**Часть1.**

**Задание 1**

Ситуация *а*

Последствия: утечка гос. тайны ввиду посещения сомнительных сайтов в интернете и копирования данных, открытие конкурирующей организации, использующей секретные данные в своих целях.

Как устранить: уволить сотрудника, сменить пароли, изменить место хранения гос. информации, изъять средство со скопированными данными, удалить подозрительные утилиты.

Как предотвратить: закрыть доступ к секретным данным для копирования или усилить контроль за доступом к этим данным. Возможно необходимо будет подписать акт о нераспространении конфиденциальной информации, ввести штрафы\увольнения за распространение информации и ввести мониторинг активности на рабочем устройстве сотрудника.

Ситуация *b*

Последствия: утечка данных, заражение компьютера вирусами, разрушение локальной сети компании, утечка паролей, взлом средств удаленного управления.

Как устранить: смена паролей, удаление потенциально опасных утилит, копирование данных для последующего восстановления.

Как предотвратить: усилить политику безопасности, ознакомить сотрудников с ней. Ввести мониторинг активности компьютеров сотрудников для выявления установки потенциально опасной программы. Можно попробовать внедрить хэширование паролей и шифрование важных данных для защиты от взлома и утечки.

**Часть 2**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Объекты | Угрозы | Источник угрозы | Методы предотвращения угрозы | Последствия |
| 1 | Дебетовая карта | * Кража физической карты * Фишинг * Социальная инженерия | * Злоумышленники * Мошенники * Веб-сайты и эл. сообщения * Подозрительные звонки | * Хранить в безопасном месте * Подключить смс уведомления * Проверять адрес веб-сайта * Подключение спам-защитника | * Потеря денежных средств * Передача персональных данных злоумышленникам |
| 2 | Считывающее устройство карт | * Скиммер * Накладная клавиатура * Вредоносное ПО и вирусы | * Вредоносное устройство * Зараженные устройства | * Оповещение сотрудников и клиентов * Антивирусы | * Кража банковских данных * Кража денег клиента * Блокировка банкомата |
| 3 | Стационарный ПК | * Атака на веб-камеру и микрофон * Угроза атаки на беспроводные сети * Угроза майнинга | * Устройство, осуществляющее несанкционированный доступ * Взлом wifi пароля * Атака на wifi сеть * Подозрительное ПО | * Антивирус * Брандмауэр * Надежный пароль * Обновление маршрутизаторов | * Нарушение конфиденциальности * Слежка * Несанкционированный доступ к сети * Использование ресурсов вашего ПК |
| 4 | Рабочее место в  Полиции | * Прослушка\жучок * Виброакустический канал * Атаки на критическую инфраструктуру | * Злоумышленник * Атака на системы электроснабжений и связи | * Аккредитация помещения * Установка белого шума * Улучшение физической защиты и создание плана восстановления после атаки | * Утеря конфиденциальных данных * Простой инфраструктуры |
| 5 | Компания по разработке ПО | * Атака на бэкенд сервер * Угроза через обмен файлами * Внутренние угрозы | * Атака на сервера, хранящие клиентские данные * Вредоносные файлы * Недоброжелательные сотрудники | * Укрепление и мониторинг состояния сервера * Использовать безопасные платформы обмена * Подписывать акт о неразглашении | * Утеря данных * Нарушение конфиденциальности * Загрязнение системы * Угроза безопасности * Утечка данных |
| 6 | Рабочее место  Управлявшего | * Радираздаточное устройство * Вирусы на рабочем ПК * Атака на производственную сеть | * Злоумышленники * Вредоносные файла * Атака на wifi сеть организации | * Копирование и архивация данных * Белый шум * Аккредитация помещения * Улучшение и мониторинг защиты сервера | * Кража конфиденциальной информации * Утеря данных * Простой инфраструктуры * Отсутствие связи по сети |

**Контрольные вопросы**

1. *Информационная безопасность* - это совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец несет убытки.
2. *Составляющие ИБ:* конфиденциальность, целостность, доступность.
3. *Информационный объект* – это среда, в которой информация создается, обрабатывается, хранится и передается. Под угрозой ИБ объекта подразумевается возможные воздействия на него, приводящие к ущербу.
4. При нарушении одной из составляющих ИБ, информационная система будет уязвима к проникновению извне.
5. 1. *Технические методы защиты информации*:  
   *Шифрование данных*: метод защиты, при котором информация преобразуется в зашифрованный вид, который доступен только авторизованным пользователям.  
   *Использование брандмауэров и антивирусного ПО*: защита сетей и компьютеров от несанкционированного доступа и вредоносных программ.  
   *Биометрическая аутентификация*: использование биологических параметров человека (например, отпечатков пальцев или распознавание лица) для идентификации пользователей.  
     
   *2. Организационные методы защиты информации:  
   Разработка политики безопасности*: установление правил и процедур для обеспечения безопасности информации в организации.  
   *Обучение персонала*: проведение обучения сотрудников по правилам безопасности информации и профилактике утечек данных.  
   *Управление доступом*: установление правил доступа к информации, определение ролей и прав пользователей.  
   *3. Физические методы защиты информации:  
   Физическая защита помещений и оборудования:* использование замков, систем контроля доступа, видеонаблюдения для обеспечения  
   физической безопасности информации.  
   *Защита от несанкционированного доступа к серверам и базам данных*: размещение серверов в защищенных помещениях, использование систем контроля доступа.