Отчет о прохождении внешнего курса

2 этап

Симонова Полина Игоревна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Пройти внешний курс «Основы кибербезопасности» на платформе Stepik. Получить начальные знания в сфере кибербезопасности.

2 Задание

Пройти все обучающие материалы, и на их основании выполнить задания и тесты.

3 Теоретическое введение

Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования.

Основной критерий стойкости пароля - это сложность его перебора. Самая основная атака на наши пароли - это банальный перебор всевозможных паролей, если мы знаем, что, например, пароль состоит из цифр и букв алфавита и каких-то еще символов, мы знаем в принципе весь алфавит, мощность этого алфавита, если мы еще, допустим, знаем длину пароля, то мы можем точно посчитать, каков размер множества всех паролей

4 Выполнение лабораторной работы

Шифрование диска переводит данные в нечитаемый код, поэтому загрузочный сектор вполне можно зашифровать. (рис. 1)

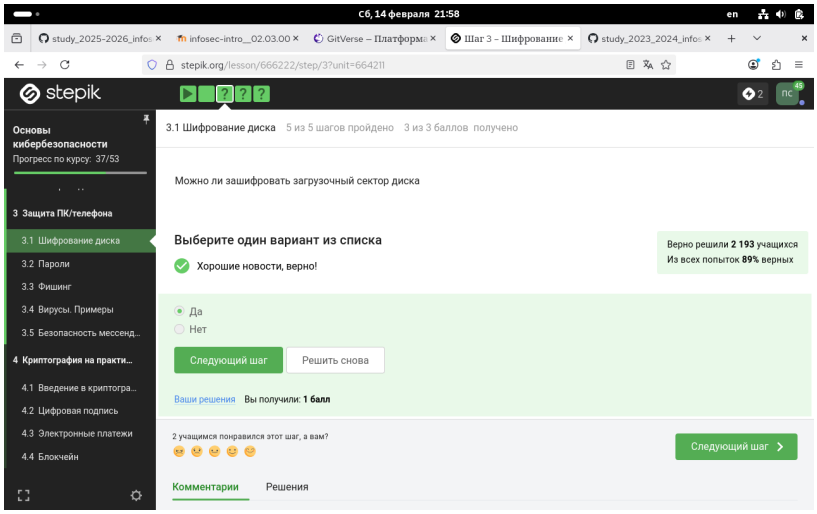

Рисунок 4.1: Задание 1

Шифрование диска основано на симмеричном шифрвании. (рис.2)

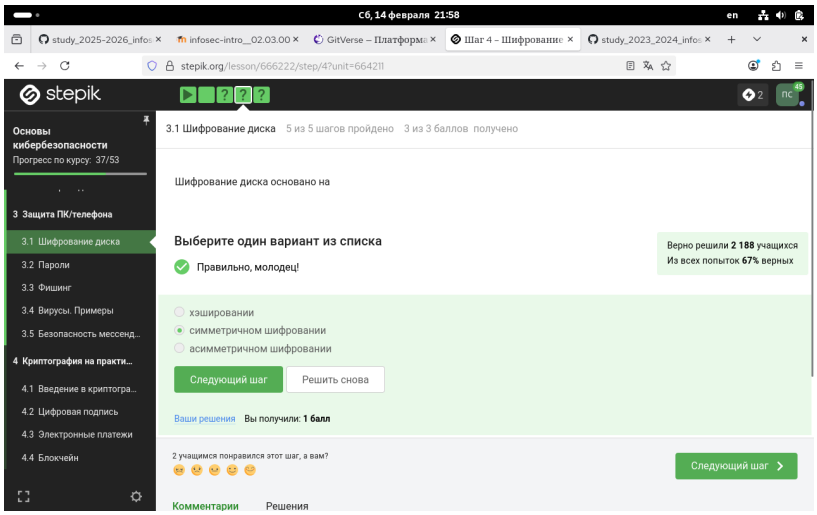

Рисунок 4.2: Задание 2

WireShark используется для анализа трафика, а Disk Utility - приложение для мониторинга памяти на макос. Соответственно, выделяем две оставшиеся программы.(рис.3)

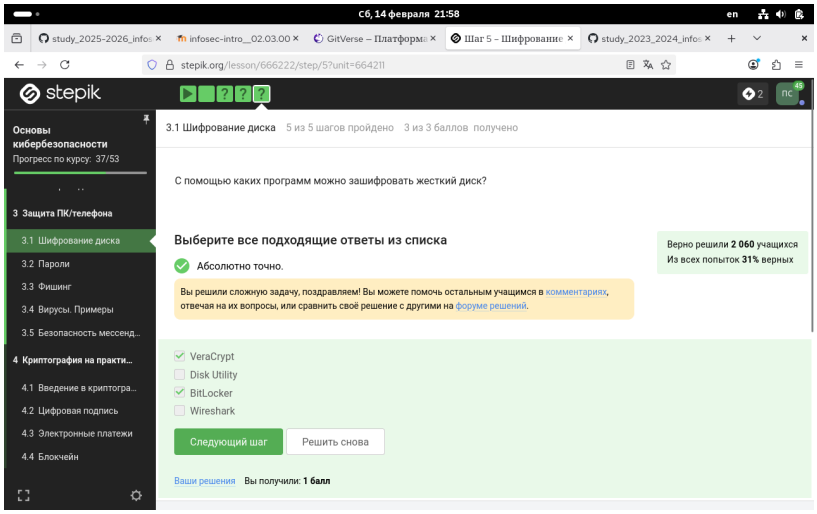

Рисунок 4.3: Задание 3

Стойкие пароли длинные, содержат заглавные и строчные символы, специальные символы и цифры. (рис.4)

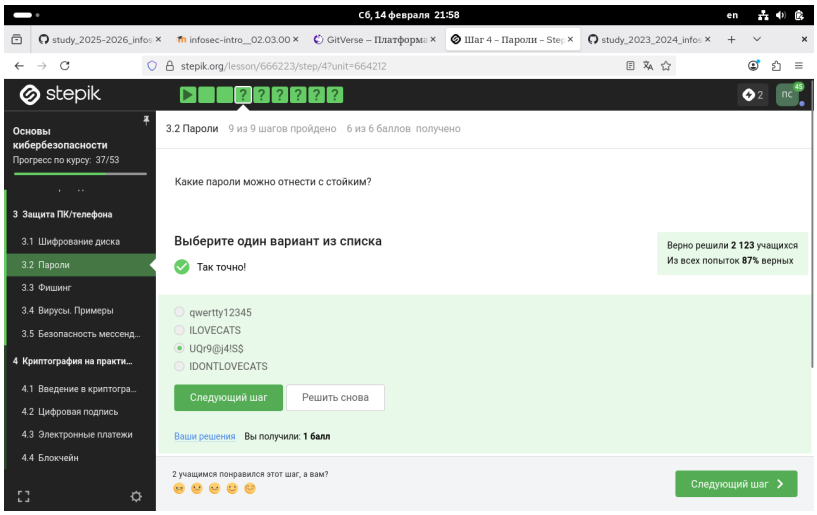

Рисунок 4.4: Задание 4

Все варианты ненавдежные, кроме менеджера паролей. (рис. 5)

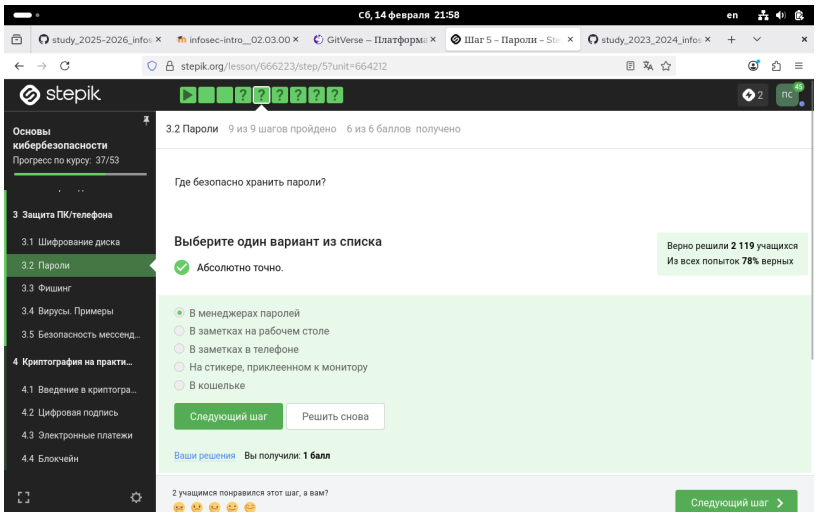

Рисунок 4.5: Задание 5

Капча проверяет, что действие выполняет человек. (рис.6)

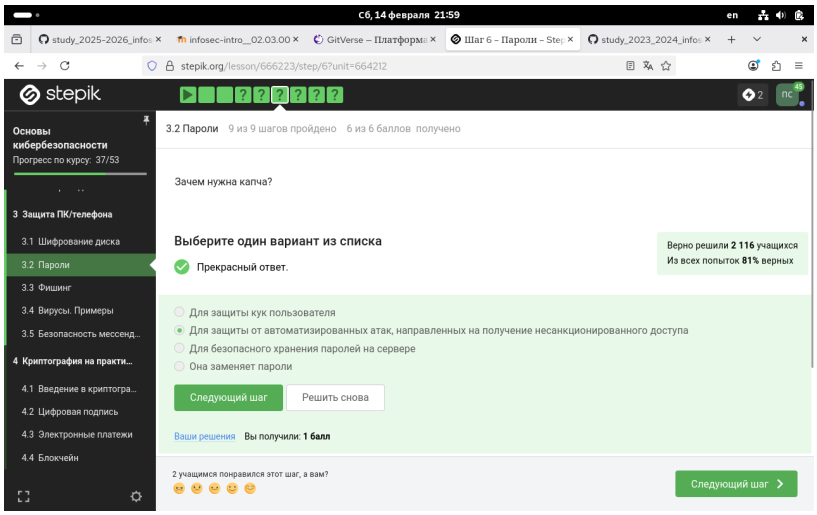

Рисунок 4.6: Задание 6

Хэширование паролей позволяет хранить их не в открытом виде (рис. 7)

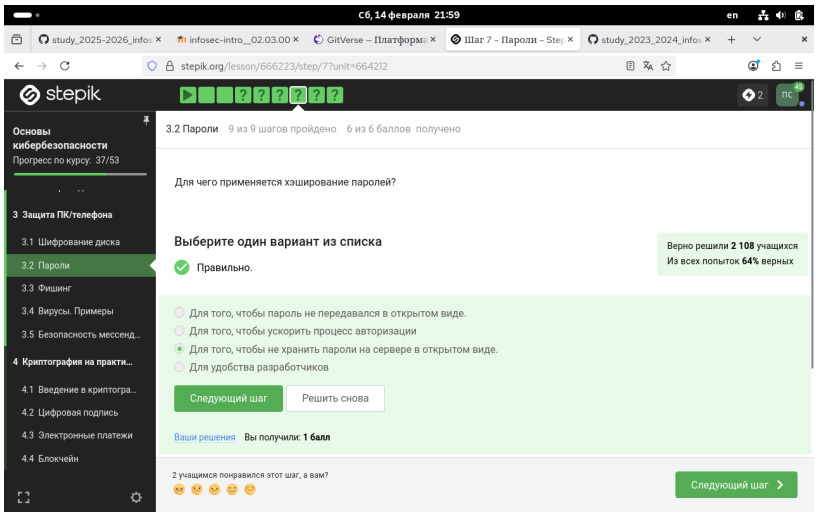

Рисунок 4.7: Задание 7

В случае доступа к серверу, соленые пароли уже не помогут. (рис.8)

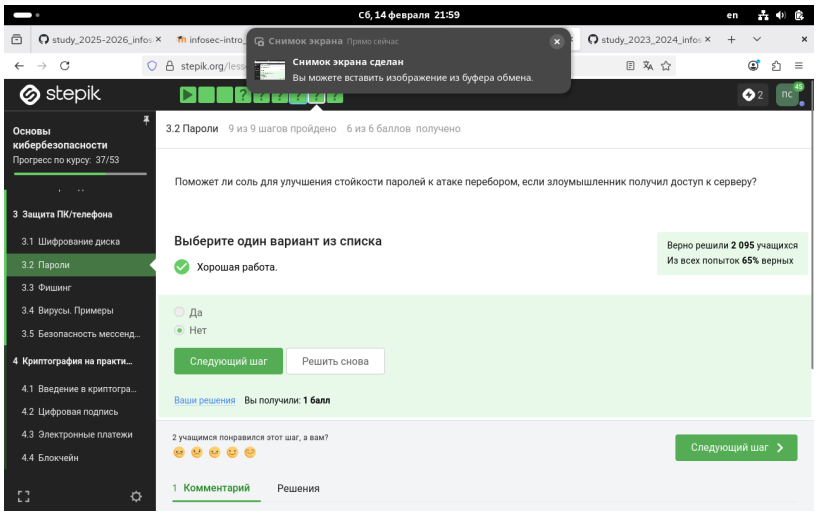

Рисунок 4.8: Задание 8

Все указанные меры надежно защищают от утечек данных. (рис.9)

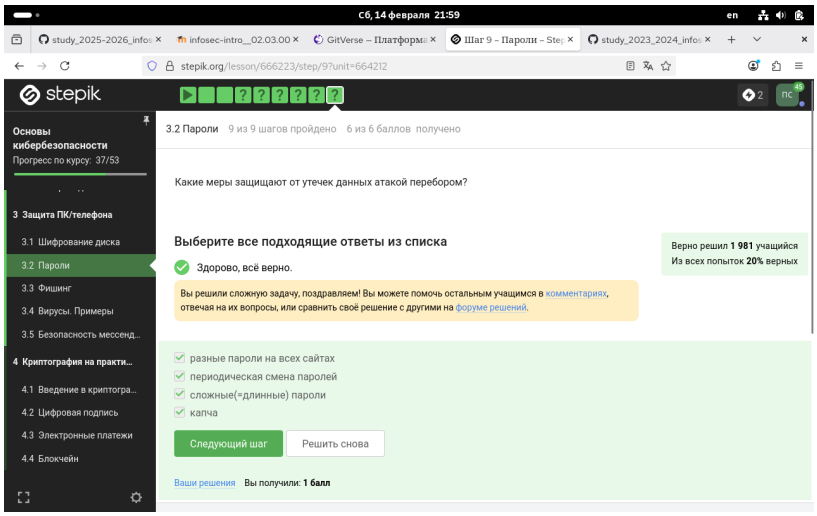

Рисунок 4.9: Задание 9

Фишинговые ссылки часто сделаны на сервисах создания сайтов, например викс или тильда, также фишинговые ссылки очень похожи на ссылки известных сервисов, но имеют небольшие различия, которые легко не заметить. (рис. 10)

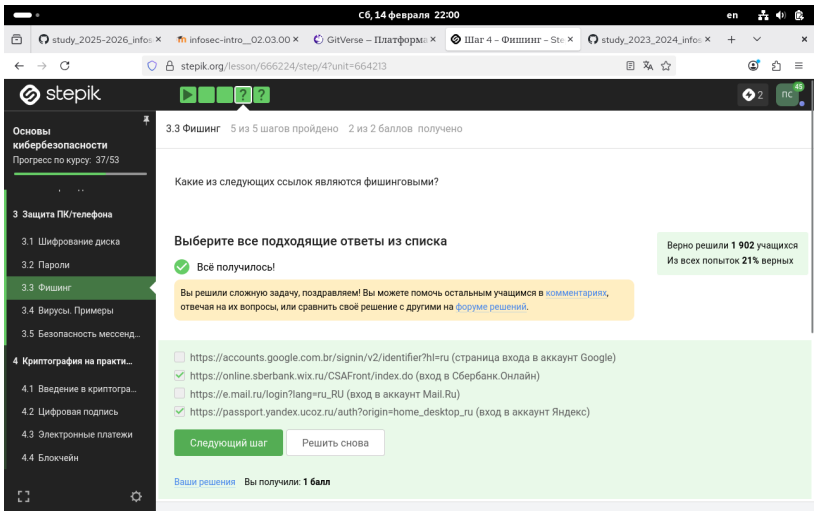

Рисунок 4.10: Задание 10

Фишинговое письмо может прийти от кого угодно, например если их взломали. (рис. 11)

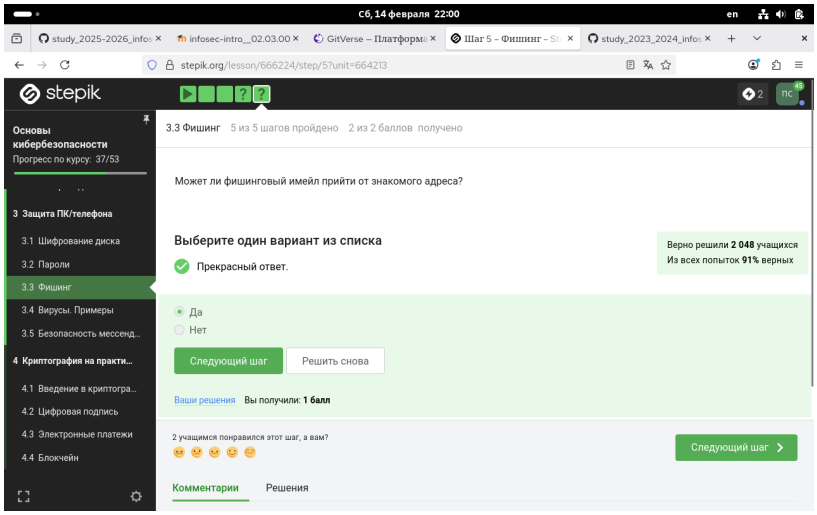

Рисунок 4.11: Задание 11

Спуфинг - от английского слова spoof, что значит подменять. (рис 12)

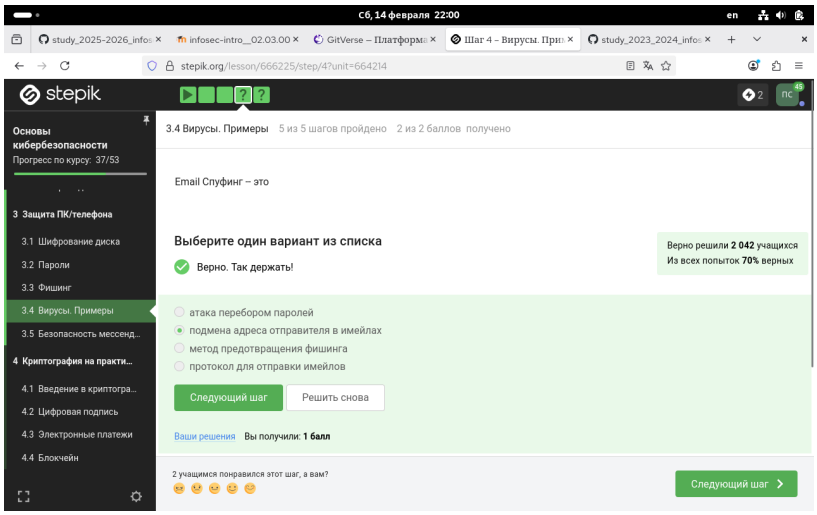

Рисунок 4.12: Задание 12

Троян маскируется под обычную программу. (рис. 13)

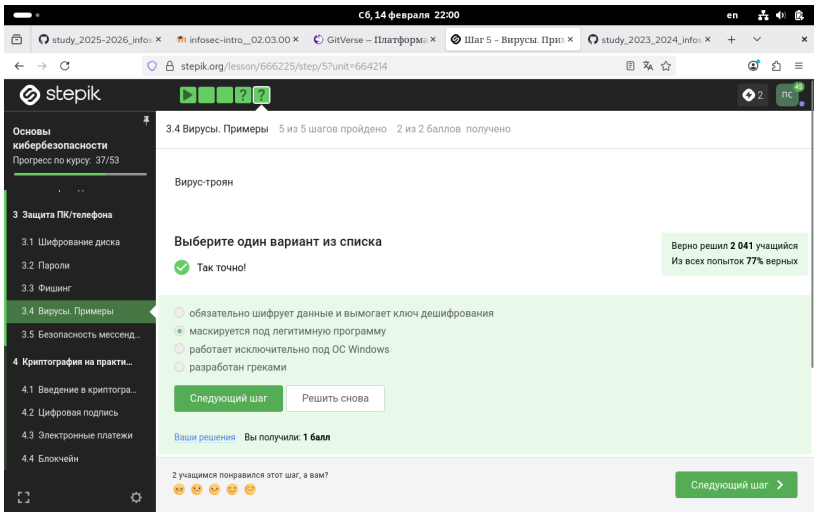

Рисунок 4.13: Задание 13

Клюс шифрования в сигнале фомируется при первом сообщении от отправителя. (рис. 14)

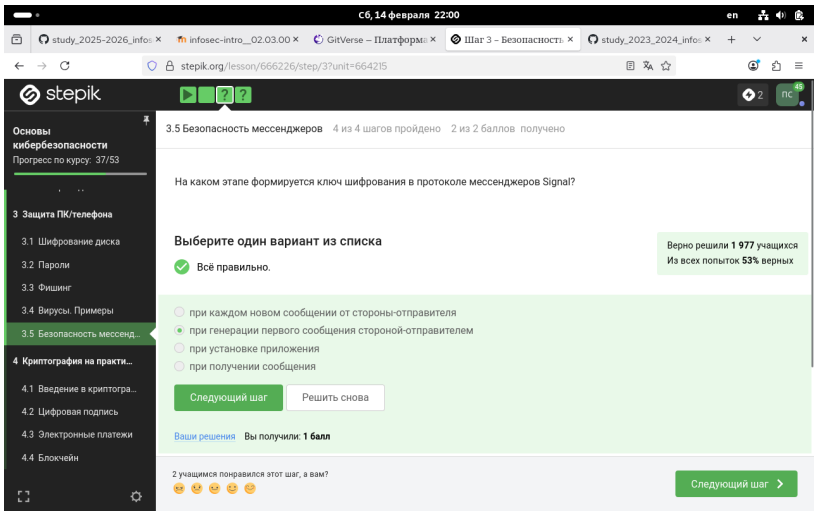

Рисунок 4.14: Задание 14

Суть сквозного шифрования в том,что сообщения передаются по узлам связи (серверам) в зашифрованном виде . (рис. 15)

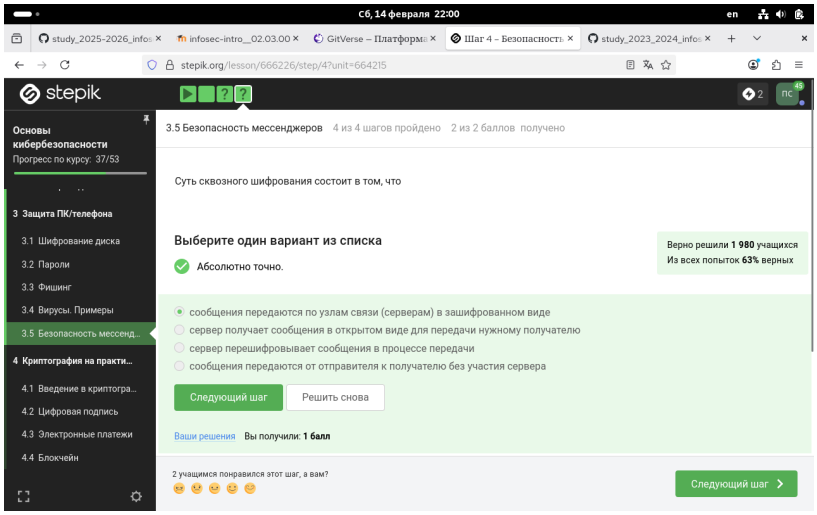

Рисунок 4.15: Задание 15

5 Выводы

Я выполнила 2 этап внешнего курса и приобрела знания о том, как приавильно защищать ПК/телефон, узнала о вирусах и фишинге, а так же научилась составлять надежные пароли.