# Прохождение внешнего курса 2 часть

**Защита ПК/телефона**

Кроитору Екатерина НБИ-бд-03-22

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Научиться Шифровать диск. Выбрать правильный пароль. Понять, что такое фишинг и вирусы и как обезопасить свои менеджеры.

# 2 Задание

Выполнить тестовую часть курса

# 3 Теоретическое введение

Поговорим немного о деталях, о том, как происходит шифрование. Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES. Это американский стандарт симметричного шифрования, он также используется для конфиденциальной передачи данных по сети. Это эффективный алгоритм, который реализован в процессорах быстро, то есть на аппаратном уровне. Благодаря тому, что это хороший алгоритм, пользователь практически не наблюдает задержек в работе, то есть данные шифруются-дешифруются быстро. Как правило, это происходит на заднем фоне, мы можем при этом работать на компьютере, будут происходить какие-то параллельные операции на шифрование и дешифрование. Мы используем пароли для • аутентификации в сети (логинимся в соц. сети, почту, Skype) • получения доступа к банковским картам (PIN код) • разблокировки телефона • доступа к компьютеру • физического доступа в здания (биометрические пароли) • доступа к электронному кошельку (парольные фразы в bitcoin) Фишинг — заполучение информации у пользователя, маскируясь под реальный сервис/продукт • поддельные интернет- страницы • телефонные звонки (от якобы банков) Mydoom почтовый червь для Microsoft Windows и Windows NT, 2004 год Червь — вредоносное ПО, распространяющееся по сети Инетнет Распространялся по почте как письмо с пометкой “Mail Delivery System” Письмо содержало вложение, открытие которого запускало червя. Червь выискивал имейл адреса во всех локальных файлах и отправлял им письмо Ущерб оценивается в $38 биллионов

Sobig почтовый червь и троян под Microsoft Windows 2003 год Троян — вирус, проникающий в систему под видом легитимного ПО Распространялся по почте как письмо с темой “Re: Details” (или подобными) Само письмо содержало текст “See the attached file for details” Вложение устанавливало утилиту WinGate proxy server для рассылки зараженных имейлов Ущерб оценивается в $30 биллионов WannaCry червь и программа-вымогатель денежных средств под Windows 2017 год Программа-вымогатель (ransomware) — вредоносное ПО, блокирующее доступ к данным (часто с помощью шифрования), и вымогающее деньги в обмен на ключ дешифрвания Эксплуатирует уязвимость реализации протокола SMB в Windows (сетевой протокол для удаленного доступа к файлам, принтерам) Ущерб оценивается в $4 биллиона Вирус самостоятельно устанавливается, генерирует ключи шифрования и шифрует некоторые файлы системы Flashback троян под MacOS 2011 год Фейковый установщик Adobe Flash Player Загружался через поддельный веб-сайт Pegasus шпионское ПО под iOS и Android 2021 год Вирус-шпион (spyware) — ПО, нацеленное на сбор приватной информации Разработка израильской компании NSO Group Вирус-троян заражет устройства через заражает через SMS, WhatsApp, iMessage Умеет читать SMS, имейлы, контакты прослушивать звонки, делать скриншоты, записывать нажатия клавиш Для начала давайте обсудим, какие требования мы выдвигаем к безопасности мессенджеров. Во-первых, мы хотим, чтобы наши сообщения доходили корректно, то есть, если мы написали «Я буду через пять минут», мы хотим, чтобы отправитель получил именно это сообщение «Я буду через пять минут», а не «через 15, 20» или «Я не буду через 5 минут». Конечно же, мы хотим, чтобы сообщения были конфиденциальны, то есть само сообщение знал только отправитель и получатель. В идеале мы хотим аутентификацию, то есть, если нам пришло сообщение от какого-то человека, мы знаем, что оно пришло от него, если мы посылаем какому-то человеку сообщение, мы знаем, что оно придет конкретно к нему, и ни к кому другу. Поскольку мы говорим с вами о сообщениях, коммуникация должна быть стойка к потере сообщений. Мы все знаем, что иногда человек бывает не в сети, иногда бывают

проблемы со связью, однако, когда человек заходит в сеть, то все сообщения, которые он не получил за это время, ему должны прийти. И два последних довольно специфичных требования к безопасности, которые мы на сегодня выдвигаем не только к мессенджерам, но и вообще к любой конфиденциальной коммуникации. Первое - это прямая секретность; прямая секретность (от английского forward secrecy) гарантирует безопасность сообщений в прошлом: имеется в виду до компрометации ключа.

# 4 Выполнение лабораторной работы

. Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES (рис. 4.1).

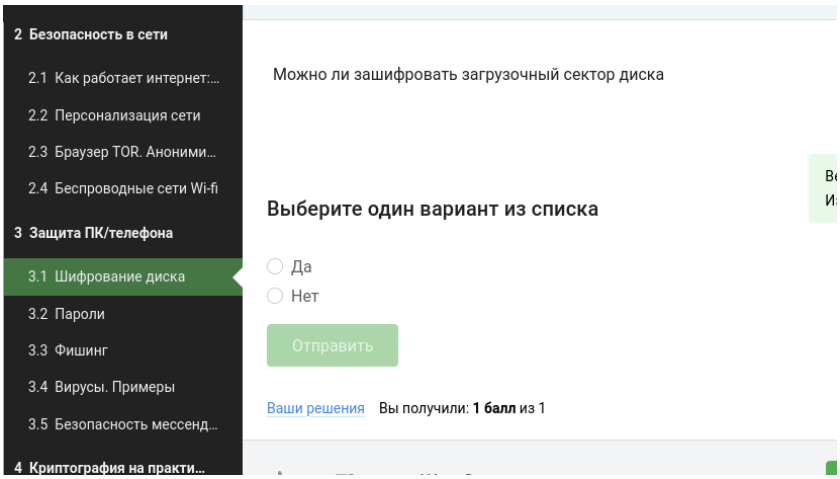



Рис. 4.1: Тест 1

Алгоритм AES это американский стандарт симметричного шифрования, он также используется для конфиденциальной передачи данных по сети. (рис. 4.2).

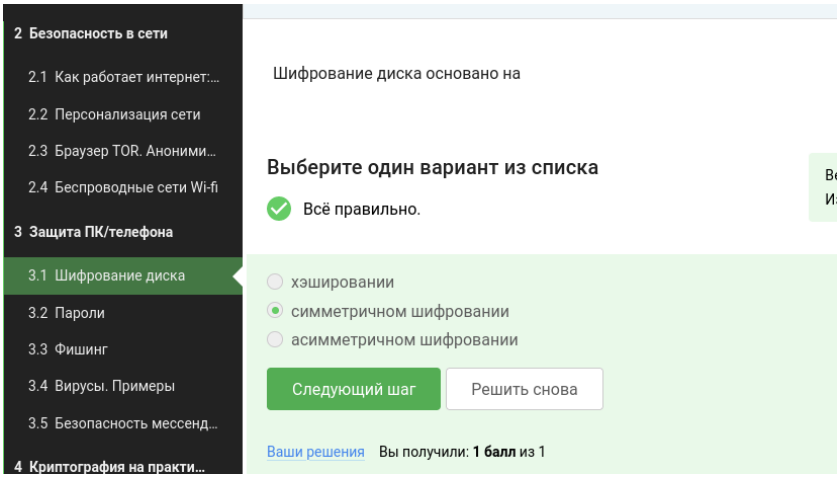



Рис. 4.2: Тест 2

Во всех популярных операционных системах есть встроенные утилиты, которые позволяют шифровать жесткий диск: для Windows это Bitlocker, в Linux – LUKS, в MacOS – это FileVault. Кроме того, есть и сторонние опенсорсные (open source) программы, то есть бесплатные: это Veracrypt, PGPDisk (рис. 4.3).

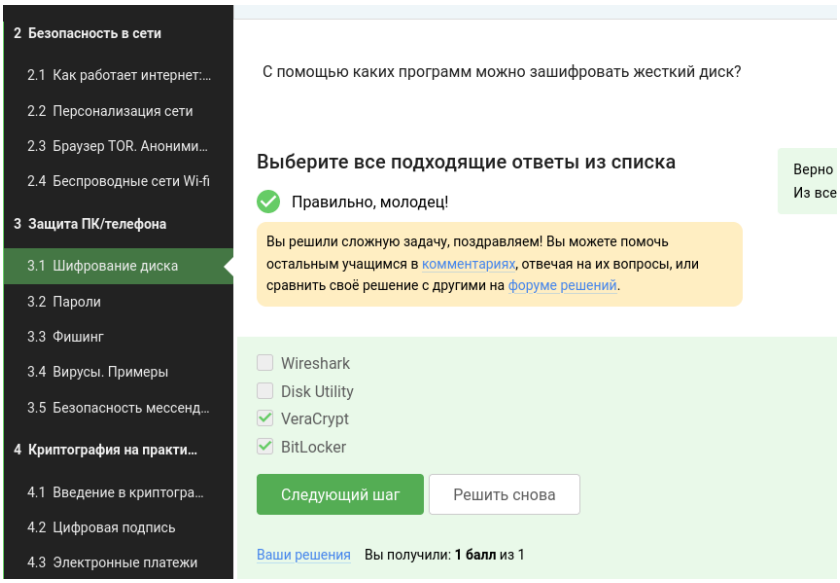



Рис. 4.3: Тест 3

Основной критерий стойкости пароля — это сложность его перебора Пример паролей длины 8, состоящих из цифр, алфавита и спец. символов ![_?]$&+*()

(26+10+13)8 =33 232 930 569 601 перебор практически невыполним (рис. 4.4).

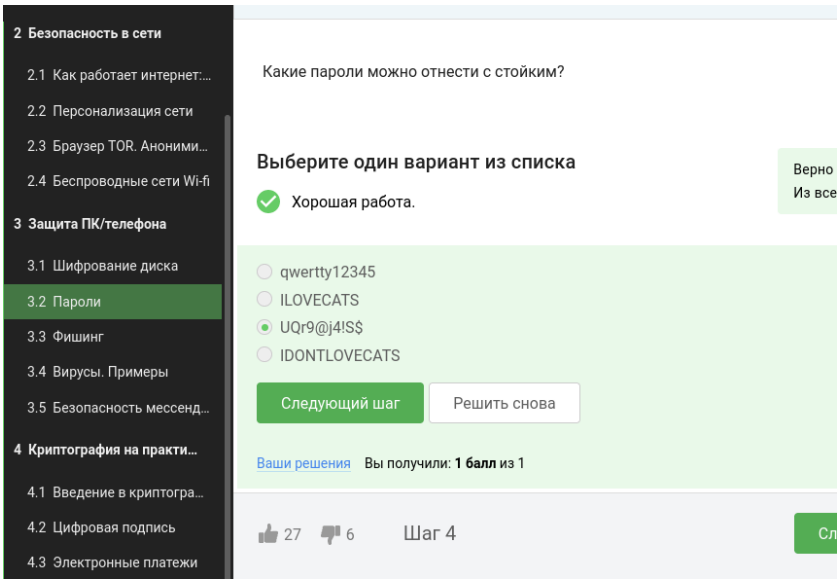



Рис. 4.4: Тест 4

Рекомендации • используйте длинные пароли с символами алфавита разного регистра, цифрами, спец. символами • используйте менеджеры паролей для хранения • регулярно меняйте пароли к критическим сервисам (почте) • используйте разные пароли для разных сайтов, программ (рис. 4.5).

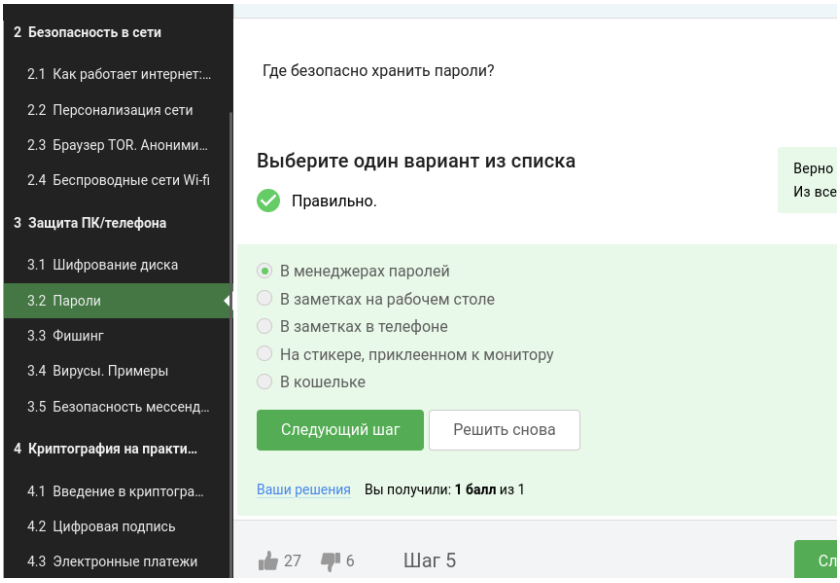



Рис. 4.5: Тест 5

Капча — тест для определения, является ли пользователь человеком или компьютером Цель — противостоять автоматизированному перебору / доступу к ресурсу (рис. 4.6).

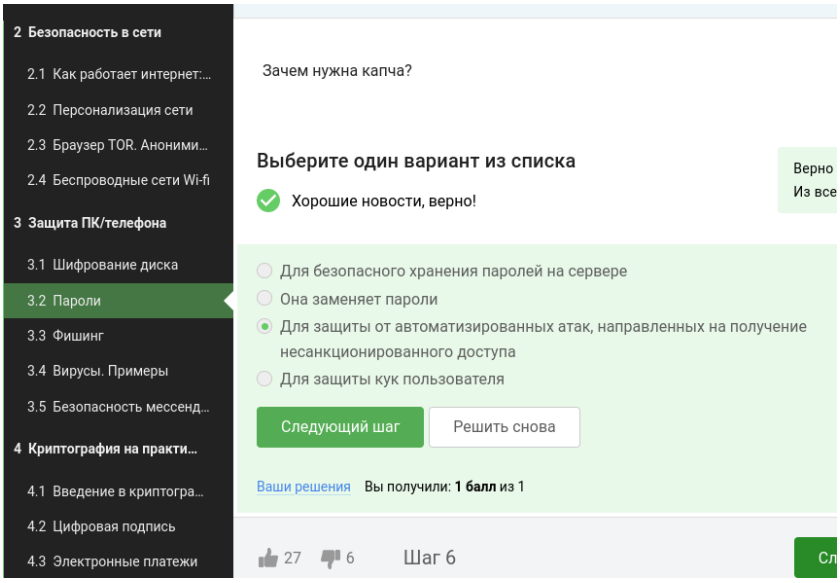



Рис. 4.6: Тест 6

Криптографическая хэш-функция получает на вход произвольные данные и

выдает фиксированное число бит Идея: имея выход хэш-функции (образ) сложно найти вход (прообраз) Примеры: SHA2, SHA3, ГОСТ 34.11-2018 (рис. 4.7).

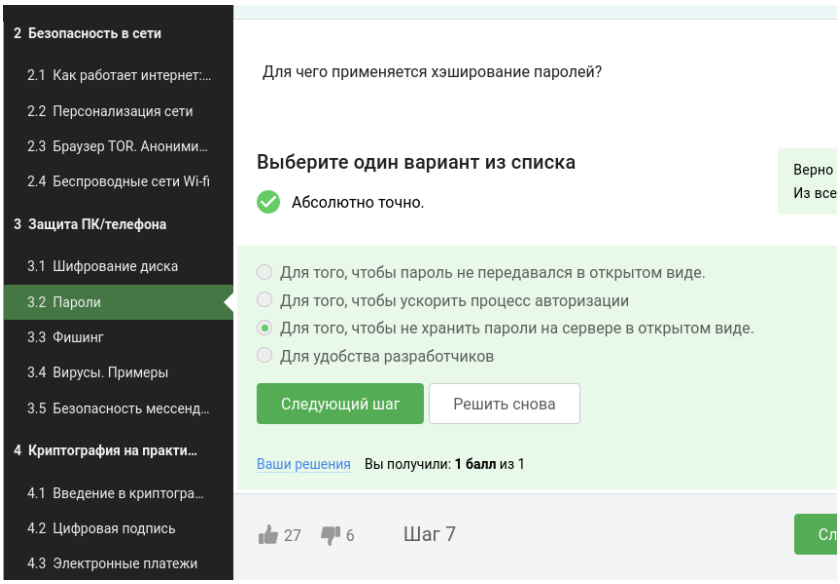



Рис. 4.7: Тест 7

Если злоумышленник получил доступ к серверу соль не поможет (рис. 4.8).

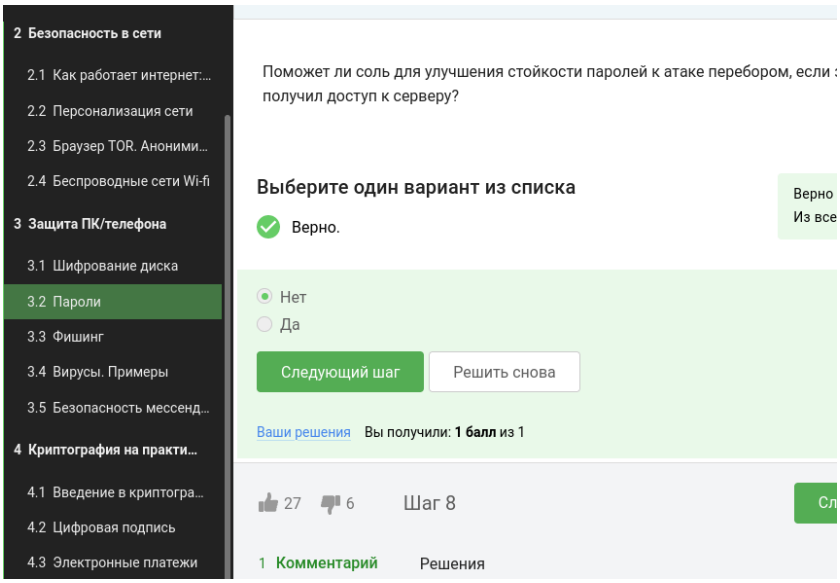



Рис. 4.8: Тест 8

Рекомендации • используйте длинные пароли с символами алфавита разного

регистра, цифрами, спец. символами • используйте менеджеры паролей для хранения • регулярно меняйте пароли к критическим сервисам (почте) • используйте разные пароли для разных сайтов, программ (рис. 4.9).

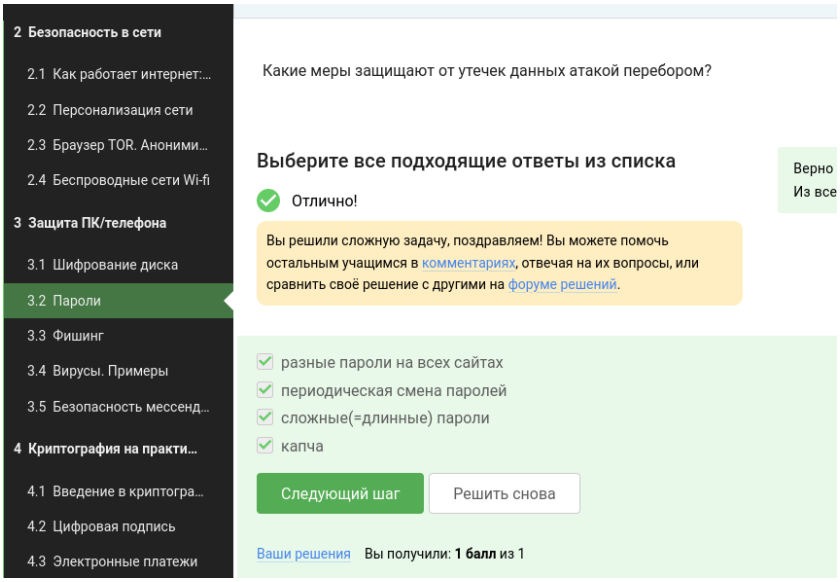
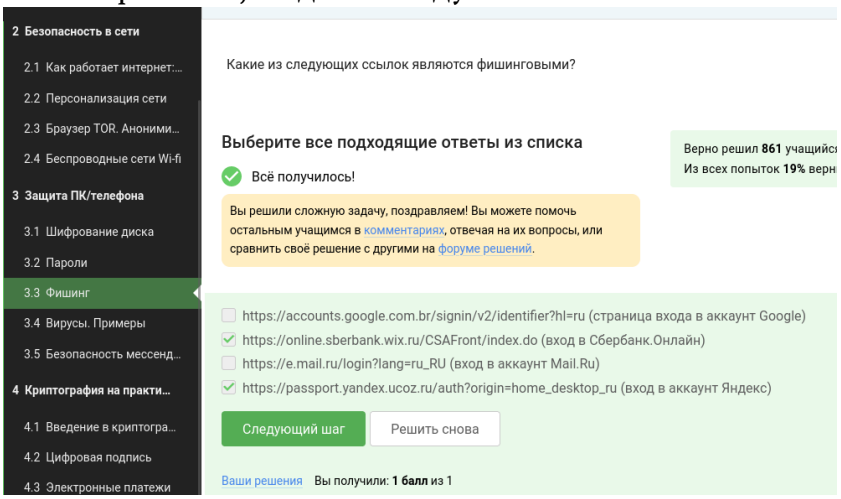



Рис. 4.9: Тест 9

(рис. **??**).

Название может и быть похожа на оригинал, но дальше идут не понятные сим-




волы, которых не должно быть

Чаще всего этим методом и пользуются мошенники (рис. 4.10).

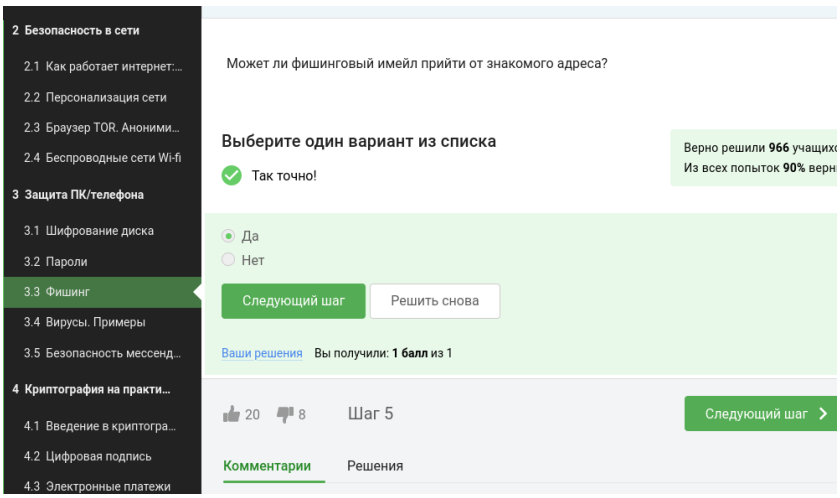



Рис. 4.10: Тест 11

Email спуфинг от англ. spoofing — подмена Суть: отправка писем с поддельным адресом отправителя. Почему работает: протокол для отправки писем SMTP не включает проверку адреса (рис. 4.11).

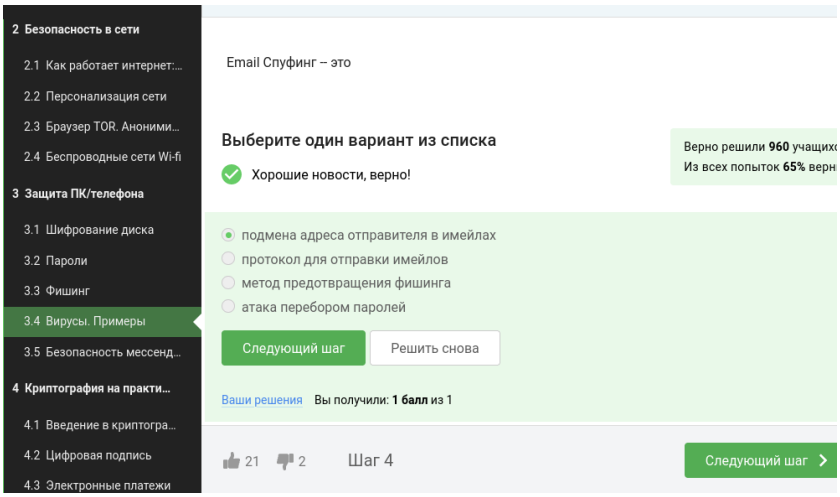



Рис. 4.11: Тест 12

Троян - это вирус, который проникает в систему под видом какого-то легитимного программного обеспечения, это аллюзия к троянскому коню. Этот вирус также распространялся по почте с вполне себе невинным письмом. Само вложение

устанавливало вполне себе легитимную утилиту от Windows, которая называлась WinGate proxy. (рис. 4.12).

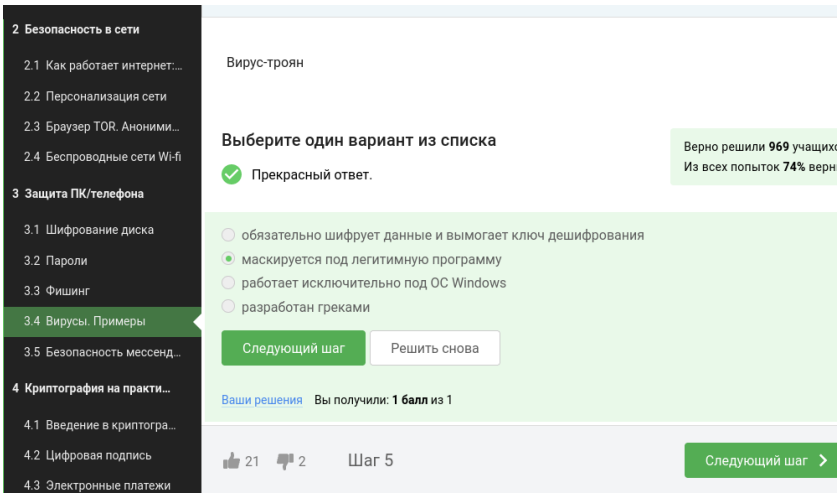



Рис. 4.12: Тест 13

сквозное шифрование - по-английски E2E или End-to-End encryption. Суть довольно простая: у нас есть два участника - Алиса и Боб, A и B, и сквозное шифрование заключается в том, что сервер, который передает сообщение, который направляет сообщение от Алисы к Бобу или от Бобу к Алисе, знает только то, куда эти сообщения должны быть направлены, но сообщения он передает в зашифрованном виде, то есть он как бы работает маршрутизатором сообщений, не зная о том, что он передает. Что происходит, если мы хотим отправить сообщение от Алисы к Бобу? Алиса шифрует свои данные, кладет на сервере шифр-текст с пометкой, что этот шифр-текст предназначен для Боба. Когда Боб заходит в сеть, сервер видит: «Ага, Боб зашел в сеть, надо обновить его сообщение», и отправляет шифр-текст от Алисы. Боб получает этот шифр-текст, дешифрует его, получает сообщение в открытом виде. При этом сервер не знает ни ключ, с помощью которого Алиса шифровала, ни тем более сообщение в открытом виде. (рис. 4.13).

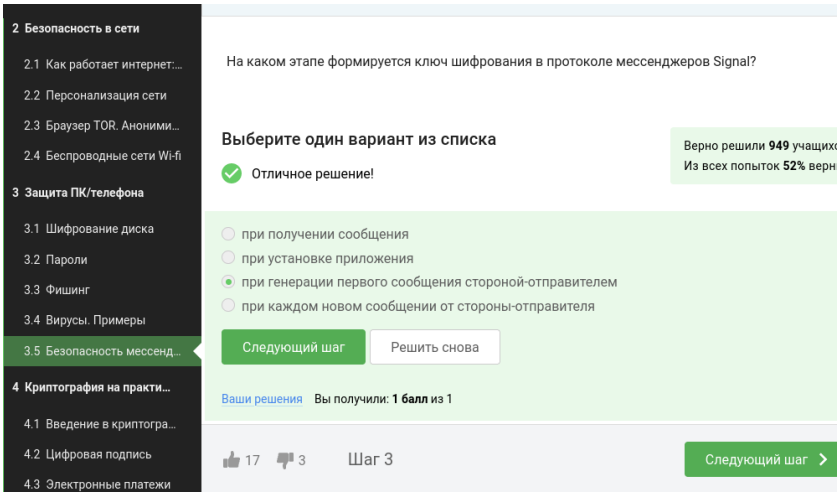



Рис. 4.13: Тест 14

(рис. 4.14).

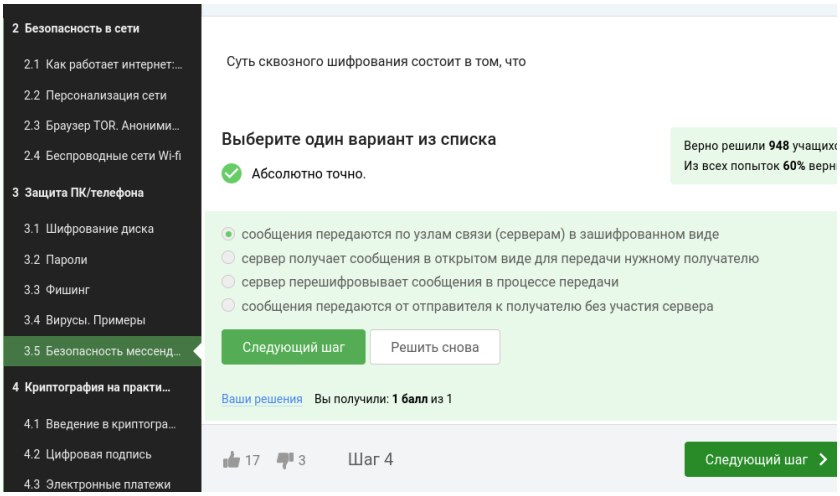



Рис. 4.14: Тест 15

# 5 Выводы

Мы научились Шифровать диск. Выбирать правильный пароль. Поняли, что такое фишинг и вирусы и как обезопасить свои менеджеры.