

# **Отчет о выполнении внешнего курса:**

**Основы кибербезопасности**

Ежова Алиса Михайловна

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение внешнего курса	7
4	Безопасность в сети	8
5	2.1) Как работает интернет: базовые сетевые протоколы	9
6	2.2) Персонализация сети:	17
7	2.3) Браузер TOR. Анонимизация:	20
8	2.4) Беспроводные сети Wi-fi:	23
9	Защита ПК/телефона	27
10	3.1) Шифрование диска:	28
11	3.2) Пароли:	31
12	3.3) Фишинг:	36
13	3.4) Вирусы. Примеры:	38
14	3.5) Безопасность мессенджеров:	40
15	Криптография на практике	42
16	4.1) Введение в криптографию	43
17	4.2) Цифровая подпись:	47
18	4.3) Электронные платежи	52
19	4.4) Блокчейн	55
20	Выводы	58

# Список иллюстраций

5.1	Протокол прикладного уровня . . . . .	9
5.2	Уровень протокола TCP . . . . .	10
5.3	Корректные адреса IPv4 . . . . .	11
5.4	DNS сервер . . . . .	12
5.5	Модель TCP/IP . . . . .	13
5.6	Протокол http предполагает . . . . .	14
5.7	Протокол http состоит из . . . . .	14
5.8	Версия протокола TLS . . . . .	15
5.9	Фаза “рукопожатия” . . . . .	16
6.1	Хранение куки-файлов . . . . .	17
6.2	Куки не используются для . . . . .	18
6.3	Куки генерируются . . . . .	19
6.4	Сессионное хранение куки-файлов . . . . .	19
7.1	Узлы в луковой сети TOR? . . . . .	20
7.2	IP-адрес получателя известен . . . . .	21
7.3	Общий секретный ключ . . . . .	22
7.4	Использование браузера Tor . . . . .	22
8.1	Wi-Fi - это . . . . .	23
8.2	Уровень протокола WiFi . . . . .	24
8.3	Уровень протокола WiFi . . . . .	25
8.4	Передача данных между хостом сети и роутером . . . . .	25
8.5	Метод для домашней сети для аутентификации . . . . .	26
10.1	Шифровка загрузочного сектора диска . . . . .	28
10.2	На чем основано шифрование диска . . . . .	29
10.3	С помощью каких программ можно зашифровать жесткий диск . . . . .	30
11.1	Стойкий пароль . . . . .	31
11.2	Менеджер паролей . . . . .	32
11.3	Необходимость капчи . . . . .	33
11.4	Хэширование паролей . . . . .	34
11.5	Соль для улучшения стойкости . . . . .	35
11.6	Меры защищают от утечек данных . . . . .	35
12.1	Фишинговые ссылки . . . . .	36

12.2 Фишинговый имейл . . . . .	37
13.1 Email Спуфинг . . . . .	38
13.2 Вирус-троян . . . . .	39
14.1 Этап формирования ключа шифрования в протоколе мессенджеров Signal . . . . .	40
14.2 Суть сквозного шифрования . . . . .	41
16.1 Асимметричные криптографические примитивы . . . . .	43
16.2 Криптографическая хэш-функция . . . . .	44
16.3 Алгоритмы цифровой подписи . . . . .	45
16.4 Код аутентификации сообщения . . . . .	46
16.5 Обмен ключам Диффи-Хэллмана . . . . .	46
17.1 Протокол электронной цифровой подписи относится к . . . . .	47
17.2 Требования на вход . . . . .	48
17.3 Электронная цифровая подпись не обеспечивает . . . . .	49
17.4 Тип сертификата электронной подписи для налоговой отчетности ФНС . . . . .	50
17.5 Организация для выдачи сертификатов . . . . .	51
18.1 Платежные системы . . . . .	52
18.2 Многофакторная аутентификация . . . . .	53
18.3 Онлайн платежи . . . . .	54
19.1 Доказательство функции . . . . .	55
19.2 Свойства консенсуса в системах блокчейна . . . . .	56
19.3 Секретные ключи . . . . .	57

# 1 Цель работы

Освоить основные принципы и концепции кибербезопасности, овладеть ключевыми навыками для обеспечения защиты информации и данных, улучшить понимание угроз в сети интернет и способов их предотвращения, а также подготовиться к применению полученных знаний в реальных ситуациях для обеспечения безопасности в цифровом пространстве.

## 2 Задание

1. Пройти курс.
2. Выполнить все задания и тесты.
3. Получить сертификат.

### **3 Выполнение внешнего курса**

## **4 Безопасность в сети**



## 5 2.1) Как работает интернет: базовые сетевые протоколы

1. Выберите протокол прикладного уровня:

HTTPS является протоколом прикладного уровня. Протокол прикладного уровня сетевой протокол верхнего уровня (7-го в сетевой модели OSI и 4-го в стеке протоколов TCP/IP), обеспечивает взаимодействие сети и пользователя.

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

☒ Отлично!

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. 5.1: Протокол прикладного уровня

2. На каком уровне работает протокол TCP?:

TCP — это протокол управления передачей (Transmission Control Protocol). Его задача — управлять отправкой данных и следить за тем, чтобы они были гаран-

тировано приняты получателем. Именно гарантия получения данных и сделала этот протокол таким востребованным

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](#)

На каком уровне работает протокол TCP?

Выберите один вариант из списка

✓ Правильно.

Верно решили 939 учащихся  
Из всех попыток 61% верных

☒ Транспортном  
☐ Прикладном  
☐ Канальном  
☐ Сетевом

[Следующий шаг](#) [Решить снова](#)

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

Рис. 5.2: Уровень протокола TCP

### 3. Выберите все корректные адреса IPv4:

Стандартный IP-адрес называется IPv4. Это четыре числа, разделенные между собой точкой, причем каждое число в двоичном формате состоит из 8 цифр. В переводе в десятичные числа это значит, что все они находятся в диапазоне от 0 до 255. Одна цифра — один бит, и выходит, что в каждом IP-адресе четыре восьмибитных числа.

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзывНет, спасибо

Выберите все корректные адреса IPv4

**Выберите все подходящие ответы из списка**

☒ Хорошие новости, верно!

Верно решил 871 учащийся  
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

Рис. 5.3: Корректные адреса IPv4

#### 4. DNS сервер:

DNS-сервер — это специализированный компьютер (или группа), который хранит IP-адреса сайтов. Последние, в свою очередь, привязаны к именам сайтов и обрабатывает запросы пользователя. В интернете много DNS-серверов, они есть у каждого провайдера и обслуживают их пользователей.

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзывНет, спасибо

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. 5.4: DNS сервер

## 5. Выберите корректную последовательность протоколов в модели TCP/IP:

Прикладной – транспортный – сетевой – канальный Модель TCP/IP — это набор правил, по которым данные перемещаются по интернету. Главными здесь являются два протокола: TCP и IP. Они нужны, чтобы устанавливать надёжный канал связи между устройствами и передавать по нему данные. Кроме TCP и IP в модели есть и другие протоколы — например, HTTP, Ethernet, FTP и UDP.

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#) [Нет, спасибо](#)

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Хорошая работа.

Верно решил 941 учащийся  
Из всех попыток 53% верных

- ☐ сетевой – прикладной – канальный – транспортный
- ☐ прикладной – транспортный – канальный – сетевой
- ☐ транспортный – сетевой – прикладной – канальный
- ☒ прикладной – транспортный – сетевой – канальный

Следующий шаг

Решить снова

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

Рис. 5.5: Модель TCP/IP

## 6. Протокол http предполагает:

Передачу данных между клиентом и сервером в открытом виде. HTTP — это протокол, позволяющий получать различные ресурсы, например HTML-документы. Протокол HTTP лежит в основе обмена данными в Интернете. HTTP является протоколом клиент-серверного взаимодействия, что означает инициирование запросов к серверу самим получателем, обычно веб-браузером (web-browser).

Протокол http предполагает

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 965 учащихся  
Из всех попыток 78% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 5.6: Протокол http предполагает

## 7. Протокол https состоит из:

Двух фаз: рукопожатия и передачи данных. Система HTTPS похожа на провод, который состоит из двух слоёв: медная сердцевина и оболочка. Медная сердцевина ☒ основная часть провода, по которой идёт ток. Оболочка защищает контакты от внешних воздействий. Так, медная сердцевина ☒ это HTTP-протокол, а защитная оболочка ☒ это SSL-сертификат.

Протокол https состоит из

Выберите один вариант из списка

✓ Отлично!

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, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 5.7: Протокол http состоит из

## 8. Версия протокола TLS определяется:

И клиентом, и сервером в процессе “переговоров”. TLS — это протокол шифрования и аутентификации, разработанный для защиты интернет-коммуникаций.

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

---

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 947 учащихся  
Из всех попыток 55% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 5.8: Версия протокола TLS

## 9. В фазе “рукопожатия” протокола TLS не предусмотрено:

Шифрование данных. Если проверка TLS не работает, убедитесь, что на устройстве нет сертификатов, добавленных вручную. Они могут конфликтовать с сертификатами, развернутыми с помощью консоли администратора. Чтобы узнать об альтернативных способах настройки, обратитесь к поставщику веб-фильтра.

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

☒ Верно.

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 из 1

Рис. 5.9: Фаза “рукопожатия”



## 6 2.2) Персонализация сети:

### 1. Куки хранят:

Идентификатор пользователя и id сессии. Файлы cookie – это небольшие фрагменты текста, передаваемые в браузер с сайта, который вы открываете. С их помощью сайт запоминает информацию о ваших посещениях.

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

---

Куки хранят:

Выберите все подходящие ответы из списка

☒ Хорошая работа.

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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 6.1: Хранение куки-файлов

### 2. Куки не используются для:

Улучшения надежности соединения. Информация является анонимной и используется исключительно в статистических целях. Данные веб-аналитики и cookie-файлы невозможно использовать для того, чтобы установить Вашу лич-

ность, поскольку они никогда не содержат персональные данные, включая Ваши имя или адрес электронной почты.

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

---

Куки не используются для

**Выберите один вариант из списка**

✓ Прекрасный ответ.

Верно решили 950 учащихся  
Из всех попыток 53% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 6.2: Куки не используются для

### 3. Куки генерируются:

Сервером. Когда устройство подключается к серверу, он генерирует данные, которые записываются в файлы cookie. Эти данные содержат уникальный идентификатор пользователя и его устройства. Компьютер отправляет эти данные на сервер, который узнает вас по ID и предлагает информацию с учетом ваших предыдущих взаимодействий с сайтом.

Куки генерируются

Выберите один вариант из списка

☒ Хорошая работа.Верно решили 968 учащихся  
Из всех попыток 79% верных☐ клиентом☒ сервером

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 6.3: Куки генерируются

#### 4. Сессионные куки хранятся в браузере?:

Да, на время пользования веб-сайтом. Временные («сессионные») файлы cookie — эти файлы позволяют Администрации Сайта соединять действия пользователя во время сеанса браузера. Сеанс браузера начинается, когда пользователь открывает окно браузера, и завершается, когда пользователь закрывает его. Временные файлы cookie создаются на короткое время.

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Хорошая работа.Верно решили 959 учащихся  
Из всех попыток 60% верных☐ Нет☒ Да, на время пользования веб-сайтом☐ Да, на некоторое время, заданное в сервером

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 6.4: Сессионное хранение куки-файлов

## 7 2.3) Браузер TOR. Анонимизация:

### 1. Сколько промежуточных узлов в луковой сети TOR?:

В луковой сети TOR 3 промежуточных узла. Зашифрованные данные передаются через несколько сетевых узлов, называемых «луковыми роутерами», каждый из которых открывает один слой шифрования, чтобы узнать следующую точку передачи данных.

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

---

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Всё правильно.

Верно решили 959 учащихся  
Из всех попыток 77% верных

☐ 2

☒ 3

☐ 4

Следующий шаг Решить снова

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

Рис. 7.1: Узлы в луковой сети TOR?

### 2. IP-адрес получателя известен:

Отправителю и выходному узлу. То есть каждый узел, принимая пакет отправителя, смотрит, может ли он доставить его конечному получателю. Если может, он его перенаправляет в соответствии со своей таблицей маршрутизации на следующий узел. Следующий узел видит, что он тоже может доставить пакет, ну и так далее, пока пакет не дойдёт до финального адреса.

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ Верно. Так держать!

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 из 1

Рис. 7.2: IP-адрес получателя известен

### 3. Отправитель генерирует общий секретный ключ:

С охранным, промежуточным и выходным узлом. Он генерирует общие ключи последовательно с охранным узлом А, далее с промежуточным узлом В, а потом и с выходным узлом С. Вначале он непосредственно генерирует общий ключ KSA, то есть между отправителем S и охранным узлом А, потом охранный узел помогает сгенерировать общий ключ между S и между В, промежуточным узлом. Он перенаправляет данные, которые идут от отправителя к промежуточному узлу.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Отличное решение!

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 из 1

Рис. 7.3: Общий секретный ключ

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

Нет, браузер Tor использует сеть Tor для защиты конфиденциальности и анонимности. Использование сети Tor имеет две основных особенности: Ваш интернет-провайдер и все, кто способен наблюдать за вашими подключениями, не смогут отслеживать ваши действия в сети, включая названия и адреса посещаемых сайтов.

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

- ☐ Да
- ☒ Нет

Следующий шаг

Решить снова

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

Рис. 7.4: Использование браузера Tor

## 8 2.4) Беспроводные сети Wi-fi:

### 1. Wi-Fi - это:

Технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11. IEEE 802.11 - набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц. Пользователям более известен по названию Wi-Fi, фактически являющемуся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance.

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

---

Wi-Fi - это

Выберите один вариант из списка

☒ 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 из 1

Рис. 8.1: Wi-Fi - это

### 2. На каком уровне работает протокол WiFi?:

Канальном. Как и все стандарты этого семейства, IEEE 802.11 работает на нижних двух уровнях модели ISO/OSI, физическом и канальном.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 972 учащихся  
Из всех попыток 58% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 8.2: Уроень протокола WiFi

### 3. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi:

WEP, WEP был быстро признан небезопасным, и в 2003 году ему на смену пришел WPA (Wi-Fi Protected Access). WPA значительно превосходит WEP по уровню безопасности. В WPA используются более мощные алгоритмы шифрования, более надежный протокол аутентификации и более широкий набор функций безопасности.



Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 973 учащихся  
Из всех попыток 60% верных

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 8.3: Уроень протокола WiFi

#### 4. Данные между хостом сети (компьютером или смартфоном) и роутером:

Передаются в зашифрованном виде после аутентификации устройств. Wi-Fi-роутер раздает сигнал в виде радиоволн другим устройствам. Излучения разлетаются во все стороны, проходят сквозь воздух и стены, чтобы долететь до ноутбука и смартфонов. Телефон, Smart TV и другие устройства подключаются к маршрутизатору, чтобы получить доступ к интернету.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Отлично!

Верно решили 975 учащихся  
Из всех попыток 53% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 8.4: Передача данных между хостом сети и роутером

5. Для домашней сети для аутентификации обычно используется метод:

WPA2 Personal, если вы подключаетесь к домашней сети и получаете сообщение о слабом шифровании, измените тип шифрования на более надежный. Распространенные типы шифрования беспроводных сетей: WEP, TKIP, WPA, WPA2 (AES/CCMP). Главное отличие между ними — уровень защиты.

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

---

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 975 учащихся  
Из всех попыток 87% верных

☒ WPA2 Personal  
☐ WPA2 Enterprise

Следующий шаг Решить снова

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

Рис. 8.5: Метод для домашней сети для аутентификации

## **9 Защита ПК/телефона**

## 10 3.1) Шифрование диска:

1. Можно ли зашифровать загрузочный сектор диска?:

Да, можно зашифровать загрузочный сектор диска. Защита загрузочного сектора диска позволяет усилить безопасность системы, так как это первый сектор, который загружается при запуске компьютера.

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

☒ Хорошие новости, 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. 10.1: Шифровка загрузочного сектора диска

2. Шифрование диска основано на:

Шифрование диска на основе использования ключей симметричного шифрования - это один из наиболее распространенных методов шифрования данных на диске. Симметричное шифрование использует один и тот же ключ как для шифрования, так и для расшифрования данных.

Шифрование диска основано на

Выберите один вариант из списка

✓ Так 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 из 1

Рис. 10.2: На чем основано шифрование диска

### 3. С помощью каких программ можно зашифровать жесткий диск?: BitLocker и VeraCrypt

Да, с помощью программного обеспечения BitLocker и VeraCrypt можно зашифровать жесткий диск для обеспечения безопасности данных. Вот краткое объяснение обеих программ:

BitLocker - это интегрированное средство шифрования диска, предоставляемое компанией Microsoft для операционных систем Windows. VeraCrypt - это бесплатное программное обеспечение с открытым исходным кодом, которое предоставляет возможности шифрования дисков на различных операционных системах, включая Windows, macOS и Linux.

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Абсолютно точно.

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

☒ BitLocker

☒ VeraCrypt

Следующий шаг

Решить снова

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

Рис. 10.3: С помощью каких программ можно зашифровать жесткий диск

## 11 3.2) Пароли:

### 1. Какие пароли можно отнести к стойким?:

Пароль - UQr9@j4!S\$ можно отнести к стойким, так как содержит 10 разнообразных символов, наличие специальных символов и случайность.

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

---

Какие пароли можно отнести к стойким?

Выберите один вариант из списка

☒ Верно. Так держать!

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

30 6 Шаг 4 Следующий шаг >

Рис. 11.1: Стойкий пароль

### 2. Где безопасно хранить пароли?:

В менеджерах паролей. Менеджеры паролей используют сильное шифрование для хранения паролей, что делает их практически непроницаемыми для злоумышленников.

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решил 971 учащийся  
Из всех попыток 74% верных

- ☒ В менеджерах паролей
- ☐ В записках на рабочем столе
- ☐ В записках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг

Решить снова

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

Рис. 11.2: Менеджер паролей

### 3. Зачем нужна капча?:

Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа. Капча необходима для защиты от различных видов автоматизированных атак, таких как спам-боты, бот-атаки на веб-ресурсы, попытки взлома аккаунтов и т.д. Поскольку автоматизированные программы часто не могут успешно пройти капчу, она помогает обеспечить защиту от несанкционированного доступа и злоупотреблений.



Зачем нужна капча?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 974 учащихся  
Из всех попыток 77% верных

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

Следующий шаг

Решить снова

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

Рис. 11.3: Необходимость капчи

#### 4. Для чего применяется хэширование паролей?:

Для того, чтобы не хранить пароли на сервере в открытом виде. Хэширование паролей применяется для обеспечения безопасности пользовательских данных. Когда пользователь создает учетную запись и устанавливает пароль, этот пароль хэшируется - таким образом, он преобразуется в набор символов, который нельзя прочитать обратно. Этот хэшированный пароль затем сохраняется на сервере. Когда пользователь входит в систему, введенный им пароль также хэшируется и сравнивается с хэшем, хранящимся на сервере.

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 из 1

Рис. 11.4: Хэширование паролей

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

Нет, если злоумышленник уже получил доступ к серверу, соль не будет эффективной, потому что она хранится вместе с зашифрованными паролями на сервере. Поэтому, если злоумышленник имеет доступ к серверу, он сможет получить и соль, и зашифрованные пароли, и, возможно, восстановить исходные пароли с помощью атаки перебором.

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

Выберите один вариант из списка

☒ Всё получилось!

Верно решили 967 учащихся  
Из всех попыток 66% верных

☐ Да  
☒ Нет

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

30 6

Шаг 8

Следующий шаг >

Рис. 11.5: Соль для улучшения стойкости

## 6. Какие меры защищают от утечек данных атакой перебором?:

Разные пароли на всех сайтах, Периодическая смена паролей, Сложные(=длинные) пароли, капча. Все варианты верны, в ходе прохождения курса мы в этом убедились.

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Правильно.

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

☒ 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. 11.6: Меры защищают от утечек данных

## 12 3.3) Фишинг:

1. Какие из следующих ссылок являются фишинговыми?:

<https://online.sberbank.wix.ru/CSAFront/index.do> (вход в Сбербанк.Онлайн) и [https://passport.yandex.ucoz.ru/auth?origin=home\\_desktop\\_ru](https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru) (вход в аккаунт Яндекс). Эти ссылки выглядят как фишинговые, потому что они содержат доменные имена, отличные от официальных доменов Сбербанка и Яндекса. Настоящие сайты Сбербанка и Яндекса имеют другие домены: [sberbank.ru](https://sberbank.ru) и [yandex.ru](https://yandex.ru) соответственно.

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

---

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно решил 861 учащийся  
Из всех попыток 19% верных

✓ 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](https://e.mail.ru/login?lang=ru_RU) (вход в аккаунт Mail.Ru)
- ☒ [https://passport.yandex.ucoz.ru/auth?origin=home\\_desktop\\_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. 12.1: Фишинговые ссылки

2. Может ли фишинговый имейл прийти от знакомого адреса?:

Да, фишинговый имейл может прийти от знакомого адреса. Киберпреступники могут подделывать адреса отправителей, чтобы создать впечатление, что имейлы приходят от знакомых или официальных организаций. Это может включать в себя подделку адресов электронной почты, чтобы выглядеть как отправитель известного человека или компании.

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

---

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Да  
☐ Нет

Здорово, всё верно.

Верно решили 966 учащихся  
Из всех попыток 90% верных

Следующий шаг Решить снова

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

👍 22 👎 8 Шаг 5 Следующий шаг >

Рис. 12.2: Фишинговый имейл

## 13 3.4) Вирусы. Примеры:

### 1. Email Спуфинг – это:

Подмена адреса отправителя в имейлах.

3.4 Вирусы. Примеры 5 из 5 шагов пройдено 2 из 2 баллов получено

---

Email Спуфинг – это

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 960 учащихся  
Из всех попыток 65% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 13.1: Email Спуфинг

### 2. Вирус-троян:

Маскируется под легитимную программу. Когда вирус-троян маскируется под легитимную программу, он представляет себя как полезное или безопасное программное обеспечение, чтобы обмануть пользователей и получить доступ к их компьютерам или украсть их конфиденциальные данные.

### Вирус-троян

Выберите один вариант из списка

✓ Правильно.

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

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

Следующий шаг

Решить снова

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

Рис. 13.2: Вирус-троян

## 14 3.5) Безопасность мессенджеров:

1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?:

При генерации первого сообщения стороной-отправителем. Signal использует протокол двухфакторной аутентификации для формирования ключа шифрования при генерации первого сообщения стороной-отправителем. Этот процесс включает в себя обмен ключами Diffie-Hellman, который позволяет сторонам обмениваться секретными ключами, не передавая их по открытым каналам связи. В итоге формируется общий секретный ключ, который используется для шифрования и расшифрования сообщений.

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

---

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Верно решили 952 учащихся  
Из всех попыток 52% верных

☒ Правильно, молодец!

☐ при каждом новом сообщении от стороны-отправителя

☒ при генерации первого сообщения стороной-отправителем

☐ при получении сообщения

☐ при установке приложения

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 14.1: Этап формирования ключа шифрования в протоколе мессенджеров Signal

2. Суть сквозного шифрования состоит в том, что:



Сообщения передаются по узлам связи (серверам) в зашифрованном виде. Сквозное шифрование используется для обеспечения конфиденциальности и безопасности передаваемых сообщений. Каждый узел расшифровывает сообщение только в том случае, если он является адресатом. Это обеспечивает защиту данных во время их передачи по сети.

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

---

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 964 учащихся  
Из всех попыток 60% верных

- ☒ сообщения передаются по узлам связи (серверам) в зашифрованном виде
- ☐ сервер получает сообщения в открытом виде для передачи нужному получателю
- ☐ сервер перешифровывает сообщения в процессе передачи
- ☐ сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг Решить снова

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

Рис. 14.2: Суть сквозного шифрования

## **15 Криптография на практике**

## 16 4.1) Введение в криптографию

### 1. В асимметричных криптографических примитивах?

Обе стороны имеют пару ключей. В асимметричной криптографии каждая сторона имеет два ключа: открытый и закрытый. Открытый ключ используется для зашифрования данных, в то время как закрытый ключ используется для их расшифровки. Использование пары ключей позволяет обеспечить безопасную передачу информации, поскольку один из ключей может быть использован для шифрования сообщения, а другой - для его расшифровки. Этот подход позволяет уменьшить риски компрометации безопасности, поскольку открытый ключ может быть распространен свободно, в то время как закрытый ключ хранится в секрете.

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

В асимметричных криптографических примитивах

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 940 учащихся  
Из всех попыток 42% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 16.1: Асимметричные криптографические примитивы

## 2. Криптографическая хэш-функция:

Стойкая к коллизиям, дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется. ПрIMITив, который выходит за рамки симметричной и асимметричной криптографии, поскольку он бесключевой. Примером такого криптографического примитива является криптографическая хэш-функция. В науке есть просто хэш-функция, а есть криптографическая хэш-функция. Криптографическая хэш-функция берет на вход произвольный объем данных, то есть какие-то биты и выдает на выходе фиксированную строку, например длины  $n$ .

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

---

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Прекрасный ответ.

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

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 16.2: Криптографическая хэш-функция

## 3. К алгоритмам цифровой подписи относятся:

RSA, ECDSA, ГОСТ Р 34.10-2012. Ежедневное применение цифровой подписи – это сертификаты. К примерам цифровой подписи относятся интернет-сертификаты, подпись RSA, американский стандарт ECDSA и отечественный стандарт ГОСТ стандарт Р 34.20.2012.

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Правильно.

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** из 1

Рис. 16.3: Алгоритмы цифровой подписи

4. Код аутентификации сообщения относится к:

Симметричным примитивам. Как правило, код аутентификации сообщения относится к симметричным примитивам криптографии, поскольку он использует один и тот же секретный ключ для создания и проверки подписи сообщения. В отличие от асимметричной криптографии, где используются пары открытого и закрытого ключей, симметричная криптография применяет только один общий ключ.

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 949 учащихся  
Из всех попыток 69% верных

- ☐ асимметричным примитивам  
☒ симметричным примитивам

Следующий шаг

Решить снова

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

Рис. 16.4: Код аутентификации сообщения

## 5. Обмен ключам Диффи-Хэллмана - это:

Асимметричный примитив генерации общего секретного ключа. Этот метод использует асимметричное шифрование, где каждая сторона генерирует свой закрытый и открытый ключи. Стороны обмениваются открытыми ключами, после чего они могут вычислить общий секретный ключ, который будет использоваться для шифрования и дешифрования сообщений между ними.

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 942 учащихся  
Из всех попыток 47% верных

- ☐ симметричный примитив генерации общего секретного ключа  
☐ асимметричный примитив генерации общего открытого ключа  
☒ асимметричный примитив генерации общего секретного ключа  
☐ асимметричный алгоритм шифрования

Следующий шаг

Решить снова

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

Рис. 16.5: Обмен ключам Диффи-Хэллмана

## 17 4.2) Цифровая подпись:

1. Протокол электронной цифровой подписи относится к:

Протоколам с публичным (или открытым) ключом. Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом, так как он использует асимметричное шифрование. В этом случае у каждого участника есть пара ключей: закрытый и открытый. Закрытый ключ известен только владельцу, а открытый ключ может быть распространен публично. При создании электронной цифровой подписи сообщения подписывается закрытым ключом отправителя, а затем можно проверить подлинность подписи с помощью открытого ключа получателя.

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

---

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Всё получилось!

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Верно решили 909 учащихся  
Из всех попыток 70% верных

Рис. 17.1: Протокол электронной цифровой подписи относится к

2. Алгоритм верификации электронной цифровой подписи требует на вход:

Подпись, открытый ключ, сообщение. Алгоритм верификации электронной цифровой подписи использует подпись, открытый ключ и сообщение для проверки подлинности и целостности данных. Когда получатель получает подпись и сообщение, он использует открытый ключ отправителя для проверки подписи. Алгоритм проверяет, что подпись действительно была создана закрытым ключом отправителя и что данные не были изменены после создания подписи.

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

---

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 903 учащихся  
Из всех попыток 45% верных

- ☐ 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. 17.2: Требования на вход

### 3. Электронная цифровая подпись не обеспечивает:

Конфиденциальность. Она предназначена для проверки подлинности и целостности данных, а не для их защиты от несанкционированного доступа. Для обеспечения конфиденциальности данных необходимо использовать другие методы, такие как шифрование. Шифрование позволяет скрыть содержимое сообщения от посторонних лиц, в то время как электронная цифровая подпись обеспечивает возможность проверки авторства и целостности данных.



Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Верно.

Верно решили **904** учащихся  
Из всех попыток **51%** верных

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

Следующий шаг

Решить снова

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

Рис. 17.3: Электронная цифровая подпись не обеспечивает

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

Усиленная квалифицированная. Усиленная квалифицированная электронная подпись (ЭП) - это самый высокий уровень сертификата электронной подписи, который обеспечивает наивысший уровень безопасности и подлинности. Для отправки налоговой отчетности в Федеральную налоговую службу (ФНС) требуется использование усиленной квалифицированной ЭП. Такой сертификат подтверждает личность владельца ЭП и его право действовать от имени организации или индивидуального предпринимателя.

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

Выберите один вариант из списка

☒ Верно.

Верно решили **904** учащихся  
Из всех попыток **67%** верных

- ☒ усиленная квалифицированная
- ☐ простая
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

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

Рис. 17.4: Тип сертификата электронной подписи для налоговой отчетности ФНС

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

В удостоверяющем (сертификационном) центре. Квалифицированный сертификат ключа проверки электронной подписи можно получить в удостоверяющем (сертификационном) центре. Удостоверяющие центры выпускают сертификаты, подтверждающие подлинность и квалификацию электронной подписи, что позволяет использовать ее для юридически значимых документов и процессов, включая отправку налоговой отчетности в налоговые органы.

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

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили **902** учащихся  
Из всех попыток **60%** 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** из 1

Рис. 17.5: Организация для выдачи сертификатов

## 18 4.3) Электронные платежи

1. Выберите из списка все платежные системы:

MasterCard и МИР, самые распространенные платежные системы.

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно. Верно решили 833 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](#).

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

Следующий шаг Решить снова

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

Рис. 18.1: Платежные системы

2. Примером многофакторной аутентификации является:

Комбинация проверка пароля + код в sms сообщении и комбинация код в sms сообщении + отпечаток пальца. Многофакторная аутентификация представляет собой процесс проверки личности пользователя с использованием нескольких различных методов подтверждения.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Абсолютно точно.

Верно решили **819** 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](#).

- ☐ 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. 18.2: Многофакторная аутентификация

### 3. При онлайн платежах сегодня используется:

Многофакторная аутентификация покупателя перед банком-эмитентом. Многофакторная аутентификация покупателя перед банком-эмитентом означает, что для завершения транзакции покупатель должен пройти процесс проверки личности с использованием нескольких различных методов подтверждения перед своим банком-эмитентом. Это делается для повышения безопасности онлайн платежей и защиты от мошенничества.

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили **878** учащихся  
Из всех попыток **59%** верных

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ однофакторная аутентификация покупателя перед банком-эквайером
- ☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- ☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг

Решить снова

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

Рис. 18.3: Онлайн платежи

## 19 4.4) Блокчейн

1. Какое свойство криптографической хэш-функции используется в доказательстве работы?:

Сложность нахождения прообраза. Свойство криптографической хэш-функции, которое используется в доказательстве работы (Proof of Work), это сложность нахождения прообраза. Криптографическая хэш-функция преобразует входные данные произвольной длины в фиксированную строку определенной длины (хэш). Однако, важной характеристикой криптографической хэш-функции является то, что она должна быть устойчива к обратному поиску - то есть, при известном хэше сложно найти исходные данные (прообраз), которые привели к этому хэшу.

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

---

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решили 892 учащихся  
Из всех попыток 48% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 19.1: Доказательство функции

## 2. Консенсус в некоторых системах блокчейн обладает свойствами:

Консенсус, живучесть, открытость, постоянства. Консенсус в системах блокчейн означает достижение единства и согласия между всеми участниками сети относительно правильности и последовательности транзакций. Это важное свойство обеспечивает работоспособность и надежность блокчейн-сети.

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

---

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Так точно!

Верно решили 803 учащихся  
Из всех попыток 22% 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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 19.2: Свойства консенсуса в системах блокчейна

## 3. Секретные ключи какого криптографического примитива хранят участники блокчейна?:

Цифровая подпись. Участники блокчейна хранят секретные ключи для использования в криптографической подписи. Цифровая подпись - это криптографический примитив, который используется для аутентификации и подтверждения подлинности цифровой информации. При проведении транзакций в блокчейне участники создают цифровую подпись, используя свой секретный ключ, чтобы подтвердить свое согласие на выполнение операции.



Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 890 учащихся  
Из всех попыток 47% верных

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

Следующий шаг

Решить снова

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

Рис. 19.3: Секретные ключи

## 20 Выводы

Кибербезопасность также стала важной темой для многих образовательных программ. Университеты и колледжи по всему миру активно включают курсы по кибербезопасности в свои программы, понимая актуальность и востребованность данной профессии в современном мире.

В целом, кибербезопасность является многогранной проблемой, требующей постоянного внимания, инноваций и адаптации к меняющемуся цифровому миру.

В заключение можно сказать, что вопросы кибербезопасности требуют комплексного подхода, включая технические, организационные и образовательные меры. Только совместные усилия могут обеспечить адекватный уровень защиты в условиях постоянно меняющегося цифрового ландшафта.

В этой работе я: - поняла, как работает Интернет, и какие у него “слабые” места

- уяснила, почему 1245YOURNAME – плохой пароль
- научилась отличать шифрование от электронной подписи
- узнать, как работают электронные платежи