Внешний курс. Раздел 2

Основы информационной безопасности

Малюга В. В.

8 марта 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Малюга Валерия Васильевна
- студентка группы НКАбд-04-23
- Российский университет дружбы народов
- https://github.com/vvmalyuga

Цель работы

Цель

Пройти второй блок курса **“Основы кибербезопасности”**,
а именно — изучить:

- шифрование данных на устройствах
- принципы безопасного хранения паролей
- методы фишинга
- виды вредоносного ПО
- сквозное шифрование в мессенджерах

Защита ПК и телефона

Шифрование диска

Шифрование диска — технология защиты информации,
переводящая данные в нечитаемый код.
Это не позволяет посторонним получить доступ к содержимому.

Иллюстрация: шифрование диска

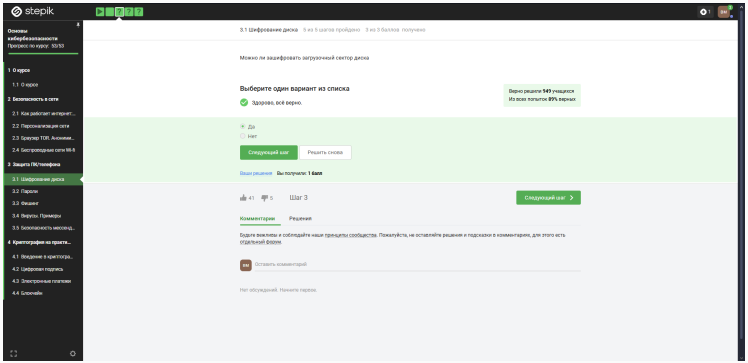

Рис. 1: Шифрование диска

Тип шифрования

Шифрование часто основано на **симметричном методе**,
когда для шифрования и дешифрования используется один и тот же ключ.

Иллюстрация: симметричное шифрование

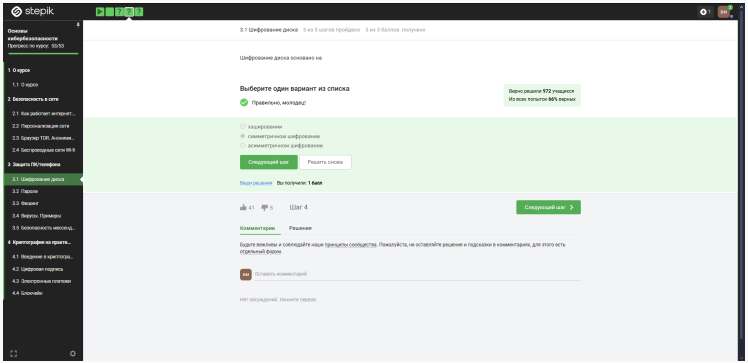

Рис. 2: Тип шифрования

Программы шифрования

Примеры программ: BitLocker, FileVault, VeraCrypt и другие.

Они позволяют настроить полное или частичное шифрование данных.

Иллюстрация: программы для шифрования

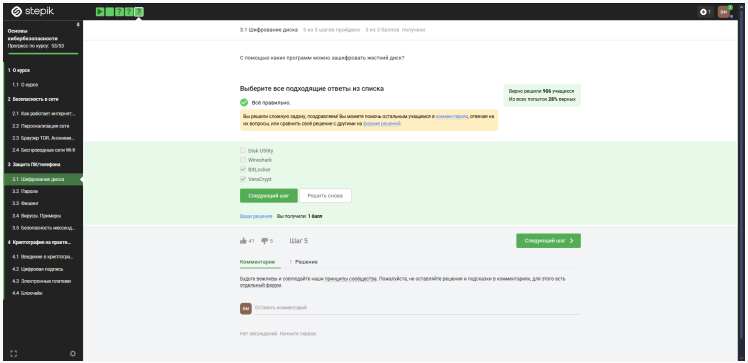

Рис. 3: Программы

Пароли

Надежный пароль

Стойкий пароль — длинный, содержит специальные символы и не основан на личной информации. Его сложно подобрать.

Иллюстрация: стойкость пароля

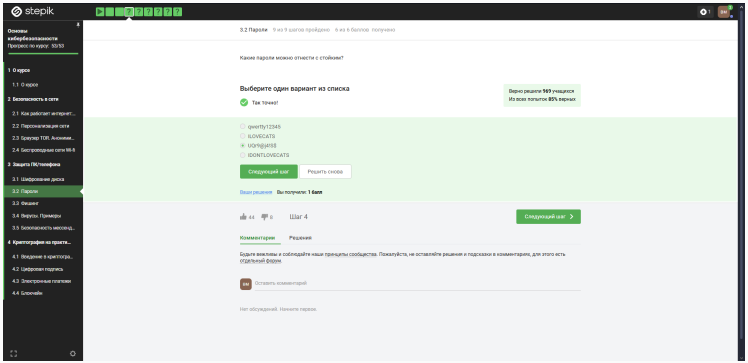

Рис. 4: Надежный пароль

Надёжное хранение

Менеджеры паролей — единственный по-настоящему безопасный способ хранения.

Другие методы (запись на бумаге, в блокноте и т.д.) ненадежны.

Иллюстрация: ненадежные способы

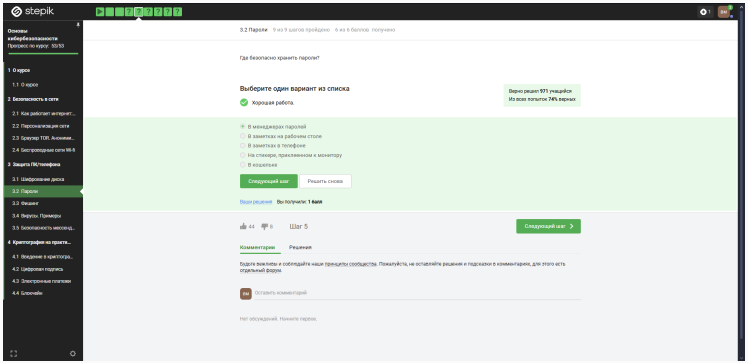

Рис. 5: Ненадежное хранение

CAPTCHA

Капча используется для определения,
что перед устройством — человек, а не бот.

Иллюстрация: капча

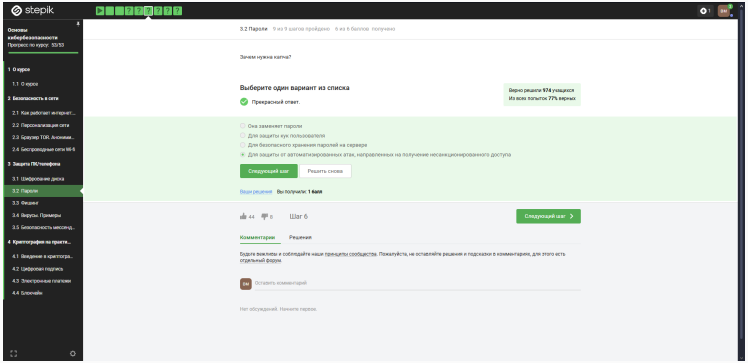

Рис. 6: CAPTCHA

Хеширование паролей

Пароли не хранятся в открытом виде.

Используются хеш-функции, которые необратимо шифруют данные.

Иллюстрация: хеширование

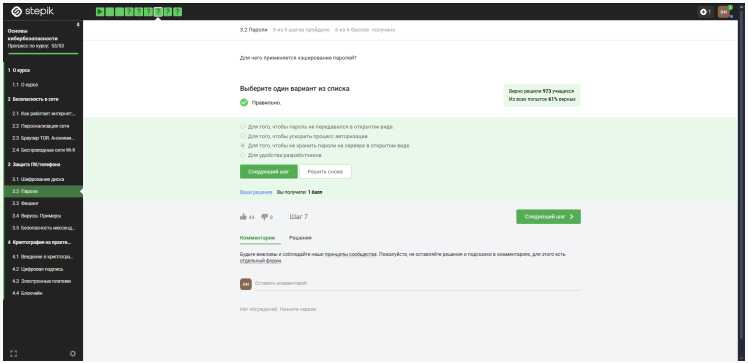

Рис. 7: Хеши паролей

Использование соли

Добавление соли в хеш-функции повышает безопасность.

Однако это не единственная мера, необходима комплексная защита.

Иллюстрация: соль

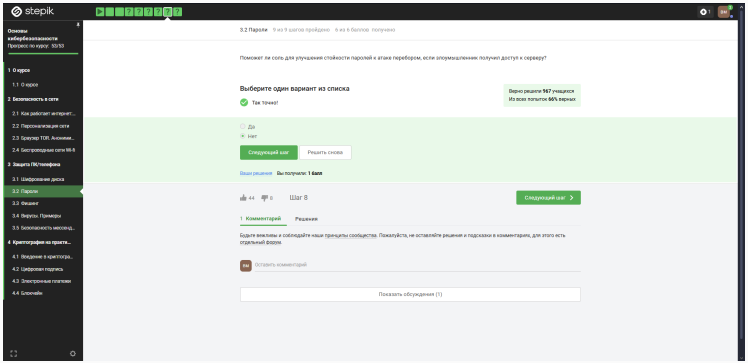

Рис. 8: Про соль

Комплексная защита

Все меры безопасности должны использоваться вместе:
хеширование, соль, шифрование и менеджеры паролей.

Иллюстрация: меры защиты

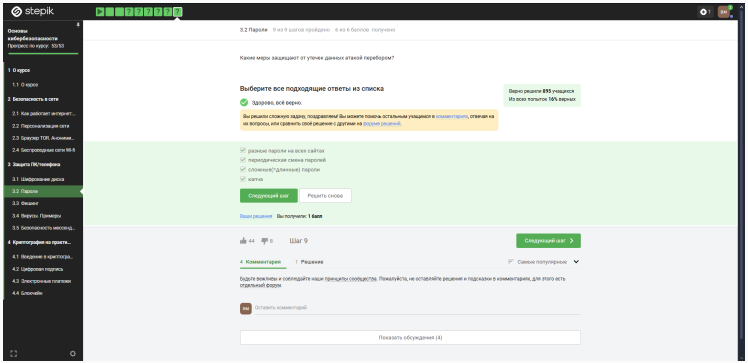

Рис. 9: Меры защиты

Фишинг

Ссылки

Фишинговые ссылки подделываются под настоящие,
но содержат небольшие отличия.

Иллюстрация: фишинговые ссылки

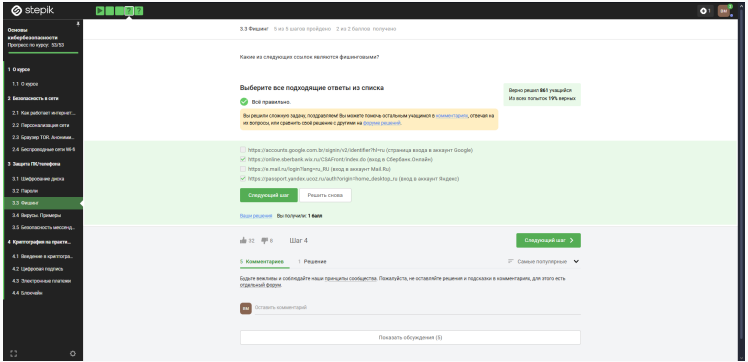

Рис. 10: Ссылки

От кого приходит фишинг

Фишинговое письмо может прийти даже от знакомого — если его аккаунт взломан.

Иллюстрация: фишинг от знакомого

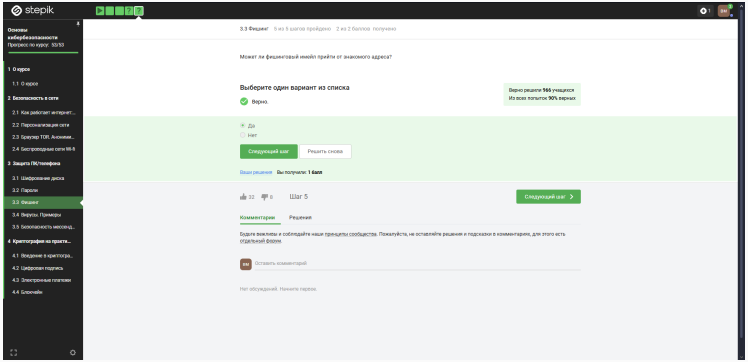

Рис. 11: Фишинг от знакомого

Вредоносное ПО

Вирусы

Вирусы — это вредоносные программы,
цель которых — нанести ущерб пользователю.

Иллюстрация: вирус

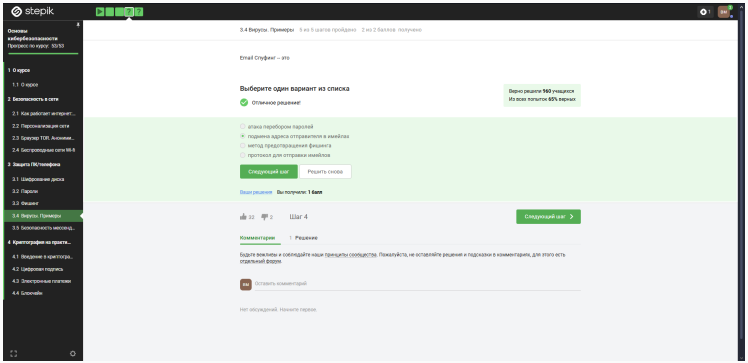

Рис. 12: Тип вируса

Троян

Троян — вредоносная программа,
маскирующаяся под легальное ПО.

Иллюстрация: троян

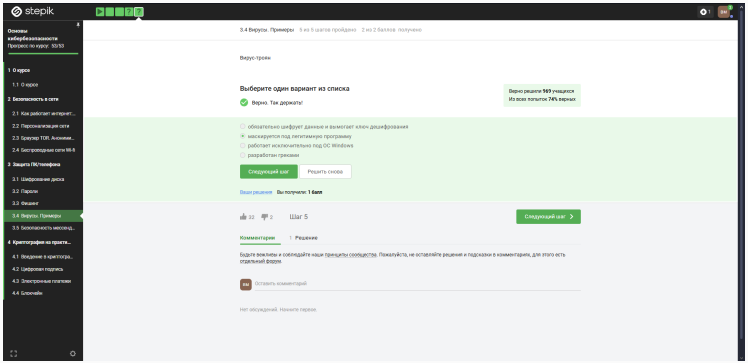

Рис. 13: Троян

Безопасность мессенджеров

Обмен ключами

При первом сообщении между пользователями происходит обмен ключами шифрования.

Иллюстрация: формирование ключа

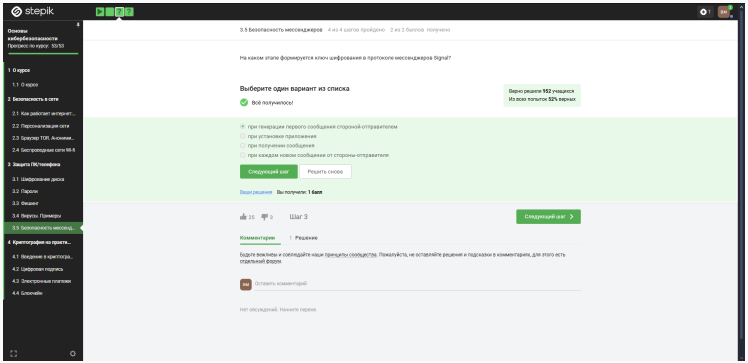

Рис. 14: Формирование ключа

Сквозное шифрование

Сообщения шифруются на стороне отправителя
и расшифровываются только получателем.

Иллюстрация: сквозное шифрование

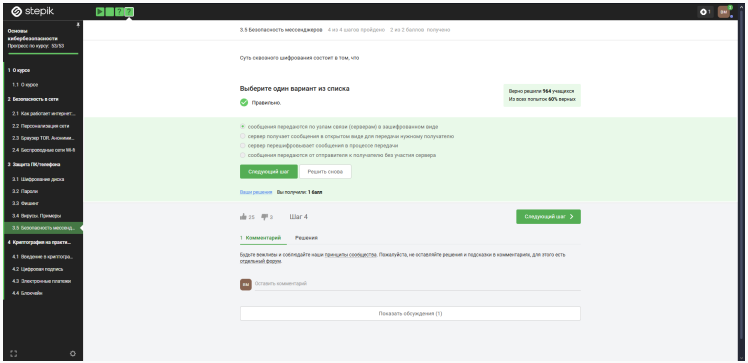

Рис. 15: Сквозное шифрование

Выводы

Выводы

- Изучены методы шифрования и защиты устройств
- Рассмотрены надежные способы хранения паролей