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

Максаков Андрей Александрович, 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

Дудатьев Иван 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 МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДОЛЖНОСТНЫМИ ЛИЦАМИ ПОДРАЗДЕЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПРИ ВЫЯВЛЕНИИ ИНФОРМАЦИОННЫХ УГРОЗ

Аннотация: Данная статья посвящена обзору существующих методов оценки эффективности разработки программного обеспечения, предназначенного для поддержки принятия решений в области технической защиты.

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].

Оценка эффективности программного обеспечения (ПО) – это отношение уровня услуг, предоставляемых программным продуктом пользователю при заданных условиях, к объёму используемых ресурсов.

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 мире, где информационная безопасность играет критически важную роль, разработка эффективных программных средств для поддержки принятия решений (СППР) должностными лицами подразделений технической защиты (ПТЗ) при

выявлении информационных угроз является первостепенной задачей. Однако для обеспечения качества и пригодности разработанного ПО необходимо применять соответствующие методы оценки его эффективности.

Цели оценки эффективности ПО для ПТЗ:

Целью оценки эффективности СППР для ПТЗ является определение степени, в которой разработанное программное обеспечение:

- **Повышает эффективность работы ПТЗ**: позволяет быстрее и точнее выявлять, анализировать и нейтрализовывать информационные угрозы.
- **Соответствует требованиям безопасности**: обеспечивает надежную защиту от несанкционированного доступа, изменения или уничтожения информации.
- **Удобно в использовании**: имеет интуитивно понятный интерфейс и не требует специальной подготовки для работы.
- **Соответствует потребностям ПТЗ**: адекватно решает задачи, стоящие перед подразделением, и предоставляет необходимую функциональность.
- **Экономически эффективно**: оправдывает затраты на разработку, внедрение и сопровождение.

Методы оценки эффективности:

Существующие методы оценки эффективности разработки ПО для СППР можно разделить на несколько категорий:

1. Оценка функциональности:

- Тестирование функциональности: проверка соответствия реализованных функций требованиям технического задания, выявление ошибок и недочетов в работе ПО.
- Анализ полноты функционала: оценка набора функций, предоставляемых системой поддержки принятия решений, с точки зрения их достаточности для решения задач ПТЗ.
- Оценка удобства использования: определение простоты и удобства работы с интерфейсом ПО, оценка интуитивности и эргономичности дизайна.
- Приемочные испытания: проверка соответствия ПО требованиям заказчика на этапе завершения разработки.

2. Оценка производительности и надежности:

- Тестирование производительности: измерение времени выполнения операций, скорости обработки данных, нагрузки, которую способно выдержать ПО, и т. д.
- Тестирование надежности: проверка устойчивости ПО к сбоям, отказам и нестандартным ситуациям.
- Оценка масштабируемости: определение способности ПО справляться с растущими объемами данных и количеством пользователей.
- Стресс-тестирование: проверка работы ПО в условиях экстремальных нагрузок.

3. Оценка безопасности:

- Тестирование на проникновение: проверка уязвимостей ПО к внешним атакам и несанкционированному доступу.
- Анализ кода на наличие уязвимостей: проверка программного кода на наличие ошибок и недочетов, которые могут быть использованы злоумышленниками.
- Оценка соответствия требованиям безопасности: проверка соблюдения стандартов и нормативов в области информационной безопасности.

4. Оценка влияния на работу ПТЗ:

- Анализ показателей эффективности работы: измерение таких показателей, как время реагирования на инциденты, количество выявленных угроз, уровень защищенности ОИ и др.
- Опрос сотрудников ПТЗ: сбор отзывов и мнений о работе с ПО, оценка его влияния на их повседневную деятельность.

○ Анализ времени принятия решений: оценка того, как СППР влияет на скорость и точность принятия решений должностными лицами.

5. Экономическая оценка:

○ Оценка затрат на разработку и внедрение: определение общей стоимости разработки, внедрения и сопровождения ПО.

○ Оценка экономической эффективности: сопоставление затрат на ПО с экономическим эффектом от его использования (снижение рисков, предотвращение ущерба и т. д.).

Методы оценки, основанные на стандартах:

При оценке эффективности ПО для ПТЗ также используются стандарты, такие как:

- ISO/IEC 25000 (SQuaRE): серия стандартов, устанавливающих требования к качеству программного обеспечения, включая функциональность, надежность, удобство использования и т. д.
- ISO/IEC 27000: Серия стандартов, устанавливающих требования к системе менеджмента информационной безопасности, в том числе к оценке и управлению рисками.
- NIST Cybersecurity Framework: Рекомендации Национального института стандартов и технологий США по обеспечению кибербезопасности, включая методы оценки эффективности защитных мер.

Рекомендации по проведению оценки:

Для эффективной оценки ПО для СППР рекомендуется:

- Планируйте оценку заранее: определите цели и методы оценки на этапе планирования разработки.
- Использовать комплексный подход: применять различные методы оценки для получения всесторонней картины.
- Привлекать специалистов по информационной безопасности: обеспечить объективность и компетентность оценки.
- Проводить оценку на всех этапах разработки: выявлять и устранять недостатки на ранних стадиях.
- Использовать реальные данные: проводить тестирование и оценку с использованием данных, характерных для повседневной работы ПТЗ.
- Документировать результаты оценки: сохранять отчеты об оценке для дальнейшего анализа и улучшения.

Заключение:

Оценка эффективности программного обеспечения для поддержки принятия решений должностными лицами ПТЗ при выявлении информационных угроз является критически важным этапом разработки. Комплексный подход, включающий оценку функциональности, производительности, надёжности, безопасности, влияния на работу ПТЗ и защиту ОИ.

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. Федеральный закон от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне».

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.