Отчёт по Внешнему Курсу - Этап 2

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

Список иллюстраций

1 Цель работы

Пройти внешний курс - Этап 2

2 Выполнение лабораторной работы

Да, можно, тогда перед самим запуском всей системы также потребуется ввести пароль (рис. 2.1).

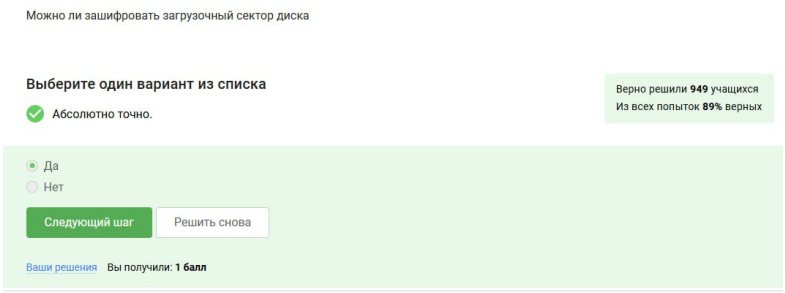

Рис. 2.1: Задание 001

Шифрование основано на алгоритме AES (рис. 2.2).

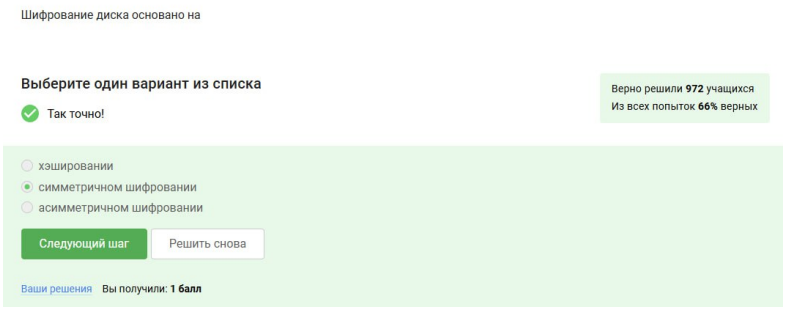

Рис. 2.2: Задание 002

BitLocker - встроенный в Windows шифровщик, VeraCrypt - сторонняя утилита для шифрования данных (рис. 2.3).

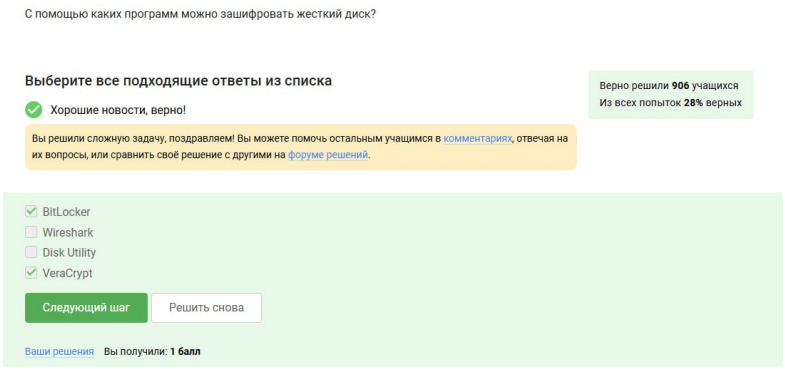

Рис. 2.3: Задание 003

Потому что есть латинские буквы - заглавные и не заглавные, а также цифры и особые символы (рис. 2.4).

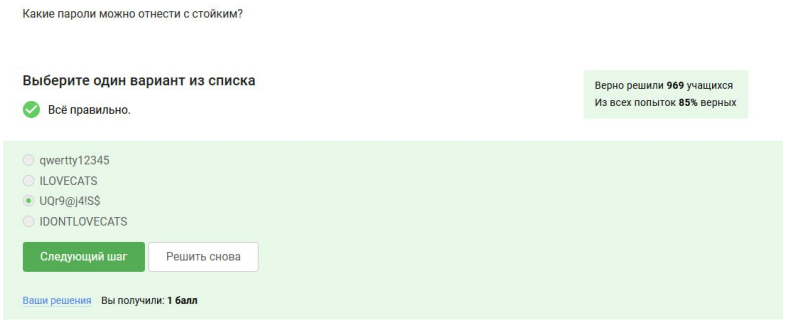

Рис. 2.4: Задание 004

Безопаснее всего хранить в менеджерах паролей, но для такого менеджера желательно всё-таки придумать очень хороший пароль и вот его придётся запомнить самому (рис. 2.5).

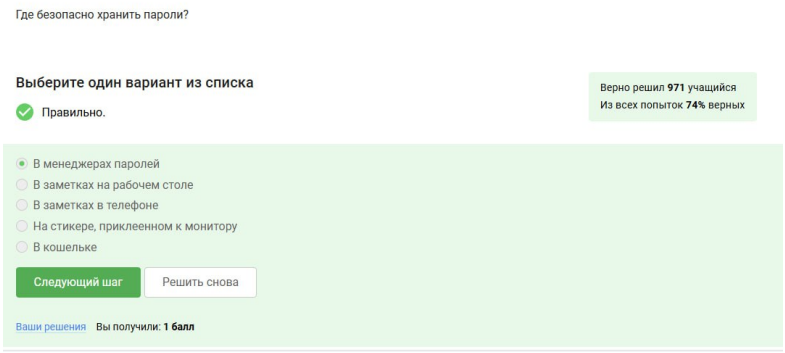

Рис. 2.5: Задание 005

Капча спасает от автоматизированных атак, правда в последнее время искусственный интеллект иногда справляется с такой защитой, иногда злоумышленники специально платят людьми за решение капчи(рис. 2.6).

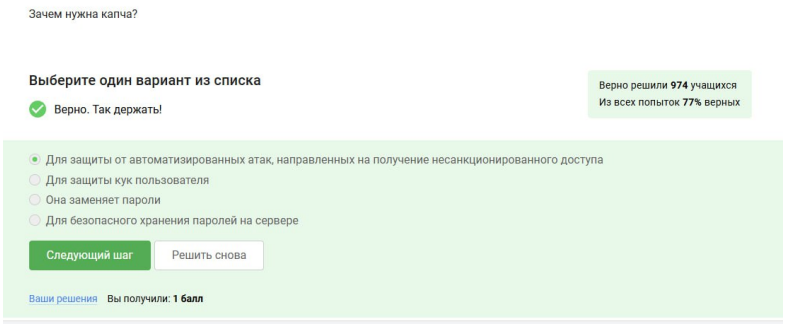

Рис. 2.6: Задание 006

Делается это для того, чтобы не хранить пароли на сервере в открытом виде, ведь иногда злоумышленники могут устроить утечку данных, но хэширование не позволит злоумышленникам воспользоваться полученными данными, ведь их будет очень сложно расшифровать (рис. 2.7).

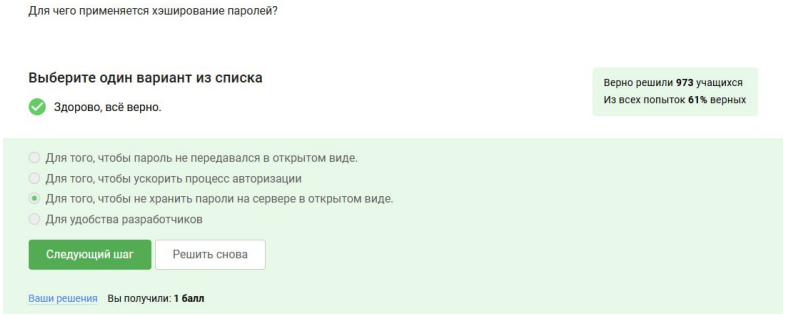

Рис. 2.7: Задание 007

Нет, т.к. соль это тоже тип данных, который хранится на сервере, ну и если у злоумышленника есть доступ к серверу, значит и соль особо ему не поможет (рис. 2.8).

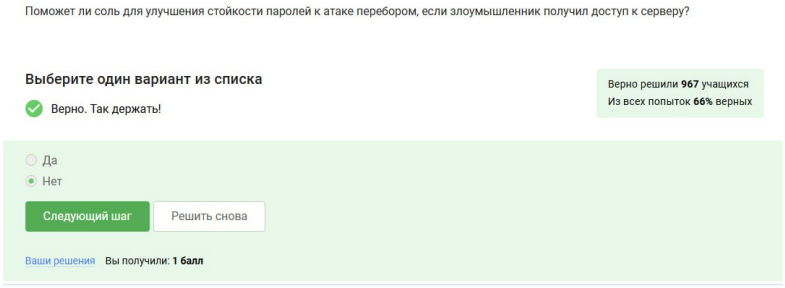

Рис. 2.8: Задание 008

Здесь все варианты подходят, как те, которые зависят именно от пользователя, так и от владельца хранилища паролей (сервера) (рис. 2.9).

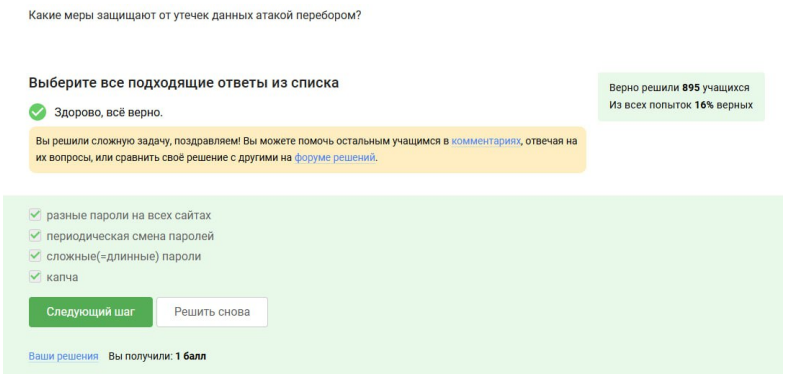

Рис. 2.9: Задание 009

Первый вариант на первый взгляд содержит странные символы .br, однако это индикатор, что это страничка в Бразилии. Второй вариант действительно фишинговый, т.к. сделан на конструкторе сайтов wix.ru - сложно поверить, что такая крупная компания, как сбербанк делала бы свой сайт не самостоятельно с нуля. Третий, это просто рабочая ссылка Mail.ru, четвёртая - фишинговая, т.к. содержит подозрительные символы .ucoz (рис. 2.10).

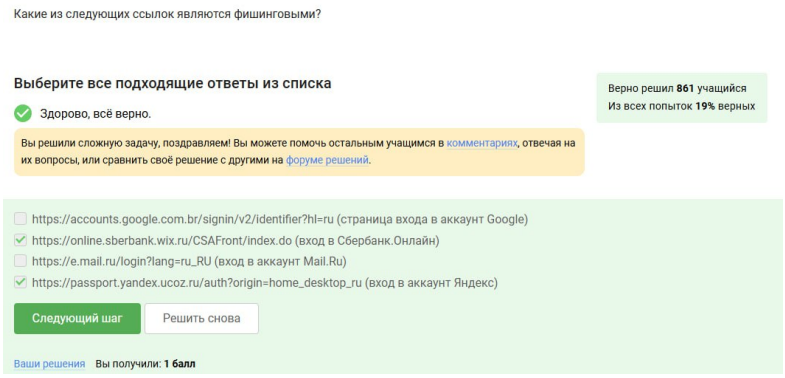

Рис. 2.10: Задание 010

Может, например, если адрес взломали, или может вы спутаете его со знакомым вам адресом (рис. 2.11).

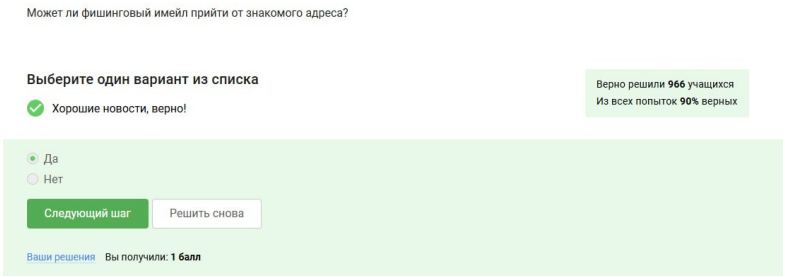

Рис. 2.11: Задание 011

Это не протокол для отправки имейлов, но email спуфинга связан с проблемой старых протоколов для отправки имейлов (рис. 2.12).

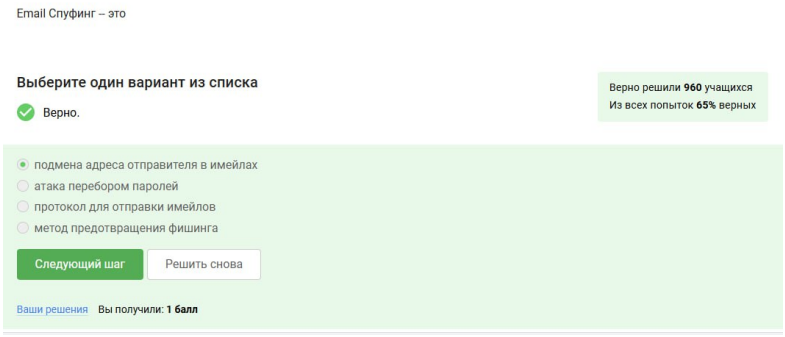

Рис. 2.12: Задание 012

Оттого он и называется Троян (рис. 2.13).

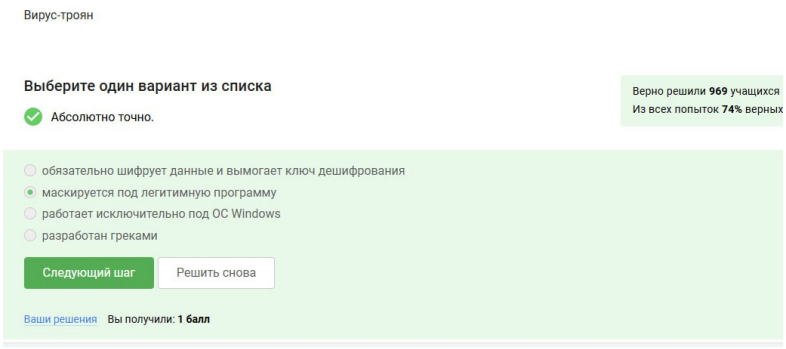

Рис. 2.13: Задание 013

Это происходит только при самом первом сообщении между пользователями (рис. 2.14).

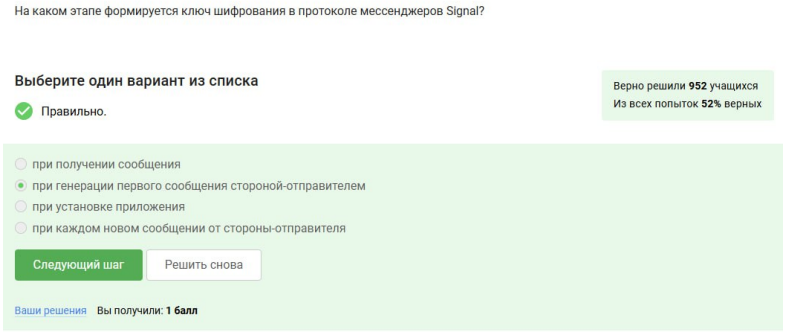

Рис. 2.14: Задание 014

Сервер лишь знает, кому эти сообщения нужно передать, а сами сообщения он не понимает (рис. 2.15).

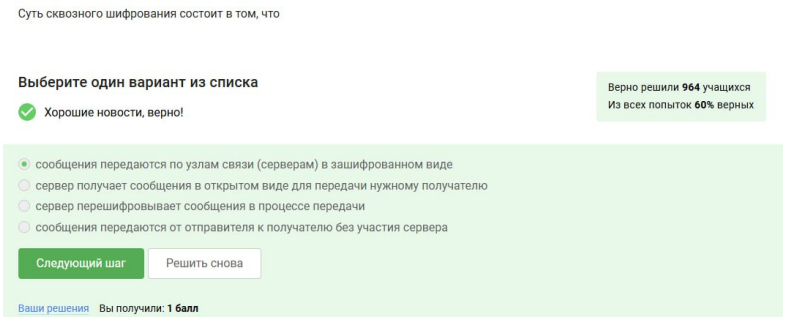

Рис. 2.15: Задание 015

3 Выводы

Этап 2 пройден успешно на максимальный балл.

4 Список литературы

Курс “Основы Кибербезопасности” на платформе Stepik