Внешний курс. Блок 2: Защита ПК/Телефона

Дисциплина: Основы информационной безопасности

Ибатулина Дарья Эдуардовна, НКАбд-01-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Пройти второй блок курса “Основы кибербезопасности”, выполнить контрольные задания к блоку.

2 Выполнение блока 2: Защита ПК/Телефона

2.1 Шифрование диска

Шифровать можно не только жесткий диск, где мы храним файлы, можно шифровать и загрузочный сектор диска. И для этого есть алгоритмы шифрования. Ответ - можно (рис. [2.1]).

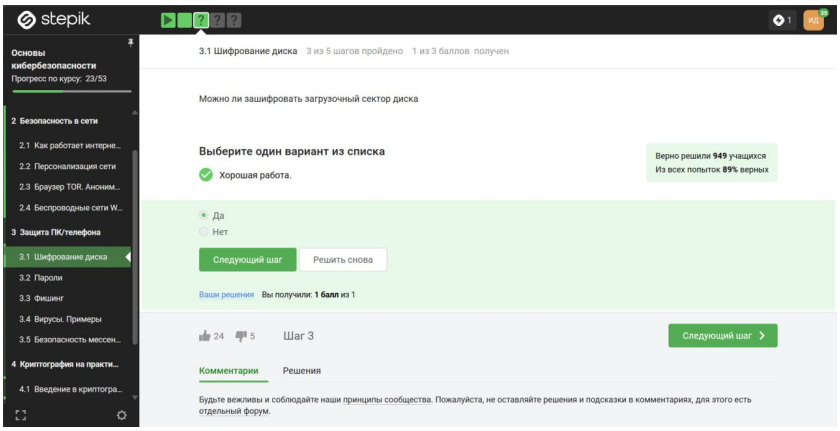

Рис. 2.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. [2.2]).

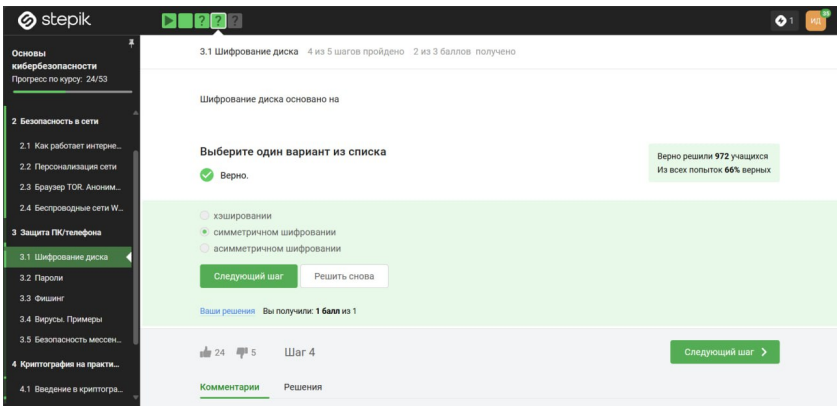

Рис. 2.2: Вопрос 3.1.2

Во всех популярных операционных системах есть встроенные утилиты, которые позволяют шифровать жесткий диск: для Windows это Bitlocker, в Linux – LUKS, в MacOS – это FileVault. Кроме того, есть и сторонние опенсорсные (open source) программы, то есть бесплатные: это Veracrypt, PGPDisk, которые можно установить себе и использовать их для шифрования ваших жестких дисков, загрузочных секторов или флешек (рис. [2.3]).

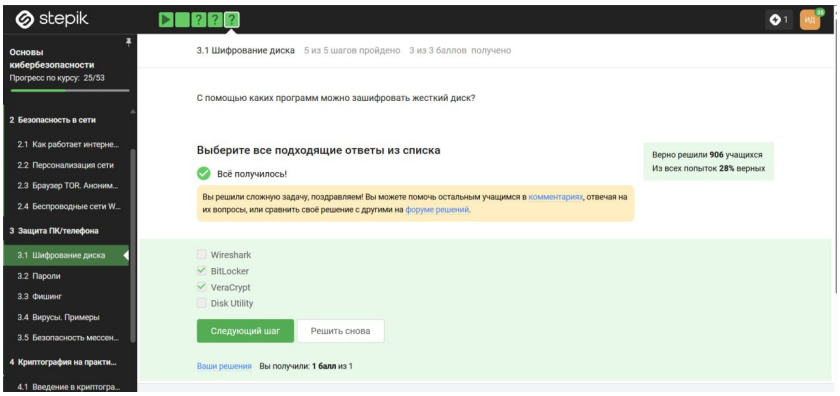

Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

Стойкий пароль должен состоять из цифр, букв нижнего регистра, верхнего регистра и спецсимволов. Как правило, при регистрации на каком-нибудь сайте или приложении вас просят добавить как минимум один спецсимвол, как минимум одну цифру, как минимум одну букву верхнего регистра, нижнего регистра. Это все сделано для того, чтобы сложность перебора вашего пароля была большой (рис. [2.4]).

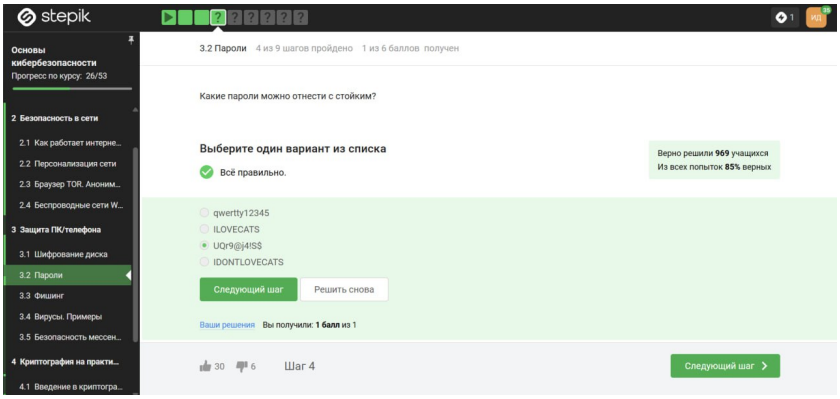

Рис. 2.4: Вопрос 3.2.1

Конечно же, безопасно хранить пароли только в менеджере паролей, но никак не в заметках телефона и на стикере монитора (рис. [2.5]).

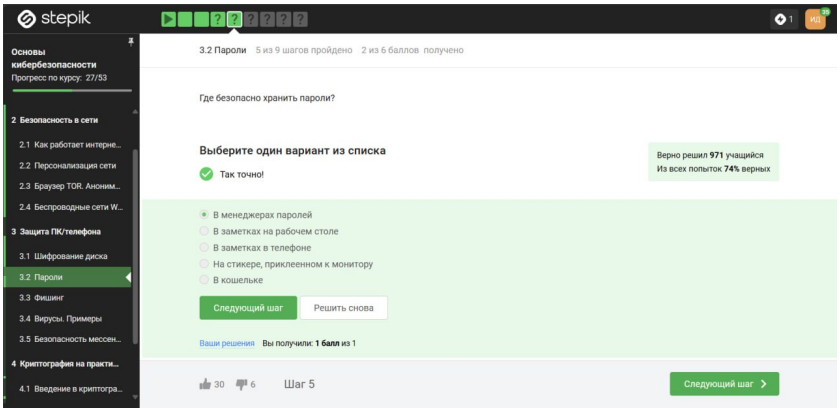

Рис. 2.5: Вопрос 3.2.2

Капча - это аббревиатура с английского; это тест для определения, является ли пользователь, который общается с веб-сервисом, человеком или компьютером, ботом, которой пытается просто-напросто перебрать все пароли (рис. [2.6]).

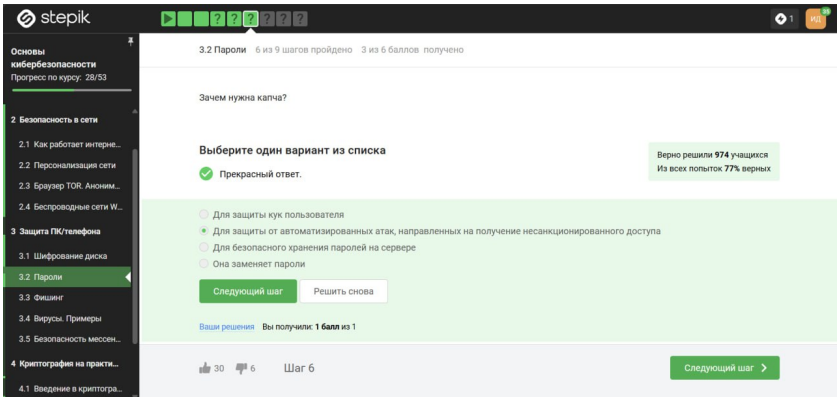

Рис. 2.6: Вопрос 3.2.3

Хранить пароли в открытом виде очень опасно, поэтому хранят их хэши (рис. [2.7]).

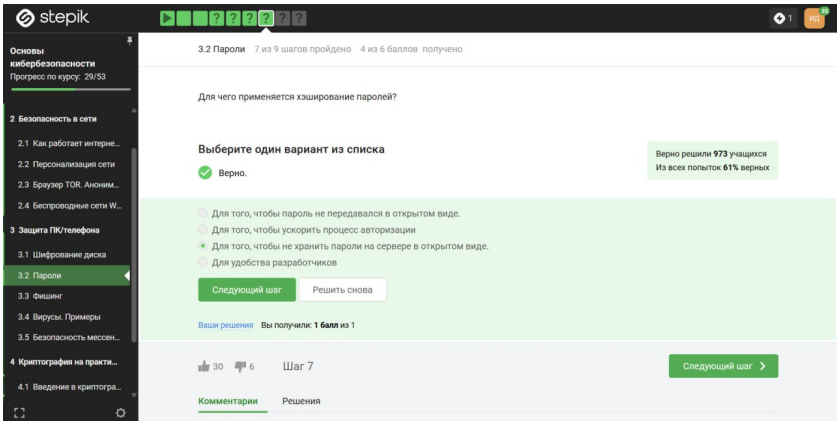

Рис. 2.7: Вопрос 3.2.4

Основная идея в защите слабых паролей - так называемая соль. Есть еще перец, про перец мы говорить не будем. Соль используется для того, чтобы увеличить стойкость пароля для пользователей, которые сами не догадались о стойкости своих паролей. Например, если у нас alice логинится с паролем 12345, что делает

при этом сервер? Сервер не хочет хранить хэш от пароля 12345, потому что, скорее всего, злоумышленник имеет таблицы с самыми популярными паролями и их хэшами. Какая функция хэш используется в конкретном сервере, все знают. В основном, много серверов используют в своих таблицах SHA2 или SHA3, и, естественно, злоумышленник может для самых частых паролей посчитать эти значения, поэтому хранить хэш от 12345 абсолютно бессмысленно, и так понятно, что это соответствует паролю 12345 (рис. [2.8]).

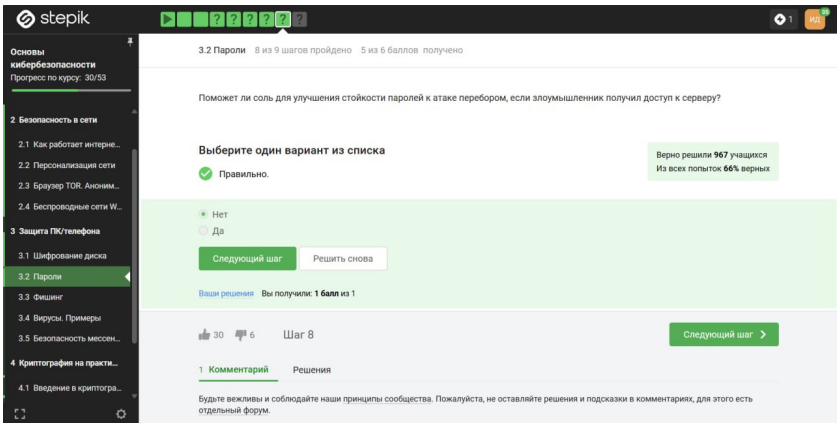

Рис. 2.8: Вопрос 3.2.5

нужно использовать длинные пароли с максимально большим алфавитом, хранить их стоит в менеджерах паролей, пароли нужно менять достаточно регулярно, особенно к таким критическим сервисам, как почта. Политика (особенно больших компаний) по безопасности состоит в том, что пароли нужно менять. И для разных сайтов, и для разных программ нужно использовать разные пароли, поскольку компрометация одного из них может вести к компрометации всех остальных, если вы используете одинаковые пароли. И напоследок, есть такой сервис для проверки, утёк ли ваш пароль где-либо: он называется haveibeenpwned.com. Вы можете зайти на этот сайт, забить какой-то свой аккаунт и проверить, засветились ваши данные в базах данных серверов, ключи к которым утекли (рис. [2.9]).

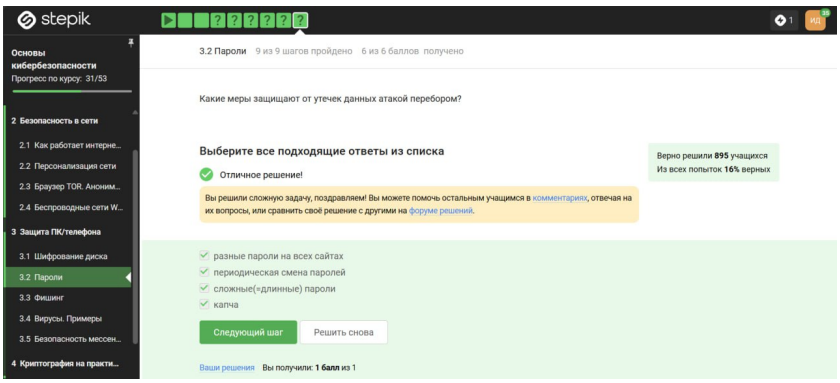

Рис. 2.9: НВопрос 3.2.6

2.3 Фишинг

пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем, начало может быть одинаковое или середина (рис. [2.10]).

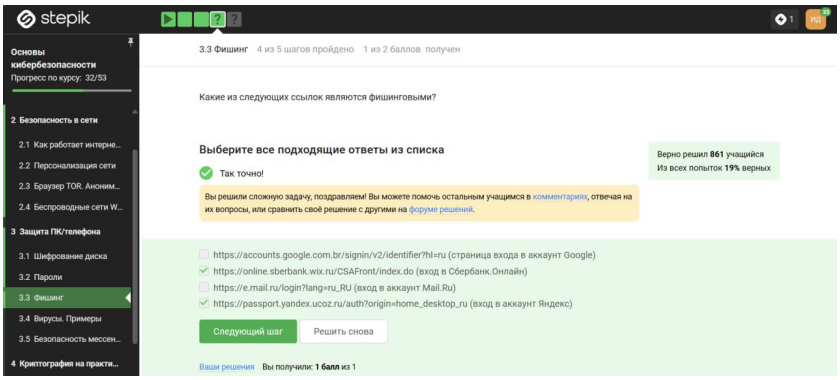

Рис. 2.10: Вопрос 3.3.1

Может фишинговое письмо прийти и от друга, знакомого или родственника, если его взломали (рис. [2.11]).

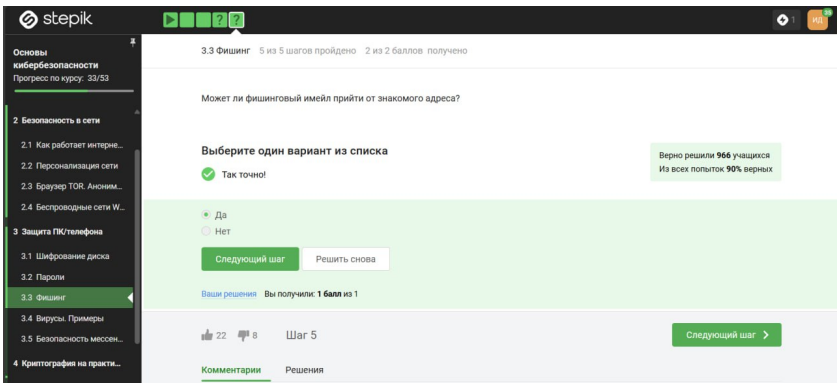

Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

Спуфинг - это подмена адреса отправителя в имейлах (рис. [2.12]).

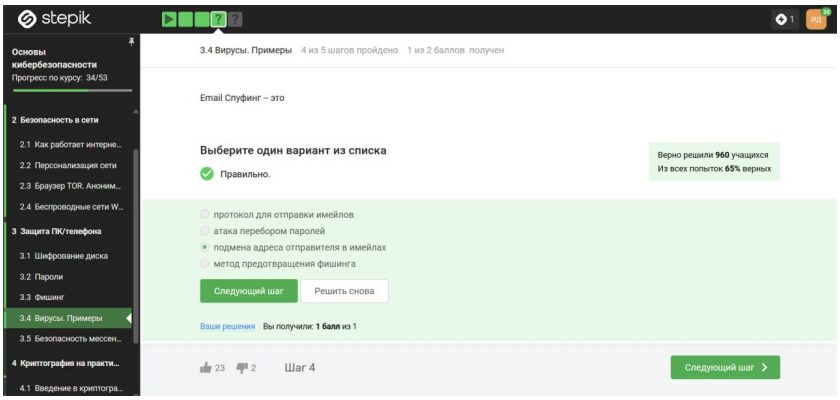

Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его (рис. [2.13]).

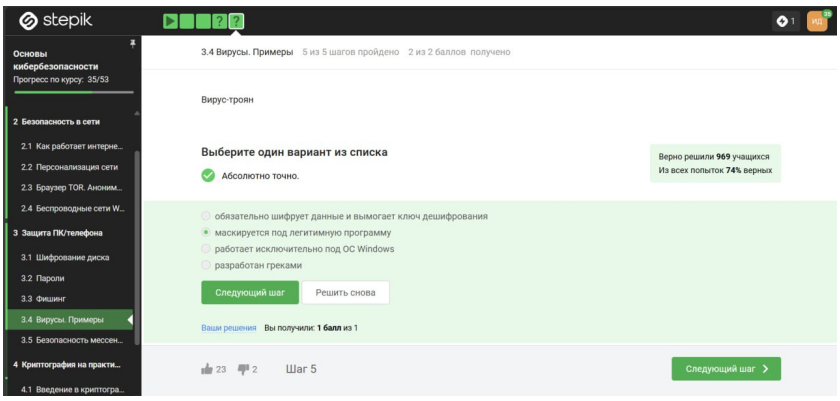

Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. [2.14]).

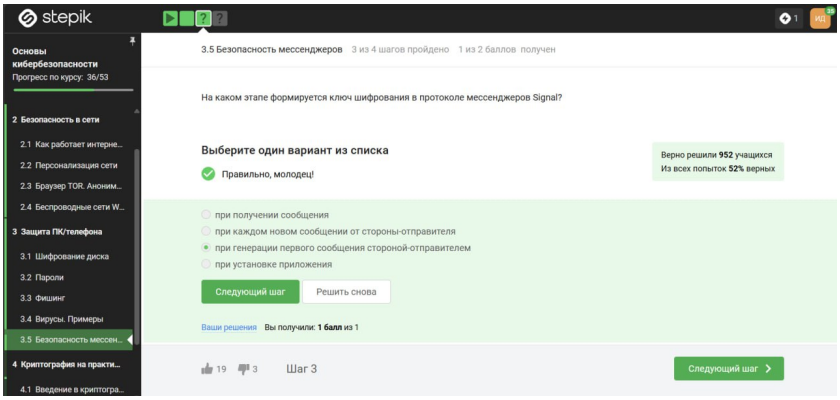

Рис. 2.14: Вопрос 3.5.1

Суть довольно простая: у нас есть два участника - Алиса и Боб, A и B, и сквозное шифрование заключается в том, что сервер, который передает сообщение, который направляет сообщение от Алисы к Бобу или от Бобу к Алисе, знает только то, куда эти сообщения должны быть направлены, но сообщения он передает в зашифрованном виде, то есть он как бы работает маршрутизатором сообщений,

не зная о том, что он передает. Что происходит, если мы хотим отправить сообщение от Алисы к Бобу? Алиса шифрует свои данные, кладет на сервере шифр-текст с пометкой, что этот шифр-текст предназначен для Боба. Когда Боб заходит в сеть, сервер видит: «Ага, Боб зашел в сеть, надо обновить его сообщение», и отправляет шифр-текст от Алисы. Боб получает этот шифр-текст, дешифрует его, получает сообщение в открытом виде. При этом сервер не знает ни ключ, с помощью которого Алиса шифровала, ни тем более сообщение в открытом виде. То есть, сообщения передаются по узлам связи в зашифрованном виде (рис. [2.15]).

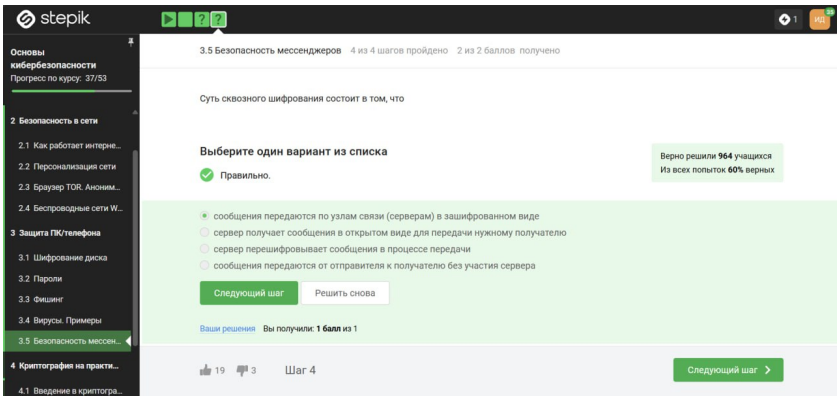

Рис. 2.15: Вопрос 3.5.2

3 Выводы

Мною был пройден второй блок курса “Основы кибербезопасности”. В результате я повторила правила составления и хранения паролей, узнала много нового о вирусах и мерах безопасности против них.