МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ИНСТИТУТ ЦИФРОВЫХ ТЕХНОЛОГИЙ, ЭЛЕКТРОНИКИ И ФИЗИКИ (ИЦТЭФ)

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ЭЛЕКТРОНИКИ (ВТиЭ)

**Отчет по лабораторной работе № 2**

по курсу “Защита информация”

**“Описание информационной системы и определение источников угроз безопасности информации”**

Выполнил студент 506 гр.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Осипенко

Проверил: ст. преп. кафедры ИБ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.С. Ладыгин.

Лабораторная работа защищена

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Цель работы:

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

# Описание информационной системы:

* Наименование персональной ИС: **UnknPC**;
* Назначение ИС:
  + Создание/редактирование документов;
  + Проектирование/разработка/тестирование различных приложений;
  + Реверс Инжиниринг приложений;
  + Создание/управление/редактирования баз данных;
  + Работа с виртуальными машинами;
  + Удаленный доступ к внешнему серверу;
  + Доступ к Интернету;
  + Доступ к онлайн магазинам;
  + Доступ к онлайн банкам;
  + Онлайн гейминг;
  + Офлайн гейминг;
  + Общение с другими людьми;
  + Проектирование/симуляция электрических принципиальных схем;
  + Трассировка печатных плат;
  + 3Д Дизайн.
* Конфигурация системы:
  + Процессор – Ryzen 5600;
  + Материнская плата – Asus Rog A520;
  + Видеокарта – Nvidia GTX 1060 6Gb;
  + Блок питания – Corsair 550W Platinum;
  + Система охлаждения – 6 внешних вентиляторов, 1 вентилятор для процессора;
  + Операционная система – Manjaro Arch linux;
  + Диски: 2 SSD (250Gb, 500Gb), 1 HDD (1Tb);
  + ОЗУ – 2 планки по 8Gb
* Пользователи: Данная ИС используется в основном одни пользователем (уровень доступа user). Авторизация не требуется.
* Внешнии интерфейсы:
  + Доступ в интернет осуществляется через 1Gb кабель, подключенный к Wifi Роутеру;
  + Имеется возможность подключить до 7ми устройств по стандарту USB;
  + Удаленный доступ через SSH.
  + Web Browser.
* Планировка помещения:

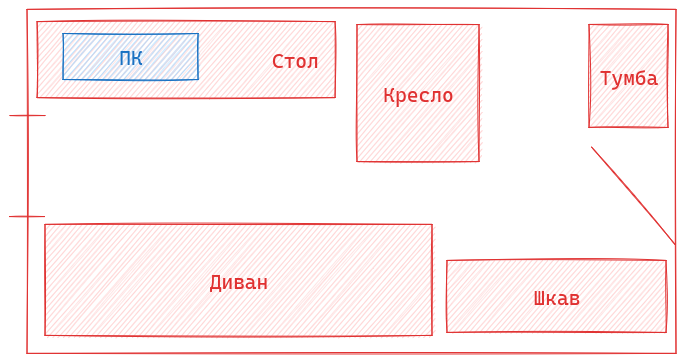


Рис. 1.1 Планировка комнаты размещения ИС

# Таблица “Возможные цели реализации угроз безопасности информации”:

| **№ вида** | **Вид нарушителя** | **Категория нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| --- | --- | --- | --- |
| 1 | Мама | Внутренний | Нарушение целостности ИС, Внедрение вредоносного ПО,  Непреднамеренные, неосторожные или неквалифицированные действия, |
| 2 | Хакер | Внешний | Нарушение целостности ИС,  Внедрение вредоносного ПО,  Получения доступа к конфиденциальным данным,  Получение финансовой выгоды. |
| 3 | Спецслужбы | Внешний | Получение доступа к конфиденциальной информации |
| 4 | Разработчики ПО | Внешний | Внедрения дополнительного, скрытого функционала,  Получение доступа к конфиденциальной информации. |
| 5 | Поставщик услуг связи | Внешний | Получение финансовой выгоды,  Непреднамеренные, неосторожные или неквалифицированные действия,  Получение конкурентных преимуществ |
| 6 | Я | Внутренний | Нарушение целостности ИС, Внедрение вредоносного ПО,  Непреднамеренные, неосторожные или неквалифицированные действия, |

# Вывод:

В ходе данной работы был изучен документом «Методика оценки угроз безопасности информации», и определены источники угроз для моей ИС.

# Контрольные вопросы:

1. Какие уровни возможностей нарушителей вам известны?

- базовыми возможностями по реализации угроз безопасности информации (Н1);

- базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);

- средними возможностями по реализации угроз безопасности информации (Н3);

- высокими возможностями по реализации угроз безопасности информации (Н4).

2. Что такое уязвимость информационной системы?

*Уязвимость ИС* – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

3. Необходимо ли заниматься обеспечением информационной безопасности персональной информационной системы? Дайте обоснованный ответ (не менее 100 слов).

Информационная безопасность персональной информационной системы является важным аспектом, которым необходимо заниматься каждому пользователю. Обеспечение безопасности персональных данных и информации помогает защитить личные и конфиденциальные данные от несанкционированного доступа, кражи, изменения или уничтожения.

Во-первых, обеспечение информационной безопасности помогает предотвратить кражу личных данных, таких как пароли, номера кредитных карт и другие конфиденциальные сведения, которые могут быть использованы злоумышленниками в корыстных целях.

Во-вторых, защита информации способствует предотвращению утечки личной информации, такой как фотографии, документы и другая информация, которая может быть использована против вас или ваших близких.

В-третьих, обеспечение информационной безопасности позволяет предотвратить неправомерное использование вашей личной информации, что может привести к финансовым потерям, репутационным рискам и другим негативным последствиям.

Для обеспечения информационной безопасности персональной системы необходимо соблюдать ряд мер и правил. Например, использовать сложные и уникальные пароли для каждого аккаунта, регулярно менять пароли, отключать автоматический вход в аккаунты, использовать двухфакторную аутентификацию, не открывать подозрительные ссылки и вложения, а также регулярно обновлять программное обеспечение и операционные системы.