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 № 4**

по курсу “Защита информация”

**“Оценка сценариев реализации угроз и актуальности угроз.**

**Модель угроз персональной ИС.”**

Выполнил студент 506 гр.

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

Проверил: ст. преп. кафедры ИБ.

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

Лабораторная работа защищена

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

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

# Модель угроз “UnknPC”:

# **1. Общее положение.**

1.1. Настоящая Модель угроз определяет объекты воздействий и виды воздействия на них, возможные цели реализации угроз информационной информации, определяет актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и из возможностей. Областью действия документа является персональная информационная система (далее ИС) “UnknPC”.

1.2. При разработке настоящей модели угроз использовался методический документ “Методика оценки угроз безопасности информации”.

1.3. Ответственность за обеспечение защиты ИС лежит на локальных пользователях данной ИС.

1.4. Разработка данной модели осуществлялась в АГУ в рамках курса “Защита информации”.

# 2. Описание систем и сетей и их характеристик как объектов защиты.

2.1. Наименование персональной ИС: **UnknPC**;

2.2. 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.

2.3. 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

2.4. Пользователи: Данная ИС используется в основном одни пользователем (уровень доступа user). Авторизация не требуется.

2.5. 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.

2.6. Планировка помещения:

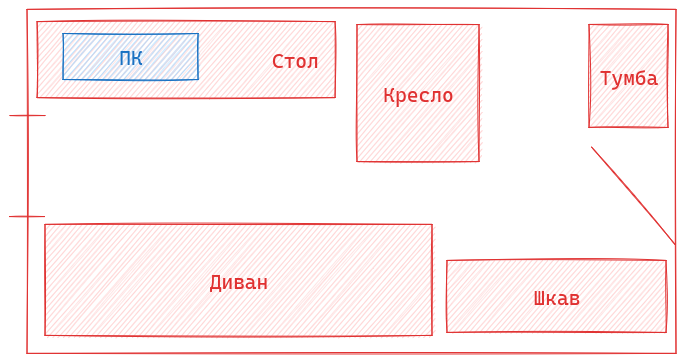


Рис. 2.1 Планировка комнаты размещения ИС

# 3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации.

| **Виды риска (ущерба)** | **Возможные негативные последствия** |
| --- | --- |
| У1: Ущерб физическому лицу | нарушение конфиденциальности персональных данных граждан; |
|
| нарушение личной семейной тайны, утрата чести и доброго имени; |
| финансовый, иной материальный ущерб физических лиц |

# 4. Возможные объекты воздействия угроз безопасности информации.

| **Объект воздействия** | **Нежелательные воздействия** |
| --- | --- |
| Сохранённые пароли в веб браузере | несанкционированный доступ к аккаунта firefox и синхронизация сохраненных паролей и сессий |
| Коллекция красивых картинок | получение доступа к папке |
| Локальные базы данных | получение доступа к локальным БД и воздействия на них |
| Админский аккаунт ОС | получение доступа к аккаунту администратора компьютера |
| Аккаунт Steam | получение несанкционированного доступа к аккаунту |
| Аккаунт Google |
| Аккаунт VK |
| Аккаунт Github |
| Банковский аккаунт/приложение |
| Персональный сайт | получение доступа к административной панели сайта,  ДДОС |
| Удаленный сервер | получение доступа к серверу |

# 5. Источники 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, |

# 6. Способы реализации (возникновения) угроз безопасности информации.

| **№ п/п** | **Вид нарушителя** | **Объект воздействия** | **Способы реализации** | **Негативные последствия** |
| --- | --- | --- | --- | --- |
| 1 | Хакеры (Н2) | ПК пользователя;  Локальная сеть и подключенные к ней устройства. | Удаленный запуск вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему.  Запуск вредоносной программы собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометирующего гипервизора;  Получение нарушителем доступа к данным и функциям, предназначенным для учетных записей с более высокими чем у нарушителя привилегиями, за счет ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. | утечка данных и возможная потеря доступа к различным аккаунтам  стыд, угрозы, травля  утечка, потеря данных  нарушение целостности системы, целостности и конфиденциальности хранимых данных  утеря коллекции игр,  собираемой долгими годами и большими средствами  потеря доступа к почте и связанных с ней аккаунтов и информации  получение несанкционированного доступа к личным перепискам и их возможная утечка  нарушение конфиденциальности приватных и целостности всех репозиториев  финансовый ущерб |
|
| 2 | Авторизованные пользователи систем и сетей (Н1) | ПК пользователя | Утечка пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации;  Нарушение функционирования программных, программно-аппаратных элементов информационной системы или информационной системы в целом из-за некорректной работы установленных обновлений (патчей) системного программного обеспечения;  Перехват управления программой за счет использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки). |

# 7. Актуальные угрозы безопасности информации.

| **Тактика** | **Основные техники** |
| --- | --- |
| Т1. Сбор информации о системах и сетях | Т1.3 – 12. |
| Т2. Получение первоначального доступа к компонентам систем и сетей | Т2.3 – 7. |
| Т3. Внедрение и исполнение вредоносного программного обеспечения в системах и сетях | Т3.1 – 9. |
| Т4. Закрепление (сохранение доступа) в системе или сети | Т4.2 – 6. |
| Т5. Управление вредоносным программным обеспечением и (или) компонентам, к которым ранее был получен доступ | Т5.1 – 3, 5 – 12. |
| Т6. Повышение привилегий по доступу к компонентам систем и сетей | Т6.1 – 9. |
| Т7. Сокрытие действий и применяемых при этом средств от обнаружения | Т7.1 – 4, 10 – 29. |
| Т8. Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям. | Т8.1 – 8. |
| Т9. Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности и информации или реализации новых угроз. | Т9.1 – 14. |
| Т10. Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям. | Т10.1 – 13. |



Рис 6.1 Возможный вектор атаки на скомпрометированной устройство.

# Вывод:

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

# Контрольные вопросы:

1. Зачем необходимо создавать Модель угроз в организации? Дать обоснованный ответ (не менее 100 слов).

Создание модели угроз в организации является критически важным шагом в процессе управления рисками. Это позволяет организациям идентифицировать, оценить и управлять потенциальными угрозами, которые могут повлиять на их бизнес, информационные системы или персонал. Модель угроз помогает в:

– Идентификации угроз: Определение потенциальных угроз, которые могут возникнуть в организации.

– Оценке рисков: Оценка вероятности и возможного влияния каждой угрозы на организацию.

– Разработке стратегий управления рисками: На основе оценки рисков, модель угроз помогает разработать эффективные стратегии управления рисками.

– Улучшении безопасности: Постоянное обновление использование модели угроз помогает организациям оставаться в курсе последних угроз и адаптироваться к изменяющимся условиям.

Таким образом, создание и постоянное обновление модели угроз позволяет организации быть лучше подготовленной к возможным угрозам и обеспечивая защиту своих активов интересов.

2. Что такое политика информационной безопасности?

Политика информационной безопасности – это набор правил, процедур и практик, которые регулируют управление информационными ресурсами организации и обеспечивают их защиту от различных угроз, таких как несанкционированный доступ, взлом, утечка данных и другие киберугрозы.