

Внешний курс

Степик по основам безопасности

Воробьев Данил Павлович

Содержание

1 Блок 1	6
2 Цель работы	7
3 Выполнение заданий блока “Основы Кибербезопасности”	8
3.1 Как работает интернет: базовые сетевые протоколы	8
3.2 Персонализация сети	11
3.3 Браузер TOR. Анонимизация	13
3.4 Беспроводные сети Wi-fi	14
4 Блок 2	17
5 Цель работы	18
6 Выполнение заданий блока “Основы Кибербезопасности”	19
6.1 Шифрование диска	19
6.2 Пароли	20
6.3 Фишинг	22
6.4 Вирусы.	23
6.5 Безопасность мессенджеров	23
7 Выводы	25
8 Блок 3	26
9 Цель работы	27
10 Выполнение заданий блока “Основы Кибербезопасности”	28
10.1 Введение в криптографию	28
10.2 Цифровая подпись	30
10.3 Электронные платежи	32
10.4 Блокчейн	34
11 Выводы	36
12 Выводы	37

Список иллюстраций

3.1	Вопрос 2.1.1	8
3.2	Вопрос 2.1.2	9
3.3	Вопрос 2.1.3	9
3.4	Вопрос 2.1.4	9
3.5	Вопрос 2.1.5	10
3.6	Вопрос 2.1.6	10
3.7	Вопрос 2.1.7	10
3.8	Вопрос 2.1.8	11
3.9	Вопрос 2.1.9	11
3.10	Вопрос 2.2.1	12
3.11	Вопрос 2.2.2	12
3.12	Вопрос 2.2.3	12
3.13	Вопрос 2.2.4	13
3.14	Вопрос 2.3.1	13
3.15	Вопрос 2.3.2	13
3.16	Вопрос 2.3.3	14
3.17	Вопрос 2.3.4	14
3.18	Вопрос 2.4.1	15
3.19	Вопрос 2.4.2	15
3.20	Вопрос 2.4.3	15
3.21	Вопрос 2.4.4	16
3.22	Вопрос 2.4.5	16
6.1	Вопрос 3.1.1	19
6.2	Вопрос 3.1.2	19
6.3	Вопрос 3.1.3	20
6.4	Вопрос 3.2.1	20
6.5	Вопрос 3.2.2	20
6.6	Вопрос 3.2.3	21
6.7	Вопрос 3.2.4	21
6.8	Вопрос 3.2.5	21
6.9	Вопрос 3.2.6	22
6.10	Вопрос 3.3.1	22
6.11	Вопрос 3.3.2	22
6.12	Вопрос 3.4.1	23
6.13	Вопрос 3.4.2	23
6.14	Вопрос 3.5.1	23

6.15 Вопрос 3.5.1	24
10.1 Вопрос 4.1.1	28
10.2 Вопрос 4.1.2	29
10.3 Вопрос 4.1.3	29
10.4 Вопрос 4.1.4	29
10.5 Вопрос 4.1.5	30
10.6 Вопрос 4.2.1	30
10.7 Вопрос 4.2.2	30
10.8 Вопрос 4.2.3	31
10.9 Вопрос 4.2.4	31
10.10 Вопрос 4.2.5	32
10.11 Вопрос 4.3.1	32
10.12 Вопрос 4.3.2	33
10.13 Вопрос 4.3.3	33
10.14 Вопрос 4.4.1	34
10.15 Вопрос 4.4.2	35
10.16 Вопрос 4.4.3	35

Список таблиц

1 Блок 1

2 Цель работы

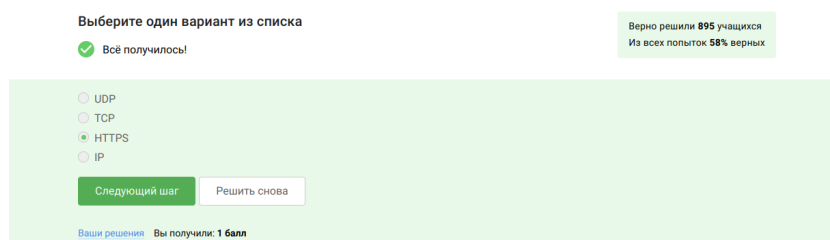
Выполнить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

3 Выполнение заданий блока

“Основы Кибербезопасности”

3.1 Как работает интернет: базовые сетевые протоколы

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS (рис. 3.1).



Выберите один вариант из списка

✓ Всё получилось!

Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

Ваши решения: Вы получили: 1 балл

Рис. 3.1: Вопрос 2.1.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. (рис. 3.2).

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 939 учащихся
Из всех попыток 61% верных

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.2: Вопрос 2.1.2

Т.к адрес состоит из большего набора чисел, а именно это 4 или 6 цифр от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно(рис. 3.3).

Выберите все подходящие ответы из списка

✓ Отлично!

Верно решил 871 учащийся
Из всех попыток 23% 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](#).

☐ 421.0.15.19
☐ 43.12.256.7
☒ 90.11.90.22
☒ 25.198.0.15

Следующий шаг Решить снова

Рис. 3.3: Вопрос 2.1.3

Основная задача DNS это сопоставлять название (доменное имя, с корректным IP-адресом) с тем, где лежит этот сервер, этот сайт. (рис. 3.4).

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 933 учащихся
Из всех попыток 66% верных

☒ сопоставляет IP адреса доменным именам
☐ сегментирует данные на транспортном уровне
☐ выбирает маршрут пакета в сети
☐ выполняет адресацию на хосте

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.4: Вопрос 2.1.4

Классификация протоколов в модели TCP/IP:

- Прикладной уровень: HTTP, RTSP, FTP, DNS.
- Транспортный уровень: TCP, UDP, SCTP, DCCP.

- Сетевой уровень: IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS(рис. 3.5).

Выберите один вариант из списка

✓ Так точно!

Верно решил 941 учащийся
Из всех попыток 53% верных

☐ сетевой – прикладной – канальный – транспортный
☐ прикладной – транспортный – канальный – сетевой
☐ транспортный – сетевой – прикладной – канальный
☒ прикладной – транспортный – сетевой – канальный

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. 3.6).

https передает зашифрованные данные, поэтому одна из фаз это передача данных, другая должна быть рукопожатием

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 965 учащихся
Из всех попыток 78% верных

☐ передачу зашифрованных данных между клиентом и сервером
☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.6: Вопрос 2.1.6

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. 3.7).

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 948 учащихся
Из всех попыток 41% верных

☐ одной фазы аутентификации сервера
☒ двух фаз: рукопожатия и передачи данных
☐ двух фаз: аутентификация клиента и сервера и шифрования данных
☐ трех фаз: аутентификация клиента, аутентификация сервера, генерация общего ключа

Следующий шаг Решить снова

Рис. 3.7: Вопрос 2.1.7

TLS определяется клиентом и сервером, чтобы возможно было подключиться (рис. 3.8).

Выберите один вариант из списка

Верно решили 947 учащихся
Из всех попыток 55% верных

☒ Правильно, молодец!

☐ сервером

☐ клиентом

☒ и клиентом, и сервером в процессе "переговоров"

☐ провайдером клиента

Следующий шаг Решить снова

Рис. 3.8: Вопрос 2.1.8

Фаза рукопожатия включает в себя:

- выбор параметров, протоколов
- аутентификация (как минимум, сервера)
- формируется общий секретный ключ К

Следовательно вариант с шифрованием лишний (рис. 3.9).

Выберите один вариант из списка

Верно решил 931 учащихся
Из всех попыток 44% верных

☒ Хорошая работа.

☐ формирование общего секретного ключа между клиентом и сервером

☐ аутентификация (как минимум одной из сторон)

☐ выбираются алгоритмы шифрования/аутентификации

☒ шифрование данных

Следующий шаг Решить снова

Рис. 3.9: Вопрос 2.1.9

3.2 Персонализация сети

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия пользователей (рис. 3.10).

Выберите все подходящие ответы из списка

✓ Верно. Так держаты!

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 **856** учащихся
Из всех попыток **18%** верных

☐ пароль пользователя
☒ идентификатор пользователя
☒ id сессии
☐ IP адрес

Следующий шаг Решить снова

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

Рис. 3.10: Вопрос 2.2.1

Куки не делают соединение надежным (рис. 3.11).

Выберите один вариант из списка

✓ Так точно!

Верно решили **950** учащихся
Из всех попыток **53%** верных

☐ аутентификации пользователя
☐ персонализации веб-страниц
☐ отслеживания информации о пользователе
☐ сборе статистики посещаемости сайта
☒ улучшения надежности соединения

Следующий шаг Решить снова

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

Рис. 3.11: Вопрос 2.2.2

Куки генерируются сервером(рис. 3.12).

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили **968** учащихся
Из всех попыток **79%** верных

☒ сервером
☐ клиентом

Следующий шаг Решить снова

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

Рис. 3.12: Вопрос 2.2.3

Куки бывают сессионные, удаляются при закрытии окна браузера (рис. 3.13).

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 959 учащихся
Из всех попыток 60% верных

☐ Нет

☐ Да, на некоторое время, заданное в сервером

☒ Да, на время пользования веб-сайтом

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

Рис. 3.13: Вопрос 2.2.4

3.3 Браузер TOR. Анонимизация

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три рутера, их не больше и не меньше (рис. 3.14).

Выберите один вариант из списка

✓ Так точно!

Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2

☒ 3

☐ 4

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранным и промежуточным узлам (рис. 3.15).

Выберите все подходящие ответы из списка

✓ Хорошая работа.

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 19% верных

☐ охранным узлу

☐ промежуточному узлу

☒ отправителю

☒ выходному узлу

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.15: Вопрос 2.3.2

В анонимных сетях, таких как Tor, общий секретный ключ для сквозного шиф-

рования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата. (рис. 3.16).

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 959 учащихся
Из всех попыток 55% верных

- ☐ только с охранным узлом
- ☐ с охранным и промежуточным узлом
- ☒ с охранным, промежуточным и выходным узлом
- ☐ с промежуточным и выходным узлом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.16: Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете. (рис. 3.17).

Выберите один вариант из списка

✓ Так точно!

Верно решил 961 учащийся
Из всех попыток 74% верных

- ☐ Да
- ☒ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.17: Вопрос 2.3.4

3.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. 3.18).

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 965 учащихся
Из всех попыток 79% верных

- ☐ сокращение от "wireless fiber"
- ☒ технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11
- ☐ метод соединения компьютеров по проводной сети Ethernet
- ☐ метод подключения смартфона с глобальной сети Интернет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.18: Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне (рис. 3.19).

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 972 учащихся
Из всех попыток 58% верных

- ☐ Транспортном
- ☐ Прикладном
- ☒ Канальном
- ☐ Сетевом

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.19: Вопрос 2.4.2

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется.(рис. 3.20).

Выберите один вариант из списка

✓ Отлично!

Верно решили 973 учащихся
Из всех попыток 60% верных

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.20: Вопрос 2.4.3

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляемую с помощью шифрования и аутентификации.(рис. 3.21).

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 53% верных

- ☐ передаются в открытом виде после аутентификации устройств
- ☐ передаются в открытом виде
- ☒ передаются в зашифрованном виде после аутентификации устройств
- ☐ передаются в зашифрованном виде

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.21: Вопрос 2.4.4

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций. (рис. 3.22).

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 975 учащихся
Из всех попыток 87% верных

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.22: Вопрос 2.4.5

4 Блок 2

5 Цель работы

Выполнить контрольные задания второго блока “Защита ПК/телефона” внешнего курса “Основы кибербезопасности”.

6 Выполнение заданий блока

“Основы Кибербезопасности”

6.1 Шифрование диска

Шифровать нужно не только жесткий диск, но и загрузочный сектор диска.
Ответ-можно (рис. 6.1).

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 949 учащихся
Из всех попыток 89% верных

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 6.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 6.2).

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 972 учащихся
Из всех попыток 66% верных

☐ хшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 6.2: Вопрос 3.1.2

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные

опенсорсные альтернативы, такие как VeraCrypt и PGPDisk. (рис. 6.3).

Вопрос 3.1.3: Какие из перечисленных программ являются открытыми (опенсорсными)?

✓ Все получилось!

Из всех попыток 28% 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.

☐ Disk Utility

☒ VeraCrypt

☒ BitLocker

☐ Wireshark

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.3: Вопрос 3.1.3

6.2 Пароли

Стойкий пароль содержит цифры строчные и заглавные буквы и специальные символы. Это усложняет перебор пароля (рис. 6.4).

Вопрос 3.2.1: Какой из перечисленных вариантов является сильным паролем?

✓ Так точно!

Верно решили 969 учащихся
Из всех попыток 85% верных

Выберите один вариант из списка

☐ qwerty12345

☐ ILOVECATS

☒ UQr9@j4IS\$

☐ IDONTLOVECATS

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.4: Вопрос 3.2.1

Безопасно хранить пароли нужно только в мессенджерах (рис. 6.5).

Вопрос 3.2.2: Где безопасно хранить пароли?

✓ Хорошие новости, верно!

Верно решил 971 учащийся
Из всех попыток 74% верных

Выберите один вариант из списка

☒ 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. 6.5: Вопрос 3.2.2

Капча - тест для определения, кто общается с веб-сервисом, человек или бот(рис. 6.6).

Выберите один вариант из списка

✓ Правильно.

Верно решили 974 учащихся
Из всех попыток 77% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.6: Вопрос 3.2.3

В целях безопасности пароли хранят не в открытом виде, а в виде хешей (рис. 6.7).

Выберите один вариант из списка

✓ Верно. Так держать!

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. 6.7: Вопрос 3.2.4

Соль - это метод защиты слабых паролей. Сервер добавляет соль к паролю пользователя. Это делает взлом слабых паролей сложнее (рис. 6.8).

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 967 учащихся
Из всех попыток 66% верных

- ☐ Да
- ☒ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.8: Вопрос 3.2.5

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в месенджерах паролей. (рис. 6.9).

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

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 **895** учащихся
Из всех попыток **16%** верных

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

Следующий шаг Решить снова

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

Рис. 6.9: Вопрос 3.2.6

6.3 Фишинг

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем (рис. 6.10).

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

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** учащихся
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 (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: ...

Рис. 6.10: Вопрос 3.3.1

Может фишинговое письмо прийти и от знакомого(рис. 6.11).

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили **966** учащихся
Из всех попыток **90%** верных

☒ Да

☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

Рис. 6.11: Вопрос 3.3.2

6.4 Вирусы.

Спуфинг - это подмена адреса отправителя в имейлах (рис. 6.12).

Выберите один вариант из списка

✓ Так точно!

Верно решили 960 учащихся
Из всех попыток 65% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.12: Вопрос 3.4.1

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его(рис. 6.13).

Выберите один вариант из списка

✓ Правильно.

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. 6.13: Вопрос 3.4.2

6.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. 6.14).

Выберите один вариант из списка

✓ Правильно.

Верно решили 952 учащихся
Из всех попыток 52% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 6.14: Вопрос 3.5.1

Сквозное шифрование позволяет передавать сообщения между пользователями (Алиса и Боб) так, что сервер знает только адресата, но не может прочитать содержимое. Алиса шифрует сообщение, сервер передает зашифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения. (рис. 6.15).

Выберите один вариант из списка

Верно решили **964** учащихся
Из всех попыток **60%** верных

☒ Абсолютно точно.

- ☒ 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. 6.15: Вопрос 3.5.1

7 Выводы

В результате я сделал второй блок курса “Основы кибербезопасности”. Узнал правила составления и хранения паролей, понял много нового о вирусах и мерах безопасности против них.

8 Блок 3

9 Цель работы

Выполнить контрольные задания третьего блока “Криптография на практике” внешнего курса “Основы кибербезопасности”.

10 Выполнение заданий блока

“Основы Кибербезопасности”

10.1 Введение в криптографию

В асимметричной криптографии у каждой из сторон есть пара ключей: открытый и секретный ключ (рис. 10.1).

Выберите один вариант из списка

Отлично!

Верно решили 940 учащихся
Из всех попыток 42% верных

- ☒ обе стороны имеют пару ключей
- ☐ обе стороны имеют общий секретный ключ
- ☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
- ☐ одна сторона публикует свой секретный ключ, другая – держит его в секрете

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.1: Вопрос 4.1.1

Криптографическая хэш-функция обладает важным свойством стойкости к коллизиям, что означает, что крайне сложно найти два разных входа, которые дают одинаковый хэш. Она принимает произвольный объем данных и выдает фиксированную строку заданной длины (например, n). Обычно функция сжимает данные, преобразуя большой набор информации в небольшое значение. (рис. 10.2).

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](#).

Верно решили **798** учащихся
Из всех попыток **11%** верных

- ☒ стойкая к коллизиям
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ эффективно вычисляется

Следующий шаг Решить снова

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

Рис. 10.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 10.3).

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](#).

Верно решили **834** учащихся
Из всех попыток **19%** верных

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

Следующий шаг Решить снова

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

Рис. 10.3: Вопрос 4.1.3

Код аутентификации сообщения (MAC) относится к симметричным примитивам, поскольку для его генерации и проверки используется общий секретный ключ, известный только отправителю и получателю, что обеспечивает целостность и аутентичность данных.(рис. 10.4).

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили **955** учащихся
Из всех попыток **69%** верных

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Следующий шаг Решить снова

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

Рис. 10.4: Вопрос 4.1.4

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана (рис. 10.5).

Выберите один вариант из списка

✓ Отлично!

Верно решили 948 учащихся
Из всех попыток 47% верных

☐ симметричный примитив генерации общего секретного ключа
☐ асимметричный примитив генерации общего открытого ключа
☒ асимметричный примитив генерации общего секретного ключа
☐ асимметричный алгоритм шифрования

Следующий шаг
 Решить снова

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

Рис. 10.5: Вопрос 4.1.5

10.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 10.6).

протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 956 учащихся
Из всех попыток 71% верных

☐ протоколам с симметричным ключом
☒ протоколам с публичным (или открытым) ключом

Следующий шаг
 Решить снова

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

Рис. 10.6: Вопрос 4.2.1

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. 10.7).

для проверки верификация электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Верно.

Верно решили 962 учащихся
Из всех попыток 46% верных

☐ подпись, секретный ключ
☐ подпись, открытый ключ
☐ подпись, секретный ключ, сообщение
☒ подпись, открытый ключ, сообщение

Следующий шаг
 Решить снова

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

Рис. 10.7: Вопрос 4.2.2

Цифровая подпись обеспечивает три ключевых функции:

1. Целостность сообщения — изменения в сообщении приводят к некорректной проверке подписи.
2. Аутентификация — позволяет установить, что подпись принадлежит конкретному владельцу.
3. Неотказ от авторства — подписавший не может отказаться от своей подписи.

Однако, если секретный ключ украден, безопасность подписи подрывается, и она не обеспечивает конфиденциальности.(рис. 10.8).

элементы цифровой подписи не обеспечивают

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 968 учащихся
Из всех попыток 53% верных

☐ аутентификацию
☐ целостность
☒ конфиденциальность
☐ неотказ от авторства

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.8: Вопрос 4.2.3

Усиленная квалифицированная подпись (УКЭП) имеет юридическую силу и равнозначна рукописной подписи. Для её получения необходимо обратиться в аккредитованный сертификационный центр с паспортом и другими данными. (рис. 10.9).

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Выберите один вариант из списка

✓ Верно. Так держат!

Верно решили 975 учащихся
Из всех попыток 68% верных

☐ простая
☐ усиленная неквалифицированная
☒ усиленная квалифицированная

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.9: Вопрос 4.2.4

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром. (рис. 10.10).

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

Отлично!

Верно решил 971 учащийся
Из всех попыток 61% верных

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 10.10: Вопрос 4.2.5

10.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. 10.11).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно.

Верно решили 900 учащихся
Из всех попыток 24% 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](#).

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 10.11: Вопрос 4.3.1

Основные категории вещей, которые мы можем использовать для доказательства своей идентичности:

1. Знание: Это что-то, что я знаю, например, пароль, PIN-код или секретный код для онлайн-платежей.

2. Владение: В онлайн-платежах используется второй фактор — это то, чем я владею, например, телефон, на который приходит код для подтверждения.
3. Свойства: Биометрические данные, такие как отпечаток пальца или сетчатка глаза, служат третьим фактором аутентификации.
4. Локация: Четвертый фактор аутентификации — это место, откуда осуществляется доступ, что также может быть учтено при проверке идентичности. (рис. 10.12).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Верно решили 896 учащихся
Из всех попыток 24% верных

Отлично!

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.

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверка пароля + код в sms сообщении
- ☒ комбинация код в sms сообщении + отпечаток пальца
- ☐ комбинация PIN код + пароль

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершает именно владелец карты или счета, а не злоумышленник(рис. 10.13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

Верно решили 957 учащихся
Из всех попыток 59% верных

Так точно!

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ однофакторная аутентификация покупателя перед банком-эквайером
- ☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- ☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.13: Вопрос 4.3.3

10.4 Блокчейн

Proof-of-Work (PoW) — это способ, который используется в блокчейне для подтверждения транзакций и создания новых блоков. В этом процессе майнеры (люди, которые занимаются добычей криптовалюты) соревнуются друг с другом за завершение транзакций в сети и за вознаграждение

Когда люди отправляют друг другу цифровые деньги, эти транзакции собираются в блоки и добавляются в общую базу данных, называемую блокчейном. Чтобы сделать сеть безопасной и защитить её от мошенничества, PoW требует много вычислительных ресурсов. Это значит, что для успешного участия в процессе нужно много мощных компьютеров.(рис. 10.14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Так точно!

Верно решили 932 учащихся
Из всех попыток 49% верных

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10.14: Вопрос 4.4.1

В основе любого блокчейна, включая биткоин, лежит консенсус — публичная структура данных (ledger), содержащая историю всех транзакций. Консенсус обеспечивает четыре ключевых свойства:

1. **Постоянство:** Добавленные данные не могут быть удалены.
2. **Согласованность:** Все участники видят и согласны с одними и теми же данными, за исключением последних изменений.
3. **Живучесть:** Возможность добавления новых транзакций в любое время.
4. **Открытость:** Любой желающий может стать участником блокчейна.

Эти свойства обеспечивают надежность и безопасность системы. (рис. 10.15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Хорошие новости, верно!

Верно решили 864 учащихся
Из всех попыток 23% 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](#).

- ☒ открытость
- ☒ консенсус
- ☒ постоянства
- ☒ живучесть

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 10.15: Вопрос 4.4.2

В блокчейне у каждого из трех участников есть секретный ключ, который они используют для подтверждения транзакций. Этот секретный ключ позволяет создавать цифровую подпись, которая служит доказательством того, что транзакция была инициирована конкретным участником. Цифровая подпись основана на паре ключей — секретном и открытом. Секретный ключ используется для подписания транзакции, а открытый ключ позволяет другим участникам проверить подлинность этой подписи. Таким образом, цифровая подпись обеспечивает безопасность и аутентичность транзакций в блокчейне. (рис. 10.16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решил 951 учащийся
Из всех попыток 48% верных

- ☐ обмен ключами
- ☐ шифрование
- ☒ цифровая подпись
- ☐ хэш-функция

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 10.16: Вопрос 4.4.3

11 Выводы

В результате 3 этапа я узнал много нового о криптографии, цифровых подписях и технологиях блокчейна. Выяснил как обеспечивается безопасность транзакций.

12 Выводы

В результате выполнения блока “Безопасность в сети” я узнал как работают сетевые протоколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.