Прохождения внешнего курса на тему Основы кибербезопасности. Часть 2

Основы информационной безопасности

Просина К. М.

17 май 2025

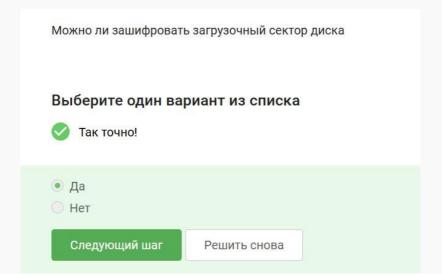
Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Просина Ксения Максимовна
- студент 2 курса
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1132231938@rudn.ru

3 Защита ПК/телефона

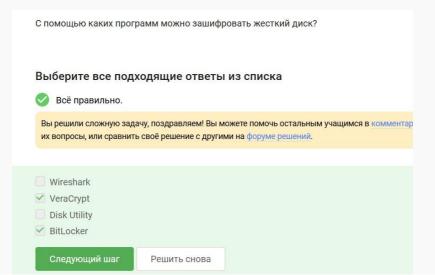


Пояснение ответа: Шифровать можно(и нужно) отдельные сектора диска(включая загрузочный сектор), флэшки с конфиденциальными данными.



Пояснение ответа: Метод шифрования:

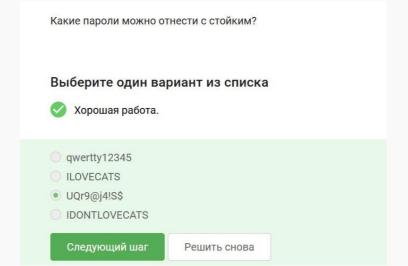
- Для процедуры Encrypt/Decrypt используется симметрические шифрования (AES)
- Данные шифруются секторами
- Шифрование ускоряется ТМР криптопроцессом
- Шифровать можно и загрузочный сектор. При этом пользователь должен запомнить пароль для дешифрирование ключа.



Пояснение ответа: Программы,с которыми можно зашифровать жесткий диск: VeraCrypt, BitLocker, LUKC, FileVault.

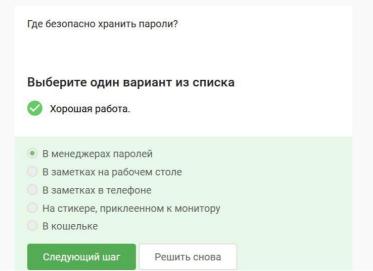
32 Пароли

Вопрос/Ответ 1

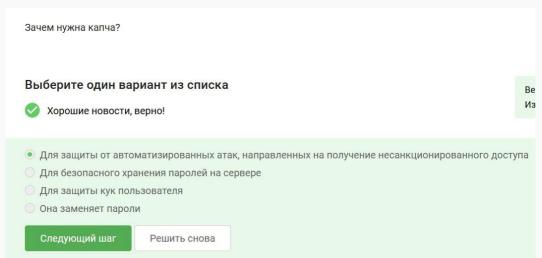


9/32

Пояснение ответа: Пароль считается стройким если в нем используются множество видов символов(буквы, цифры, знаки, буквы в большом регистре), чем больше видов, тем больше нужно переборов, чтобы его взломать.



Пояснение ответа: Наиболее безопасным является хранение паролей именно в менеджерах паролей.



Пояснение ответа: Капча проверяет пользователя не является ли он программой перебора данных для взлома, обычно используются разные методы, такие как: нахождения правильной картинки или набора букв/цифр. Итак, капча защищает от автоматизированных атак, направленные на получение несанкционированного доступа.

Вопрос/Ответ 4

Для чего применяется хэширование паролей? Выберите один вариант из списка Отличное решение! 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 Следующий шаг Решить снова

15/32

Пояснение ответа: Хеширование паролей используется для того, чтобы не хранить паролина сервере в открытом виде, это делается для безопасности.

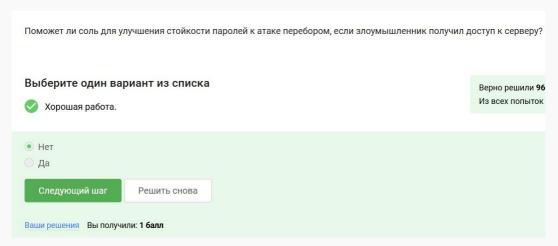
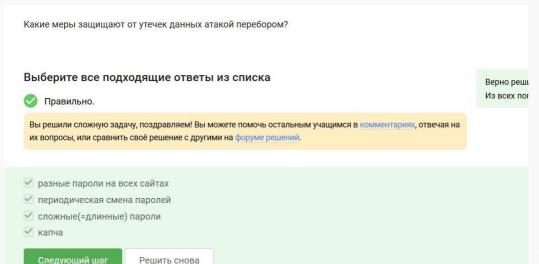


Рис. 8: Вопрос/Ответ 5

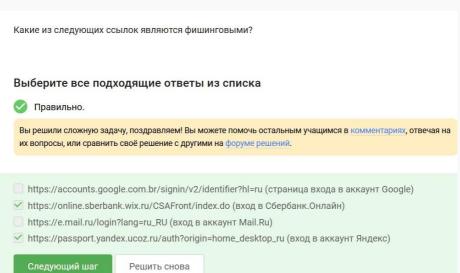
Пояснение ответа: Соль не поможет для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу, так как соль добавляется во время хеширования, но это никак не меняет пароль пользователя и он остается прежним, что позволяет злоумышленнику добраться до цели.



Пояснение ответа: Меры защиты от утечек данных перебором:

- Использовать длинные пароли с символами алфавита разного регистра, цифрами, спец. символами
- Использовать менеджеры паролей для хранения
- Регуляное изменение пароли к критическим сервисам
- Использование разных паролей для разных сайтов, программ.

33 Фишинг



Пояснение ответа: В ссылке https://online.sberbank.wix.ru/CSAFront/index.do:

- Домен wix.ru это беспратный хостинг, никак не связанный со Сбербанком.
- online.sberbank- это всего лишь поддомен хостинга wix.ru, а не настоящий сайт Сбербанка, настоящий- sberbank.ru или online.sberbank.ru

В ссылке https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru:

- ucoz.ru- это также бесплатный конструктор сайтов
- passport.yandex- поддомен ucoz.ru

Вопрос/Ответ 2

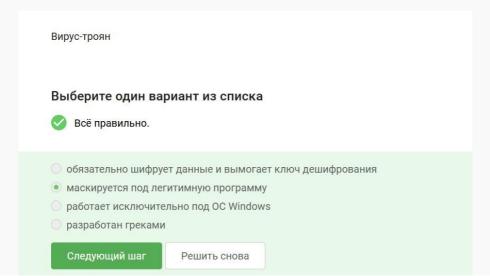
Может ли фишинговый имейл прийти от знакомого адреса? Выберите один вариант из списка Правильно, молодец! Да Нет Следующий шаг Решить снова

Пояснение ответа: Фишинговый имейл может прийти от знакомого адреса, это называется ір или имейл spoofing- подмена адреса отправителя.

Вопрос/Ответ 1

Email Спуфинг -- это Выберите один вариант из списка Верно. Так держать! метод предотвращения фишинга подмена адреса отправителя в имейлах атака перебором паролей протокол для отправки имейлов Следующий шаг Решить снова

Пояснение ответа: Email Спуфинг- это подмена адреса отправителя в имейлах.



Пояснение ответа:

Троян- вирус, проникающий в систему под видом легитимного ПО.

Вопрос/Ответ 1

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

- Здорово, всё верно.
- при каждом новом сообщении от стороны-отправителя
- 💿 при генерации первого сообщения стороной-отправителем
- при установке приложения
- при получении сообщения

Следующий шаг

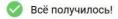
Решить снова

Пояснение ответа: Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителя.

Вопрос/Ответ 2

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка



- сообщения передаются по узлам связи (серверам) в зашифрованном виде
- 🔘 сервер получает сообщения в открытом виде для передачи нужному получателю
- сервер перешифровывает сообщения в процессе передачи
- осообщения передаются от отправителя к получателю без участия сервера

Следующий шаг

Решить снова

Пояснение ответа: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде.