Лабораторная работа №2
Описание информационной системы и определение источников угроз безопасности информации

В данной работе предполагается продолжение знакомства с документом «Методика оценки угроз безопасности информации», а также подготовка к созданию модели нарушителя персональной информационной системы.

Теоретические сведения

Прежде, чем приступать к определению источников угроз безопасности информации, необходимо описать информационную систему, в которой хранится и обрабатывается защищаемая информация. Такое описание становится вторым разделом разрабатываемой модели угроз «Описание систем и сетей и их характеристика как объектов защиты» и содержит:

- наименование систем и сетей, для которых разработана модель угроз безопасности информации;
- класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;
- нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;
- назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;
- состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;
- описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);
- описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;
- информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления.

После этого необходимо предположить список возможных нарушителей, который является третьим разделом «Источники угроз безопасности информации», разрабатываемой модели угроз и содержит:

- характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации;
- категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации;
- описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

Задания:

1. Собрать сведения об информационной системе.

Учитывая специфику проведения лабораторных занятий, мы продолжим разработку модели угроз, однако исключим из неё некоторые неактуальные пункты, представленные в Теоретических сведениях данного текстового документа.

1.1. Дайте наименование вашей персональной информационной системе.

Пример: ПК Фамилия И.О.

Требование к данному пункту: простое и адекватное название.

1.2. Опишите назначение, задачи (функции) систем и сетей, состав обрабатываемой информации.

Пример: ИС «Наименование» используется для создания и редактирования документов, создания мультимедийных файлов, выхода в Интернет и оплату покупок в онлайн-магазинах.

Требование к данному пункту: перечислить не менее 15 задач, для которых используется персональная ИС.

1.3. Опишите состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей.

Образец:

Конфигурация включает в себя следующие элементы:

Материнская плата:
Видеокарта:
Процессор:
ОЗУ:
Блок питания:
Жесткий диск:
Система охлаждения:
Операционная система:
Тип устройства:

1.4. Опишите группы внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации).

Пример: Данная ИС используется двумя пользователями с равными правами доступа (уровень доступа – администратор). Авторизация не требуется.

1.5. Опишите внешние интерфейсы и взаимодействие системы и сети с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет».

Требование к данному пункту: описать способы выхода в Интернет, возможность подключения внешних устройств (флешки, удалённый доступ и др.)

1.6. Приведите схематичное расположение элементов информационной системы внутри помещения.

Требование к данному пункту: отразить на схеме расположение дверей, окон, основных и крупных объектов помещения (шкафы, столы), расположение ПК, расположение точки доступа в Интернет, способ подключения.

2. Определить источники угроз безопасности информации.

2.1. Изучить с.20-25 Методики оценки угроз безопасности информации (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

2.2. Выделить актуальные для своей ИС виды нарушителей, подлежащих оценке (из перечня на странице 21).

2.3. На основании выбранных актуальных видов нарушителей составить таблицу «Возможные цели реализации угроз безопасности информации» (образец – с. 48).

Содержание отчёта:

1. Титульный лист.
2. Описание информационной системы.
3. Таблица «Возможные цели реализации угроз безопасности информации»

4. Вывод.
5. Ответ на контрольные вопросы:
   a. Какие уровни возможностей нарушителей вам известны?
   b. Что такое уязвимость информационной системы?
   c. Необходимо ли заниматься обеспечением информационной безопасности персональной информационной системы? Дайте обоснованный ответ (не менее 100 слов).