Отчёт по выполнению внешних курсов

Основы кибербезопасности

Боровиков Даниил Александрович НПИбд-01-22

Содержание

List of Figures

1 Цель работы

Пройти спец. курс “Основы кибербезопасности” и получить сертификат.

2 Выполнение лабораторной работы

2.1 Раздел 3: “Защита ПК/телефона”

2.1.1 (3.1) “Шифрование диска”

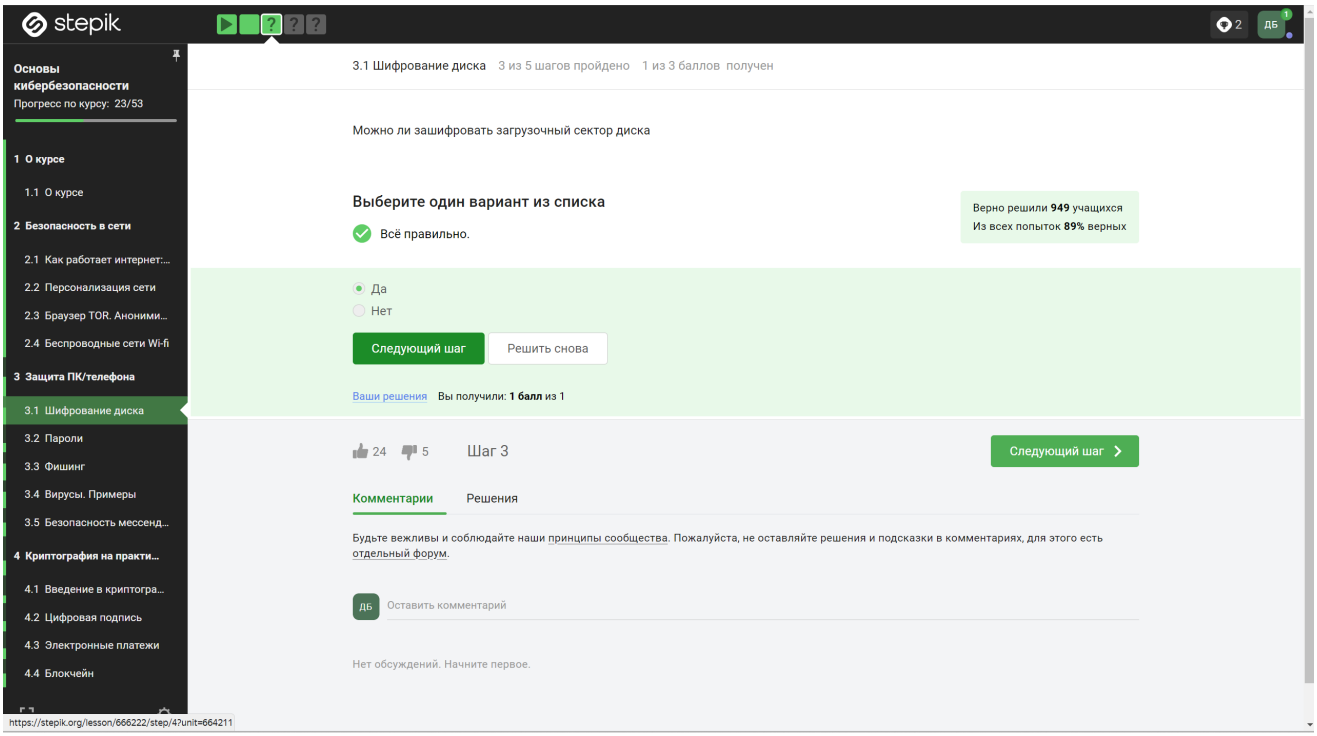

Figure 2.1: Рис. 3.1 Раздел (3.1) – Вопрос 1

Вопрос: Можно ли зашифровать загрузочный сектор диска

Ответ: Да, можно зашифровать загрузочный сектор диска

Пояснение: Зашифрованный загрузочный сектор обеспечивает дополнительный

уровень безопасности, защищая данные даже на этапе загрузки операционной системы.

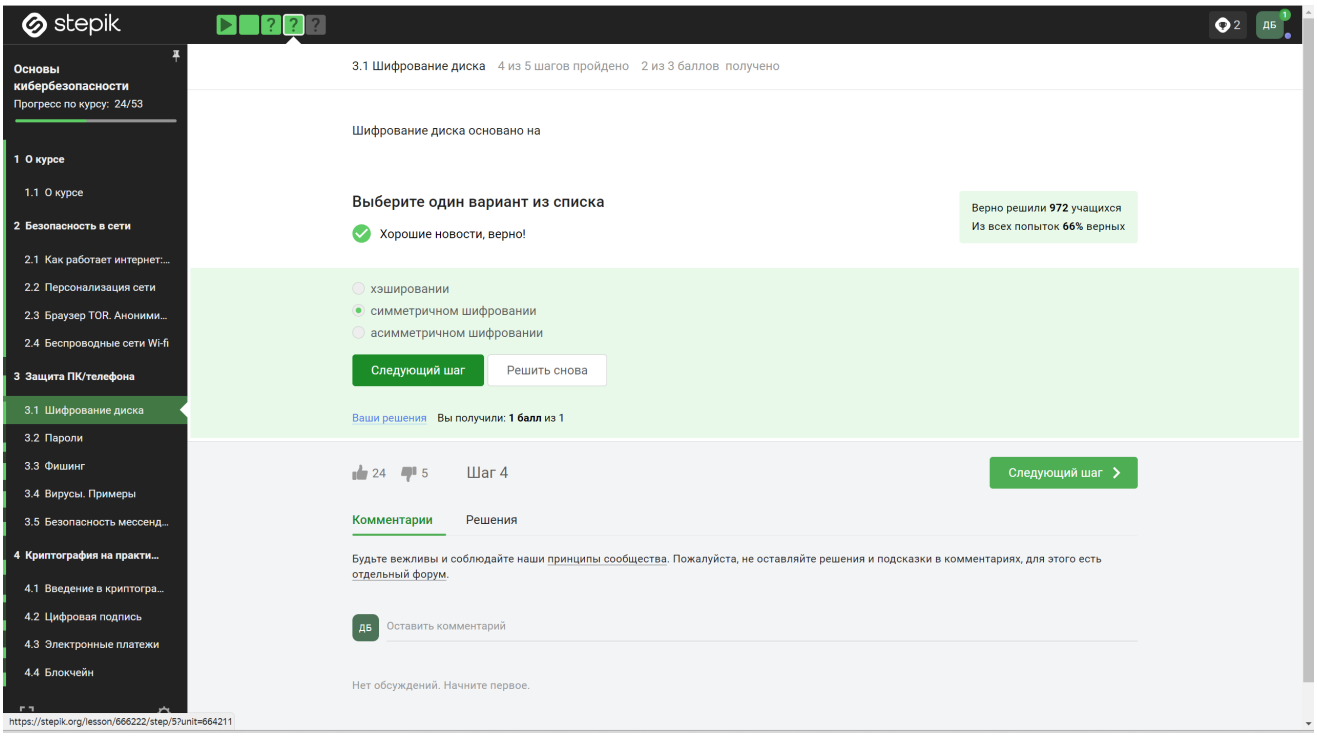

Figure 2.2: Рис. 3.2 Раздел (3.1) – Вопрос 2

Вопрос: Шифрование диска основано на

Ответ: Шифрование диска основано на симметричном шифровании

Пояснение: Симметричное шифрование использует один ключ для шифрования и расшифрования данных, что обеспечивает эффективную защиту информации на диске.

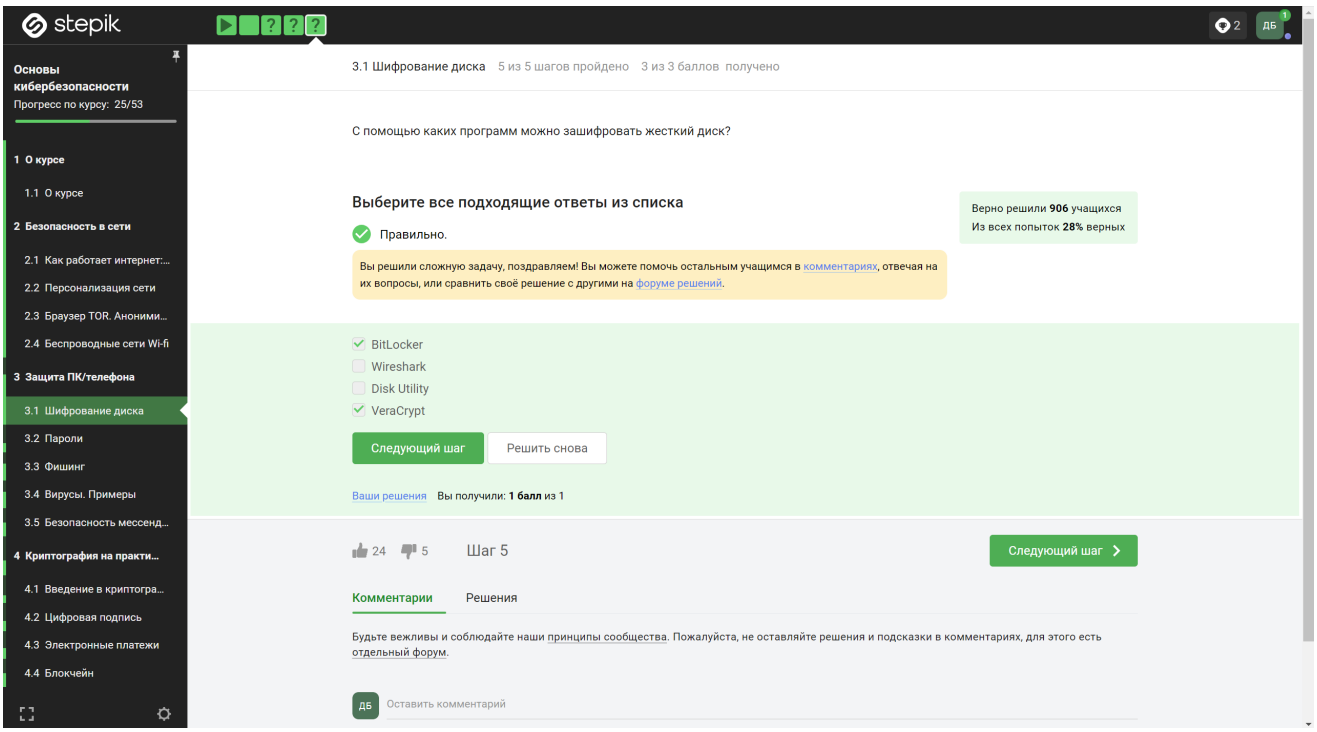

Figure 2.3: Рис. 3.3 Раздел (3.1) – Вопрос 3

Вопрос: С помощью каких программ можно зашифровать жесткий диск?
Ответ: С помощью BitLocker и VeraCrypt можно зашифровать жесткий диск
Пояснение: BitLocker (для Windows) и VeraCrypt (кроссплатформенное решение) позволяют зашифровать жесткий диск, обеспечивая защиту данных от несанкционированного доступа.

2.1.2 (3.2) “Пароли”

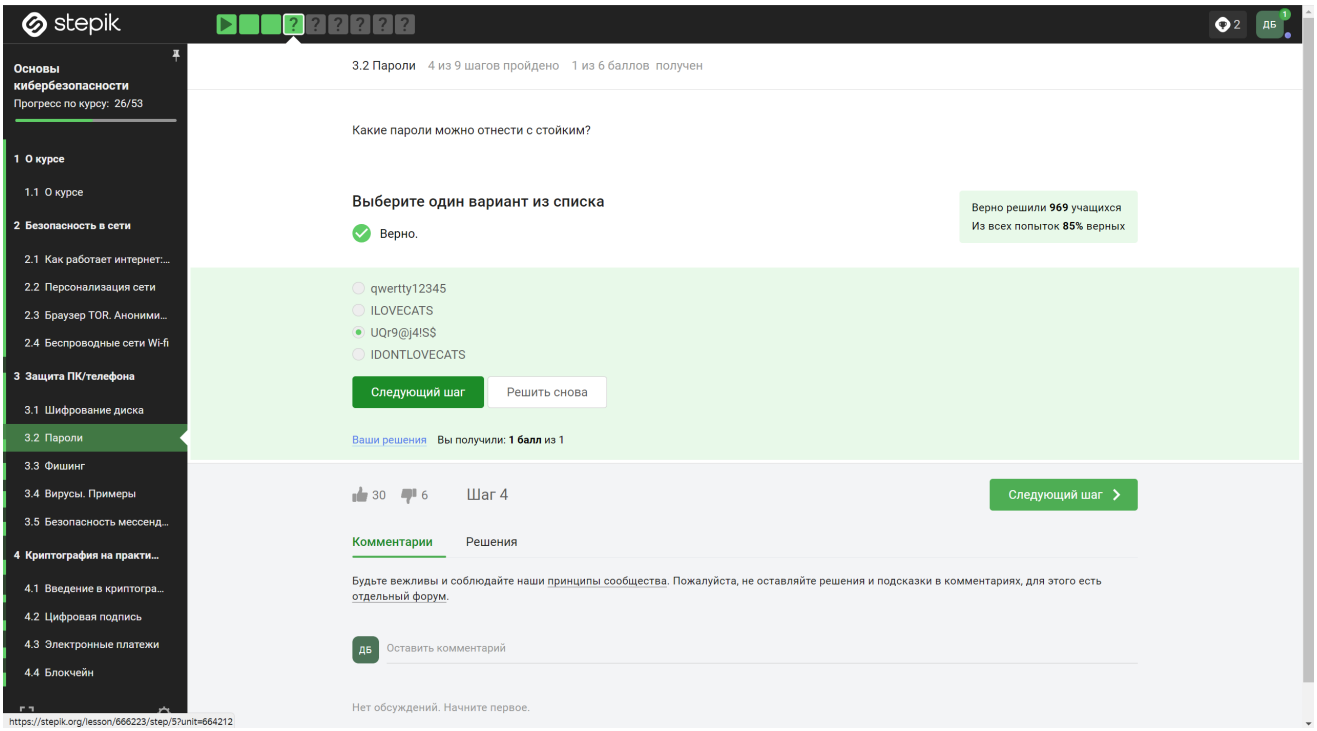

Figure 2.4: Рис. 3.4 Раздел (3.2) – Вопрос 1

Вопрос: Какие пароли можно отнести к стойким?

Ответ: UQr9@j4!S$, потому что тут используется сложный набор символов

Пояснение: Сложные пароли, содержащие комбинации символов разного регистра, цифр и специальных символов, обычно являются стойкими к взлому.

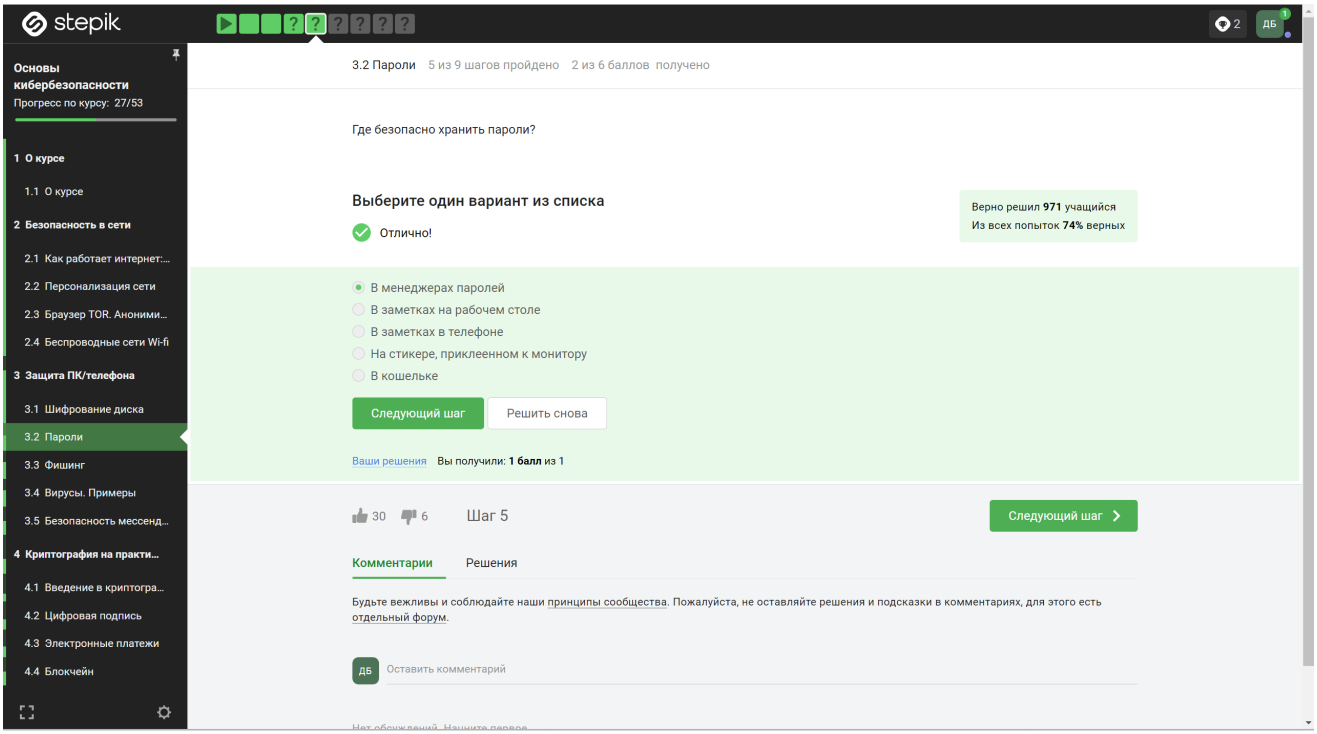

Figure 2.5: Рис. 3.5 Раздел (3.2) – Вопрос 2

Вопрос: Где безопасно хранить пароли?

Ответ: Безопасно хранить пароли в менеджерах паролей

Пояснение: Менеджеры паролей обеспечивают шифрование и безопасное хранение паролей, уменьшая риск утечки или взлома учетных данных.

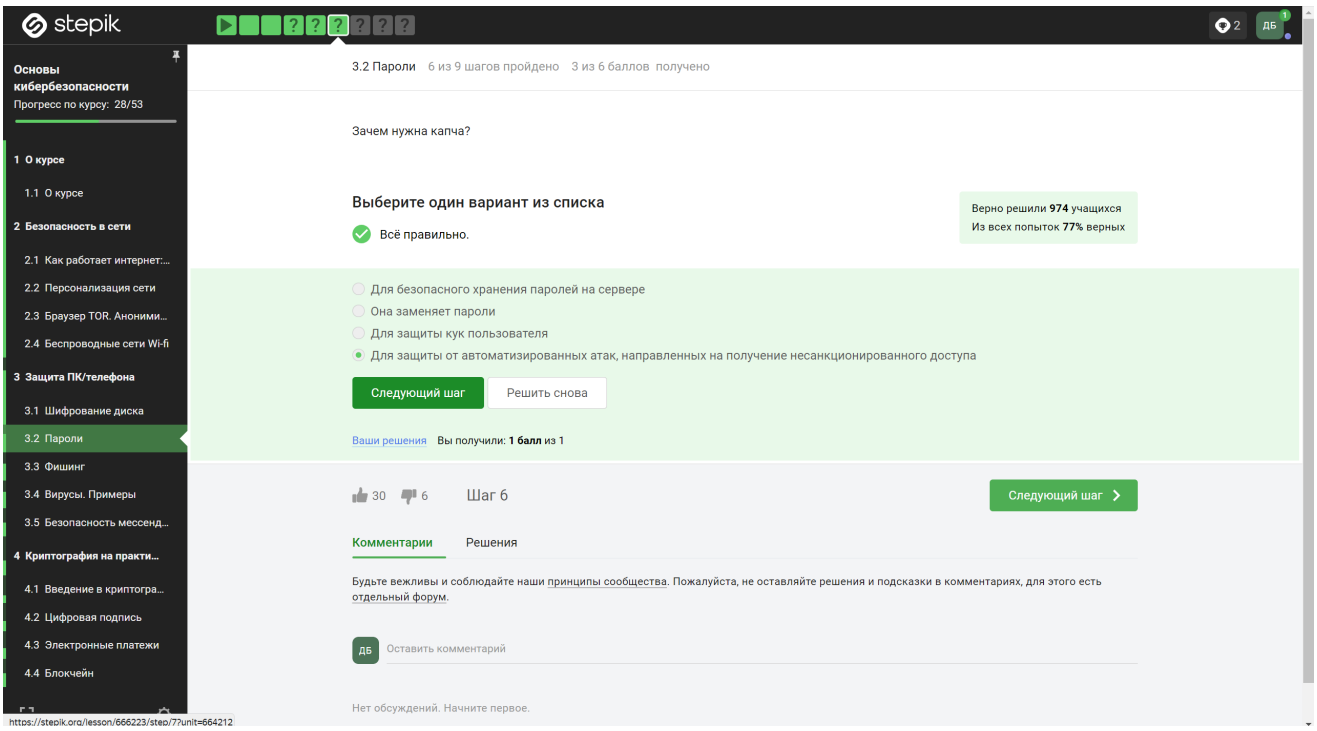

Figure 2.6: Рис. 3.6 Раздел (3.2) – Вопрос 3

Вопрос: Зачем нужна капча?

Ответ: Капча нужна для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

Пояснение: Капча обычно используется для различия между человеком и компьютерной программой, предотвращая автоматизированные атаки на веб-ресурсы.

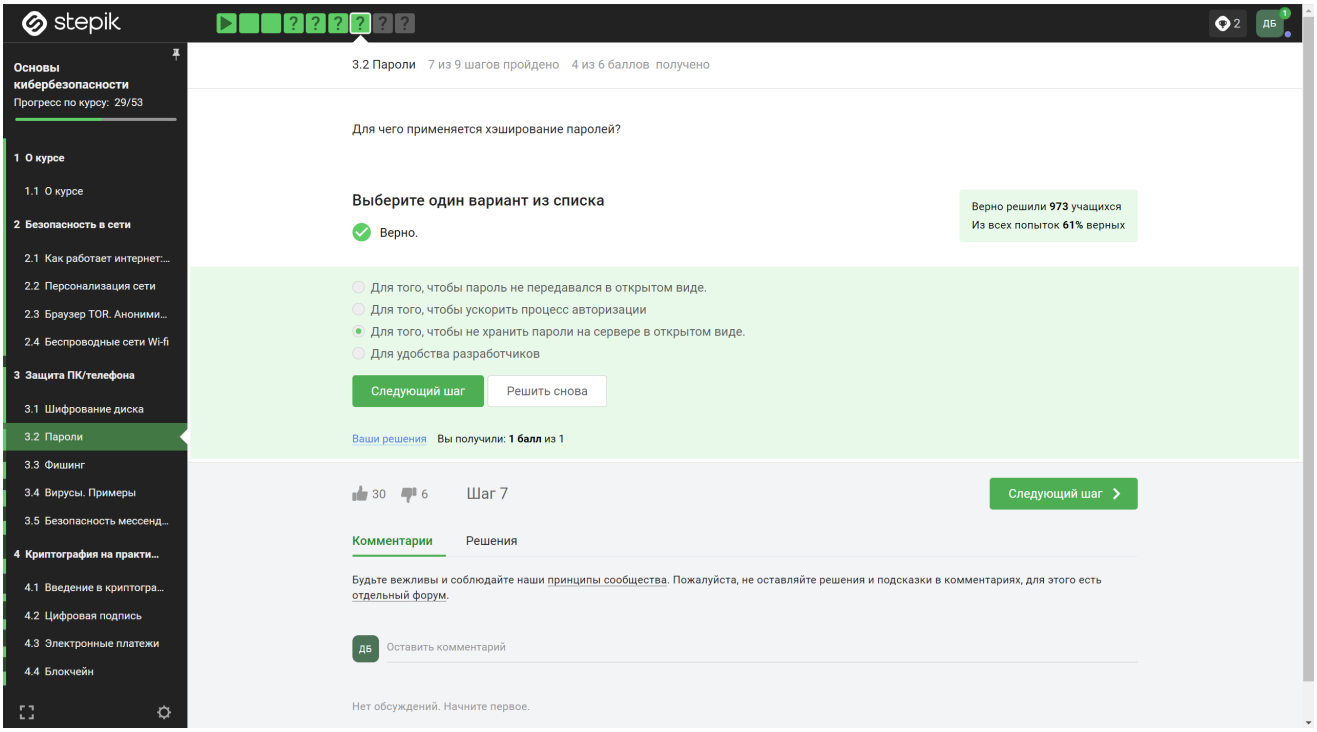

Figure 2.7: Рис. 3.7 Раздел (3.2) – Вопрос 4

Вопрос: Для чего применяется хэширование паролей?

Ответ: Хэширование паролей применяется для того, чтобы не хранить пароли на сервере в открытом виде.

Пояснение: Хэширование паролей обеспечивает безопасное хранение учетных данных, представляя их в виде непонятных для чтения хэш-значений.

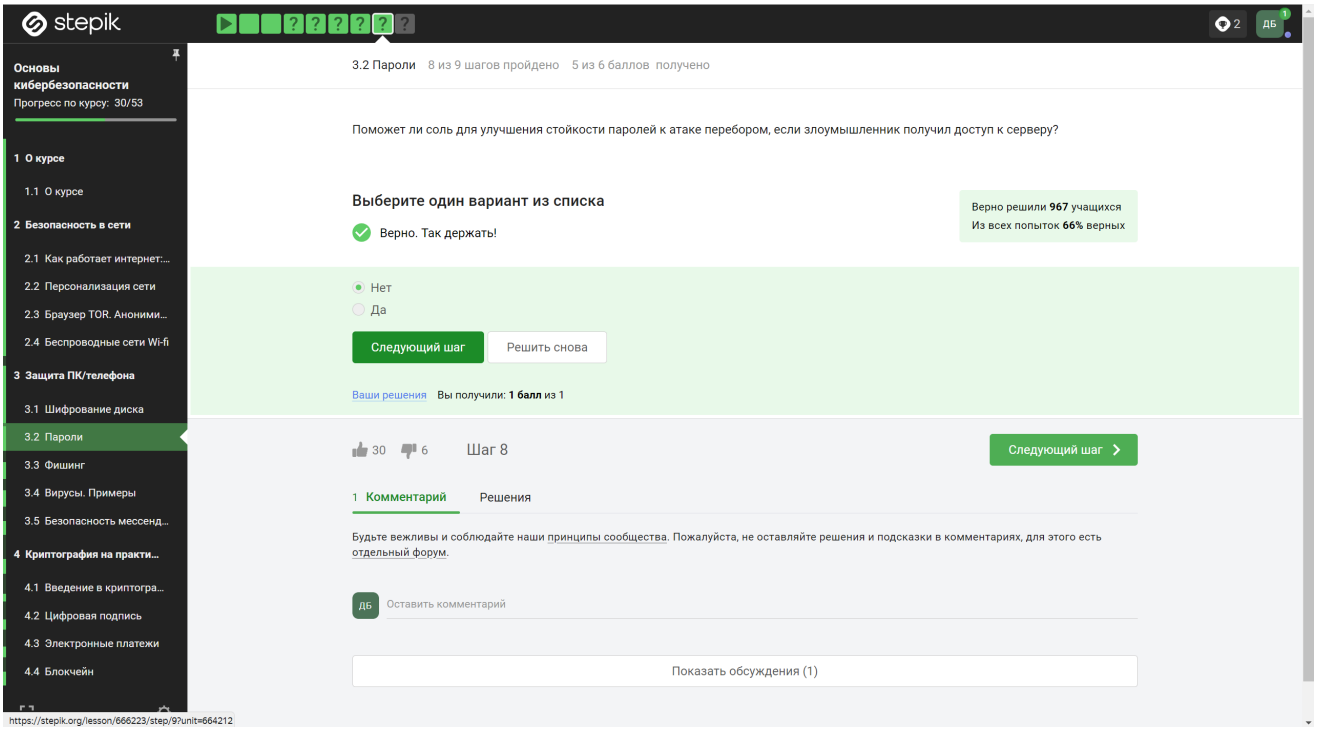

Figure 2.8: Рис. 3.8 Раздел (3.2) – Вопрос 5

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

Ответ: Нет, не поможет

Пояснение: Соль используется для усложнения хэширования паролей, но если злоумышленник получил доступ к серверу, он также получит доступ и к соли, уменьшая эффективность ее применения.

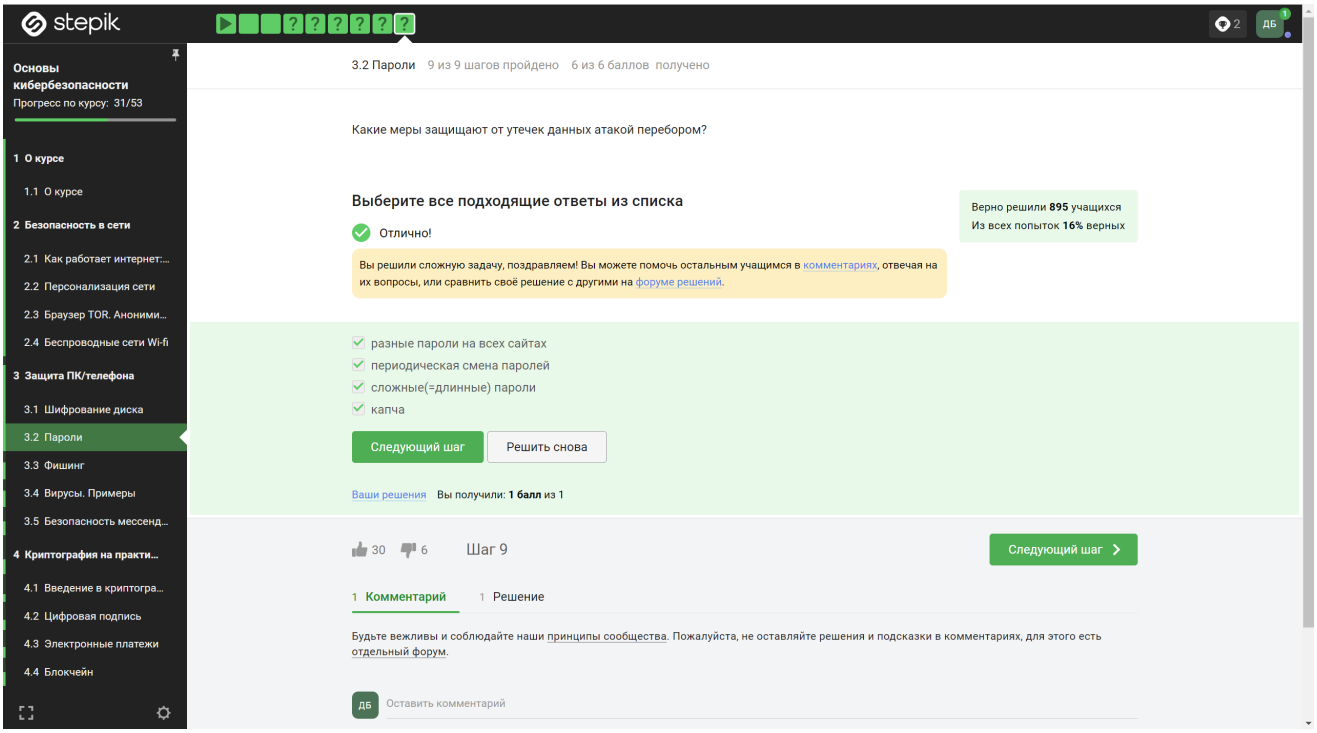

Figure 2.9: Рис. 3.9 Раздел (3.2) – Вопрос 6

Вопрос: Какие меры защищают от утечек данных атакой перебором?

Ответ: Всё перечисленное на слайде является отличной защитой

Пояснение: Комбинация сложных паролей, хэширования, соли и других мер безопасности обеспечивает надежную защиту от атак перебором.

2.1.3 (3.3) “Фишинг”

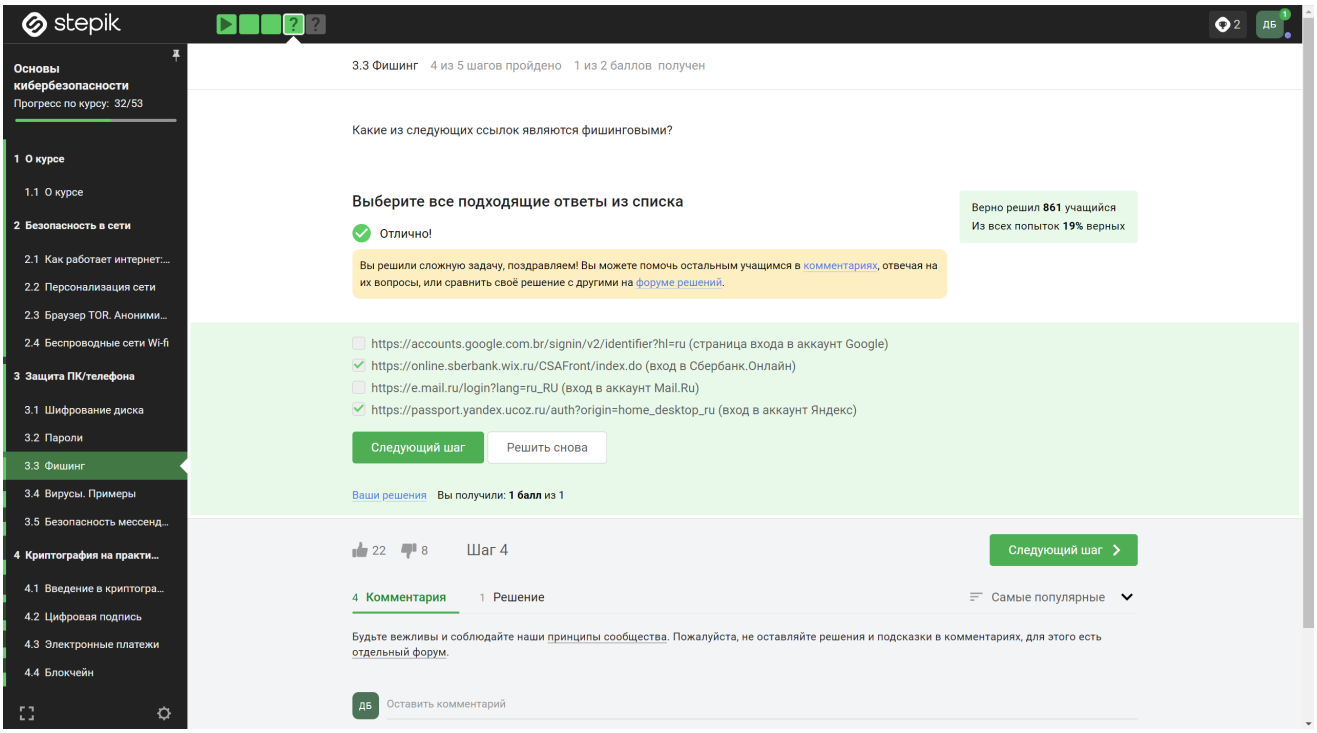

Figure 2.10: Рис. 3.10 Раздел (3.3) – Вопрос 1

Вопрос: Какие из следующих ссылок являются фишинговыми?

Ответ: Фишинговая ссылка — это мошенническая ссылка, которая выглядит достоверно, но на самом деле используется для кражи личных данных пользователя. Тут подходят сайты Сбербанка (.wix лишняя) и Яндекса (.ucoz лишняя)

Пояснение: Фишинговые сайты часто имитируют легитимные ресурсы, чтобы заполучить личную информацию пользователей.

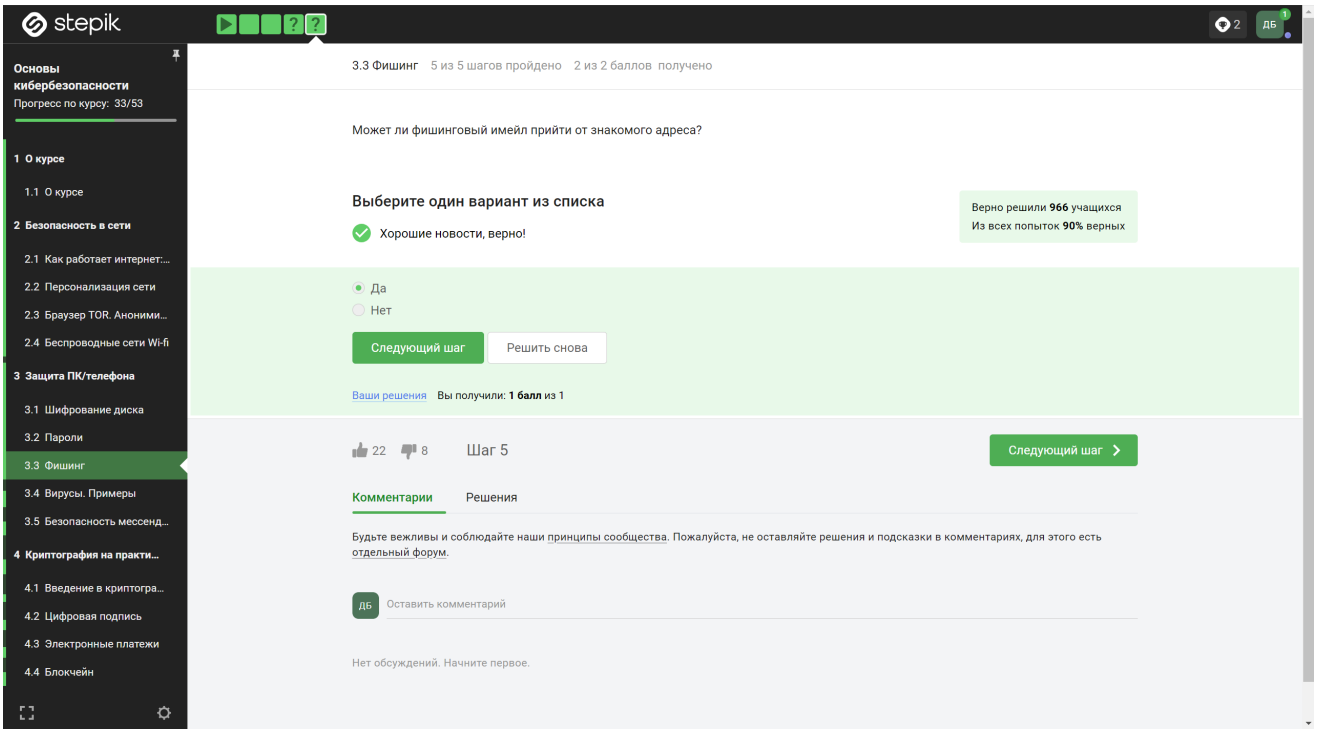

Figure 2.11: Рис. 3.11 Раздел (3.3) – Вопрос 2

Вопрос: Может ли фишинговый имейл прийти от знакомого адреса?

Ответ: Может, потому что они маскируются под известные пользователям сайты и почты

Пояснение: Злоумышленники могут подделывать адреса отправителей, включая адреса знакомых, чтобы придать их письмам вид легитимности и увеличить вероятность попадания на фишинговые сайты.

2.1.4 (3.4) “Вирусы. Примеры”

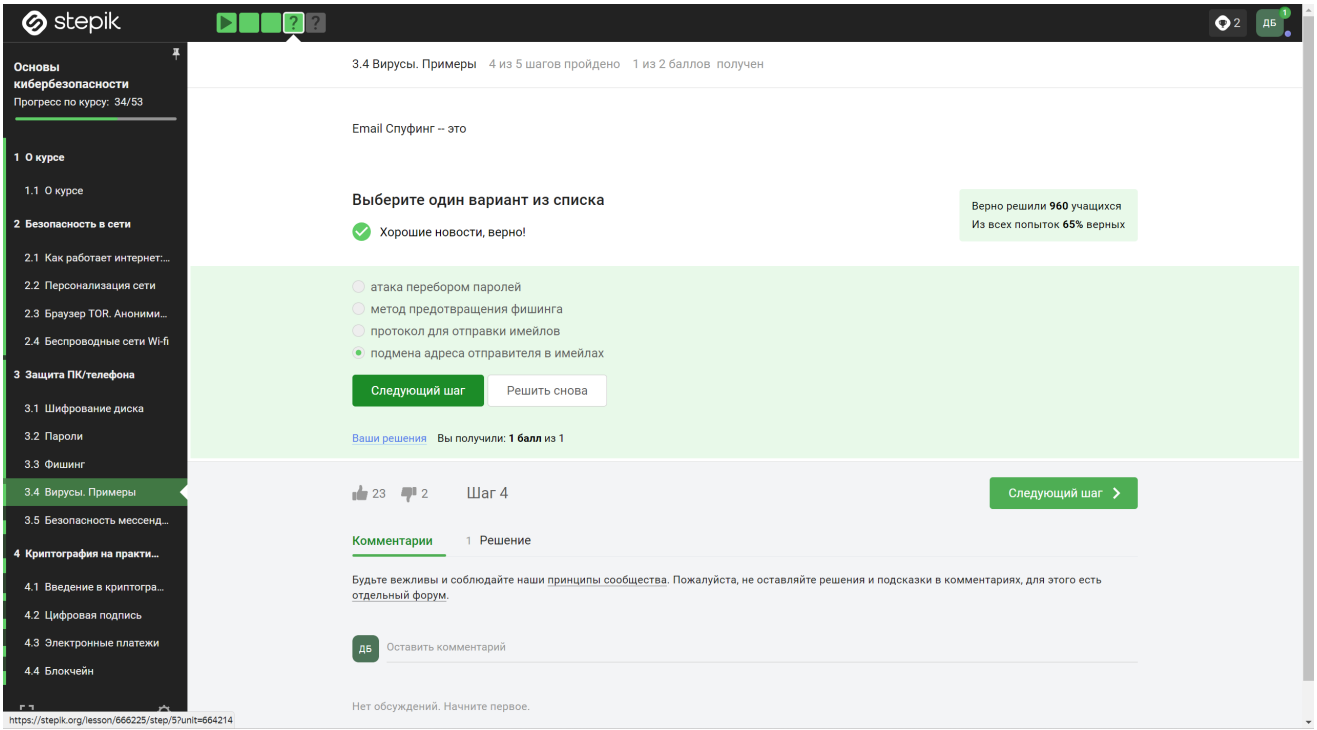

Figure 2.12: Рис. 3.12 Раздел (3.4) – Вопрос 1

Вопрос: Email Спуфинг - это

Ответ: Email Спуфинг - это подмена адреса отправителя в имейлах

Пояснение: Email Спуфинг позволяет злоумышленникам изменять адрес отправителя в электронных письмах с целью маскировки своей личности или создания ложного впечатления.

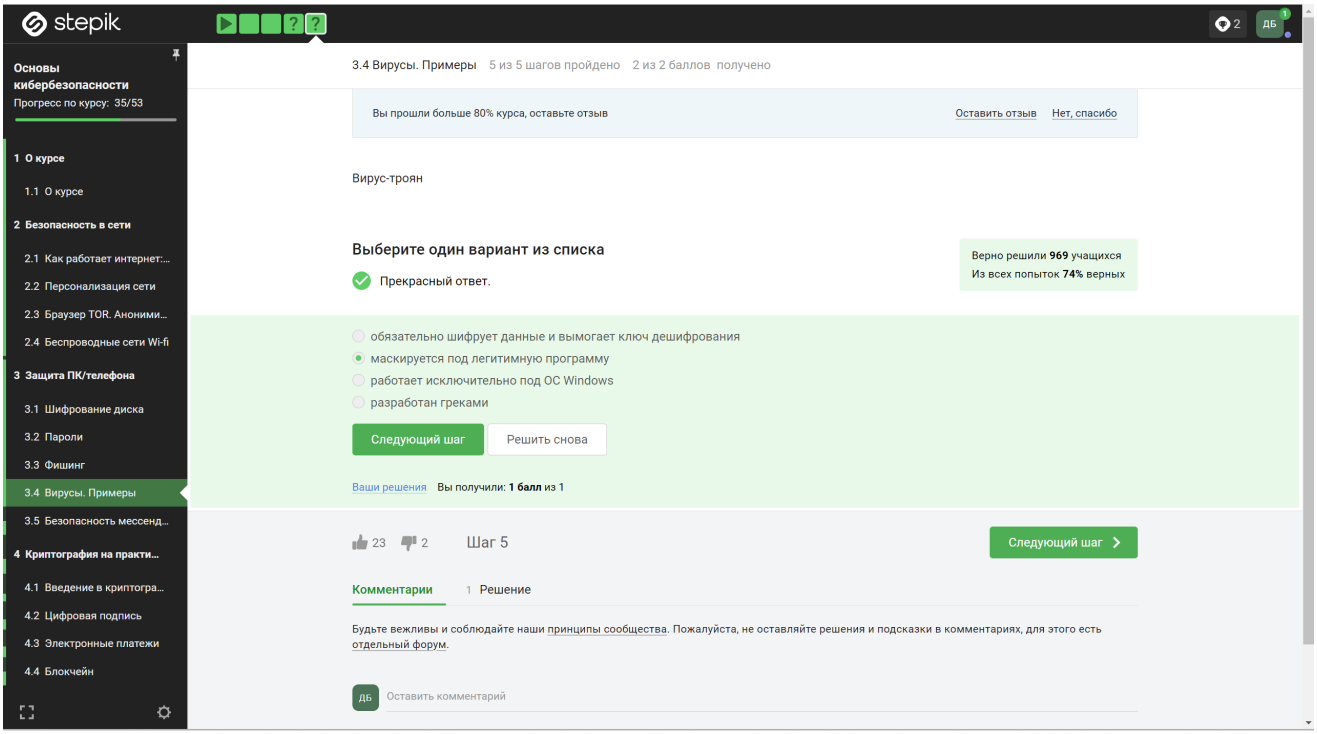

Figure 2.13: Рис. 3.13 Раздел (3.4) – Вопрос 2

Вопрос: Вирус-троян

Ответ: Он маскируется под легитимную программу или игры, чтобы взломать компьютер или украсть данные

Пояснение: Вирус-троян представляет собой вредоносное программное обеспечение, которое скрыто внедряется в систему под видом полезной программы, чтобы незаметно получить доступ к компьютеру и осуществить кражу данных или другие атаки.

2.1.5 (3.5) “Безопасность мессенджеров”

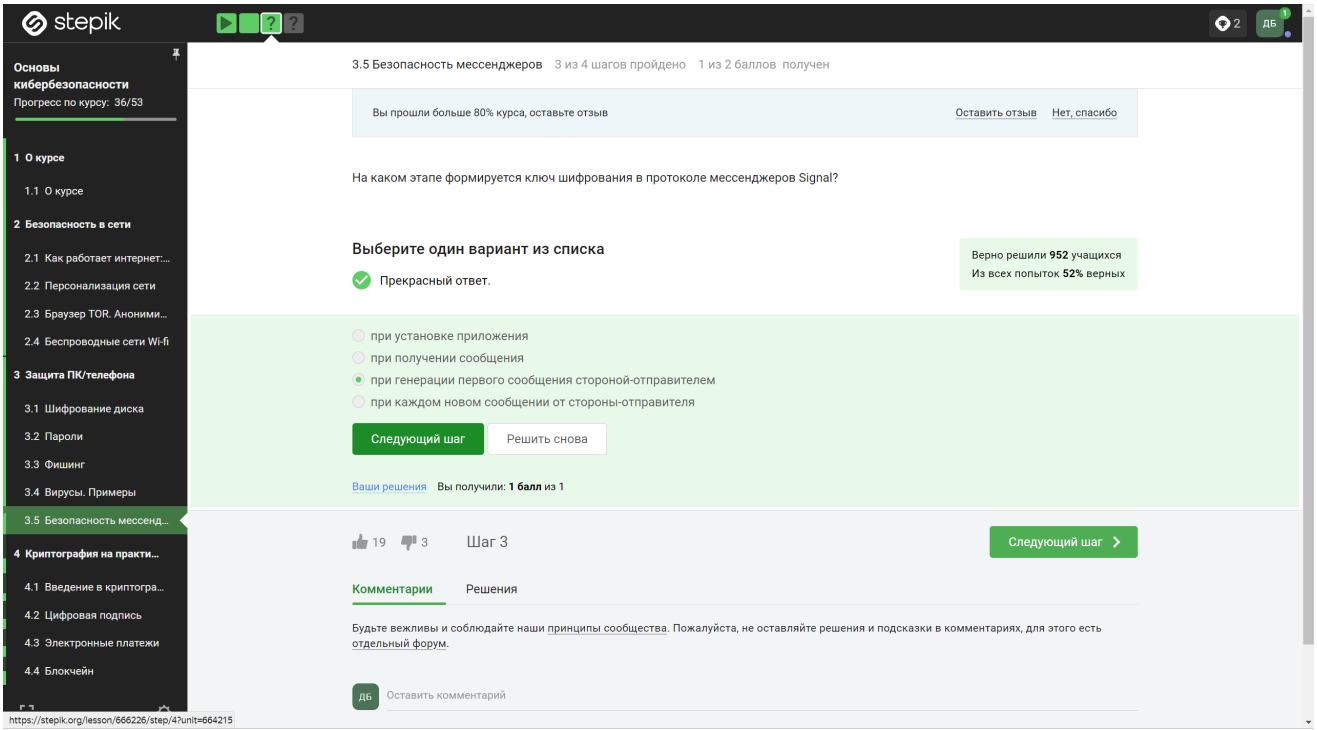

Figure 2.14: Рис. 3.14 Раздел (3.5) – Вопрос 1

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

Ответ: Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителем

Пояснение: Протокол мессенджера Signal использует протокол обмена ключами Диффи-Хеллмана, который формирует общий ключ шифрования при первом обмене сообщениями между отправителем и получателем.

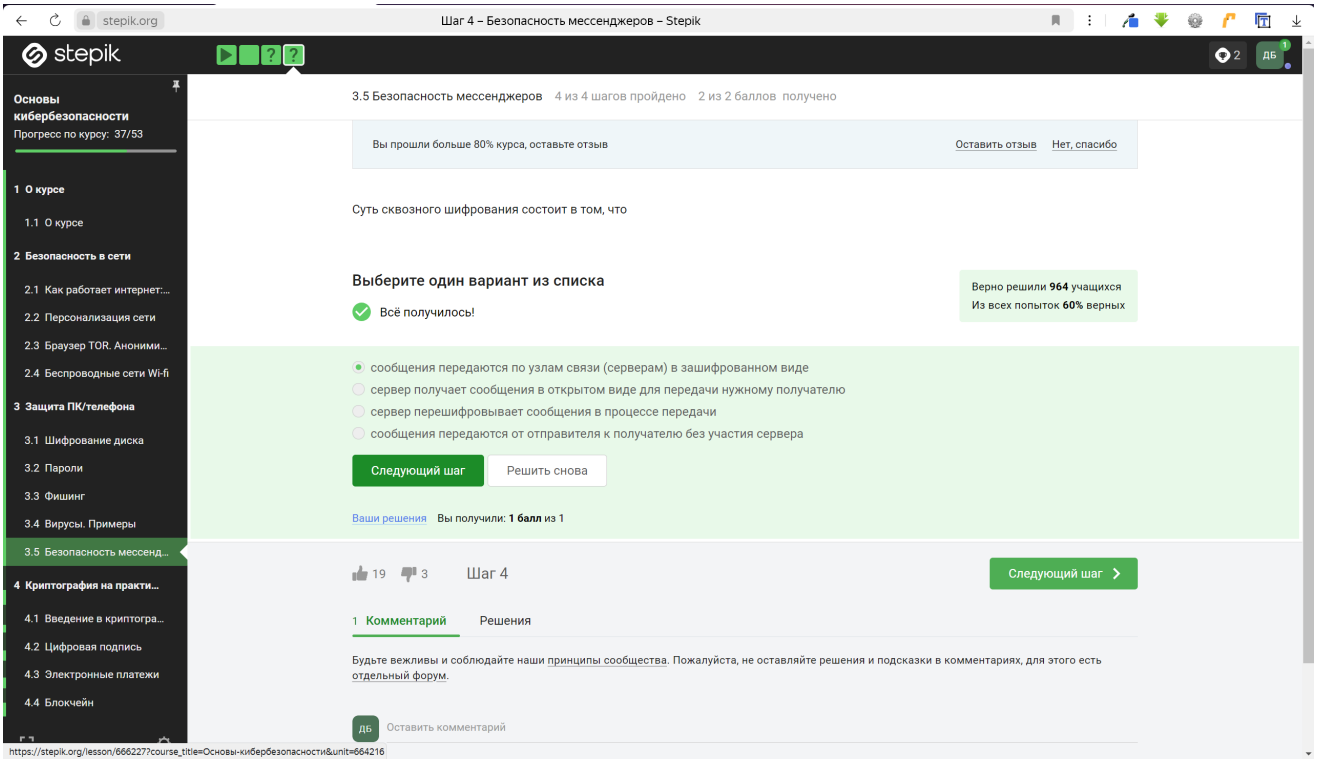

Figure 2.15: Рис. 3.15 Раздел (3.5) – Вопрос 2

Вопрос: Суть сквозного шифрования состоит в том, что

Ответ: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде

Пояснение: Сквозное шифрование (end-to-end encryption) обеспечивает защищенную передачу данных между отправителем и получателем, где сообщения шифруются на устройстве отправителя и расшифровываются только на устройстве получателя, минуя промежуточные серверы.

3 Вывод

В ходе прохождения внешних курсов были получены навыки о “Безопасности в сети”, “Защите ПК/телефона” и “Криптографии”.