

Отчёт по прохождению внешнего курса

Основы информационной безопасности

Бережной Иван Александрович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение тестов	7
3.1	Прохождение первого этапа	7
3.2	Прохождение второго этапа	15
3.3	Прохождение третьего этапа	22
3.4	Сертификат	28
4	Выводы	29

Список иллюстраций

3.1	Протокол прикладного уровня	7
3.2	Уровень работы протокола TCP	8
3.3	Корректные IP	8
3.4	Функция DNS	8
3.5	Последовательность уровней TCP/IP	9
3.6	HTTP	9
3.7	HTTPS	10
3.8	TLS определяется всеми	10
3.9	TLS	10
3.10	Содержимое куки	11
3.11	Куки не используется для	11
3.12	Где генерируются куки	12
3.13	Сессионные куки	12
3.14	Количество узлов TOR	12
3.15	Скрытие IP	13
3.16	Множественные ключи	13
3.17	Одностороннее использование TOR	13
3.18	Определение Wi-Fi	14
3.19	Уровень работы Wi-Fi	14
3.20	Небезопасный метод шифрования	14
3.21	Передача данных Wi-Fi	15
3.22	Метод аутентификации в домашней сети	15
3.23	Возможность шифровки загрузочного сектора диска	16
3.24	Симметричное шифрование диска	16
3.25	Программы для шифрования диска	16
3.26	Устойчивые к брутфорсу пароли	17
3.27	Безопасное место для хранения паролей	17
3.28	Капча	18
3.29	Хэширование паролей	18
3.30	Соль	18
3.31	Методы защиты данных от утечек	19
3.32	Фишинговые ссылки	19
3.33	Фишинговый имейл	20
3.34	Имейл спуфинг	20
3.35	Вирус-троян	20
3.36	Signal	21
3.37	Суть сквозного шифрования	21

3.38 Ассиметричные криптографические примитивы	22
3.39 Криптографическая хэш-функция	22
3.40 Алгоритмы цифровой подписи	23
3.41 Код аутентификации сообщения	23
3.42 Обмен ключами Диффи-Хеллмена	23
3.43 Протокол электронной цифровой подписи	24
3.44 Верификация ЭЦП	24
3.45 ЭЦП не обеспечивает	25
3.46 Тип ЭЦП для отправки налоговой отчётности в ФНС	25
3.47 СА	25
3.48 Платёжные системы	26
3.49 Примеры многофакторной аутентификации	26
3.50 Аутентификация при онлайн платежах	27
3.51 Proof of work	27
3.52 Consensus	27
3.53 Что хранят участники блокчейна	28
3.54 “Сертификат”	28

1 Цель работы

Ознакомиться с основными понятиями информационной безопасности

2 Задание

Пройти все этапы курса

3 Выполнение тестов

Поскольку тестов в совокупности не так много, а на отдельных этапах их вообще мало, я решил, что более целесообразно будет сделать один отчёт по прохождению всего курса, нежели делать множество отчётов по каждому этапу.

3.1 Прохождение первого этапа

Протоколом прикладного уровня является HTTPS, поскольку он устанавливает правила общения с внешним ресурсом (рис. 3.1).

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Здорово, всё 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: Протокол прикладного уровня

Протокол TCP работает на транспортном уровне, поскольку определяет правила передачи пакетов (рис. 3.2).

На каком уровне работает протокол TCP?

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

Рис. 3.2: Уровень работы протокола TCP

Валидными IP-адресами считаются адреса, содержащие 4 октета, каждый из которых состоит из чисел в диапазоне от 0 до 255 (рис. 3.3).

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

✓ Отличное решение!

Верно решил 871 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](#).

☐ 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

Рис. 3.3: Корректные IP

DNS - специальные сервера, которые сообщают устройству, какой IP привязан к домену (рис. 3.4).

DNS сервер

Выберите один вариант из списка

✓ Здорово, всё верно.

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: Функция DNS

Последовательность протоколов определяется абстрактной моделью OSI (рис. 3.5).

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Хорошие новости, верно!

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: Последовательность уровней TCP/IP

HTTP не шифрует данные (рис. 3.6).

Протокол http предполагает

Выберите один вариант из списка

✓ Правильно, молодец!

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: HTTP

Для успешной передачи данных в протоколе HTTPS была реализована двух-фазная передача, состоящая из рукопожатия и непосредственно передачи (рис. 3.7).

Протокол https состоит из

Выберите один вариант из списка

✓ Всё правильно.

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

Рис. 3.7: HTTPS

В каждом устройстве определена своя версия протокола TLS. При общении выбирается наименьшая, поскольку присутствует поддержка обратной совместимости (рис. 3.8).

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Хорошие новости, 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

Рис. 3.8: TLS определяется всеми

Шифрование данных происходит после рукопожатия (рис. 3.9).

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Правильно.

Верно решил 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

Рис. 3.9: TLS

Куки не хранят чувствительные данные, поскольку их не составляет труда перехватить (рис. 3.10).

Куки хранят:

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.10: Содержимое куки

Куки не используются для улучшения надёжности соединения, поскольку создавались с другой целью (рис. 3.11).

Куки не используются для

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 надёжности соединения

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.11: Куки не используется для

Куки генерируются сервером в ходе общения с пользователем, затем отправляются этому пользователю и хранятся на его хосте (рис. 3.12).

Куки генерируются

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 968 учащихся
Из всех попыток 79% верных

☐ клиентом

☒ сервером

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.12: Где генерируются куки

Сессионные куки хранятся до тех пор, пока эта сессия не завершится. Отсюда и название (рис. 3.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 959 учащихся
Из всех попыток 60% верных

☐ Да, на некоторое время, заданное в сервером

☒ Да, на время пользования веб-сайтом

☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.13: Сессионные куки

В луковой маршрутизации используется 3 ноды (рис. 3.14).

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

✓ Правильно, молодец!

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: Количество узлов TOR

Благодаря тройному шифрованию адрес получателя известен только отправителю и выходной ноде. Таким образом ни одна нода не обладает полной информацией о всех участниках “общения” (рис. 3.15 и рис. 3.16).

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

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

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.15: Скрытие IP

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Отлично!

Верно решили 959 учащихся
Из всех попыток 55% верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.16: Множественные ключи

Получателю необязательно использовать Tor при общении, поскольку всю дешифровку осуществляют ноды (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

✓ Здорово, всё верно.

Верно решил 961 учащийся
Из всех попыток 74% верных

- ☒ Нет
- ☐ Да

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.17: Одностороннее использование TOR

Определение Wi-Fi (рис. 3.18).

Wi-Fi - это

Выберите один вариант из списка

✓ Здорово, всё 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](#) Вы получили: 1 балл

Рис. 3.18: Определение Wi-Fi

Wi-Fi работает на канальном уровне, поскольку связывает локальные устройства с интернетом (рис. 3.19).

На каком уровне работает протокол Wi-Fi?

Выберите один вариант из списка

✓ Здорово, всё верно.

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: Уровень работы Wi-Fi

WEP считается устаревшим и небезопасным, потому что его ключ шифрования ограничен 40 битами (рис. 3.20).

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Правильно, молодец!

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: Небезопасный метод шифрования

Данные между хостом и роутером передаются в зашифрованном виде, дабы исключить использование данных при перехвате (рис. 3.21).

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Хорошие новости, верно!

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: Передача данных Wi-Fi

Для домашней сети используется WPA2 Personal, поскольку это удобнее для пользователей, ведь Enterprise использует динамические ключи (рис. 3.22).

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Так точно!

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: Метод аутентификации в домашней сети

3.2 Прохождение второго этапа

Загрузочный сектор диска можно и рекомендуется шифровать (рис. 3.23).

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Так точно!

Верно решили 949 учащихся
Из всех попыток 89% верных

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.23: Возможность шифровки загрузочного сектора диска

Шифрование дисков симметричное, поскольку оно гораздо быстрее асимметричного, что идёт в плюс пользователям (рис. 3.24).

Шифрование диска основано на

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 972 учащихся
Из всех попыток 66% верных

☐ хэшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.24: Симметричное шифрование диска

BitLocker установлен в Windows по умолчанию, а VeraCrypt является наиболее популярной сторонней программой для шифрования дисков (рис. 3.25).

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Правильно, молодец!

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](#).

☐ Disk Utility
☐ Wireshark
☒ VeraCrypt
☒ BitLocker

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.25: Программы для шифрования диска

Пароли должны состоять из цифр, символов и спец. символов, чтобы подобрать было труднее (рис. 3.26).

Какие пароли можно отнести к стойким?

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 969 учащихся
Из всех попыток 85% верных

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQ*9@j4!s\$
- ☐ IDONTLOVECATS

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.26: Устойчивые к брутфорсу пароли

Пароли безопасно хранить в менеджере паролей, а пароль от него самого нужно хранить на нецифровом носителе или в голове (рис. 3.27).

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Прекрасный ответ.

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

Рис. 3.27: Безопасное место для хранения паролей

Капча используется для защиты от брутфорса ботами (рис. 3.28).

Зачем нужна капча?

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
- ☐ Для безопасного хранения паролей на сервере
- ☐ Она заменяет пароли

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.28: Капча

Хэширование паролей нужно, чтобы сделать потенциальные утечки баз данных менее опасными (рис. 3.29).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Правильно, молодец!

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. 3.29: Хэширование паролей

Соль помогает изменить хэш слабого пароля, но это не защищает от перебора (рис. 3.30).

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

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 967 учащихся
Из всех попыток 66% верных

- ☒ Нет
- ☐ Да

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.30: Соль

Все методы, которые усложняют пароль или замедляют возможность перебора, помогут защитить от брутфорса (рис. 3.31).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

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

✓ 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](#).

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

Следующий шаг Решить снова

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

Рис. 3.31: Методы защиты данных от утечек

Фишинговые ссылки похожи на настоящие, но имеют в пути другие доменные зоны или как-то видоизменяют сам путь (рис. 3.32).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

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

✓ 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**

Рис. 3.32: Фишинговые ссылки

Фишинговый имейл может прийти от знакомого адреса, если используется слабый протокол почтового сервиса (рис. 3.33).

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. 3.33: Фишинговый имейл

Спуфинг уже практически неактуален, поскольку придуманы более защищённые протоколы отправки Email (рис. 3.34).

Email Спуфинг – это

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили **960** учащихся
Из всех попыток **65%** верных

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

Следующий шаг Решить снова

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

Рис. 3.34: Имейл спуфинг

Троян маскируется под легитимную программу и пытается получить контроль над устройством (рис. 3.35).

Вирус-троян

Выберите один вариант из списка

✓ Всё получилось!

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. 3.35: Вирус-троян

Ключ шифрования в протоколе Signal генерируется при отправке первого со-

общения пользователем (рис. 3.36).

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Верно решили **952** учащихся
Из всех попыток **52%** верных

☒ Отлично!

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 3.36: Signal

Сквозное шифрование использует пару ключей для конфиденциального общения узлов (рис. 3.37).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

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

☒ Верно. Так держать!

- ☒ 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. 3.37: Суть сквозного шифрования

Для правильной работы криптографических примитивов требуется наличие пары ключей у всех участников общения (рис. 3.38).

3.3 Прохождение третьего этапа

В асимметричных криптографических примитивах

Выберите один вариант из списка

Верно решили 940 учащихся
Из всех попыток 42% верных

✓ Правильно, молодец!

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.38: Ассимитричные криптографические примитивы

Криптографическая хэш-функция не обеспечивает конфиденциальность зашифрованных данных, поскольку её невозможно вычислить в обратном порядке (рис. 3.39).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 798 учащихся
Из всех попыток 11% 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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.39: Криптографическая хэш-функция

Перечисление алгоритмов цифровой подписи (рис. 3.40).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

Верно решили **834** 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](#).

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

Следующий шаг

Решить снова

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

Рис. 3.40: Алгоритмы цифровой подписи

Код аутентификации сообщения относится к симметричным примитивам, поскольку используется симметричное шифрование (рис. 3.41).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Всё получилось!

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

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Следующий шаг

Решить снова

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

Рис. 3.41: Код аутентификации сообщения

Определение обмена ключами Диффи-Хеллмана (рис. 3.42).

Обмен ключам Диффи-Хеллмана - это

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. 3.42: Обмен ключами Диффи-Хеллмана

Протокол электронной цифровой подписи относится к протоколам с публичным ключом, ведь пользователи могут проверить подпись этим ключом (рис. 3.43).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Правильно.

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. 3.43: Протокол электронной цифровой подписи

Механизм работы верификации ЭЦП (рис. 3.44).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили **962** учащихся
Из всех попыток **46%** верных

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

Следующий шаг Решить снова

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

Рис. 3.44: Верификация ЭЦП

ЭПС не обеспечивает конфиденциальность, поскольку содержит информацию о пользователе, сделавшем эту подпись (рис. 3.45).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 968 учащихся
Из всех попыток 53% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.45: ЭЦП не обеспечивает

Усиленная квалифицированная электронная подпись при отправке налоговой отчётности в ФНС требуется для обеспечения юридической значимости, безопасности и достоверности (рис. 3.46).

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

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 68% верных

- ☐ усиленная неквалифицированная
- ☐ простая
- ☒ усиленная квалифицированная

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.46: Тип ЭЦП для отправки налоговой отчётности в ФНС

Сертификаты для доменов выдают сертифицированные центры (рис. 3.47).

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

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решил 971 учащихся
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. 3.47: CA

Список платёжных систем (рис. 3.48).

Выберите из списка все платёжные системы.

Выберите все подходящие ответы из списка

✓ Отлично!

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. 3.48: Платёжные системы

Многофакторная аутентификация подразумевает собой ввод нескольких ключей для доступа к информации (рис. 3.49).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Так точно!

Верно решили **896** 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**

Рис. 3.49: Примеры многофакторной аутентификации

Для безопасности платёжных счетов пользователей при онлайн оплатах сегодня используется многофакторная аутентификация перед банком-эмитентом (рис. 3.50).

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Отлично!

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

Рис. 3.50: Аутентификация при онлайн платежах

Устройство proof of work (рис. 3.51).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Здорово, всё верно.

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. 3.51: Proof of work

Консенсус позволяет участникам блокчейна согласовывать операции без доверия друг к другу (рис. 3.52).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Всё получилось!

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](#).

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 3.52: Consensus

Все участники блокчейна хранят цифровую подпись (рис. 3.53).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Всё получилось!

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. 3.53: Что хранят участники блокчейна

Данный курс не предусматривает выдачу сертификатов, поэтому прикладываю скриншот-доказательство прохождения курса (рис. 3.54).

3.4 Сертификат

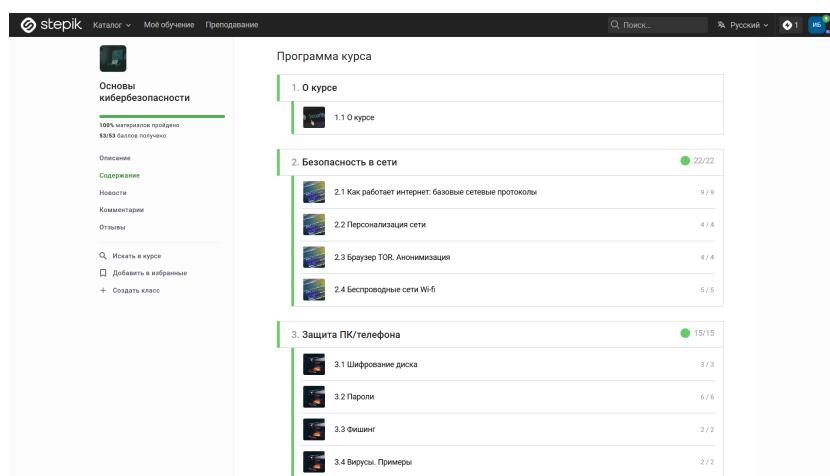


Рис. 3.54: “Сертификат”

4 Выводы

В результате прохождения внешнего курса мы узнали, как обеспечивается безопасность в сети, с помощью каких протоколов общаются устройства в ней, как защитить свои устройства и аккаунты от злоумышленников, а также рассмотрели криптографическую составляющую сети.