Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

Кафедра защиты информации

ОТЧЕТ

Практическое занятие №4

«Анализ угроз безопасности информации»

Выполнили:

студенты гр. №

Кухоцковолец А. М.

Панкратьев Е. С.

Габрусь С. П.

Проверил:

Столер Д.В.

Минск 2024

**Цель занятия:** изучить классификацию угроз безопасности информации, методику их оценки и получить практические навыки по ее применению для заданных информационных объектов.

Результаты выполнения практического задания.

Таблица 1 – Анализ угроз для заданных информационных объектов

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Краткое описание защищаемого объекта | Угроза безопасности информации / вид угрозы безопасности информации | Возможные негативные последствия вследствие реализации угрозы | Ущерб  (в случае приемлемости указать почему) | Метод защиты | Средство защиты или мероприятие |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. Карта флеш памяти с разъемом USB, которая содержит информацию распространение и (или) предоставление которой ограниченно. Устройство хранится на столе. Информация, записанная на устройстве, больше нигде не продублирована | 1.1 Вирусная атака на флеш-память | Потеря данных, инфицирование системы | Не приемлем | Технический метод | Антивирусное программное обеспечение |
| 1.2 Утеря флеш-карты | Потеря конфиденциальных данных | Не приемлем | Организационный метод | Перенос флеш-карты в безопасное место хранения |
| 1.3 Несанкционированный доступ к флеш-памяти | Разглашение конфиденциальной информации | Не приемлем | Организационный метод | Установка физических барьеров, ограничивающих доступ |
| 1.4 Физическое повреждение флеш-памяти | Утрата доступа к данным | Не приемлем | Технический метод | Создание резервных копий данных |
| 1.5 Подмена флеш-памяти на поддельную | Несанкционированный доступ к данным, внедрение вредоносного ПО | Не приемлем | Технический метод | Проверка подлинности устройств перед использованием |

Продолжение таблицы 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Краткое описание защищаемого объекта | Угроза безопасности информации / вид угрозы безопасности информации | Возможные негативные последствия вследствие реализации угрозы | Ущерб  (в случае приемлемости указать почему) | Метод защиты | Средство защиты или мероприятие |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2. Персональный компьютер, подключенный к сети Интернет. На компьютере хранится информация распространение и (или) предоставление которой ограничено. В информационной сети на сервере содержится резервная копия этой информации. Компьютер стоит на столе в помещении | 2.1 Вредоносное программное обеспечение | Инфицирование системы, потеря данных | Не приемлем | Технический метод | Антивирусное программное обеспечение, брандмауэры |
| 2.2 Физическая кража или утеря компьютера | Разглашение конфиденциальной информации | Не приемлем | Организационный метод | Установка физических замков на дверь помещения, где находится компьютер |
| 2.3 Несанкционированный доступ к компьютеру | Разглашение конфиденциальной информации | Не приемлем | Организационный метод | Установка паролей на компьютер и аккаунты пользователей |
| 2.4 Утечка данных через сеть Интернет | Разглашение конфиденциальной информации | Не приемлем | Технический метод | Шифрование данных, использование виртуальной частной сети (VPN) |
| 2.5 Физическое повреждение компьютера | Потеря доступа к данным | Приемлем  (резервная копия содержится на сервере) |  |  |

Продолжение таблицы 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Краткое описание защищаемого объекта | Угроза безопасности информации / вид угрозы безопасности информации | Возможные негативные последствия вследствие реализации угрозы | Ущерб  (в случае приемлемости указать почему) | Метод защиты | Средство защиты или мероприятие |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3. Банковская карта, хранящаяся в тумбочке ее владельца. Карта выпущена в одном экземпляре | 3.1 Утеря банковской карты | Несанкционированный доступ к средствам на карте | Неприемлемо | Технический | Хранение карты в безопасном месте, например, в сейфе |
| 3.2 Клонирование банковской карты | Несанкционированные транзакции, потеря денежных средств | Неприемлемо | Технический метод | Использование банковских карт с технологией чипа и PIN-кодом |
| 3.3 Физическая кража тумбочки с картой | Несанкционированный доступ к средствам на карте | Неприемлемо | Технический | Установка физических замков на дверь, хранение карты в сейфе |
| 3.4 Сканирование данных с банковской карты через скиммер | Несанкционированные транзакции, потеря денежных средств | Неприемлемо | Технический метод | Проверка банкоматов на наличие вмонтированных скиммеров перед использованием |
| 3.5 Фишинг | Получение доступа к конфиденциальной информации о карте путем обмана пользователя, потеря денежных средств | Неприемлемо | Организационный метод | Обучение владельца карты узнавать подозрительные запросы и сообщения, использование антивирусного программного обеспечения с функцией анти-фишинга |