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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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.
   1. 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.

ПК Лаптев А.В.

* 1. Внести информацию об угрозах, полученную в Лабораторной работе №3 «Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности».

ИС ПК Лаптев А.В. используется для: написания программного кода; создания и редактирования текстовых, графических и мультимедийных файлов; серфинга в Интернете; разработки и трассировки печатных плат.

1. Предложить возможные сценарии реализации угроз.
   1. Выбрать из Приложения 11 к Методике оценки угроз безопасности информациивсе актуальные тактики и основные техники реализации угроз (данные внести в таблицу с соответствующим названием).
   2. Подробно описать один из возможных вариантов реализации угроз, для описания использовать простую блок-схему или язык uml.

Актуальные для ИС виды нарушителей, подлежащих оценке:

1. Отдельные физические лица (хакеры).
2. Семья и родственники.
3. Разработка модели угроз персональной ИС.
   1. 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.

**Вывод:** в ходе выполнения лабораторной работы былопродолжено 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: Нарушителей принято разделять на следующие уровни:

* Нарушитель, обладающий базовыми возможностями
* Нарушитель, обладающий базовыми повышенными возможностями
* Нарушитель, обладающий средними возможностями
* Нарушитель, обладающий высокими возможностями

1. Что такое политика информационной безопасности?

Ответ: Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.