

Внешний курс. Часть 1: Безопасность в сети

Основы информационной безопасности

Александрова У.В.

Содержание

1	Цель работы	3
2	Выполнение заданий	4
2.1	Как работает интернет: базовые сетевые протоколы	4
2.2	Персонализация сети	7
2.3	Браузер TOR	8
2.4	Беспроводные сети Wi-fi	10
3	Выводы	12

1 Цель работы

Цель работы - выполнить контрольные задания первого раздела курса “Основы Кибербезопасности”

2 Выполнение заданий

2.1 Как работает интернет: базовые сетевые протоколы

HTTPS - протокол прикладного уровня (рис. 2.1).

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

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

Рис. 2.1: Вопрос 2.1.1

Transmission control protocol работает на транспортном уровне (рис. 2.2).

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 939 учащихся
Из всех попыток 61% верных

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

Следующий шаг Решить снова

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

Рис. 2.2: Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255 (рис. 2.3).

Выберите все подходящие ответы из списка

✓ Отличное решение!

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](#).

Верно решил 871 учащийся
Из всех попыток 23% верных

☐ 421.0.15.19
☐ 43.12.256.7
☒ 90.11.90.22
☒ 25.198.0.15

Следующий шаг Решить снова

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

Рис. 2.3: Вопрос 2.1.3

DNS-сервер (рис. 2.4).

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 из 1

Рис. 2.4: Вопрос 2.1.4

Распределение протоколов в модели TCP/IP:

- Прикладной уровень: HTTP, RTSP, FTP, DNS.
- Транспортный уровень: TCP, UDP, SCTP, DCCP.
- Сетевой (Межсетевой) уровень: IP.
- Уровень сетевого доступа (Канальный): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS. (рис. 2.5).

Выберите один вариант из списка

✓ Всё получилось!

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 из 1

Рис. 2.5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные (а https передает уже зашифрованные) (рис. 2.6).

Выберите один вариант из списка

✓ 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 из 1

Рис. 2.6: Вопрос 2.1.6

Https передает зашифрованные данные, поэтому одна из фаз - передача данных, другая должна быть рукопожатием (рис. 2.7).

Выберите один вариант из списка

✓ Здорово, всё верно.

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: 1 балл из 1

Рис. 2.7: Вопрос 2.1.7

TLS определяется как клиентом, так и сервером (рис. 2.8).

Выберите один вариант из списка

✓ Верно.

Верно решили 931 учащийся
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 из 1

Рис. 2.8: Вопрос 2.1.8

Шифрование данных (рис. 2.9).

Выберите один вариант из списка

✓ Абсолютно точно.

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, аутентификации сервера, генерация общего ключа

Следующий шаг Решить снова

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

Рис. 2.9: Вопрос 2.1.9

2.2 Персонализация сети

Куки хранят ID сессии и идентификатор (рис. 2.10).

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

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](#).

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

Следующий шаг Решить снова

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

Рис. 2.10: Вопрос 2.2.1

Куки не делают соединение более надежным, даже наоборот (рис. 2.11).

Выберите один вариант из списка

✓ Правильно.

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 из 1

Рис. 2.11: Вопрос 2.2.2

Куки генерируются сервером (рис. 2.12).

Выберите один вариант из списка

✓ Так точно!

Верно решили 968 учащихся
Из всех попыток 79% верных

- ☒ сервером
- ☐ клиентом

Следующий шаг Решить снова

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

Рис. 2.12: Вопрос 2.2.3

Сессионные куки хранятся лишь в течение сессии (рис. 2.13).

Выберите один вариант из списка

✓ Правильно.

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 Решить снова

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

Рис. 2.13: Вопрос 2.2.4

2.3 Браузер TOR

Необходимо три узла: входной, промежуточный и выходной (рис. 2.14).

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2
☒ 3
☐ 4

Следующий шаг

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

Рис. 2.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 2.15).

Выберите все подходящие ответы из списка

✓ Правильно.

Верно решили 906 учащихся
Из всех попыток 19% 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](#).

☐ охранному узлу
☐ промежуточному узлу
☒ отправителю
☒ выходному узлу

Следующий шаг

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

Рис. 2.15: Вопрос 2.3.2

Отправитель генерирует общий секретный ключ с узлами, через которые идет передача, то есть со всеми (рис. 2.16).

Выберите один вариант из списка

✓ Хорошие новости, верно!

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

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

Рис. 2.16: Вопрос 2.3.3

Для получения пакетов не обязательно использовать TOR (рис. 2.17).

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решил 961 учащийся
Из всех попыток 74% верных

☐ Да

☒ Нет

Следующий шаг Решить снова

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

Рис. 2.17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

Wi-Fi (рис. 2.18).

Выберите один вариант из списка

✓ Всё правильно.

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 из 1

Рис. 2.18: Вопрос 2.4.1

Wi-Fi располагается как канальный уровень ниже интернет-уровня интернет-протокола (рис. 2.19).

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 из 1

Рис. 2.19: Вопрос 2.4.2

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности (рис. 2.20).

Выберите один вариант из списка

✓ Правильно.

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

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

Рис. 2.20: Вопрос 2.4.3

Нужно аутентифицировать устройства, а потом передать зашифрованные данные (рис. 2.21).

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 975 учащихся
Из всех попыток 53% верных

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

Следующий шаг Решить снова

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

Рис. 2.21: Вопрос 2.4.4

WPA2 Personal для личного использования, а enterprise - для предприятий (рис. 2.22).

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 975 учащихся
Из всех попыток 87% верных

☒ WPA2 Personal
☐ WPA2 Enterprise

Следующий шаг Решить снова

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

Рис. 2.22: Вопрос 2.4.5

3 Выводы

Я выполнила задания первого раздела внешнего курса и получила знания о работе базовых сетевых протоколов, куки сетей Wi-Fi и браузера TOR.

Внешний курс. Часть 2: Защита ПК/Телефона

Основы информационной безопасности

Александрова У.В.

Содержание

1	Цель работы	3
2	Выполнение блока 2: Защита ПК/Телефона	4
2.1	Шифрование диска	4
2.2	Пароли	5
2.3	Фишинг	7
2.4	Вирусы. Примеры	8
2.5	Безопасность мессенджеров	8
3	Выводы	10

1 Цель работы

Цель работы - выполнение контрольных заданий второго раздела курса “Основы Кибербезопасности”.

2 Выполнение блока 2: Защита ПК/Телефона

2.1 Шифрование диска

Зашифровать загрузочный сектор диска можно (рис. 2.1).

Выберите один вариант из списка

✓ Отлично!

Верно решили 949 учащихся
Из всех попыток 89% верных

☒ Да
☐ Нет

Следующий шаг Решить снова

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

Рис. 2.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 2.2).

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 972 учащихся
Из всех попыток 66% верных

☐ хэшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг Решить снова

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

Рис. 2.2: Вопрос 3.1.2

С помощью этих программ можно зашифровать жесткий диск (рис. 2.3).

Выберите все подходящие ответы из списка

Отлично!

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 свое решение с другими на форуме решений.

☐ Wireshark
☒ VeraCrypt
☒ BitLocker
☐ Disk Utility

Следующий шаг
 Решить снова

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

Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

Стойкий пароль должен быть со специальными символами и достаточной длины (рис. 2.4).

Выберите один вариант из списка

Здорово, всё верно.

Верно решили 969 учащихся
Из всех попыток 85% верных

☐ qwerty12345
☐ ILOVECATS
☒ UQr9@4IS\$
☐ IDONTLOVECATS

Следующий шаг
 Решить снова

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

Рис. 2.4: Вопрос 3.2.1

Менеджер паролей - это самый безопасный вариант (рис. 2.5).

Выберите один вариант из списка

Правильно, молодец!

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 из 1

Рис. 2.5: Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном не бот (рис. 2.6).

Выберите один вариант из списка

✓ Отличное решение!

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 из 1

Рис. 2.6: Вопрос 3.2.3

Опасно хранить пароли в открытом виде, для этого есть хэши (рис. 2.7).

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 из 1

Рис. 2.7: Вопрос 3.2.4

Соль не может помочь для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу (рис. 2.8).

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 из 1

Рис. 2.8: Вопрос 3.2.5

Все приведенные меры верны (рис. 2.9).

Выберите все подходящие ответы из списка

Верно решили 895 учащихся
Из всех попыток 16% 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](#).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.9: НВопрос 3.2.6

2.3 Фишинг

В фишинговых ссылках есть отличия (рис. 2.10).

Выберите все подходящие ответы из списка

Верно решил 861 учащийся
Из всех попыток 19% верных

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](#).

- ☐ <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 из 1

Рис. 2.10: Вопрос 3.3.1

Да, может, если пользователя со знакомым адресом взломали (рис. 2.11).

Выберите один вариант из списка

Верно решили 966 учащихся
Из всех попыток 90% верных

Правильно.

- ☒ Да
- ☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

Email Спуфинг – это (рис. 2.12).

Email Спуфинг – это

Выберите один вариант из списка

✔ Правильно, молодец!

Верно решили 960 учащихся
Из всех попыток 65% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

Вирус-троян

Выберите один вариант из списка

✔ Отлично!

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 из 1

Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

При установке первого сообщения отправителем формируется ключ шифрования (рис. 2.14).

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Прекрасный ответ.

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** из 1

Рис. 2.14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде (рис. 2.15).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Верно. Так держать!

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** из 1

Рис. 2.15: Вопрос 3.5.2

3 Выводы

Я прошла второй раздел внешнего курса и получила знания о правилах хранения паролей и основную информацию о вирусах.

Внешний курс. Раздел 3: Криптография на практике

Основы информационной безопасности

Александрова У.В.

Содержание

1	Цель работы	3
2	Выполнение блока 3: Криптография на практике	4
2.1	Введение в криптографию	4
2.2	Цифровая подпись	6
2.3	Электронные платежи	8
2.4	Блокчейн	9
3	Выводы	11

1 Цель работы

Цель работы - выполнить контрольные задания третьего раздела курса “Основы Кибербезопасности”.

2 Выполнение блока 3: Криптография на практике

2.1 Введение в криптографию

Определение асимметричного шифрования с двумя ключами (рис. 2.1).

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решили 940 учащихся
Из всех попыток 42% верных

- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☒ 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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.1: Вопрос 4.1.1

Условия криптографической хэш-функции (рис. 2.2).

Криптографическая хэш-функция

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 798 учащихся
Из всех попыток 11% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.2: Вопрос 4.1.2

Алгоритмы цифровой подписи (рис. 2.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ 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](#).

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 из 1

Рис. 2.3: Вопрос 4.1.3

Аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (рис. 2.4)

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Всё получилось!

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 955 учащихся
Из всех попыток 69% верных

☐ асимметричным примитивам
☒ симметричным примитивам

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.4: Вопрос 4.1.4

Обмен ключам Диффи-Хэллмана - это (рис. 2.5).

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Всё правильно.

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 из 1

Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

Протокол ЭЦП относится к протоколам с публичным ключом (рис. 2.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 947 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 из 1

Рис. 2.6: Вопрос 4.2.1

Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ и сообщение (рис. 2.7).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 943 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 из 1

Рис. 2.7: Вопрос 4.2.2

Электронная подпись не обеспечивает обеспечивает конфиденциальность (рис. 2.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Так точно!

Верно решили 944 учащихся
Из всех попыток 52% верных

- ☐ аутентификацию
- ☐ неотказ от авторства
- ☐ целостность
- ☒ конфиденциальность

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 2.9).

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

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 944 учащихся
Из всех попыток 68% верных

- ☐ простая
- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.9: Вопрос 4.2.4

В удостоверяющем (сертификационном) центре можно получить квалифицированный сертификат ключа проверки электронной подписи (рис. 2.10).

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

Выберите один вариант из списка

Верно решили 942 учащихся
Из всех попыток 60% верных

☒ Так точно!

☐ 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 из 1

Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

MasterCard, МИР - платежные системы (рис. 2.11).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно решили 873 учащихся
Из всех попыток 24% верных

☒ Правильно, молодец!

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](#).

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Следующий шаг Решить снова

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

Рис. 2.11: Вопрос 4.3.1

Примеры многофакторной аутентификации (рис. 2.12).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Абсолютно точно.

Верно решили **859** 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](#).

- ☐ 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** из 1

Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 2.13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Правильно.

Верно решили **918** 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** из 1

Рис. 2.13: Вопрос 4.3.3

2.4 Блокчейн

PoW (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне (рис. 2.14).

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 из 1

Рис. 2.14: Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети (рис. 2.15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

Верно решили 845 учащихся
Из всех попыток 23% 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](#).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.15: Вопрос 4.4.2

Цифровая подпись (рис. 2.16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 932 учащихся
Из всех попыток 47% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.16: Вопрос 4.4.3

3 Выводы

Я прошла третий раздел внешнего курса и получила полезные знания.