МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт цифровых технологий, электроники и физики

Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа № 4

Оценка сценариев реализации угроз и актуальности угроз. Модель угроз персональной ИС.

Выполнил студент 595 гр.

_____ А.В. Лаптев

Проверил:

_____ П.С. Ладыгин

Лабораторная работа защищена

«___» _____2023 г.

Оценка _____

Барнаул 2023

Цель работы: продолжить знакомство с документом «Методика оценки угроз безопасности информации», а также получить навыки по созданию модели нарушителя персональной информационной системы.

Задачи:

1. Дополнить перечень угроз.
    a. Используя банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), выбрать актуальные для своей информационной системы угрозы. Таких угроз должно быть выбрано не менее 5.
    b. Внести информацию об угрозах, полученную в Лабораторной работе №3 «Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности».

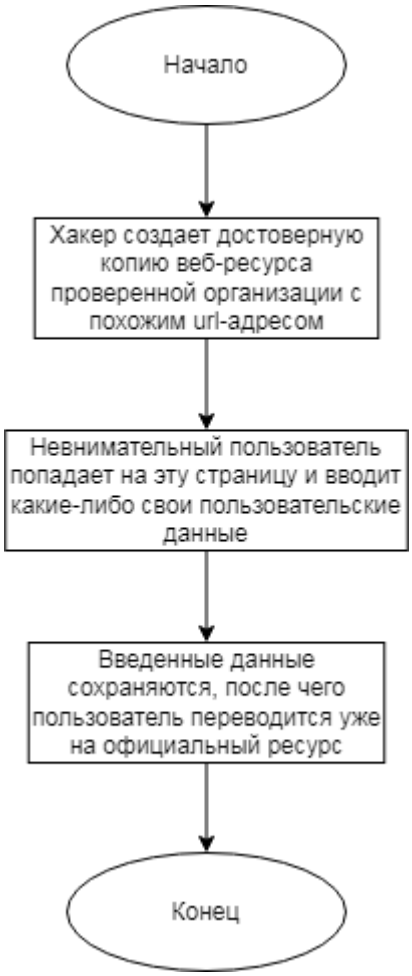
№	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры) (H2)	Внешний	Удаленное автоматизированное рабочее место (АРМ) пользователя: Несанкционированный доступ к операционной системе АРМ пользователя, нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Доступ через локальную и внешнюю вычислительные сети	Внедрение вредоносного ПО
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
				Сетевые интерфейсы коммутатора сети, где расположен веб-сервер	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
2	Авторизованные пользователи систем и сетей (H1)	Внутренний	АРМ пользователя	Доступ через локальную и внешнюю вычислительные сети	Ошибочные действия в ходе настройки АРМ пользователя
3	Разработчики программных, программно-аппаратных средств (H1)	Внутренний	АРМ пользователя	Пользовательский веб-интерфейс доступа к базе данных информационной системы	Возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации

					функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API).
4	Поставщики вычислительных услуг, услуг связи (H1)	Внутренний	Удаленное автоматизированное рабочее место (АРМ) пользователя: Несанкционированный доступ к операционной системе АРМ пользователя, нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Пользовательский веб-интерфейс доступа к базе данных информационной системы	Возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API).
5	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (H1)	Внутренний	АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
				Доступ через локальную и внешнюю вычислительные сети	Ошибочные действия в ходе настройки АРМ пользователя

2. Предложить возможные сценарии реализации угроз.
    a. Выбрать из Приложения 11 к Методике оценки угроз безопасности информации все актуальные тактики и основные техники реализации угроз (данные внести в таблицу с соответствующим названием).

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.
		Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
Т2	Получение первоначального доступа к компонентам систем и сетей Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий	Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное ПО или предназначенных для вредоносных функций
		Т2.9. Несанкционированное подключение внешних устройств
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы.
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах

b. Подробно описать один из возможных вариантов реализации угроз, для описания использовать простую блок-схему или язык uml.



3. Разработка модели угроз персональной ИС.
    a. Собрать в единый документ с названием «Модель угроз «Название вашей ИС»» все ранее полученные результаты (Лабораторных работ 1-4) по примеру, приведенному на страницах 39-41 Методики оценки угроз безопасности (см. Приложение).

Вывод: в ходе выполнения лабораторной работы было продолжено знакомство с документом «Методика оценки угроз безопасности информации», а также получены навыки по созданию модели нарушителя персональной информационной системы.

Ответы на контрольные вопросы:

1. Зачем необходимо создавать модель угроз в организации? Дать обоснованный ответ.

Ответ: Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

В систему защиты включаются только те средства, которые нейтрализуют актуальные угрозы.

2. Что такое политика информационной безопасности?

Ответ: Политика информационной безопасности – совокупность правил, процедур, практических методов, руководящих принципов в области ИБ, используемых организацией в своей деятельности.