Внешний курс раздел 2

Защита ПК/телефона

Александр Андреевич Шуплецов

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить основы защиты данных ПК/телефона.

2 Выполнение работы

1. Загрузочный сектор диска, как и другие сектора диска, можно зашифровать.

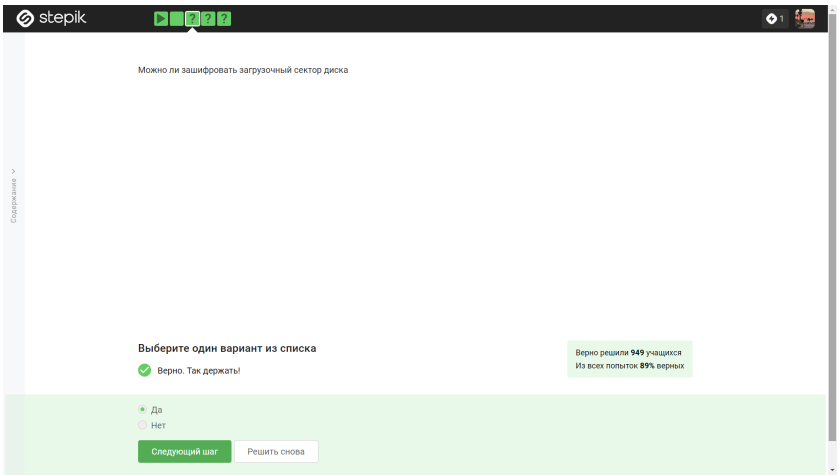

Рис. 2.1: первое задание

2. Шифрование диска основано на симметричном шифровании, как правило на алгоритме AES.

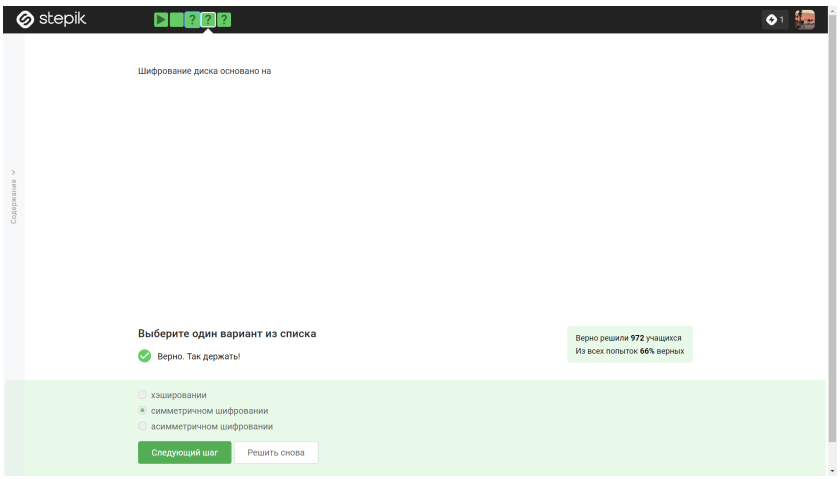

Рис. 2.2: второе задание

3. VeraCrypt и BitLocker - примеры программ, с помощью которых можно зашифровать жесткий диск.

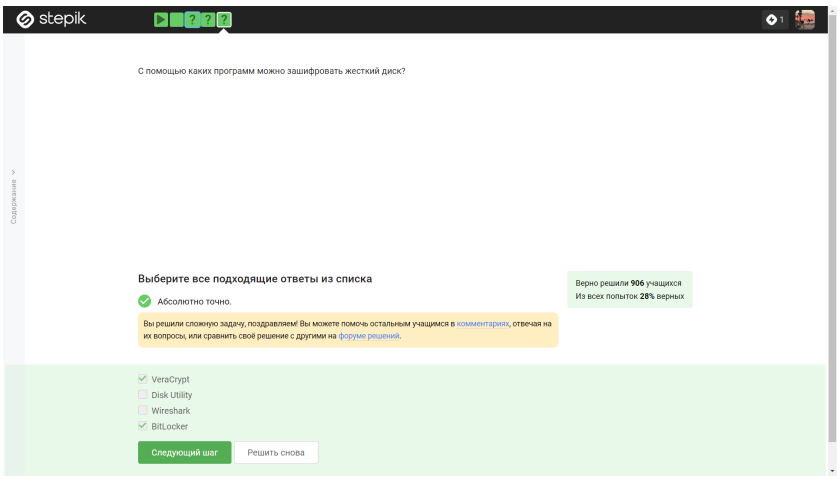

Рис. 2.3: третье задание

4. К стойким паролям обычно относят пароли, содержащие большие и маленькие буквы алфавита, цифры, специальные символы, не имеющие реальной смысловой нагрузки, выберем такой пароль из списка.

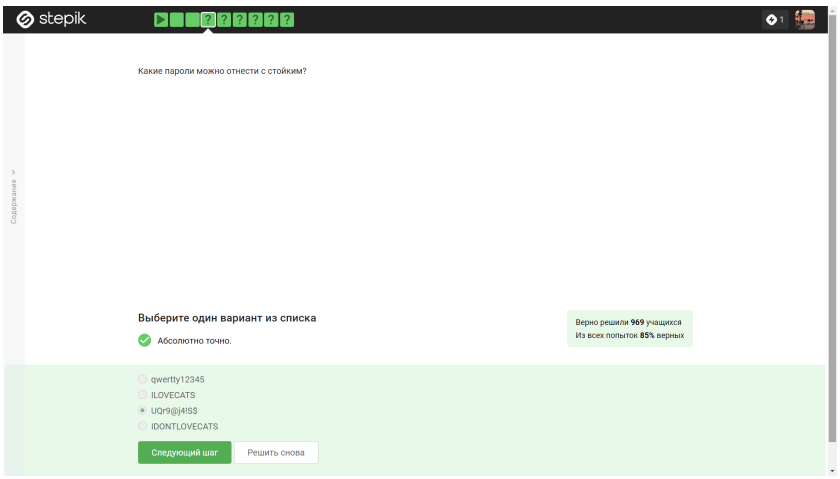

Рис. 2.4: четвертое задание

5. Менеджеры паролей являются самым безопасным методом хранения паролей.

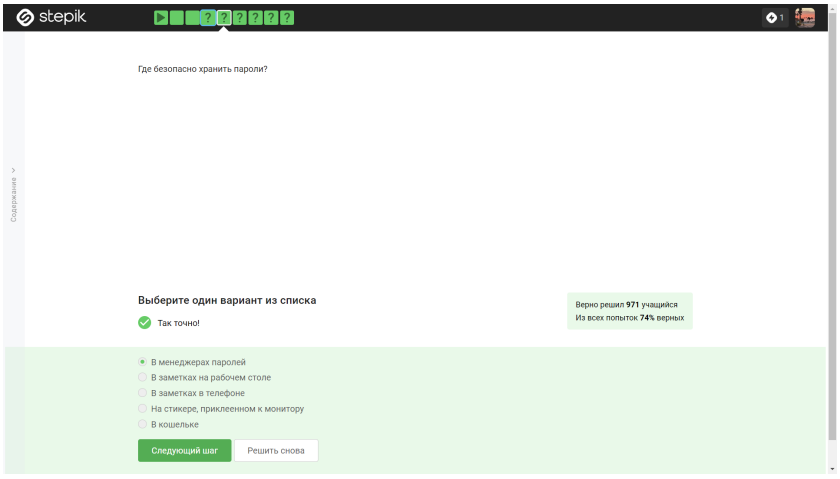

Рис. 2.5: пятое задание

6. Капча нужна для защиты от автоматизированных атак, направленных на получение несанкционированного доступа, она не используется для замены паролей, защиты кук пользователя, безопасного хранения паролей на сервере.

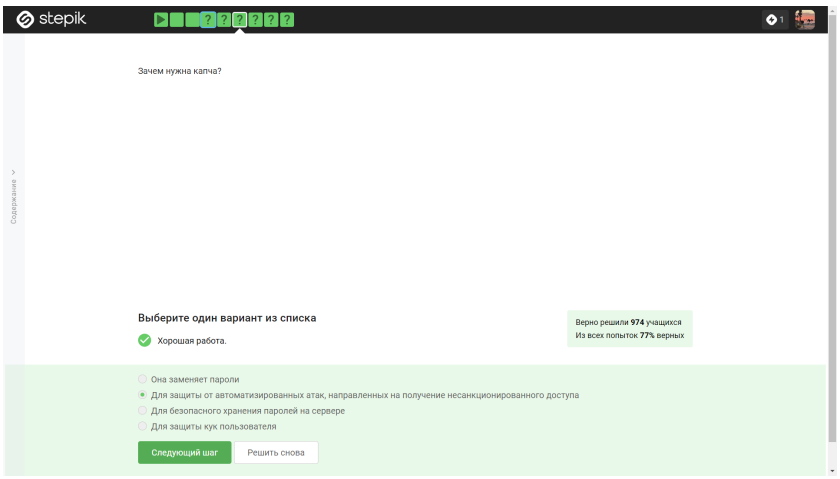

Рис. 2.6: шестое задание

7. Хэширование паролей нужно для того, чтобы не хранить пароли на сервере в открытом виде, для конфиденциальности паролей пользователей.

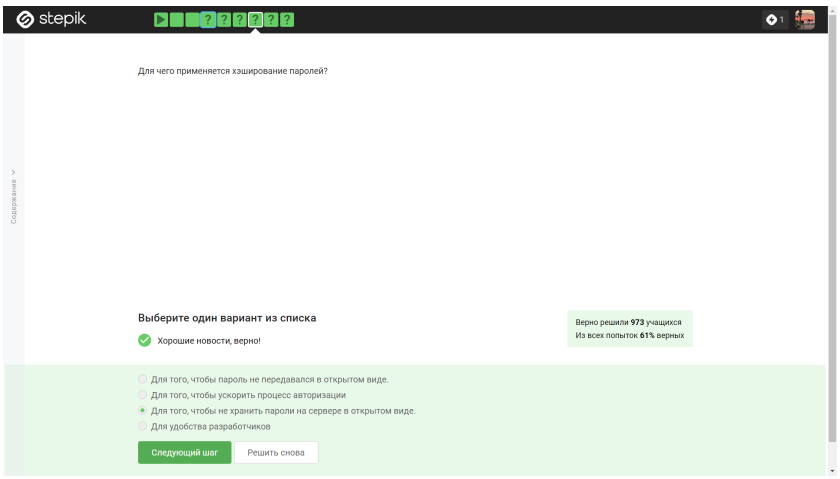

Рис. 2.7: седьмое задание

8. Соль для улучшения стойкости паролей не поможет, если злоумышленник получил доступ к серверу, так как она хранится на сервере.

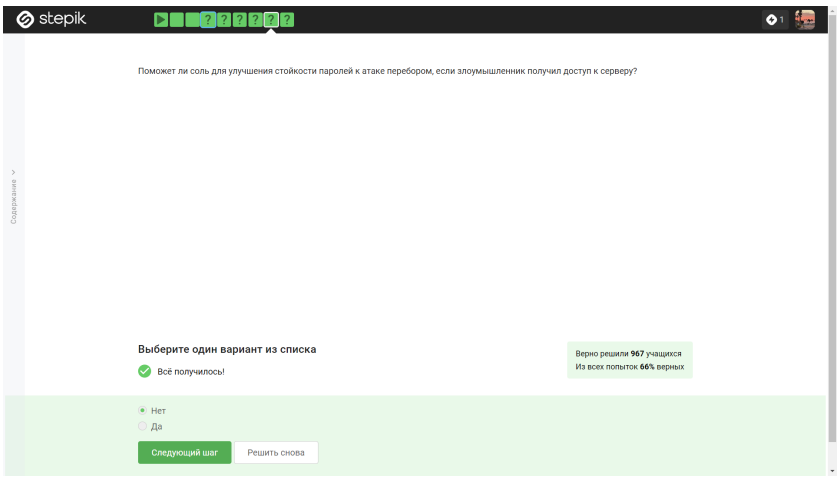

Рис. 2.8: восьмое задание

9. Разные пароли на всех сайтах, периодическая смена паролей, сложные пароли, капча защищают от утечек данных атакой перебором.

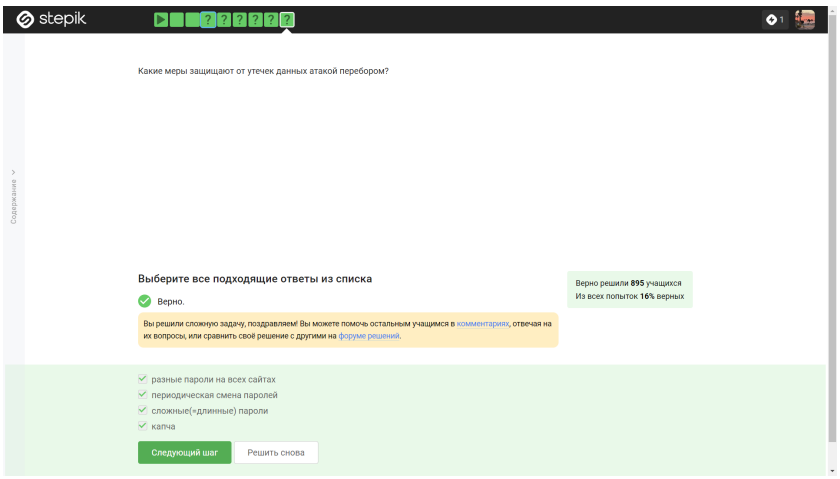

Рис. 2.9: девятое задание

10. Среди представленных ссылок, ссылка для входа в сбербанк и для входа в яндекс являются фишинговыми, так как не имеют никакого отношения к сбербанку и яндексу соответственно.

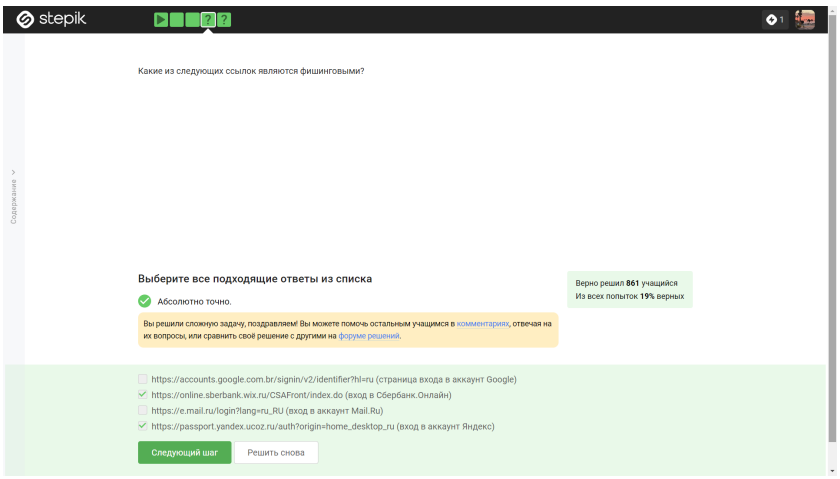

Рис. 2.10: десятое задание

11. Фишинговый имейл может прийти от знакомого адреса, этот вид фишинга называется спуфинг.

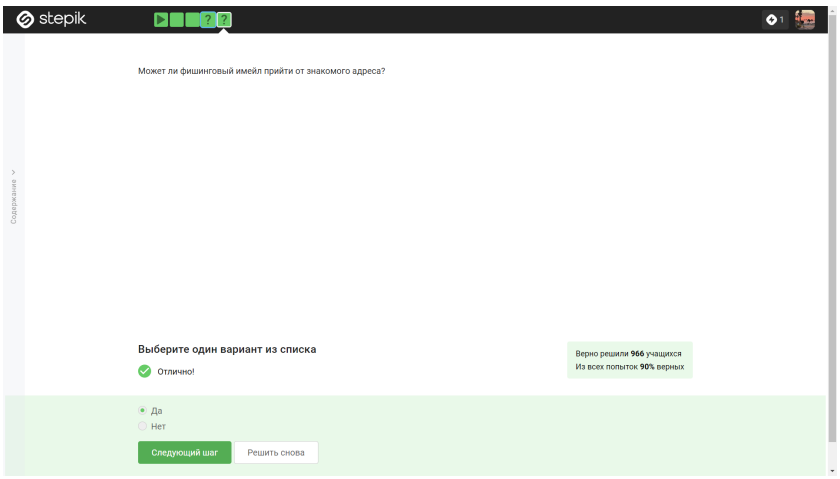

Рис. 2.11: одиннадцатое задание

12. Спуфинг - это подмена адреса отправителя в имейлах, вид фишинга.

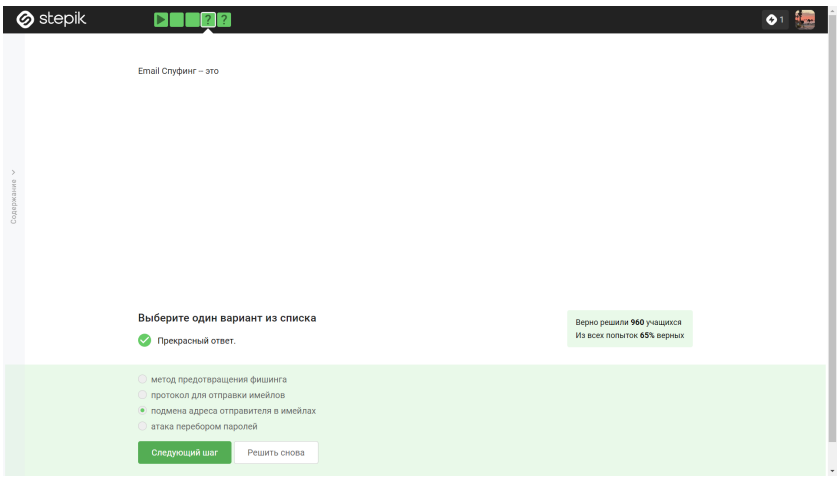

Рис. 2.12: двенадцатое задание

13. Вирус-троян маскируется под легитимную программу, при этом содержа в себе вредоносное ПО.

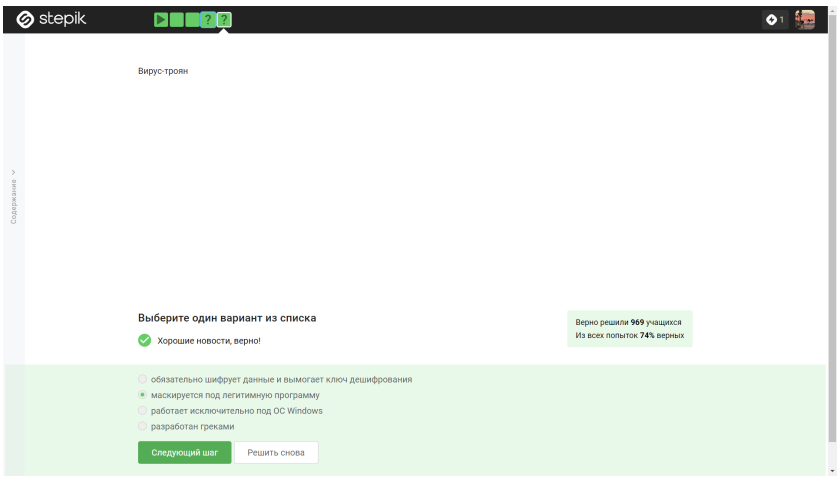

Рис. 2.13: тринадцатое задание

14. В протоколе мессенджеров Signal ключ шифрования формируется при генерации первого сообщения стороной-отправителем.

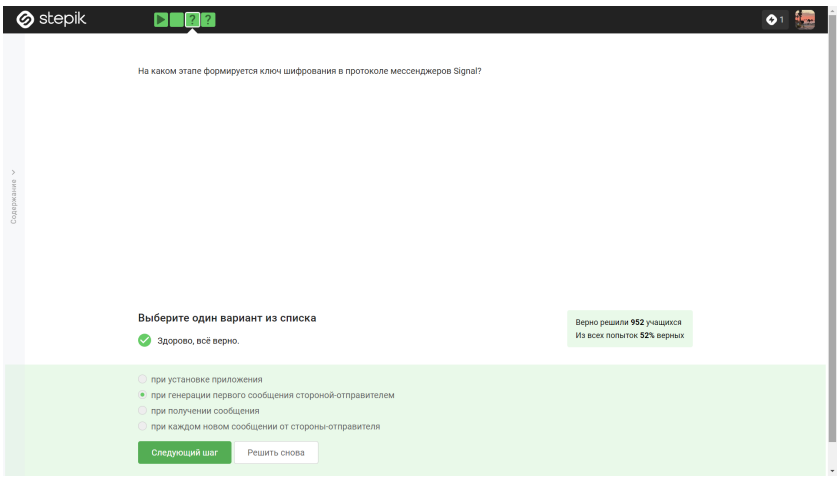

Рис. 2.14: четырнадцатое задание

15. Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде.

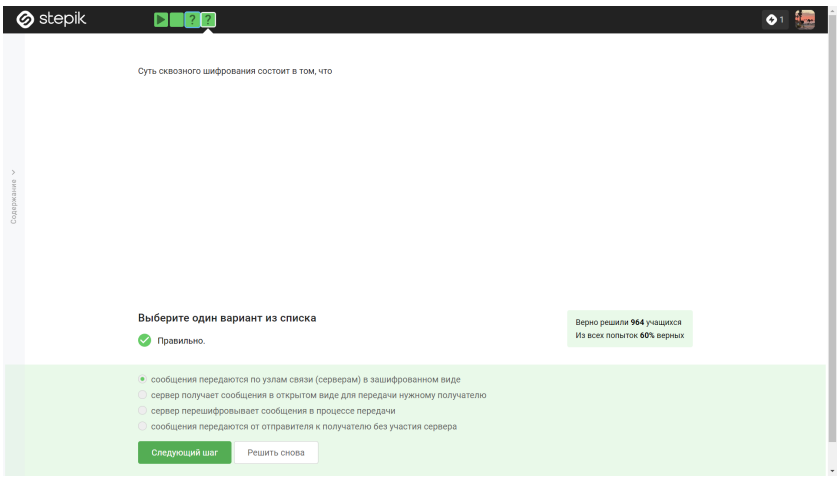

Рис. 2.15: пятнадцатое задание

3 Выводы

Я изучил основы защиты данных ПК/телефона.

4 Список литературы

Конспекты к лекциям курса “Основы кибербезопасности”.