КРИТЕРИИ ДЛЯ ВЫБОРА И РАЗРАБОТКИ СРЕДСТВ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ

П.А. Фильченков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Критериями для выбора и разработки средств аудита безопасности информационных систем (ИС) учреждений здравоохранения (УЗ) являются:

– требования к обеспечению информационной безопасности в УЗ, которые фигурируют в следующих локальных документах УЗ: политика информационной безопасности, регламенты, инструкции и приказы по вопросам обеспечения информационной безопасности ИС;

– состав аппаратного и программного обеспечения ИС УЗ;

– топология ИС.

С учетом перечисленных критериев работникам УЗ, отвечающим за информационную безопасность, необходимо проводить следующее.

1. Категорирование ИС, аппаратно-программного обеспечения ИС, а также средств защиты информации, используемых в ИС.

2. Определение потенциальных угроз и уязвимостей аппаратно-программного обеспечения ИС и средств защиты информации, используемых в ИС, с применением базы данных общеизвестных уязвимостей информационной безопасности CVE (от англ. Common Vulnerabilities and Exposures) [1] и банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России [2].

3. Поиск эксплойтов, которые целесообразно применять для проверки триггеров ИС и систем мониторинга, компилирование их в выполняемую программу (скрипт), для дальнейшей реализации [3].

4. Запуск скомпилированной программы и наблюдение за триггерами, которые должны среагировать на каждый эксплойт. Это действие должно реализовываться 4 способами:

1) за пределами контролируемой зоны УЗ от лица неавторизованного пользователя;

2) за пределами контролируемой зоны УЗ от лица авторизованного пользователя;

3) внутри локальной вычислительной сети УЗ от лица сотрудника учреждения с автоматизированного рабочего места;

4) внутри локальной вычислительной сети УЗ от лица неавторизованного пользователя при условии подмены IP и MAC адресов.

В большинстве случаев программное обеспечение для аудита информационной безопасности ИС разрабатывается под определенные задачи и на основании текущих угроз и уязвимостей.

Список литературы

1. CVE [Электронный ресурс]. – Режим доступа: https://www.cve.org/. – Дата доступа: 05.05.2024.

2. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat-section/. – Дата доступа: 05.05.2024.

3. Дербин, Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности: учебное пособие / Е. А. Дербин, А. В. Царегородцев. – Москва: ИНФРА-М. – 2024. – 267 с.