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

Челышев Александр Павлович, студент,
ФГБОУ ВО «Краснодарское высшее военное училище имени генерала армии С. М. Штеменко», г. Краснодар

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

Головинский Анатолий 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

СУЩЕСТВУЮЩИЕ ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ДОЛЖНОСТНЫМИ ЛИЦАМИ ПОДРАЗДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЫЯВЛЕНИИ УГРОЗ

Аннотация: В данной статье представлен обзор существующих программных решений, которые помогают специалистам по ИБ выявлять, анализировать и исключать угрозы, а также принимать стратегические решения в области информационной безопасности.

Цель исследования – представить систематизированный обзор существующих угроз и предложить практические рекомендации по обеспечению безопасности информации в условиях потенциального воздействия технических каналов утечки.

Ключевые слова: Техническая защита информации, система поддержки принятия решений, оценка эффективности программного обеспечения.

Термины и определения:

Информация – любые сведения (сообщения, данные) не зависимо от формы их представления [2].

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

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 [5].

Техническая защита информации – Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [1].

Введение. В современном цифровом мире информационная безопасность (ИБ) является ключевым аспектом функционирования любой организации. Подразделения ИБ сталкиваются с постоянным потоком угроз, требующих оперативного и грамотного реагирования. Для эффективного управления инцидентами и принятия обоснованных

решений должностные лица подразделений ИБ нуждаются в современных программных средствах, обеспечивающих поддержку принятия управленческих решений (СПУР).

Роль СПУР в деятельности подразделений ИБ:

СПУР – это информационные системы, которые предоставляют должностным лицам подразделений ИБ инструменты для анализа данных, оценки рисков, моделирования ситуаций, выбора оптимальных стратегий и контроля их реализации. Основные задачи СПУР:

- **Сбор и объединение данных:** сбор информации из различных источников, таких как системы обнаружения вторжений (СОВ), системы управления событиями безопасности (SIEM), журналы аудита, сканеры уязвимостей и др.
- **Анализ данных:** обработка и анализ собранной информации для выявления закономерностей, аномалий и потенциальных угроз.
- **Визуализация данных:** представление результатов анализа в наглядной и понятной форме, например, в виде графиков, диаграмм и карт.
- **Оценка рисков:** определение вероятности возникновения угроз и их потенциального воздействия на бизнес.
- **Моделирование ситуаций:** разработка сценариев развития угроз и оценка эффективности различных вариантов реагирования.
- **Формирование рекомендаций:** Предоставление обоснованных рекомендаций по принятию управленческих решений.
- **Контроль исполнения решений:** Отслеживание результатов реализации принятых решений.
- **Отчетность:** формирование отчетов о состоянии информационной безопасности, выявленных угрозах и принятых мерах.

Существующие виды программного обеспечения для поддержки принятия управленческих решений в ИБ:

1. Системы управления событиями и инцидентами безопасности (SIEM):

- Основные инструменты для мониторинга и анализа событий безопасности.
- Собирают логи из различных источников, сопоставляют их и выявляют аномалии и подозрительную активность.
- Позволяют в реальном времени отслеживать инциденты и реагировать на них.
- **Примеры:** Splunk Enterprise Security, IBM QRadar, LogRhythm, Micro Focus ArcSight.

2. Системы обнаружения и предотвращения вторжений (IDS/IPS):

- Выявляют сетевые атаки и другие виды угроз на основе сигнатур и правил.
- IPS могут автоматически блокировать атаки, в то время как IDS просто оповещает о них.
- Помогают оперативно реагировать на угрозы и предотвращать их распространение.
- **Примеры:** Snort, Suricata, Check Point IPS, Cisco Firepower.

3. Системы управления уязвимостями (Vulnerability Management):

- Сканируют сети и системы на наличие уязвимостей.
- Предоставляют отчеты об обнаруженных уязвимостях и рекомендации по их устранению.
- Позволяют приоритизировать уязвимости по уровню риска.
- **Примеры:** Nessus, Qualys Vulnerability Management, Rapid7 InsightVM, Tenable.io.

4. Системы управления рисками информационной безопасности (GRC – управление, риски и соответствие требованиям):

- Помогают организациям управлять рисками, соблюдать нормативные требования и обеспечивать соответствие стандартам безопасности.
- Автоматизируют процессы управления рисками, аудита и контроля соответствия.
- **Примеры:** RSA Archer, ServiceNow GRC, MetricStream, LogicManager.

5. Системы анализа угроз (Threat Intelligence):

- Собирают информацию о текущих угрозах из различных источников, таких как разведка с открытым исходным кодом (OSINT), Даркнет и коммерческие базы данных.
- Позволяют получить представление о тактиках, методах и процедурах (TTP) злоумышленников.
- Помогают проактивно защищаться от угроз и адаптировать меры безопасности.
- **Примеры:** Recorded Future, ThreatConnect, CrowdStrike Falcon Intelligence, Anomali.

6. Системы моделирования инцидентов (Incident Response Platforms):

- Предоставляют платформы для планирования, координации и анализа действий при реагировании на инциденты, связанные с безопасностью.
- Автоматизируют повторяющиеся задачи, связанные с реагированием на инциденты.
- Помогают сократить время реагирования и минимизировать ущерб от инцидентов.
- **Примеры:** Demisto (Palo Alto Networks), ServiceNow Security Incident Response, TheHive, Swimlane.

7. Информационные панели и средства визуализации (Dashboards and Visualization Tools):

- Предоставляют наглядные представления ключевых показателей безопасности.
- Помогают быстро отслеживать состояние безопасности и выявлять аномалии.
- Могут быть адаптированы под конкретные потребности организации.
- **Примеры:** Grafana, Kibana, Power BI, Tableau.

Критерии выбора СПУР:

При выборе программного обеспечения для поддержки принятия управленческих решений в сфере информационной безопасности необходимо учитывать следующие факторы:

- **Функциональность:** Набор необходимых функций и возможностей для решения конкретных задач.
- **Масштабируемость:** способность системы обрабатывать растущие объемы данных и количество пользователей.
- **Интеграция:** Возможность интеграции с другими системами и средствами безопасности.
- **Производительность:** Скорость и надежность работы системы.
- **Удобство использования:** Интуитивно понятный интерфейс и простота работы.
- **Стоимость:** Соотношение цены и качества.
- **Поддержка:** Наличие качественной технической поддержки от поставщика.
- **Соответствие нормативным требованиям:** соответствие стандартам и требованиям законодательства в области информационной безопасности.

Тенденции развития СПУР:

- **Использование искусственного интеллекта и машинного обучения:** для автоматизации анализа данных, выявления аномалий и прогнозирования угроз.
- **Облачные решения:** переход к облачным сервисам для обеспечения большей гибкости, масштабируемости и доступности.
- **Интеграция и автоматизация:** создание единых платформ, объединяющих различные инструменты и процессы информационной безопасности.
- **Расширенная аналитика:** более глубокий анализ данных для выявления более сложных угроз.
- **Проактивная защита:** переход от реактивного к проактивному подходу к обеспечению безопасности.

Заключение:

Программные решения для поддержки принятия управленческих решений в сфере информационной безопасности играют ключевую роль в обеспечении защиты организаций от современных угроз. Выбор конкретных инструментов зависит от потребностей и ресурсов организации. Однако внедрение современных СПУР является необходимым условием для эффективного управления информационной безопасностью и минимизации рисков. Постоянное развитие технологий и угроз требует от специалистов по ИБ непрерывного обучения и адаптации к новым решениям и методам защиты.

Список литературы:

1. Рекомендации по стандартизации Р 50.1.056 – 2005 «Техническая защита информации. Основные термины и определения», утверждены Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479.
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Доктрина информационной безопасности, утвержденная Указом Президента РФ от 5 декабря 2016 года №646.
4. Стародубцев А.А. Система поддержки принятия решений / Актуальные проблемы авиации и космонавтики 2016 г.
5. 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. –
6. Петриченко Г.С., Григорян Н.К., Медовщиков М.И. 2012. Методика разработки экспертной системы руководителя для принятия управленческих решений. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации, Управление. Т.1 (140): 60-66.
7. Петриченко Г.С., Нарыжная Н.Ю., Гоголев В.Н. 2008. Моделирование управленческих ситуаций по защите информации с применением иерархической системы неисправностей. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации, Управление. 2008. Т.2 (55): 103-107.