# Внешний курс. Блок 2. Защита ПК/телефона

Основы информационной безопасности

Мурашов Иван Вячеславович

# Содержание

1	Целі	Цель работы													
2	Вып	олнение заданий	6												
	2.1	Шифрование диска	6												
	2.2	Пароли	7												
		Фишинг													
	2.4	Вирусы. Примеры	11												
		Безопасность мессенджеров													
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																				3
2.6	Вопрос 3.2.3																				ç
2.7	Вопрос 3.2.4																				ç
2.8	Вопрос 3.2.5																				ç
2.9	НВопрос 3.2.6																				10
2.10	Вопрос 3.3.1																		•		10
2.11	Вопрос 3.3.2																				11
2.12	Вопрос 3.4.1																				11
2.13	Вопрос 3.4.2																				12
2.14	Вопрос 3.5.1																				12
2.15	Вопрос 3.5.2																_				13

## Список таблиц

# 1 Цель работы

Выполнение контрольных заданий 2го блока внешнего курса "Основы Кибербезопасности".

## 2 Выполнение заданий

## 2.1 Шифрование диска

Шифрование диска - технология защиты информации, которая переводит данные на диске в нечитаемый код. Само собой можно зашифровать загрузочный сектор диска (рис. 2.1).

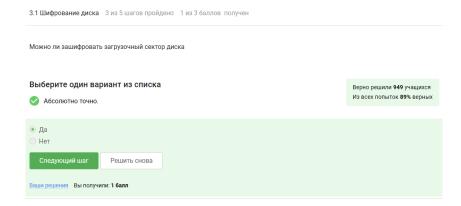


Рис. 2.1: Вопрос 3.1.1

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

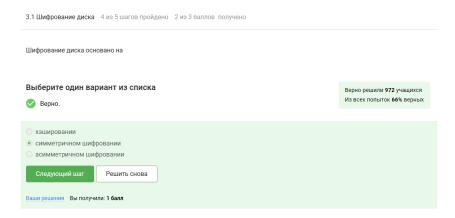


Рис. 2.2: Вопрос 3.1.2

Отмечены программы, с помощью которых можно зашифровать жетский диск (рис. 2.3).

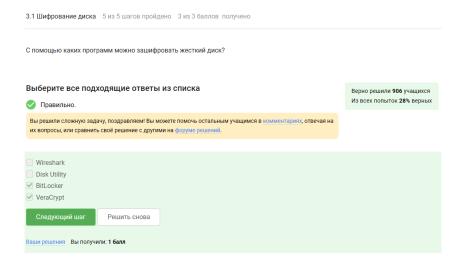


Рис. 2.3: Вопрос 3.1.3

## 2.2 Пароли

Стойкий пароль - тот, который тяжлее подобрать, он должен быть со спец. символами и длинный (рис. 2.4).



Рис. 2.4: Вопрос 3.2.1

Все варианты, кроме менеджера паролей, совершенно не надежные (рис. 2.5).

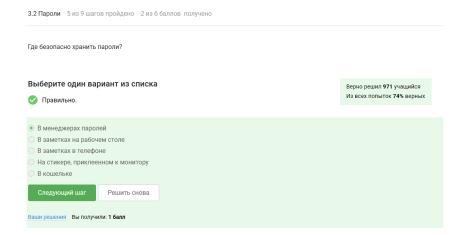


Рис. 2.5: Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном "не робот" (рис. 2.6).

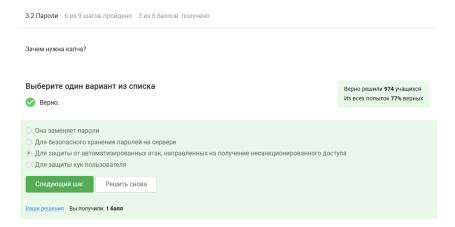


Рис. 2.6: Вопрос 3.2.3

Опасно хранить пароли в открытом виде, поэтому хранят их хэши (рис. 2.7).

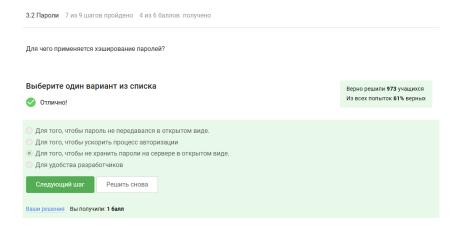


Рис. 2.7: Вопрос 3.2.4

Соль не поможет (рис. 2.8).

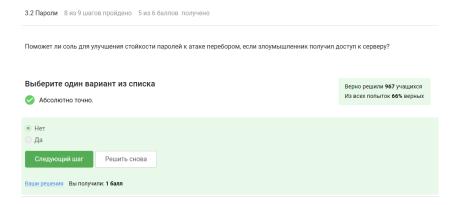


Рис. 2.8: Вопрос 3.2.5

Все приведенные меры защищают от утечек данных (рис. 2.9).

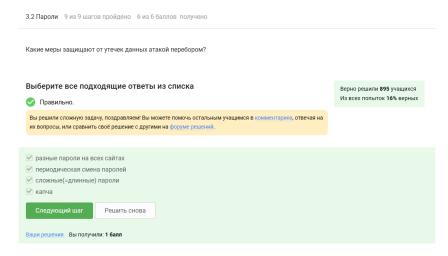


Рис. 2.9: НВопрос 3.2.6

#### 2.3 Фишинг

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями (рис. 2.10).

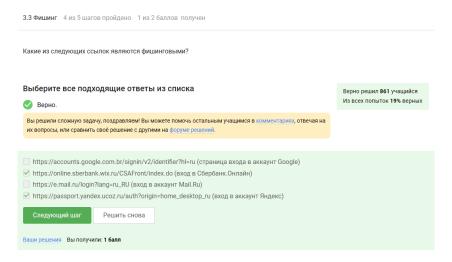


Рис. 2.10: Вопрос 3.3.1

Да, может, например, если пользователя со знакомым адресом взломали (рис. 2.11).

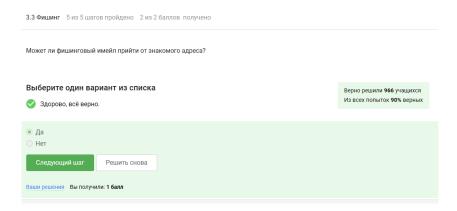


Рис. 2.11: Вопрос 3.3.2

## 2.4 Вирусы. Примеры

Ответ дан в соответствии с определением (рис. 2.12).

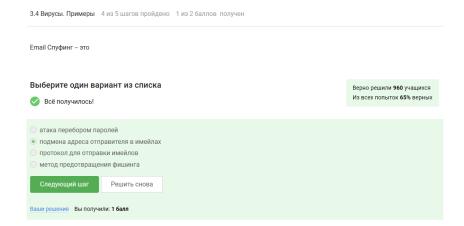


Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

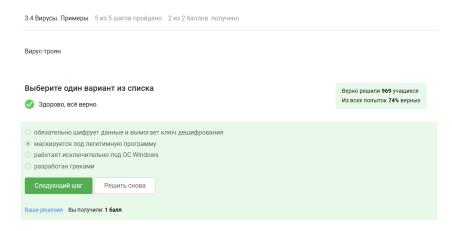


Рис. 2.13: Вопрос 3.4.2

#### 2.5 Безопасность мессенджеров

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

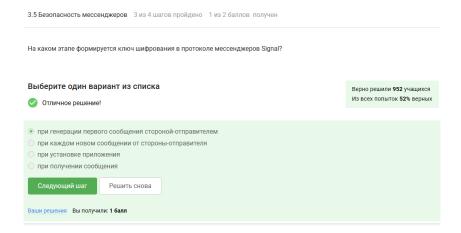


Рис. 2.14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообзения передаются по узлам связи в зашифрованном виде (рис. 2.15).

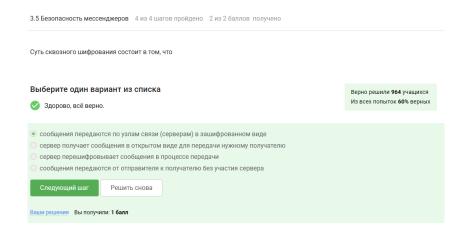


Рис. 2.15: Вопрос 3.5.2

# 3 Выводы

Был пройден второй блок курса "Основы кибербезопасности", мной были изучены правила хранения паролей и основная информация о вирусах