

Внешний курс

Основы кибербезопасности

Галиева Аделина Руслановна

Содержание

1	Цель работы	6
2	Прохождение курса	7
3	Безопасность в сети	8
4	Защита ПК/телефона	30
5	Криптография на практике	45
6	Выводы	61

Список иллюстраций

3.1	Протокол прикладного уровня	8
3.2	Протокол TCP	9
3.3	Адреса IPv-4	10
3.4	DNS сервер	11
3.5	Протокол в модели TCP/IP	12
3.6	Протокол http	13
3.7	Протокол https	14
3.8	Протокол TLS	15
3.9	Протокол TLS	16
3.10	Куки хранят	17
3.11	Куки не используются	18
3.12	Куки генерируются	19
3.13	Сессионные куки	20
3.14	Промежуточные узлы TOR	21
3.15	Браузер TOR	22
3.16	Секретный ключ	23
3.17	Браузер TOR	24
3.18	Wi-Fi	25
3.19	Протокол Wi-Fi	26
3.20	Шифрование Wi-Fi	27
3.21	Данные между хостом и роутером	28
3.22	Метод	29
4.1	Загрузочный сектор диска	30
4.2	Шифрование диска	31
4.3	Жесткий диск	32
4.4	Пароли	33
4.5	Хранение паролей	34
4.6	Капча	35
4.7	Хэширование паролей	36
4.8	Стойкость паролей	37
4.9	Меры защиты паролей	38
4.10	Фишинговые ссылки	39
4.11	Фишинговый имейл	40
4.12	Спуфинг	41
4.13	Вирус-троян	42
4.14	Мессенджер Signal	43

4.15 Сквозное шифрование	44
5.1 Криптографические примитивы	45
5.2 Криптографическая хэш-функция	46
5.3 Цифровые подписи	47
5.4 Аутентификация сообщения	48
5.5 Обмен ключам	49
5.6 Протокол электронной подписи	50
5.7 Алгоритм верификации	51
5.8 Электронная подпись	52
5.9 ФНС	53
5.10 Сертификат ключа	54
5.11 Платежные системы	55
5.12 Многофакторная аутентификация	56
5.13 Онлайн платежи	57
5.14 Криптографическая хэш-функция	58
5.15 Консенсус в некоторых системах	59
5.16 Секретные ключи	60
6.1 Окончание курса	61

Список таблиц

1 Цель работы

Изучить основы кибербезопасности.

2 Прохождение курса

1. Введение в курс

3 Безопасность в сети

2. 1. Как работает интернет: базовые сетевые протоколы.

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено
9 из 9 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

[Нет, спасибо](#)

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Всё получилось!

Верно решили **895** учащихся

Из всех попыток **58%** верных

- ☐ UDP
- ☐ TCP
- ☒ HTTPS
- ☐ IP

Следующий шаг

Решить снова

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

Рис. 3.1: Протокол прикладного уровня

На каком уровне работает протокол TCP?

Выберите один вариант из списка

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

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

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

Рис. 3.2: Протокол TCP

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

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

- ☐ 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. 3.3: Адреса IPv-4

DNS сервер

Выберите один вариант из списка

Верно решили **933** учащихся
Из всех попыток **66%** верных

✓ Отличное решение!

- ☒ 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. 3.4: DNS сервер

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено

9 из 9 баллов получено

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

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

☒ Абсолютно точно.

- ☐ 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. 3.5: Протокол в модели TCP/IP

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено

9 из 9 баллов получено

Протокол http предполагает

Выберите один вариант из списка

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

☒ Верно.

- ☐ 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. 3.6: Протокол http

Протокол https состоит из

Выберите один вариант из списка

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

☒ Правильно.

- ☐ 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. 3.7: Протокол https

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. 3.8: Протокол TLS

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

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

☒ Абсолютно точно.

- ☐ 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. 3.9: Протокол TLS

2. 2. Персонализация сети.

Куки хранят:

Выберите все подходящие ответы из списка

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

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

Следующий шаг

Решить снова

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

Рис. 3.10: Куки хранят

Куки не используются для

Выберите один вариант из списка

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

☒ Отличное решение!

- ☐ 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. 3.11: Куки не используются

Куки генерируются

Выберите один вариант из списка

☒ Всё получилось!

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

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

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

Рис. 3.12: Куки генерируются

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

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

☒ Хорошая работа.

- ☐ 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. 3.13: Сессионные куки

2. 3. Браузер TOR. Анимация.

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

Верно решили **959** учащихся
Из всех попыток **77%** верных

☒ Всё правильно.

- ☐ 2
- ☒ 3
- ☐ 4

Следующий шаг

Решить снова

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

Рис. 3.14: Промежуточные узлы TOR

IP-адрес получателя известен

Выберите все подходящие ответы из списка

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

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

Следующий шаг

Решить снова

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

Рис. 3.15: Браузер TOR

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

Верно решили **959** учащихся
Из всех попыток **55%** верных

☒ Всё получилось!

- ☐ 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. 3.16: Секретный ключ

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

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

Выберите один вариант из списка

Верно решил 961 учащийся
Из всех попыток 74% верных

☒ Всё правильно.

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Рис. 3.17: Браузер TOR

2. 4. Беспроводные сети Wi-Fi.

Wi-Fi - это

Выберите один вариант из списка

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

☒ Верно. Так держать!

- ☐ 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. 3.18: Wi-Fi

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

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

☒ Абсолютно точно.

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Следующий шаг

Решить снова

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

Рис. 3.19: Протокол Wi-Fi

2.4 Беспроводные сети Wi-fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

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

☒ Верно. Так держать!

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Следующий шаг

Решить снова

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

Рис. 3.20: Шифрование Wi-Fi

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

Верно решили **975** учащихся
Из всех попыток **53%** верных

☒ Здорово, всё верно.

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

Следующий шаг

Решить снова

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

Рис. 3.21: Данные между хостом и роутером

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

Верно решили **975** учащихся
Из всех попыток **87%** верных

✓ Хорошая работа.

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Рис. 3.22: Метод

4 Защита ПК/телефона

3. 1. Шифрование диска.

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

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Отличное решение!

☐ Да

☐ Нет

[Следующий шаг](#) [Решить снова](#)

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

Верно решили 949 учащихся
Из всех попыток 89% верных

Рис. 4.1: Загрузочный сектор диска

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

Шифрование диска основано на

Выберите один вариант из списка

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

☒ Здорово, всё верно.

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Следующий шаг

Решить снова

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

Рис. 4.2: Шифрование диска

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

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

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

☒ 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](#).

- ☒ BitLocker
- ☒ VeraCrypt
- ☐ Wireshark
- ☐ Disk Utility

Следующий шаг

Решить снова

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

Рис. 4.3: Жесткий диск

3. 2. Пароли.

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

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

✓ Прекрасный ответ.

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

Следующий шаг

Решить снова

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

Рис. 4.4: Пароли

Где безопасно хранить пароли?

Выберите один вариант из списка

Верно решил **971** учащихся
Из всех попыток **74%** верных

☒ Отлично!

- ☒ 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. 4.5: Хранение паролей

Зачем нужна капча?

Выберите один вариант из списка

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

☒ Всё получилось!

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

Следующий шаг

Решить снова

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

Рис. 4.6: Капча

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

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

☒ Всё получилось!

- ☐ 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. 4.7: Хэширование паролей

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

Выберите один вариант из списка

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

☒ Всё получилось!

☐ Да

☒ Нет

Следующий шаг

Решить снова


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

Рис. 4.8: Стойкость паролей

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

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

- ☒ 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. 4.9: Меры защиты паролей

3. 3. Фишинг.

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

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

☒ 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](#).

- ☐ <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. 4.10: Фишинговые ссылки

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

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

☒ Прекрасный ответ.

☒ Да
☐ Нет

Следующий шаг

Решить снова

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

Рис. 4.11: Фишинговый имейл

3. 4. Вирусы. Примеры.

Email Спуфинг – это

Выберите один вариант из списка

протоколы



Прекрасный ответ.

5 из 5 шагов пройдено

9 из 9 баллов получено

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

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

Следующий шаг

Решить снова

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

Рис. 4.12: Спуфинг

Вирус-троян

Выберите один вариант из списка

Верно решили **969** учащихся
Из всех попыток **74%** верных

☒ Верно. Так держать!

- ☐ 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. 4.13: Вирус-троян

3. 5. Безопасность мессенджеров.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Верно решили **947** учащихся
Из всех попыток **52%** верных

☒ Хорошие новости, верно!

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

Следующий шаг

Решить снова

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

Рис. 4.14: Мессенджер Signal

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

Верно решили **946** учащихся
Из всех попыток **60%** верных

☒ Хорошая работа.

- ☒ 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. 4.15: Сквозное шифрование

5 Криптография на практике

4. 1. Введение в криптографию.

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

В асимметричных криптографических примитивах

Выберите один вариант из списка

Верно решили 911 учащихся
Из всех попыток 42% верных

☒ Отлично!

☐ обе стороны имеют общий секретный ключ

☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей

☒ обе стороны имеют пару ключей

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

Следующий шаг

Решить снова

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

Рис. 5.1: Криптографические примитивы

Криптографическая хэш-функция

О курсе

Выберите все подходящие ответы из списка

Верно решили 752 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](#).

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

Следующий шаг

Решить снова

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

Рис. 5.2: Криптографическая хэш-функция

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили **766** учащихся
Из всех попыток **18%** 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](#).

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

Следующий шаг

Решить снова

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

Рис. 5.3: Цифровые подписи

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Код аутентификации сообщения относится к

Безопасность в сети

Вопрос из списка

Верно решили **874** учащихся
Из всех попыток **69%** верных

✓

 Правильно, молодец!

☐ асимметричным примитивам

☒ симметричным примитивам

Следующий шаг

Решить снова

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

Рис. 5.4: Аутентификация сообщения

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

Верно решили **868** учащихся
Из всех попыток **46%** верных

✓ Прекрасный ответ.

- ☐ 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. 5.5: Обмен ключам

4. 2. Цифровая подпись.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

Верно решили **836** 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. 5.6: Протокол электронной подписи

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Верно решили **830** учащихся
Из всех попыток **45%** верных

☒ Всё получилось!

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

Следующий шаг

Решить снова

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

Рис. 5.7: Алгоритм верификации

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Отлично!

Верно решил **831** учащийся
Из всех попыток **51%** верных

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

Следующий шаг

Решить снова

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

Рис. 5.8: Электронная подпись

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

Выберите один вариант из списка

Верно решил **831** учащийся
Из всех попыток **66%** верных

✓ Всё получилось!

- ☐ усиленная неквалифицированная
- ☐ простая
- ☒ усиленная квалифицированная

Следующий шаг

Решить снова

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

Рис. 5.9: ФНС

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

Выберите один вариант из списка

Верно решили **829** учащихся
Из всех попыток **60%** верных

☒ Хорошая работа.

- ☐ 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. 5.10: Сертификат ключа

4. 3. Электронные платежи.

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно решили **768** учащихся
Из всех попыток **23%** 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](#).

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

Следующий шаг

Решить снова

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

Рис. 5.11: Платежные системы

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Верно решили **747** учащихся
Из всех попыток **22%** 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](#).

- ☐ 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** из 1

Рис. 5.12: Многофакторная аутентификация

При онлайн платежах сегодня используется

Выберите один вариант из списка

Верно решили **805** учащихся
Из всех попыток **58%** верных

☒ Верно.

- ☒ 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. 5.13: Онлайн платежи

4. 4. Блокчейн.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Верно решил **821** учащихся
Из всех попыток **48%** верных

☒ Верно.

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

Следующий шаг

Решить снова


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

Рис. 5.14: Криптографическая хэш-функция

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решили 734 учащихся
Из всех попыток 21% 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](#).

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

Следующий шаг

Решить снова

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

Рис. 5.15: Консенсус в некоторых системах

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Верно решили **819** учащихся
Из всех попыток **46%** верных

✓ Всё правильно.

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

Следующий шаг

Решить снова

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

Рис. 5.16: Секретные ключи

6 Выводы

Сертификат не выдается.

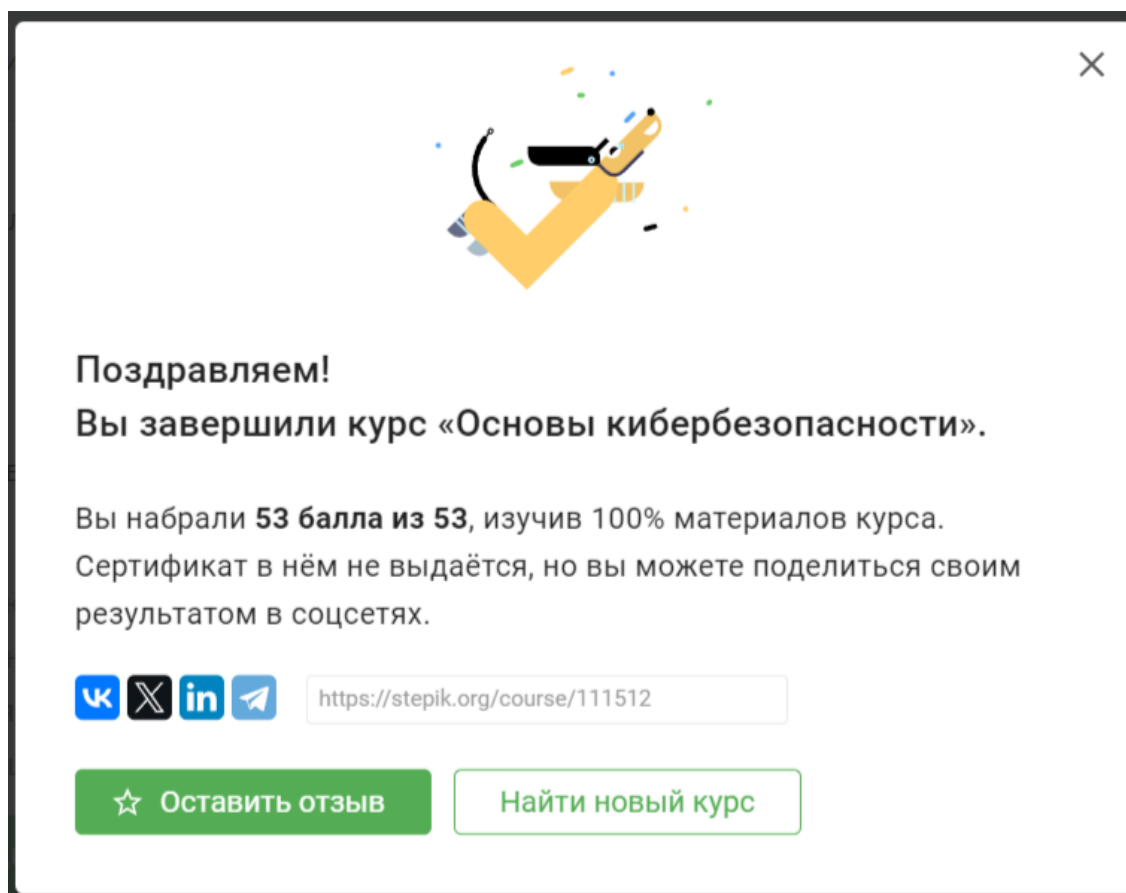


Рис. 6.1: Окончание курса