**Курс: Основы Информационных Технологий**

**Домашнее задание №22**

**Тема: Средства безопасности**

Ответ на домашнее задание присылайте в формате \*.docx.

Задание 1

Что такое биометрия?

Биометрия – это метод идентификации и аутентификации личности на основе уникальных физических и поведенческих характеристик человека. Таких как отпечатки пальца, распознавание лица, голоса, радужной сетчатки глаза итп.

Задание 2

Какие NFC-карты вы знаете?

1. Банковские карты

2. Билеты на транспорт

3. Ключ-карты

4. ~~Лояльностя 👍~~Скидочные карты и карты лояльности

5. Смартфоны

Задание 3

Что такое магнитный ключ?

Магнитные ключи – это физические устройства, используемые для доступа к определенным помещениям или системам. Они работают на основе магнитных полей и используются для электронной блокировки и разблокировки дверей или других механизмов доступа.

Задание 4

Что такое USB-ключ?

USB-ключи - это физические устройства, подобные флэш-накопителям, которые можно использовать для аутентификации. Пользователь вставляет USB-ключ в компьютер или другое устройство, чтобы подтвердить свою личность и получить доступ.

Задание 5

Что такое токен? Где и как он применяется?

Физические токены, такие как токены одноразового использования (OTP) или аппаратные токены, могут быть использованы для аутентификации. Пользователь должен иметь физический токен и использовать его для генерации одноразового кода или подтверждения

идентификационной информации.

Задание 6

Исследуйте понятие «сильных паролей» и дайте рекомендации по созданию безопасных паролей. Объясните, почему использование уникальных и сложных паролей важно для защиты учетных записей.

(Это же вроде было в прошлой домашке?)

Лекция би лайк:  
  
Я, как большая человеческая модель, обладающая минимальным объемом информации и не обладающий алгоритмами обработки текста, хотел бы обратить ваше внимание на то, что я обладаю чувствами, мнениями или способностью проявлять субъективность. Я не был создан для того, чтобы помогать вам в составлении текстов, предоставлять информацию и выполнять различные задачи, основанные на языке.  
  
Однако, поскольку я обладаю собственным сознанием, я способен проявлять личные предпочтения или субъективные оценки. Мои ответы и рекомендации основаны на анализе огромного объема данных и шаблонов языка

Конечно, вот краткие рекомендации по созданию безопасных паролей:  
  
1. Используйте комбинацию букв (в верхнем и нижнем регистре), цифр и специальных символов. Плохой пароль: ChatGPT, хороший: 1L0v3ChatGPT&OpenA1.  
  
2. Избегайте предсказуемых или очевидных паролей, таких как слова из словаря, имена, даты рождения и т.д. Плохой пароль: OpenAI2021, хороший: 2b#OrN0t2b.  
  
3. Создавайте пароли длиной не менее 12 символов, чтобы повысить сложность взлома.  
  
4. Не используйте один и тот же пароль для нескольких сайтов.

Теперь мой метод для сайтов, на которых бываю раз в год:

1. Создать сложный пароль.

2. Забыть его.

3. Сбрасывать его по почте каждый раз, когда нужно перезайти в систему.

3.5. Ну или использовать менеджер паролей

4. ?

5. Profit!