

# **Внешний курс. Блок 2: Защита ПК/Телефона**

Основы информационной безопасности

Петрова Алевтина Александровна

## **Содержание**

### **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. 1).

3.1 Шифрование диска 3 из 5 шагов пройдено 1 из 3 баллов получен

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

✓ Правильно, молодец!

☒ Да  
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

### Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 2).

3.1 Шифрование диска 4 из 5 шагов пройдено 2 из 3 баллов получено

Шифрование диска основано на

Выберите один вариант из списка

✓ Отлично!

☐ хэшировании  
☒ симметричном шифровании  
☐ асимметричном шифровании

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

### Вопрос 3.1.2

Отмечены программы, с помощью которых можно зашифровать жесткий диск (рис. 3).

3.1 Шифрование диска 5 из 5 шагов пройдено 3 из 3 баллов получено

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Хорошие новости, верно!

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](#).

☒ VeraCrypt  
☒ BitLocker  
☐ Wireshark  
☐ Disk Utility

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

### Вопрос 3.1.3

## 2.2 Пароли

Стойкий пароль - тот, который тяжелее подобрать, он должен быть со спец. символами и длинный (рис. 4).

3.2 Пароли 4 из 9 шагов пройдено 1 из 6 баллов получен

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё правильно.

Верно решено  
Из всех правильных ответов

- ☐ qwerty12345
- ☐ iLOVECATS
- ☒ UQr9@j4iS\$
- ☐ iDONTLOVECATS

Следующий шаг Решить снова

### Вопрос 3.2.1

Все варианты, кроме менеджера паролей, совершенно не надежные (рис. 5).

3.2 Пароли 5 из 9 шагов пройдено 2 из 6 баллов получено

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Всё получилось!

Ваше решение  
Из всех правильных ответов

- ☒ 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

### Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном “не робот”(рис. 6).

3.2 Пароли 6 из 9 шагов пройдено 3 из 6 баллов получено

Зачем нужна капча?

Выберите один вариант из списка

✓ Отлично!

Верно решено  
Из всех правильных ответов

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

Следующий шаг Решить снова

### Вопрос 3.2.3

Опасно хранить пароли в открытом виде, поэтому хранят их хэши (рис. 7).

3.2 Пароли 7 из 9 шагов пройдено 4 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

☒ Хорошая работа.

☐ 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

Верно! Из всех попыток 66% верны

### Вопрос 3.2.4

Соль не поможет (рис. 8).

3.2 Пароли 8 из 9 шагов пройдено 5 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

☒ Правильно, молодец!

☐ Да

☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Верно решили 967 уч-щ Из всех попыток 66% верны

### Вопрос 3.2.5

Все приведенные меры защищают от утечек данных атакой перебором (рис. 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

☒ Здорово, всё 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: ...

Верно решили 1 Из всех попыток 66% верны

### Вопрос 3.2.6

## 2.3 Фишинг

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями (рис. 10).

3.3 Фишинг 3 из 5 шагов пройдено 1 из 2 баллов получен

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

✓ Отличное решение!

Верно решил 861 учащийся  
Из всех попыток 19% 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](#).

- ☐ <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](https://e.mail.ru/login?lang=ru_RU) (вход в аккаунт Mail.Ru)
- ☒ [https://passport.yandex.ucoz.ru/auth?origin=home\\_desktop\\_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

### Вопрос 3.3.1

Да, может, например, если пользователя со знакомым адресом взломали (рис. 11).

3.3 Фишинг 4 из 5 шагов пройдено 2 из 2 баллов получено

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

✓ Хорошая работа.

- ☒ Да
- ☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

### Вопрос 3.3.2

## 2.4 Вирусы. Примеры

Ответ дан в соответствии с определением (рис. 12).

3.4 Вирусы. Примеры 4 из 5 шагов пройдено 1 из 2 баллов получен

Email Спуфинг – это

Выберите один вариант из списка

☒ Так точно!

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

[Следующий шаг](#) [Решить снова](#)

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

### Вопрос 3.4.1

Трояны маскируются под обычную программу (рис. 13).

3.4 Вирусы. Примеры 5 из 5 шагов пройдено 2 из 2 баллов получено

Вирус-троян

Выберите один вариант из списка

☒ Верно.

☐ 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**

### Вопрос 3.4.2

## 2.5 Безопасность мессенджеров

При установке первого сообщения отправителем формируется ключ шифрования (рис. 14).

3.5 Безопасность мессенджеров 3 из 4 шагов пройдено 1 из 2 баллов получен

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

☒ Так точно!

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

[Следующий шаг](#) [Решить снова](#)

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

### Вопрос 3.5.1

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

☒ Хорошая работа.

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

Вопрос 3.5.2

## 3 Выводы

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