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 № 2

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

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 источников угроз безопасности информации для описанной информационной системы.

**Задачи:**

1. Собрать сведения об информационной системе.
   1. Дать наименование персональной информационной системе.

ПК Лаптев А.В.

* 1. Описать назначение, задачи (функции) систем и сетей, состав обрабатываемой информации.

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

Конфигурация включает в себя следующие элементы:

Материнская плата: -

Видеокарта: Intel Iris Xe Graphics

Процессор: Intel Core i5-1135G7 CPU @ 2,4 GHz, 4 ядра, 8 потоков

ОЗУ: DDR4 8Gb

Блок питания: -

ПЗУ: 512Gb SSD (WDC PC SN730)

Система охлаждения: -

Операционная система: Windows 11 Home Single Language

Тип устройства: ноутбук

* 1. Описать группы внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа.

Данная ИС используется одним пользователем с правами доступа администратора. Требуется авторизация.

* 1. Описать внешние интерфейсы и взаимодействие системы и сети с пользователями, иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет».

USB-разъемы (х2)

HDMI-разъем

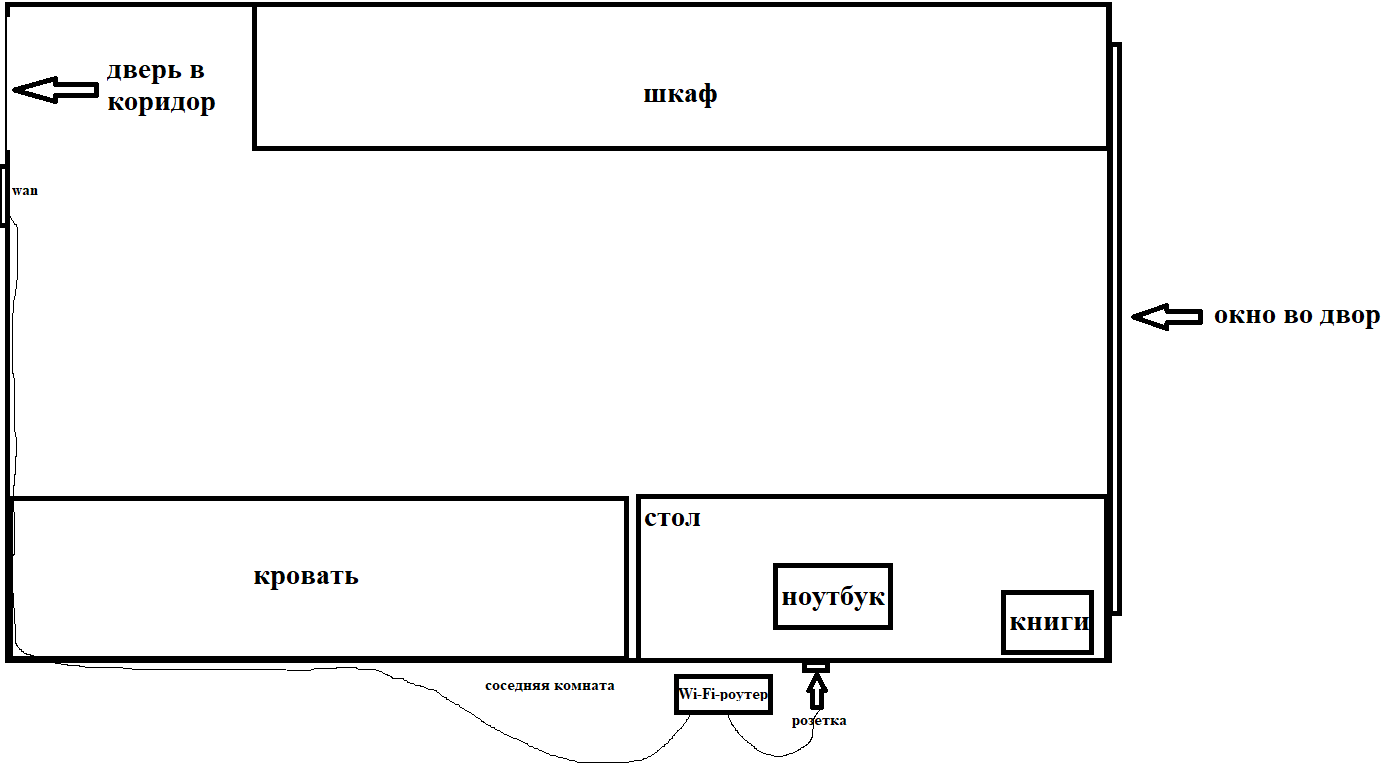
Wi-Fi модуль

Дисплей

Клавиатура

Bluetooth модуль

* 1. Привести схематичное расположение элементов информационной системы внутри помещения.



1. Определить источники угроз безопасности информации.
   1. Частично изучить документ «Методика оценки угроз безопасности информации».
   2. Выделить актуальные для своей ИС виды нарушителей, подлежащих оценке.

Актуальные для ИС виды нарушителей, подлежащих оценке:

1. Отдельные физические лица (хакеры).
2. Семья и родственники.
   1. На основании выбранных актуальных видов нарушителей составить таблицу «Возможные цели реализации угроз безопасности информации.

|  |  |  |  |
| --- | --- | --- | --- |
| № вида | Виды нарушителя | Категории нарушителя | Возможные цели реализации угроз безопасности информации |
| 1 | Отдельные физические лица (хакеры) | Внутренний | Получение целевой информации о пользователе для получения материальной, финансовой, коммерческой или иной выгоды. Пранк, самоутверждение |
| 2 | Авторизованные пользователи систем и сетей | Внешний | Случайные, неосторожные, неквалифицированные действия в системе |

**Вывод:** в ходе выполнения лабораторной работы былопродолжено знакомство с документом «Методика оценки угроз безопасности информации», а также получены навыки по определению источников угроз безопасности информации для описанной информационной системы.

**Ответы на контрольные вопросы:**

1. Какие уровни возможностей нарушителей вам известны?

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 уязвимость информационной системы?

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.

1. Необходимо ли заниматься обеспечением информационной безопасности персональной информационной системы?

Ответ: Да конечно же нужно. В настоящее время на нашем ПК хранится практически вся информация, личные данные, пароли, документы и т.д. Мошенники могут совершать противозаконные действия, зная только номер вашего паспорта, ведь в некоторых случаях остальные данные гражданина не требуются. А по статистике, самым частым способом противоправного использования персональных данных гражданина, а это как правило паспортные данные, является оформление банковских кредитов. Также на общее обозрение может быть выставлена та личная информация, которая дискредитирует вас в обществе, и нанесет непоправимый вред вашей репутации. Часто бывает, что людям, которые не следят за безопасностью своего ПК, и из-за этого им приходится менять место работы, а иногда и место проживания.