**Охотин Данил Александрович,** 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

**Уколов Евгений Сергеевич,**
Военнослужащий, Монино

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

**Чапаев Илья Сергеевич,** студент,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко», г. Краснодар

# ОЦЕНКА ЭФФЕКТИВНОСТИ СУЩЕСТВУЮЩИХ ПРОГРАММНЫХ РЕШЕНИЙ ПО ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ВОЗНИКНОВЕНИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Аннотация:** В статье проводится оценка эффективности существующих программных решений, предназначенных для поддержки принятия решений в условиях возникновения угроз информационной безопасности. Рассматриваются различные типы программного обеспечения, анализируются их возможности, преимущества и недостатки. Результаты исследования позволяют определить наиболее эффективные инструменты и выявить области для их дальнейшего совершенствования.

**Ключевые слова:** оценка эффективности, угроза информационной безопасности, информационная безопасность.

**Термины и определения:**

1. **Информационная безопасность –** состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз [1].

2. **Эффективность –** основополагающий показатель предприятия, который связан с характеристикой результативности деятельности предприятия, его производственно-хозяйственной, коммерческой, инвестиционной, и иных видов деятельности, имеющих отношение к производству, как в текущем периоде, так и в перспективе [2].

**Введение.** Системы поддержки принятия решений (СППР) играют важную роль в обеспечении информационной безопасности (ИБ). В данной статье проводится оценка эффективности существующих программных решений для СППР, применяемых при возникновении угроз ИБ. Цель исследования – выявить наиболее эффективные инструменты и определить направления для их дальнейшего совершенствования.

**1. Системы управления информацией и событиями безопасности (SIEM):**

**Описание:** SIEM-системы собирают, анализируют и агрегируют данные из различных источников (журналы событий, сетевой трафик, журналы безопасности и т.д.) для обнаружения аномалий и инцидентов безопасности. Они предоставляют интерфейс для анализа данных, оповещения о событиях и формирования отчетов.

**Основные функции:**

– Сбор и централизация данных из различных источников.
– Обнаружение аномальной активности и инцидентов безопасности.
– Корреляция событий для выявления сложных атак.
– Генерация отчетов и оповещений.
– Возможности визуализации данных [3].

**Примеры:** Splunk, IBM QRadar, Elastic Security, Microsoft Sentinel.

**2. Системы оркестрации, автоматизации и реагирования на инциденты безопасности (SOAR):**

**Описание:** SOAR-системы автоматизируют процессы реагирования на инциденты безопасности, позволяя ускорить и оптимизировать действия специалистов по ИБ. Они интегрируются с другими инструментами безопасности и предоставляют возможности для автоматического выполнения типовых задач.

**Основные функции:**

– Автоматизация процессов реагирования на инциденты.
– Оркестрация работы различных инструментов безопасности.
– Автоматическое расследование инцидентов.
– Визуализация и управление процессами реагирования.
– Анализ уязвимостей и управление исправлениями [4].

**Примеры:** Palo Alto Networks Cortex XSOAR, Splunk Phantom, IBM Resilient.

**3. Платформы управления угрозами (TIP):**

**Описание:** TIP-системы собирают, анализируют и предоставляют информацию об угрозах из различных источников (фиды угроз, разведывательные данные, отчёты об инцидентах). Они позволяют специалистам по ИБ лучше понимать текущие и будущие угрозы, а также принимать более обоснованные решения.

**Основные функции:**

– Сбор и анализ данных об угрозах из различных источников.
– Приоритизация угроз на основе их потенциального риска.
– Обмен информацией об угрозах с другими организациями.
– Визуализация и анализ данных об угрозах.
– Интеграция с другими системами безопасности [5].

**Примеры:** Recorded Future, ThreatQuotient, Anomali.

**4. Системы управления уязвимостями:**

**Описание:** Системы управления уязвимостями помогают выявлять и приоритизировать уязвимости в инфраструктуре организаций. Они выполняют сканирование на уязвимости, предоставляют отчёты и помогают в планировании работ по их устранению.

**Основные функции:**

– Автоматизированное сканирование на уязвимости.
– Приоритизация уязвимостей на основе их потенциального риска.
– Отчётность и аналитика по уязвимостям.
– Управление исправлениями и патчами [6].

**Примеры:** Qualys, Tenable, Rapid7.

**5. Системы визуализации данных и аналитические платформы:**

**Описание:** Эти системы предоставляют интерфейс для визуализации данных из различных источников и анализа информации о безопасности. Они позволяют специалистам по ИБ получать более наглядное представление о текущей ситуации и принимать более обоснованные решения [7].

**Основные функции:**

– Визуализация данных из различных источников.

– Интерактивный анализ данных.

– Создание настраиваемых панелей мониторинга.

– Возможности машинного обучения и искусственного интеллекта.

**Примеры:** Tableau, Power BI, Grafana.

**Оценка эффективности программных решений для поддержки принятия решений при угрозах ИБ**

**Критерии оценки:**

Для оценки эффективности программных решений мы будем использовать следующие критерии:

**1. Функциональность:**

– Набор предоставляемых функций, их полнота и соответствие задачам ИБ.

– Возможность обнаружения и анализа различных типов угроз.

– Поддержка интеграции с другими инструментами и системами.

– Гибкость настройки и адаптации к специфическим потребностям.

**2. Производительность:**

– Скорость обработки данных и выполнения аналитических запросов.

– Способность обрабатывать большие объемы данных в режиме реального времени.

– Масштабируемость и способность работать в крупных и распределенных инфраструктурах.

– Надежность и отказоустойчивость.

**3. Удобство использования:**

– Интуитивность и понятность интерфейса.

– Простота настройки и управления.

– Наличие удобных инструментов для визуализации и анализа данных.

– Качество документации и поддержки.

**4. Соответствие требованиям:**

– Соответствие потребностям и ожиданиям специалистов по ИБ.

– Способность решать конкретные задачи и обеспечивать желаемый уровень защиты.

– Возможность интеграции в существующие бизнес-процессы.

– Соответствие законодательным и регуляторным требованиям.

**5. Общая эффективность:**

– Реальная эффективность в обнаружении и предотвращении угроз.

– Влияние на скорость реагирования и устранения инцидентов.

– Влияние на общую стоимость владения и использования системы.

– Соотношение между ценой и качеством.

**1. Системы управления информацией и событиями безопасности (SIEM):**

– **Функциональность:** Высокая (широкий спектр функций для сбора, анализа и корреляции событий).

– **Производительность:** Средняя (зависит от масштаба системы и используемого оборудования, может быть ресурсоемким при больших объемах данных).

– **Удобство использования:** Среднее (требует обучения и настройки, интерфейс может быть сложным для начинающих пользователей).

– **Соответствие требованиям:** Высокое (соответствует основным потребностям ИБ, но требует настройки под специфику организации).

– **Общая эффективность:** Высокая (позволяет обнаруживать и анализировать широкий спектр угроз, но требует квалифицированного персонала для эффективной работы).

**2. Системы оркестрации, автоматизации и реагирования на инциденты безопасности (SOAR):**

– **Функциональность:** Высокая (автоматизация процессов реагирования, интеграция с другими инструментами).

– **Производительность:** Высокая (автоматизация и оркестрация позволяют значительно ускорить процессы).

– **Удобство использования:** Среднее (требует понимания процессов реагирования на инциденты и настройки автоматизаций).

– **Соответствие требованиям:** Высокое (обеспечивает быстрое и эффективное реагирование на инциденты, но может потребовать интеграции с другими системами).

– **Общая эффективность:** Высокая (снижает нагрузку на персонал и сокращает время реагирования на инциденты, но требует точной настройки и интеграции).

**3. Платформы управления угрозами (TIP):**

– **Функциональность:** Высокая (сбор и анализ данных об угрозах, приоритизация угроз).

– **Производительность:** Средняя (зависит от источников данных и объема обрабатываемой информации).

– **Удобство использования:** Среднее (может требовать обучения для анализа и интерпретации данных об угрозах).

– **Соответствие требованиям:** Высокое (позволяет специалистам ИБ быть в курсе последних угроз и атак, но эффективность зависит от качества источников данных).

– **Общая эффективность:** Средняя (помогает в приоритизации угроз, но требует интеграции с другими системами для эффективного реагирования).

**4. Системы управления уязвимостями:**

– **Функциональность:** Высокая (автоматическое сканирование и приоритизация уязвимостей).

– **Производительность:** Высокая (сканирование и анализ уязвимостей происходит достаточно быстро).

– **Удобство использования:** Среднее (требует настройки и интерпретации результатов сканирования).

– **Соответствие требованиям:** Высокое (помогает в выявлении слабых мест, но требует планомерной работы по устранению уязвимостей).

– **Общая эффективность:** Средняя (снижает риск эксплуатации уязвимостей, но требует интеграции с другими системами для эффективного реагирования).

**5. Системы визуализации данных и аналитические платформы:**

– **Функциональность:** Средняя (визуализация и анализ данных).

– **Производительность:** Высокая (быстрое построение графиков и дашбордов).

– **Удобство использования:** Высокое (простой и интуитивно понятный интерфейс, гибкие возможности настройки).

– **Соответствие требованиям:** Среднее (может помочь в анализе данных, но не является самостоятельным решением для обеспечения ИБ).

– **Общая эффективность:** Средняя (помогает визуализировать данные и принимать более обоснованные решения, но не заменяет другие специализированные системы).

**Вывод**

Проведенный в статье анализ программных решений для поддержки принятия решений при возникновении угроз информационной безопасности (ИБ) показал, что каждый из рассмотренных типов систем обладает своими преимуществами и недостатками. **Наиболее**

**эффективными решениями на сегодняшний день являются Системы управления информацией и событиями безопасности (SIEM) и Системы оркестрации, автоматизации и реагирования на инциденты безопасности (SOAR)**, которые обеспечивают комплексный подход к обнаружению, анализу и реагированию на угрозы. Однако, их эффективность во многом зависит от квалификации персонала и качества интеграции с другими системами.

**Наиболее перспективными решениями для дальнейшего развития являются Платформы управления угрозами (TIP) и Системы визуализации данных и аналитические платформы**, так как они способны значительно улучшить качество аналитики и прогнозирования угроз, а также предоставляют более наглядные и удобные инструменты для работы со сложными данными. При этом, необходимо отметить, что **интеграция всех этих типов систем в единую экосистему является ключевым фактором для достижения максимальной эффективности в обеспечении информационной безопасности.** Для достижения этого требуется дальнейшее развитие стандартов обмена данными и улучшение интеграционных возможностей различных программных решений.

*Список литературы:*

1. Указ Президента РФ от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

2. Афанасьева, А. Б. Оценка эффективности деятельности предприятия / А. Б. Афанасьева. – Текст: непосредственный // Молодой ученый. – 2022. – № 37 (432). – С. 27-29. – URL: https://moluch.ru/archive/432/94964/ (дата обращения: 20.01.2025).3. Постановление правительства Российской Федерации от 15.07.2022 № 1272

3. Кирсанов Д. Г., Айдинян А. Р. Эффективное обеспечение безопасности с помощью SIEM // Молодой исследователь дона. 2024. Т. 9. № 3 (48)

4. SOAR-системы [Электронный ресурс]. – Режим доступа https:// www.securityvision.ru

5. Петросян, А. А. Инструменты анализа инцидентов информационной безопасности / А. А. Петросян. – Текст: непосредственный // Молодой ученый. – 2024. – № 4 (503). – С. 30-31. – URL: https://moluch.ru/archive/503/110776/ (дата обращения: 20.01.2025).

6. SOAR-системы [Электронный ресурс]. – Режим доступа https:// www.securityvision.ru

7. Толкачева Е.В. Роль аналитических платформ для обработки и анализа больших данных организаций в условиях цифровизации экономик [Электронный ресурс]. – Режим доступа https:// rep.polessu.by