Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По индивидуальному заданию №10**

Студент: Даваев Николай Евгеньевич

Дисциплина/Профессиональный модуль: ОС

Выполнил студент

Группы: 2ОИБАС-1222

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

**Индивидуальная работа №10**

**Цель работы:** изучить угрозы информационной безопасности; научиться определять угрозы и способы их предотвращения

**Задание:**

1. Заполнить таблицу

2. Ответить на контрольные вопросы

**Ход работы:**

**№1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Объект защиты** | **Наименование угрозы** | **Источник угрозы** | **Последствия** | **Как избежать угрозы** |
| Банковская карта | Кража карты | Физический доступ злоумышленников к карте | Несанкционированные транзакции, потеря средств | Носите карту в безопасном месте, не показывайте ее другим, активируйте системы SMS-уведомлений о транзакциях. |
| Фишинг | Мошеннические веб-сайты, электронные сообщения | Передача конфиденциальных данных злоумышленникам | Внимательно проверяйте URL-адреса веб-сайтов и электронные сообщения, не раскрывайте личные данные. |
|  | Компрометация банковской системы | Атаки на серверы банка | Несанкционированный доступ и утечка данных | Используйте банкинговские приложения с двухфакторной аутентификацией и следуйте рекомендациям банка по безопасности. |
| Социальная инженерия | Злоумышленники, обманывающие пользователей | Выдача конфиденциальных данных | Будьте осторожны, не предоставляйте личные данные по телефону или электронной почте без проверки подлинности. |
| Домашний компьютер | Спам-почта и нежелательные сообщения | Навязчивая рассылка электронной почты | Загрязнение почтового ящика, потенциальные мошеннические схемы | Используйте фильтры для электронной почты, не открывайте подозрительные вложения и ссылки. |
| Атаки на веб-камеру и микрофон | Взлом или несанкционированный доступ к устройствам | Нарушение конфиденциальности и слежка | Закройте веб-камеру и микрофон, используйте антивирусное ПО и брандмауэры. |
| Угрозы через обмен файлами | Зараженные файлы и обмен данными | Загрязнение компьютера и потеря данных | Проверяйте файлы на вирусы перед открытием, используйте надежные и безопасные платформы для обмена файлами. |
| Атаки на беспроводные сети | Взлом паролей Wi-Fi, атаки на сеть | Несанкционированный доступ к вашей сети | Используйте сильные пароли для Wi-Fi, отключите WPS (Wi-Fi Protected Setup), обновляйте маршрутизатор. |
| Потеря данных из-за сбоев | Неисправности жестких дисков, ошибки в работе | Потеря важных данных | Регулярно создавайте резервные копии данных, используйте средства мониторинга состояния дисков. |
| Банкомат | Скимминг | Вредоносные устройства, установленные на банкомате | Кража банковских данных и денег клиентов | Регулярная проверка банкоматов на наличие скиммеров, защитные устройства, обучение клиентов. |
| Вирусы и вредоносное ПО | Загрязненные носители, зараженные банкоматы | Потеря данных и блокировка банкомата | Регулярное обновление антивирусов, ограничение доступа к внешним носителям. |
| Физическое воздействие | Попытка взлома банкомата, взрывы | Утеря денег, угроза безопасности клиентов | Физическая защита банкоматов, системы тревожной сигнализации. |
| Сетевые атаки | Атаки на сеть банка и банкоматы | Потеря доступа к банковским данным и деньгам | Защита сети, использование средств обнаружения вторжений. |
| Угрозы со стороны сотрудников | Несоблюдение политики безопасности сотрудниками | Утеря данных и доступ к банковским ресурсам | Обучение сотрудников, мониторинг и соблюдение политики безопасности. |
| Атаки на операционную систему | Уязвимости в операционной системе банкомата | Компрометация системы и данных | Регулярное обновление операционной системы и защита от известных уязвимостей. |
| Отказ в обслуживании (DoS) | Массовые запросы к банкомату | Простой банкомата и недоступность для клиентов | Используйте средства защиты от DoS-атак и мониторьте сеть. |
| Угрозы через облачные службы | Утечки данных из облачных хранилищ | Потеря конфиденциальных данных | Используйте сильные пароли и шифрование для облачных аккаунтов банкоматов. |

**№2**

Контрольные вопросы

1.Что принято называть угрозой информационной безопасности?

Угрозой информационной безопасности могут быть различные виды атак и действий, направленных на нарушение конфиденциальности, целостности или доступности информации. Некоторые из наиболее распространенных угроз информационной безопасности включают в себя: Вирусы, черви и другие вредоносные программы Фишинг и социальная инженерия DDoS-атаки (атаки на отказ в обслуживании)Несанкционированный доступ к данным Утечки информации и нарушения конфиденциальности Кибершпионаж и киберпреступность Недостатки в защите информационных систем и программного обеспечения

2.Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

Методы защиты информации могут быть классифицированы по различным критериям, включая характер проводимых мероприятий. Вот некоторые основные методы защиты информации:

1. Физическая защита:

- Контроль доступа к помещениям и оборудованию

- Использование сейфов, замков, камер видеонаблюдения и других средств физической безопасности

2. Логическая (компьютерная) защита:

- Аутентификация (пароли, биометрическая идентификация и т.д.)

- Шифрование данных и сетевого трафика

- Установка и обновление антивирусного и антишпионского ПО

- Файерволы и другие средства контроля сетевого трафика

3. Организационные меры: Проведение обучения сотрудников по правилам информационной безопасности. Установление политик безопасности и процедур управления доступом. Регулярное аудирование систем безопасности и контроль соответствия стандартам

4. Криптографические методы:Использование криптографических алгоритмов для защиты данных и коммуникаций

5. Физическая разрушаемость: Уничтожение бумажных документов, жестких дисков, USB-накопителей и других носителей информации после использования

3.Какова классификация угроз информационной безопасности?

Угрозы информационной безопасности могут быть классифицированы по различным критериям. Одним из основных подходов к классификации угроз является деление их на следующие категории:

1. Внутренние угрозы:

- Несанкционированный доступ сотрудников к конфиденциальной информации

- Умышленные или случайные действия сотрудников, приводящие к утечке данных или нарушению безопасности

2. Внешние угрозы:

- Кибератаки со стороны хакеров, злоумышленников и кибершпионов

- Вредоносные программы, включая вирусы, троянские программы, шпионское ПО и другие виды вредоносного кода

3. Физические угрозы:

- Кража или утрата физических носителей информации (например, утерянные или украденные ноутбуки, USB-накопители и т.д.)

- Физические разрушения, такие как пожары, наводнения и другие чрезвычайные ситуации

4. Социальная инженерия:

- Манипуляция людьми с целью получения конфиденциальной информации (например, методы фишинга, обмана и манипуляции)

5. Угрозы связанные с технологиями:

- Уязвимости в программном обеспечении и аппаратных средствах

- Недостатки в процедурах и политиках безопасности

4.Что понимается под термином информационный объект?

Информационный объект - это конкретная единица информации, которая имеет ценность и требует защиты. Это может быть файл, документ, база данных, электронное сообщение, либо другой носитель информации, который содержит конфиденциальные или важные данные для организации или лица. Защита информационных объектов является ключевой частью обеспечения информационной безопасности.

5.Что представляет собой угроза права собственности?

Угроза права собственности представляет собой потенциальную опасность для законных прав собственности человека или организации на их имущество, интеллектуальную собственность или другие активы. Это может включать в себя различные виды угроз, такие как: Кража: Физическое похищение имущества или воровство информации. Вандализм: Умышленное повреждение или уничтожение имущества. Мошенничество: Обман для получения незаконного доступа к имуществу или для его незаконного перевода. Неправомерное завладение: Незаконное захватывание имущества или его использование без разрешения. Нарушение интеллектуальной собственности: Незаконное использование патентов, авторских прав, товарных знаков или других видов интеллектуальной собственности. Угрозы со стороны конкурентов: Недобросовестные действия конкурентов, направленные на ослабление позиции собственника имущества. Юридические угрозы: Угрозы со стороны правительственных органов, регуляторов или других юридических структур, такие как налоговые проверки, конфискация имущества и т.д.