

Информация

- Баптишта Матеуж Андре
- Студент, НКАбд-01-23
- Российский университет дружбы народов
- 1032225099@pfur.ru



Цель работы

Пройти второй блок курса “Основы кибербезопасности”

Выполнение блока 2: Защита ПК/Телефона

Шифрование диска

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Соответственно, можно (рис. (fig:001?)).

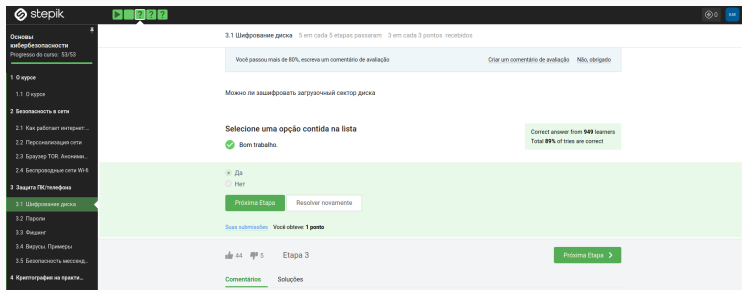


Рис. 1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. (fig:002?)).

Стойкий пароль - тот, который тяжелее подобрать, он должен быть со спец. символами и длинный (рис. (fig:004?)).

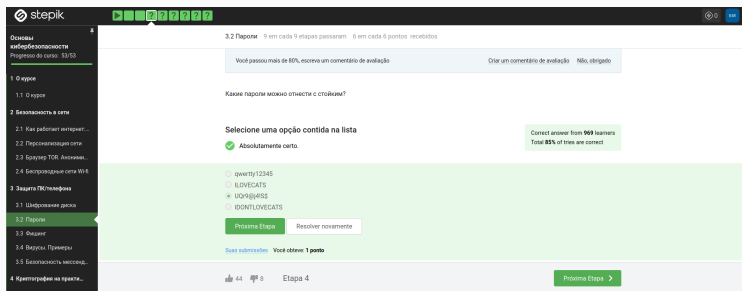


Рис. 4: Вопрос 3.2.1

Все варианты, кроме менеджера паролей, совершенно не надежные (рис. (fig:005?)).



Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями (рис. (fig:010?)).

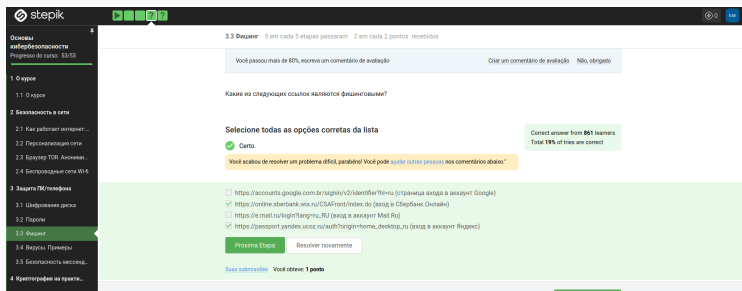


Рис. 10: Вопрос 3.3.1

Да, может, например, если пользователя со знакомым адресом взломали (рис. (fig:011?)).



Ответ дан в соответствии с определением (рис. (fig:012?)).

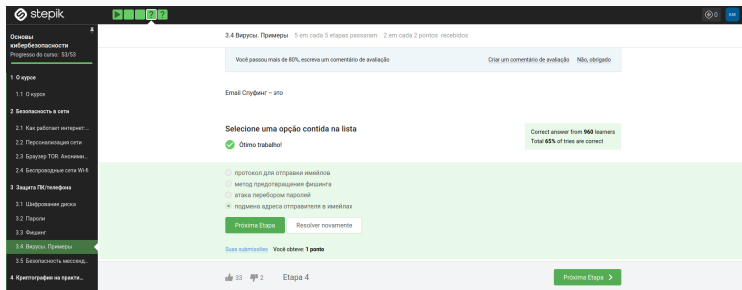
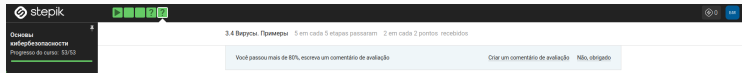


Рис. 12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. (fig:013?)).



При установке первого сообщения отправителем формируется ключ шифрования (рис. (fig:014?)).

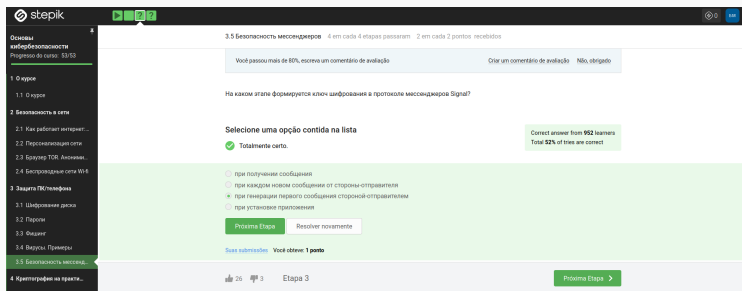


Рис. 14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде (рис. (fig:015?)).

Выводы

Был пройден второй блок курса “Основы кибербезопасности”, изучены правила хранения паролей и основная информация о вирусах