и существующими информационными системами (SIEM, IDS, IPS, сканеры уязвимостей, и т. д.).

– Подтверждение из источников:

• Согласно результат опроса [4], сложность интеграции в существующую ИТ-инфраструктуру является основным препятствием для 21% опрошенных при внедрении информационной безопасности (ИБ)

• В статье [5] отмечается, что отсутствие стандартизированных API для обмена данными между СППР и другими системами является одной из основных причин проблем интеграции.

– **Последствия:** Дублирование данных, неполная картина ситуации, замедление процессов анализа и принятия решений.

1.2. Недостаточная функциональность:

– **Описание:** Ограниченный набор функций СППР, не позволяющий обрабатывать весь спектр угроз и решать широкий круг задач, стоящих перед специалистами по ИБ.

– Подтверждение из источников:

• Исследование [6] показывает, что большинство современных СППР не поддерживают анализ сложных взаимосвязей между событиями безопасности, что снижает их прогностическую способность.

– **Последствия:** Игнорирование важных событий, замедление реагирования на инциденты, неэффективное использование ресурсов.

1.3. Проблемы масштабируемости:

– **Описание:** Неспособность СППР обрабатывать большие объемы данных, особенно в крупных организациях, с разветвленной инфраструктурой и большим количеством пользователей.

– Подтверждение из источников:

• Результаты исследования [7] показывают, что при увеличении объема данных производительность многих СППР снижается экспоненциально, делая их непригодными для использования.

– **Последствия:** Невозможность обрабатывать все поступающие данные, задержки в принятии решений, пропуск потенциальных угроз.

1.4. Низкая производительность:

– **Описание:** Медленная работа СППР, особенно при обработке больших объемов данных или выполнении сложных аналитических запросов.

– Подтверждение из источников:

• В статье [8] указывается на недостаток оптимизации алгоритмов обработки данных в современных СППР, что приводит к задержкам и низкой эффективности.

– **Последствия:** Замедление процессов принятия решений, неэффективное использование ресурсов, снижение доверия пользователей.

2. Организационные и кадровые проблемы:

2.1. Недостаток квалифицированного персонала:

– **Описание:** Нехватка специалистов, обладающих знаниями и навыками, необходимыми для настройки, внедрения и использования СППР.

– **Последствия:** Неправильная настройка СППР, неэффективное использование, отказ от использования системы.

2.2. Недостаточное понимание процессов принятия решений:

– **Описание:** Разработчики СППР часто не учитывают особенности процессов принятия решений в области ИБ, что приводит к созданию систем, не отвечающих потребностям пользователей.

– **Последствия:** Неудобство использования СППР, низкая мотивация пользователей, неполное использование возможностей системы.

2.3. Проблемы с адаптацией к специфическим потребностям:

– **Описание:** Недостаточная гибкость СППР, невозможность адаптировать их к специфическим требованиям различных организаций и отраслей.

– **Последствия:** Неполное использование возможностей системы, необходимость доработки и модификации, неэффективное использование ресурсов.

2.4. Высокая стоимость внедрения и поддержки:

– **Описание:** Высокие затраты на покупку, внедрение, настройку и сопровождение СППР, особенно для малых и средних предприятий.

– **Последствия:** Невозможность внедрения СППР для многих организаций, неэффективное распределение ресурсов, отказ от использования системы.

Вывод

Проведенный анализ проблем применения программного обеспечения для создания систем поддержки принятия решений (СППР) должностных лиц подразделений информационной безопасности (ИБ) выявил ряд серьезных препятствий, снижающих эффективность этих систем. Среди них наиболее мешающими являются сложность интеграции с существующими системами, недостаточная функциональность, нехватка квалифицированного персонала и отсутствие гибкости в настройке. Эти проблемы в совокупности приводят к неполному использованию потенциала СППР, задержкам в принятии решений и, как следствие, к ослаблению защиты информационных активов. Для преодоления этих вызовов необходимы комплексные решения, направленные на стандартизацию интеграционных процессов, расширение функциональных возможностей, развитие кадрового потенциала и создание гибких, настраиваемых СППР, отвечающих специфическим потребностям организаций.

Список литературы:

1. ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения» утверждён постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 года №2467.

2. Беленков Д.А. Система поддержки принятия решений для органов государственного управления // Форум молодых ученых 2019 г. № 11.

3. Постановление правительства Российской Федерации от 15.07.2022 № 1272

4. Как грамотно интегрировать кибербезопасность в производственный процесс [Электронный ресурс]. – Режим доступа https:// malware.ru.

5. Взаимодействие в распределенных системах [Электронный ресурс]. – Режим доступа https:// geeksforgeeks.org

6. 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. – URL: https://moluch.ru/archive/484/105947/ (дата обращения: 20.01.2025).

7. Производительность систем Хранилищ данных (часть 1) [Электронный ресурс]. – Режим доступа https:// iso.ru.

8. Акимкина, Э.Э Оптимизация обработки данных в системах поддержки принятия решений с элементами обслуживания / Вестник ВГУ, серия: системный анализ и информационные технологии, 2017, № 2.