Внешний курс. Блок 2: Защита ПК/телефона

Дисцеплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

1	Цель работы															
2		Выполнение заданий блока "Основы Кибербезопасности"														
	2.1	Шифрование диска	6													
	2.2	Пароли	7													
	2.3	Фишинг	10													
	2.4	Вирусы	11													
	2.5	Безопасность мессенджеров	12													
3	Выв	ОДЫ	14													

Список иллюстраций

2.1	Вопрос 3.1.1															6
2.2	Вопрос 3.1.2															7
2.3	Вопрос 3.1.3															7
2.4	Вопрос 3.2.1															8
2.5	Вопрос 3.2.2															8
2.6	Вопрос 3.2.3															9
2.7	Вопрос 3.2.4															9
2.8	Вопрос 3.2.5															10
2.9	Вопрос 3.2.6															10
2.10	Вопрос 3.3.1															11
2.11	Вопрос 3.3.2															11
2.12	Вопрос 3.4.1															12
2.13	Вопрос 3.4.2															12
2.14	Вопрос 3.5.1															13
2 15	Βοπρος 3 5 1															13

Список таблиц

1 Цель работы

Выполненить контрольные задания второго блока "Защита ПК/телефона" внешнего курса "Основы кибербезопасности".

2 Выполнение заданий блока "Основы Кибербезопасности"

2.1 Шифрование диска

Шифровать нужно не только жесткий диск, но и загрузочный сектор диска. Ответ-можно (рис. 2.1).

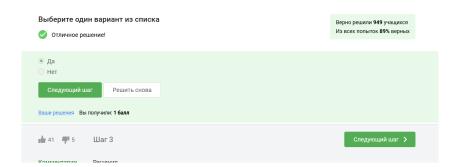


Рис. 2.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 2.2).



Рис. 2.2: Вопрос 3.1.2

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные опенсорсные альтернативы, такие как Veracrypt и PGPDisk. (рис. 2.3).

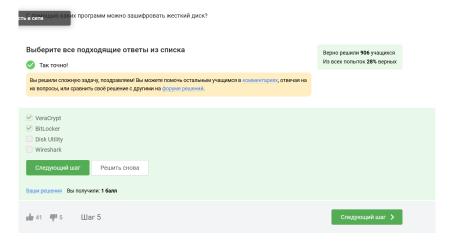


Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

Стойкий пароль содержит цифры стройчные и заглавные буквы и специальные символы. Это усложняет перебор пароля (рис. 2.4).

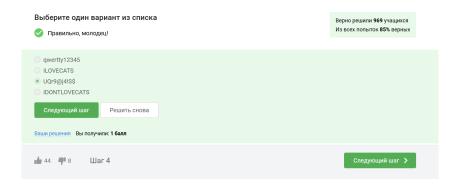


Рис. 2.4: Вопрос 3.2.1

Безопасно хранить пароли нужно только в месенджерах (рис. 2.5).

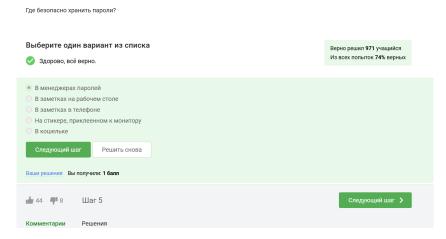


Рис. 2.5: Вопрос 3.2.2

Капча - тест для определения, кто общается с веб-сервисом, человек или бот(рис. 2.6).

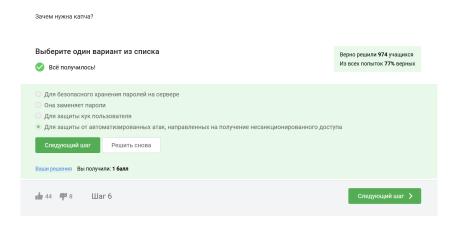


Рис. 2.6: Вопрос 3.2.3

В целях безопасности пароли хранят не в открвтом виде, а в виде хешей (рис. 2.7).

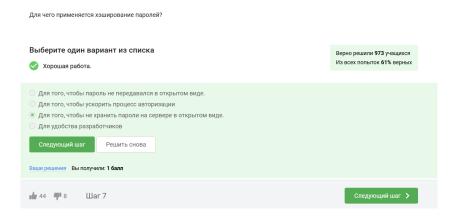


Рис. 2.7: Вопрос 3.2.4

Соль - это метод защиты слабых паролей. Сервер добавляет соль к паролю пользователя. Это делает взлом слабых паролей сложнее (рис. 2.8).

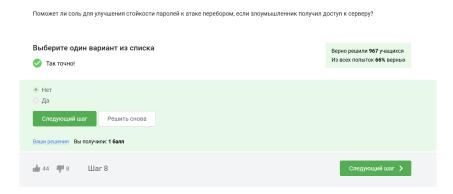


Рис. 2.8: Вопрос 3.2.5

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в месенджерах паролей. (рис. 2.9).

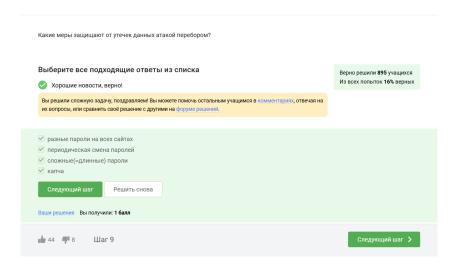


Рис. 2.9: Вопрос 3.2.6

2.3 Фишинг

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем (рис. 2.10).

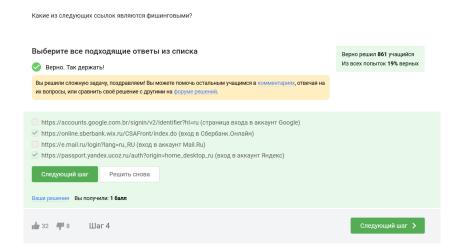


Рис. 2.10: Вопрос 3.3.1

Может фишинговое письмо прийти и от знакомого(рис. 2.11).

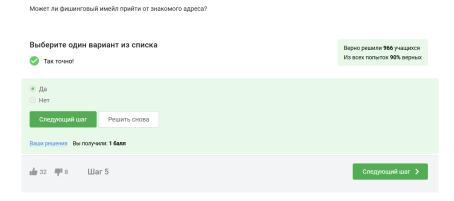


Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы.

Спуфинг - это подмена адреса отправителя в имейлах (рис. 2.12).

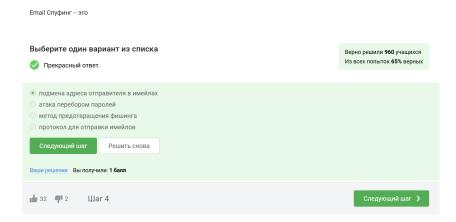


Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его(рис. 2.13).

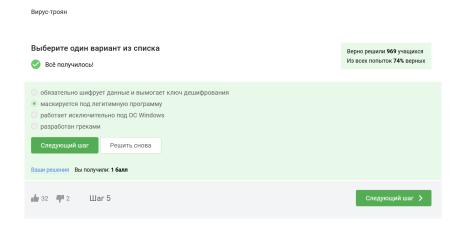


Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. 2.14).

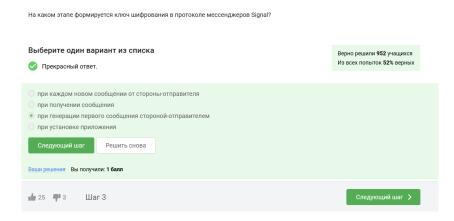


Рис. 2.14: Вопрос 3.5.1

Сквозное шифрование позволяет передавать сообщения между пользователями (Алиса и Боб) так, что сервер знает только адресата, но не может прочитать содержимое. Алиса шифрует сообщение, сервер передает шифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения. (рис. 2.15).

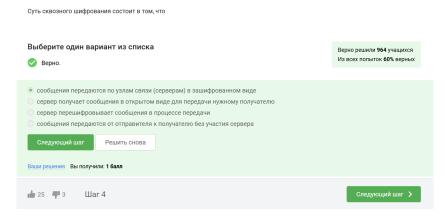


Рис. 2.15: Вопрос 3.5.1

3 Выводы

В результате я сделала второй блок курса "Основы кибербезопасности". Узнала правила составления и хранения паролей, поняла много нового о вирусах и мерах безопасности против них.