

Внешний курс

Основы кибербезопасности

Бекназарова Виктория Тиграновна

Содержание

1	Цель работы	6
2	Прохождение курса	7
3	Цифровая подпись	47
4	Электронные платежи	52
5	Блокчейн	55
6	Выводы	58

Список иллюстраций

2.1	Протокол прикладного уровня	7
2.2	Протокол TCP	8
2.3	Адреса IPv-4	9
2.4	DNS сервер	10
2.5	Протокол в модели TCP/IP	11
2.6	Протокол http	12
2.7	Протокол https	13
2.8	Протокол TLS	14
2.9	Протокол TLS	15
2.10	Куки хранят	16
2.11	Куки не используются	17
2.12	Куки генерируются	18
2.13	Сессионные куки	19
2.14	Промежуточные узлы TOR	20
2.15	Браузер TOR	21
2.16	Секретный ключ	22
2.17	Браузер TOR	23
2.18	Wi-Fi	24
2.19	Протокол Wi-Fi	25
2.20	Шифрование Wi-Fi	26
2.21	Загрузочный сектор диска	27
2.22	Шифрование диска	28
2.23	Жесткий диск	29
2.24	Пароли	30
2.25	Хранение паролей	31
2.26	Капча	32
2.27	Хэширование паролей	33
2.28	Стойкость паролей	34
2.29	Меры защиты паролей	35
2.30	Фишинговые ссылки	36
2.31	Фишинговый имейл	37
2.32	Спуфинг	38
2.33	Вирус-троян	39
2.34	Мессенджер Signal	40
2.35	Сквозное шифрование	41
2.36	Криптографические примитивы	42
2.37	Криптографическая хэш-функция	43

2.38	Цифровые подписи	44
2.39	Аутентификация сообщения	45
2.40	Обмен ключам	46
3.1	Протокол электронной подписи	47
3.2	Алгоритм верификации	48
3.3	Электронная подпись	49
3.4	ФНС	50
3.5	Сертификат ключа	51
4.1	Платежные системы	52
4.2	Многофакторная аутентификация	53
4.3	Онлайн платежи	54
5.1	Криптографическая хэш-функция	55
5.2	Консенсус в некоторых системах	56
5.3	Секретные ключи	57

Список таблиц

1 Цель работы

Изучить основы кибербезопасности

2 Прохождение курса

1. Введение в курс #Безопасность в сети
2. 1.Как работает интернет:базовые сетевые протоколы.

2.1 Как работает интернет: базовые сетевые протоколы

Выберите протокол прикладного уровня

Выберите один вариант из списка

Верно решили **895** учащихся
Из всех попыток **58%** верных

☒ Правильно, молодец!

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг

Решить снова

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

Рис. 2.1: Протокол прикладного уровня

2.1 Как работает интернет: базовые сетевые протоколы

На каком уровне работает протокол TCP?

Выберите один вариант из списка

Верно решили **939** учащихся
Из всех попыток **61%** верных

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 2.2: Протокол TCP

Шаг 9 из 15

2.1 Как работает интернет: базовые сетевые протоколы

Выберите все корректные адреса IPv4

Верно решил **871** учащихся
Из всех попыток **23%** верных

Выберите все подходящие ответы из списка

✓ Абсолютно 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](#).

☐ 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: Адреса IPv-4

2.1 Как работает интернет: базовые сетевые протоколы

DNS сервер

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: DNS сервер

Шаг 11 из 15

2.1 Как работает интернет: базовые сетевые протоколы

Выберите корректную последовательность протоколов в модели TCP/IP

Верно решил **941** учащихся
Из всех попыток **53%** верных

Выберите один вариант из списка

☒ Хорошая работа.

☐ 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: Протокол в модели TCP/IP

11

< Шаг 12 из 15 >

2.1 Как работает интернет: базовые сетевые протоколы

Протокол http предполагает

Верно решили **965** учащихся
Из всех попыток **78%** верных

Выберите один вариант из списка

☒ Отличное решение!

☐ 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: Протокол http

2.1 Как работает интернет: базовые сетевые протоколы

Протокол https состоит из

Выберите один вариант из списка

Верно решили **948** учащихся
Из всех попыток **41%** верных

☒ Отлично!

- ☐ 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** из 1

Рис. 2.7: Протокол https

2.1 Как работает интернет: базовые сетевые протоколы

Версия протокола TLS определяется

Выберите один вариант из списка

Верно решили **947** учащихся
Из всех попыток **55%** верных

☒ Верно.

- ☐ сервером
- ☐ клиентом
- ☒ и клиентом, и сервером в процессе “переговоров”
- ☐ провайдером клиента

Следующий шаг

Решить снова

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

Рис. 2.8: Протокол TLS

Шаг 15 из 15

2.1 Как работает интернет: базовые сетевые протоколы

В фазе “рукопожатия” протокола TLS не предусмотрено

Верно решил **931** учащихся
Из всех попыток **44%** верных

Выберите один вариант из списка

☒ Верно. Так держать!

☐ 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. 2.9: Протокол TLS

#Персонализация сети.

Шаг 3 из 6

2.2 Персонализация сети

Куки хранят:

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

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☐ пароль пользователя

☒ идентификатор пользователя

☒ id сессии

☐ IP адрес

Следующий шаг

Решить снова

Рис. 2.10: Куки хранят

16

< Шаг 4 из 6 >

2.2 Персонализация сети

Куки не используются для

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

Выберите один вариант из списка

☒ Верно. Так держать!

☐ 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: Куки не используются

< Шаг 5 из 6 >

2.2 Персонализация сети

Куки генерируются

Верно решили 968 учащихся
Из всех попыток 79% верных

Выберите один вариант из списка

☒ Верно.

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

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

Рис. 2.12: Куки генерируются

Шаг 6 из 6

2.2 Персонализация сети

Сессионные куки хранятся в браузере?

Верно решили **959** учащихся
Из всех попыток **60%** верных

Выберите один вариант из списка

☒ Верно. Так держать!

☐ Нет

☐ Да, на некоторое время, заданное в сервером

☒ Да, на время пользования веб-сайтом

Следующий шаг

Решить снова

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

Рис. 2.13: Сессионные куки

#Браузер TOR. Анимация.

Шаг 3 из 6

2.3 Браузер TOR. Анонимизация

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

Верно решили **959** учащихся

Из всех попыток **77%** верных

☒ Здорово, всё верно.

☐ 2

☐ 3

☐ 4

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл** из 1

Рис. 2.14: Промежуточные узлы TOR

Шаг 4 из 6

2.3 Браузер TOR. Анонимизация

IP-адрес получателя известен

Верно решили **906** учащихся
Из всех попыток **19%** верных

Выберите все подходящие ответы из списка

☒ Абсолютно 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](#).

☐ охранному узлу
☐ промежуточному узлу
☒ отправителю
☒ выходному узлу

Следующий шаг

Решить снова

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

Рис. 2.15: Браузер TOR

< Шаг 5 из 6 >

2.3 Браузер TOR. Анонимизация

Отправитель генерирует общий секретный ключ

Верно решили 959 учащихся
Из всех попыток 55% верных

Выберите один вариант из списка

☒ Хорошая работа.

☐ 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** из 1

Рис. 2.16: Секретный ключ

< Шаг 6 из 6 >

2.3 Браузер TOR. Анонимизация

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

Верно решил **961** учащийся
Из всех попыток **74%** верных

Выберите один вариант из списка

☒ Верно. Так держать!

☐ Нет
☐ Да

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл** из 1

Рис. 2.17: Браузер TOR

#Беспроводные сети. Wi-Fi

23

2.4 Беспроводные сети Wi-fi

Wi-Fi - это

Выберите один вариант из списка

Верно решили **965** учащихся
Из всех попыток **79%** верных



Хорошие новости, верно!

- ☐ 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: Wi-Fi

Шаг 5 из 8

2.4 Беспроводные сети Wi-fi

На каком уровне работает протокол WiFi?

Верно решили **972** учащихся
Из всех попыток **58%** верных

Выберите один вариант из списка

✓ Так точно!

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Следующий шаг

Решить снова

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

Рис. 2.19: Протокол Wi-Fi

Шаг 6 из 8

2.4 Беспроводные сети Wi-Fi

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Верно решили **973** учащихся
Из всех попыток **60%** верных

Выберите один вариант из списка

✓ Прекрасный ответ.

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Следующий шаг

Решить снова

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

Рис. 2.20: Шифрование Wi-Fi

#3.Защита ПК/телефона #Шифрование диска

26

3.1 Шифрование диска 5 из 5 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Верно.

Верно решили **949** учащихся
Из всех попыток **89%** верных

☒ Да

☐ Нет

Следующий шаг

Решить снова

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

Рис. 2.21: Загрузочный сектор диска

3.1 Шифрование диска

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Шифрование диска основано на

Выберите один вариант из списка

Верно решили **972** учащихся
Из всех попыток **66%** верных

☒ Абсолютно точно.

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Следующий шаг

Решить снова

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

Рис. 2.22: Шифрование диска

< Шаг 5 из 5 >

3.1 Шифрование диска

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв

Нет, спасибо

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

Верно решили **906** учащихся
Из всех попыток **28%** верных

✓ 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](#).

☐ Disk Utility

☐ Wireshark

☒ BitLocker

☒ VeraCrypt

Рис. 2.23: Жесткий диск

#Пароли

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

☒ Отличное решение!

Верно решили **969** учащихся
Из всех попыток **85%** верных

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

Следующий шаг

Решить снова

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

Рис. 2.24: Пароли

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Где безопасно хранить пароли?

Выберите один вариант из списка



Верно. Так держать!

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. 2.25: Хранение паролей

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Зачем нужна капча?

Выберите один вариант из списка

Верно решили **974** учащихся
Из всех попыток **77%** верных

☒ Хорошие новости, верно!

☐ Она заменяет пароли

☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

☐ Для защиты кук пользователя

☐ Для безопасного хранения паролей на сервере

Следующий шаг

Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 2.26: Капча

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Для чего применяется хэширование паролей?

Выберите один вариант из списка

Верно решили **973** учащихся
Из всех попыток **61%** верных

☒ Отличное решение!

- ☐ 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. 2.27: Хэширование паролей

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#) [Нет, спасибо](#)

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

Выберите один вариант из списка

☒ Так точно!

☐ Нет

☐ Да

Следующий шаг

Решить снова

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

Верно решили **967** учащихся
Из всех попыток **66%** верных

Рис. 2.28: Стойкость паролей

3.2 Пароли

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Верно решили **895** учащихся

Из всех попыток **16%** 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](#).



разные пароли на всех сайтах



периодическая смена паролей



сложные(=длинные) пароли



капча

Следующий шаг

Решить снова

Рис. 2.29: Меры защиты паролей

#Фишинг

3.3 Фишинг

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

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

☒ Здорово, всё верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

- ☐ <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

Рис. 2.30: Фишинговые ссылки

3.3 Фишинг

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Абсолютно точно.

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Верно решили **957** учащихся
Из всех попыток **90%** верных

Рис. 2.31: Фишинговый имейл

#Вирусы.Примеры

3.4 Вирусы. Примеры

Email Спуфинг -- это

Выберите один вариант из списка

Верно решили **958** учащихся
Из всех попыток **65%** верных

☒ Прекрасный ответ.

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

Следующий шаг

Решить снова


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

Рис. 2.32: Спуфинг

3.4 Вирусы. Примеры

Вирус-троян

Выберите один вариант из списка

 Отлично!

Верно решили **956** 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. 2.33: Вирус-троян

#Безопасность мессенджеров

3.5 Безопасность мессенджеров

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Верно решили **928** учащихся
Из всех попыток **52%** верных

☒ Всё получилось!

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

Следующий шаг

Решить снова

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

Рис. 2.34: Мессенджер Signal

3.5 Безопасность мессенджеров

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

Верно решили **927** учащихся
Из всех попыток **60%** верных

☒ Правильно, молодец!

☐ 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. 2.35: Сквозное шифрование

#4.Криптография на практике # ВВведение в криптографию

4.1 Введение в криптографию

В асимметричных криптографических примитивах

Выберите один вариант из списка

Верно решили **892** учащихся
Из всех попыток **42%** верных

☒ Верно.

- ☒ обе стороны имеют пару ключей
- ☐ 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
- ☐ обе стороны имеют общий секретный ключ

Следующий шаг

Решить снова

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

Рис. 2.36: Криптографические примитивы

4.1 Введение в криптографию

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили **736** учащихся
Из всех попыток **11%** 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](#).

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

Следующий шаг

Решить снова

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

Рис. 2.37: Криптографическая хэш-функция

4.1 Введение в криптографию

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили **749** учащихся
Из всех попыток **18%** верных

☒ Здорово, всё верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

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

Следующий шаг

Решить снова

Рис. 2.38: Цифровые подписи

Шаг 0 из 7

4.1 Введение в криптографию

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Так точно!

☐ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг

Решить снова

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

Верно решили **856** учащихся
Из всех попыток **69%** верных

Рис. 2.39: Аутентификация сообщения

4.1 Введение в криптографию

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

Верно решили **849** учащихся
Из всех попыток **46%** верных

☒ Абсолютно точно.

- ☐ 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. 2.40: Обмен ключам

3 Цифровая подпись

4.2 Цифровая подпись

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

Верно решили **816** учащихся
Из всех попыток **70%** верных

☒ Хорошие новости, верно!

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

Следующий шаг

Решить снова

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

Рис. 3.1: Протокол электронной подписи

4.2 Цифровая подпись

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Верно решили **811** учащихся
Из всех попыток **45%** верных

☒ Хорошая работа.

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

Следующий шаг

Решить снова

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

Рис. 3.2: Алгоритм верификации

4.2 Цифровая подпись

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

Верно решили **812** учащихся
Из всех попыток **51%** верных

☒ Правильно, молодец!

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

Следующий шаг

Решить снова

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

Рис. 3.3: Электронная подпись

4.2 Цифровая подпись

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

Выберите один вариант из списка

☒ Верно.

Верно решили **812** учащихся
Из всех попыток **66%** верных

- ☒ усиленная квалифицированная
- ☐ простая
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

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

Рис. 3.4: ФНС

4.2 Цифровая подпись

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

Выберите один вариант из списка

Верно решили **810** учащихся
Из всех попыток **60%** верных

☒ Верно. Так держать!

- ☐ 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. 3.5: Сертификат ключа

4 Электронные платежи

4.3 Электронные платежи

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно решили **748** учащихся
Из всех попыток **23%** 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](#).

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

Следующий шаг

Решить снова

Рис. 4.1: Платежные системы

4.3 Электронные платежи

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Верно решили **728** учащихся
Из всех попыток **22%** верных

✓ Отличное решение!

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. 4.2: Многофакторная аутентификация

4.3 Электронные платежи

При онлайн платежах сегодня используется

Выберите один вариант из списка

Верно решили **785** учащихся
Из всех попыток **58%** верных

☒ Верно. Так держать!

- ☐ 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. 4.3: Онлайн платежи

5 Блокчейн

4.4 Блокчейн

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Верно решил **801** учащийся
Из всех попыток **47%** верных

✓ Отличное решение!

☐ фиксированная длина выходных данных

☒ сложность нахождения прообраза

☐ обеспечение целостности

☐ эффективность вычисления

Следующий шаг

Решить снова

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

Рис. 5.1: Криптографическая хэш-функция

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решили **716** учащихся
Из всех попыток **22%** верных

☒ 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](#).

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

Следующий шаг

Решить снова

Рис. 5.2: Консенсус в некоторых системах

4.4 Блокчейн

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Верно решили **799** учащихся
Из всех попыток **46%** верных

☒ Верно.

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

Следующий шаг

Решить снова

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

Рис. 5.3: Секретные ключи

6 Выводы

Моё обучение

Основы кибербезопасности

100% материалов пройдено

53/53 баллов получено

☆ Оставить отзыв

Сертификат не выдаётся

Сертификат не выдается.