Внешний курс. Блок 2: Защита ПК/Телефона

Воинов Кирилл Викторович

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 10
2.5 Безопасность мессенджеров 11

3 Выводы **13**

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 8
2.7 Вопрос 3.2.4 9
2.8 Вопрос 3.2.5 9
2.9 НВопрос 3.2.6 9
2.10 Вопрос 3.3.1 10
2.11 Вопрос 3.3.2 10
2.12 Вопрос 3.4.1 11
2.13 Вопрос 3.4.2 11
2.14 Вопрос 3.5.1 12
2.15 Вопрос 3.5.2 12

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).

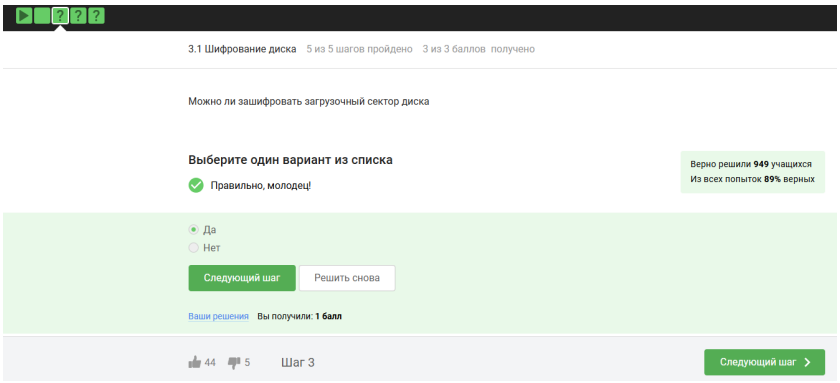

Рис. 2.1: Вопрос 3.1.1

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

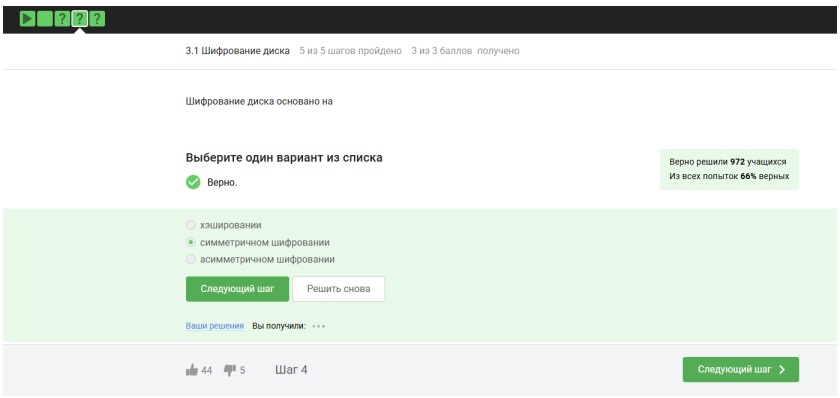

Рис. 2.2: Вопрос 3.1.2

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

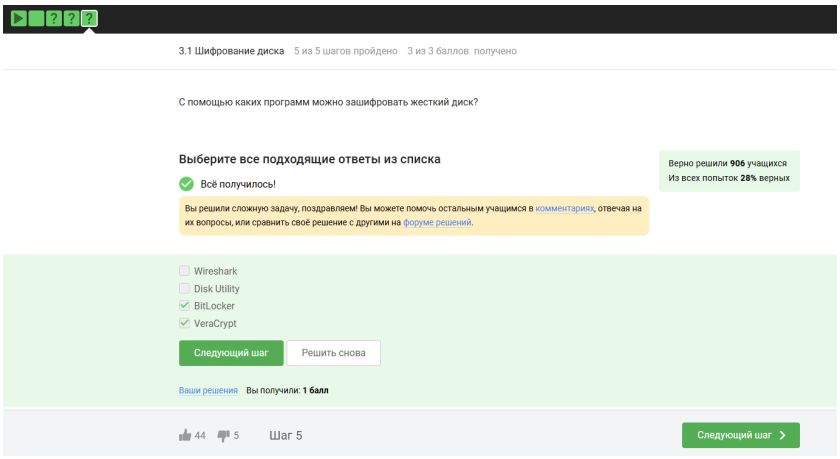

Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

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

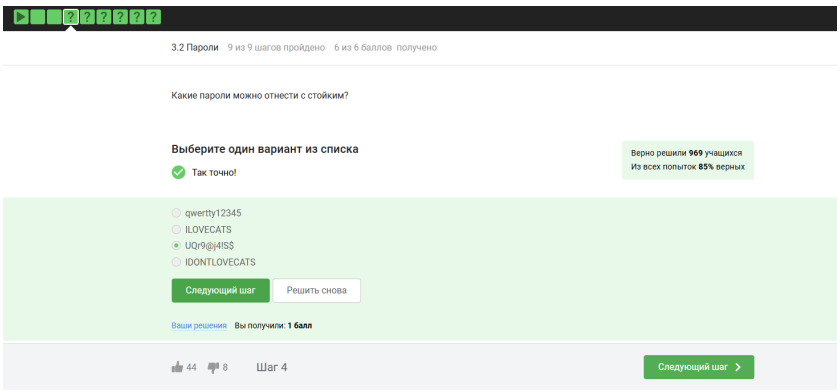

Рис. 2.4: Вопрос 3.2.1

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

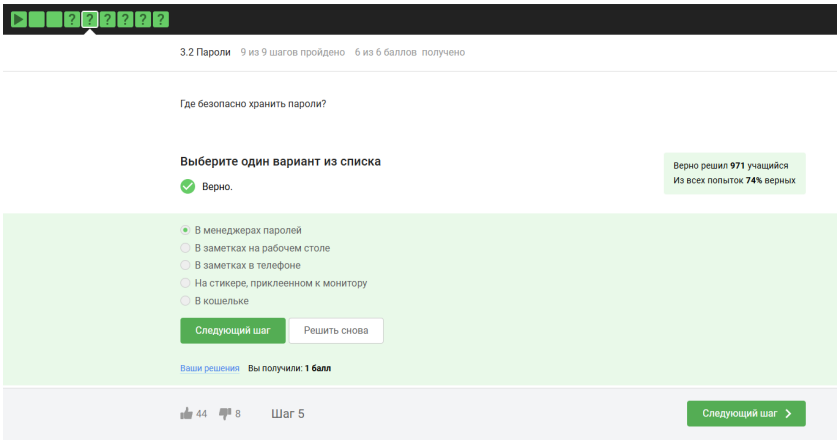

Рис. 2.5: Вопрос 3.2.2

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

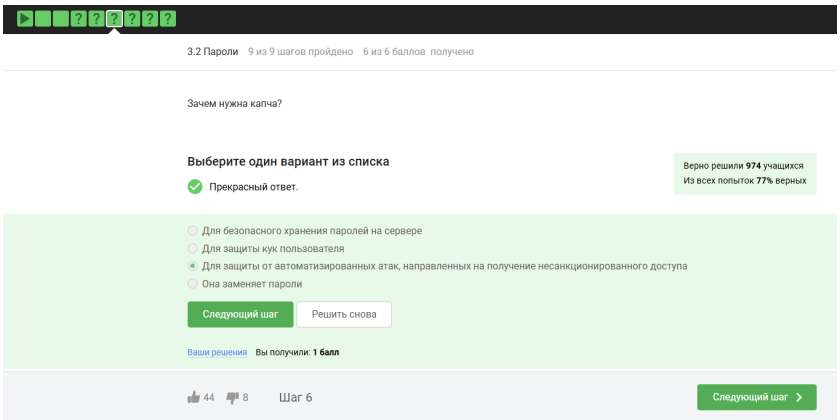

Рис. 2.6: Вопрос 3.2.3

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

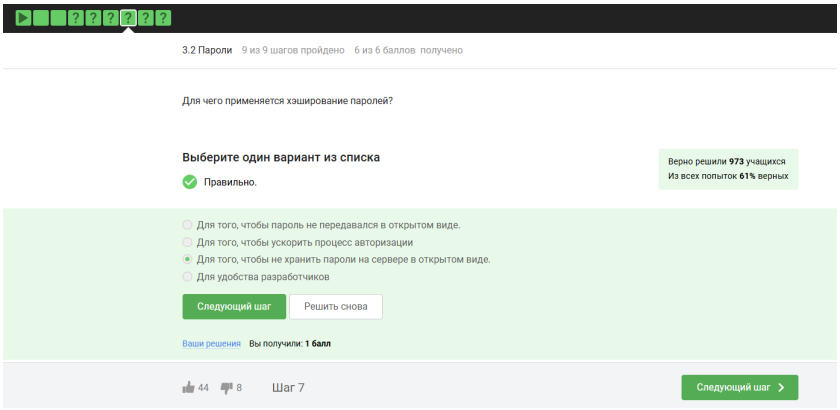

Рис. 2.7: Вопрос 3.2.4

Соль не поможет, круг из нее, теоретически, возможно (рис. 2.8).

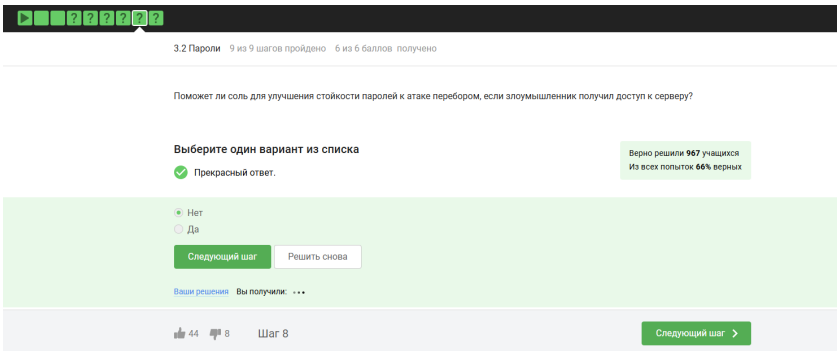

Рис. 2.8: Вопрос 3.2.5

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

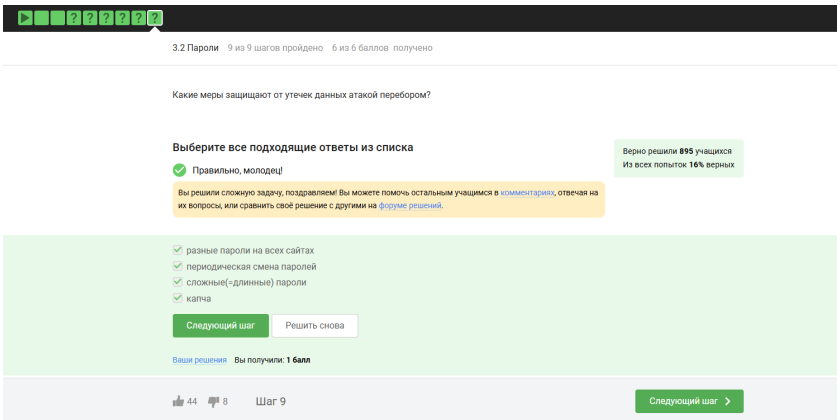

Рис. 2.9: НВопрос 3.2.6

2.3 Фишинг

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

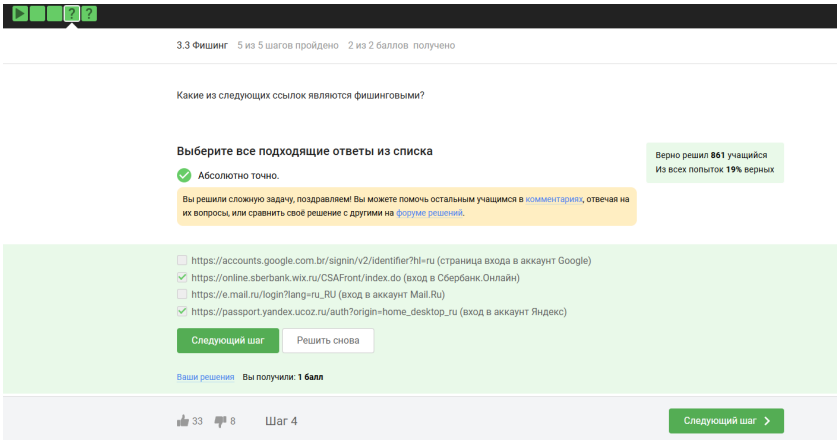

Рис. 2.10: Вопрос 3.3.1

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

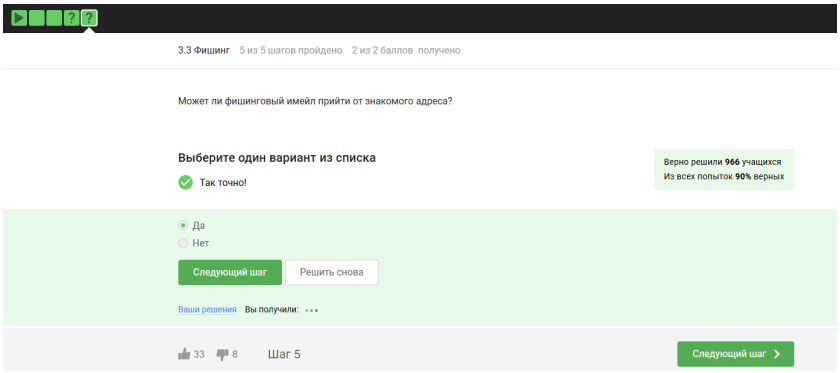

Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

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

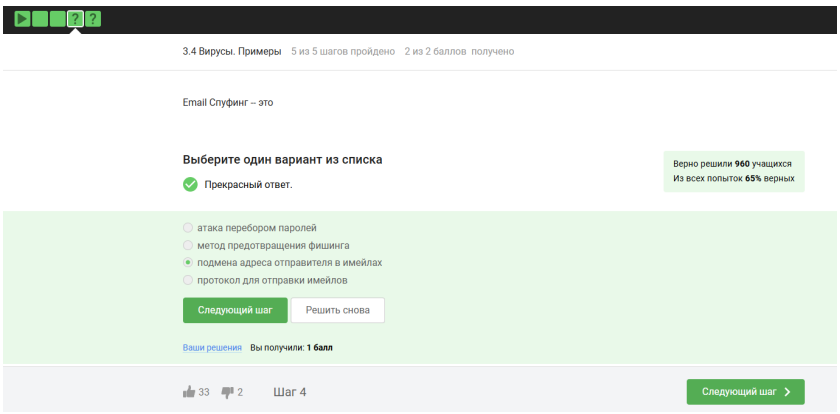

Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

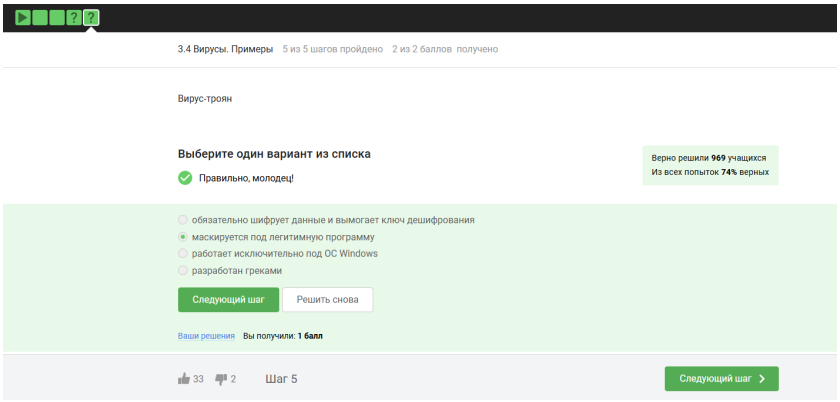

Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

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

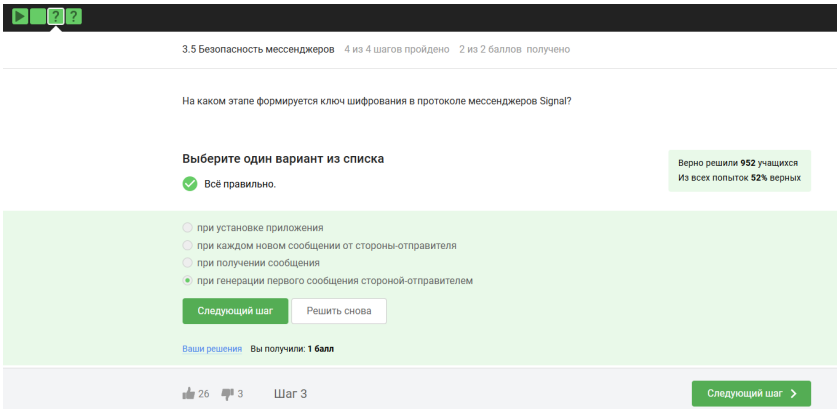

Рис. 2.14: Вопрос 3.5.1

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

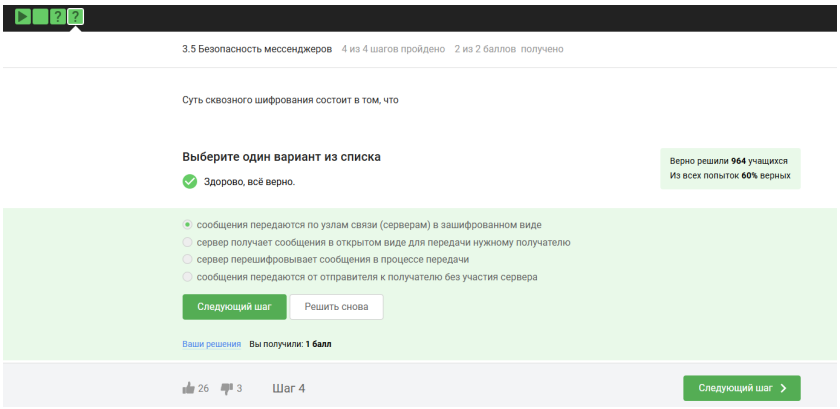

Рис. 2.15: Вопрос 3.5.2

3 Выводы

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