

Прохождения внешнего курса на тему Основы кибербезопасности. Часть 2

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	3	Защита ПК/телефона	5
1.1	3.1	Шифрование диска	5
1.2	3.2	Пароли	7
1.3	3.3	Фишинг	11
1.4	3.4	Беспроводные сети WiFi	13
1.5	3.5	Безопасность мессенджеров	14

Список иллюстраций

1.1	Вопрос/Ответ 1	5
1.2	Вопрос/Ответ 2	6
1.3	Вопрос/Ответ 3	7
1.4	Вопрос/Ответ 1	8
1.5	Вопрос/Ответ 2	9
1.6	Вопрос/Ответ 3	9
1.7	Вопрос/Ответ 4	10
1.8	Вопрос/Ответ 5	10
1.9	Вопрос/Ответ 6	11
1.10	Вопрос/Ответ 1	12
1.11	Вопрос/Ответ 2	13
1.12	Вопрос/Ответ 1	13
1.13	Вопрос/Ответ 2	14
1.14	Вопрос/Ответ 1	14
1.15	Вопрос/Ответ 2	15

Список таблиц

1 3 Защита ПК/телефона

1.1 3.1 Шифрование диска

Вопрос/Ответ 1 (рис. 1.1)

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Так точно!

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Рис. 1.1: Вопрос/Ответ 1

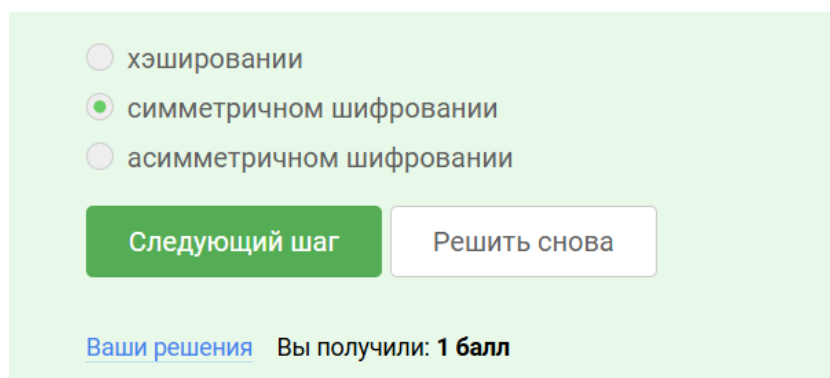
Пояснение ответа: Шифровать можно(и нужно) отдельные сектора диска(включая загрузочный сектор), флэшки с конфиденциальными данными.

Вопрос/Ответ 2 (рис. 1.2)

Шифрование диска основано на

Выберите один вариант из списка

☒ Прекрасный ответ.



☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг **Решить снова**

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

Рис. 1.2: Вопрос/Ответ 2

Пояснение ответа: Метод шифрования:

- Для процедуры Encrypt/Decrypt используется симметрические шифрования (AES)
- Данные шифруются секторами
- Шифрование ускоряется TMP криптопроцессом
- Шифровать можно и загрузочный сектор. При этом пользователь должен запомнить пароль для дешифрирование ключа.

Вопрос/Ответ 3 (рис. 1.3)

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Всё правильно.

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

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

Следующий шаг

Решить снова

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

Рис. 1.3: Вопрос/Ответ 3

Пояснение ответа: Программы, с которыми можно зашифровать жесткий диск: VeraCrypt, BitLocker, LUKS, FileVault.

1.2 3.2 Пароли

Вопрос/Ответ 1 (рис. 1.4)

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

☒ Хорошая работа.

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

Следующий шаг

Решить снова

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

Рис. 1.4: Вопрос/Ответ 1

Пояснение ответа: Пароль считается стойким если в нем используются множество видов символов(буквы, цифры, знаки, буквы в большом регистре), чем больше видов, тем больше нужно переборов, чтобы его взломать.

Вопрос/Ответ 2 (рис. 1.5)

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Хорошая работа.

☒ 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**

Рис. 1.5: Вопрос/Ответ 2

Пояснение ответа: Наиболее безопасным является хранение паролей именно в менеджерах паролей.

Вопрос/Ответ 3 (рис. 1.6)

Зачем нужна капча?

Выберите один вариант из списка

☒ Хорошие новости, верно!

Ве
Из

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 1.6: Вопрос/Ответ 3

Пояснение ответа: Капча проверяет пользователя не является ли он програм-

мой перебора данных для взлома, обычно используются разные методы, такие как: нахождения правильной картинки или набора букв/цифр. Итак, капча защищает от автоматизированных атак, направленные на получение несанкционированного доступа.

Вопрос/Ответ 4 (рис. 1.7)

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Отличное решение!

- ☐ 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**

Рис. 1.7: Вопрос/Ответ 4

Пояснение ответа: Хеширование паролей используется для того, чтобы не хранить пароли на сервере в открытом виде, это делается для безопасности.

Вопрос/Ответ 5 (рис. 1.8)

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

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 96
Из всех попыток

- ☒ Нет
- ☐ Да

Следующий шаг Решить снова

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

Рис. 1.8: Вопрос/Ответ 5

Пояснение ответа: Соль не поможет для улучшения стойкости паролей к атаке

перебором, если злоумышленник получил доступ к серверу, так как соль добавляется во время хеширования, но это никак не меняет пароль пользователя и он остается прежним, что позволяет злоумышленнику добраться до цели.

Вопрос/Ответ 6 (рис. 1.9)

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Верно решено
Из всех предложенных

✓ 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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 1.9: Вопрос/Ответ 6

Пояснение ответа: Меры защиты от утечек данных перебором:

- Использовать длинные пароли с символами алфавита разного регистра, цифрами, спец. символами
- Использовать менеджеры паролей для хранения
- Регулярное изменение пароли к критическим сервисам
- Использование разных паролей для разных сайтов, программ.

1.3 3.3 Фишинг

Вопрос/Ответ 1 (рис. 1.10)

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

✔ 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

Рис. 1.10: Вопрос/Ответ 1

Пояснение ответа: В ссылке <https://online.sberbank.wix.ru/CSAFront/index.do>:

- Домен wix.ru - это бесплатный хостинг, никак не связанный со Сбербанком.
- [online.sberbank](https://online.sberbank.wix.ru/CSAFront/index.do)- это всего лишь поддомен хостинга wix.ru, а не настоящий сайт Сбербанка, настоящий- sberbank.ru или online.sberbank.ru

В ссылке https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru:

- ucoz.ru- это также бесплатный конструктор сайтов
- [passport.yandex](https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru)- поддомен ucoz.ru

Вопрос/Ответ 2 (рис. 1.11)

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Правильно, молодец!

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Рис. 1.11: Вопрос/Ответ 2

Пояснение ответа: Фишинговый имейл может прийти от знакомого адреса, это называется ip или имейл spoofing- подмена адреса отправителя.

1.4 3.4 Беспроводные сети WiFi

Вопрос/Ответ 1 (рис. 1.12)

Email Спуфинг – это

Выберите один вариант из списка

☒ Верно. Так держать!

☐ метод предотвращения фишинга

☒ подмена адреса отправителя в имейлах

☐ атака перебором паролей

☐ протокол для отправки имейлов

Следующий шаг

Решить снова

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

Рис. 1.12: Вопрос/Ответ 1

Пояснение ответа: Email Спуфинг- это подмена адреса отправителя в имейлах.

Вопрос/Ответ 2 (рис. 1.13)

Вирус-троян

Выберите один вариант из списка

✓ Всё правильно.

- ☐ 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**

Рис. 1.13: Вопрос/Ответ 2

Пояснение ответа:

Троян- вирус, проникающий в систему под видом легитимного ПО.

1.5 3.5 Безопасность мессенджеров

Вопрос/Ответ 1 (рис. 1.14)

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Здорово, всё верно.

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

Следующий шаг Решить снова

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

Рис. 1.14: Вопрос/Ответ 1

Пояснение ответа: Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителя.

Вопрос/Ответ 2 (рис. 1.15)

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Всё получилось!

- ☒ 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

Рис. 1.15: Вопрос/Ответ 2

Пояснение ответа: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде.