Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Факультет математики и информационных технологий

Кафедра фундаментальной информатики

ЛАБОРАТОРНАЯ РАБОТА №1

по дисциплине: Системы информационной безопасности предприятия

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Автор лабораторной работы А. Е. Конышев

Обозначение лабораторной работы ЛР–02069964–02.03.02–08–23

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель Е. Н. Гришанов

Оценка: \_\_\_\_\_\_\_

Саранск 2023

Цель работы: Анализ и классификация угроз конкретного предприятия.

**Ход работы:**

Ознакомиться с теоретическим материалом.

Выполнить задания.

Задания:

Определить угрозы и риски для информационной безопасности предприятия.

Классифицировать угрозы и риски.

Разработать рекомендации для предотвращения угроз.

**Описание выполнения работы.**

В качестве исследуемого предприятия возьмем центр детского развития.

**Описание предприятия:**

Центр детского развития представляет собой 2-х этажное здание с небольшим количеством комнат. На первом этаже расположены административные комнаты, служебные помещения, санузел, буфет, спорт зал, некоторое число комнат для цифрового обучения (компьютерные классы). На втором этаже так же расположены комнаты цифрового обучения, а также серверная комната, где в основном хранится и информация для работы этого центра.

**Возможные угрозы:**

Выход из строя оборудования, обрыв линии электропередачи, ошибки в работе ОС и ПО, затопление, попадание молнии, столкновение автомобиля со зданием, кража персональных данных из БД, несанкционированный доступ в помещения для обучения детей и помещения для персонала, старение носителей информации, использование инфраструктуры центра не по назначению, компьютерные вирусы.

**Классификация угроз:**

**По природе возникновения:**

*Естественные:*

Затопление, попадании молнии, старение носителей информации.

*Искусственные:*

Обрыв линии электропередачи, ошибки в работе ОС и ПО, столкновение автомобиля со зданием, кража персональных данных из БД, несанкционированный доступ в помещения для обучения детей и помещения для персонала, использование инфраструктуры центра не по назначению, компьютерные вирусы.

**По положению источника угрозы:**

*Вне контролируемой АС:*

Затопление, попадание молнии, столкновение автомобиля.

*В пределах АС:*

Выход из строя оборудования, обрыв линии электропередачи, ошибки в работе ОС и ПО, кража персональных данных из БД, несанкционированный доступ в помещения для обучения детей и помещения для персонала, старение носителей информации, использование инфраструктуры центра не по назначению, компьютерные вирусы.

**По степени воздействия на АС:**

*Пассивные угрозы:*

Угроза разглашения.

*Активные угрозы:*

кража персональных данных из БД, компьютерные вирусы.

**Рекомендации:**

Для эффективного устранения угроз и обеспечения безопасности нашего центра детского развития, рекомендуется следовать следующим рекомендациям:

* **Выход из строя оборудования:**
  + Регулярное проведение технического обслуживания оборудования, включая проверку наличия обновлений прошивки и драйверов.
  + Зарезервирование критически важных компонентов оборудования и поддержание их в актуальном состоянии.
    - **Обрыв линии электропередачи:**
  + Рассмотрение возможности установки резервного источника питания, такого как генератор или ИБП, для обеспечения непрерывности питания.
  + Регулярная проверка состояния электрической инфраструктуры и проведение необходимого обслуживания и обновления оборудования.
    - **Ошибки в работе ОС и ПО:**
  + Следование обновлениям и патчам операционной системы и программного обеспечения, и их своевременная установка.
  + Регулярное создание резервных копий данных и системных настроек, чтобы в случае сбоя была возможность быстрого восстановления.
    - **Затопление:**
  + Разработка плана эвакуации, чтобы персонал знал, как действовать в случае угрозы затопления.
  + Регулярная проверка систем водоотведения и проведение необходимого обслуживания, чтобы предотвратить затопление.
  + Плановые проверки состояния крыши здания
  + Оценка предполагаемого ущерба, для резервирования данных и перевода здания в режим, при котором включенным остается сервер.
    - **Попадание молнии:**
  + Установка громоотводов на крыше здания. Громоотводы представляют собой металлические конструкции, которые направляют электрический разряд в землю. Они должны быть установлены на всех углах крыши и направлены в сторону от земли.
  + Размещение молниезащиты. Молниезащита представляет собой систему проводов и тросов, которая соединяет заземляющий провод с металлическими конструкциями здания. Она должна быть установлена на всех частях здания, где есть вероятность попадания молнии.
  + Использование изолирующих материалов. Для предотвращения проникновения электрического тока через стены и крышу здания, необходимо использовать изоляционные материалы, такие как минеральная вата или пенопласт.
    - **Столкновение автомобиля со зданием:**
  + Установка бетонных ограждений, изолирование входа от проезда автомобилей
    - **Кража персональных данных из БД:**
  + Обеспечение безопасности БД путем реализации мер защиты, таких как шифрование данных, установка многоуровневой аутентификации и контроль доступа.
  + Регулярное обновление и патчинг программного обеспечения, используемого для управления БД, с целью устранения известных уязвимостей.
  + Обучение сотрудников по вопросам безопасности данных и проведение аудитов для выявления потенциальных уязвимостей.
    - **Несанкционированный доступ в помещения для обучения детей и помещения для персонала:**
  + Установка системы контроля доступа, ведение пропусков, электронных замков, систем видеонаблюдения.
    - **Старение носителей информации:**
  + Разработка плана регулярного обновления и замены носителей информации, таких как жесткие диски или флэш-накопители, в соответствии с рекомендациями производителей.
  + Регулярное создание резервных копий данных и их хранение на надежных и актуальных носителях.
  + Мониторинг состояния носителей информации и замена поврежденных или устаревших носителей вовремя.
    - **Использование инфраструктуры центра не по назначению:**
  + Мониторинг деятельности обучающихся и персонала
    - **Компьютерные вирусы:**
  + Установка и регулярное обновление антивирусного программного обеспечения на всех компьютерах и серверах.

Перед началом учебных действий дети и персонал должны знать правила поведения в аудиториях, комплексе действий во время ЧП, техники безопасности, плане эвакуации. Рекомендуется так же прохождение теста на знания по ТБ для доступа к занятиям.