

Отчёт по прохождению контрольных мероприятий дополнительного курса

Основы информационной безопасности

Соловьев Богдан НКАбд-04-23

Содержание

2. Вторая глава

3. Третья глава

4. Четвёртая глава

Вторая глава: Безопасность в сети

Выберите протокол прикладного уровня

Выберите один вариант из списка

☒ Верно. Так держать!

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

UDP (User Datagram Protocol) — это один из основных протоколов для передачи данных в сети. Он не нуждается в установлении соединения перед передачей данных и не гарантирует их доставку.

Проще говоря, UDP используется в случаях, когда важнее снизить задержки, чем обеспечить полную надёжность доставки.

TCP (Transmission Control Protocol) — протокол обмена сообщениями в сети Интернет. Он управляет отправкой данных и следит за тем, чтобы они дошли до получателя в целости.

HTTP (HyperText Transfer Protocol) — это протокол для передачи информации в интернете. Он является основой для обмена информацией между веб-браузерами и серверами.

С помощью HTTP пользователи получают доступ к веб-страницам, загружают файлы и отправляют данные через интернет.

На каком уровне работает протокол TCP?



Выберите один вариант из списка



Отлично!

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

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка



Отличное решение!



Вы решили сложную задачу, поздравляем! Вы можете помочь остальных вопросы, или сравнить своё решение с другими на [форуме реп](#)

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Значения не могут превышать 255 в десятичной системе исчисления

DNS сервер

Выберите один вариант из списка



Отлично!




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

Следующий шаг

Решить снова

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

 Отлично!

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

Следующий шаг

Решить  ова

Корректная последовательность уровней системы протоколов TCP/IP выглядит следующим образом:

Канальный уровень. Отвечает за взаимодействие по сетевому оборудованию, например по Ethernet-кабелю или Wi-Fi. Примеры протоколов: Ethernet, Wi-Fi, Bluetooth.

Межсетевой уровень. Помогает отдельным сетям общаться друг с другом. Основной протокол — IP (Internet Protocol). Здесь также работают такие дополнительные протоколы, как ICMP, ARP и DNS.

Транспортный уровень. Отвечает за передачу данных между устройствами, например, по протоколам TCP и UDP.

Прикладной уровень. Помогает приложениям общаться друг с другом с помощью интерфейсов или API. Содержит набор протоколов, которые отвечают за работу различных сервисов, таких как HTTP для веб-страниц, SMTP для электронной почты и FTP для передачи файлов.

Протокол http предполагает



Выберите один вариант из списка



Так точно!

- ☐ 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**

Протокол https состоит из

Выберите один вариант из списка

☒ Верно.

- ☐ одной фазы аутентификации сервера
- ☒ двух фаз: рукопожатия и передачи данных
- ☐ двух фаз: аутентификация клиента и сервера и шифрования данных
- ☐ трех фаз: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

HTTP (HyperText Transfer Protocol) — это протокол прикладного уровня, который используется для передачи данных в сети Интернет. Он определяет правила и формат обмена данными между клиентом (например, веб-браузером) и сервером

Версия протокола TLS определяется

Выберите один вариант из списка

☒ Правильно.

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

Следующий шаг

Решить снова

В фазе "рукопожатия" протокола TLS не предусмотрено



Выберите один вариант из списка

☒ Всё получилось!

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

В фазе рукопожатия происходит:

1. выбор параметров, протоколов
2. аутентификация (как минимум, сервера)
3. формируется общий секретный ключ K

Куки хранят:

Выберите все подходящие ответы из списка

☒ Абсолютно точно.

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

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

Куки не используются для

Выберите один вариант из списка

☒ Абсолютно точно.

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

Сбор куки упрощает и делает комфортным взаимодействие с веб-ресурсом. Благодаря им не требуется заново заходить в свой аккаунт в соцсетях или собирать корзину в интернет-магазинах.

Какую информацию собирают куки-файлы:

Учётные данные. Cookies помогают отмечать, что пользователь уже был авторизован ранее. Благодаря этому не нужно каждый раз заново входить в личный кабинет при открытии или обновлении страницы. Даже если у пользователя нет учётной записи, сайт может присвоить ему уникальный идентификатор, чтобы в следующий раз «узнать» посетителя.

Персональные настройки. Сайты запоминают выбранный город, язык, товары в корзине, валюту и масштаб страницы. Эти данные собирают интернет-магазины. Они нужны, чтобы автоматически подставлять нужную валюту, город доставки и содержимое корзины с товарами. Благодаря этому пользователи могут в любой момент быстро продолжить покупки.

Куки генерируются

Выберите один вариант из списка

☒ Правильно, молодец!

☐ клиентом

☒ сервером

Куки генерируются сервером, чтобы запомнить пользователя и показать ему ответ в соответствии с его предпочтениями при повторном посещении веб-сайта

Сессионные куки хранятся в браузере?



Выберите один вариант из списка

☒ Всё правильно.

☐ Да, на некоторое время, заданное в сервером

☐ Нет

☒ Да, на время пользования веб-сайтом

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Так точно!

☐ 2

☒ 3

☐ 4

количество узлов задано жёстко в коде программы и не изменяется через конфигурационные файлы. Длина цепочки из трёх узлов оптимальна, так как наиболее опасными считаются атаки пересечения, которые эффективны при съёме трафика с начального узла (или перед ним) и с конечного узла (или после него).

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Прекрасный ответ.

Вы решили сложную задачу, поздравляем! Вы можете помочь о
их вопросы, или сравнить своё решение с другими на [форуме рк](#)

- ☐ охранному узлу
- ☐ промежуточному узлу
- ☒ отправителю
- ☒ выходному узлу

Узлы разделяются на охранный узел, промежуточный и выходной. Соответственно выходной узел, поскольку он является узлом перед получателем, знает, кому направлен пакет.

Охранный узел знает, от кого пришёл пакет, поскольку он непосредственно является следующим узлом после отправителя, в то время как промежуточный узел не знает ни от кого этот пакет, ни кому он предназначен. В браузере Tor всегда есть три роутера, их не больше и не меньше. Их не меньше потому, что меньшего числа узлов не хватает для анонимизации, а большее число узлов не дает большую анонимизацию, поэтому выбирается всегда 3 луковых роутера.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка




Хорошие новости, верно!

- ☐ только с охранным узлом
- ☐ с охранным и промежуточным узлом
- ☒ с охранным, промежуточным и выходным узлом
- ☐ с промежуточным и выходным узлом

пояснение выше

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

Выберите один вариант из списка

☒ Прекрасный ответ. 

Верно решил **961** учащихся
Из всех попыток **74%** верно

☐ Нет

☐ Да

Получателю не обязательно использовать браузер Tor или другой луковый браузер для успешного получения пакетов.

Tor скрывает маршрутизацию и обеспечивает анонимность, но сам протокол передачи данных (например, TCP/IP) работает независимо от того, использует ли получатель Tor. Главное — чтобы отправитель правильно указал адрес получателя, а сеть обеспечила доставку пакетов.

Wi-Fi - это

Выберите один вариант из списка



Абсолютно 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

Можно догаться методом исключения

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

☒ Верно.

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Канальный уровень — это второй уровень модели OSI, который объединяет устройства в одной локальной сети, например компьютеры, принтеры и коммутаторы. Его функция — правильно передать данные между этими узлами.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

 Отличное решение!

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

WEP (Wired Equivalent Privacy) — один из старейших протоколов безопасности беспроводных сетей. Он был разработан в конце 1990-х годов как способ защиты беспроводных сетей и призван обеспечить уровень безопасности, эквивалентный проводным сетям.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка


☒ Здорово, всё верно.

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

В большинстве домашних и офисных сетей данные между устройством (компьютером, смартфоном) и роутером передаются в открытом виде, если не используется дополнительное шифрование

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

 Отлично!

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Enterprise используется когда есть база данных пользователей

Третья глава: Защита ПК/телефона

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Хорошая работа.



☐ Да

☐ Нет

Можно

Шифрование диска основано на

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Симметричное шифрование — это метод, при котором для шифрования и дешифрования данных используется один и тот же ключ. То есть и отправитель, и получатель информации должны иметь одинаковый секретный ключ, чтобы зашифровать и расшифровать сообщения.

Асимметричное шифрование — это метод, в котором используются два ключа: открытый (публичный) и закрытый (приватный). 12 Открытый ключ используется для шифрования, а закрытый — для дешифрования. В отличие от симметричного метода, ключи не совпадают, что делает возможным обмен информацией без предварительного обмена секретами

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Хорошая работа.

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

☒ VeraCrypt

☒ BitLocker

☐ Wireshark

☐ Disk Utility

Wireshark — бесплатная профессиональная программа для анализа сетевой активности, изучения пакетов, просмотра сетевой статистики и составления отчётов.

Disk Utility — утилита для работы с файловыми системами жёстких и оптических дисков в macOS. Но зашифровать не получится с её помощью

Какие пароли можно отнести с стойким?

Выберите один вариант из списка


☒ Отлично!

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

Хороший пароль должен содержать цифры, буквы в разных регистрах, специальные знаки и быть длинным

Где безопасно хранить пароли?

Выберите один вариант из списка

 **Правильно, молодец!**

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

Пароли нельзя хранить в заметках, потому что эти программы никак дополнительно не защищены, в кошельке и на стикере не стоит хранить, потому что, по личному опыту, легко потерять

Зачем нужна капча?

Выберите один вариант из списка

☒ Верно.

Верно
Из всех

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

Капча не позволяет заходить на сайт автоматически (и обучает ИИ)

Для чего применяется хэширование паролей?

Выберите один вариант из списка

- ☒ Абсолютно точно.
- ☐ 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

Если удастся взломать базу данных, то если пароль хэширован, им всё равно нельзя будет воспользоваться

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

Выберите один вариант из списка

☒ Хорошие новости, верно!

☐ Нет

☐ Да

Верно решили **967**

Из всех попыток **61**

это шутка

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Всё получилось!


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

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

все вышеперечисленное помогает

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

 Хорошие новости, 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)

в ссылках присутствуют лишние элементы (wix и ucoz)

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ Да

☐ Нет

Email Спуфинг -- это

Выберите один вариант из списка



Так точно!

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

Вирус-троян

Выберите один вариант из списка

☒ **Правильно, молодец!**

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

Четвертая глава: Криптография на практике

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Хорошие новости, верно!

- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
- ☒ обе стороны имеют пару ключей
- ☐ обе стороны имеют общий секретный ключ

Асимметричное шифрование — это метод, в котором используются два ключа: открытый (публичный) и закрытый (приватный). 12 Открытый ключ используется для шифрования, а закрытый — для дешифрования. В отличие от симметричного метода, ключи не совпадают, что делает возможным обмен информацией без предварительного обмена секретами

Криптографическая хэш-функция

Выберите все подходящие ответы из списка


☒ 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 захэшированных данных
- ☒ эффективно вычисляется
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

 Верно. Так держать!

Вы решили сложную задачу, поздравляем! Вы можете помочь о
их вопросы, или сравнить своё решение с другими на [форуме р](#)

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

Код аутентификации сообщения относится к

Выберите один вариант из списка



Верно.

☐ асимметричным примитивам

☒ симметричным примитивам

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Хорошая работа.

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

Протокол Диффи — Хэллмана (англ. Diffie–Hellman key exchange protocol, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Хорошие новости, верно!



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Здорово, всё верно.



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

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Всё получилось!

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

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

Выберите один вариант из списка



Так точно!



- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная
- ☐ простая

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

Выберите один вариант из списка


☒ Хорошая работа.

Верно решил
Из всех по

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

 Правильно.

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

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

BitCoin - криптовалюта, SecurePay - ПО, POS терминал - это терминал, как и банкомат

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Хорошая работа.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных 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

Капча не является частью аутентификации, пин-код и пароль - это просто пароль, то есть это один тип аутентификации

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ 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

Потому что важнее защитить счёт человека от краж, а не от случайных зачислений

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Отлично!

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

В доказательстве работы (Proof of Work, PoW), используемом в блокчейне (например, в Bitcoin), ключевое свойство хэш-функции — это вычислительная сложность подбора входных данных для получения хэша с заданными условиями (например, хэш с определённым количеством нулей в начале).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно.

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

- ☒ открытость
- ☒ консенсус
- ☒ живучесть
- ☒ постоянства

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ обмен ключами
- ☐ шифрование
- ☒ цифровая подпись
- ☐ хэш-функция

участники хранят адрес кошелька