

Отчёт к прохождению Внешнего курса

Основы кибербезопасности

Четвергова Мария Викторовна

Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6

Список иллюстраций

Список таблиц

1 Цель работы

Слушатели курса «Основы кибербезопасности» узнают, как обеспечивается безопасность интернет-трафика, какие пароли нужно выбирать и как их хранить, познакомятся с методами защиты сообщений в мессенджерах (WhatsApp, Telegram), поймут, как работают механизмы аутентификации в электронных платежах, а также зачем нас иногда просят выбрать квадраты, где изображены светофоры.

2 Последовательность выполнения работы

Разберём каждый раздел курса.

1 часть. Безопасность в сети

###Как работает интернет: базовые сетевые протоколы

В модели TCP/IP существует несколько уровней, а именно 4. И сейчас мы рассмотрим последовательно все четыре уровня модели TCP/IP. На самом верхнем уровне, прикладном работают пользовательские программы, и задача прикладного уровня - обеспечить доступ для этих пользовательских программ к услугам Интернет. Мы с вами пользуемся достаточно большим спектром программ в интернете, и каждая программа использует свой протокол. Например, браузеры и веб-страницы используют протокол HTTP или его современную версию HTTPS.

Все эти протоколы прикладного уровня работают над транспортным уровнем, это следующий уровень в модели TCP/IP. Транспортный уровень обеспечивает передачу данных между процессами на одной машине или хосте (host). Хост - это устройство, которое подключено к интернету. Это может быть компьютер, смартфон. И транспортный уровень отвечает за корректное распределение пакетов между программами. То есть он знает, что какие-то данные пришли нам в Skype, какие-то данные пришли нам на почту, какие-то данные должны прийти в наш браузер. Кроме того, протокол транспортного уровня, ответственный за адресацию, должен понимать, для какого процесса пришёл тот или иной пакет. На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. Этот протокол, в отличие от второго примера – UDP, обеспечивает надежную передачу

пакетов.

Транспортный уровень работает над следующим уровнем модели TCP, так называемым сетевым или межсетевым уровнем. В этом уровне принимает участие не только программа, не только наша машина, но уже наш роутер, то есть то устройство, к которому мы подключаемся, чтобы получить интернет. Сетевой уровень ответственен за передачу данных между различными физическими сетями; так, например, мы можем подключиться с компьютера, подключаясь через WiFi-сеть, к другому компьютеру, который, быть может, подключен через проводной интернет.

Сетевой уровень работает над так называемым канальным уровнем или самым низким уровнем модели TCP/IP. И в этой модели работает уже физика. Здесь происходит физическая передача данных. И здесь мы уже будем говорить о пропускной способности канала, об обеспечении помехоустойчивости, и основные примеры протоколов канального уровня непосредственно связаны с тем, как мы передаем данные.

Вот эти четыре уровня модели TCP/IP и происходят между тем, как мы запросили на нашей машине открыть какую-то веб-страницу. То есть наш запрос происходит через прикладной уровень от браузера в транспортный уровень, который понимает, что это идет от браузера, в сеть, которая нам говорит, что мы хотим получить такой-то веб-сайт. И мы передаем всю эту информации в виде бит, в виде потока данных в сеть. И для того, чтобы получить назад ответ, происходит ровно тот же самый протокол, тот же самый алгоритм.

Прохождение тестовой части:

stepik

2.1

2.2

2.3

2.4

2.5

2.6

2.7

2.8

2.9

2.10

2.11

2.12

2.13

2.14

2.15

2.16

2.17

2.18

2.19

2.20

2.21

2.22

2.23

2.24

2.25

2.26

2.27

2.28

2.29

2.30

2.31

2.32

2.33

2.34

2.35

2.36

2.37

2.38

2.39

2.40

2.41

2.42

2.43

2.44

2.45

2.46

2.47

2.48

2.49

2.50

2.51

2.52

2.53

2.54

2.55

2.56

2.57

2.58

2.59

2.60

2.61

2.62

2.63

2.64

2.65

2.66

2.67

2.68

2.69

2.70

2.71

2.72

2.73

2.74

2.75

2.76

2.77

2.78

2.79

2.80

2.81

2.82

2.83

2.84

2.85

2.86

2.87

2.88

2.89

2.90

2.91

2.92

2.93

2.94

2.95

2.96

2.97

2.98

2.99

3.00

3.01

3.02

3.03

3.04

3.05

3.06

3.07

3.08

3.09

3.10

3.11

3.12

3.13

3.14

3.15

3.16

3.17

3.18

3.19

3.20

3.21

3.22

3.23

3.24

3.25

3.26

3.27

3.28

3.29

3.30

3.31

3.32

3.33

3.34

3.35

3.36

3.37

3.38

3.39

3.40

3.41

3.42

3.43

3.44

3.45

3.46

3.47

3.48

3.49

3.50

3.51

3.52

3.53

3.54

3.55

3.56

3.57

3.58

3.59

3.60

3.61

3.62

3.63

3.64

3.65

3.66

3.67

3.68

3.69

3.70

3.71

3.72

3.73

3.74

3.75

3.76

3.77

3.78

3.79

3.80

3.81

3.82

3.83

3.84

3.85

3.86

3.87

3.88

3.89

3.90

3.91

3.92

3.93

3.94

3.95

3.96

3.97

3.98

3.99

4.00

4.01

4.02

4.03

4.04

4.05

4.06

4.07

4.08

4.09

4.10

4.11

4.12

4.13

4.14

4.15

4.16

4.17

4.18

4.19

4.20

4.21

4.22

4.23

4.24

4.25

4.26

4.27

4.28

4.29

4.30

4.31

4.32

4.33

4.34

4.35

4.36

4.37

4.38

4.39

4.40

4.41

4.42

4.43

4.44

4.45

4.46

4.47

4.48

4.49

4.50

4.51

4.52

4.53

4.54

4.55

4.56

4.57

4.58

4.59

4.60

4.61

4.62

4.63

4.64

4.65

4.66

4.67

4.68

4.69

4.70

4.71

4.72

4.73

4.74

4.75

4.76

4.77

4.78

4.79

4.80

4.81

4.82

4.83

4.84

4.85

4.86

4.87

4.88

4.89

4.90

4.91

4.92

4.93

4.94

4.95

4.96

4.97

4.98

4.99

5.00

5.01

5.02

5.03

5.04

5.05

5.06

5.07

5.08

5.09

5.10

5.11

5.12

5.13

5.14

5.15

5.16

5.17

5.18

5.19

5.20

5.21

5.22

5.23

5.24

5.25

5.26

5.27

5.28

5.29

5.30

5.31

5.32

5.33

5.34

5.35

5.36

5.37

5.38

5.39

5.40

5.41

5.42

5.43

5.44

5.45

5.46

5.47

5.48

5.49

5.50

5.51

5.52

5.53

5.54

5.55

5.56

5.57

5.58

5.59

5.60

5.61

5.62

5.63

5.64

5.65

5.66

5.67

5.68

5.69

5.70

5.71

5.72

5.73

5.74

5.75

5.76

5.77

5.78

5.79

5.80

5.81

5.82

5.83

5.84

5.85

5.86

5.87

5.88

5.89

5.90

5.91

5.92

5.93

5.94

5.95

5.96

5.97

5.98

5.99

6.00

6.01

6.02

6.03

6.04

6.05

6.06

6.07

6.08

6.09

6.10

6.11

6.12

6.13

6.14

6.15

6.16

6.17

6.18

6.19

6.20

6.21

6.22

6.23

6.24

6.25

6.26

6.27

6.28

6.29

6.30

6.31

6.32

6.33

6.34

6.35

6.36

6.37

6.38

6.39

6.40

6.41

6.42

6.43

6.44

6.45

6.46

6.47

6.48

6.49

6.50

6.51

6.52

6.53

6.54

6.55

6.56

6.57

6.58

6.59

6.60

6.61

6.62

6.63

6.64

6.65

6.66

6.67

6.68

6.69

6.70

6.71

6.72

6.73

6.74

6.75

6.76

6.77

6.78

6.79

6.80

6.81

6.82

6.83

6.84

6.85

6.86

6.87

6.88

6.89

6.90

6.91

6.92

6.93

6.94

6.95

6.96

6.97

6.98

6.99

7.00

7.01

7.02

7.03

7.04

7.05

7.06

7.07

7.08

7.09

7.10

7.11

7.12

7.13

7.14

7.15

7.16

7.17

7.18

7.19

7.20

7.21

7.22

7.23

7.24

7.25

7.26

7.27

7.28

7.29

7.30

7.31

7.32

7.33

7.34

7.35

7.36

7.37

7.38

7.39

7.40

7.41

7.42

7.43

7.44

7.45

7.46

7.47

7.48

7.49

7.50

7.51

7.52

7.53

7.54

7.55

7.56

7.57

7.58

7.59

7.60

7.61

7.62

7.63

7.64

7.65

7.66

7.67

7.68

7.69

7.70

7.71

7.72

7.73

7.74

7.75

7.76

7.77

7.78

7.79

7.80

7.81

7.82

7.83

7.84

7.85

7.86

7.87

7.88

7.89

7.90

7.91

7.92

7.93

7.94

7.95

7.96

7.97

7.98

7.99

8.00

8.01

8.02

8.03

8.04

8.05

8.06

8.07

8.08

8.09

8.10

8.11

8.12

8.13

8.14

8.15

8.16

8.17

8.18

8.19

8.20

8.21

8.22

8.23

8.24

8.25

8.26

8.27

8.28

8.29

8.30

8.31

8.32

8.33

8.34

8.35

8.36

8.37

8.38

8.39

8.40

8.41

8.42

8.43

8.44

8.45

8.46

8.47

8.48

8.49

8.50

8.51

8.52

8.53

8.54

8.55

8.56

8.57

8.58

8.59

8.60

8.61

8.62

8.63

8.64

8.65

8.66

8.67

8.68

8.69

8.70

8.71

8.72

8.73

8.74

8.75

8.76

8.77

8.78

8.79

8.80

8.81

8.82

8.83

8.84

8.85

8.86

8.87

8.88

8.89

8.90

8.91

8.92

8.93

8.94

8.95

8.96

8.97

8.98

8.99

9.00

9.01

9.02

9.03

9.04

9.05

9.06

9.07

9.08

9.09

9.10

9.11

9.12

9.13

9.14

9.15

9.16

9.17

9.18

9.19

9.20

9.21

9.22

9.23

9.24

9.25

9.26

9.27

9.28

9.29

9.30

9.31

9.32

9.33

9.34

9.35

9.36

9.37

9.38

9.39

9.40

9.41

9.42

9.43

9.44

9.45

9.46

9.47

9.48

9.49

9.50

9.51

9.52

9.53

9.54

9.55

9.56

9.57

9.58

9.59

9.60

9.61

9.62

9.63

9.64

9.65

9.66

9.67

9.68

9.69

9.70

9.71

9.72

9.73

9.74

9.75

9.76

9.77

9.78

9.79

9.80

9.81

9.82

9.83

9.84

9.85

9.86

9.87

9.88

9.89

9.90

9.91

9.92

9.93

9.94

9.95

9.96

9.97

9.98

9.99

10.00

10.01

10.02

10.03

10.04

10.05

10.06

10.07

10.08

10.09

10.10

10.11

10.12

10.13

10.14

10.15

10.16

10.17

10.18

10.19

10.20

10.21

10.22

10.23

10.24

10.25

10.26

10.27

10.28

10.29

10.30

10.31

10.32

10.33

10.34

10.35

10.36

10.37

10.38

10.39

10.40

10.41

10.42

10.43

10.44

10.45

10.46

10.47

10.48

10.49

10.50

10.51

10.52

10.53

10.54

10.55

10.56

10.57

10.58

10.59

10.60

10.61

10.62

10.63

10.64

10.65

10.66

10.67

10.68

10.69

10.70

10.71

10.72

10.73

10.74

10.75

10.76

10.77

10.78

10.79

10.80

10.81

10.82

10.83

10.84

10.85

10.86

10.87

10.88

10.89

10.90

10.91

10.92

10.93

10.94

10.95

10.96

10.97

10.98

10.99

11.00

11.01

11.02

11.03

11.04

11.05

11.06

11.07

11.08

11.09

11.10

11.11

11.12

11.13

11.14

11.15

11.16

11.17

11.18

11.19

11.20

11.21

11.22

11.23

11.24

11.25

11.26

11.27

11.28

11.29

11.30

11.31

11.32

11.33

11.34

11.35

11.36

11.37

11.38

11.39

11.40

11.41

11.42

11.43

11.44

11.45

11.46

11.47

11.48

11.49

11.50

11.51

11.52

11.53

11.54

11.55

11.56

11.57

11.58

11.59

11.60

11.61

11.62

11.63

11.64

11.65

11.66

11.67

11.68

11.69

11.70

11.71

11.72

11.73

11.74

11.75

11.76

11.77

11.78

11.79

11.80

11.81

11.82

11.83

11.84

11.85

11.86

11.87

11.88

11.89

11.90

11.91

11.92

11.93

11.94

11.95

11.96

11.97

11.98

11.99

12.00

12.01

12.02

12.03

12.04

12.05

12.06

12.07

12.08

12.09

12.10

12.11

12.12

12.13

12.14

12.15

12.16

12.17

12.18

12.19

12.20

12.21

12.22

12.23

12.24

12.25

12.26

12.27

12.28

12.29

12.30

12.31

12.32

12.33

12.34

12.35

12.36

12.37

12.38

12.39

12.40

12.41

12.42

12.43

12.44

12.45

12.46

12.47

12.48

12.49

12.50

12.51

12.52

12.53

12.54

12.55

12.56

12.57

12.58

12.59

12.60

12.61

12.62

12.63

12.64

12.65

12.66

12.67

12.68

12.69

12.70

12.71

12.72

12.73

12.74

12.75

12.76

12.77

12.78

12.79

12.80

12.81

12.82

12.83

12.84

12.85

12.86

12.87

12.88

12.89

12.90

12.91

12.92

12.93

12.94

12.95

12.96

12.97

12.98

12.99

13.00

13.01

13.02

13.03

13.04

13.05

13.06

13.07

13.08

13.09

13.10

13.11

13.12

13.13

13.14

13.15

13.16

13.17

13.18

13.19

13.20

13.21

13.22

13.23

13.24

13.25

13.26

13.27

13.28

13.29

13.30

13.31

13.32

13.33

13.34

13.35

13.36

13.37

13.38

13.39

13.40

13.41

13.42

13.43

13.44

13.45

13.46

13.47

13.48

13.49

13.50

13.51

13.52

13.53

13.54

13.55

13.56

13.57

13.58

13.59

13.60

13.61

13.62

13.63

13.64

13.65

13.66

13.67

13.68

13.69

13.70

13.71

13.72

13.73

13.74

13.75

13.76

13.77

13.78

13.79

13.80

13.81

13.82

13.83

13.84

13.85

13.86

13.87

13.88

13.89

13.90

13.91

13.92

13.93

13.94

13.95

Основы кибербезопасности
Прогресс по курсу: 5/53

1 0 курс
1.1 0 курс
2 Безопасность в сети
2.1 Как работает интернет...

2.1 Как работает интернет: базовые сетевые протоколы 11 из 13 шагов пройдено 5 из 8 баллов получено

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

Отличный ответ!

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

Ваш ответ Вы получили: 1 балл

92 11 Шаг 11

Комментарии Решение

Будьте внимательны и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте отзывы и подкормки в комментариях, для этого есть отдельный форум

Основы кибербезопасности
Прогресс по курсу: 6/53

1 0 курс
1.1 0 курс
2 Безопасность в сети
2.1 Как работает интернет...

2.1 Как работает интернет: базовые сетевые протоколы 13 из 16 шагов пройдено 6 из 9 баллов получено

Протокол http предполагает

Выберите один вариант из списка

Отлично!

Верно решил 946 учащийся
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

Ваш ответ Вы получили: 1 балл

92 11 Шаг 12

Комментарии Решение

Будьте внимательны и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте отзывы и подкормки в комментариях, для этого есть отдельный форум

Основы кибербезопасности
Прогресс по курсу: 7/53

1 0 курс
1.1 0 курс
2 Безопасность в сети
2.1 Как работает интернет...

2.1 Как работает интернет: базовые сетевые протоколы 13 из 16 шагов пройдено 7 из 9 баллов получено

Протокол https состоит из

Выберите один вариант из списка

Прекрасный ответ!

Верно решила 948 учащийся
Из всех попыток 41% верных

одной фазы аутентификации сервера
двух фаз: рукопожатия и передачи данных
двух фаз: аутентификация клиента и сервера и шифрование данных
трех фаз: аутентификация клиента, аутентификация сервера, генерация общего ключа

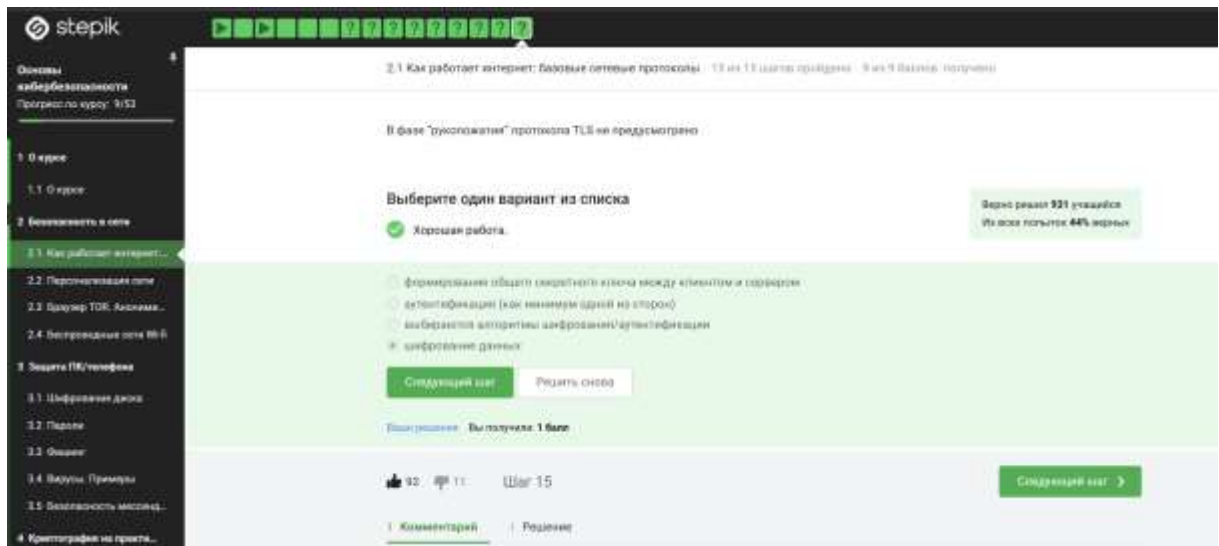
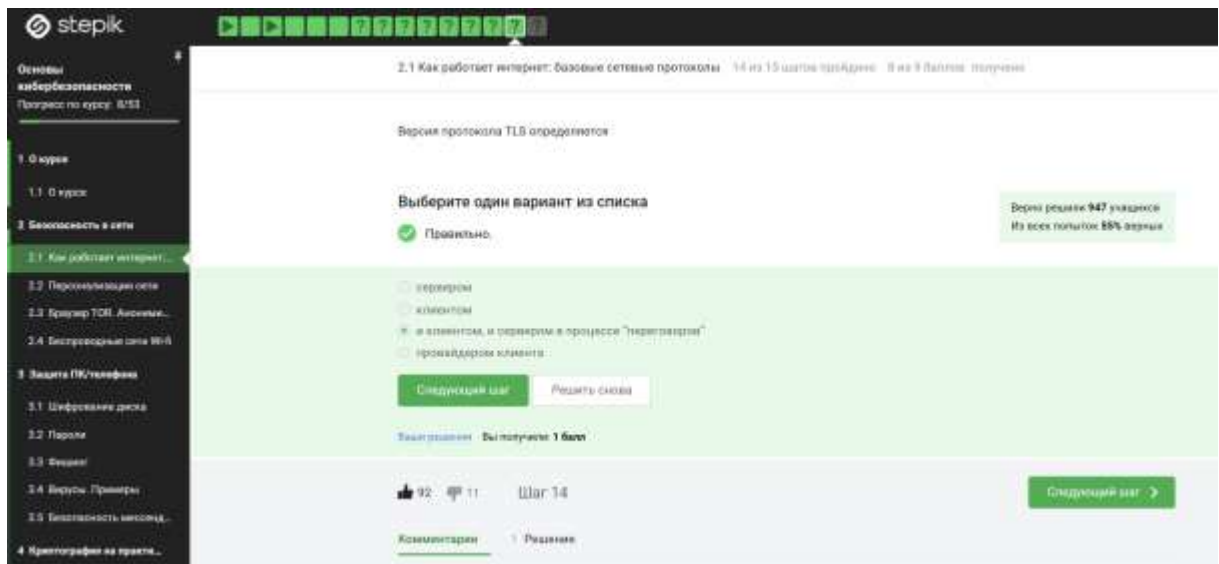
Следующий шаг Решить снова

Ваш ответ Вы получили: 1 балл

92 11 Шаг 13

Комментарии Решение

Самые популярные



Персонализация сети

Прохождение тестовой части

stepik

2.2 Персонализация сети

3 из 6 шагов пройдено 1 из 4 баллов получено

Основа кибербезопасности

Прогресс по курсу: 10/30

1 Этап

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Кранер TOR, Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Цифровая гигиена

3.2 Пароли

3.3 Фейки

3.4 Версии, Примеры

3.5 Безопасность мессен...

4 Критерии на практике...

4.1 Вопросы к критериям

4.2 Цифровая гигиена

4.3 Электронные подписи

4.4 Безопасность

Курс хранит:

Выберите все подходящие ответы из списка

Верно: 85% учащихся
Из всех попыток 18% верных

Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в этом вопросе, ставя на него вопрос, или сравнить свой ответ с другими на форуме решений.

☐ IP-адрес
 ☒ идентификатор пользователя
 ☒ cookies
 ☐ пароль пользователя

Следующий шаг

Решить задачу

Ваш ответ:

Вы получили 1 балл

36

13

Шаг 3

Следующий шаг

Комментарий

Решение

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решение и подсказки в комментариях, для этого есть специальный форум.

stepik

2.2 Персонализация сети

4 из 6 шагов пройдено 3 из 4 баллов получено

Основа кибербезопасности

Прогресс по курсу: 11/30

1 Этап

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Кранер TOR, Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Цифровая гигиена

3.2 Пароли

3.3 Фейки

3.4 Версии, Примеры

3.5 Безопасность мессен...

4 Критерии на практике...

4.1 Вопросы к критериям

4.2 Цифровая гигиена

4.3 Электронные подписи

4.4 Безопасность

Курс не используется для:

Выберите один вариант из списка

Верно: 96% учащихся
Из всех попыток 53% верных

Правильно.

☐ идентификация пользователя
 ☐ персонализация веб-страниц
 ☐ отслеживание информации о пользователе
 ☐ сбор статистики посещаемости сайта
 ☒ улучшение надежности соединения

Следующий шаг

Решить задачу

Свой ответ:

Вы получили 1.5 балла

36

13

Шаг 4

Следующий шаг

Комментарий

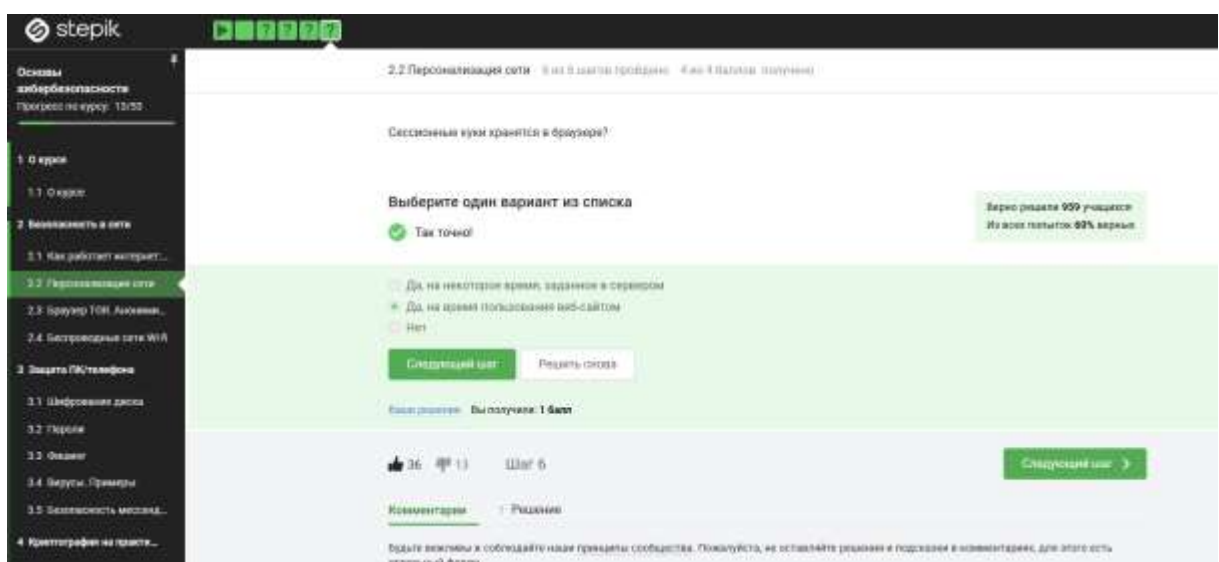
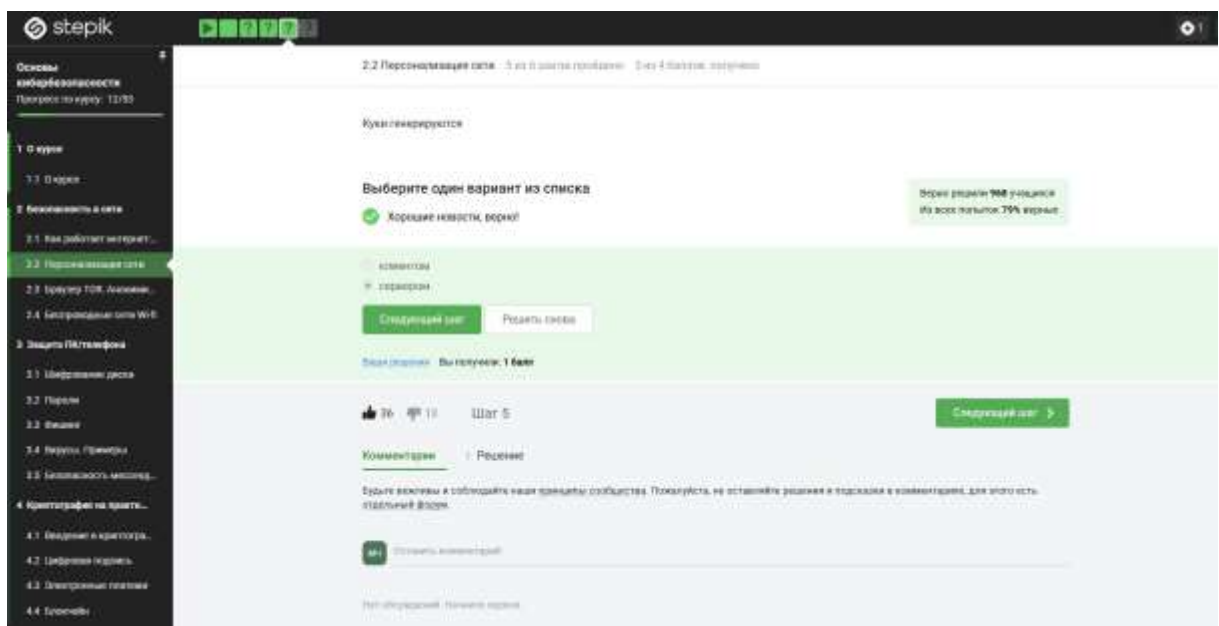
Решение

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решение и подсказки в комментариях, для этого есть специальный форум.

13

Создать комментарий

12



Браузер TOR. Анонимизация

Выполнение тестовой части:

stepik

2.3

2.3

2.3

2.3

2.3

2.3

Основы кибербезопасности

Прогресс по курсу: 14/50

1. 0 курса

1.1 0 курса

2. Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимизация

2.4 Беспроводная сеть Wi-Fi

3. Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Вредонос. Примеры

3.5 Безопасность методов...

4. Криптография на практике...

4.1 Введение в криптографию...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

2.3 Браузер TOR. Анонимизация

2 из 6 шагов пройдено

1 из 4 баллов получено

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

✓

Отличное решение!

Всего решено 858 учениками

Из всех попыток 77% верны

2

3

4

Следующий шаг

Решить снова

Ваше решение: Вы получили: 1 балл

43

4

Шаг 3

Следующий шаг

Комментарии

Рецензии

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решения и подписки в комментариях, для этого есть отдельный форум.

43

31 добавить комментарий

stepik

2.3

2.3

2.3

2.3

2.3

2.3

Основы кибербезопасности

Прогресс по курсу: 15/50

1. 0 курса

1.1 0 курса

2. Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимизация

2.4 Беспроводная сеть Wi-Fi

3. Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Вредонос. Примеры

3.5 Безопасность методов...

4. Криптография на практике...

4.1 Введение в криптографию...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

2.3 Браузер TOR. Анонимизация

4 из 6 шагов пройдено

2 из 4 баллов получено

IP-адрес принимающей машины

Выберите все подходящие ответы из списка

✓

Абсолютно точно.

Всего решено 908 учениками

Из всех попыток 10% верны

одному узлу

промежуточному узлу

отправителю

выдающему узлу

Следующий шаг

Решить снова

Ваше решение: Вы получили: 1 балл

43

4

Шаг 4

Следующий шаг

4

Комментарии

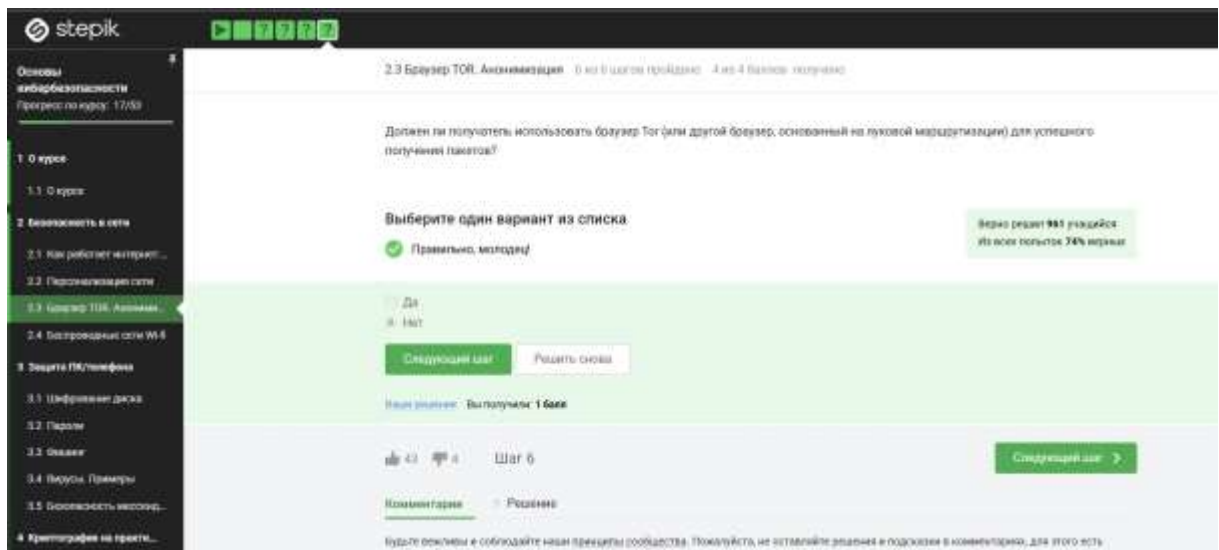
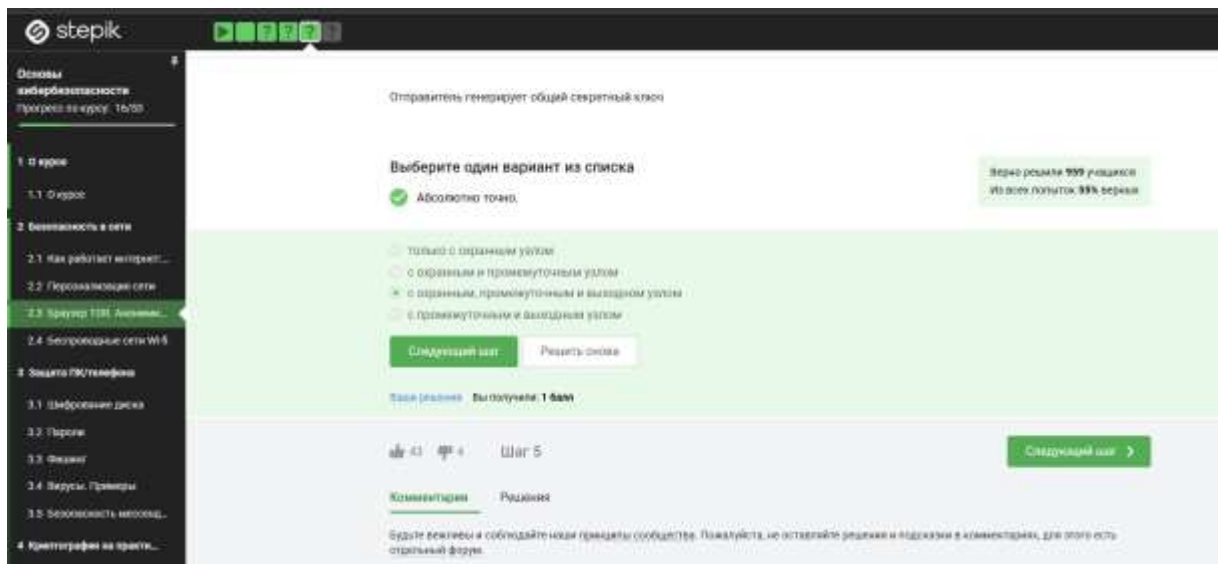
Рецензии

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решения и подписки в комментариях, для этого есть отдельный форум.

43

31 добавить комментарий

14



Беспроводные сети Wi-fi

Выполнение тестовой части:

stepik

Основы кибербезопасности
Прогресс по курсу: 18/58

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Вишн

3.4 Версии. Примеры

3.5 Безопасность мессенд...

4 Криптография на приме...

4.1 Введение в криптогра...

4.2 Шифрование подписи

2.4 Беспроводные сети Wi-Fi 4 из 5 шагов пройдено 1 из 5 баллов получено

Wi-Fi - это

Выберите один вариант из списка

✓ Правильно.

Верно решили 945 учащихся
Из всех попыток 76% верные

☐ изобретением от "Apple's iPhone"
☒ технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11
☐ метод соединения компьютеров по проводной сети Ethernet
☐ метод подключения смартфона к глобальной сети Интернет

Следующий шаг Решить снова

Ваше решение Вы получили 1 балл

39 4 Шаг 4

Следующий шаг

1 Комментарий Решения

Курс полезен и соблюдайте правила сообщества. Пожалуйста, не оставляйте отзывы и подраки в комментариях, для этого есть отдельный форум.

stepik

Основы кибербезопасности
Прогресс по курсу: 18/58

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Вишн

3.4 Версии. Примеры

3.5 Безопасность мессенд...

2.4 Беспроводные сети Wi-Fi 5 из 5 шагов пройдено 2 из 5 баллов получено

На каком уровне работает протокол WIFI?

Выберите один вариант из списка

✓ Верно.

Верно решили 972 учащихся
Из всех попыток 86% верные

☐ Транспортном
☐ Прикладном
☒ Канальном
☐ Сетевом

Следующий шаг Решить снова

Ваше решение Вы получили 1 балл

38 4 Шаг 5

Следующий шаг

Комментарии Решения

stepik

1

2

3

4

5

6

Основы кибербезопасности

Прогресс по курсу: 24/100

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Брандмауэр TCP/IP. Аппарат...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вредные программы

3.5 Безопасность мессендж...

4 Криптография на практике...

4.1 Введение в криптогра...

4.2 Цифровая подпись

2.4 Беспроводные сети Wi-Fi

6 из 8 шагов пройдено

3 из 5 баллов получено

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

Верно. Так держат!

Верно решили 973 учащихся

Из всех попыток 60% верны

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг

Решить снова

Ваш результат:

Вы получили: 1 балл

35

4

Шаг 6

Следующий шаг

Комментарии

Решения

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте реакции и подвохи в комментариях, для этого есть отдельный форум.

stepik

1

2

3

4

5

6

Основы кибербезопасности

Прогресс по курсу: 24/100

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Брандмауэр TCP/IP. Аппарат...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вредные программы

3.5 Безопасность мессендж...

4 Криптография на практике...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные подписи

2.4 Беспроводные сети Wi-Fi

7 из 8 шагов пройдено

4 из 5 баллов получено

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

Так точно!

Верно решили 979 учащихся

Из всех попыток 53% верны

☒ 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

Ваш результат:

Вы получили: 1 балл

34

4

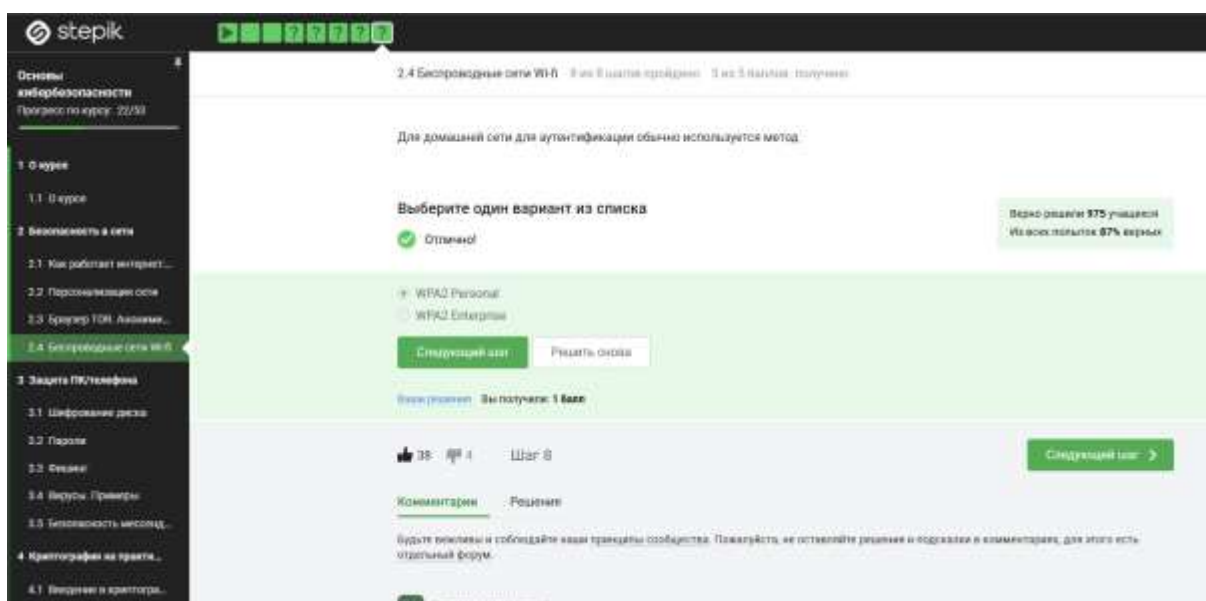
Шаг 7

Следующий шаг

Комментарии

Решения

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте реакции и подвохи в комментариях, для этого есть отдельный форум.



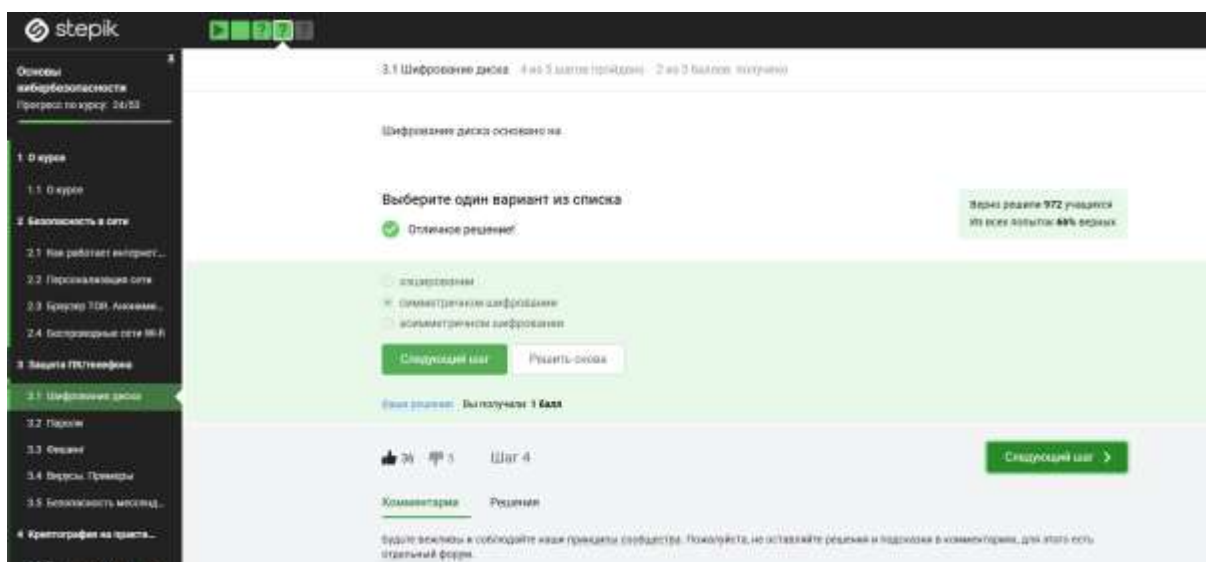
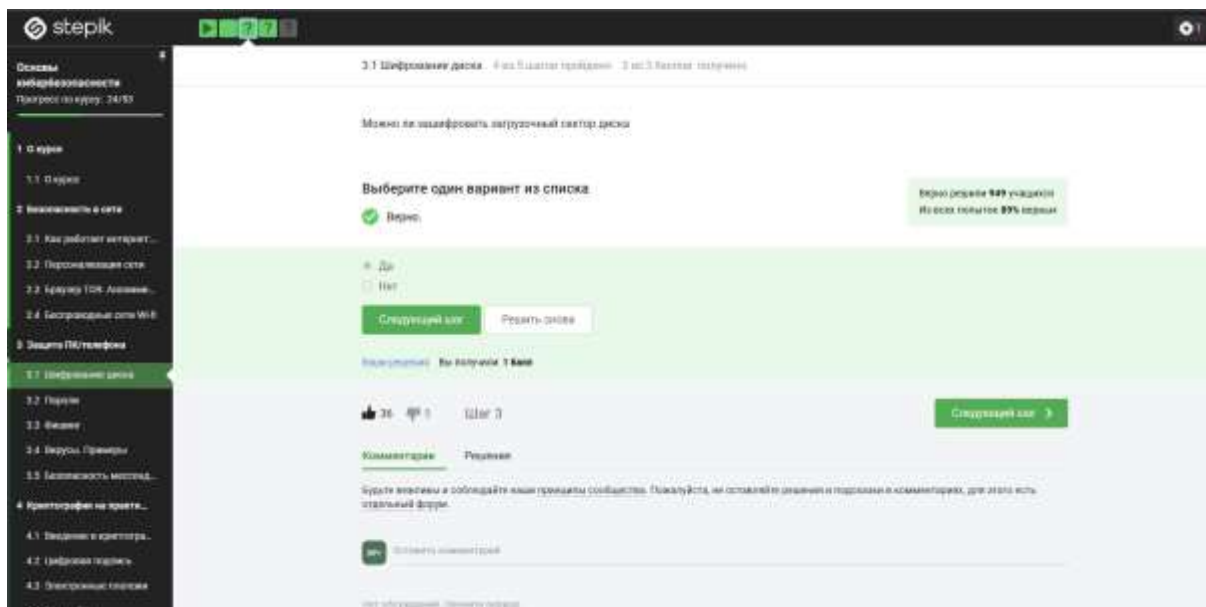
2 часть. Защита ПК/телефона

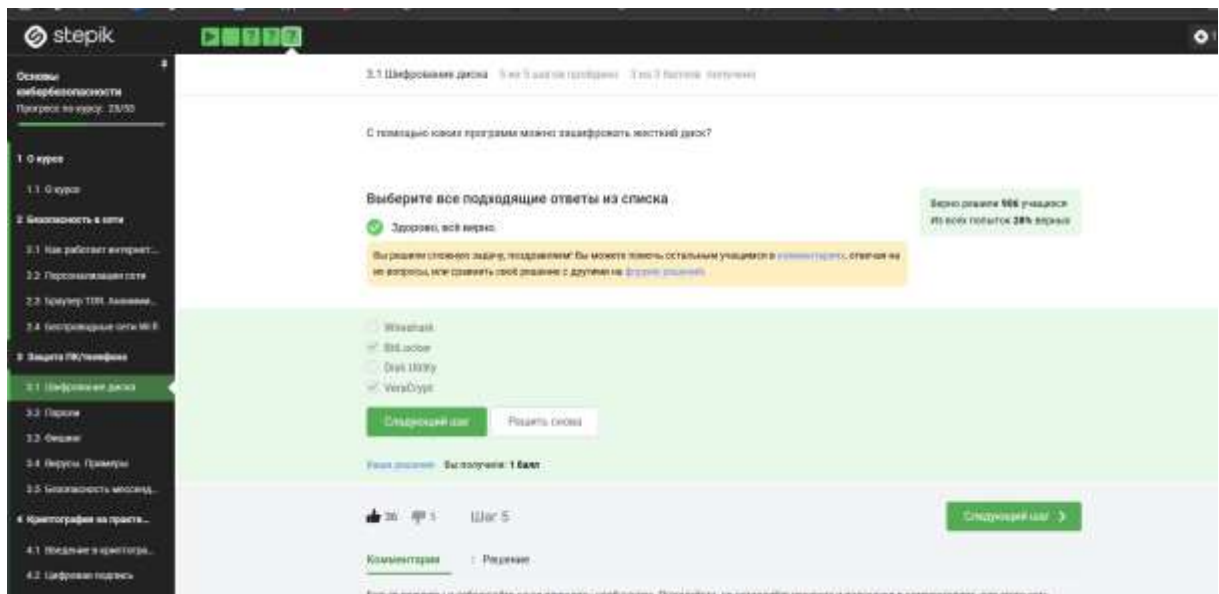
Шифрование диска

В этой лекции мы с вами поговорим о том, как шифруются носители информации и зачем это нужно. Зачем же шифровать жесткий диск, спросите вы. И ответ на этот вопрос довольно прост - шифровать жесткий диск нужно для того, чтобы избежать утечки наших персональных данных в случае утери или кражи нашего ноутбука. По статистике, это одна из основных причин утечки каких-то конфиденциальных данных типа наших паролей и каких-то документов, и шифрование жесткого диска позволяет избежать этих утечек. То есть, если злоумышленник получит физический доступ к вашему компьютеру или ноутбуку, не зная пароля, то есть не зная ключа шифрования, он не сможет получить доступ к вашим файлам. Вообще, эта политика шифрования жесткого диска часто является обязательной для таких серьезных компаний, как Яндекс, Google или в некоторых университетах. Сотрудники обязаны на своем корпоративном ноутбуке шифровать жесткий диск.

Рассмотрим, как это работает. Если не углубляться в детали, то шифрование жесткого диска происходит в три этапа. На самом первом этапе пользователь с помощью какой-то из утилит (про утилиты мы говорим позднее) генерирует ключ для шифрования.

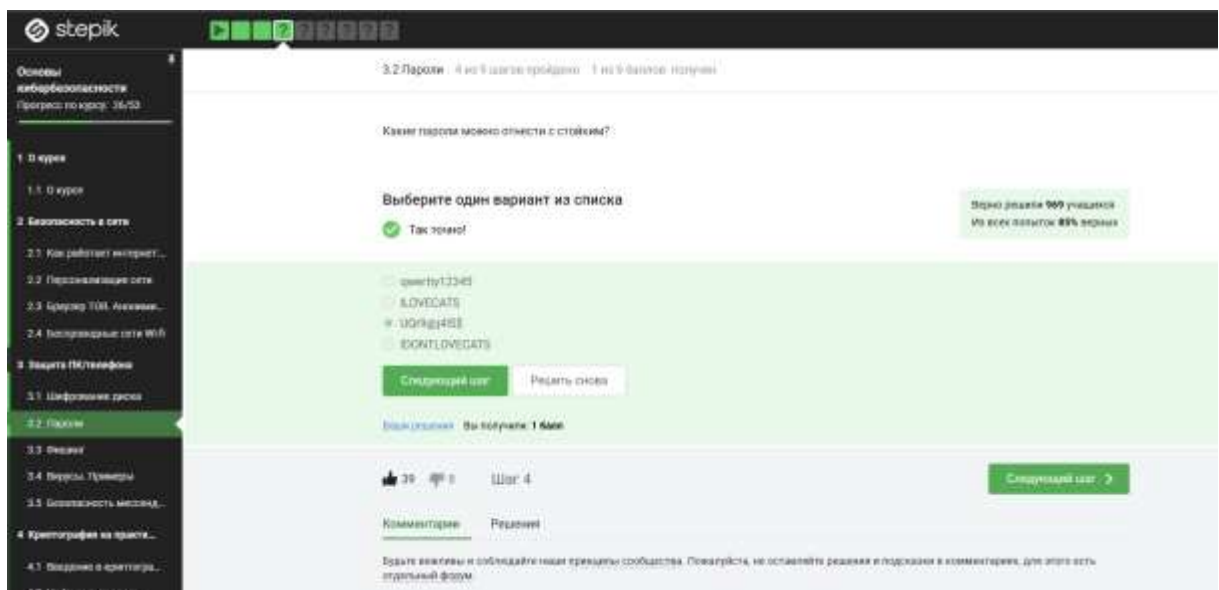
Прохождение тестовой части:





Пароли

Прохождение тестовой части:



stepik

Основы информационной безопасности

Прогресс по курсу: 26/100

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Передача данных по сети

2.3 Создание ТОК: Асимметри...

2.4 Безопасность сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование дисков

3.2 Пароли

3.3 Фейки

3.4 Верус: Превью

3.5 Безопасность мессендж...

4 Криптография на практике...

4.1 Проверка и критика

3.2 Пароли

5 из 9 вопросов пройдено

Тема 6.100% пройдено

Знаком ли вам кэтч?

Выберите один вариант из списка

✓ Все правильно

Верно ответили 974 учащихся

Из всех попыток 77% верные

Для защиты от оптимизированных атак, направленных на получение несанкционированного доступа

Для запоминат паролей

Для защиты кукл пользователей

Для безопасного хранения паролей на сервере

Следующий шаг

Решить снова

Правильно

Вы получили 3 балла

👍 99

👎 5

Шаг 6

Следующий шаг

Комментарии

Решение

Будьте внимательны и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте отзывы и подражки в комментариях, для этого есть

stepik

Основы кибербезопасности
Прогресс по курсу: 26/33

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимиз...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейкинг

3.4 Виртуал. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике...

4.1 Введение в криптографию...

3.2 Пароли 7 из 9 шагов пройдено 4 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Все получилось!

Верно решили 975 учащихся
Из всех попыток 61% верных

☐ Для того, чтобы пароли не передавались 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

👍 39 🗳 8 Шаг 7

Следующий шаг

Комментарии Решения

Будьте внимательны и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решения и подвохи в комментариях, для этого есть специальный форум

stepik

Основы кибербезопасности
Прогресс по курсу: 30/33

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимиз...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейкинг

3.4 Виртуал. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике...

4.1 Введение в криптографию...

3.2 Пароли 8 из 9 шагов пройдено 5 из 6 баллов получено

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

Выберите один вариант из списка

✓ Хорошая новость, верно!

Верно решили 967 учащихся
Из всех попыток 66% верных

☒ Нет

☐ Да

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 34 🗳 8 Шаг 8

Следующий шаг

Комментарии Решения

Будьте внимательны и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте решения и подвохи в комментариях, для этого есть специальный форум

stepik

Основы кибербезопасности
Прогресс по курсу: 31/33

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимиз...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейкинг

3.4 Виртуал. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике...

4.1 Введение в криптографию...

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

Какие меры защищают от утечки данных атакой перебором?

Выберите все подходящие ответы из списка

✓ Правильно, молодцы!

Верно решили 895 учащихся
Из всех попыток 38% верных

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на вопросы, или сравнить свой ответ с другими на форуме решений.

☒ разные пароли на всех сайтах

☒ периодическая смена паролей

☒ словенно(-длинные) пароли

☒ мемы

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 39 🗳 8 Шаг 9

Следующий шаг

Комментарии Решения

2 Самые популярные

Фишинг

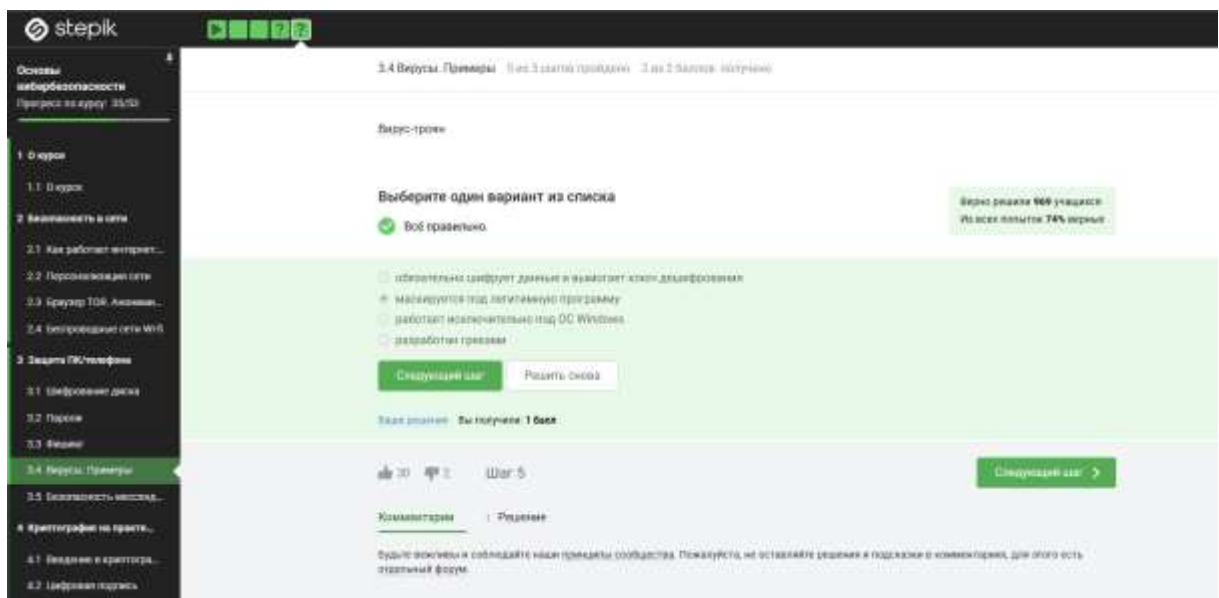
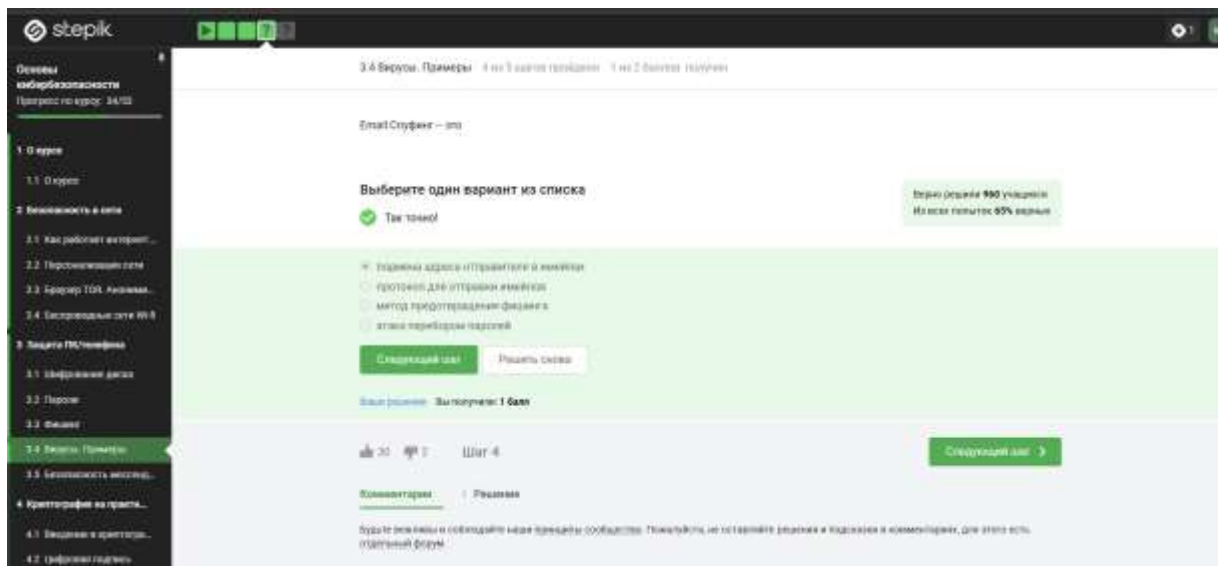
Прохождение тестовой части:

The screenshot shows the StepiK course interface for the 'Основы кибербезопасности' (Basics of Cybersecurity) course. The progress bar indicates 82/89. The left sidebar lists the course structure, with '3.3 Фишинг' (Phishing) selected. The main content area displays a test question: '3.3 Фишинг: 4 из 5 шагов пройдено, 1 из 2 баллов получено'. The question is 'Какие из следующих ссылок являются фишинговыми?' (Which of the following links are phishing links?). The instruction is 'Выберите все подходящие ответы из списка' (Select all suitable answers from the list). The options are: 'Хорошие новости, верю!' (Good news, I believe!), 'https://accounts.google.com/SignInFlow/SignIn?hl=ru' (Google login page), 'https://online.sberbank.ru/CSAFront/index.do' (Sberbank Online login page), 'https://mail.ru/login?lang=ru_RU' (Mail.ru login page), and 'https://passport.yandex.ru/auth/login?name_devokop.ru' (Yandex login page). The correct answers are the Google, Sberbank, and Mail.ru links. The user has selected 'Хорошие новости, верю!' and 'https://accounts.google.com/SignInFlow/SignIn?hl=ru'. The feedback shows 'Ваш ответ: Вы получили: 1 балл' (Your answer: You received: 1 point). The next step is 'Следующий шаг' (Next step).

The screenshot shows the StepiK course interface for the 'Основы кибербезопасности' (Basics of Cybersecurity) course. The progress bar indicates 83/89. The left sidebar lists the course structure, with '3.3 Фишинг' (Phishing) selected. The main content area displays a test question: '3.3 Фишинг: 5 из 5 шагов пройдено, 2 из 2 баллов получено'. The question is 'Может ли фишинговый email прийти от знакомого адреса?' (Can a phishing email come from a familiar address?). The instruction is 'Выберите один вариант из списка' (Select one option from the list). The options are 'Верно' (Correct) and 'Нет' (No). The user has selected 'Верно'. The feedback shows 'Ваш ответ: Вы получили: 1 балл' (Your answer: You received: 1 point). The next step is 'Следующий шаг' (Next step).

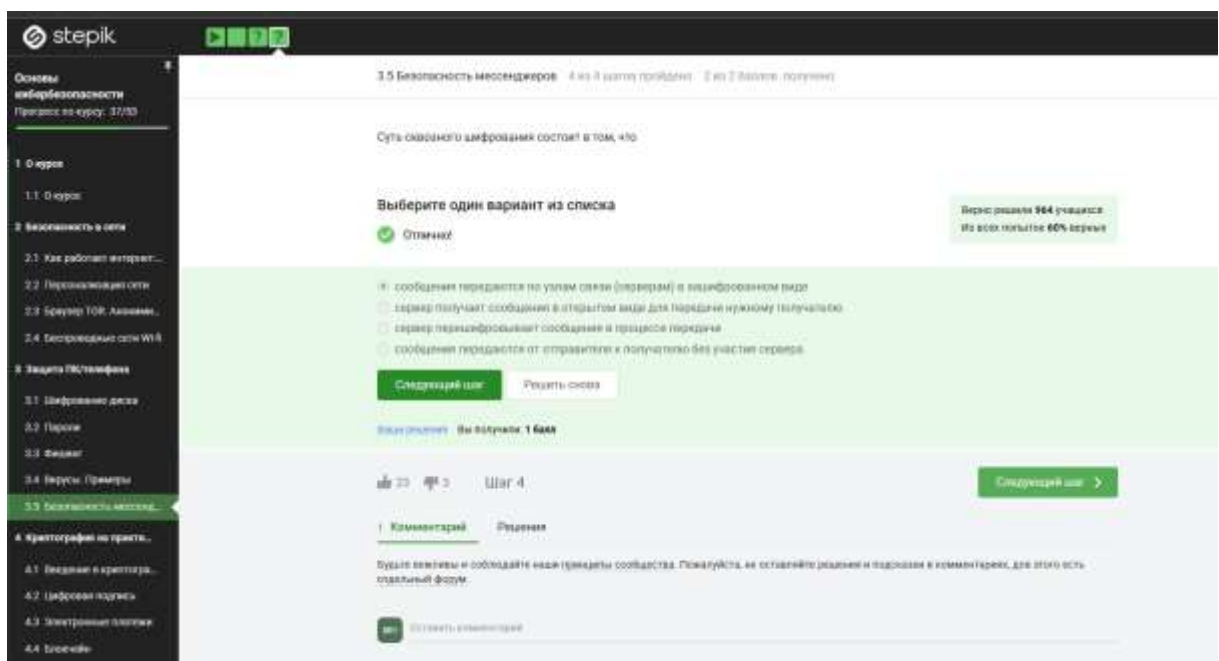
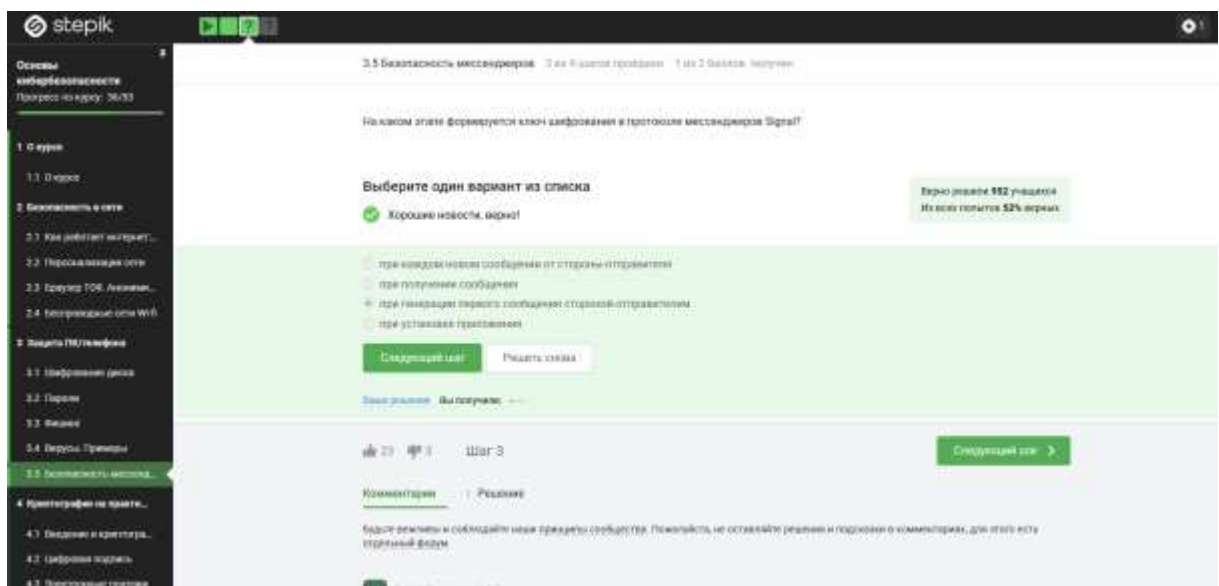
Вирусы. Примеры

Прохождение тестовой части:



Безопасность мессенджеров

Прохождение тестовой части:



3 часть. Криптография на практике

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. Моя сегодняшняя цель – это научить вас отличать основные криптографические протоколы, их еще называют примитивами, а именно – симметричное

шифрование, аутентификацию, цифровую подпись и хэширование.

Для того, чтобы мы с вами говорили на одном языке и чтобы вы не плавали в этих понятиях, имеет смысл структурировать их и определить, зачем они нужны и какую функцию они несут. Эти разные протоколы – подпись, симметричное шифрование, аутентификация – играют разную роль, и поэтому они также по-разному строятся. Как они строятся, мы рассказывать в этом курсе не будем, это довольно сложные математические объекты, и аппарат, который нужно знать, чтобы понимать, как она устроена, очень сложный. Но зачем эти примитивы сделаны и какую цель они преследуют, мы сегодня с вами разберём.

Выполнение тестовой части:

The image displays two screenshots of the Stepik learning management system interface, specifically showing quiz questions related to cryptography.

Top Screenshot:

- Header:** stepik logo, progress bar (4.1 Введение в криптографию, 5 из 7 шагов пройдено, 5 из 5 баллов получено).
- Left Sidebar:** Меню курса (0 курс, 1.1 0 курс, 2 Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Другой ТОН, Аноним..., 2.4 Безопасность сети Wi-Fi, 3 Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Вирусы, 3.4 Вредные программы, 3.5 Безопасность мессендж...).
- Main Content:** 4.1 Введение в криптографию. 5 из 7 шагов пройдено. 5 из 5 баллов получено. В асимметричные криптографические примитивы. Выберите один вариант из списка. ☒ Абсолютно ложно. ☐ обе стороны имеют пару ключей. ☐ обе стороны имеют общий секретный ключ. ☐ 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. . Вы ответили правильно. Вы получили 1 балл.
- Bottom:** 30 лайков, 4 комментария, Шаг 3, , Комментарий, Решение.

Bottom Screenshot:

- Header:** stepik logo, progress bar (4.1 Введение в криптографию, 6 из 7 шагов пройдено, 6 из 7 баллов получено).
- Left Sidebar:** Меню курса (0 курс, 1.1 0 курс, 2 Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Другой ТОН, Аноним..., 2.4 Безопасность сети Wi-Fi, 3 Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Вирусы, 3.4 Вредные программы, 3.5 Безопасность мессендж..., 4 Криптография на практике, 4.1 Введение в криптографию, 4.2 Асимметричные криптографические примитивы).
- Main Content:** 4.1 Введение в криптографию. 6 из 7 шагов пройдено. 6 из 7 баллов получено. Криптографическая хэш-функция. Выберите все подходящие ответы из списка. ☒ Верно. Так должно быть. ☐ эффективно реализуется. ☐ обеспечивает конфиденциальность зашифрованных данных. ☒ дает на выходе фиксированное число бит независимо от объема входных данных. ☒ устойчив к коллизиям. . Вы ответили правильно. Вы получили 1 балл.
- Bottom:** 30 лайков, 4 комментария, Шаг 4, , Комментарий, Решение.

stepik

Основы кибербезопасности
Прогресс по курсу: 40/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Брандмауэр TCP. Атаки...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Веруны. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике

4.1 Введение в криптографию

4.2 Цифровая подпись

4.1 Введение в криптографию 5 из 7 этапов пройдено 3 из 5 баллов получено

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Хорошая работа

Вы решили сложный задачу, поздравляем! Вы являетесь очень острым умом! В комментариях, ставьте на этот вопрос, или сравните свой рейтинг с другими на форуме решений.

Верно решено 824 учащихся
Из всех попыток 19% верных

☐ AES

☐ SHA2

☒ RSA

☒ ECDSA

☒ ГОСТ Р 34.10-2012

Следующий шаг

Решить снова

Наш рейтинг: Вы получили 1 балл

30 4 5 Шаг 5

Следующий шаг

Комментарии

Решения

Самый популярный

stepik

Основы кибербезопасности
Прогресс по курсу: 41/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Брандмауэр TCP. Атаки...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Веруны. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике

4.1 Введение в криптографию

4.2 Цифровая подпись

4.1 Введение в криптографию 6 из 7 этапов пройдено 4 из 5 баллов получено

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решено 935 учащихся
Из всех попыток 89% верных

☐ асимметричным примитивом

☒ симметричным примитивом

Следующий шаг

Решить снова

Наш рейтинг: Вы получили 1 балл

30 4 6 Шаг 6

Следующий шаг

Комментарии

Решения

stepik

Основы кибербезопасности
Прогресс по курсу: 42/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Брандмауэр TCP. Атаки...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Веруны. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике

4.1 Введение в криптографию

4.2 Цифровая подпись

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

Обмен ключом Диффи-Хеллмана - это

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решено 948 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

Наш рейтинг: Вы получили 1 балл

30 4 7 Шаг 7

Следующий шаг

1 Комментарий

Решения

Будьте основаны и соблюдайте наши пределы сообщества. Пожалуйста, не оставляйте решений и поджигов в комментариях, для этого есть специальный форум

Цифровая подпись

Прохождение тестовой части:

stepik

Основы кибербезопасности
Прогресс по курсу: 40/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR, Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Вредны. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Подписанные сообщения

4.2 Цифровая подпись: 4 из 5 шагов пройдено, 1 из 5 баллов получено

Процесс электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Так точно!

☐ процессом с симметричным ключом

☐ процессом с публичным (или открытым) ключом

Следующий шаг

Решить снова

Вы получили: 4 балла

75 4 3 Шаг 4

Следующий шаг

Комментарии

Рецензия

Будьте вежливы и соблюдайте наши традиции сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум

stepik

Основы кибербезопасности
Прогресс по курсу: 44/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR, Аноним...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейки

3.4 Пароли. Примеры

3.5 Безопасность мессенд...

4 Криптография на практике...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Подписанные сообщения

4.2 Цифровая подпись: 5 из 5 шагов пройдено, 2 из 5 баллов получено

Алгоритм верификации электронной цифровой подписи требует из вход

Выберите один вариант из списка

☒ Абсолютно точно

☐ подпись, секретный ключ, сообщение

☐ подпись, открытый ключ, сообщение

☐ подпись, секретный ключ

☐ подпись, открытый ключ

Следующий шаг

Решить снова

Вы получили: 1 балл

25 4 3 Шаг 5

Следующий шаг

Комментарии

Рецензия

Будьте вежливы и соблюдайте наши традиции сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум

stepik

1

2

3

4

5

6

7

8

Основы кибербезопасности

Прогресс по курсу: 45/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимизация...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейкит

3.4 Верусы. Промиды

3.5 Безопасность мессенджеров

4 Криптография на практике...

4.1 Введение в криптографию...

4.2 Цифровая подпись

6 из 8 шагов пройдено

3 из 5 баллов получено

Электронная цифровая подпись не обеспечивает:

Выберите один вариант из списка

Хорошие новости, верно!

Верно решили 988 учащихся

Из всех попыток 93% верных

целостность

☒ конфиденциальность

искл. от авторства

аутентификация

Следующий шаг

Решить снова

Ваше решение

Вы получили 1 балл

25

5

Шаг 6

Следующий шаг

Комментарии

Решения

Пожалуйста, соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.

stepik

1

2

3

4

5

6

7

8

Основы кибербезопасности

Прогресс по курсу: 46/50

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Браузер TOR. Анонимизация...

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фейкит

3.4 Верусы. Промиды

3.5 Безопасность мессенджеров

4 Криптография на практике...

4.1 Введение в криптографию...

4.2 Цифровая подпись

4.2 Цифровая подпись

7 из 8 шагов пройдено

4 из 5 баллов получено

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

Выберите один вариант из списка

Отличное решение!

Верно решили 979 учащихся

Из всех попыток 88% верных

усиленный неквалифицированный

простой

☒ усиленный квалифицированный

Следующий шаг

Решить снова

Ваше решение

Вы получили 1 балл

25

3

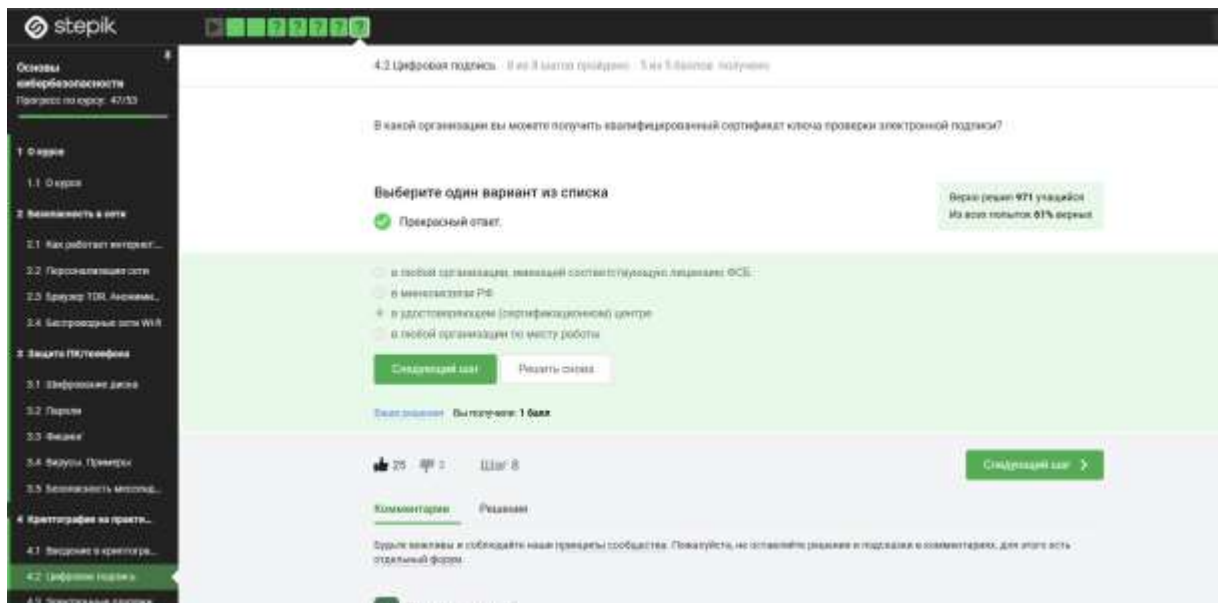
Шаг 7

Следующий шаг

Комментарии

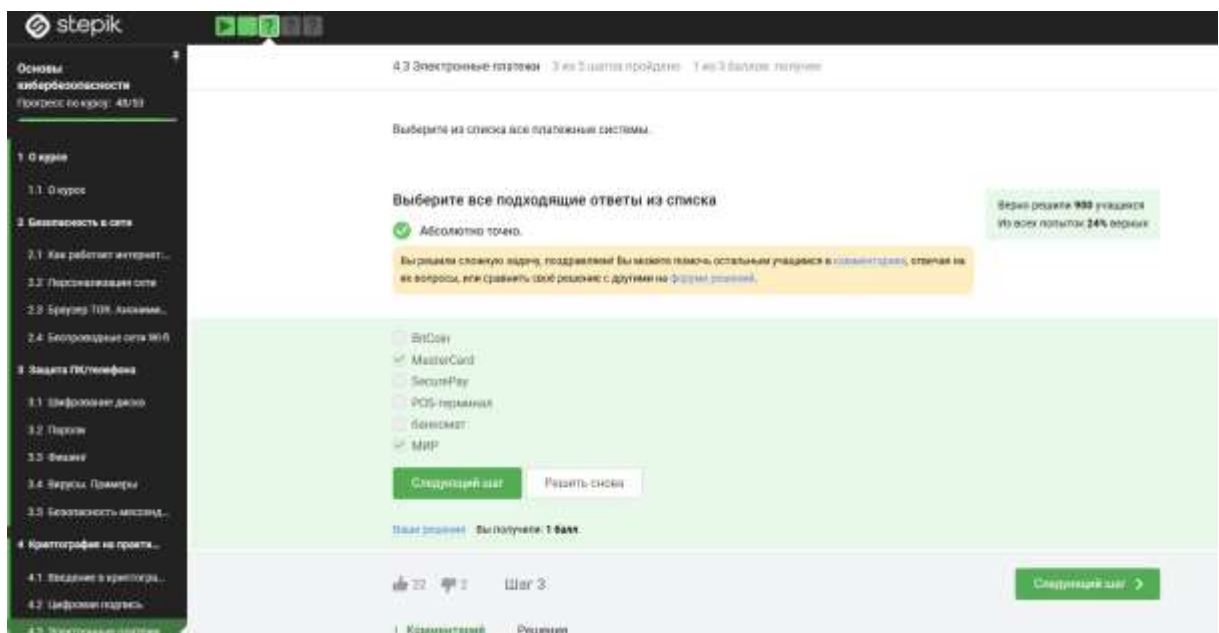
Решения

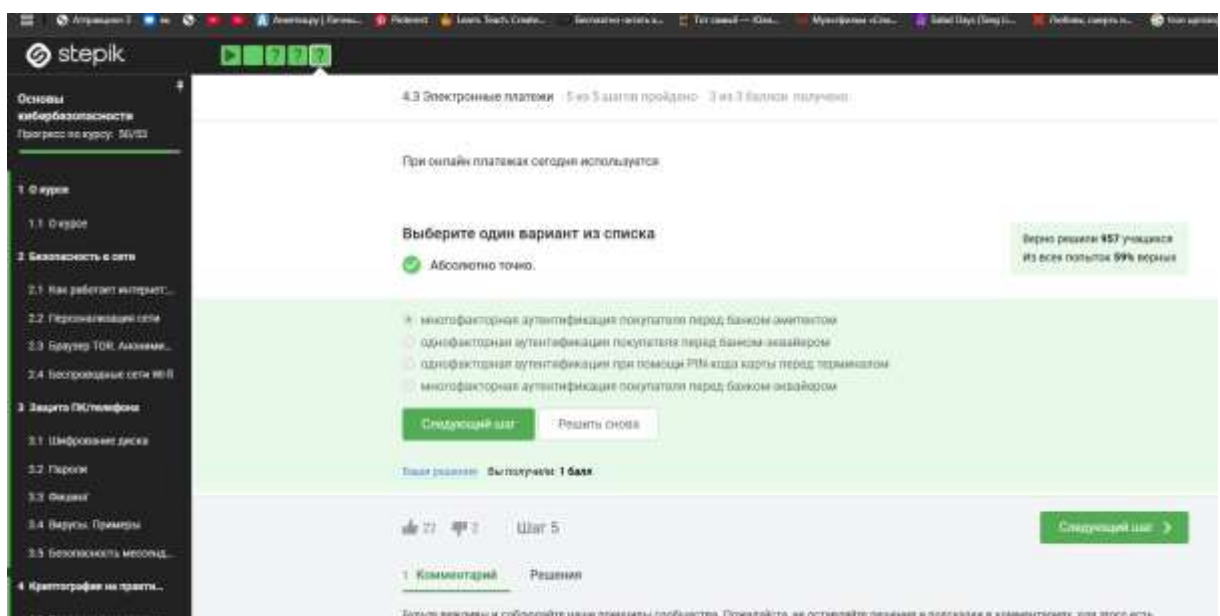
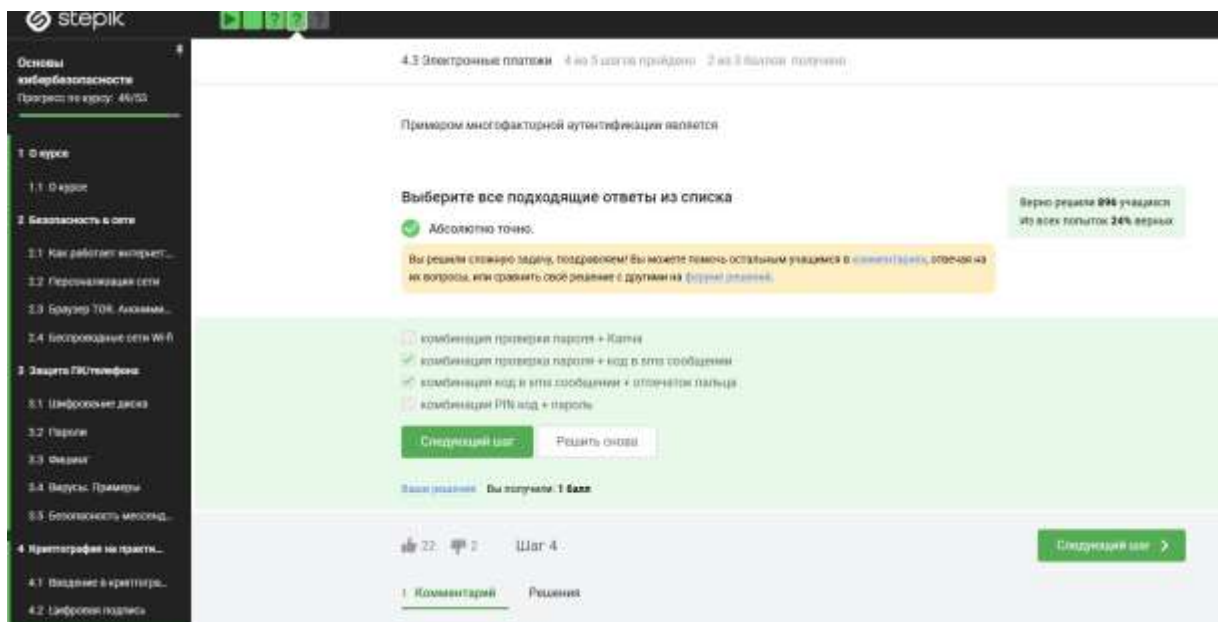
Пожалуйста, соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.



Электронные платежи

Прохождение тестовой части:





Блокчейн

Прохождение тестовой части:

stepik

4.4 Блокчейн

4 из 6 частей пройдено

1 из 2 баллов: получено

Основы кибербезопасности

Прогресс по курсу: 51/53

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Протокол TCP. Адаптив...

2.4 Беспроводные сети Wi-Fi

3 Защита IT-инфраструктуры

3.1 Шифрование данных

3.2 Пароли

3.3 Фейкит

3.4 Версии. Примеры

3.5 Безопасность мессенджеров

4 Криптография на практике

4.1 Введение в криптографию...

Каково свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓

Пребранный ответ

✗

фиксированной длины выходных данных

✗

сложность нахождения преобразования

✗

универсальная целостности

✗

эффективность дешифрования

Следующий шаг

Решить снова

Ваши решения

Вы получили: 1 балл

👍 31

👎 3

Шаг 4

Следующий шаг

1 Комментарий

Решения

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте отзывы и поддержки в комментариях, для этого есть отдельный форум.

stepik

4.4 Блокчейн

5 из 6 частей пройдено

2 из 2 баллов: получено

Основы кибербезопасности

Прогресс по курсу: 52/53

1 0 курс

1.1 0 курс

2 Безопасность в сети

2.1 Как работает интернет...

2.2 Персонализация сети

2.3 Протокол TCP. Адаптив...

2.4 Беспроводные сети Wi-Fi

3 Защита IT-инфраструктуры

3.1 Шифрование данных

3.2 Пароли

3.3 Фейкит

3.4 Версии. Примеры

3.5 Безопасность мессенджеров

4 Криптография на практике

4.1 Введение в криптографию...

4.2 Шифрование данных

4.3 Электронные подписи

Консенсус в некоторых системах блокчейн обладает свойством

Выберите все подходящие ответы из списка

✓

Хорошие новости, верно!

✗

Вы решили слишком быстро, поздравляем! Вы можете помочь остальным учащимся в комментариях, ответив на их вопросы, или сравнить свой решение с другими на [Форум решений](#).

✓

постоянства

✓

актуальность

✓

открытость

✓

консенсус

Следующий шаг

Решить снова

Ваши решения

Вы получили: 1 балл

👍 31

👎 3

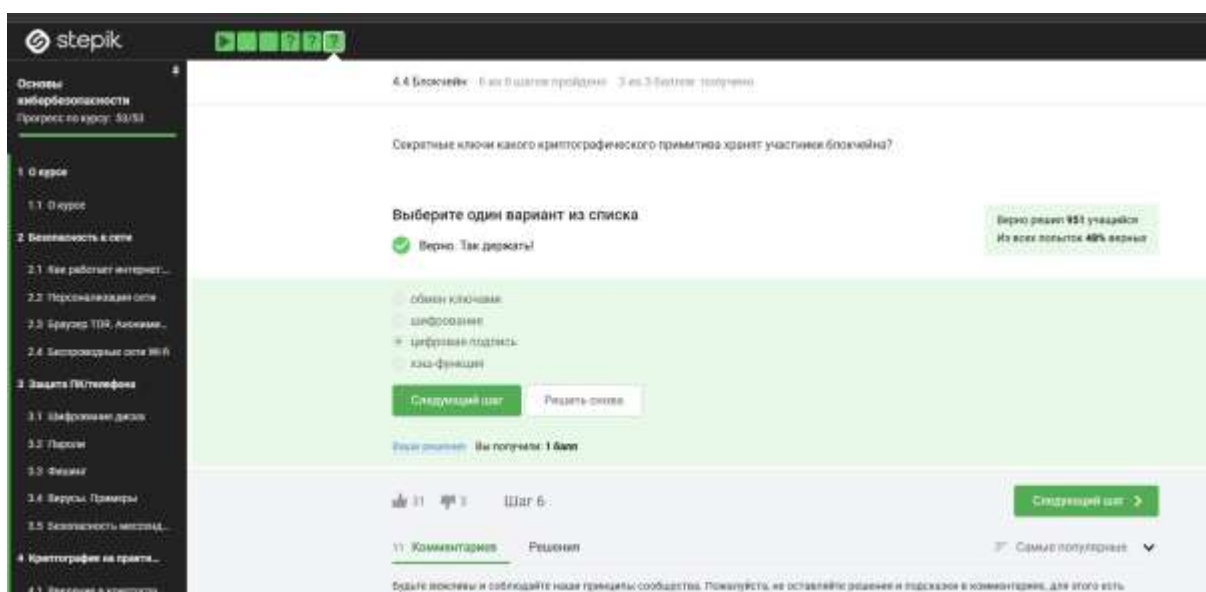
Шаг 5

Следующий шаг

1 Комментарий

Решения

Будьте вежливы и соблюдайте наши правила сообщества. Пожалуйста, не оставляйте отзывы и поддержки в комментариях, для этого есть отдельный форум.



4. Выводы.

Прохождение курса позволило достичь поставленных учебных целей и существенно углубить понимание ключевых аспектов информационной безопасности и технологий интернета.

Понимание работы Интернета и выявление слабых мест. Изучены принципы функционирования глобальной сети, её структуры и архитектуры. Освоено понятие сетевых протоколов и осознаны потенциальные угрозы безопасности данных при передаче через Интернет. Особое внимание уделялось вопросам конфиденциальности и защиты персональных данных пользователей.

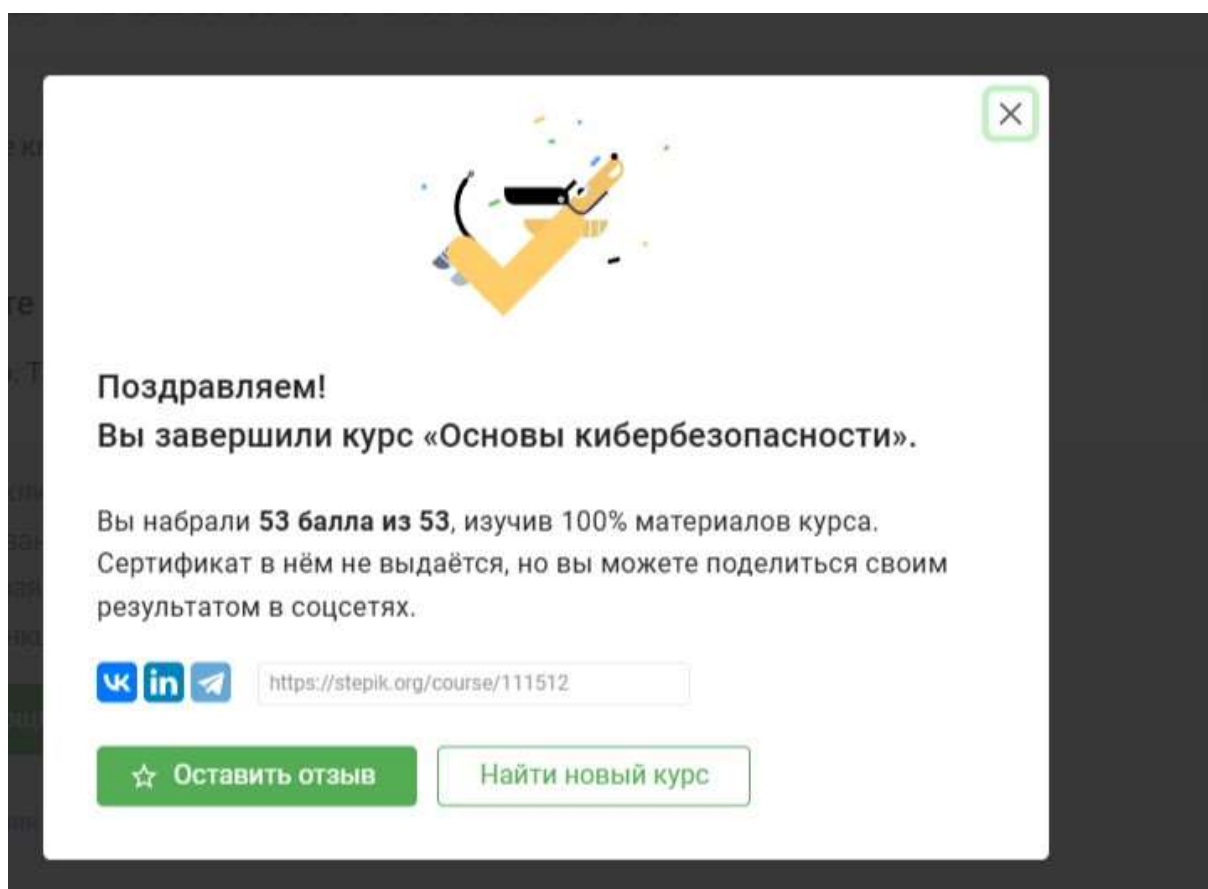
Осознание опасности простых паролей. Проанализированы риски использования очевидных комбинаций символов в качестве пароля. Рассмотрены механизмы взлома паролей методом подбора и продемонстрирована необходимость использования сложных, уникальных и надёжных паролей для предотвращения несанкционированного доступа к аккаунтам.

Различие между шифрованием и электронной подписью. Разобраны концепции криптографии, изучены различия между методами шифрования и электронными цифровыми подписями. Получены практические навыки определения защищённых коммуникаций и верификации цифровых

документов посредством ЭЦП.

Знание принципов электронных платежей. Изучение механизмов совершения онлайн-платежей, методов аутентификации и авторизации клиентов, используемых финансовых стандартов и правил обработки транзакций. Овладение основными инструментами анализа рисков мошенничества и обеспечением безопасной среды оплаты товаров и услуг.

Сертификат не выдаётся. Скрин о прохождении курса:



:::

{#refs} :::