Курс по основам кибербезопасности

Этап 2

Ведьмина Александра Сергеевна

Российский университет дружбы народов, Москва, Россия



Докладчик

- Ведьмина Александра Сергеевна
- студентка
- Российский университет дружбы народов
- · 1132236003@rudn.ru
- https://asvedjmina.github.io/ru/

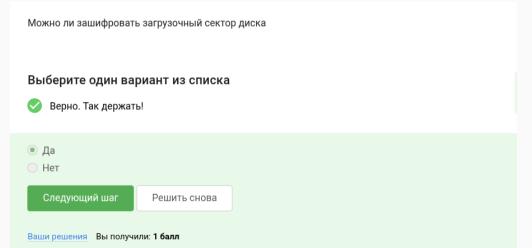


Цель работы

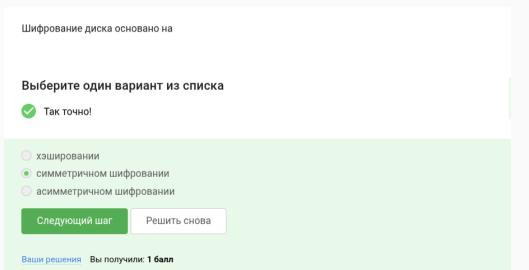
Цель работы

Выполнить задания второй части курса по кибербезопасности.

Конечно, можно. Шифрование переводит данные на диске в нераспознаваемый набор символов.



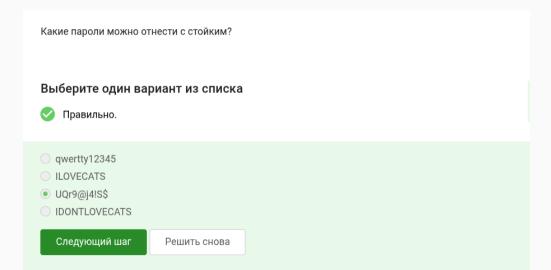
Используется симметричное шифрование.



Bitlocker, vercrypt, есть и много иных.

С помощ	ью каких программ можно зашифровать жесткий диск?
Выбери	ите все подходящие ответы из списка
🕢 Верн	но. Так держать!
-	или сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на осы, или сравнить своё решение с другими на форуме решений.
✓ VeraC	rypt
✓ BitLoc	eker
Wiresh	hark

Пароль должен состоять из разнородных символов и быть сложным для подбора.



В прочих перечисленных вариантах пароль легко украсть.

Где безопасно хранить	пароли?				
Выберите один ва	риант из списка				
Всё получилось!					
@ B	W				
 В менеджерах паро В заметках на рабоч 					
В заметках в телефоне					
На стикере, приклее	енном к монитору				
В кошельке					
Следующий шаг	Решить снова				

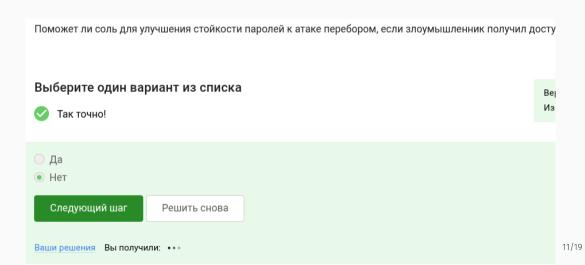
Капча смотрит подозрительные действия и спрашивает, робот вы или нет.

Зачем нужна капча?				
Выберите один вариант из списка				
Отличное решение!	Из			
Она заменяет пароли				
 Для безопасного хранения паролей на сервере 				
Для защиты от автоматизированных атак, направленных на получение несанкционированного доступ	a			
Для защиты кук пользователя				
Следующий шаг Решить снова				

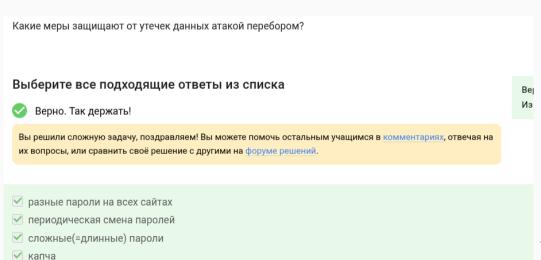
Для их безопасности. хэш сложно взломать.

Для чего применяется хэширование паролей?				
D. C				
Выберите один вариант из списка				
Правильно, молодец!	Из			
 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				

Не поможет.



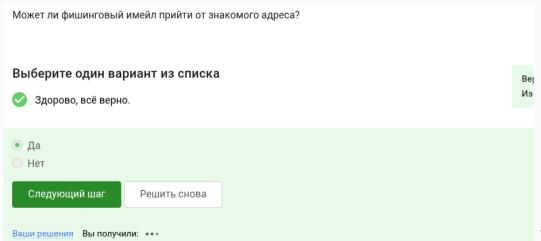
Все перечисленные варианты весьма эфеективны.



Есть отличия от оригинальных ссылок у сбера и яндекса.

Какие из следующих ссылок являются фишинговыми?	
Выберите все подходящие ответы из списка	Bej
Хорошие новости, верно!	Из
Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на	
их вопросы, или сравнить своё решение с другими на форуме решений.	
https://accounts.google.com.br/signin/v2/identifier?hl=ru (страница входа в аккаунт Google)	
✓ https://online.sberbank.wix.ru/CSAFront/index.do (вход в Сбербанк.Онлайн)	
☐ https://e.mail.ru/login?lang=ru_RU (вход в аккаунт Mail.Ru)	
https://pagpart.vanday.usaz.ru/auth?arigin=hama_daaktan_ru/ayan_n_ayyayuTuunaya	

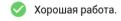
Да, знакомый адрес могут взломать.



От английского spoof — обман, подделка.

Email Спуфинг -- это

Выберите один вариант из списка

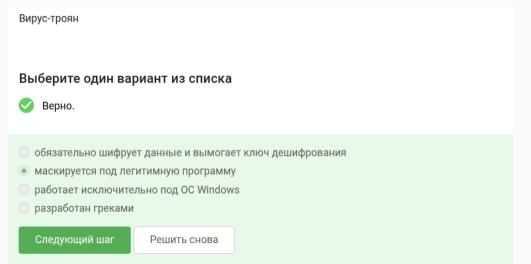


- подмена адреса отправителя в имейлах
- 🔾 метод предотвращения фишинга
- 🔾 атака перебором паролей
- 🔾 протокол для отправки имейлов

Следующий шаг

Решить снова

На то он и троян, что маскируется и сразу не поймёшь, что это вирус.



Сразу же при первом сообщении.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка



Верно. Так держать!

- при установке приложения
- при генерации первого сообщения стороной-отправителем
- 🔘 при каждом новом сообщении от стороны-отправителя
- при получении сообщения

Данные в зашифрованном виде передаются по узлам.

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка



Отлично!

- 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

Выводы

Выводы

Все задания выполнены.