Федеральное государственное образовательное бюджетное

учреждение высшего образования

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

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По индивидуальной работе “Выявление угроз информационной безопасности в конкретных ситуациях”**

Студент: Гамидов Аслан Эльчинович

Дисциплина/Профессиональный модуль: Обеспечение информационной безопасности автоматизированных систем

Выполнил студент

Группы: 2ОИБАС-1322

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Объект защиты | Наименование угрозы | Источник угрозы | Последствия | Как избежать угрозы |
| Банковская карта | Кража карты | Физический доступ злоумышленника 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. |
| Рабочее место директора | Кража документов | Физический доступ к бумажным документам | Утеря конфиденциальных бизнес-данных, нарушение конфиденциальности | Используйте сейфы, ограничьте доступ к документам, обучайте сотрудников обращаться с конфиденциальной информацией. |
| Атака на рабочее место через открытые Wi-Fi сети | Нескрываемые или незащищенные сети Wi-Fi | Перехват данных и доступ к устройству | Используйте виртуальные частные сети (VPN), избегайте подключения к открытым Wi-Fi сетям на рабочем устройстве |
| Социальные сети | Мошеннические аккаунты, фейковые профили | Репутационный ущерб, фишинг-попытки, утеря конфиденциальных данных | Будьте осторожны в социальных сетях, не публикуйте чувствительную информацию, настройте приватность аккаунтов. |
| Угрозы сотрудников | Внутренние угрозы, недобросовестные сотрудники | Утеря конфиденциальных данных, нарушение политики безопасности | Установите строгие правила доступа, мониторьте действия сотрудников, обучайте их правилам информационной безопасности. |
| Внутренние угрозы данных | Утечка данных среди сотрудников | Несанкционированное раскрытие конфиденциальной информации | Ограничьте доступ к конфиденциальным данным только необходимым сотрудникам, внедрите системы мониторинга |
| Домашний комьютер | 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 |
| Рабочее место в больнице | Атаки на медицинское оборудование | Вредоносные воздействия на медицинское оборудование | Нарушение функциональности оборудования, опасность для пациентов | Обновляйте программное обеспечение медицинского оборудования, ограничьте физический доступ. |
| Угрозы через медицинские приложения | Вредоносные приложения и атаки на медицинское ПО | Компрометация системы и медицинских данных | Загружайте приложения только из официальных источников, обновляйте ПО. |
| Атаки на медицинские записи | Несанкционированный доступ к медицинским записям | Нарушение конфиденциальности пациентов, медицинских ошибок | Ограничьте доступ к медицинским данным и ведите журналы мониторинга |
| Нарушение физической безопасности | Утеря или кража устройств | Потеря данных и доступ к медицинской информации | Защитите устройства паролем, используйте средства удаленной блокировки и стирания данных. |
| Атаки на критическую инфраструктуру | Атаки на системы электроснабжения и связи | Простой инфраструктуры и риск для пациентов | Улучшите физическую защиту критической инфраструктуры и создайте планы восстановления после кризиса. |
| Фирма по разработке ПО | Атаки на бэкэнд-серверы | Атаки на серверы, хранящие клиентские данные | Утеря данных, нарушение конфиденциальности | Укрепите безопасность бэкэнд-серверов и мониторьте их состояние. |
| Атаки на внутренние системы | Несанкционированный доступ в офисы и серверные помещения | Нарушение безопасности, физическая угроза | Установите системы контроля доступа и мониторинга внутренних помещений. |
| Угрозы через обмен файлами | Вредоносные файлы и загрузки | Загрязнение системы и угрозы безопасности | Проверяйте файлы на вирусы перед открытием и используйте безопасные платформы для обмена файлами. |
| Угрозы через облачные службы | Утечки данных из облачных хранилищ | Потеря конфиденциальных данных | Используйте сильные пароли и шифрование для облачных аккаунтов |
| Нарушение физической безопасности | Утеря или кража устройств | Потеря данных и доступ к конфиденциальной информации | Защитите устройства паролем, используйте средства удаленной блокировки и стирания данных. |
| 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. |

Контрольные вопросы

1. Что принято называть угрозой информационной безопасности?

Угрозой информационной безопасности называется любое событие, действие или обстоятельство, которое может представлять риск для конфиденциальности, целостности или доступности данных и информационных систем. Это включает в себя вирусы, хакерские атаки, утечки данных, фишинг, а также физические угрозы и ошибки сотрудников, которые могут привести к потере данных и ущербу для информационной безопасности. Эффективная защита от таких угроз включает в себя меры технической, организационной и образовательной безопасности.

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

Методы защиты информации классифицируются на три основных

типа:

1. Технические методы, включающие в себя использование шифрования, брандмауэров, антивирусов и других технологий для обеспечения безопасности данных.
2. Организационные методы, включающие в себя разработку политик и процедур безопасности, обучение сотрудников и управление доступом.
3. Физические методы, включающие в себя физическую защиту оборудования и доступ к нему, а также меры предотвращения природных бедствий и катастроф. Комбинированный подход, включающий элементы всех трех методов, обеспечивает наиболее надежную защиту информации.
4. Какова классификация угроз информационной безопасности?

Угрозы информационной безопасности классифицируются на следующие основные категории:

1. Технические угрозы: Включают в себя вирусы, хакерские атаки, фишинг, утечку данных и другие технологические методы, которые нарушают целостность и конфиденциальность информации.
2. Организационные угрозы: Связаны с недобросовестными сотрудниками, нарушением политики безопасности и ошибками в управлении информационной безопасностью.
3. Физические угрозы: Охватывают природные бедствия, кражи, пожары и другие события, которые могут повредить физическое оборудование и инфраструктуру.

Классификация угроз информационной безопасности помогает оценить риски и разработать соответствующие стратегии защиты.

1. 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.

1. Что представляет собой угроза права собственности?

Угроза права собственности представляет собой потенциальную опасность для владельцев имущества или интеллектуальной собственности. Это может включать в себя кражу, повреждение или несанкционированное использование физических активов, таких как имущество и техническое оборудование, а также интеллектуальных активов, таких как авторские права, патенты и торговые марки. Угроза права собственности может привести к финансовым потерям и ущербу для бизнеса или частного лица, поэтому ее важно эффективно предотвращать и контролировать.