

Внешний курс. Безопасность в сети

Дисциплина: Основы информационной безопасности

Нилова Кристина Артуровна

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	12
3.3	Браузер TOR. Анонимизация	13
3.4	Беспроводные сети Wi-fi	15
4	Блок 2	18
5	Цель работы	19
6	Выполнение заданий блока “Основы Кибербезопасности”	20
6.1	Шифрование диска	20
6.2	Пароли	21
6.3	Фишинг	24
6.4	Вирусы.	25
6.5	Безопасность мессенджеров	26
7	Выводы	28
8	Блок 3	29
9	Цель работы	30
10	Выполнение заданий блока “Основы Кибербезопасности”	31
10.1	Введение в криптографию	31
10.2	Цифровая подпись	33
10.3	Электронные платежи	36
10.4	Блокчейн	38
11	Выводы	40
12	Выводы	41

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	11
3.8	Вопрос 2.1.8	11
3.9	Вопрос 2.1.9	12
3.10	Вопрос 2.2.1	12
3.11	Вопрос 2.2.2	12
3.12	Вопрос 2.2.3	13
3.13	Вопрос 2.2.4	13
3.14	Вопрос 2.3.1	13
3.15	Вопрос 2.3.2	14
3.16	Вопрос 2.3.3	14
3.17	Вопрос 2.3.4	15
3.18	Вопрос 2.4.1	15
3.19	Вопрос 2.4.2	16
3.20	Вопрос 2.4.3	16
3.21	Вопрос 2.4.4	17
3.22	Вопрос 2.4.5	17
6.1	Вопрос 3.1.1	20
6.2	Вопрос 3.1.2	21
6.3	Вопрос 3.1.3	21
6.4	Вопрос 3.2.1	22
6.5	Вопрос 3.2.2	22
6.6	Вопрос 3.2.3	22
6.7	Вопрос 3.2.4	23
6.8	Вопрос 3.2.5	23
6.9	Вопрос 3.2.6	24
6.10	Вопрос 3.3.1	24
6.11	Вопрос 3.3.2	25
6.12	Вопрос 3.4.1	25
6.13	Вопрос 3.4.2	26
6.14	Вопрос 3.5.1	26

6.15 Вопрос 3.5.1	27
10.1 Вопрос 4.1.1	31
10.2 Вопрос 4.1.2	32
10.3 Вопрос 4.1.3	32
10.4 Вопрос 4.1.4	33
10.5 Вопрос 4.1.5	33
10.6 Вопрос 4.2.1	34
10.7 Вопрос 4.2.2	34
10.8 Вопрос 4.2.3	35
10.9 Вопрос 4.2.4	35
10.10 Вопрос 4.2.5	36
10.11 Вопрос 4.3.1	36
10.12 Вопрос 4.3.2	37
10.13 Вопрос 4.3.3	37
10.14 Вопрос 4.4.1	38
10.15 Вопрос 4.4.2	39
10.16 Вопрос 4.4.3	39

Список таблиц

1 Блок 1

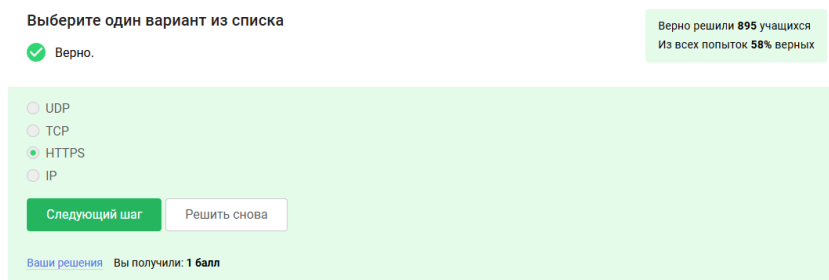
2 Цель работы

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

✓ Верно.

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).

На каком уровне работает протокол TCP?

Выберите один вариант из списка

✓ Всё получилось!

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 большого 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

✓ 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](#).

☐ 421.0.15.19
☐ 43.12.256.7
☒ 90.11.90.22
☒ 25.198.0.15

Следующий шаг
 Решить снова

[Ваши решения](#)

Рис. 3.3: Вопрос 2.1.3

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

Выберите один вариант из списка

✓ Правильно, молодец!

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

✓ Всё правильно.

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

✓ Правильно.

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: 

👍 102 🗣 13 Шаг 12 Следующий шаг >

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

✓ Верно. Так держать!

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: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 102 🗣️ 13 Шаг 13 Следующий шаг >

Рис. 3.7: Вопрос 2.1.7

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

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 947 учащихся
Из всех попыток 55% верных

☐ сервером
☐ клиентом
☒ и клиентом, и сервером в процессе "переговоров"
☐ провайдером клиента

Следующий шаг Решить снова

Ваши решения Вы получили: ...

Рис. 3.8: Вопрос 2.1.8

Фаза рукопожатия включает в себя:

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

Следовательно вариант с шифрованием лишний (рис. 3.9).

Выберите один вариант из списка

✓ Хорошая работа.

Верно решил 931 учащихся
Из всех попыток 44% верных

- ☐ формирование общего секретного ключа между клиентом и сервером
- ☐ аутентификация (как минимум одной из сторон)
- ☐ выбираются алгоритмы шифрования/аутентификации
- ☒ шифрование данных

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

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

✓ Прекрасный ответ.

Верно решили 856 учащихся
Из всех попыток 18% 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](#).

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

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

✓ Верно. Так держать!

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](#)

Рис. 3.11: Вопрос 2.2.2

Куки генерируются сервером(рис. 3.12).

Выберите один вариант из списка

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

☐ клиентом

☒ сервером

Следующий шаг

[Ваши решения](#) [Вы получили](#) 🏆

Рис. 3.12: Вопрос 2.2.3

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

Выберите один вариант из списка

Хорошая работа. Верно решили 959 учащихся
Из всех попыток 60% верных

☐ Да, на некоторое время, заданное в сервером

☐ Нет

☒ Да, на время пользования веб-сайтом

Следующий шаг

[Ваши решения](#)

👍 40 🗳 13 Шаг 6

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 роутера, их не больше и не меньше (рис. 3.14).

Выберите один вариант из списка

Всё правильно. Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2

☒ 3

☐ 4

Следующий шаг

[Ваши решения](#)

Рис. 3.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 3.15).

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](#).

Верно решили 906 учащихся
Из всех попыток 19% верных

- ☐ охранному узлу
- ☐ промежуточному узлу
- ☒ отправителю
- ☒ выходному узлу

Следующий шаг Решить снова

[Ваши решения](#)

Рис. 3.15: Вопрос 2.3.2

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

Правильно.

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).

Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

Выберите один вариант из списка

☒ Всё получилось!

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).

Wi-Fi - это

Выберите один вариант из списка

☒ Верно.

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

Рис. 3.18: Вопрос 2.4.1

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

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Всё правильно.

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).

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

Ваши решения

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).

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✔ Отлично!

Верно решили 975 учащихся
Из всех попыток 53% верных

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

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✔ Всё получилось!

Верно решили 975 учащихся
Из всех попыток 87% верных

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 🏆

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).

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Да

☐ Нет

Здорово, всё верно.

Верно решили 949 учащихся
Из всех попыток 89% верных

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).

Шифрование диска основано на

Выберите один вариант из списка

✓ Правильно, молодец!

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. 6.2: Вопрос 3.1.2

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные open-source альтернативы, такие как VeraCrypt и PGPDisk. (рис. 6.3).

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Хорошие новости, верно!

Верно решили 906 учащихся
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](#).

☒ BitLocker
☐ Wireshark
☐ Disk Utility
☒ VeraCrypt

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).

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Правильно.

Верно решили 969 учащихся
Из всех попыток 85% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 6.4: Вопрос 3.2.1

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

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Всё получилось!

Верно решил 971 учащийся
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

👍 44 🗣 8 Шаг 5

Следующий шаг >

Рис. 6.5: Вопрос 3.2.2

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

Зачем нужна капча?

Выберите один вариант из списка

✓ Так точно!

Верно решили 974 учащихся
Из всех попыток 77% верных

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

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).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

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. 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).

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 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).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

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

✓ Правильно, молодец!

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. 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).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно решил **861** учащихся
Из всех попыток **19%** верных

✓ 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](#).

- ☐ <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. 6.10: Вопрос 3.3.1

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

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 966 учащихся
Из всех попыток 90% верных

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 6.11: Вопрос 3.3.2

6.4 Вирусы.

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

Email Спуфинг – это

Выберите один вариант из списка

✓ Отлично!

Верно решили 960 учащихся
Из всех попыток 65% верных

☐ протокол для отправки имейлов
☒ подмена адреса отправителя в имейлах
☐ метод предотвращения фишинга
☐ 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).

Вирус-троян

Выберите один вариант из списка

✓ Отличное решение!

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).

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. 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).

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. 6.15: Вопрос 3.5.1

7 Выводы

В результате я сделала второй блок курса “Основы кибербезопасности”. Узнала правила составления и хранения паролей, поняла 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).

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Верно.

Верно решили 940 учащихся
Из всех попыток 42% верных

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

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).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 798 учащихся
Из всех попыток 11% верных

✓ Так точно!

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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

Рис. 10.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 10.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили 834 учащихся
Из всех попыток 19% верных

✓ 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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

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).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 955 учащихся
Из всех попыток 69% верных

☒ симметричным примитивам
☐ асимметричным 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).

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Верно.

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: ...

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

✓ Хорошая работа.

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

28 3 Шаг 4 Следующий шаг >

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).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Правильно.

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

28 3 Шаг 5 Следующий шаг >

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).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Верно.

Верно решили 968 учащихся
Из всех попыток 53% верных

☐ неотказ от авторства
☐ целостность
☒ конфиденциальность
☐ аутентификацию

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

✓ Отлично!

Верно решили 975 учащихся
Из всех попыток 68% верных

☒ усиленная квалифицированная
☐ усиленная неквалифицированная
☐ простая

Следующий шаг Решить снова

Ваши решения Вы получили: ...

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

☒ Так точно!

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

☒ 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](#).

☐ 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. 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 **896** учащихся
Из всех попыток **24%** верных

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверки 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

✓ Отличное решение!

Верно решили **957** учащихся
Из всех попыток **59%** верных

- ☒ 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**

👍 25 🗨 2 Шаг 5 Следующий шаг >

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

✓ Отлично!

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

✓ Отличное решение!

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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

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

✓ Правильно, молодец!

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 узнала много нового о криптографии, цифровых подписях и технологиях блокчейна. Выяснила, как обеспечивается безопасность транзакций.

12 Выводы

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