**Рекомендуемая структура модели угроз**

**безопасности информации**

УТВЕРЖДАЮ

Руководитель органа

государственной власти

(организации) или иное

уполномоченное лицо

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

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Модель угроз безопасности информации

«ПК Лаптев А.В.»

1. **Общие положения**

Данный документ предназначен для описания угроз безопасности персональной ИС и распространяется на ИС «ПК Лаптев А.В.».

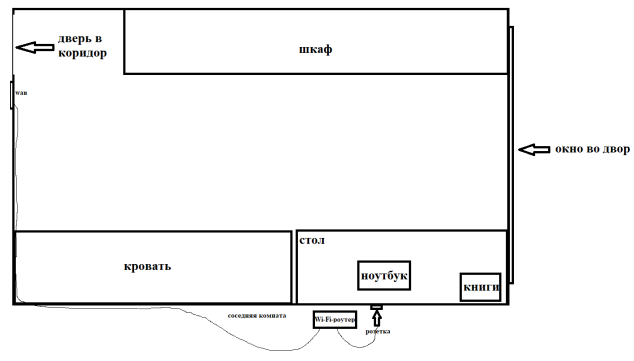
1. **Описание систем и сетей и их характеристика как объектов защиты**

Конфигурация включает в себя следующие элементы:

* 1. Материнская плата: -
  2. Видеокарта: Intel Iris X e Graphics
  3. Процессор: Intel Core i5-1135G7 CPU @ 2,4 GHz, 4 ядра, 8 потоков
  4. ОЗУ: DDR4 8Gb
  5. Блок питания: -
  6. ПЗУ: 512Gb SSD (WDC PC SN730)
  7. Система охлаждения: -
  8. Операционная система: Windows 11 Home Single Language
  9. Тип устройства: ноутбук

Внешние интерфейсы:

* 1. USB-разъемы (х2)
  2. HDMI-разъем
  3. Wi-Fi модуль
  4. Дисплей
  5. Клавиатура
  6. Bluetooth модуль



*Рис. 1. Статическое расположение ИС в помещении.*

1. **Возможные негативные последствия от реализации (возникновения) угроз безопасности информации**

*Таблица 1*

*Виды рисков и возможные негативные последствия*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | 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. **Возможные объекты воздействия угроз безопасности информации**

*Таблица 2*

*Наименование компонентов систем и видов воздействия на них*

|  |  |  |
| --- | --- | --- |
| Негативные последствия | Объекты воздействия | Виды воздействия |
| Нарушение неприкосновенности частной жизни | Архивы с семейными фотографиями (20 штук) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Приложения, которые имеют доступ к микрофону или веб-камере (MS Teams, Discord, Zoom, Google Meet) | Несанкционированный доступ к данным: запись голоса, видеозаписи; использование их для психологического воздействия, шантажа |
| Нарушение тайны переписки, телефонных переговоров, иных сообщений | Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Нарушение личной, семейной тайны, утрата чести и доброго имени | Архивы с семейными фотографиями (20 штук) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах | Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| Сохраненный локально игровой прогресс | Повреждение носителя, на котором располагается сохраненный прогресс |
| Финансовый, иной материальный ущерб физическому лицу | Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| Нарушение конфиденциальности (утечка) персональных данных | Архивы с семейными фотографиями (20) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| «Травля» гражданина в сети «Интернет» | Архивы с семейными фотографиями (20) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Приложения, которые имеют доступ к микрофону или веб-камере (MS Teams, Discord, Zoom, Google Meet) | Несанкционированный доступ к данным: запись голоса, видеозаписи; использование их для психологического воздействия, шантажа |
| Разглашение персональных данных граждан | Архивы с семейными фотографиями (20 штук) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| Нарушение законодательства Российской Федерации | Менеджер паролей в браузере | Хищение аккаунтов, получение доступа к конфиденциальным данным аккаунтов |
| Облачные хранилища (Google Drive, Яндекс Диск) | Несанкционированный доступ к данным, хранящимся в облаке, хищение или манипуляции с данными (подмена, удаление и др.) |
| Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| Архивы с семейными фотографиями (20 штук) | Несанкционированный доступ к содержимому архивов, манипуляции с их содержимым (подмена, редактирование, удаление, выкладывание в открытый доступ) |
| Частная переписка в приложении мессенжера (Whats App, Telegram) | Несанкционированный доступ к личной переписке и ее попадание в открытый доступ |
| Приложения, которые имеют доступ к микрофону или веб-камере (MS Teams, Discord, Zoom, Google Meet) | Несанкционированный доступ к данным: запись голоса, видеозаписи; использование их для психологического воздействия, шантажа |
| Потеря (хищение) денежных средств | Пароли, пин-коды для банковских сервисов | Хищение пин-кодов для доступа к средствам на банковских счетах |
| Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) | Файлы с отчетами по лабораторным и практическим работам, научно-исследовательским работам (40 штук) | Выход из строя носителя информации или всего компьютера в целом |
| Исходный код программ для практических заданий, лабораторных и научно-исследовательских работ (120 штук) | Выход из строя носителя информации или всего компьютера в целом |
| Операционная система | Критические нарушения в работе ОС, требующие ее переустановки или восстановления |

1. **Источники угроз безопасности**

*Таблица 3*

*Категории актуальных нарушителей*

|  |  |  |
| --- | --- | --- |
| 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. **Способы реализации (возникновения) угроз безопасности информации**

*Таблица 4*

*Описание способов реализации угроз безопасности*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | 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 | Доступ через локальную и внешнюю вычислительные сети | Внедрение вредоносного ПО |
| Съемные машинные носители информации, подключаемые к АРМ пользователя | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |
| Сетевые интерфейсы коммутатора сети, где расположен веб-сервер | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |
| 2 | Авторизованные пользователи систем и сетей (Н1) | Внутренний | АРМ пользователя | Доступ через локальную и внешнюю вычислительные сети | Ошибочные действия в ходе настройки АРМ пользователя |
| 3 | Разработчики программных, программно-аппаратных средств  (Н1) | Внутренний | АРМ пользователя | Пользовательский веб-интерфейс доступа к базе данных информационной системы | Возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). |
| 4 | Поставщики вычислительных услуг, услуг связи  (Н1) | Внутренний | Удаленное автоматизированное рабочее место (АРМ) пользователя:  Несанкционированный доступ к операционной системе АРМ пользователя, нарушение конфиденциальности информации, содержащейся на АРМ пользователя | Пользовательский веб-интерфейс доступа к базе данных информационной системы | Возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). |
| 5 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ  (Н1) | Внутренний | АРМ пользователя | Съемные машинные носители информации, подключаемые к АРМ пользователя | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |
| Доступ через локальную и внешнюю вычислительные сети | Ошибочные действия в ходе настройки АРМ пользователя |