

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

Стариков Данила Андреевич

Содержание

1	Цель работы	3
2	Выполнение лабораторной работы	4
2.1	Шифрование диска	4
2.2	Пароли	6
2.3	Фишинг	10
2.4	Вирусы. Примеры	12
2.5	Безопасность мессенджеров	14
3	Выводы	16

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

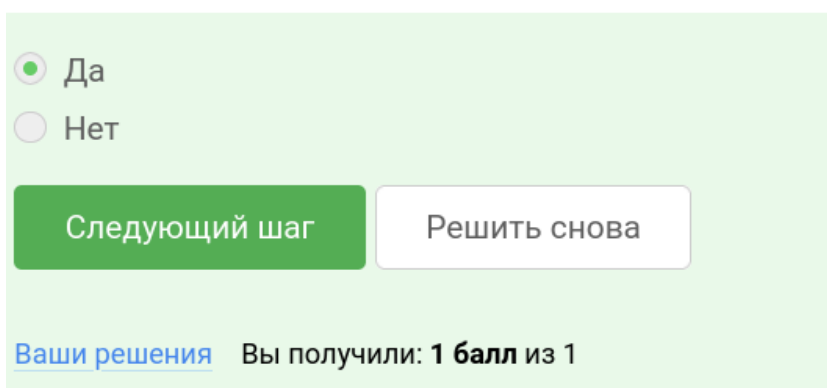
- Вопрос 1. Можно ли зашифровать загрузочный сектор диска(рис. 2.1)

Ответ: *Да*.

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Всё получилось!



The screenshot shows a quiz interface with a light green background. At the top, there are two radio button options: 'Да' (Yes) which is selected with a green dot, and 'Нет' (No) which is unselected. Below the options are two buttons: a green button labeled 'Следующий шаг' (Next step) and a white button with a grey border labeled 'Решить снова' (Solve again). At the bottom, there is a blue link 'Ваши решения' (Your solutions) followed by the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 2.1: Скриншот выполнения задания

- Вопрос 2. Шифрование диска основано на(рис. 2.2)

Ответ: *симметричном шифровании.*

Шифрование диска основано на

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.2: Скриншот выполнения задания

- Вопрос 3. С помощью каких программ можно зашифровать жесткий диск?(рис. 2.3)

Ответ: *BitLocker и VeraCrypt.*

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

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

- ☒ BitLocker
- ☐ Disk Utility
- ☒ VeraCrypt
- ☐ Wireshark

Следующий шаг

Решить снова

Рис. 2.3: Скриншот выполнения задания

2.2 Пароли

- Вопрос 1. Какие пароли можно отнести с стойким?(рис. 2.4)

Ответ: *UQr9@j4!S\$.*

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё получилось!

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQr9@j4!S\$
- ☐ IDONTLOVECATS

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.4: Скриншот выполнения задания

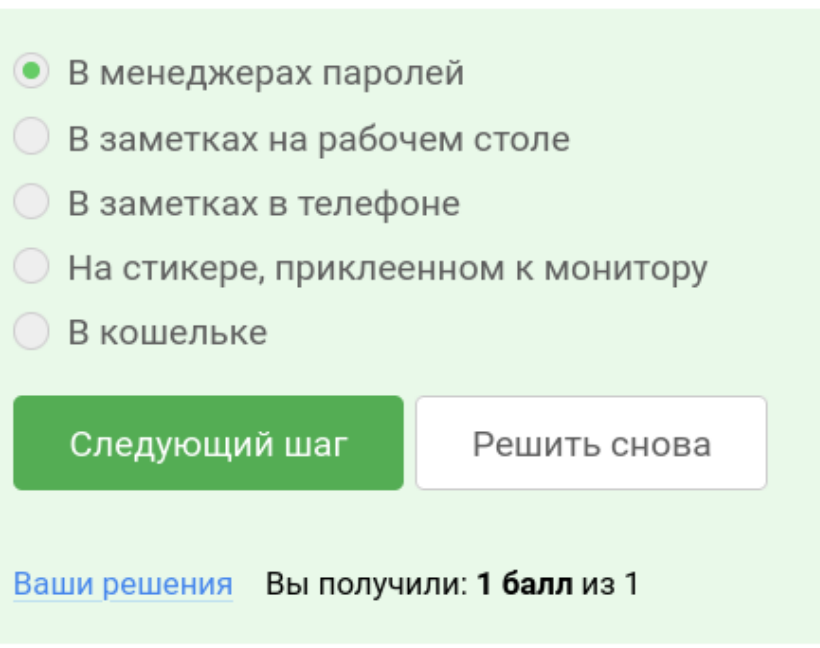
- Вопрос 2. Где безопасно хранить пароли?(рис. 2.5)

Ответ: *В менеджерах паролей.*

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Верно.



☒ В менеджерах паролей

☐ В заметках на рабочем столе

☐ В заметках в телефоне

☐ На стикере, приклеенном к монитору

☐ В кошельке

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.5: Скриншот выполнения задания

- Вопрос 3. Зачем нужна капча?(рис. 2.6)

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

Зачем нужна капча?

Выберите один вариант из списка

Вер
Из

✓ Всё правильно.

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.6: Скриншот выполнения задания

- Вопрос 4. Для чего применяется хэширование паролей?(рис. 2.7)

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

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Всё правильно.

- ☐ 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 из 1

Рис. 2.7: Скриншот выполнения задания

- Вопрос 5. Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?(рис. 2.8)

Ответ: *Нет.*

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

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 967 уч
Из всех попыток 66%

☐ Да
☒ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.8: Скриншот выполнения задания

- Вопрос 6. Какие меры защищают от утечек данных атакой перебором?(рис. 2.9)

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

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё 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 из 1

Рис. 2.9: Скриншот выполнения задания

2.3 Фишинг

- Вопрос 1. Какие из следующих ссылок являются фишинговыми?(рис. 2.10)

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).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

✓ Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё 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> (вход в Сбербанк.Онлайн)
- ☐ https://e.mail.ru/login?lang=ru_RU (вход в аккаунт Mail.Ru)
- ☒ https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.10: Скриншот выполнения задания

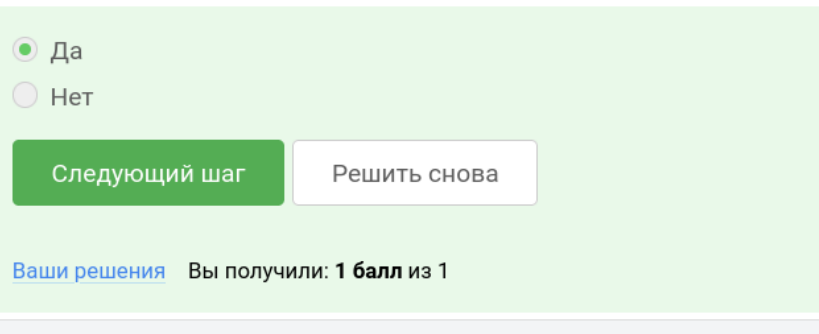
- Вопрос 2. Может ли фишинговый имейл прийти от знакомого адреса?(рис. 2.11)

Ответ: Да.

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Так точно!



☐ Да

☐ Нет

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.11: Скриншот выполнения задания


2.4 Вирусы. Примеры

- Вопрос 1. Email Спуфинг – это(рис. 2.12)

Ответ: *подмена адреса отправителя в имейлах.*

Email Спуфинг – это

Выберите один вариант из списка

 Отлично!

- ☐ метод предотвращения фишинга
- ☒ подмена адреса отправителя в имейлах
- ☐ протокол для отправки имейлов
- ☐ атака перебором паролей

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.12: Скриншот выполнения задания

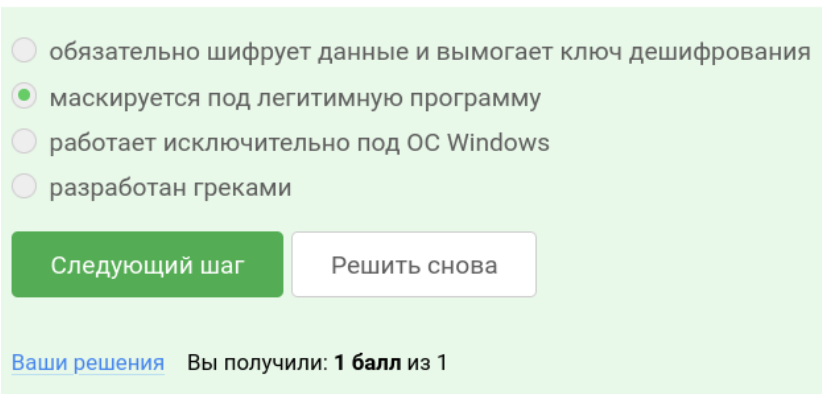
- Вопрос 2. Вирус-троян(рис. 2.13)

Ответ: *маскируется под легитимную программу.*

Вирус-троян

Выберите один вариант из списка

✓ Прекрасный ответ.



The screenshot shows a quiz interface with a light green background. At the top, the question "Вирус-троян" is displayed. Below it, the instruction "Выберите один вариант из списка" is shown. A green checkmark icon is followed by the text "Прекрасный ответ.". Below this, there is a list of four radio button options: "обязательно шифрует данные и требует ключ дешифрования", "маскируется под легитимную программу", "работает исключительно под ОС Windows", and "разработан греками". The second option is selected. At the bottom of the list, there are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). Below the buttons, the text "Ваши решения" (Your solutions) is followed by "Вы получили: 1 балл из 1" (You received: 1 point out of 1).

☐ обязательно шифрует данные и требует ключ дешифрования

☒ маскируется под легитимную программу

☐ работает исключительно под ОС Windows

☐ разработан греками

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.13: Скриншот выполнения задания

2.5 Безопасность мессенджеров

- Вопрос 1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?(рис. 2.14)

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

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Абсолютно точно.

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 2.14: Скриншот выполнения задания

- Вопрос 2. Суть сквозного шифрования состоит в том, что(рис. 2.15)

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

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Всё правильно.

- ☒ 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** из 1

Рис. 2.15: 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.