

Прохождение внешних курсов

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

1	Цель работы	6
2	Безопасность в сети	7
2.1	Как работает интернет базовые сетевые протоколы	7
2.2	Персонализация сети	11
2.3	Браузер TOR. Анонимизация	13
2.4	Беспроводные сети Wi-fi	15
3	Защита ПК/телефона	19
3.1	Шифрование диска	19
3.2	Пароли	20
3.3	Фишинг	23
3.4	Вирусы. Примеры	24
3.5	Безопасность мессенджеров	25
4	Криптография на практике	26
4.1	Введение в криптографию	26
4.2	Цифровая подпись	28
4.3	Электронные платежи	30
4.4	Блокчейн	31
5	Выводы	33

Список иллюстраций

2.1	Задание 1.1.1	7
2.2	Задание 1.1.2	8
2.3	Задание 1.1.3	8
2.4	Задание 1.1.4	9
2.5	Задание 1.1.5	9
2.6	Задание 1.1.6	10
2.7	Задание 1.1.7	10
2.8	Задание 1.1.8	11
2.9	Задание 1.1.9	11
2.10	Задание 1.2.1	12
2.11	Задание 1.2.2	12
2.12	Задание 1.2.3	13
2.13	Задание 1.2.4	13
2.14	Задание 1.3.1	14
2.15	Задание 1.3.2	14
2.16	Задание 1.3.3	15
2.17	Задание 1.3.4	15
2.18	Задание 1.4.1	16
2.19	Задание 1.4.2	16
2.20	Задание 1.4.3	17
2.21	Задание 1.4.4	17
2.22	Задание 1.4.5	18
3.1	Задание 2.1.1	19
3.2	Задание 2.1.2	19
3.3	Задание 2.1.3	20
3.4	Задание 2.2.1	20
3.5	Задание 2.2.2	21
3.6	Задание 2.2.3	21
3.7	Задание 2.2.4	22
3.8	Задание 2.2.5	22
3.9	Задание 2.2.6	23
3.10	Задание 2.3.1	23
3.11	Задание 2.3.2	24
3.12	Задание 2.4.1	24
3.13	Задание 2.4.2	24
3.14	Задание 2.5.1	25

3.15 Задание 2.5.2	25
4.1 Задание 3.1.1	26
4.2 Задание 3.1.2	27
4.3 Задание 3.1.3	27
4.4 Задание 3.1.4	27
4.5 Задание 3.1.5	28
4.6 Задание 3.2.1	28
4.7 Задание 3.2.2	29
4.8 Задание 3.2.3	29
4.9 Задание 3.2.4	29
4.10 Задание 3.2.5	30
4.11 Задание 3.3.1	30
4.12 Задание 3.3.2	31
4.13 Задание 3.3.3	31
4.14 Задание 3.4.1	32
4.15 Задание 3.4.2	32
4.16 Задание 3.4.3	32

Список таблиц

1 Цель работы

Познакомиться с основами кибербезопасности

2 Безопасность в сети

2.1 Как работает интернет базовые сетевые протоколы

1. Протоколом прикладного уровня является протокол HTTPS, он отвечает за работу с приложениями. (рис. 2.1)

2.1 Как работает интернет: базовые сетевые протоколы 7 из 15 шагов пройдено 1 из 9 баллов получен

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.1: Задание 1.1.1

2. Протокол TCP отвечает за передачу данных внутри одной машины, следовательно, он работает на транспортном уровне. (рис. 2.2)

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Правильно.

Верно решили **939** учащихся
Из всех попыток **61%** верных

- ☒ Транспортном
- ☐ Прикладном
- ☐ Канальном
- ☐ Сетевом

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 из 1

Рис. 2.2: Задание 1.1.2

3. Адреса IPv4 состоит из 4 чисел от 0 до 255. (рис. 2.3)

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

☒ Все правильно.

Верно решил **871** учащихся
Из всех попыток **23%** верных

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](#).

- ☐ 421.0.15.19
- ☐ 43.12.256.7
- ☒ 90.11.90.22
- ☒ 25.198.0.15

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.3: Задание 1.1.3

4. Функция DNS сервера является: сопоставить доменный и IP адреса. (рис. 2.4)

DNS сервер

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 933 учащихся
Из всех попыток 66% верных

- ☒ сопоставляет IP адреса доменным именам
- ☐ сегментирует данные на транспортном уровне
- ☐ выбирает маршрут пакета в сети
- ☐ выполняет адресацию на хосте

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.4: Задание 1.1.4

5. Модель TCP/IP состоит из следующих уровней: прикладной(работа с приложением) - транспортный(передача информации внутри машины) - сетевой(передача информации по сети) - канальный(работа с информацией на физическом уровне). (рис. 2.5)

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Правильно.

Верно решил 941 учащийся
Из всех попыток 53% верных

- ☐ сетевой – прикладной – канальный – транспортный
- ☐ прикладной – транспортный – канальный – сетевой
- ☐ транспортный – сетевой – прикладной – канальный
- ☒ прикладной – транспортный – сетевой – канальный

Следующий шаг

Решить снова

Ваши решения Вы получили: ... из 1

Рис. 2.5: Задание 1.1.5

6. Протокол HTTP предполагает передачу данных в открытом виде, а протокол HTTPS, который использует TLS, передает зашифрованные данные. (рис. 2.6)

2.1 Как работает интернет: базовые сетевые протоколы 12 из 15 шагов пройдено 6 из 9 баллов получено

Протокол http предполагает

Выберите один вариант из списка

Верно решили **965** учащихся
Из всех попыток **78%** верных

☒ Верно. Так держаты!

☐ передачу зашифрованных данных между клиентом и сервером

☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 2.6: Задание 1.1.6

7. Так как http не использует TLS при передаче данных, то этот протокол состоит из двух фаз: рукопожатие и передача данных. (рис. 2.7)

2.1 Как работает интернет: базовые сетевые протоколы 13 из 15 шагов пройдено 7 из 9 баллов получено

Протокол https состоит из

Выберите один вариант из списка

Верно решили **948** учащихся
Из всех попыток **41%** верных

☒ Всё получилось!

☐ одной фазы аутентификации сервера

☒ двух фаз: рукопожатия и передачи данных

☐ двух фаз: аутентификация клиента и сервера и шифрования данных

☐ трех фаз: аутентификация клиента, аутентификация сервера, генерация общего ключа

Следующий шаг Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 2.7: Задание 1.1.7

8. Версию TLS клиент и сервер определяют во время 'переговоров'. (рис. 2.8)

2.1 Как работает интернет: базовые сетевые протоколы 14 из 15 шагов пройдено 8 из 9 баллов получено

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 947 учащихся
Из всех попыток 55% верных

- ☐ сервером
- ☐ клиентом
- ☒ и клиентом, и сервером в процессе "переговоров"
- ☐ провайдером клиента

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.8: Задание 1.1.8

9. В протоколе TLS шифрование данных предусмотрено в фазе: "Данных" (рис. 2.9)

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Отлично!

Верно решил 931 учащийся
Из всех попыток 44% верных

- ☐ формирование общего секретного ключа между клиентом и сервером
- ☐ аутентификация (как минимум одной из сторон)
- ☐ выбираются алгоритмы шифрования/аутентификации
- ☒ шифрование данных

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.9: Задание 1.1.9

2.2 Персонализация сети

1. Куки хранят id пользователя и id сессии, а также информацию о действиях пользователя на сайте. (рис. ??)

Куки хранят:

Выберите все подходящие ответы из списка

✓ Всё получилось!

Верно решили 856 учащихся
Из всех попыток 18% верных

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](#).

- ☐ IP адрес
- ☒ идентификатор пользователя
- ☒ id сессии
- ☐ пароль пользователя

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.10: Задание 1.2.1

2. Куки не используются для улучшения надежности соединения, они служат для того, чтобы сохранять информацию о сессии на сервере. (рис. ??)

Куки не используются для

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 950 учащихся
Из всех попыток 53% верных

- ☐ аутентификации пользователя
- ☐ персонализации веб-страниц
- ☐ отслеживания информации о пользователе
- ☐ сборе статистики посещаемости сайта
- ☒ улучшения надежности соединения

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.11: Задание 1.2.2

3. Сервер генерирует куки и возвращает их вместе с ответом на запрос. (рис. ??)

2.2 Персонализация сети 5 из 6 шагов пройдено 3 из 4 баллов получено

Куки генерируются

Выберите один вариант из списка

✓ Правильно.

Верно решили 968 учащихся
Из всех попыток 79% верных

☒ сервером
☐ клиентом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.12: Задание 1.2.3

4. Куки бывают сессионные и постоянные, первые хранятся на сервере и удаляются после закрытия сайта. (рис. 2.13)

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 959 учащихся
Из всех попыток 60% верных

☐ Да, на некоторое время, заданное в сервере
☒ Да, на время пользования веб-сайтом
☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.13: Задание 1.2.4

2.3 Браузер TOR. Анонимизация

1. В луковой маршрутизации существует три узла: охранный, промежуточный и выходной. (рис. 2.14)

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2
☒ 3
☐ 4

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.14: Задание 1.3.1

2. В луковой маршрутизации IP адрес получателя известен: отправителю и выходному узлу. (рис. 2.15)

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Отлично!

Верно решили 906 учащихся
Из всех попыток 19% верных

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](#).

☐ охранному узлу
☐ промежуточному узлу
☒ отправителю
☒ выходному узлу

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.15: Задание 1.3.2

3. Отправитель генерирует три общих секретных ключа: для охранного узла, для промежуточного и для выходного. (рис. 2.16)

2.3 Браузер TOR. Анонимизация 5 из 6 шагов пройдено 3 из 4 баллов получено

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 959 учащихся
Из всех попыток 55% верных

☐ только с охраным узлом
 ☐ с охраным и промежуточным узлом
 ☒ с охраным, промежуточным и выходным узлом
 ☐ с промежуточным и выходным узлом

Следующий шаг
 Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.16: Задание 1.3.3

4. Браузер Tor используется для анонимизации, а не для гарантии успешного получения пакетов. (рис. 2.17)

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Должен ли получатель использовать браузер Тор (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решил 961 учащийся
Из всех попыток 74% верных

☐ Да
 ☒ Нет

Следующий шаг
 Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 2.17: Задание 1.3.4

2.4 Беспроводные сети Wi-fi

1. Wi-fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11. (рис. 2.18)

2.4 Беспроводные сети Wi-Fi 4 из 8 шагов пройдено 1 из 5 баллов получен

Wi-Fi - это

Выберите один вариант из списка

Верно решили 965 учащихся
Из всех попыток 79% верных

☒ Так точно!

☐ сокращение от "wireless fiber"

☒ технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11

☐ метод соединения компьютеров по проводной сети Ethernet

☐ метод подключения смартфона с глобальной сети Интернет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.18: Задание 1.4.1

2. Протокол Wi-fi работает на самом низком канальном уровне, как Ethernet.
(рис. 2.19)

2.4 Беспроводные сети Wi-Fi 5 из 8 шагов пройдено 2 из 5 баллов получено

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

Верно решили 972 учащихся
Из всех попыток 58% верных

☒ Верно. Так держать!

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.19: Задание 1.4.2

3. WEP является небезопасным методом шифрования, так как имеет очень короткую длину ключа. (рис. 2.20)

2.4 Беспроводные сети Wi-Fi 6 из 8 шагов пройдено 3 из 5 баллов получено

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.20: Задание 1.4.3

4. Данные между хостом сети и роутером передаются в зашифрованном виде, после аутентификации, чтобы их нельзя было перехватить. (рис. 2.21)

2.4 Беспроводные сети Wi-Fi 7 из 8 шагов пройдено 4 из 5 баллов получено

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 975 учащихся
Из всех попыток 53% верных

☒ передаются в зашифрованном виде после аутентификации устройств
☐ передаются в открытом виде
☐ передаются в открытом виде после аутентификации устройств
☐ передаются в зашифрованном виде

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.21: Задание 1.4.4

5. Для домашней сети для аутентификации обычно используется метод Personal(подключение по паролю), второй метод используется для больших корпоративных сетей, он проверяет есть ли пользователь в базе данных. (рис. 2.22)

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 975 учащихся
Из всех попыток 87% верных

☒ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.22: Задание 1.4.5

3 Защита ПК/телефона

3.1 Шифрование диска

1. Можно зашифровать любой сектор диска. (рис. 3.1)

3.1 Шифрование диска 4 из 5 шагов пройдено 2 из 3 баллов получено

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Отлично!

Верно решили 949 учащихся
Из всех попыток 89% верных

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.1: Задание 2.1.1

2. Для шифрования диска используется симметричное шифрование, то есть один секретный ключ для шифрования и дешифрования данных. (рис. 3.2)

3.1 Шифрование диска 4 из 5 шагов пройдено 2 из 3 баллов получено

Шифрование диска основано на

Выберите один вариант из списка

☒ Правильно.

Верно решили 972 учащихся
Из всех попыток 66% верных

☐ хэшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.2: Задание 2.1.2

3. BitLocker - для Windows, в Linux – LUKS, в MacOS – это FileVault. (рис. 3.3)

3.1 Шифрование диска 5 из 5 шагов пройдено 3 из 3 баллов получено

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Хорошие новости, верно!

Верно решили 906 учащихся
Из всех попыток 28% верных

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](#).

☐ Wireshark
☐ Disk Utility
☒ BitLocker
☒ VeraCrypt

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.3: Задание 2.1.3

3.2 Пароли

1. Стойкий пароль не должен быть коротким и должен состоять из различных символов, букв разного регистра и цифр. (рис. 3.4)

Какие пароли можно отнести к стойким?

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 969 учащихся
Из всех попыток 85% верных

☐ qwerty12345
☐ ILOVECATS
☒ UQr9@j4!\$\$
☐ IDONTLOVECATS

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.4: Задание 2.2.1

2. Пароли необходимо хранить в безопасном месте, чтобы их не смогли обнаружить случайно, например, в менеджерах для паролей. (рис. 3.5)

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решил 971 учащихся
Из всех попыток 74% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 3.5: Задание 2.2.2

3. Капча используется для предотвращения запросов к серверу со стороны ботов, что затрудняет автоматизированный перебор паролей. (рис. 3.6)

Зачем нужна капча?

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 974 учащихся
Из всех попыток 77% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 3.6: Задание 2.2.3

4. Хэширование паролей используется серверами, чтобы не хранить пароль в открытом виде, а вместо него хранить результат применения хэш-функции к паролю. (рис. 3.7)

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Правильно.

Верно решили 973 учащихся
Из всех попыток 61% верных

- ☐ 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

Ваши решения Вы получили: 1 балл из 1

Рис. 3.7: Задание 2.2.4

5. Ответ нет, так как соль используется для того, чтобы не хранить результат хэширования часто используемого пароля, так как если злоумышленник получит доступ к серверу, где хранятся хэш-пароли, он сразу поймет прообраз хэширования. (рис. 3.8)

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

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 967 учащихся
Из всех попыток 66% верных

- ☐ Да
- ☒ Нет

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 3.8: Задание 2.2.5

6. От атак перебором помогают следующие действия: капча, длинные и сложные пароли, различные пароли, периодическая смена паролей. (рис. 3.9)

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Верно решили **895** учащихся
Из всех попыток **16%** верных

✓ Абсолютно 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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 3.9: Задание 2.2.6

3.3 Фишинг

1. В данном задании рассматривается такой тип фишинговых атак, как адресный фишинг, когда мы вроде бы переходим на известную нам страницу, но она является поддельной. (рис. 3.10)

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Верно решил **861** учащихся
Из всех попыток **19%** верных

✓ Здорово, всё верно.

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

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 3.10: Задание 2.3.1

2. Да такое возможно, это называет спуфинг, это происходит, потому что SMTP не включает в себя проверку адреса отправителя. (рис. 3.11)

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Всё получилось!

Верно решили **966** учащихся
Из всех попыток **90%** верных

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 3.11: Задание 2.3.2

3.4 Вирусы. Примеры

1. Email спуфинг - это подмена адреса отправителя в емейлах. (рис. 3.12)

Email Спуфинг – это

Выберите один вариант из списка

☒ Отличное решение!

Верно решили **960** учащихся
Из всех попыток **65%** верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 3.12: Задание 2.4.1

2. Троян - это вирус, который маскируется под легитимное ПО. (рис. 3.13)

Вирус-троян

Выберите один вариант из списка

☒ Отлично!

Верно решили **969** учащихся
Из всех попыток **74%** верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 3.13: Задание 2.4.2

3.5 Безопасность мессенджеров

1. В протоколе мессенджеров Signal ключ формируется при генерации первого сообщения стороной-отправителем. (рис. 3.14)

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 952 учащихся
Из всех попыток 52% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.14: Задание 2.5.1

2. Суть сквозного шифрования состоит в том, что отправитель передает на сервер уже зашифрованное сообщение, сервер отправляет зашифрованные данные получателю, а тот их дешифрует, таким образом сервер знает только куда надо передать сообщение. (рис. 3.15)

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 964 учащихся
Из всех попыток 60% верных

- ☒ 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

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 3.15: Задание 2.5.2

4 Криптография на практике

4.1 Введение в криптографию

1. В асимметричных криптографических примитивах обе стороны имеют пару ключей - публичный и секретный. (рис. 4.1)

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 940 учащихся
Из всех попыток 42% верных

☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете

☒ обе стороны имеют пару ключей

☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей

☐ обе стороны имеют общий секретный ключ

Следующий шаг Решить снова

Рис. 4.1: Задание 3.1.1

2. Криптографическая хэш-функция обладает следующими свойствами: возвращает последовательность бит фиксированной длины, устойчива к коллизиям и эффективно вычисляется. (рис. 4.2)

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили **798** учащихся
Из всех попыток **11%** верных

✓ Правильно.

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](#).

- ☒ стойкая к коллизиям
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ эффективно вычисляется
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 4.2: Задание 3.1.2

3. К алгоритмам цифровой подписи относятся: RSA, американский стандарт ECDSA, российский стандарт ГОСТ Р 34.10-2012. (рис. 4.3)

Выберите все подходящие ответы из списка

Верно решили **834** учащихся
Из всех попыток **19%** верных

✓ Всё получилось!

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](#).

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

[Следующий шаг](#) [Решить снова](#)

Рис. 4.3: Задание 3.1.3

4. Код аутентификации сообщения относится к симметричным примитивам. (рис. 4.4)

Код аутентификации сообщения относится к

Выберите один вариант из списка

Верно решили **955** учащихся
Из всех попыток **69%** верных

✓ Отличное решение!

- ☒ симметричным примитивам
- ☐ асимметричным примитивам

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 4.4: Задание 3.1.4

5. Обмен ключам Диффи-Хэллмана - это ассиметричный примитив, который используется для генерации общего секретного ключа. (рис. 4.5)

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 948 учащихся
Из всех попыток 47% верных

- ☐ симметричный примитив генерации общего секретного ключа
- ☐ асимметричный примитив генерации общего открытого ключа
- ☒ асимметричный примитив генерации общего секретного ключа
- ☐ асимметричный алгоритм шифрования

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4.5: Задание 3.1.5

4.2 Цифровая подпись

1. Протокол электронной цифровой подписи относится к ассиметричным протоколам, то есть с публичным и секретным ключами. (рис. 4.6)

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 932 учащихся
Из всех попыток 71% верных

- ☐ протоколом с симметричным ключом
- ☒ протоколом с публичным (или открытым) ключом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4.6: Задание 3.2.1

2. Алгоритм верификации электронной цифровой подписи требует на вход три вещи - это подпись, сообщение и открытый ключ. (рис. 4.7)

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 926 учащихся
Из всех попыток 46% верных

- ☐ подпись, секретный ключ, сообщение
- ☒ подпись, открытый ключ, сообщение
- ☐ подпись, секретный ключ
- ☐ подпись, открытый ключ

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 4.7: Задание 3.2.2

3. Электронная цифровая подпись не обеспечивает конфиденциальности - она используется для аутентификации, проверки на целостность и неотказ от авторства. (рис. 4.8)

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 927 учащихся
Из всех попыток 52% верных

- ☒ конфиденциальность
- ☐ аутентификацию
- ☐ целостность
- ☐ неотказ от авторства

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 4.8: Задание 3.2.3

4. Для отправки налоговой отчетности в ФНС необходимо использовать усиленную квалифицированную подпись. (рис. 4.9)

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 927 учащихся
Из всех попыток 68% верных

- ☐ простая
- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 4.9: Задание 3.2.4

5. Квалифицированный сертификат можно получить в сертификационном центре. (рис. 4.10)

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решили 925 учащихся
Из всех попыток 60% верных

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4.10: Задание 3.2.5

4.3 Электронные платежи

1. Выбираем платежные системы MasterCard и МИР. (рис. 4.11)

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Хорошая работа.

Верно решили 856 учащихся
Из всех попыток 23% верных

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](#).

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Следующий шаг Решить снова

Рис. 4.11: Задание 3.3.1

2. Примером многофакторной аутентификации является то, что я выбрал. (рис. 4.12)

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Хорошие новости, верно!

Верно решили 842 учащихся
Из всех попыток 23% верных

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](#).

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверка пароля + код в sms сообщении
- ☒ комбинация код в sms сообщении + отпечаток пальца
- ☐ комбинация PIN код + пароль

Следующий шаг Решить снова

Рис. 4.12: Задание 3.3.2

- При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 4.13)

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Так точно!

Верно решил 901 учащийся
Из всех попыток 59% верных

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ однофакторная аутентификация покупателя перед банком-эквайером
- ☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- ☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг Решить снова

Рис. 4.13: Задание 3.3.3

4.4 Блокчейн

- В доказательстве работы используется сложность вычисления прообраза хэш-функции, так как единственным эффективным способом атаки на хэш-функцию является перебор. (рис. 4.14)

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Верно решили 915 учащихся
Из всех попыток 49% верных

☒ Отличное решение!

☐ фиксированная длина выходных данных

☒ сложность нахождения прообраза

☐ обеспечение целостности

☐ эффективность вычисления

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4.14: Задание 3.4.1

2. Консенсус в некоторых системах блокчейн обладает свойствами - живучесть, консенсус, постоянства, открытость. (рис. 4.15)

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решили 826 учащихся
Из всех попыток 22% верных

☒ Верно.

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](#).

☒ живучесть

☒ консенсус

☒ постоянства

☒ открытость

Следующий шаг Решить снова

Рис. 4.15: Задание 3.4.2

3. Участники блокчейна хранят секретные ключи электронной подписи, которые используют для подписи транзакций. (рис. 4.16)

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Верно решили 913 учащихся
Из всех попыток 47% верных

☒ Правильно.

☐ обмен ключами

☐ шифрование

☒ цифровая подпись

☐ хэш-функция

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4.16: Задание 3.4.3

5 Выводы

Были изучены основы кибербезопасности.