Основы кибербезопасности

Этап 2

Ведьмина Александра Сергеевна

Содержание

# 1 Цель работы

Выполнить задания второй части курса по кибербезопасности.

# 2 Выполнение лабораторной работы

Конечно, можно. Шифрование переводит данные на диске в нераспознаваемый набор символов.

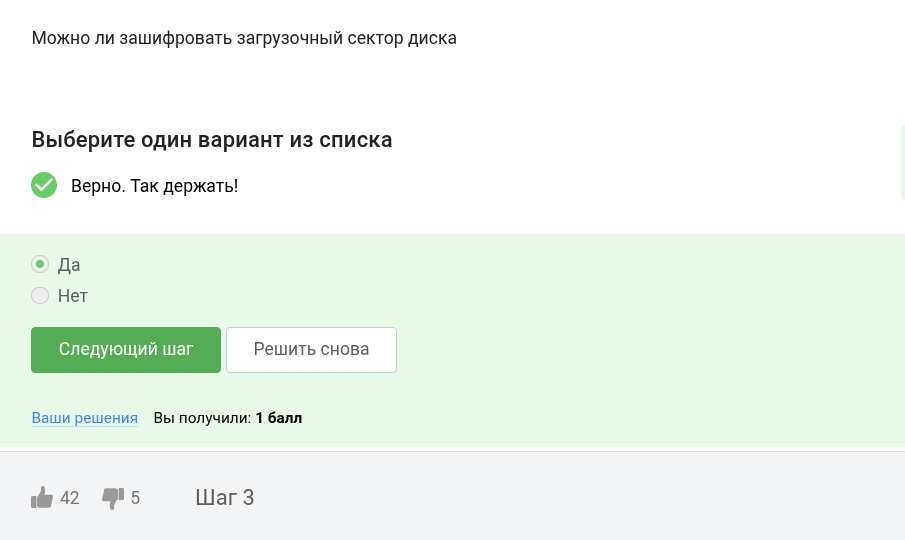


Рис. 1: Задание 1

Используется симметричное шифрование.

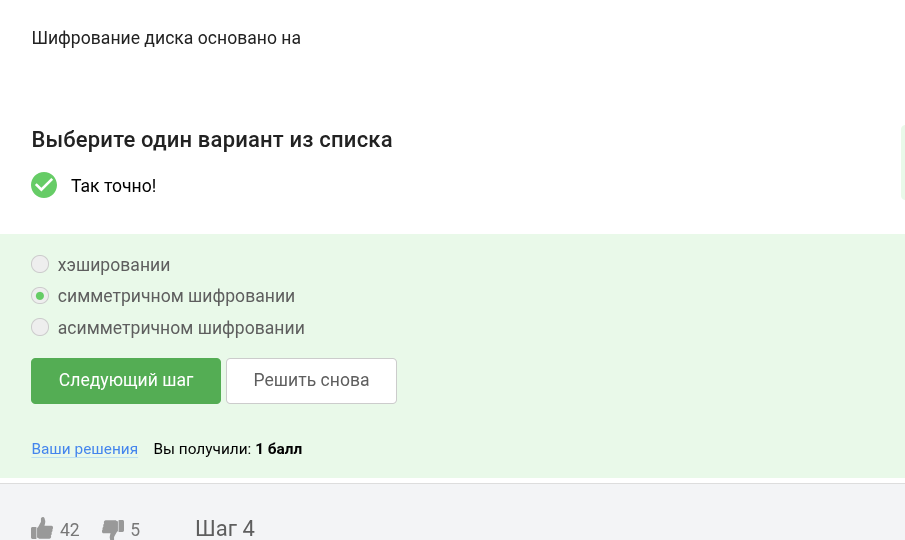


Рис. 2: Задание 2

Bitlocker, vercrypt, есть и много иных.

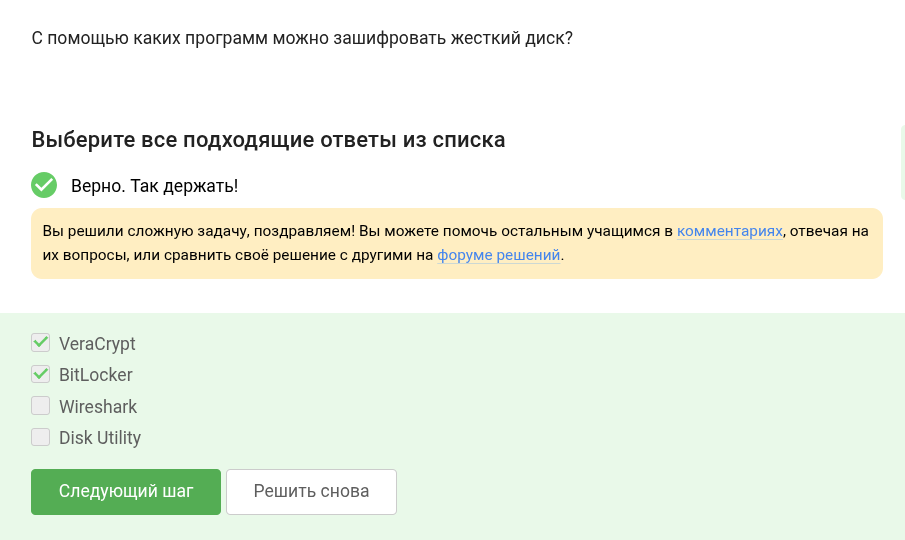


Рис. 3: Задание 3

Пароль должен состоять из разнородных символов и быть сложным для подбора.

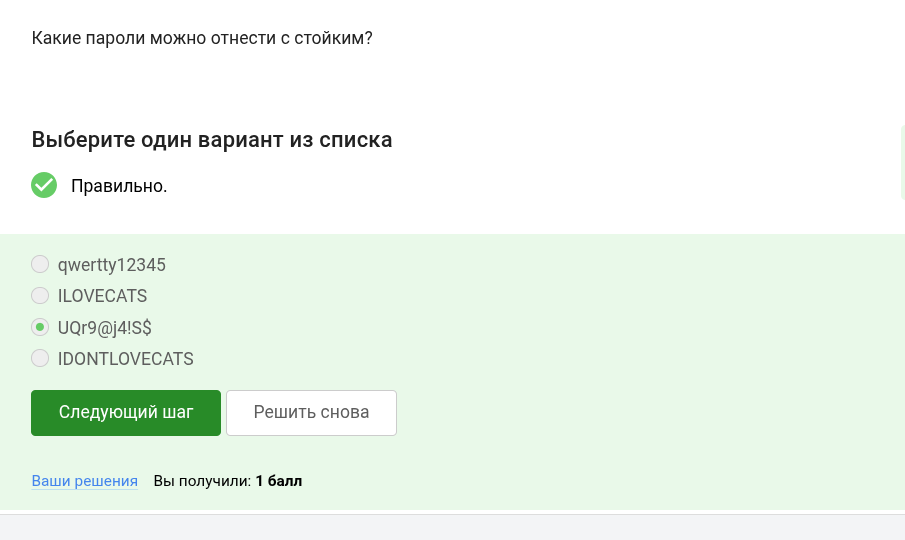


Рис. 4: Задание 4

В прочих перечисленных вариантах пароль легко украсть.

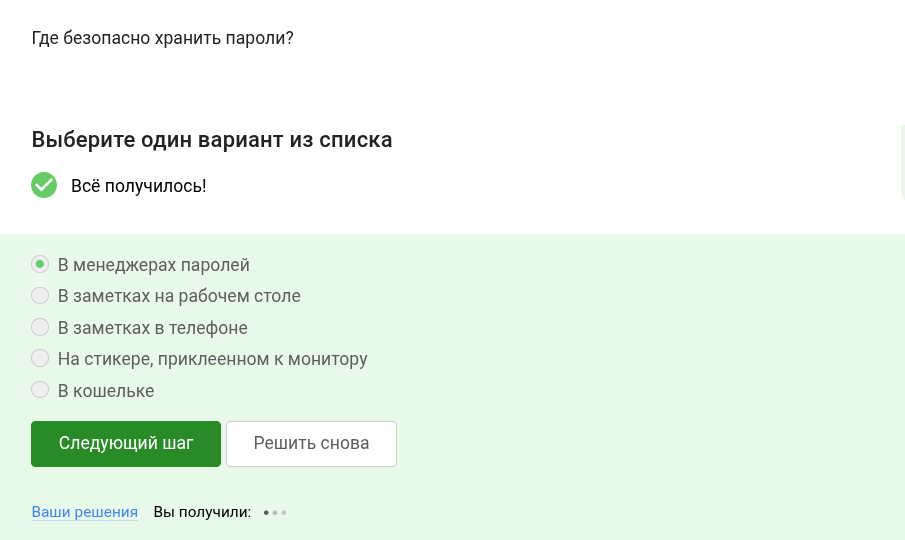


Рис. 5: Задание 5

Капча смотрит подозрительные действия и спрашивает, робот вы или нет.

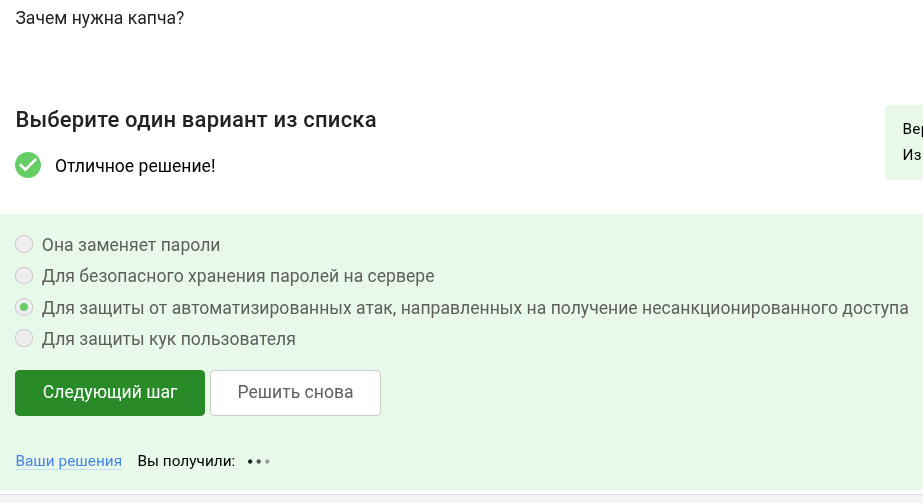


Рис. 6: Задание 6

Для их безопасности. хэш сложно взломать.

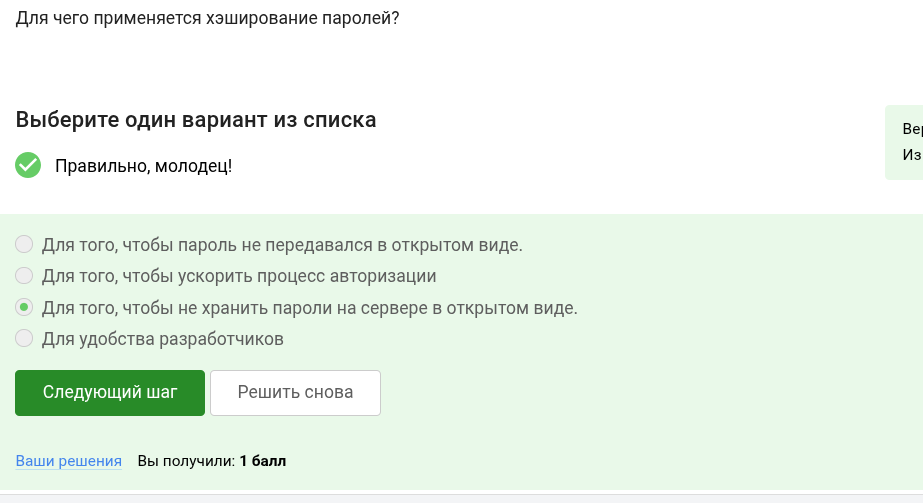


Рис. 7: Задание 7

Не поможет.

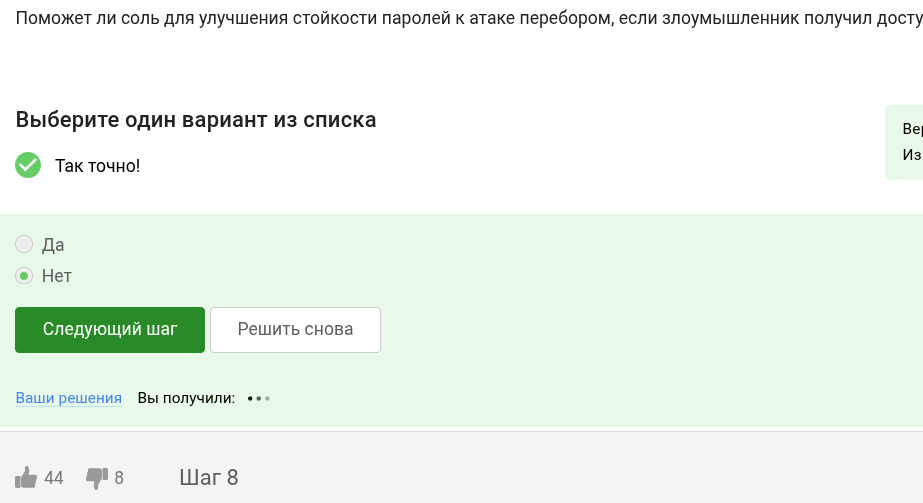


Рис. 8: Задание 8

Все перечисленные варианты весьма эфеективны.

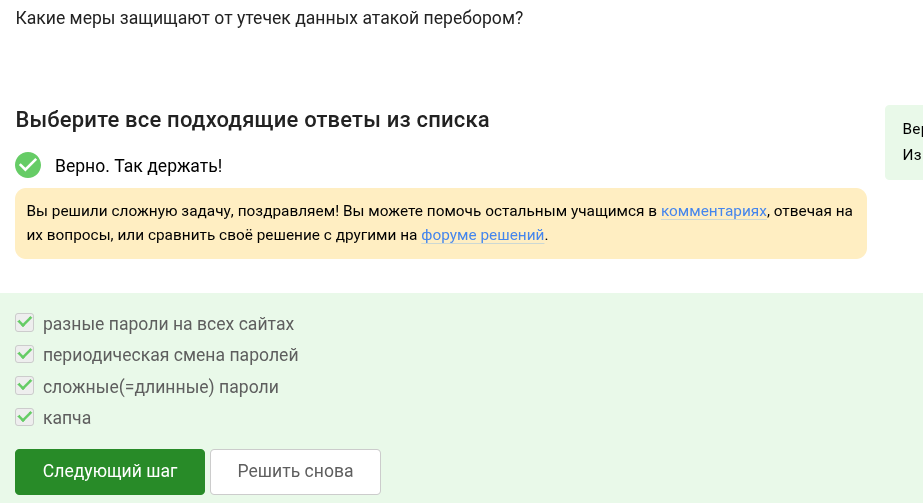


Рис. 9: Задание 9

Есть отличия от оригинальных ссылок у сбера и яндекса.

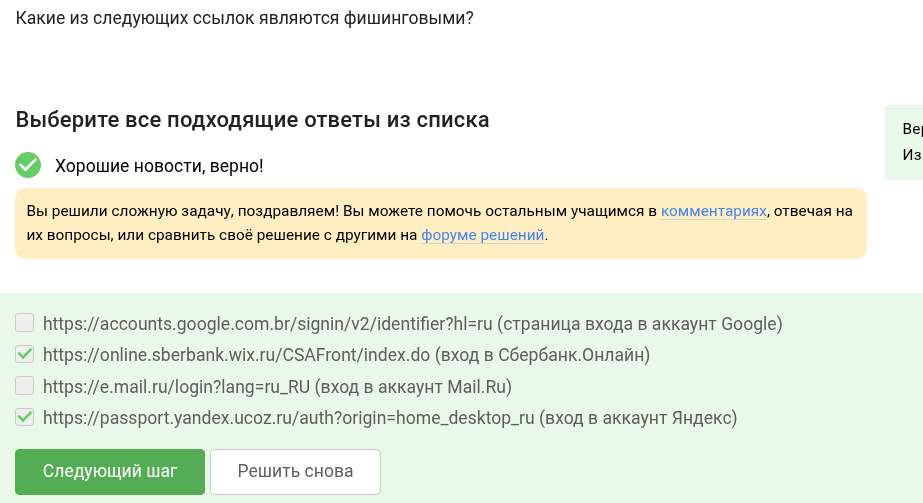


Рис. 10: Задание 10

Да, знакомый адрес могут взломать.

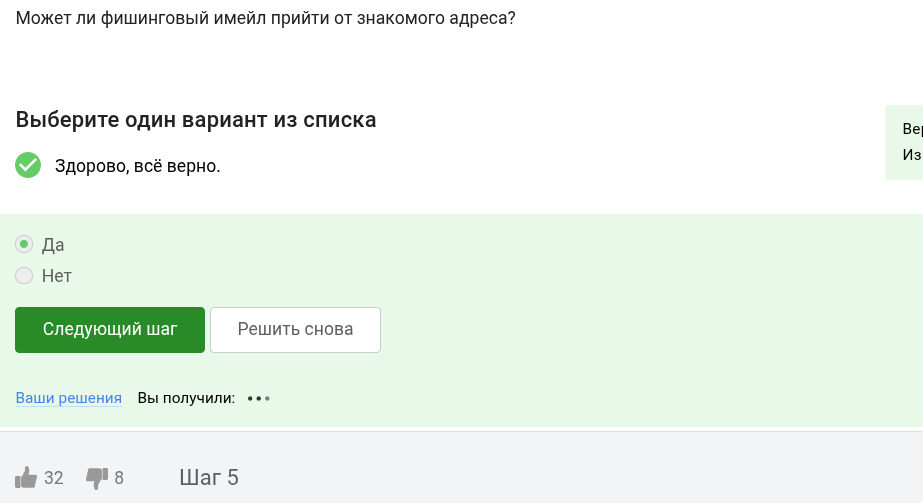


Рис. 11: Задание 11

От английского spoof — обман, подделка.

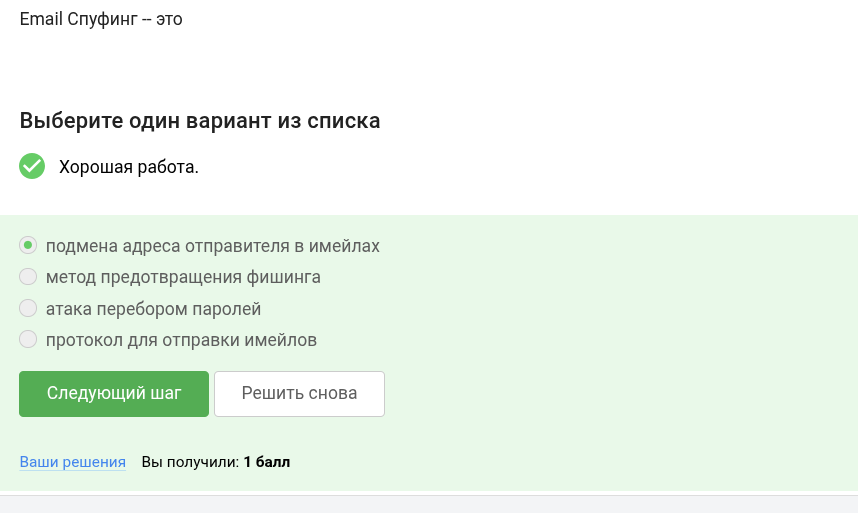


Рис. 12: Задание 12

На то он и троян, что маскируется и сразу не поймёшь, что это вирус.

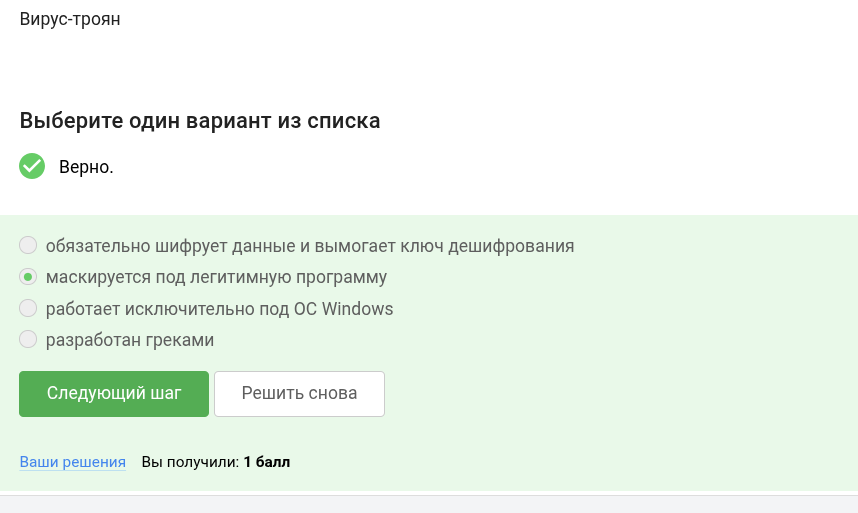


Рис. 13: Задание 13

Сразу же при первом сообщении.

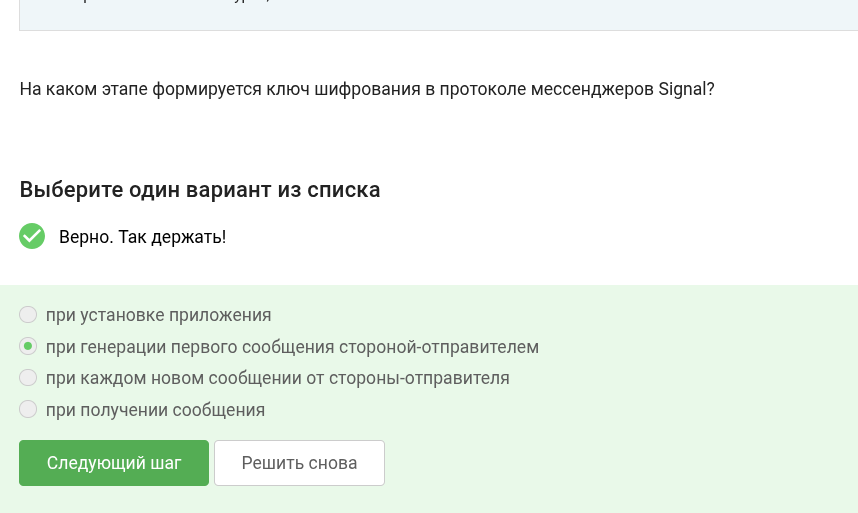


Рис. 14: Задание 14

Данные в зашифрованном виде передаются по узлам.

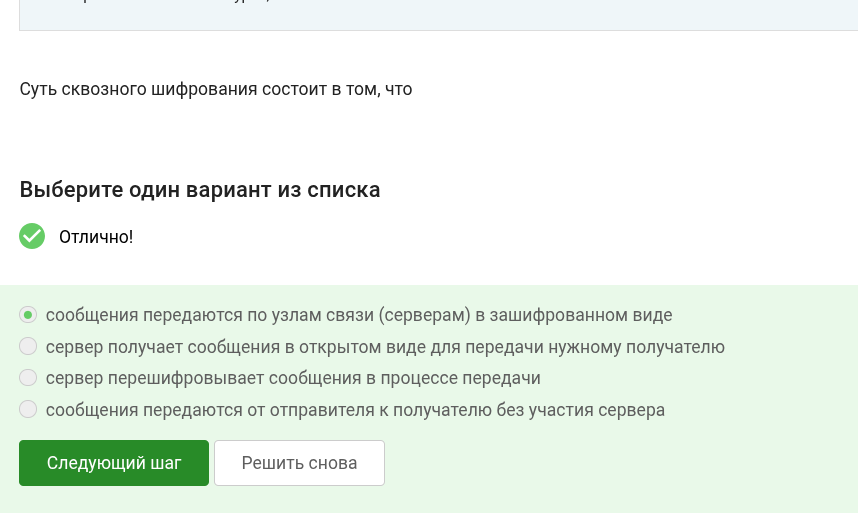


Рис. 15: Задание 15

# 3 Выводы

Все задания выполнены.