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. № 251003

Новиченко Н.С.

Дедов Н.Ю

Стельмах А.С.

Скрылёв И.А.

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 Кража: флешка может быть украдена и использована злоумышленником для доступа к конфиденциальной информации./Угроза конфиденциальности | Потеря конфиденциальных данных, таких как личные данные, бизнес-информация, пароли и т.д. Нарушение конфиденциальности и безопасности информации. Возможное использование украденной информации для мошенничества или других вредоносных целей. Утечка чувствительных данных, что может привести к финансовым потерям или нарушению законодательства о защите данных. | Ущерб может быть значительным, так как потеря конфиденциальных данных может нанести серьезный урон как личностной сфере, так и бизнесу. | Шифрование данных на флешке. Установка пароля доступа к флешке. Ограничение физического доступа к флешке. Удаленное управление или стирание данных в случае утери флешки./техничесие | Использование криптографических методов шифрования данных на флешке. Установка пароля доступа к флешке для предотвращения несанкционированного доступа к данным. Шифрование файлов и папок на флешке для дополнительной защиты. Удаленное управление флешкой через специализированные программы для удаленного стирания данных в случае потери или кражи. |
| 1.2 Вредоносное ПО: злоумышленник может вставить флешку с вредоносным программным обеспечением, которое может повредить данные на компьютере./Угроза доступности, угроза целостности | Потеря конфиденциальных данных, таких как личные данные, финансовая информация, пароли и т.д. Вред для компьютера или других устройств, на которых будет использоваться зараженная флешка. Распространение вредоносного ПО на другие устройства, если флешка подключается к другим компьютерам. Удаленное управление зараженным устройством или утечка чувствительных данных. | Ущерб может быть серьезным, так как вредоносное ПО может привести к потере данных, утечке конфиденциальной информации, финансовым потерям, а также к угрозам безопасности и конфиденциальности. | Регулярная проверка флешек на наличие вредоносных программ. Использование антивирусного ПО для сканирования флешек перед их использованием. Ограничение доступа к флешкам из ненадежных источников. Обновление программного обеспечения на компьютерах для борьбы с известными уязвимостями. /технические | Использование антивирусного ПО с функцией сканирования и обнаружения вредоносных программ на флешках. Ограничение автозапуска программ с флешек. Шифрование данных на флешке для предотвращения несанкционированного доступа и изменения данных. Обучение пользователей о мерах безопасности при работе с внешними устройствами хранения данных. |
| 1.3 Утеря: если флешка потеряется, конфиденциальная информация на ней может попасть в чужие руки./угроза сохранности | Потеря конфиденциальных данных, таких как личные данные, бизнес-информация, финансовая информация, пароли и т.д. Нарушение конфиденциальности и безопасности информации. Возможное использование украденной информации для мошенничества, идентификационных целей или других вредоносных действий. Утечка чувствительных данных, что может привести к финансовым потерям, ущербу репутации и нарушению законодательства о защите данных. | Ущерб может быть значительным, так как потеря флешки с конфиденциальными данными может нанести серьезный урон как личностной сфере, так и бизнесу. Возможно, что утерянная флешка может быть использована для несанкционированного доступа к данным и информации на ней. | Шифрование данных на флешке для предотвращения несанкционированного доступа к ним. Установка пароля доступа к флешке для предотвращения доступа к данным. Ограничение физического доступа к флешке, например, хранение в безопасном месте. Регулярное резервное копирование данных с флешки на другие носители./правовое | Использование криптографических методов шифрования данных на флешке. Установка пароля доступа к флешке для предотвращения несанкционированного доступа к данным. Хранение флешки в безопасном месте или использование защищенного контейнера для хранения. Регулярное выполнение резервного копирования данных с флешки на другие носители для минимизации потерь в случае ее утери. |
| 1.4 Несанкционированный доступ: если кто-то получит доступ к флешке без разрешения, это может привести к утечке конфиденциальных данных./угроза конфиденциальности | Кража конфиденциальных данных, таких как личные данные, финансовая информация, пароли и т.д. Нарушение конфиденциальности и безопасности информации. Возможное использование украденной информации для мошенничества, идентификационных целей или других вредоносных действий. Утечка чувствительных данных, что может привести к финансовым потерям, ущербу репутации и нарушению законодательства о защите данных. | Ущерб может быть серьезным, так как несанкционированный доступ к флешке может привести к утрате конфиденциальных данных, финансовым потерям, ущербу репутации и нарушению законодательства о защите данных. Возможно, что украденная информация будет использована для вредоносных целей. | Установка пароля доступа к флешке для предотвращения несанкционированного доступа к данным. Шифрование данных на флешке для защиты информации от несанкционированного просмотра. Ограничение физического доступа к флешке, например, хранение в безопасном месте. Запрет автозапуска программ с флешки для предотвращения запуска вредоносного ПО./техническое | Использование пароля доступа или биометрической аутентификации для разблокировки флешки. Шифрование данных на флешке с использованием надежных алгоритмов шифрования. Регулярное обновление антивирусного ПО для обнаружения вредоносных программ на флешке. Обучение пользователей о мерах безопасности при использовании флешек и о рисках несанкционированного доступа. |
| 1.5 Физические повреждения: флешка может быть случайно повреждена или испорчена, что приведет к потере данных./угроза целостности | Потеря доступа к данным, хранимым на флешке. Уничтожение информации, хранящейся на флешке. Невозможность использования флешки для передачи или хранения данных. Повреждение флешки может привести к потере ценных данных, включая фотографии, документы, видео и другие файлы. | Ущерб может быть значительным, так как физические повреждения флешки могут привести к потере данных, финансовым потерям (если данные невозможно восстановить), а также к неудобствам и временным затратам на восстановление данных или замену флешки. | Хранение флешки в защищенном кейсе или контейнере для предотвращения повреждений при падениях или ударам. Избегание экстремальных температурных условий, таких как перегрев или переохлаждение, которые могут повредить флешку. Осторожное обращение с флешкой, чтобы избежать физических повреждений./техническое | Использование защитного чехла или кейса для флешки. Регулярная проверка флешки на наличие физических повреждений. Резервное копирование данных с флешки на другие носители для предотвращения потери данных в случае повреждения флешки. Проведение профилактического обслуживания флешки, такого как очистка контактов и проверка целостности корпуса. |

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 ПО: компьютер может заразиться вирусами, троянами, шпионскими программами и другим вредоносным ПО через интернет./угроза целостности, угроза доступности | Возможные негативные последствия: потеря личных данных, финансовые потери, нанесение ущерба репутации, утрата доступа к компьютеру или данным. | Ущерб: приемлем, так как вредоносное ПО может привести к серьезным последствиям для пользователя и его данных. | Метод защиты: использование антивирусного программного обеспечения, брандмауэра и регулярное обновление программ и операционной системы./техническое | Средство защиты или мероприятие: установка надежного антивирусного программного обеспечения, настройка брандмауэра для блокировки вредоносных соединений, обновление программ и операционной системы для закрытия уязвимостей. |
| 2.2 Фишинг: злоумышленники могут отправить фальшивые электронные письма или создать поддельные веб-сайты для кражи личной информации пользователя./угроза конфиденциальности | Возможные негативные последствия: кража личных данных (логины, пароли, финансовая информация), доступ к банковским счетам, идентификационной информации. | Ущерб: приемлем, так как утрата личных данных и доступ к финансовым средствам может привести к серьезным финансовым потерям и угрозе для личной безопасности. | Метод защиты: обучение пользователей о методах фишинга, использование двухфакторной аутентификации, проверка подлинности веб-сайтов перед вводом личных данных./техническое | Средство защиты или мероприятие: обучение сотрудников о методах фишинга и как их избегать, использование антивирусного программного обеспечения с функцией анти-фишинга, аккуратность при открытии электронных писем и переходе по ссылкам. |
| 2.3 Сетевые атаки: компьютер на столе может стать целью хакеров, которые могут попытаться проникнуть в систему через открытые порты или слабые пароли./угроза сохранности | Возможные негативные последствия: физическое повреждение компьютера, потеря данных, нарушение работы устройства. | Ущерб: приемлем, так как физическое повреждение компьютера может привести к потере данных и недоступности устройства для работы. | Метод защиты: размещение компьютера в безопасном месте, использование защитных кожухов или кейсов./техническое | Средство защиты или мероприятие: установка системы видеонаблюдения для контроля доступа к компьютеру, использование кабельных замков для фиксации устройства, обучение сотрудников о правилах обращения с компьютерным оборудованием. |
| 2.4 Утечка данных: если компьютер не защищен должным образом, конфиденциальная информация может быть украдена или скомпрометирована./угроза конфиденциальности, угроза сохранности | Возможные негативные последствия: утечка конфиденциальных данных, нарушение приватности пользователей, угроза безопасности информации. | Ущерб: приемлем, так как утечка конфиденциальных данных может привести к серьезным последствиям, включая финансовые потери и утрату доверия клиентов. | Метод защиты: использование сильных паролей, шифрование данных, обновление программного обеспечения./техническое | Средство защиты или мероприятие: регулярное обучение сотрудников по правилам безопасности информации, установка антивирусного программного обеспечения, использование механизмов двухфакторной аутентификации. |
| 2.5 Недостаточная защита: отсутствие антивирусного программного обеспечения, брандмауэра или обновлений безопасности может сделать компьютер уязвимым для различных угроз./угроза сохранности | Возможные негативные последствия: заражение компьютера вредоносным программным обеспечением (вирусами, троянами, шпионскими программами), утеря данных, утечка конфиденциальной информации. | Ущерб: приемлем, так как потеря данных и утечка конфиденциальной информации могут привести к финансовым потерям и нарушению приватности. | Метод защиты: установка антивирусного программного обеспечения, регулярное обновление операционной системы и программ, ограничение доступа к недоверенным сайтам и файлам./организационные | Средство защиты или мероприятие: использование брандмауэра для блокировки нежелательного трафика, обучение пользователей правилам безопасности в сети, регулярное резервное копирование данных. |

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 | Фишинг: атака, при которой злоумышленники маскируются под доверенные организации или лица, чтобы получить конфиденциальную информацию, такую как номер банковской карты, срок действия и CVV-код./угроза конфиденциальности, угроза сохранности | Возможные негативные последствия вследствие реализации угрозы: Потеря конфиденциальной информации, включая данные банковских карт, возможные финансовые потери, риск идентификации и мошенничества. | Ущерб: Высокий уровень ущерба, так как кража данных банковских карт может привести к финансовым потерям и потере доверия клиентов. Неприемлемо. | Метод защиты: Повышение осведомленности сотрудников и клиентов о методах фишинга, использование антивирусного программного обеспечения, обновление программного обеспечения и мониторинг подозрительной активности./организационные | Средство защиты или мероприятие: Обучение сотрудников о методах фишинга, двухфакторная аутентификация, использование защищенных каналов связи для обмена конфиденциальной информацией, регулярные аудиты безопасности. |
| 3.2 Кибератаки на платежные системы: злоумышленники могут использовать вредоносное программное обеспечение для взлома платежных систем и получения доступа к данным банковских карт./угроза сохранности, угроза конфиденциальности | Возможные негативные последствия вследствие реализации угрозы: Потеря конфиденциальной информации, нарушение работы систем, утечка чувствительных данных, нарушение репутации компании, финансовые потери, прерывание бизнес-процессов. | Ущерб: Высокий уровень ущерба, так как кибератака может привести к серьезным последствиям для компании, включая финансовые потери, утрату доверия клиентов и партнеров, а также нарушение законодательства о защите данных. Неприемлемо. | Метод защиты: Регулярное обновление программного обеспечения, мониторинг сетевой активности, обучение сотрудников по вопросам кибербезопасности, создание плана реагирования на инциденты./правовые | Средство защиты или мероприятие: Установка средств защиты от вредоносного программного обеспечения (антивирусов, брандмауэров), использование механизмов шифрования данных, регулярные аудиты безопасности, создание резервных копий данных. |
| 3.3 Кража личных данных: злоумышленники могут взламывать базы данных банков или онлайн-сервисов для получения личной информации клиентов, включая данные банковских карт./угроза конфиденциальности, угроза сохранности | Возможные негативные последствия вследствие реализации угрозы: Потеря личной конфиденциальной информации, риск кражи идентификационных данных, возможное использование информации для мошенничества или кражи личности. | Ущерб: Высокий уровень ущерба, так как кража личных данных может привести к серьезным последствиям для человека, включая финансовые потери, нарушение приватности, утрату доверия к онлайн-сервисам и компаниям. Неприемлемо. | Метод защиты: Соблюдение мер безопасности при работе с личными данными, использование надежных паролей, ограничение доступа к личной информации, обучение по вопросам кибербезопасности./правовые | Средство защиты или мероприятие: Использование двухфакторной аутентификации, шифрование данных, регулярное обновление программного обеспечения, ограничение доступа к личной информации только необходимым лицам. |
| 3.4 Скимминг: злоумышленники могут устанавливать скиммеры на банкоматах или устройствах для оплаты, чтобы копировать данные с магнитной полосы банковских карт./ угроза сохранности, угроза конфиденциальности | - Возможные негативные последствия вследствие реализации угрозы: Потеря финансовых средств, раскрытие личной информации, риск стать жертвой мошенничества, потеря доверия к онлайн-сервисам. | Ущерб: Высокий уровень ущерба, так как скаммеры могут нанести серьезные финансовые потери и повредить репутацию пострадавшего. Неприемлемо | Метод защиты: Обучение по вопросам кибербезопасности, осознанное поведение при работе в интернете, проверка подлинности сайтов и сервисов перед предоставлением личной информации./организационные | Средство защиты или мероприятие: Использование антивирусного программного обеспечения, осторожность при открывании вложений в электронных письмах, никогда не предоставлять личные данные на ненадежных сайтах, использование безопасных способов оплаты. |
| 3.5 Несанкционированный доступ к онлайн-аккаунту: злоумышленники могут использовать слабые пароли или методы аутентификации для взлома онлайн-аккаунтов и получения доступа к информации о банковских картах./ угроза сохранности, угроза конфиденциальности | Возможные негативные последствия вследствие реализации угрозы: Потеря контроля над личными данными, утечка конфиденциальной информации, потеря доступа к важным онлайн-сервисам и ресурсам, возможные финансовые потери. | Ущерб: Высокий уровень ущерба, так как несанкционированный доступ к онлайн-аккаунту может привести к серьезным последствиям, включая кражу личных данных, финансовых средств и нарушение приватности. - | Метод защиты: Использование сильных и уникальных паролей для каждого онлайн-аккаунта, активация двухфакторной аутентификации, регулярное обновление паролей, осторожность при открытии подозрительных ссылок и вложений в электронных письмах. -/правовые | Средство защиты или мероприятие: Использование парольных менеджеров для хранения и генерации безопасных паролей, регулярная проверка активности в своих онлайн-аккаунтах, мониторинг подозрительной активности и немедленное реагирование на подозрительные события. |