

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).

The screenshot shows a quiz interface with a progress bar at the top indicating 3.1 out of 5 steps completed and 3 out of 3 points earned. The question is 'Можно ли зашифровать загрузочный сектор диска' (Can you encrypt the boot sector of the disk?). The user has selected 'Да' (Yes), which is marked as correct. A green box indicates that 949 students answered correctly, with an 89% success rate. The interface includes buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). At the bottom, there are social media-like icons for likes (44) and dislikes (5), and a 'Шаг 3' (Step 3) indicator.

Рис. 2.1: Вопрос 3.1.1

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

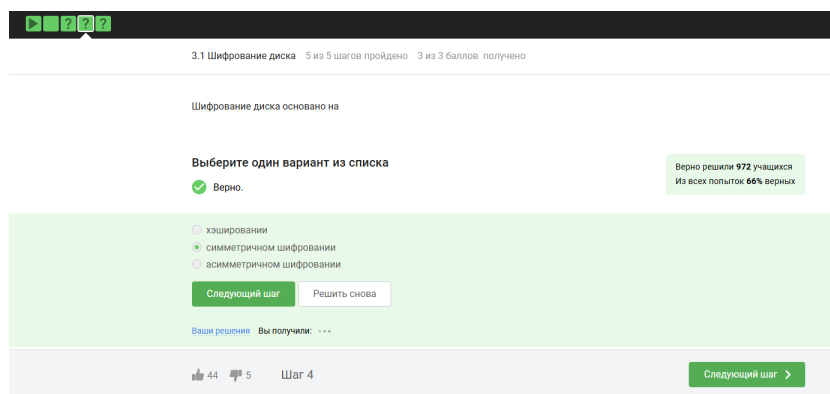


Рис. 2.2: Вопрос 3.1.2

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

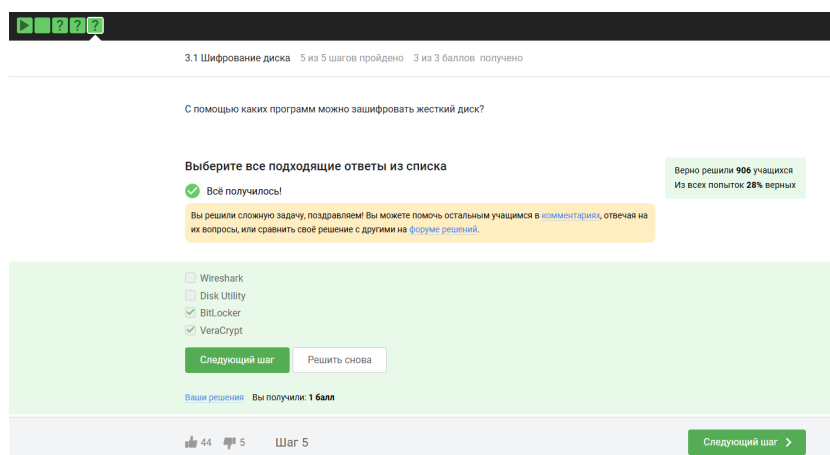


Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Так точно!

Верно решили 969 учащихся
Из всех попыток 85% верных

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQ9@j4iS\$
- ☐ IDONTLOVECATS

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 8 Шаг 4 Следующий шаг >

Рис. 2.4: Вопрос 3.2.1

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Верно.

Верно решил 971 учащийся
Из всех попыток 74% верных

- ☒ В менеджерах паролей
- ☐ В записках на рабочем столе
- ☐ В записках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 8 Шаг 5 Следующий шаг >

Рис. 2.5: Вопрос 3.2.2

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Зачем нужна капча?

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 974 учащихся
Из всех попыток 77% верных

- ☐ Для безопасного хранения паролей на сервере
- ☐ Для защиты кук пользователя
- ☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа
- ☐ Она заменяет пароли

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 8 Шаг 6 Следующий шаг >

Рис. 2.6: Вопрос 3.2.3

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Правильно.

Верно решили 972 учащихся
Из всех попыток 61% верных

- ☐ Для того, чтобы пароль не передавался в открытом виде.
- ☐ Для того, чтобы ускорить процесс авторизации.
- ☒ Для того, чтобы не хранить пароли на сервере в открытом виде.
- ☐ Для удобства разработчиков

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 8 Шаг 7 Следующий шаг >

Рис. 2.7: Вопрос 3.2.4

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 967 учащихся
Из всех попыток 66% верных

- ☒ Нет
- ☐ Да

Следующий шаг Решить снова

Ваши решения Вы получили: ...

44 8 Шаг 8 Следующий шаг >

Рис. 2.8: Вопрос 3.2.5

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

Верно решили 895 учащихся
Из всех попыток 14% верных

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на форуме решений.

- ☒ разные пароли на всех сайтах
- ☒ периодическая смена паролей
- ☒ сложные(-длинные) пароли
- ☒ капча

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 8 Шаг 9 Следующий шаг >

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).

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно решил 861 учащихся
Из всех попыток 19% верных

✓ Абсолютно точно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на [форуме решений](#).

- ☐ <https://accounts.google.com.br/signin/v2/identifier?hl=ru> (страница входа в аккаунт Google)
- ☒ <https://online.sberbank.wix.ru/CSAFront/index.do> (выход в Сбербанк.Онлайн)
- ☐ https://e.mail.ru/login?lang=ru_RU (выход в аккаунт Mail.Ru)
- ☒ https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (выход в аккаунт Яндекс)

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

33 8 Шаг 4 Следующий шаг >

Рис. 2.10: Вопрос 3.3.1

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

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

Верно решили 966 учащихся
Из всех попыток 90% верных

✓ Так точно!

☒ Да

☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: ...

33 8 Шаг 5 Следующий шаг >

Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

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

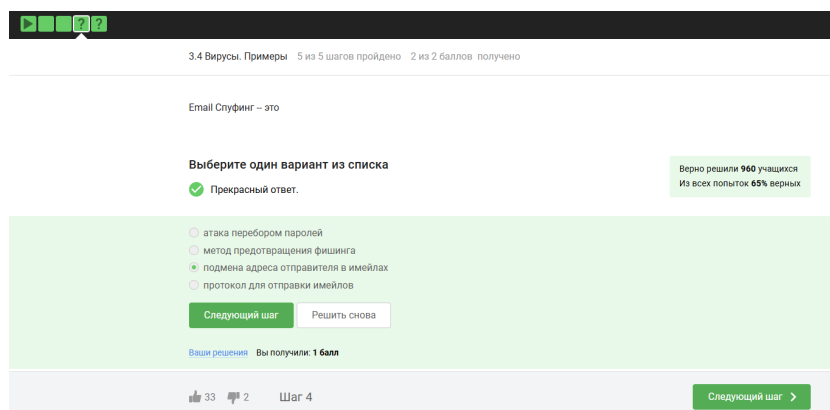


Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

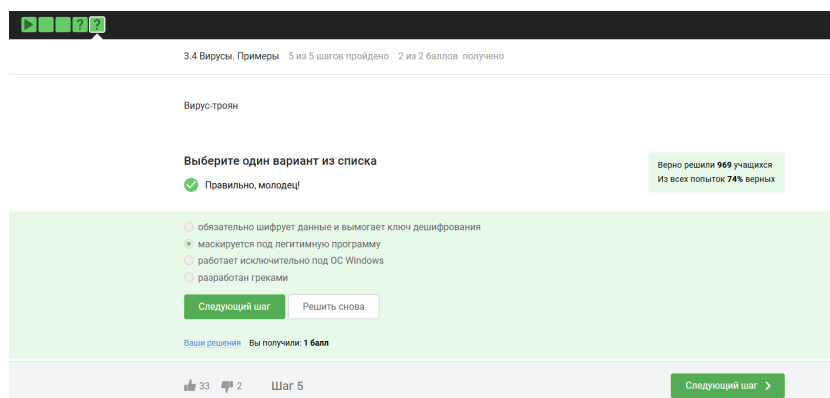


Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

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

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 952 учащихся
Из всех попыток 52% верных

- ☐ при установке приложения
- ☐ при каждом новом сообщении от стороны-отправителя
- ☐ при получении сообщения
- ☒ при генерации первого сообщения стороной-отправителем

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Шаг 3

Следующий шаг >

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).

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 964 учащихся
Из всех попыток 60% верных

- ☒ сообщения передаются по узлам связи (серверам) в зашифрованном виде
- ☐ сервер получает сообщения в открытом виде для передачи нужному получателю
- ☐ сервер перешифровывает сообщения в процессе передачи
- ☐ сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Шаг 4

Следующий шаг >

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