Отчёт прохождения внешнего курса

Защита ПК/Телефона

Тарутина Кристина

Содержание

1	Цель работы	5
2	Выполнение контрольных заданий	6
3	Выводы	13
Сп	исок литературы	14

Список иллюстраций

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

Список таблиц

1 Цель работы

Провести контроль усвоения теоритического материала раздела "Защита ПК/Телефона"

2 Выполнение контрольных заданий

Да, конечно, и не только его. ЗАшифровать также можно, например, весь жёсткий диск или его сегмент(рис. 2.1).



Рис. 2.1: Задание 1

Шифрование больших объемов данных, таких как жесткий диск или его сегменты, а также крупные флешки, обычно выполняется с использованием симметричного шифрования, чаще всего алгоритма AES. Этот алгоритм является американским стандартом симметричного шифрования и широко применяется для защиты конфиденциальной информации при передаче по сети. AES - это эффективный алгоритм, который может быть реализован на аппаратном уровне, что обеспечивает высокую скорость шифрования и дешифрования. Благодаря своей производительности пользователь практически не замечает задержек в работе, поскольку операции шифрования и дешифрования выполняются быстро. (рис. 2.2).



Рис. 2.2: Задание 2

BitLocker - это утилита системы Windows, a VeraCrypt - бесплатная прогламма (рис. 2.3).

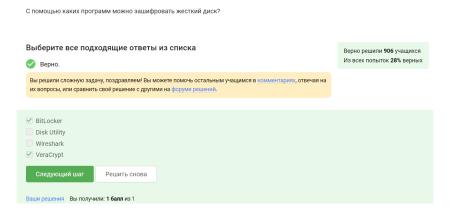


Рис. 2.3: Задание 3

Стойкие пароли это те, которые невозможно перебрать. Среди данных нам вариантов к стойким относится только один.(рис. 2.4).



Рис. 2.4: Задание 4

В менеджерах паролях. Все остальные варианты даже в рамках здравого смысла звучат абсурдно, а подобные менеджеры специализуются на хранении и хорошо защищены(рис. 2.5).



Рис. 2.5: Задание 5

Для защиты от автоматизированных атак. Она призвана распознавать ботов, но некоторые из них уже натренированы решать капчу, а ещ есть сайты, где капчу за копейки решают люди.(рис. 2.6).

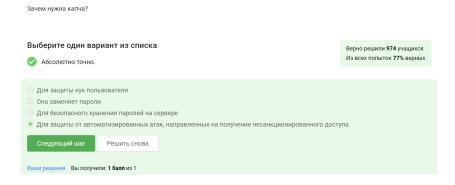


Рис. 2.6: Задание 6

Чтобы не хранить пароли на сервере в открытом виде. ЭТо позволяет повысить безопасность.(рис. 2.7).

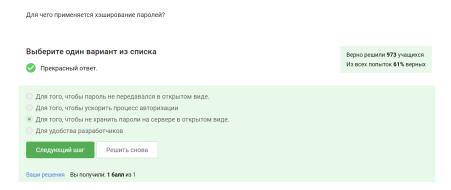


Рис. 2.7: Задание 7

Конечно нет. У него уже есть доступ к серверу, а значит и данные о самой соли(рис. 2.8).

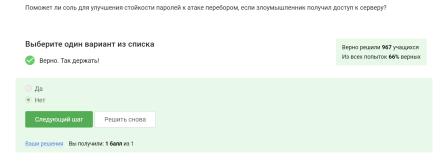


Рис. 2.8: Задание 8

ЭТо задание с маленьким подвохом. Здесь верны все ответы. ИХ комплекс может лучше всего обезопасить нас от подобного рода утечек данных(рис. 2.9).

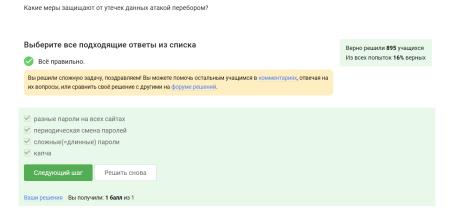


Рис. 2.9: Задание 9

Страница входа в Google не является фишинговой, это просто бразильская страница. Отсюда и такое странное сочетание букв. Страница маил ру тоже правильная (рис. 2.10).

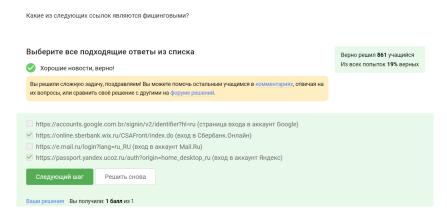


Рис. 2.10: Задание 10

Конечно может. МОжет быть так, что это очень похожий имеил, например не Alan@mail.ru, а Alam@mail.ru. Чем длиньше название, тем сложнее заметить. Но и простой взлом аккаунта никто не отменял(рис. 2.11).

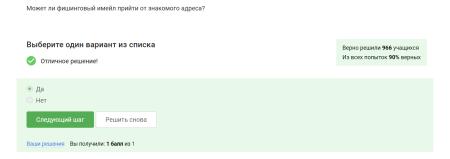


Рис. 2.11: Задание 11

Это подмена адреса отправителя в имейлах. Такого рода атаки нанесли крупные финанские потери компаниям в своё время(рис. 2.12).



Рис. 2.12: Задание 12

Ну, здесь можно вспомнить всем известного троянского коня и даже так догадаться. Конечно он маскируется под легитимную систему(рис. 2.13).

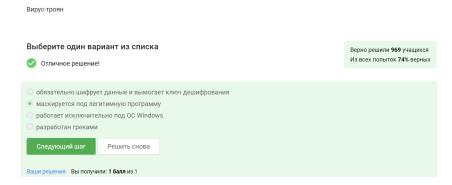


Рис. 2.13: Задание 13

При генераци первого сообщения стороной отправителем. В ином случае это либо было бы небезопасно, либо, если при каждом сообщении, попросту избыточно(рис. 2.14).

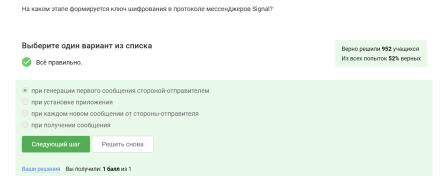


Рис. 2.14: Задание 14

СОобщения передаются в зашифрованном виде. Это довольно хороший способ передачи данных (рис. 2.15).

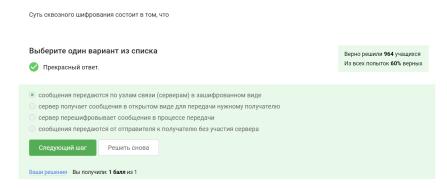


Рис. 2.15: Задание 15

3 Выводы

Мы успешно прошли контроль усвоения теоритического материала раздела "Защита ПК/Телефона"

Список литературы