

Курс Stepik Основы кибербезопасности

Основы информационной безопасности

Басманова Дарья Кирилловна

Содержание

1	Цель работы	6
2	Задание	7
3	Выполнение внешнего курса	8
4	2.Безопасность сети	9
5	2.1 Как работает интернет: базовые сетевые протоколы	10
6	2.2 Персонализация сети	16
7	2.3. Браузер TOR. Анонимизация	19
8	2.4 Беспроводные сети Wi-fi	22
9	3. Защита ПК/телефона	25
10	3.1. Шифрование диска:	26
11	3.3. Фишинг:	32
12	3.4. Вирусы. Примеры:	34
13	3.5. Безопасность мессенджеров:	36
14	Криптография на практике.	38
15	4.2. Цифровая подпись	42
16	Выводы	51

Список иллюстраций

5.1	ответ - TTPS	10
5.2	ответ - Транспортном	11
5.3	ответ на IPv4	11
5.4	ответ- сопоставляет IP адреса доменным именам	12
5.5	ответ - прикладной – транспортный – сетевой – канальный	13
5.6	ответ на вопрос	13
5.7	ответ - двух фаз: рукопожатия и передачи данных	14
5.8	ответ- и клиентом, и сервером в процессе “переговоров”	14
5.9	ответ - шифрование данных	15
6.1	ответ - идентификатор пользователя	16
6.2	ответ - улучшения надежности соединения	17
6.3	ответ - сервером	17
6.4	ответ - Да, на время пользования веб-сайтом	18
7.1	ответ - 3	19
7.2	ответ - отправител, выходному узлу	20
7.3	ответ - с охраным, промежуточным и выходном узлом	20
7.4	ответ - нет	21
8.1	ответ дан	22
8.2	ответ - Канальном	23
8.3	ответ - WEP	23
8.4	ответ на фото	24
8.5	ответ - WPA2 Personal	24
10.1	Шифровка загрузочного сектора диска	26
10.2	На чем основано шифрование диска	27
10.3	Стойкий пароль	28
10.4	Менеджер паролей	29
10.5	Необходимость капчи	29
10.6	Хэширование паролей	30
10.7	Соль для улучшения стойкости	31
10.8	Меры защищают от утечек данных	31
11.1	Фишинговые ссылки	32
11.2	Фишинговый имейл	33

12.1 Email Спуфинг	34
12.2 Вирус-троян	35
13.1 Этап формирования ключа шифрования в протоколе мессенджеров Signal	36
13.2 Суть сквозного шифрования	37
14.1 Название рисунка	38
14.2 Криптографическая хэш-функция	39
14.3 К алгоритмам цифровой подписи относятся	40
14.4 Код аутентификации сообщения относится к	40
14.5 Обмен ключам Диффи-Хэллмана – это	41
15.1 Протокол электронной цифровой подписи относится к	43
15.2 Алгоритм верификации электронной цифровой подписи требует на вход	43
15.3 Электронная цифровая подпись не обеспечивает	44
15.4 Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?	45
15.5 В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?	45
15.6 Выберите из списка все платежные системы.	46
15.7 Примером многофакторной аутентификации является	47
15.8 При онлайн платежах сегодня используется	48
15.9 Какое свойство криптографической хэш-функции используется в доказательстве работы?	49
15.10 Консенсус в некоторых системах блокчейн обладает свойствами	49
15.11 Секретные ключи какого криптографического примитива хранят участники блокчейна?	50

Список таблиц

1 Цель работы

Цель изучения основ кибербезопасности:

- Понять угрозы и риски в киберпространстве, включая различные типы кибератак и их влияние на организации и отдельных лиц.
- Получить знания о основных принципах и технологиях кибербезопасности, таких как шифрование, управление доступом и обнаружение вторжений.
- Развить навыки оценки и управления рисками кибербезопасности, что позволяет принимать обоснованные решения для защиты систем и данных.
- Понять законодательные и нормативные требования, связанные с кибербезопасностью, и обеспечить соответствие им.
- Научиться эффективно реагировать на кибератаки, включая сдерживание, обнаружение и восстановление.
- Повысить осведомленность о передовых методах киберпреступников и быть в курсе последних тенденций в сфере кибербезопасности.
- Подготовить специалистов по кибербезопасности к защите критически важных активов, таких как конфиденциальные данные, финансовые системы и критическая инфраструктура.
- Способствовать созданию более безопасного и надежного киберпространства для всех.

2 Задание

Задачи

- понять, как работает Интернет, и какие у него “слабые” места
- уяснить, почему 1245YOURNAME – плохой пароль
- научиться отличать шифрование от электронной подписи
- узнать, как работают электронные платежи

3 Выполнение внешнего курса

4 2.Бензопастность сети

5 2.1 Как работает интернет: базовые сетевые протоколы

2.1.1. 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.

✓ Всё получилось!

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг

Решить снова

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

Рис. 5.1: ответ - TTPS

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

✓ Абсолютно точно.

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

[Следующий шаг](#) [Решить снова](#)

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

Рис. 5.2: ответ - Транспортном

2.1.3. 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.

☐ 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. 5.3: ответ на IPv4

2.1.4. 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.

The image shows a quiz interface with a light green background. It contains a list of four options, each preceded by a radio button. The first option is selected. Below the list are two buttons: a green one labeled 'Следующий шаг' and a white one labeled 'Решить снова'. At the bottom, there is a link 'Ваши решения' and a score display 'Вы получили: 1 балл из 1'.

- ☒ 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: ответ- сопоставляет IP адреса доменным именам

2.1.5. Выберите корректную последовательность протоколов в модели TCP/IP

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

✓ Хорошие новости, верно!

- ☐ 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: ответ - прикладной – транспортный – сетевой – канальный

2.1.6. Протокол http предполагает

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)

✓ Хорошая работа.

- ☐ 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: ответ на вопрос

2.1.7. Протокол https состоит из

Система HTTPS похожа на провод, который состоит из двух слоёв: медная сердцевина и оболочка. Медная сердцевина ☒ основная часть провода, по кото-

рой идёт ток. Оболочка защищает контакты от внешних воздействий. Так, мед-
ная сердцевина ☒ это HTTP-протокол, а защитная оболочка ☒ это SSL-сертифика

○ 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: ответ - двух фаз: рукопожатия и передачи данных

2.1.8. Версия протокола TLS определяется

Что такое TLS-рукопожатие? TLS — это протокол шифрования и аутентифика-
ции, разработанный для защиты интернет-коммуникаций.

○ 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: ответ- и клиентом, и сервером в процессе “переговоров”

2.1.9. В фазе “рукопожатия” протокола TLS не предусмотрено

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

☐ формирование общего секретного ключа между клиентом и сервером

☐ аутентификация (как минимум одной из сторон)

☐ выбираются алгоритмы шифрования/аутентификации

☒ шифрование данных

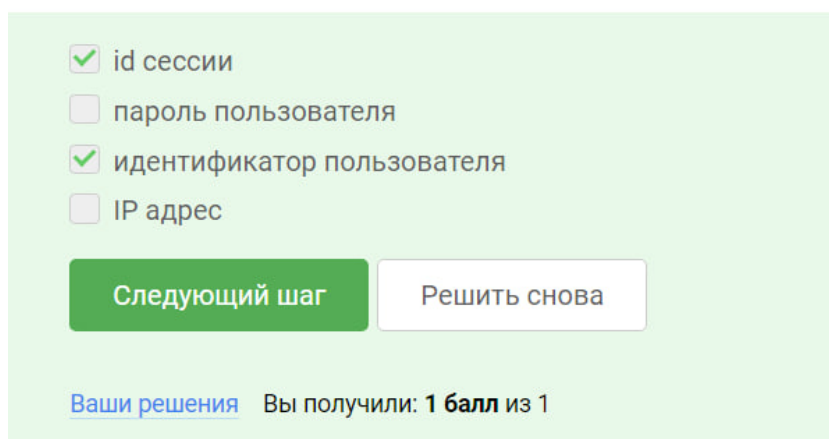
[Ваше решение](#) Вы получили: **1 балл** из 1

Рис. 5.9: ответ - шифрование данных

6 2.2 Персонализация сети

2.2.1. Куки хранят:

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



The image shows a light green rectangular box containing a list of four items, each with a checkbox and text:

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

Below the list are two buttons: a green button with the text "Следующий шаг" and a white button with a grey border and the text "Решить снова".

At the bottom left of the box is a blue link "Ваши решения" followed by the text "Вы получили: 1 балл из 1".

Рис. 6.1: ответ - идентификатор пользователя

2.2.2. Куки не используются для

Информация является анонимной и используется исключительно в статистических целях. Данные веб-аналитики и cookie-файлы невозможно использовать для того, чтобы установить Вашу личность, поскольку они никогда не содержат персональные данные, включая Ваши имя или адрес электронной почты.

A screenshot of a quiz interface with a light green background. It contains five radio button options: 'аутентификации пользователя', 'персонализации веб-страниц', 'отслеживания информации о пользователе', 'сборе статистики посещаемости сайта', and 'улучшения надежности соединения'. The last option is selected. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link and 'Вы получили: 1 балл из 1'.

☐ 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: ответ - улучшения надежности соединения

2.2.3. Куки генерируются

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.

A screenshot of a quiz interface with a light green background. It contains two radio button options: 'сервером' (selected) and 'клиентом'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link and 'Вы получили: 1 балл из 1'.

☒ сервером

☐ клиентом

Следующий шаг Решить снова

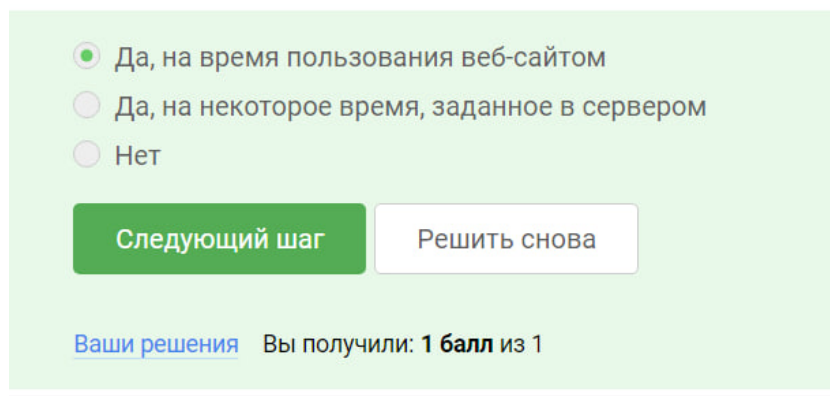
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 6.3: ответ - сервером

2.2.4. Сессионные куки хранятся в браузере?

Временные («сессионные») файлы cookie — эти файлы позволяют Администрации Сайта соединять действия пользователя во время сеанса браузера. Се-

анс браузера начинается, когда пользователь открывает окно браузера, и завершается, когда пользователь закрывает его. Временные файлы cookie создаются на короткое время.



The image shows a quiz interface with a light green background. It contains three radio button options, two buttons, and a score display.

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

Below the options are two buttons: a green button labeled "Следующий шаг" and a white button with a grey border labeled "Решить снова".

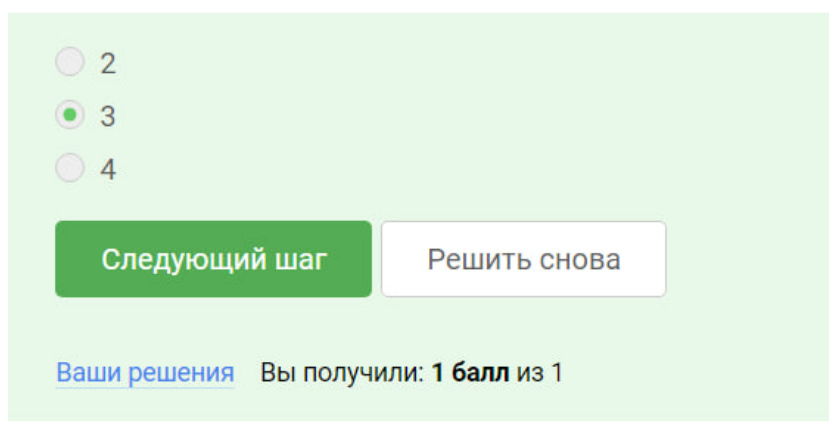
At the bottom, there is a link "Ваши решения" and a score display "Вы получили: **1 балл** из 1".

Рис. 6.4: ответ - Да, на время пользования веб-сайтом

7 2.3. Браузер TOR. Анонимизация

2.3.1. Сколько промежуточных узлов в луковой сети TOR?

3, луковой сети сообщения обернуты в несколько слоев шифрования, подобно слоям лука. 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

☐ 4

[Следующий шаг](#) [Решить снова](#)

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

Рис. 7.1: ответ - 3

2.3.2. IP-адрес получателя известен

отправителю, 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

☐ охранному узлу

☐ промежуточному узлу

☒ отправителю

☒ выходному узлу

Следующий шаг **Решить снова**

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

Рис. 7.2: ответ - отправител, выходному узлу

2.3.3. Отправитель генерирует общий секретный ключ

с охранным, промежуточным и выходном 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 K_{SA} , 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.

☐ только с охранным узлом

☐ с охранным и промежуточным узлом

☒ с охранным, промежуточным и выходным узлом

☐ с промежуточным и выходным узлом

Следующий шаг **Решить снова**

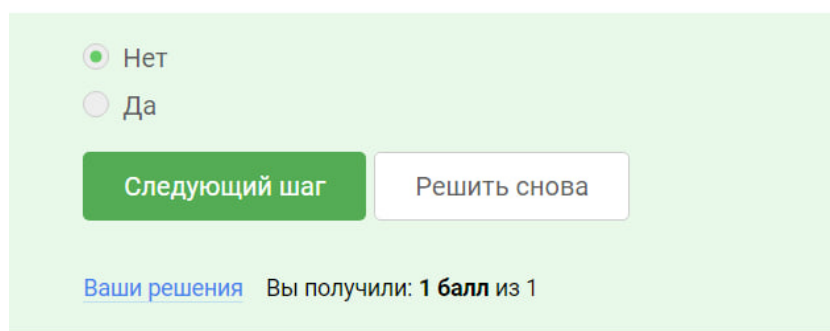
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 7.3: ответ - с охранным, промежуточным и выходном узлом

2.3.4. 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.

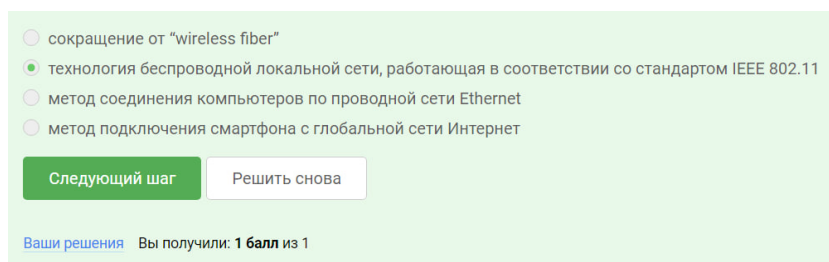


The image shows a quiz interface with a light green background. At the top, there are two radio button options: 'Нет' (No) with a green dot, and 'Да' (Yes) with a grey dot. Below the options are two buttons: a green button labeled 'Следующий шаг' (Next step) and a white button with a grey border labeled 'Решить снова' (Solve again). At the bottom, there is a blue link 'Ваши решения' (Your solutions) followed by the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 7.4: ответ - нет

8 2.4 Беспроводные сети Wi-fi

2.4.1. 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.



The screenshot shows a quiz interface with four radio button options. The second option, 'технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11', is selected with a green dot. Below the options are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

- ☐ 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: ответ дан

2.4.2. На каком уровне работает протокол WiFi? Канальном. Как и все стандарты этого семейства, Wi-Fi 802.11 работает на нижних двух уровнях модели ISO/OSI, физическом и канальном.

Рис. 8.2: ответ - Канальном

2.4.3. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

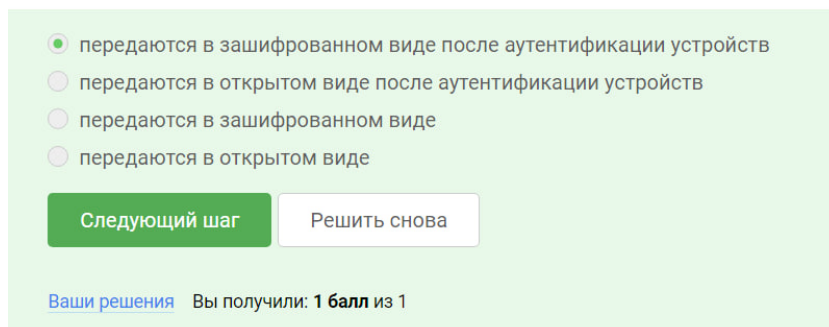
WEP

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.

Рис. 8.3: ответ - WEP

2.4.4. 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



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

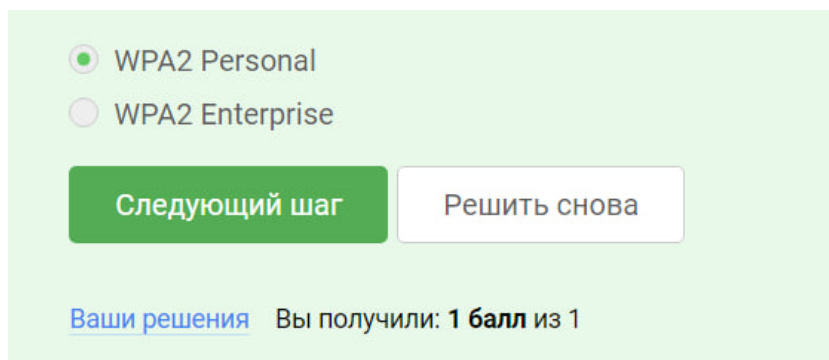
[Следующий шаг](#) [Решить снова](#)

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

Рис. 8.4: ответ на фото

2.4.5. 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.



☒ WPA2 Personal
☐ WPA2 Enterprise

[Следующий шаг](#) [Решить снова](#)

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

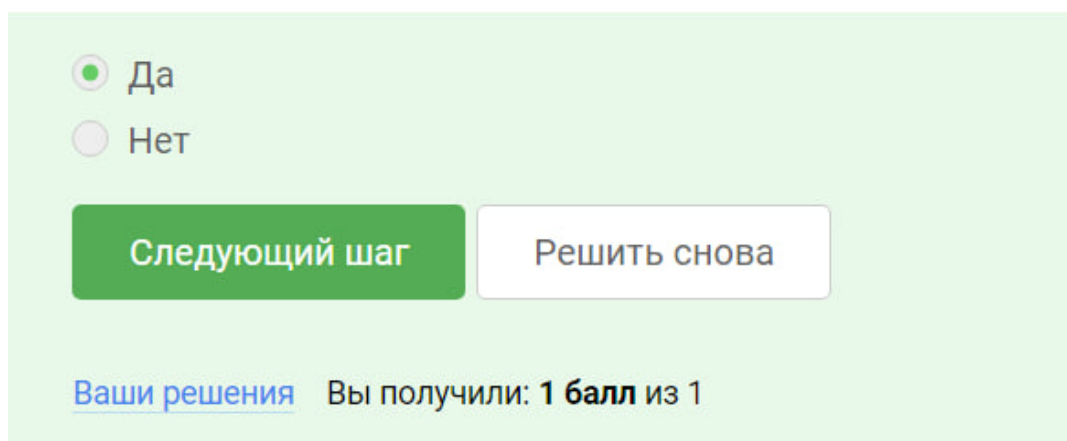
Рис. 8.5: ответ - WPA2 Personal

9 3. Защита ПК/телефона

10 3.1. Шифрование диска:

3.1.1. 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.

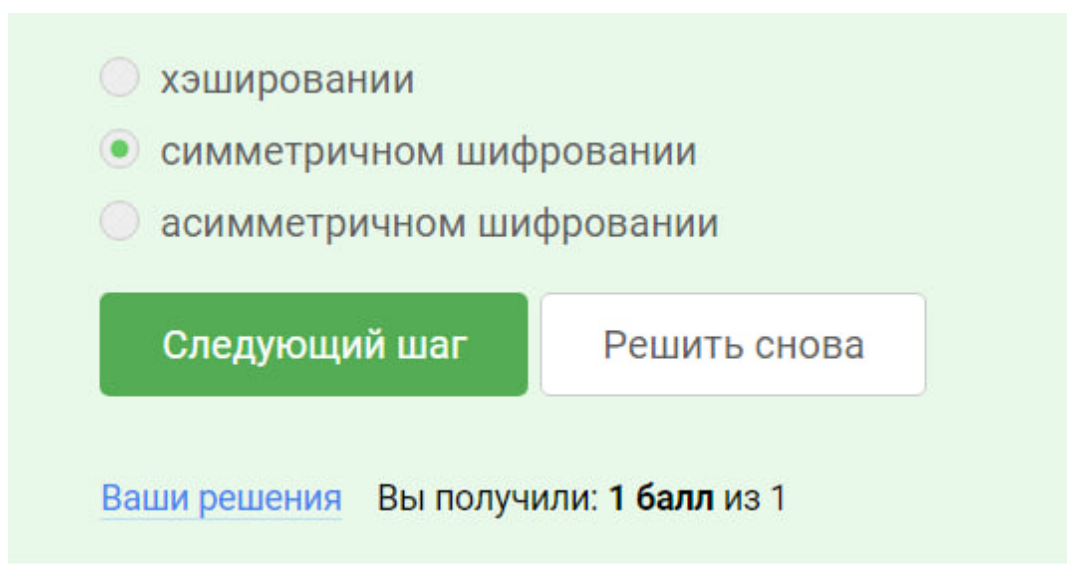


The image shows a quiz interface with a light green background. At the top, there are two radio button options: 'Да' (Yes) which is selected, and 'Нет' (No). Below these are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a blue link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 10.1: Шифровка загрузочного сектора диска

3.1.2. 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.



☐ 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

3.1.3. 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.

☐ Wireshark

☐ Disk Utility

☒ VeraCrypt

☒ BitLocker

Следующий шаг **Решить снова**

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

3.2.

Пароли:

3.2.1. 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.

☐ qwerty12345

☐ ILOVECATS

☒ UQr9@j4!S\$

☐ IDONTLOVECATS

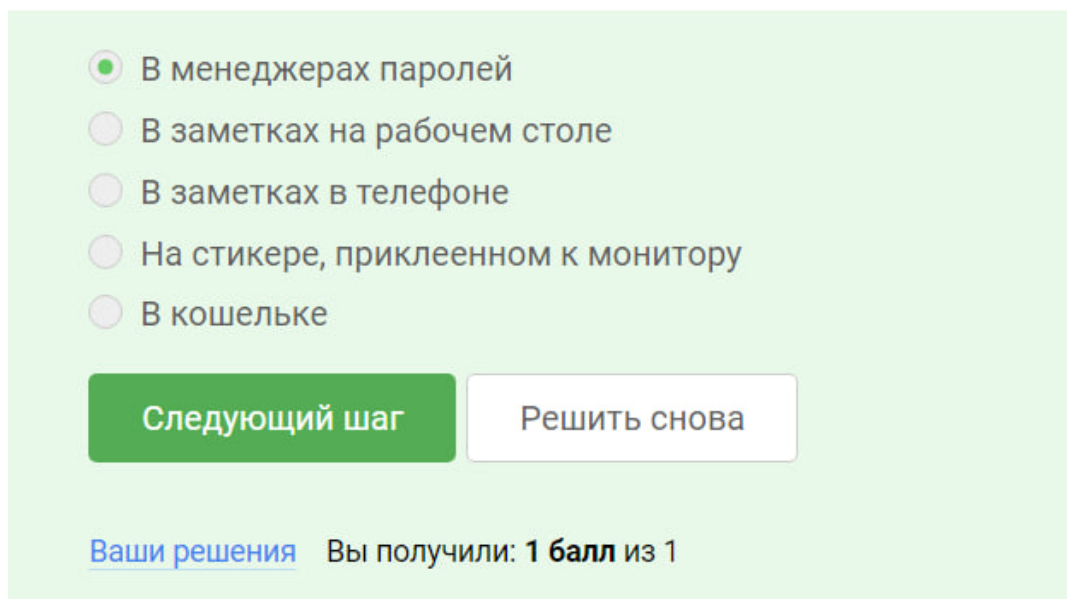
Следующий шаг **Решить снова**

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

Рис. 10.3: Стойкий пароль

3.2.2. Где безопасно хранить пароли?:

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



A screenshot of a quiz interface with a light green background. It contains a list of five radio button options. The first option, 'В менеджерах паролей', is selected. Below the list are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a blue link 'Ваши решения' followed by the text 'Вы получили: 1 балл из 1'.

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

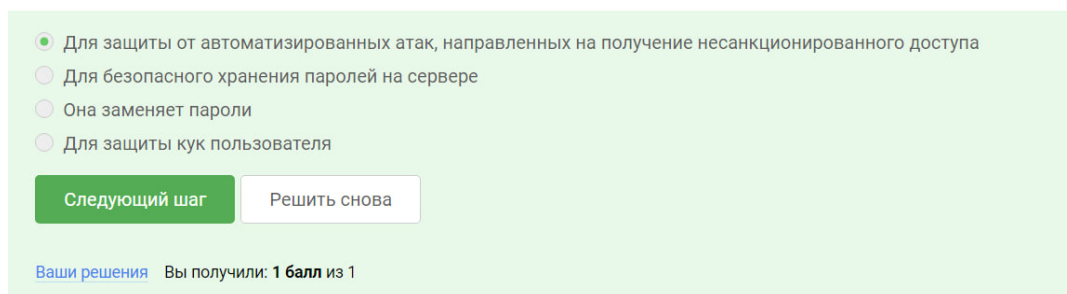
Следующий шаг Решить снова

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

Рис. 10.4: Менеджер паролей

3.2.3. 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.



A screenshot of a quiz interface with a light green background. It contains a list of five radio button options. The first option, 'Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа', is selected. Below the list are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a blue link 'Ваши решения' followed by the text 'Вы получили: 1 балл из 1'.

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

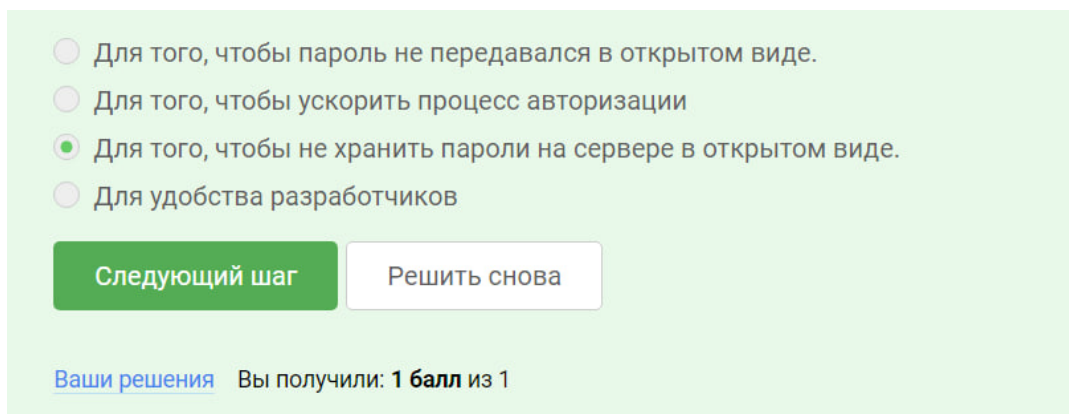
Следующий шаг Решить снова

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

Рис. 10.5: Необходимость капчи

3.2.4. 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.



The image shows a quiz interface with a light green background. It contains four radio button options for the question 'Для чего применяется хэширование паролей?'. The third option, 'Для того, чтобы не хранить пароли на сервере в открытом виде.', is selected. Below the options are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

- ☐ 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. 10.6: Хэширование паролей

3.2.5. 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.

☐ Да

☒ Нет

[Следующий шаг](#) [Решить снова](#)

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

Рис. 10.7: Соль для улучшения стойкости

3.2.6. 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.

☒ разные пароли на всех сайтах

☒ периодическая смена паролей

☒ сложные(=длинные) пароли

☒ капча

[Следующий шаг](#) [Решить снова](#)

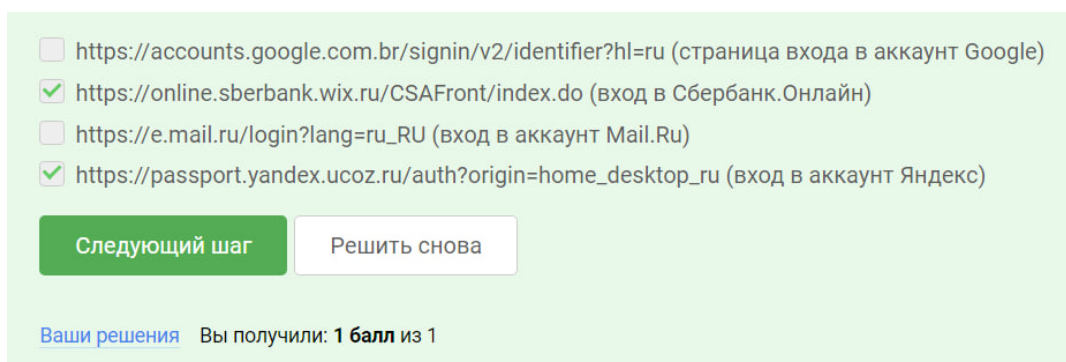
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 10.8: Меры защищают от утечек данных

11 3.3. Фишинг:

3.3.1. 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 (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 и yandex.ru соответственно.



The screenshot shows a quiz interface with a light green background. It contains a list of four URLs, each preceded by a checkbox. The first and third URLs have unchecked checkboxes, while the second and fourth have checked checkboxes. Below the list are two buttons: a green one labeled 'Следующий шаг' and a white one labeled 'Решить снова'. At the bottom, there is a line of text: 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

- ☐ <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. 11.1: Фишинговые ссылки

3.3.2. 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.

☒ Да
☐ Нет

[Следующий шаг](#) [Решить снова](#)

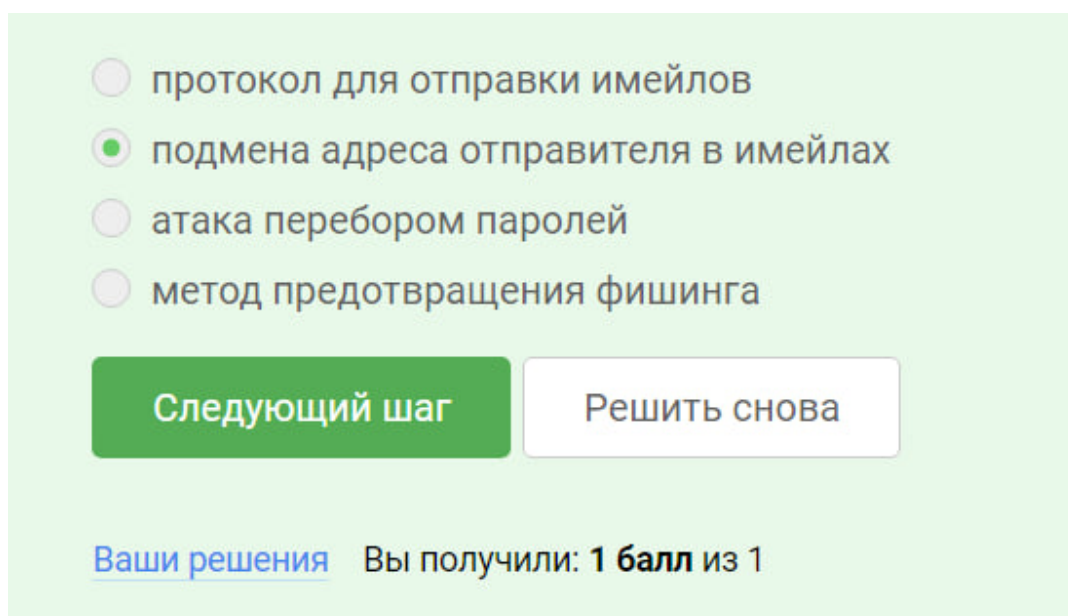
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 11.2: Фишинговый имейл

12 3.4. Вирусы. Примеры:

3.4.1. Email Спуфинг – это:

Подмена адреса отправителя в имейлах.



The image shows a quiz interface with a light green background. It contains four radio button options, two buttons at the bottom, and a score summary at the very bottom.

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

Below the options are two buttons: a green button labeled "Следующий шаг" and a white button with a grey border labeled "Решить снова".

At the bottom, there is a link "Ваши решения" and a score display: "Вы получили: 1 балл из 1".

Рис. 12.1: Email Спуфинг

3.4.2. 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.

☐ обязательно шифрует данные и требует ключ дешифрования

☒ маскируется под легитимную программу

☐ работает исключительно под ОС Windows

☐ разработан греками

[Следующий шаг](#) [Решить снова](#)

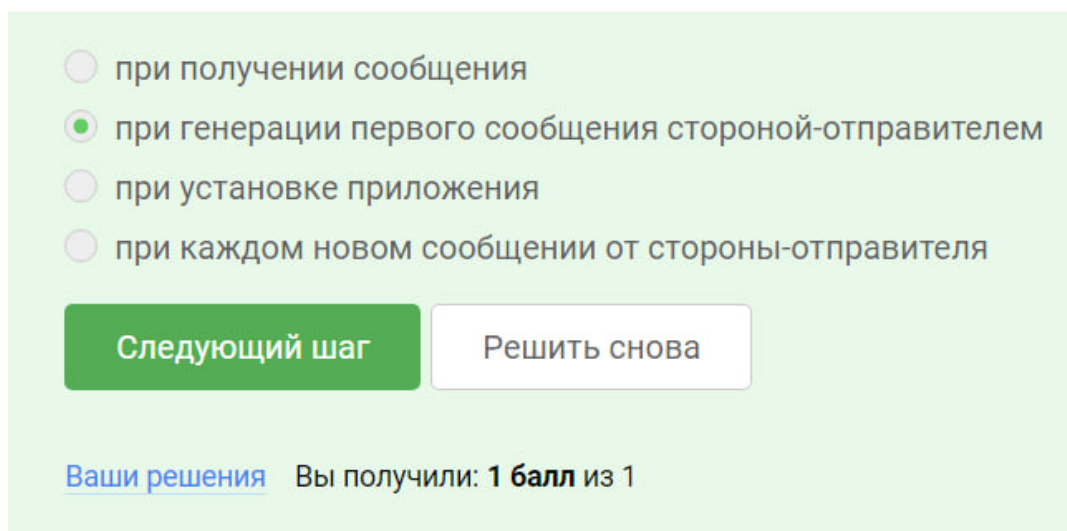
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 12.2: Вирус-троян

13 3.5. Безопасность мессенджеров:

3.5.1. 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.



The screenshot shows a quiz interface with a light green background. It contains four radio button options for a question. The second option is selected. Below the options are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a score display: 'Ваши решения' (Your solutions) in blue, followed by 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

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

Следующий шаг Решить снова

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

Рис. 13.1: Этап формирования ключа шифрования в протоколе мессенджеров Signal

3.5.2. 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.

☒ 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. 13.2: Суть сквозного шифрования

14 Криптография на практике.

#4.1. Введение в криптографию

Довольно часто люди, даже те, которые работают в IT-секторе, путают основные криптографические понятия. Они иногда не отличают цифровую подпись от шифрования, от аутентификации, от хэш-функции. Цель нашей работы – это научиться отличать основные криптографические протоколы, а именно – симметричное шифрование, аутентификацию, цифровую подпись и хэширование.

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 14.1: Название рисунка

Для того, чтобы ответить на вопрос мы должны знать, что первый раздел – это симметричная криптография, второй раздел – это асимметричная криптография. Определяющее свойство симметричной криптографии состоит в том, что она включает себя протоколы, где две или более стороны имеют общие секретные ключи, поэтому она и называется симметричной. К таким протоколам относятся симметричное шифрование и некоторые протоколы аутентификации. Часто

симметричный протокол довольно сложно построить, сложно установить потенциальный канал связи, исключительно основываясь на симметричных протоколах, поскольку нам нужно сгенерировать общий секретный ключ, то есть либо как-то физически встретиться с другим человеком и с другим устройством, либо что-то такое сделать, чтобы мы сгенерировали общий секрет. И элегантным решением этого вопроса являются протоколы асимметричной криптографии.

4.1.2. Криптографическая хэш-функция

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

Рис. 14.2: Криптографическая хэш-функция

Примитив, 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 .

4.1.3. К алгоритмам цифровой подписи относятся AES SHA2 RSA ECDSA ГОСТ Р 34.10-2012

A screenshot of a quiz interface with a light green background. It contains a list of five options for digital signature algorithms: AES, SHA2, RSA, ECDSA, and ГОСТ Р 34.10-2012. The first two are unchecked, while the last three are checked with green checkmarks. Below the list are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 14.3: К алгоритмам цифровой подписи относятся

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.

4.1.4. Код аутентификации сообщения относится к симметричным примитивам асимметричным примитивам

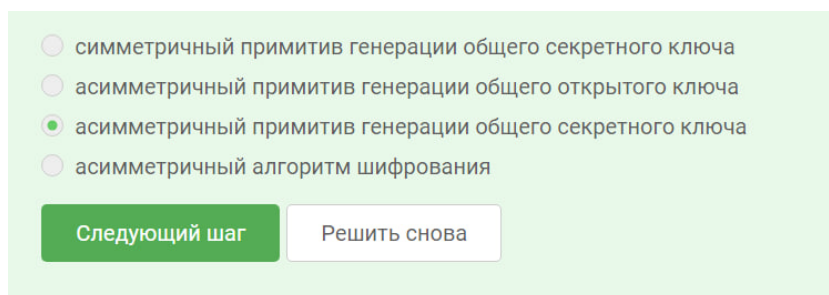
A screenshot of a quiz interface with a light green background. It contains two radio button options: 'асимметричным примитивам' (asymmetric primitive) and 'симметричным примитивам' (symmetric primitive). The second option is selected, indicated by a green dot. Below the options are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 14.4: Код аутентификации сообщения относится к

Где используется цифровая подпись? Во-первых, она используется в обеспечении целостности. В симметричном шифрование с аутентификацией обеспечивалась целостность за счет того, что у нас был общий секретный ключ, и мы запускали примитив, который называется код аутентификации сообщений – это примитив симметричной криптографии. Примитив асимметричной криптографии, который обеспечивает целостность документа – это цифровая подпись. Кроме того, сообщение может быть аутентифицировано: аутентификация

говорит о том, что именно тот человек, у которого есть ключ pk_A , подписал конкретно этот документ.

4.1.5. Обмен ключам Диффи-Хэллмана – это симметричный примитив генерации общего секретного ключа асимметричный примитив генерации общего открытого ключа асимметричный примитив генерации общего секретного ключа асимметричный алгоритм шифрования



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

Следующий шагРешить снова

Рис. 14.5: Обмен ключам Диффи-Хэллмана – это

15 4.2. Цифровая подпись

Цифровая подпись предназначена, во-первых, для обеспечения целостности сообщения, если сообщение в процессе передачи было изменено, то подпись этого измененного сообщения будет проверена некорректно, то есть при проверке корректности подписи мы узнаем о том, что сообщение было изменено. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения и можно установить принадлежность подписи владельцу, никто другой не смог бы поставить такую подпись под этим сообщением. В третьих – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал.

4.2.1 Протокол электронной цифровой подписи относится к протоколам с симметричным ключом протоколам с публичным (или открытым) ключом Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом. В протоколах с публичным ключом используется пара ключей: открытый ключ, который может быть распространен публично, и закрытый ключ, который известен только владельцу. Эти протоколы обеспечивают безопасную передачу информации, аутентификацию и целостность данных.

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

Следующий шаг Решить снова

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

Рис. 15.1: Протокол электронной цифровой подписи относится к

4.2.2. Алгоритм верификации электронной цифровой подписи требует на вход подпись, секретный ключ подписи, открытый ключ, сообщение подпись, секретный ключ, сообщение подпись, открытый ключ

То есть каждая машина запускает процедуру Verify, которая берет на вход само обновление, подпись и открытый ключ разработчика, и в случае если верификация прошла успешно, мы можем установить это обновление.

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

Следующий шаг Решить снова

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

Рис. 15.2: Алгоритм верификации электронной цифровой подписи требует на вход

4.2.3. Электронная цифровая подпись не обеспечивает аутентификацию неотказ от авторства целостность конфиденциальность

Электронная цифровая подпись обеспечивает аутентификацию, неотказ от авторства и целостность данных. Однако она не обеспечивает конфиденциаль-

ность, так как электронная цифровая подпись предназначена для проверки подлинности и целостности сообщения, а не для его защиты от прослушивания или чтения третьими лицами. Для обеспечения конфиденциальности данных обычно применяются другие методы шифрования.

The screenshot shows a quiz interface with a light green background. It contains four radio button options: 'целостность' (integrity), 'конфиденциальность' (confidentiality), 'неотказ от авторства' (non-repudiation), and 'аутентификацию' (authentication). The 'конфиденциальность' option is selected, indicated by a green dot. Below the options are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 15.3: Электронная цифровая подпись не обеспечивает

4.2.4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС? простая усиленная неквалифицированная усиленная квалифицированная Для отправки налоговой отчетности в ФНС требуется использовать усиленный квалифицированный сертификат электронной подписи. Усиленный квалифицированный сертификат обеспечивает высокий уровень безопасности и подтверждает личность владельца сертификата. Он является обязательным для взаимодействия с государственными органами, включая налоговую службу.

☐ простая

☒ усиленная квалифицированная

☐ усиленная неквалифицированная

[Следующий шаг](#) [Решить снова](#)

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

Рис. 15.4: Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

4.2.5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи? в любой организации, имеющей соответствующую лицензию ФСБ в минкомсвязи РФ в удостоверяющем (сертификационном) центре в любой организации по месту работы Квалифицированный сертификат ключа проверки электронной подписи можно получить в удостоверяющем (сертификационном) центре. Удостоверяющие центры предоставляют услуги по выдаче сертификатов ключей проверки электронной подписи, подтверждая личность владельца и обеспечивая безопасность электронных документов.

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

[Следующий шаг](#) [Решить снова](#)

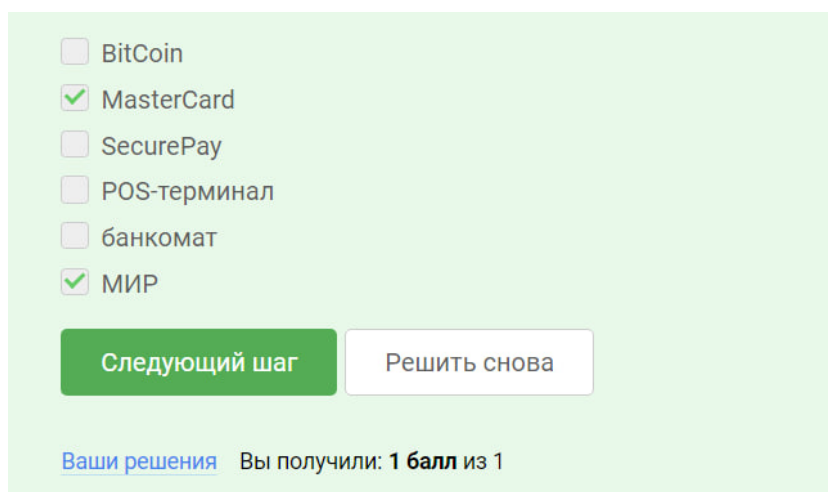
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 15.5: В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

#4.3. Электронные платежи Наверное, всем интересно, что происходит, когда мы оплачиваем наши покупки электронной картой. Происходит как минимум

две вещи: первая – и основная техническая часть, где работает криптография – это авторизация нашей покупки; вторая – транзакция. Транзакция – это мало интересный этап, по крайней мере для нас в этой лекции, мы сегодня будем рассматривать первый этап – авторизацию покупки. Там происходит как минимум три вещи. Первая – это аутентификация владельца карты; вторая – проверка банком-эмитентом. Это банк, который выдал вам вашу карточку, он хранит и владеет вашими деньгами на карточке, проверяет, достаточно ли средств на карте для того, чтобы осуществить эту покупку, не наложены ли какие-то ограничения на карту (есть карты, с помощью которых нельзя совершать покупки в онлайн-магазинах).

4.3.1. Выберите из списка все платежные системы. BitCoin MasterCard SecurePay POS-терминал банкомат МИР



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

Следующий шаг Решить снова

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

Рис. 15.6: Выберите из списка все платежные системы.

4.3.2. Примером многофакторной аутентификации является комбинация проверки пароля + Капча комбинация проверка пароля + код в sms сообщении комбинация код в sms сообщении + отпечаток пальца комбинация PIN код + пароль Примером многофакторной аутентификации является комбинация проверки пароля + код в SMS сообщении. В данном случае для подтверждения личности пользователя требуется знание пароля (что пользователь знает) и получение

уникального кода через SMS (что пользователь имеет). Этот подход обеспечивает более высокий уровень безопасности, чем простая проверка по паролю.

The screenshot shows a multi-factor authentication interface with a light green background. It contains four radio button options: 'комбинация проверки пароля + Капча' (unchecked), 'комбинация проверка пароля + код в sms сообщении' (checked), 'комбинация код в sms сообщении + отпечаток пальца' (checked), and 'комбинация PIN код + пароль' (unchecked). Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a link 'Ваши решения' and a score 'Вы получили: 1 балл из 1'.

Рис. 15.7: Примером многофакторной аутентификации является

4.3.3. При онлайн платежах сегодня используется 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 На сегодняшний день, при онлайн платежах часто используется многофакторная аутентификация покупателя перед банком-эмитентом. Это может включать в себя, например, ввод пароля, получение одноразового кода через SMS или приложение банка, использование биометрических данных и т.д. Этот подход обеспечивает более высокий уровень безопасности платежей.

Однако, однофакторная аутентификация покупателя перед банком-эквайером или при помощи PIN-кода карты перед терминалом также может использоваться в определенных случаях, но она менее безопасна по сравнению с многофакторной аутентификацией.

☒ 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. 15.8: При онлайн платежах сегодня используется

#4.4. Блокчейн

Под крипто мы понимаем криптографию как науку, и вы уже знаете довольно много примитивов и терминов из этой области. А вот криптовалюта - это разновидность цифровых денег, которые построены на основе технологии блокчейн. Почему она называется криптовалютой? Потому что для ее корректной работы используются криптографические примитивы. Что я понимаю под корректной работой? Мы все знаем, что деньги должно быть сложно скопировать, и для того, чтобы криптографическую валюту было сложно подделать или скопировать, используются криптографические примитивы. Вторая цель - это обеспечение того, чтобы в криптовалюте одни и те же деньги нельзя было потратить дважды.

4.4.1. Какое свойство криптографической хэш-функции используется в доказательстве работы? фиксированная длина выходных данных сложность нахождения прообраза обеспечение целостности эффективность вычисления

Свойство криптографической хэш-функции, которое используется в доказательстве работы (Proof of Work), это сложность нахождения прообраза. В случае Proof of Work, участники сети должны выполнять вычислительно сложные задачи для того, чтобы создать новый блок в блокчейне или подтвердить транзакцию. Эти задачи обычно основаны на поиске определенного значения хэш-функции, которое удовлетворяет определенным условиям (например, начинается с определенного количества нулей). Хэш-функции также обеспечивают целостность данных, так как любое изменение входных данных приводит к изменению выходного хэша. Фиксированная длина выходных

данных и эффективность вычисления также являются важными свойствами криптографических хэш-функций, но в контексте Proof of Work они не являются основными для доказательства работы.

A screenshot of a quiz interface with a light green background. It contains four radio button options: 'фиксированная длина выходных данных', 'сложность нахождения прообраза' (which is selected), 'обеспечение целостности', and 'эффективность вычисления'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

Рис. 15.9: Какое свойство криптографической хэш-функции используется в доказательстве работы?

4.4.2. Консенсус в некоторых системах блокчейн обладает свойствами Постоянства Открытость Живучесть Консенсус

Живучесть относится к способности блокчейн-сети продолжать работать, даже если некоторые из ее узлов выйдут из строя или будут скомпрометированы. Это достигается за счет распределенного характера блокчейна, где данные хранятся и проверяются на множестве узлов, что делает сеть устойчивой к сбоям.

A screenshot of a quiz interface with a light green background. It contains four checked checkbox options: 'открытость', 'постоянства', 'консенсус', and 'живучесть'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

Рис. 15.10: Консенсус в некоторых системах блокчейн обладает свойствами

4.4.3. Секретные ключи какого криптографического примитива хранят участники блокчейна? обмен ключами шифрование цифровая подпись хэш-функция

☐ обмен ключами

☐ шифрование

☒ цифровая подпись

☐ хэш-функция

Следующий шаг

Решить снова

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

Рис. 15.11: Секретные ключи какого криптографического примитива хранят участники блокчейна?

Многократная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать: 1) то, что я знаю – это либо пароль, либо PIN-код, либо в случае онлайн-платежей это секретный код, 2) конкретно в онлайн-платежах мы еще используем второй фактор – это то, чем я владею, например, телефон, именно поэтому нам часто приходит код, который вы должны подтвердить или вбить в ваш браузер, 3) другой фактор аутентификации – это свойства, например, биометрия, отпечаток пальца, сетчатки глаза, 4) четвертый фактор аутентификации – локация. Способ аутентификации, как правило, выбирается банком.

Важно помнить что, существует платежная система без двойной аутентификации, раньше они были популярны, сейчас, скорее всего, они уже менее популярны, это карточки Visa Electron, MasterCard Maestro, с помощью этих карт нельзя осуществлять онлайн-платежи, в потому что эти карты не поддерживают двойную аутентификацию, но как минимум двойная аутентификация должна быть поддержана, если мы хотим оплачивать покупки онлайн.

16 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