Внешний курс. Этап 2

Защита ПК/телефона

Татьяна Александровна Буллер

Содержание

1	Цель работы															
2	Вып	ыполнение контрольных заданий														
	2.1	Шифрование диска	6													
	2.2	Пароли	9													
	2.3	Фишинг	13													
	2.4	Вирусы. Примеры	14													
	2.5	Безопасность мессенджеров	15													
3	Выв	оды	17													

Список таблиц

Список иллюстраций

2.1	Задание 1.	•	•		•	•		•		•								•	•		6
2.2	задание 2 .																				7
2.3	Задание 3 .																				8
2.4	Задание 4 .																				9
2.5	Задание 5 .																				10
2.6	Задание 6 .																				10
2.7	Задание 7 .																				11
2.8	Задание 8 .																				11
2.9	Задание 9 .																				12
2.10	Задание 10																				13
2.11	Задание 11																				13
2.12	Задание 12																				14
2.13	Задание 13																				15
2.14	Задание 14																				15
2.15	Залание 15																				16

1 Цель работы

Получение и закрепление на практике знаний о базовых мерах обеспечения безопасности электронных устройств и основных ошибках пользователей.

2 Выполнение контрольных заданий

2.1 Шифрование диска

Можно ли зашифровать загрузочный сектор диска

Select one option from the list

Right.

Да
Нет

Next step
Solve again

Рис. 2.1: Задание 1

Зашифровать можно любой раздел диска, в том числе загрузочный, чем нередко пользуются злоумышленники.

Шифрование диска основано на

Select one option from the list



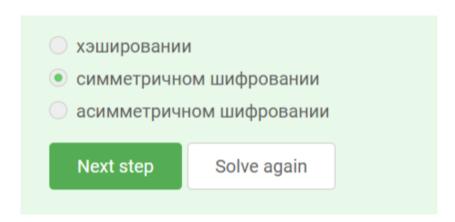


Рис. 2.2: задание 2

Шифрование диска основано на симметричном шифровании с использованием постоянного ключа: пароля.

Select all correct options from the list Fabulous answer. You've solved a complex problem, congratulations! Now you can help other learners in comquestions, or compare your solution with others on solution forum. Wireshark BitLocker VeraCrypt Disk Utility Next step Solve again

Рис. 2.3: Задание 3

Wireshark - инструмент анализа сетевого трафика, Disk Utility - утилита для работы с дисками, но не для их шифрования. Наиболее популярные инструменты для шифрования дисков - VeraCrypt и BitLocker.

2.2 Пароли

Какие пароли можно отнести с стойким?

Select one option from the list

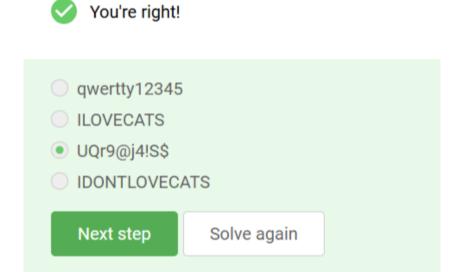


Рис. 2.4: Задание 4

Пароли 1, 2 и 4 не содержат специальных символов и представляют собой достаточно предсказуемые фразы в одном регистре, что делает их уязвимыми даже к перебору без словаря. Наиболее безопасен из представленных третий пароль.

Где безопасно хранить пароли?

Select one option from the list

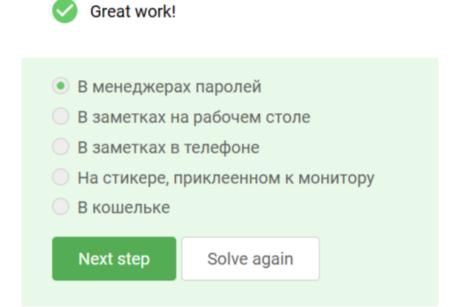


Рис. 2.5: Задание 5

Пароли должны храниться в специализированных приложениях, но не в местах, где к ним может получить доступ третье лицо.

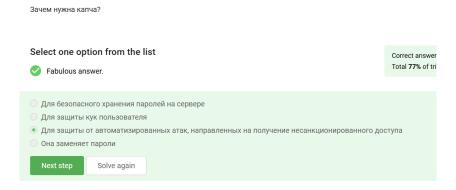


Рис. 2.6: Задание 6

Капча - "проверка на человека", защищает от автоматизированных атак.

Для чего применяется хэширование паролей?

Select one option from the list

✓ You're right!

Для того, чтобы пароль не передавался в открытом виде.

Для того, чтобы ускорить процесс авторизации

Для того, чтобы не хранить пароли на сервере в открытом виде.

Для удобства разработчиков

Next step

Solve again

Рис. 2.7: Задание 7

Хэширование паролей применяется для шифрования паролей и усложнения получения доступа к учетным записям конкретных пользователей, если злоумышленник получил доступ к базе данных сервера.

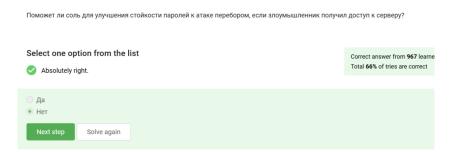


Рис. 2.8: Задание 8

Select all correct options from the list Good job. You've solved a complex problem, congratulations! Now you can help other learne questions, or compare your solution with others on solution forum. paзные пароли на всех сайтах периодическая смена паролей сложные(=длинные) пароли капча Next step Solve again

Рис. 2.9: Задание 9

Все перечисленное (как длинные/сложные пароли, так и регулярное их обновление, разные пароли на всех сайтах и капча) защитят пользователя в случае, если сервер подвергнется атаке перебором. Длинные пароли подобрать сложнее, регулярное обновление и разные пароли на сайтах позволяют избежать совпадения со слитыми базами, капча - убедиться, что войти пытается человек, а не брутфорс-скрипт.

2.3 Фишинг

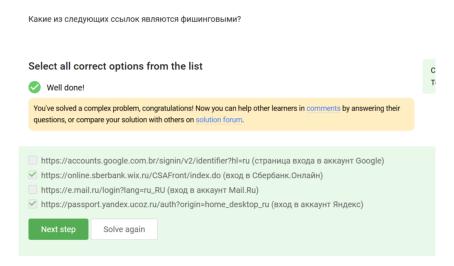


Рис. 2.10: Задание 10

Фишинговыми являются 2 и 4 ссылки, так как сайт, под который они пытаются мимикрировать, является доменом не второго, а третьего уровня (основными являются соответственно wix.ru и ucoz.ru).

Select one option from the list

Ves!

Может ли фишинговый имейл прийти от знакомого адреса?

ДаНетNext stepSolve again

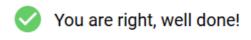
Рис. 2.11: Задание 11

Фишинговое письмо может прийти со знакомого адреса, если владелец аккаунта был взломан.

2.4 Вирусы. Примеры

Email Спуфинг -- это

Select one option from the list



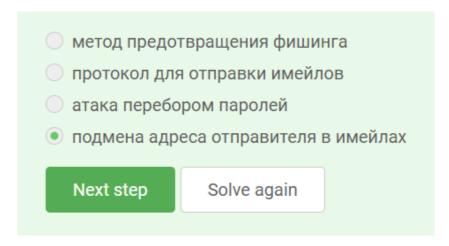


Рис. 2.12: Задание 12

Спуфингом называется подмена адреса. Атака перебора паролей - брутфорс, протоколов электронной почты имеется великое множество, точно как и методов предотвращения фишинга.

Вирус-троян

Select one option from the list

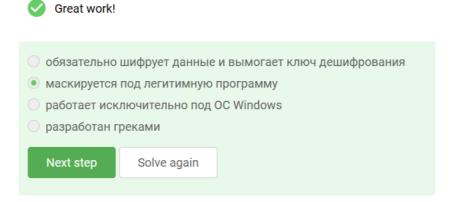


Рис. 2.13: Задание 13

Троян - вирус, маскирующийся под легитимную программу. Название идет от легенды о троянском коне, однако вирус вовсе не обязательно работает только с отдельной операционной системой или разработан греками.

2.5 Безопасность мессенджеров

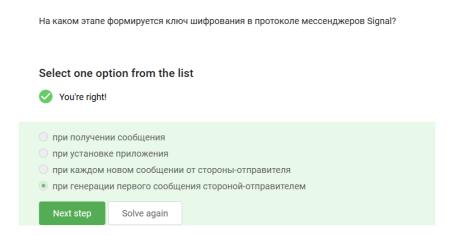


Рис. 2.14: Задание 14

Рис. 2.15: Задание 15

Суть сквозного шифрования состоит в том, что сообщение не расшифровывается на сервере и недоступно в открытом виде никому, кроме отправителя и получателя.

3 Выводы

Получены и закреплены на практике знания о базовых мерах обеспечения безопасности электронных устройств и основных ошибках пользователей.