

Внешний курс

Отчёт по разделу 2

Аскеров Александр Эдуардович

Содержание

1	Пункт 3.1	4
2	Пункт 3.2	6
3	Пункт 3.3	10
4	Пункт 3.4	12
5	Пункт 3.5	14

Список иллюстраций

1.1	Шифрование загрузочного сектора диска	4
1.2	Шифрование диска	5
1.3	Программы для шифрования жёсткого диска	5
2.1	Стойкие пароли	6
2.2	Безопасное место для хранения паролей	7
2.3	Смысл капчи	7
2.4	Хэширование паролей	8
2.5	Атака перебором	8
2.6	Меры защиты от атаки перебором	9
3.1	Фишинговые ссылки	10
3.2	Фишинговый имейл от знакомого адреса	11
4.1	Email Спуфинг	12
4.2	Вирус-троян	13
5.1	Этап формирования ключа шифрования в протоколе в Signal . . .	14
5.2	Сквозное шифрование	14

1 Пункт 3.1

Укажем, можно ли зашифровать загрузочный сектор диска.

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Всё получилось!

☐ Да

☐ Нет

Рис. 1.1: Шифрование загрузочного сектора диска

Выберем, на чём основано шифрование диска.

Шифрование диска основано на

Выберите один вариант из списка

☒ Прекрасный ответ.

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Рис. 1.2: Шифрование диска

Укажем, с помощью каких программ можно зашифровать жёсткий диск.

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

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

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

Рис. 1.3: Программы для шифрования жёсткого диска

2 Пункт 3.2

Выберем пароли, которые можно отнести к стойким.

Какие пароли можно отнести к стойким?

Выберите один вариант из списка

☒ Здорово, всё верно.

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

Рис. 2.1: Стойкие пароли

Нам подходит только тот пароль, в котором присутствуют буквы, символы, цифры, разный регистр, а также он должен быть достаточно длинным.

Выберем, где безопасно хранить пароли.

Где безопасно хранить пароли?

Выберите один вариант из списка



Всё получилось!

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

Рис. 2.2: Безопасное место для хранения паролей

Укажем, зачем нужна капча.

Зачем нужна капча?

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили **974** учащихся
Из всех попыток **77%** верных

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

Рис. 2.3: Смысл капчи

Укажем, для чего применяется хэширование паролей.

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Отлично!

- ☐ 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

Рис. 2.4: Хэширование паролей

Скажем, поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу.

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

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 967 учащихся
Из всех попыток 66% верных

- ☒ Нет
- ☐ Да

Рис. 2.5: Атака перебором

Скажем, какие меры защищают от утечек данных атакой перебором.

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных вопросы, или сравнить своё решение с другими на [форуме решен](#)

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

Рис. 2.6: Меры защиты от атаки перебором

3 Пункт 3.3

Выберем, какие из следующих ссылок являются фишинговыми.

Какие из следующих ссылок являются фишинговыми?

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](#).

- ☐ <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)

Рис. 3.1: Фишинговые ссылки

Эти ссылки являются фишинговыми, так как их доменные имена отличаются от настоящих доменных имён сайтов, на которые хочет зайти пользователь.

Скажем, может ли фишинговый имейл прийти от знакомого адреса.

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Правильно.

☐ Да

☐ Нет

Рис. 3.2: Фишинговый имейл от знакомого адреса

4 Пункт 3.4

Скажем, что такое Email Спуфинг.

Email Спуфинг – это

Выберите один вариант из списка



Так точно!

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

Рис. 4.1: Email Спуфинг

Выберем, как работает вирус-троян.

Вирус-троян

Выберите один вариант из списка

☒ Отличное решение!

- ☐ обязательно шифрует данные и вымогает ключ дешифрования
- ☒ маскируется под легитимную программу
- ☐ работает исключительно под ОС Windows
- ☐ разработан греками

Рис. 4.2: Вирус-троян

5 Пункт 3.5

Скажем, на каком этапе формируется ключ шифрования в протоколе в Signal.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

☒ Отличное решение!

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

Рис. 5.1: Этап формирования ключа шифрования в протоколе в Signal

Выберем суть сквозного шифрования.

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

☒ Отлично!

- ☒ 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

Рис. 5.2: Сквозное шифрование