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 № 3

**Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности**

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 определению актуальных способов реализации угроз безопасности информации и соответствующих им видов нарушителей и их возможности.

**Задачи:**

1. Определить виды нарушителей, актуальные для персональной ИС.
   1. Используя таблицу «Возможные цели реализации угроз безопасности информации нарушителями, полученную в лабораторной работе №2, оценить цели реализации данных угроз. Для этого необходимо составить таблицу по примеру Приложения 7 «Методики оценки угроз безопасности».

| Виды нарушителей | Возможные цели реализации угроз безопасности информации | Соответствие целей видам риска (ущерба) и возможным негативным последствиям |
| --- | --- | --- |
| Нанесение ущерба физическому лицу |
| Отдельные физические лица (хакеры) | Получение целевой информации о пользователе для получения материальной, финансовой, коммерческой или иной выгоды. Пранк, самоутверждение | У1 – нарушение личной, семейной тайны, утрата чести и доброго имени, финансовый, иной ущерб физическим лицам |
| Авторизованные пользователи систем и сетей | Случайные, неосторожные, неквалифицированные действия в системе | У1 – финансовый, иной материальный ущерб физическим лицам |

* 1. Используя таблицу «Уровни возможностей нарушителей по реализации угроз безопасности информации» (с.56-59), составить таблицу по примеру на с. 60.

| № | Виды риска (ущерба) и возможные негативные последствия | Виды актуального нарушителя | Категория нарушителя | Уровень возможностей нарушителя |
| --- | --- | --- | --- | --- |
| 1 | У1:  Нарушение конфиденциальности персональных данных граждан;  Нарушение личной, семейной тайны, утрата чести и доброго имени;  Финансовый, иной материальный ущерб физическим лицам | Отдельные физические лица (хакеры) | Внутренний | Н2 |
| Авторизованные пользователи систем и сетей | Внешний | Н1 |

1. Определить актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности.
   1. Объединить ранее составленные таблицы и получить новую по примеру на с.62.

| № | Вид нарушителя | Категория нарушителя | Объект воздействия | Доступные интерфейсы | Способы реализации |
| --- | --- | --- | --- | --- | --- |
| 1 | Отдельные физические лица (хакеры) (Н2) | Внешний | Удаленное автоматизированное рабочее место (АРМ) пользователя:  Несанкционированный доступ к операционной системе АРМ пользователя, нарушение конфиденциальности информации, содержащейся на АРМ пользователя |  |  |
| 2 | Авторизованные пользователи систем и сетей (Н1) | Внутренний | АРМ пользователя |  |  |

**Вывод:** в ходе выполнения лабораторной работы былопродолжено знакомство с документом «Методика оценки угроз безопасности информации», а также получены навыки по определению актуальных способов реализации угроз безопасности информации и соответствующих им видов нарушителей и их возможности.

**Ответы на контрольные вопросы:**

1. С какими видами нарушителей вы встречались в своей практике использования ИС?

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. Опишите три любых сценария утечки данных из вашей ИС?

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.