

Второй этап внешнего курса

Основы информационной безопасности

Казазаев Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- [1132231427@rudn.ru]
- https://github.com/KazazaevDaniil/study_2024-2025_infosec-intro

Вводная часть

Внешний кур состоит из трех этапов.

Первый этап курса состоит из 5 частей:

1. Шифрование диска
2. Пароли
3. Фишинг
4. Вирусы
5. Безопасность мессенджеров

Выполнение второго этапа
внешнего курса.

Шифрование диска

Загрузочный сектор диска можно зашифровать. (рис. 1)

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Всё правильно.

☐ Да

☐ Нет

Следующий шаг

Решить снова

Рис. 1: Первый вопрос

Симметричное шифрование - основа шифрования диска. (рис. 2)

Шифрование диска основано на

Выберите один вариант из списка

☒ Верно.

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

Рис. 2: Второй вопрос

BitLocker - шифратор ОС Windwos, VeraCrypt - утилита для шифрования. (рис. 3)

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

Верно решено
Из всех предложенных

✓ Верно. Так держать!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими [решений](#).

- ☐ Wireshark
- ☐ Disk Utility
- ☒ BitLocker
- ☒ VeraCrypt

Следующий шаг

Решить снова

Рис. 3: Третий вопрос

Пароли

Хороший пароль тот, который является нестандартным и его сложно подобрать. (рис. 4)

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

☒ Правильно, молодец!

☐ qwerty12345

☐ ILOVECATS

☒ UQr9@j4!S\$

☐ IDONTLOVECATS

Следующий шаг

Решить снова

Рис. 4: Первый вопрос

Лучше всего хранить пароли в менеджерах паролей, так как они обеспечены большей степенью защиты. (рис. 5)

Где безопасно хранить пароли?

Выберите один вариант из списка



Всё получилось!

- ☒ В менеджерах паролей
- ☐ В заметках на рабочем столе
- ☐ В заметках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг

Решить снова

Капчк нужна для предотвращения автоматизированных атак, которые могут подобрать пароль автоматически.(рис. 6)

Зачем нужна капча?

Выберите один вариант из списка

Верно решили **974** учащихся
Из всех попыток **77%** верно

✓ Прекрасный ответ.

- ☐ Для защиты кук пользователя
- ☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа
- ☐ Она заменяет пароли
- ☐ Для безопасного хранения паролей на сервере

Следующий шаг Решить снова

Рис. 6: Третий вопрос

Хеширование необходимо, чтобы защитить пароль, а не хранить его на сервере в открытом виде.(рис. 7)

Для чего применяется хэширование паролей?

Выберите один вариант из списка

Верно решили!
Из всех попыток

✔ 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

Рис. 7: Четвертый вопрос

Если злоумышленник получил доступ к серверу, метод соли не поможет от перебора паролей.(рис. 8)

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?

Верно решили **967** учащихся
Из всех попыток **66%** верно

Выберите один вариант из списка

☒ Всё получилось!

☐ Да

☒ Нет

Следующий шаг

Решить снова

Рис. 8: Пятый вопрос

Все перечисленные методы хороши для защиты пароля.(рис. 9)

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Верно р
Из всех

☒ Хорошая работа.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных [комментариях](#), отвечая на их вопросы, или сравнить своё решение с [решений](#).

- ☒ разные пароли на всех сайтах
- ☒ периодическая смена паролей
- ☒ сложные(=длинные) пароли
- ☒ капча

Следующий шаг

Решить снова

Рис. 9: Шестой вопрос

Фишинг



Фишинговыми ссылками являются те, у которых домене есть непонятные симфолы или слова.(рис. 10)

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно решил **861** учащийся
Из всех попыток **19%** верно

☒ Так точно!

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://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

Следующий шаг Решить снова

Рис. 10: Первый вопрос

Фишинговая ссылка может прийти от знакомого пользователя, так как существует метод Спуфинга, когда злоумышленник подделывает адрес. (рис. 11)

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Верно.

☐ Да

☐ Нет

Следующий шаг

Решить снова

Верно
Из всех

Рис. 11: Второй вопрос

Вирусы

Спуфинг - подмена адреса отправителя. (рис. 12)

Email Спуфинг – это

Выберите один вариант из списка



Всё получилось!

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

Следующий шаг

Решить снова

Рис. 12: Первый вопрос

Вирус Троян - вирус, который маскируется под обычный файл, но внутри у него вредоносный код. (рис. 13)

Вирус-троян

Выберите один вариант из списка

Верно решили 4
Из всех попыток

☒ Так точно!

- ☐ обязательно шифрует данные и вымогает ключ дешифрования
- ☒ маскируется под легитимную программу
- ☐ работает исключительно под ОС Windows
- ☐ разработан греками

Следующий шаг Решить снова

Рис. 13: Второй вопрос

Безопасность мессенджеров

Ключ шифрования Signal формируется на этапе генерации сообщения со стороны-отправителя. (рис. 14)

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Верно решили **952** учащихся
Из всех попыток **52%** верно

✓ Всё получилось!

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

Следующий шаг Решить снова

Рис. 14: Первый вопрос

Суть сквозного шифрования в передаче сообщения по узлам связи в зашифрованном виде.
(рис. 15)

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

Верно решили **964** учащихся
Из всех попыток **60%** верно

☒ Отличное решение!

- ☒ 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
- ☐ сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг Решить снова

Рис. 15: Второй вопрос

Вывод

Выполнен второй этап внешнего курса