

Внешний курс. Блок 2: Защита ПК/Телефона

Основы информационной безопасности

ИБРАХИМ МОХСЕЙН МОХАММЕД АЛИ АЛЬКАМАЛЬ

Содержание

1 Цель работы	5
2 Выполнение блока 2: Защита ПК/Телефона	6
2.1 Шифрование диска	6
2.2 Пароли	7
2.3 Фишинг	10
2.4 Вирусы. Примеры	11
2.5 Безопасность мессенджеров	12
3 Выводы	14

Список иллюстраций

2.1	Вопрос 3.1.1	6
2.2	Вопрос 3.1.2	7
2.3	Вопрос 3.1.3	7
2.4	Вопрос 3.2.1	8
2.5	Вопрос 3.2.2	8
2.6	Вопрос 3.2.3	9
2.7	Вопрос 3.2.4	9
2.8	Вопрос 3.2.5	10
2.9	НВопрос 3.2.6	10
2.10	Вопрос 3.3.1	11
2.11	Вопрос 3.3.2	11
2.12	Вопрос 3.4.1	12
2.13	Вопрос 3.4.2	12
2.14	Вопрос 3.5.1	13
2.15	Вопрос 3.5.2	13

Список таблиц

1 Цель работы

Пройти второй блок курса “Основы кибербезопасности”

2 Выполнение блока 2: Защита ПК/Телефона

2.1 Шифрование диска

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Соответственно, можно (рис. 2.1).

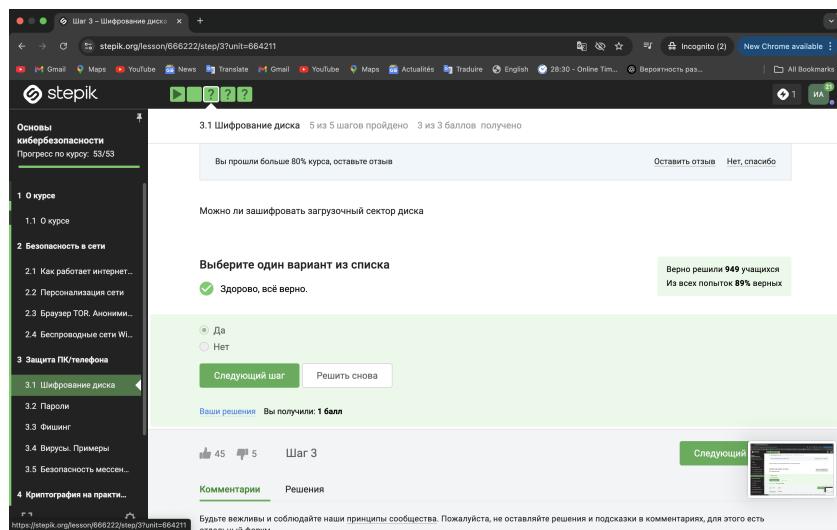


Рис. 2.1: Вопрос 3.1.1

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

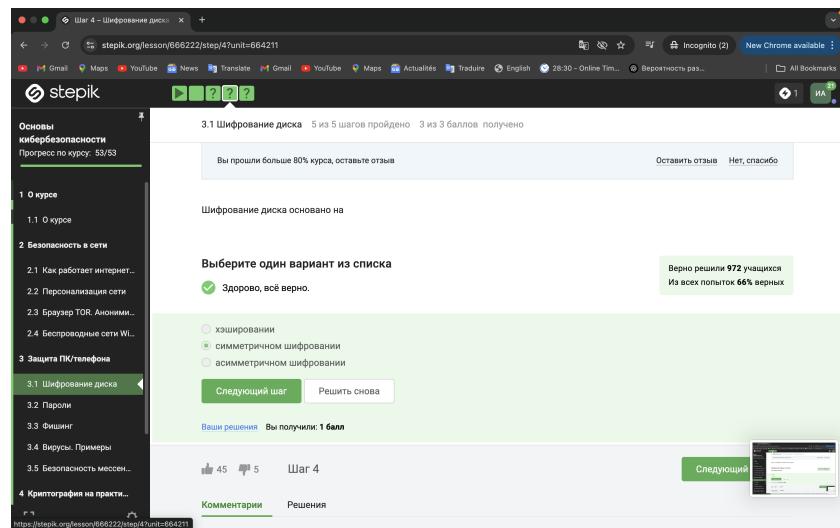


Рис. 2.2: Вопрос 3.1.2

Отмечены программы, с помощью которых можно зашифровать жесткий диск (рис. 2.3).

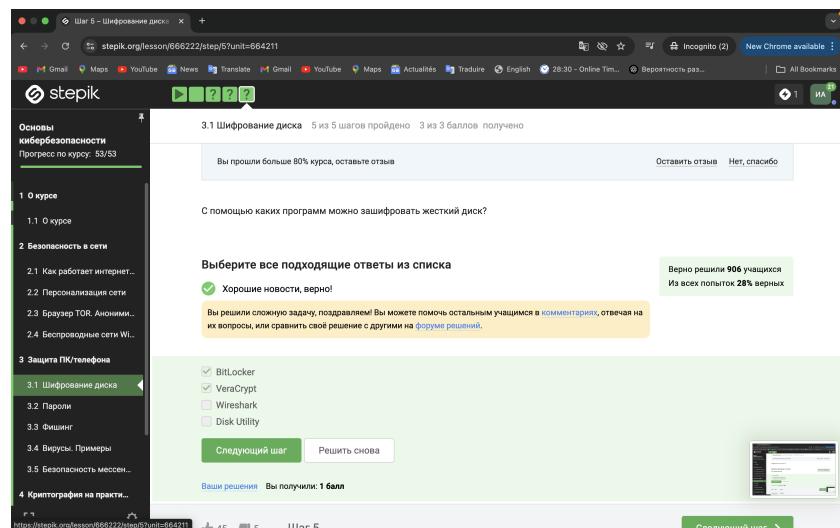


Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

Стойкий пароль - тот, который тяжелее подобрать, он должен быть со спец. символами и длинный (рис. 2.4).

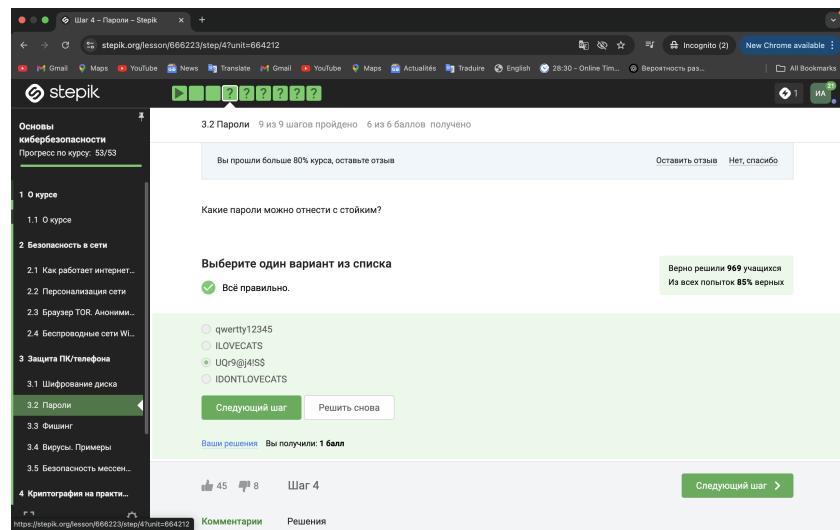


Рис. 2.4: Вопрос 3.2.1

Все варианты, кроме менеджера паролей, совершенно не надежные (рис. 2.5).

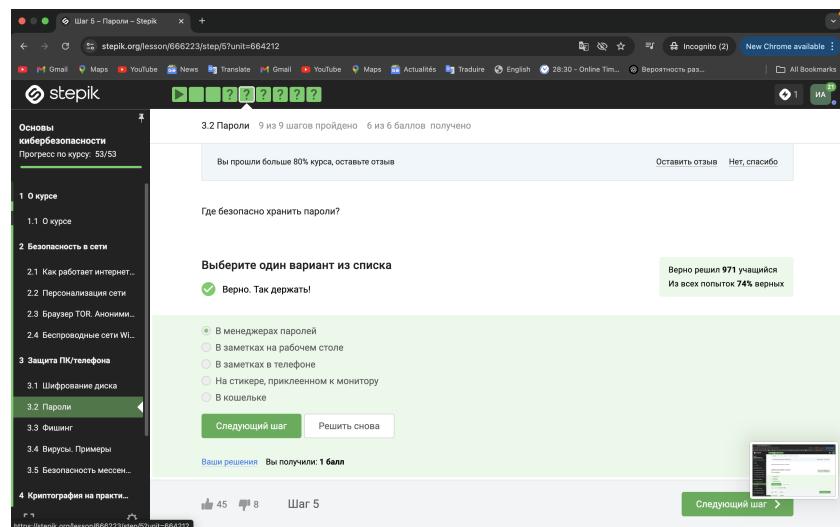


Рис. 2.5: Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном “не робот”(рис. 2.6).

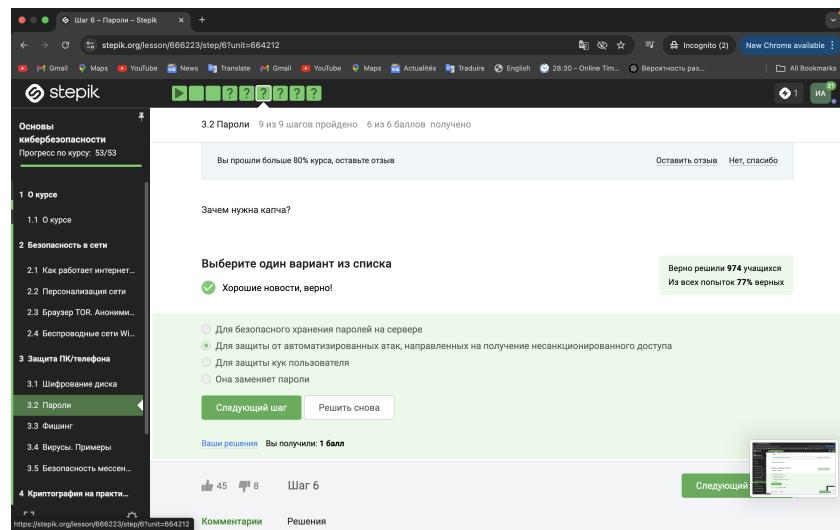


Рис. 2.6: Вопрос 3.2.3

Опасно хранить пароли в открытом виде, поэтому хранят их хэши (рис. 2.7).

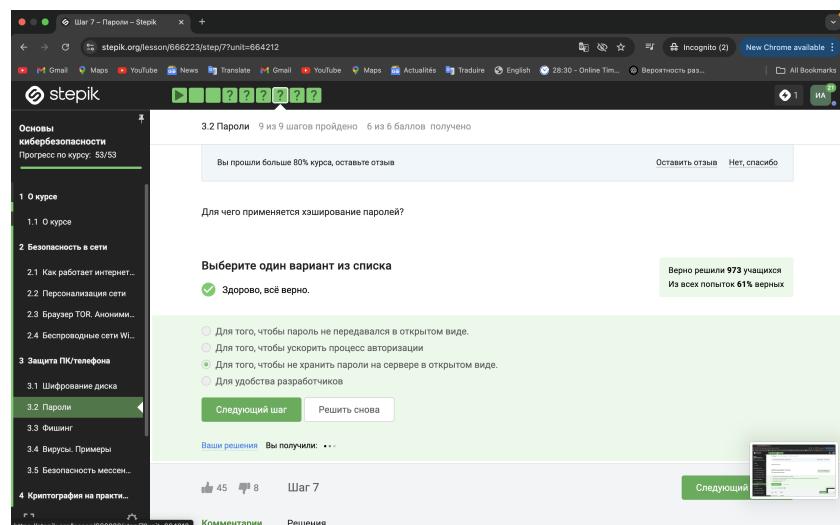


Рис. 2.7: Вопрос 3.2.4

Соль не поможет (рис. 2.8).

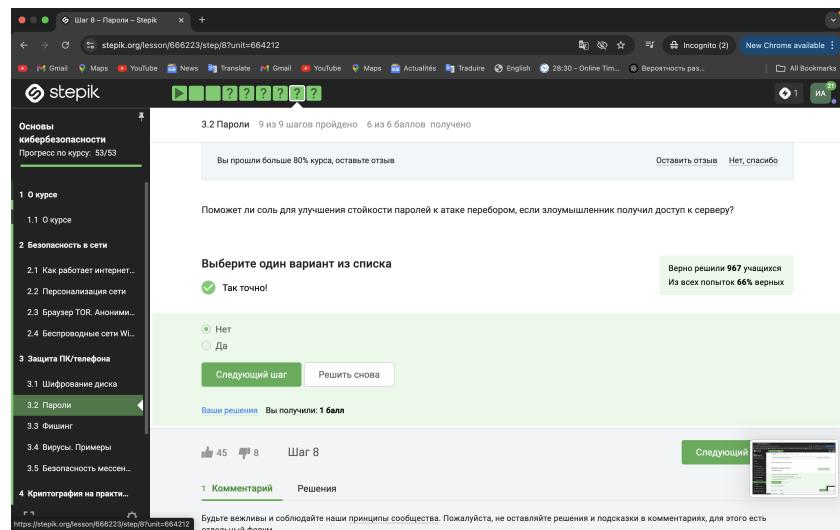


Рис. 2.8: Вопрос 3.2.5

Все приведенные меры защищают от утечек данных (рис. 2.9).

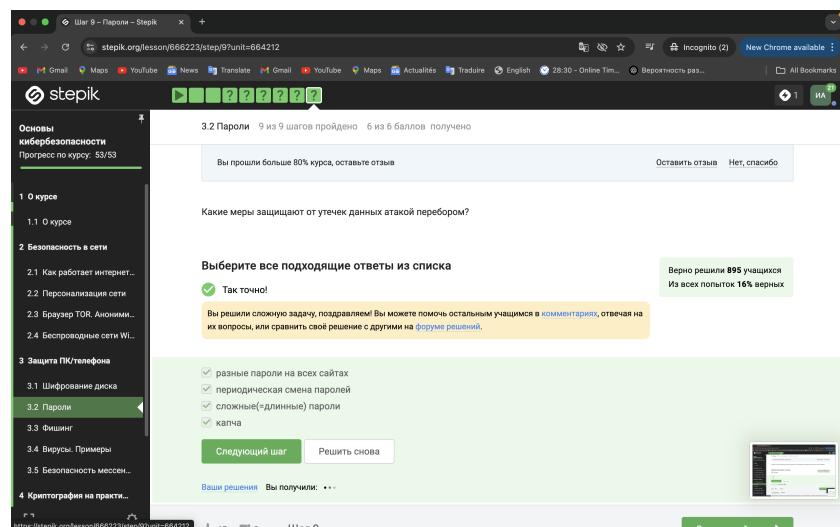


Рис. 2.9: Вопрос 3.2.6

2.3 Фишинг

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями (рис. 2.10).

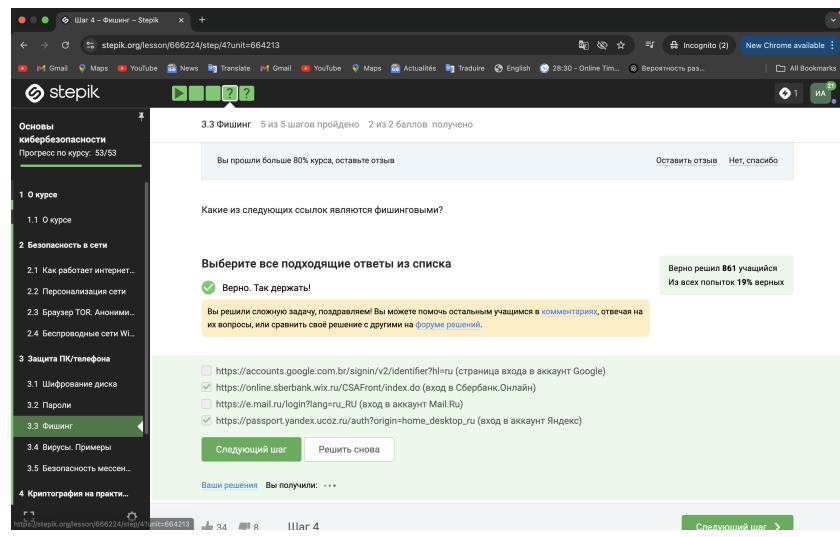


Рис. 2.10: Вопрос 3.3.1

Да, может, например, если пользователя со знакомым адресом взломали (рис. 2.11).

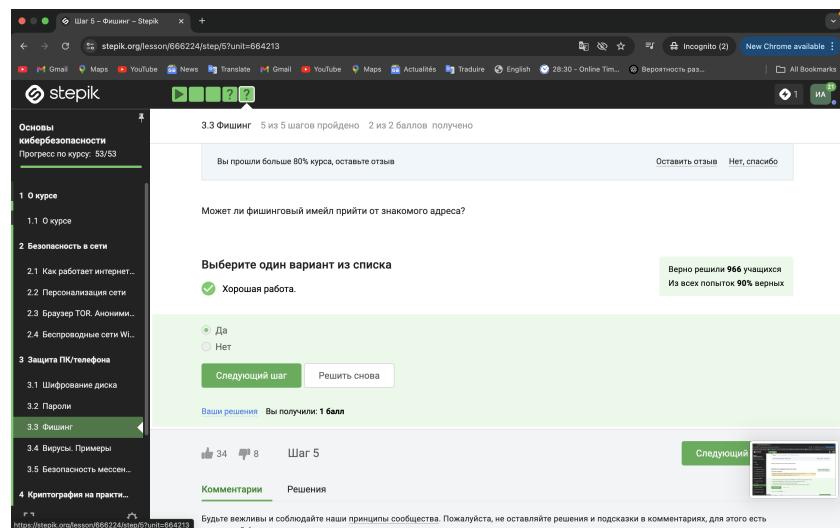


Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

Ответ дан в соответствии с определением (рис. 2.12).

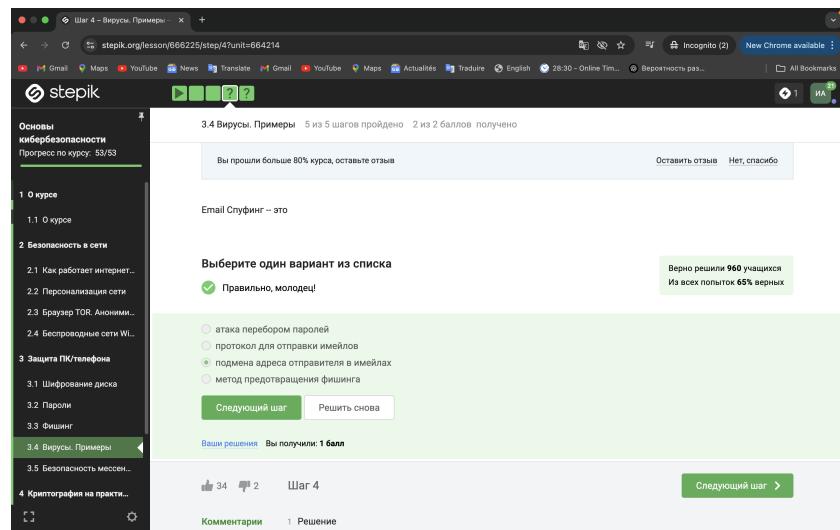


Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

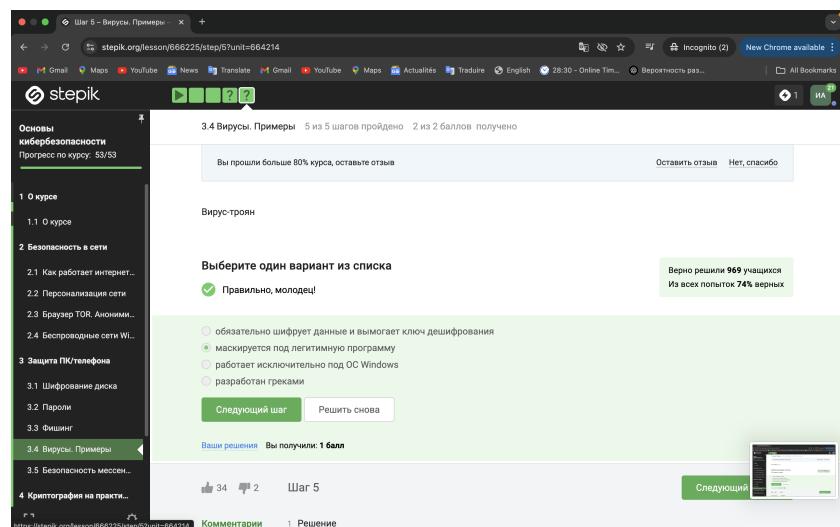


Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

При установке первого сообщения отправителем формируется ключ шифрования (рис. 2.14).

The screenshot shows a Stepik course interface. The left sidebar lists topics: 1. О курсе, 1.1 О курсе, 2. Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Браузер TOR. Аноним..., 2.4 Беспроводные сети Wi..., 3. Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Фишинг, 3.4 Вирусы. Примеры, 3.5 Безопасность мессен..., and 4. Криптография на практи... The main content area displays a question titled "3.5 Безопасность мессенджеров" (Step 3 - Message Security). It asks: "На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?". Below the question is a list of four options with radio buttons. The first option is selected: "при каждом новом сообщении от стороны-отправителя". A green checkmark indicates the answer is correct. The text "Отлично!" is displayed. At the bottom, there are buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again). The right side shows statistics: "Верно решили 952 учащихся" and "Из всех попыток 52% верных". The URL in the address bar is <https://stepik.org/lesson/668226/step/3?unit=664215>.

Рис. 2.14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде (рис. 2.15).

The screenshot shows a Stepik course interface. The left sidebar lists topics: 1. О курсе, 1.1 О курсе, 2. Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Браузер TOR. Аноним..., 2.4 Беспроводные сети Wi..., 3. Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Фишинг, 3.4 Вирусы. Примеры, 3.5 Безопасность мессен..., and 4. Криптография на практи... The main content area displays a question titled "3.5 Безопасность мессенджеров" (Step 4 - Message Security). It asks: "Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде". Below the question is a list of five options with radio buttons. The fourth option is selected: "сообщения передаются по узлам связи (серверам) в зашифрованном виде". A green checkmark indicates the answer is correct. The text "Хорошие новости, верно!" is displayed. At the bottom, there are buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again). The right side shows statistics: "Верно решили 964 учащихся" and "Из всех попыток 60% верных". The URL in the address bar is <https://stepik.org/lesson/668226/step/4?unit=664215>.

Рис. 2.15: Вопрос 3.5.2

3 Выводы

Был пройден второй блок курса “Основы кибербезопасности”, изучены правила хранения паролей и основная информация о вирусах