Отчет по части “Защита ПК/телефона” курса “Основы кибербезопасности”

Стариков Данила Андреевич

Содержание

# 1 Цель работы

Познакомиться со следующими понятиями: - Шифрование диска - Пароли, хранилища паролей - Защита от вирусов - Фишинг - Безопасность мессенджеров

# 2 Выполнение лабораторной работы

## 2.1 Шифрование диска

* Вопрос 1. Можно ли зашифровать загрузочный сектор диска(рис. 1)

Ответ: *Да*.

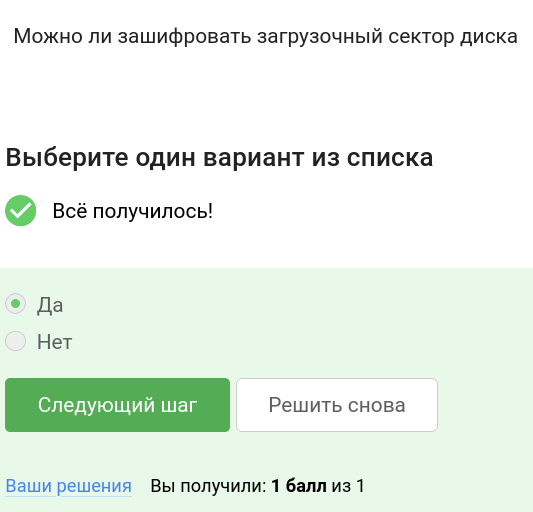


Рис. 1: Скриншот выполнения задания

* Вопрос 2. Шифрование диска основано на(рис. 2)

Ответ: *симметричном шифровании*.

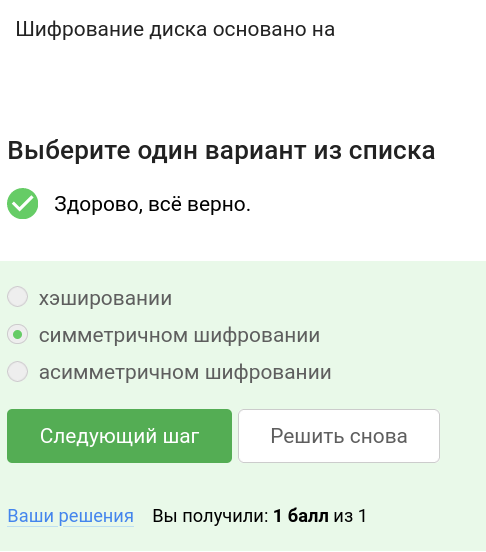


Рис. 2: Скриншот выполнения задания

* Вопрос 3. С помощью каких программ можно зашифровать жесткий диск?(рис. 3)

Ответ: *BitLocker и VeraCrypt*.

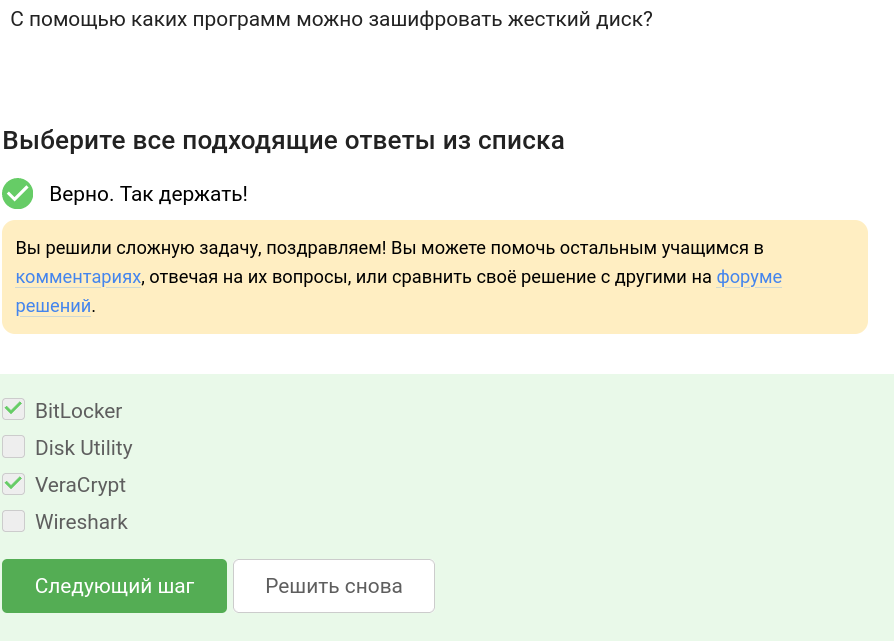


Рис. 3: Скриншот выполнения задания

## 2.2 Пароли

* Вопрос 1. Какие пароли можно отнести с стойким?(рис. 4)

Ответ: *UQr9@j4!S$*.

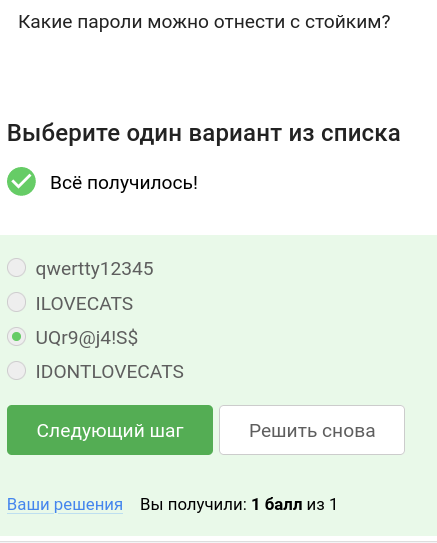


Рис. 4: Скриншот выполнения задания

* Вопрос 2. Где безопасно хранить пароли?(рис. 5)

Ответ: *В менеджерах паролей*.

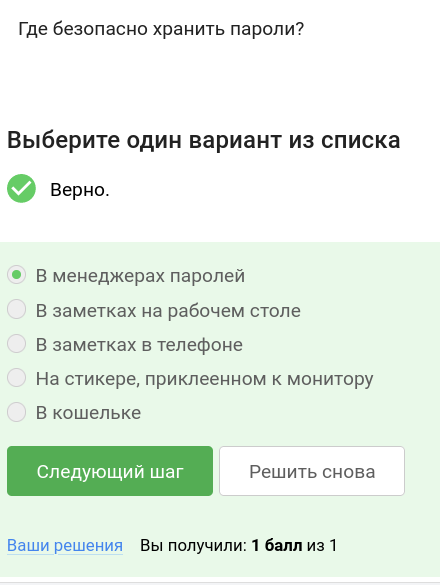


Рис. 5: Скриншот выполнения задания

* Вопрос 3. Зачем нужна капча?(рис. 6)

Ответ: *Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа*.

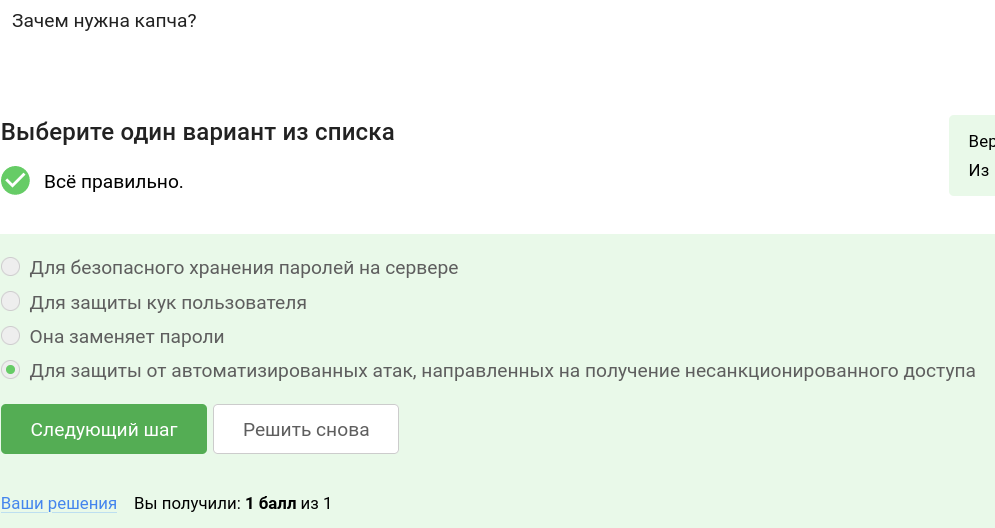


Рис. 6: Скриншот выполнения задания

* Вопрос 4. Для чего применяется хэширование паролей?(рис. 7)

Ответ: *Для того, чтобы не хранить пароли на сервере в открытом виде.*.

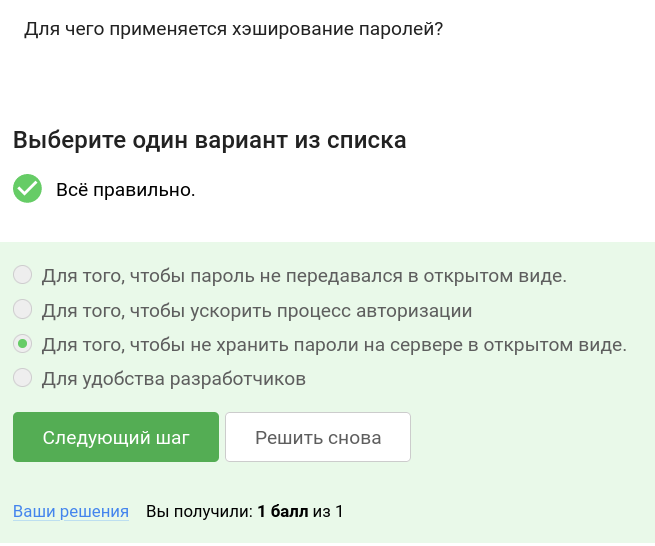


Рис. 7: Скриншот выполнения задания

* Вопрос 5. Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?(рис. 8)

Ответ: *Нет*.

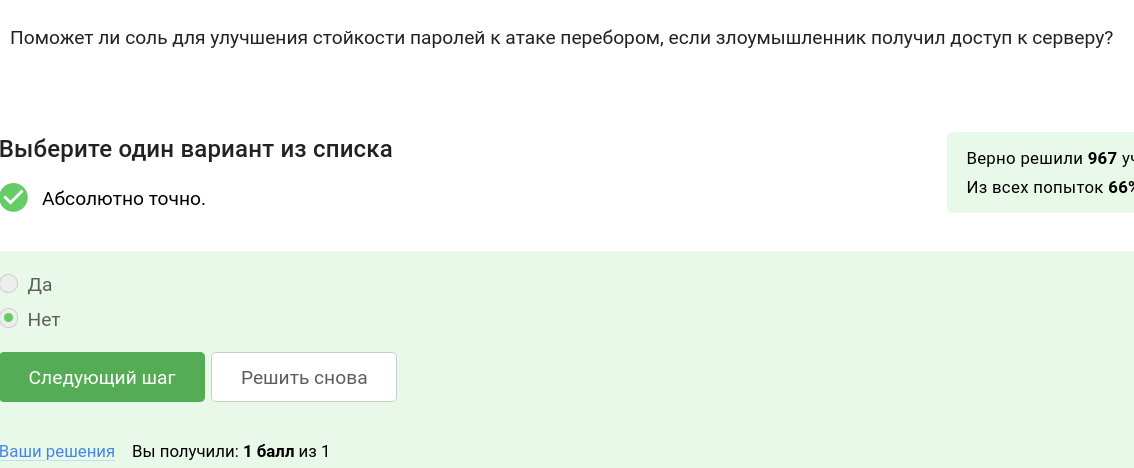


Рис. 8: Скриншот выполнения задания

* Вопрос 6. Какие меры защищают от утечек данных атакой перебором?(рис. 9)

Ответ: *разные пароли на всех сайтах, периодическая смена паролей, сложные(=длинные) пароли, капча*.

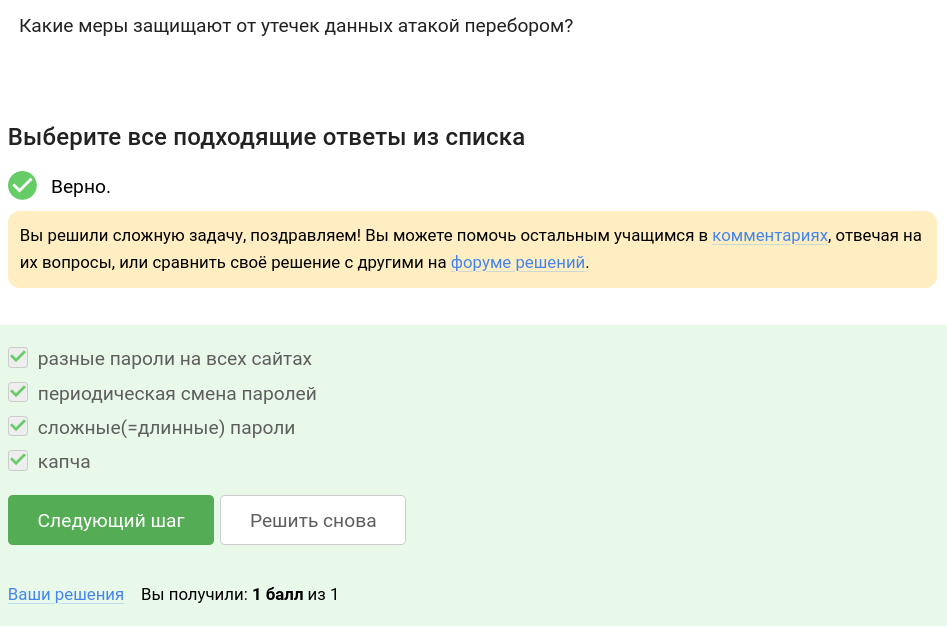


Рис. 9: Скриншот выполнения задания

## 2.3 Фишинг

* Вопрос 1. Какие из следующих ссылок являются фишинговыми?(рис. 10)

Ответ: *https://online.sberbank.wix.ru/CSAFront/index.do (вход в Сбербанк.Онлайн) и https://passport.yandex.ucoz.ru/auth?origin=home\_desktop\_ru (вход в аккаунт Яндекс)*.

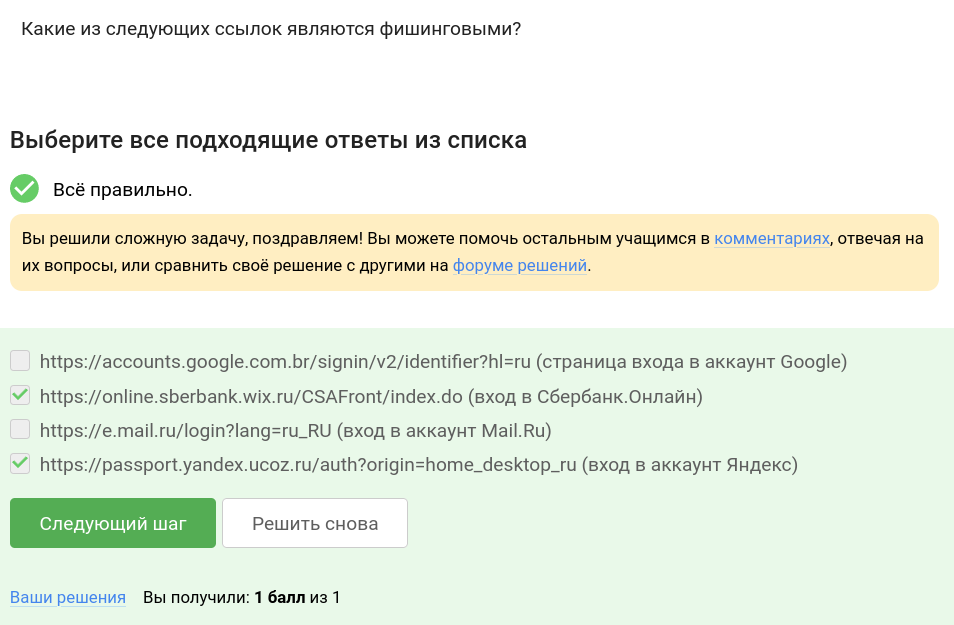


Рис. 10: Скриншот выполнения задания

* Вопрос 2. Может ли фишинговый имейл прийти от знакомого адреса?(рис. 11)

Ответ: *Да*.

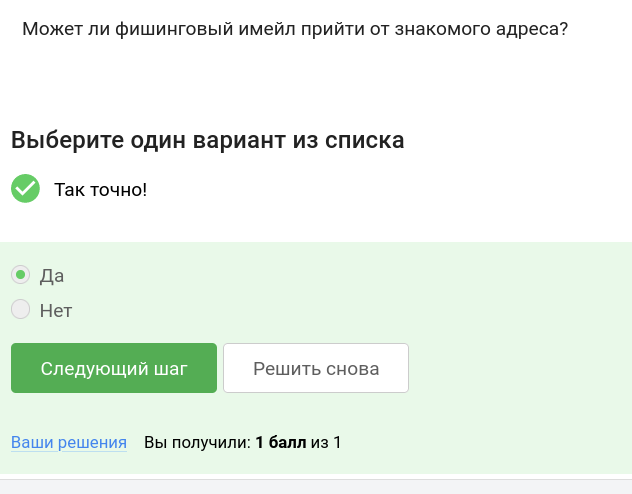


Рис. 11: Скриншот выполнения задания

## 2.4 Вирусы. Примеры

* Вопрос 1. Email Спуфинг – это(рис. 12)

Ответ: *подмена адреса отправителя в имейлах*.

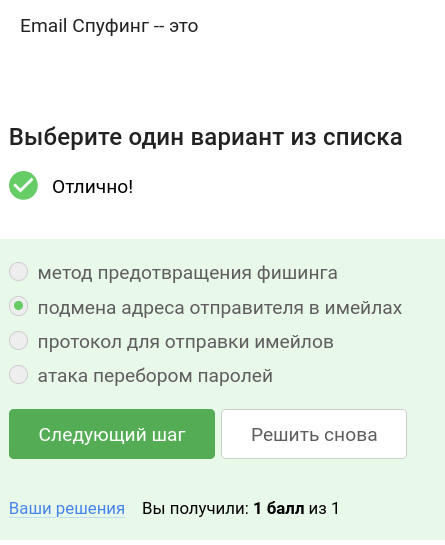


Рис. 12: Скриншот выполнения задания

* Вопрос 2. Вирус-троян(рис. 13)

Ответ: *маскируется под легитимную программу*.

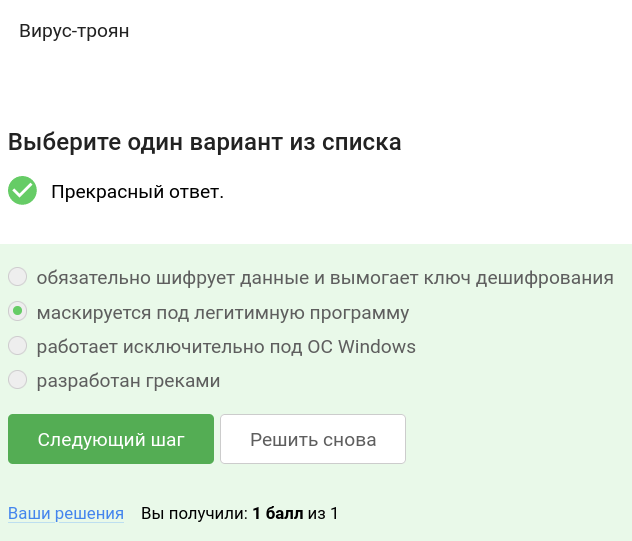


Рис. 13: Скриншот выполнения задания

## 2.5 Безопасность мессенджеров

* Вопрос 1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?(рис. 14)

Ответ: *при генерации первого сообщения стороной-отправителем*.

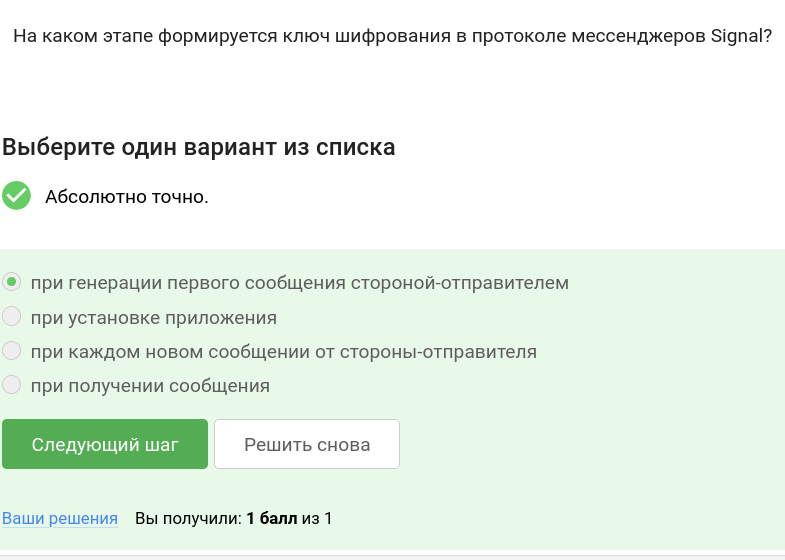


Рис. 14: Скриншот выполнения задания

* Вопрос 2. Суть сквозного шифрования состоит в том, что(рис. 15)

Ответ: *сообщения передаются по узлам связи (серверам) в зашифрованном виде*.

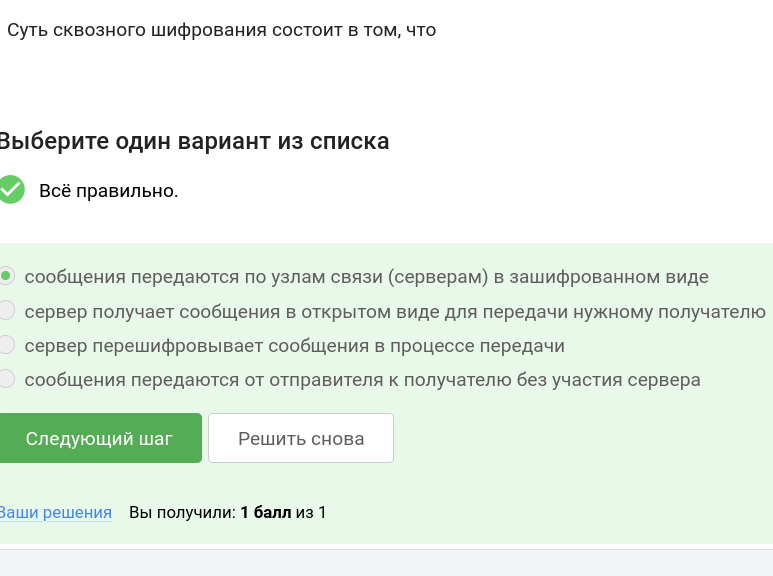


Рис. 15: Скриншот выполнения задания

# 3 Выводы

В рамках второго модуля познакомились с основами защиты ПК и смартфона: шифрование диска, пароли и их хранилища, защита от вирусов, фишинг, безопасность мессенджеров.