

# **Отчёт по Внешнему Курсу - Этап 2**

**Основы информационной безопасности**

Чистов Даниил Максимович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Выводы</b>	<b>12</b>
<b>4</b>	<b>Список литературы</b>	<b>13</b>

## Список иллюстраций

2.1	Задание 001	5
2.2	Задание 002	5
2.3	Задание 003	6
2.4	Задание 004	6
2.5	Задание 005	7
2.6	Задание 006	7
2.7	Задание 007	8
2.8	Задание 008	8
2.9	Задание 009	8
2.10	Задание 010	9
2.11	Задание 011	9
2.12	Задание 012	10
2.13	Задание 013	10
2.14	Задание 014	10
2.15	Задание 015	11

# **1 Цель работы**

Пройти внешний курс - Этап 2

## 2 Выполнение лабораторной работы

Да, можно, тогда перед самым запуском всей системы также потребуется ввести пароль (рис. 2.1).

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 949 учащихся  
Из всех попыток 89% верных

☒ Да  
☐ Нет

Следующий шаг    Решить снова

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

Рис. 2.1: Задание 001

Шифрование основано на алгоритме AES (рис. 2.2).

Шифрование диска основано на

Выберите один вариант из списка

☒ Так точно!

Верно решили 972 учащихся  
Из всех попыток 66% верных

☐ хэшировании  
☒ симметричном шифровании  
☐ асимметричном шифровании

Следующий шаг    Решить снова

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

Рис. 2.2: Задание 002

BitLocker - встроенный в Windows шифровщик, VeraCrypt - сторонняя утилита для шифрования данных (рис. 2.3).

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 своё решение с другими на [форуме решений](#).

Верно решили 906 учащихся  
Из всех попыток 28% верных

☒ BitLocker  
☐ Wireshark  
☐ Disk Utility  
☒ VeraCrypt

Следующий шаг
 Решить снова

[Ваши решения](#)
Вы получили: 1 балл

Рис. 2.3: Задание 003

Потому что есть латинские буквы - заглавные и не заглавные, а также цифры и особые символы (рис. 2.4).

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 969 учащихся  
Из всех попыток 85% верных

☐ qwerty12345  
☐ ILOVECATS  
☒ UQ!9@j4lS\$  
☐ IDONTLOVECATS

Следующий шаг
 Решить снова

[Ваши решения](#)
Вы получили: 1 балл

Рис. 2.4: Задание 004

Безопаснее всего хранить в менеджерах паролей, но для такого менеджера желательно всё-таки придумать очень хороший пароль и вот его придётся запомнить самому (рис. 2.5).

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Правильно.

Верно решил 971 учащихся  
Из всех попыток 74% верных

- ☒ 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. 2.5: Задание 005

Капча спасает от автоматизированных атак, правда в последнее время искусственный интеллект иногда справляется с такой защитой, иногда злоумышленники специально платят людьми за решение капчи(рис. 2.6).

Зачем нужна капча?

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 974 учащихся  
Из всех попыток 77% верных

- ☒ 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

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

Рис. 2.6: Задание 006

Делается это для того, чтобы не хранить пароли на сервере в открытом виде, ведь иногда злоумышленники могут устроить утечку данных, но хэширование не позволит злоумышленникам воспользоваться полученными данными, ведь их будет очень сложно расшифровать (рис. 2.7).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 973 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

Рис. 2.7: Задание 007

Нет, т.к. соль это тоже тип данных, который хранится на сервере, ну и если у злоумышленника есть доступ к серверу, значит и соль особо ему не поможет (рис. 2.8).

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

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решили 967 учащихся  
Из всех попыток 66% верных

☐ Да  
☒ Нет

Следующий шаг
 Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.8: Задание 008

Здесь все варианты подходят, как те, которые зависят именно от пользователя, так и от владельца хранилища паролей (сервера) (рис. 2.9).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

Верно решили 895 учащихся  
Из всех попыток 16% верных

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. 2.9: Задание 009



Первый вариант на первый взгляд содержит странные символы .br, однако это индикатор, что это страничка в Бразилии. Второй вариант действительно фишинговый, т.к. сделан на конструкторе сайтов wix.ru - сложно поверить, что такая крупная компания, как сбербанк делала бы свой сайт не самостоятельно с нуля. Третий, это просто рабочая ссылка Mail.ru, четвёртая - фишинговая, т.к. содержит подозрительные символы .ucoz (рис. 2.10).

Какие из следующих ссылок являются фишинговыми?

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](#).

Верно решил 861 учащийся  
Из всех попыток 19% верных

- ☐ <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

Рис. 2.10: Задание 010

Может, например, если адрес взломали, или может вы спутаете его со знакомым вам адресом (рис. 2.11).

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 966 учащихся  
Из всех попыток 90% верных

☒ Да

☐ Нет

Следующий шаг    Решить снова

Ваши решения    Вы получили: 1 балл

Рис. 2.11: Задание 011

Это не протокол для отправки имейлов, но email спуфинга связан с проблемой старых протоколов для отправки имейлов (рис. 2.12).

Email Спуфинг – это

Выберите один вариант из списка

☒ Верно.

Верно решили 960 учащихся  
Из всех попыток 65% верных

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.12: Задание 012

Оттого он и называется Троян (рис. 2.13).

Вирус-троян

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 969 учащихся  
Из всех попыток 74% верных

☐ 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. 2.13: Задание 013

Это происходит только при самом первом сообщении между пользователями (рис. 2.14).

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

☒ Правильно.

Верно решили 952 учащихся  
Из всех попыток 52% верных

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.14: Задание 014

Сервер лишь знает, кому эти сообщения нужно передать, а сами сообщения он не понимает (рис. 2.15).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

☒ Хорошие новости, 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**

Рис. 2.15: Задание 015

## **3 Выводы**

Этап 2 пройден успешно на максимальный балл.

## **4 Список литературы**

Курс “Основы Кибербезопасности” на платформе Stepik