

Результат выполнения внешнего курса на Степике

Внешний курс

Филиппьева Ксения Дмитриевна

Содержание

1 Цель работы	6
2 Выполнение заданий блока “Основы Кибербезопасности”	7
2.1 Устройство интернета и сетевые протоколы	7
2.2 Идентификация через куки	12
2.3 Анонимность в сети через TOR	14
2.4 Wi-Fi и его защита	16
2.5 Шифрование диска	18
2.6 Безопасные пароли	20
2.7 Фишинг	24
2.8 Вредоносные программы	25
2.9 Шифрование в мессенджерах	27
2.10 Основы криптографии	28
2.11 Электронная подпись	31
2.12 Платёжные системы	33
2.13 Блокчейн	36
3 Общий результат	38

Список иллюстраций

2.1	Вопрос 2.1	7
2.2	Вопрос 2.1	8
2.3	Вопрос 2.1	8
2.4	Вопрос 2.1	9
2.5	Вопрос 2.1	10
2.6	Вопрос 2.1	10
2.7	Вопрос 2.1	11
2.8	Вопрос 2.1	11
2.9	Вопрос 2.1	12
2.10	Вопрос 2.2	12
2.11	Вопрос 2.2	13
2.12	Вопрос 2.2.	13
2.13	Вопрос 2.2	14
2.14	Вопрос 2.3	14
2.15	Вопрос 2.3.	15
2.16	Вопрос 2.3	15
2.17	Вопрос 2.3	16
2.18	Вопрос 2.4	16
2.19	Вопрос 2.4	17
2.20	Вопрос 2.4	17
2.21	Вопрос 2.4	18
2.22	Вопрос 2.4	18
2.23	Вопрос 3.1.	19
2.24	Вопрос 3.1	19
2.25	Вопрос 3.1	20
2.26	Вопрос 3.2	21
2.27	Вопрос 3.2	22
2.28	Вопрос 3.2	22
2.29	Вопрос 3.2	23
2.30	Вопрос 3.2	23
2.31	Вопрос 3.2	24
2.32	Вопрос 3.3	24
2.33	Вопрос 3.3	25
2.34	Вопрос 3.4	26
2.35	Вопрос 3.4	27
2.36	Вопрос 3.5	27
2.37	Вопрос 3.5	28

2.38 Вопрос 4.1	28
2.39 Вопрос 4.1	29
2.40 Вопрос 4.1	29
2.41 Вопрос 4.1	30
2.42 Вопрос 4.1	30
2.43 Вопрос 4.2	31
2.44 Вопрос 4.2	31
2.45 Вопрос 4.2	32
2.46 Вопрос 4.2	33
2.47 Вопрос 4.2	33
2.48 Вопрос 4.3	34
2.49 Вопрос 4.3	35
2.50 Вопрос 4.3	35
2.51 Вопрос 4.4	36
2.52 Вопрос 4.4	37
2.53 Вопрос 4.4	37
3.1 Финал	38

Список таблиц

1 Цель работы

Целью работы является выполнение контрольных заданий первого модуля курса “Основы кибербезопасности” по теме “Безопасность в сети”.

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Устройство интернета и сетевые протоколы

HTTPS — это протокол прикладного уровня, который требуется в первом вопросе (рис. 2.1).

Выберите протокол прикладного уровня

Выберите один вариант из списка

Всё правильно.

UDP
 TCP
 HTTPS
 IP

[Следующий шаг](#) [Решить снова](#)

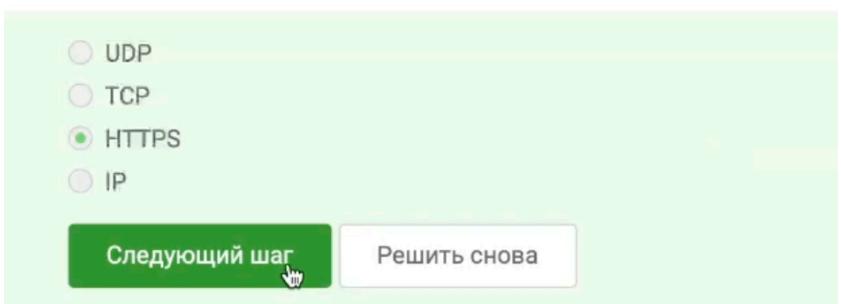


Рис. 2.1: Вопрос 2.1

Примерами протоколов транспортного уровня являются TCP и другие. TCP дал название модели (рис. 2.2).

На каком уровне работает протокол TCP?

Выберите один вариант из списка

Всё получилось!

Транспортном
 Прикладном
 Канальном
 Сетевом

Следующий шаг **Решить снова**

Рис. 2.2: Вопрос 2.1

IP-адрес должен состоять из 4 или 6 чисел в диапазоне от 0 до 255. Если встречаются числа больше 255 — это ошибка (рис. 2.3).

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

Прекрасный ответ.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на 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**



Рис. 2.3: Вопрос 2.1

DNS-сервер связывает доменное имя с соответствующим IP-адресом, определяя местоположение нужного ресурса (рис. 2.4).

DNS сервер

Выберите один вариант из списка

 Правильно, молодец!

- сопоставляет IP адреса доменным именам
- сегментирует данные на транспортном уровне
- выбирает маршрут пакета в сети
- выполняет адресацию на хосте

Следующий шаг

Решить снова

Рис. 2.4: Вопрос 2.1

Протоколы по уровням TCP/IP:

- Прикладной: HTTP, RTSP, FTP, DNS
- Транспортный: TCP, UDP, SCTP, DCCP
- Сетевой: IP
- Канальный: Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM, MPLS

(рис. 2.5)

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

 Абсолютно точно.

- сетевой – прикладной – канальный – транспортный
- прикладной – транспортный – канальный – сетевой
- транспортный – сетевой – прикладной – канальный
- прикладной – транспортный – сетевой – канальный

Следующий шаг

Решить снова

Рис. 2.5: Вопрос 2.1

HTTP не шифрует данные, в отличие от HTTPS, который применяет шифрование (рис. 2.6).

Протокол http предполагает

Выберите один вариант из списка

 Правильно, молодец!

- передачу зашифрованных данных между клиентом и сервером
- передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

Рис. 2.6: Вопрос 2.1

TLS настраивается как клиентом, так и сервером для установления соединения (рис. 2.7).

Протокол https состоит из

Выберите один вариант из списка

Верно. Так держать!

- 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

Рис. 2.7: Вопрос 2.1

Установление соединения по TLS требует согласования между клиентом и сервером (рис. 2.8).

Версия протокола TLS определяется

Выберите один вариант из списка

Хорошая работа.

- сервером
- клиентом
- и клиентом, и сервером в процессе "переговоров"
- провайдером клиента

Следующий шаг

Решить снова

Рис. 2.8: Вопрос 2.1

Фаза TLS-рукопожатия включает:

- выбор алгоритмов и параметров
- проверку подлинности (обычно сервера)

- создание общего секретного ключа

Вариант с дополнительным шифрованием здесь не нужен (рис. 2.9).

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

Так 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

Рис. 2.9: Вопрос 2.1

2.2 Идентификация через куки

Куки-файлы содержат параметры сессии: идентификатор пользователя, сессии, тип браузера и действия пользователя (рис. 2.10).

Куки хранят:

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 свое решение с другими на [форуме решений](#).

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

Следующий шаг

Решить снова

Рис. 2.10: Вопрос 2.2

Куки не обеспечивают безопасную передачу данных (рис. 2.11).

Куки не используются для

Выберите один вариант из списка

Так точно!

- аутентификации пользователя
- персонализации веб-страниц
- отслеживания информации о пользователе
- сборе статистики посещаемости сайта
- улучшения надежности соединения

Следующий шаг

Решить снова

Рис. 2.11: Вопрос 2.2

Сервер формирует куки и передаёт их клиенту (рис. 2.12).

Куки генерируются

Выберите один вариант из списка

Верно. Так держать!

- клиентом
- сервером

Следующий шаг

Решить снова

Рис. 2.12: Вопрос 2.2.

Сессионные куки удаляются при завершении сессии, например, после закрытия браузера (рис. 2.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

 Всё правильно.

- Нет
- Да, на время пользования веб-сайтом
- Да, на некоторое время, заданное в сервером

Следующий шаг

Решить снова

Рис. 2.13: Вопрос 2.2

2.3 Анонимность в сети через TOR

Маршрутизация в Tor включает три узла: охранный, промежуточный и выходной. Это фиксированная структура (рис. 2.14).

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

 Хорошие новости, верно!

- 2
- 3
- 4

Следующий шаг

Решить снова

Рис. 2.14: Вопрос 2.3

IP-адрес пользователя скрыт от охранного и промежуточного узлов (рис. 2.15).

IP-адрес получателя известен

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](#).

- охранному узлу
- промежуточному узлу
- отправителю
- выходному узлу

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.15: Вопрос 2.3.

Tor использует все три узла для формирования общего ключа шифрования. Каждый из них вносит вклад в процесс (рис. 2.16).

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

Абсолютно точно.

- только с охранным узлом
- с охранным и промежуточным узлом
- с охранным, промежуточным и выходном узлом
- с промежуточным и выходным узлом

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.16: Вопрос 2.3

Tor не требуется для получения данных, а используется для маскировки личности пользователя (рис. 2.17).

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

Выберите один вариант из списка

Правильно, молодец!

Да
 Нет

Следующий шаг **Решить снова**

Верно решил 961 учащийся
Из всех попыток 74% верных

Рис. 2.17: Вопрос 2.3

2.4 Wi-Fi и его защита

Wi-Fi — это технология беспроводной связи, основанная на стандарте IEEE 802.11 (рис. 2.18).

Wi-Fi - это

Выберите один вариант из списка

Так точно!

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**

Верно решили 965 учащихся
Из всех попыток 79% верных

Рис. 2.18: Вопрос 2.4

Он функционирует на канальном уровне сетевой модели (рис. 2.19).

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

 Верно.

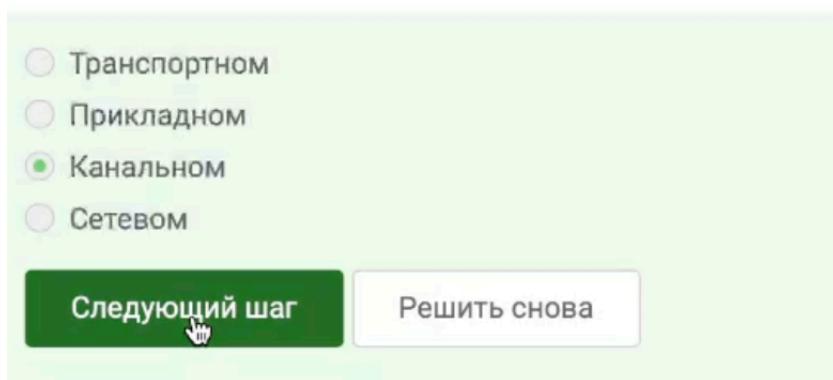


Рис. 2.19: Вопрос 2.4

WEP является устаревшим и легко взламываемым методом шифрования. Его использование не рекомендуется (рис. 2.20).

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

 Так точно!

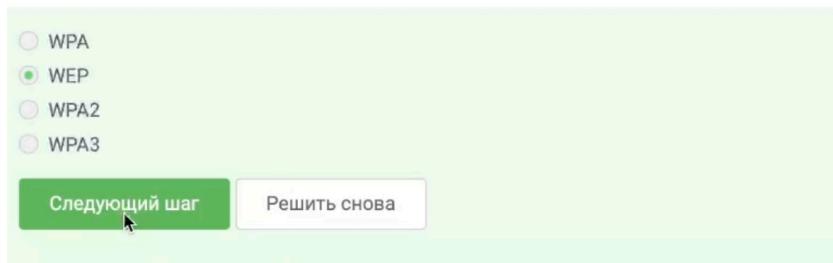


Рис. 2.20: Вопрос 2.4

Шифрование Wi-Fi защищает соединение между устройством и маршрутизатором (рис. 2.21).

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

Здорово, всё верно.

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

Следующий шаг

Решить снова

Рис. 2.21: Вопрос 2.4

WPA2 Personal применяется в домашних условиях, WPA2 Enterprise — в компаниях (рис. 2.22).

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

Хорошие новости, верно!

- WPA2 Personal
- WPA2 Enterprise

Следующий шаг

Решить снова

Рис. 2.22: Вопрос 2.4

2.5 Шифрование диска

Рекомендуется защищать как основной раздел, так и загрузочную область диска (рис. 2.23).

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

 Всё получилось!

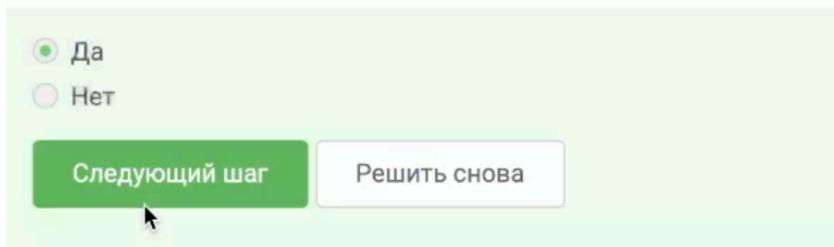


Рис. 2.23: Вопрос 3.1.

Используется симметричное шифрование (рис. 2.24).

Шифрование диска основано на

Выберите один вариант из списка

 Отличное решение!

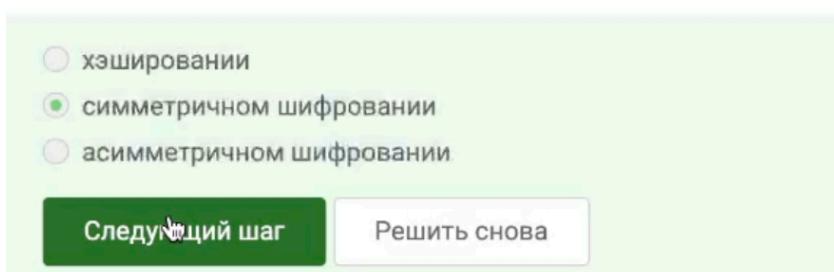


Рис. 2.24: Вопрос 3.1

ОС включают встроенные средства шифрования, а также доступны альтернативы с открытым кодом: BitLocker, LUKS, FileVault, Veracrypt (рис. 2.25).

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы 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](#).

<input type="checkbox"/> Wireshark	<input checked="" type="checkbox"/> BitLocker	<input type="checkbox"/> Disk Utility	<input checked="" type="checkbox"/> VeraCrypt
------------------------------------	---	---------------------------------------	---

[Следующий шаг](#) [Решить снова](#)

Рис. 2.25: Вопрос 3.1

2.6 Безопасные пароли

Надёжный пароль должен содержать буквы в разном регистре, цифры и спецсимволы (рис. 2.26).

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

 Абсолютно точно.

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.26: Вопрос 3.2

Пароли следует хранить в менеджерах, а не в обычных мессенджерах (рис. 2.27).

Где безопасно хранить пароли?

Выберите один вариант из списка

 Хорошая работа.

В менеджерах паролей
 В заметках на рабочем столе
 В заметках в телефоне
 На стикере, приkleенном к монитору
 В кошельке

Следующий шаг **Решить снова**

Рис. 2.27: Вопрос 3.2

CAPTCHA помогает отличить человека от робота (рис. 2.28).

Зачем нужна капча?

Выберите один вариант из списка

 Здорово, всё верно.

Вер
Из

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

Следующий шаг **Решить снова**

Рис. 2.28: Вопрос 3.2

Пароли хранятся в виде хэш-сумм, а не открытым текстом (рис. 2.29).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

 Правильно, молодец!

- 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

Рис. 2.29: Вопрос 3.2

Соль используется для усиления защиты пароля на сервере (рис. 2.30).

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

Выберите один вариант из списка

 Верно.

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

- Да
- Нет

Следующий шаг

Решить снова

Рис. 2.30: Вопрос 3.2

Рекомендуется использовать сложные и длинные пароли, регулярно их менять и хранить в безопасном месте (рис. 2.31).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Абсолютно точно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментахих 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. 2.31: Вопрос 3.2

2.7 Фишинг

Фишинговые сайты маскируются под настоящие, но с изменённым адресом (рис. 2.32).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно. Так держать!

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. 2.32: Вопрос 3.3

Фишинг может поступить и с адреса знакомого пользователя (рис. 2.33).

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

Верно.

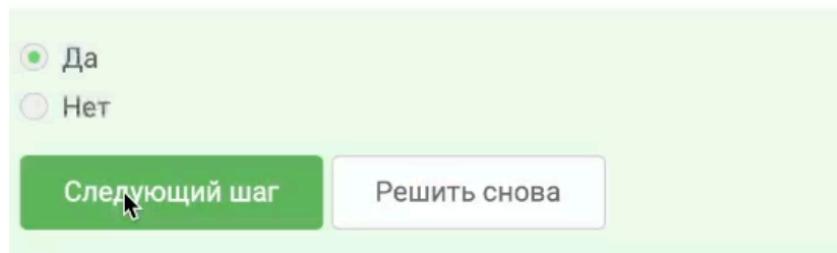


Рис. 2.33: Вопрос 3.3

2.8 Вредоносные программы

Спуфинг — подделка адреса отправителя email (рис. 2.34).

Email Спффинг -- это

Выберите один вариант из списка

 Отличное решение!

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.34: Вопрос 3.4

Трояны маскируются под обычное ПО, заражая систему при запуске (рис. 2.35).

Вирус-троян

Выберите один вариант из списка

Так точно!

- обязательно шифрует данные и вымогает ключ дешифрования
- маскируется под легитимную программу
- работает исключительно под ОС Windows
- разработан греками

Следующий шаг

Решить снова

Рис. 2.35: Вопрос 3.4

2.9 Шифрование в мессенджерах

При отправке первого сообщения создаётся ключ шифрования (рис. 2.36).

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Правильно.

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

Следующий шаг

Решить снова

Рис. 2.36: Вопрос 3.5

Сквозное шифрование скрывает содержимое переписки от сервера: только получатель может расшифровать сообщение (рис. 2.37).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

Абсолютно точно.

- 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

Рис. 2.37: Вопрос 3.5

2.10 Основы криптографии

Асимметричное шифрование использует пару ключей — публичный и приватный (рис. 2.38).

В асимметричных криптографических примитивах

Выберите один вариант из списка

Прекрасный ответ.

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

Следующий шаг

Решить снова

Рис. 2.38: Вопрос 4.1

Хэш-функции преобразуют данные в строку фиксированной длины и защищены от коллизий (рис. 2.39).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

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 захэшированных данных
 стойкая к коллизиям
 эффективно вычисляется
 дает на выходе фиксированное число бит независимо от объема входных данных

[Следующий шаг](#) [Решить снова](#)

Рис. 2.39: Вопрос 4.1

Представлены алгоритмы цифровых подписей (рис. 2.40).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

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](#).

AES
 SHA2
 RSA
 ECDSA
 ГОСТ Р 34.10-2012

[Следующий шаг](#) [Решить снова](#)

Рис. 2.40: Вопрос 4.1

MAC использует общий ключ для обеспечения целостности и аутентичности (рис. 2.41).

Код аутентификации сообщения относится к

Выберите один вариант из списка

 Верно. Так держать!

симметричным примитивам
 асимметричным примитивам

Следующий шаг  **Решить снова**

Рис. 2.41: Вопрос 4.1

Ответ основан на протоколе Диффи-Хеллмана (рис. 2.42).

Обмен ключами Диффи-Хэллмана - это

Выберите один вариант из списка

 Отличное решение!

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**

Рис. 2.42: Вопрос 4.1

2.11 Электронная подпись

ЭЦП использует криптографию с открытым ключом (рис. 2.43).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

 Хорошая работа.

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

Следующий шаг  **Решить снова**

Рис. 2.43: Вопрос 4.2

Для верификации используются обновление, подпись и открытый ключ (рис. 2.44).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

 Хорошая работа.

подпись, открытый ключ, сообщение
 подпись, открытый ключ
 подпись, секретный ключ, сообщение
 подпись, секретный ключ

Следующий шаг  **Решить снова**

Рис. 2.44: Вопрос 4.2

Подпись обеспечивает:

1. Целостность

2. Подтверждение личности

3. Неотказуемость

При компрометации ключа подпись становится ненадёжной (рис. 2.45).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка



Отличное решение!

- конфиденциальность
- аутентификацию
- неотказ от авторства
- целостность

Следующий шаг

Решить снова

Рис. 2.45: Вопрос 4.2

УКЭП приравнивается к обычной подписи и выдаётся удостоверяющим центром (рис. 2.46).

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

Выберите один вариант из списка

Хорошие новости, верно!

- простая
- усиленная квалифицированная
- усиленная неквалифицированная

[Следующий шаг](#)

[Решить снова](#)

Верно реши
Из всех поп

Рис. 2.46: Вопрос 4.2

Сертификат заверяется подписью удостоверяющего центра (рис. 2.47).

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

Выберите один вариант из списка

Отличное решение!

- в любой организации, имеющей соответствующую лицензию ФСБ
- в минкомсвязи РФ
- в удостоверяющем (сертификационном) центре
- в любой организации по месту работы

[Следующий шаг](#)

[Решить снова](#)

Верно реши
Из всех поп

Рис. 2.47: Вопрос 4.2

2.12 Платёжные системы

Среди популярных систем — Visa, MasterCard и МИР (рис. 2.48).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

 Абсолютно точно.

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

- BitCoin
- MasterCard
- SecurePay
- POS-терминал
- банкомат
- МФР

Следующий шаг

Решить снова

Рис. 2.48: Вопрос 4.3

Факторы идентификации:

1. Что я знаю — пароль
2. Что я имею — устройство
3. Кто я — биометрия
4. Где я — геолокация (рис. 2.49)

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

 Правильно, молодец!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [коих](#) 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

Рис. 2.49: Вопрос 4.3

Для онлайн-платежей банки применяют многофакторную аутентификацию (рис. 2.50).

При онлайн платежах сегодня используется

Выберите один вариант из списка

 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

Рис. 2.50: Вопрос 4.3

2.13 Блокчейн

Proof-of-Work — это способ валидации транзакций и создания блоков с помощью вычислений (рис. 2.51).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

 Отличное решение!

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.51: Вопрос 4.4

Свойства блокчейна:

1. Неизменяемость
2. Согласованность
3. Доступность
4. Открытость (рис. 2.52)

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

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](#).

- живучесть
- постоянства
- консенсус
- открытость

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.52: Вопрос 4.4

Участники используют закрытые ключи для создания цифровых подписей, подтверждающих транзакции. Публичный ключ позволяет проверить подпись (рис. 2.53).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Абсолютно точно.

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 2.53: Вопрос 4.4

3 Общий результат

Финальный результат (рис. 3.1).

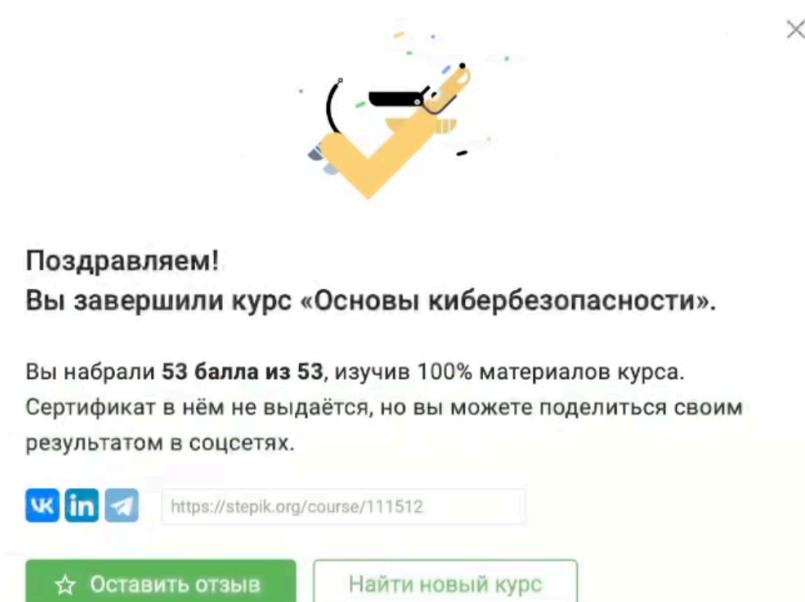


Рис. 3.1: Финал