

Отчёт по прохождению внешнего курса

Основы кибербезопасности

Городянский Фёдор Николаевич

Содержание

1	Цель и задание работы	5
2	Выполнение лабораторной работы	6
2.1	Выполнение заданий из раздела “Безопасность в сети”.	7
2.2	Выполнение заданий из раздела “Защита ПК/Телефона”	21
2.3	Выполнение заданий из раздела “Криптография на практике” . .	31
3	Выводы	39

Список иллюстраций

Список таблиц

1 Цель и задание работы

Пройти курс по основам кибербезопасности.

2 Выполнение лабораторной работы

2.1 Выполнение заданий из раздела “Безопасность в сети”.

Выберите протокол прикладног

Выберите один вариант

☒ Верно.

- ☐ UDP
- ☐ TCP
- ☒ HTTPS
- ☐ IP

Следующий шаг

Решить

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

1. Как работает интернет: базовые сетевые протоколы.

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Абсолютно точно.

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

7

Следующий шаг

Решить снова

Выберите все корректные адреса IPv4

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](#).

☐ 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

DNS сервер

Выберите один вариант из списка

✓ Отличное решение!

- ☒ 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

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

☒ Правильно.

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

Следующий шаг

Решить снова

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

Протокол http предполагает

Выберите один вариант из списка

☒ Хорошие новости, верно!

- ☐ 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

Протокол https состоит из

Выберите один вариант из списка

☒ Всё получилось!

- ☐ 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

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

Версия протокола TLS определяется

Выберите один вариант из списка

☒ Верно.

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

Следующий шаг

Решить снова

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

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Отличное решение!

- ☐ 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

Куки хранят:

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

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

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

Следующий шаг

Решить снова

2. Персонализация сети. [Ваши решения](#) Вы получили: **1 балл** из 1

Куки не используются для

Выберите один вариант из списка



Отлично!

- ☐ 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

Куки генерируются

Выберите один вариант из списка

☒ Верно. Так держать!

☐ сервером

☐ клиентом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Сессионные куки хранятся в браузере?

Выберите один вариант из списка



Верно. Так держать!

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

Следующий шаг

Решить снова

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

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Правильно.

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

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

3. Браузер TOR: Анонимизация.

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Прекрасный ответ.

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

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Абсолютно точно.

- ☐ 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

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

Выберите один вариант из списка

☒ Так точно!

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

- ☒ Нет
- ☐ Да

Следующий шаг

Решить снова

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

Wi-Fi - это

Выберите один вариант из списка

✓ Всё получилось!

- ☐ 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

4. Беспроводные сети Wi-fi.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Отлично!

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

Следующий шаг

Решить снова

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

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

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

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

☒ Здорово, всё верно.

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


Следующий шаг

Решить снова

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

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

 Верно.

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг


Решить снова

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

2.2 Выполнение заданий из раздела “Защита ПК/Телефона”

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

 Правильно.

- ☒ Да
☐ Нет

Следующий шаг


Решить снова

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

1. Шифрование диска.

Шифрование диска основано на

Выберите один вариант из списка

 Хорошая работа.

- ☐ хэшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг

Решить снова

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

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ 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](#).

☐ Disk Utility

☒ BitLocker

☐ Wireshark

☒ VeraCrypt


Следующий шаг

Решить снова

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

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

 Отлично!

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

Следующий шаг

Решить снова

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

2. Пароли.

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

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

Зачем нужна капча?

Выберите один вариант из списка

✓ Отлично!

Верн
Из в

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

Следующий шаг

Решить снова

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

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

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

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

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили **967** уч:
Из всех попыток **66%**

- ☐ Да
- ☒ Нет

Следующий шаг

Решить снова

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

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

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

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

✓ 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

3. Фишинг

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

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Отличное решение!

☐ Да

☐ Нет


Следующий шаг

Решить снова

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

Email Спуфинг – это

Выберите один вариант из списка

 Правильно.

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

Следующий шаг

Решить снова

4. Вирусы.Примеры.

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

Вирус-троян

Выберите один вариант из списка

✓ Отлично!

- ☐ 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

На каком этапе формируется ключ шифрования в протоколе мессенджера?

Выберите один вариант из списка

✓ Отличное решение!

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

Следующий шаг


Решить снова

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

5. Безопасность мессенджеров.

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

 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

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

2.3 Выполнение заданий из раздела “Криптография на практике”

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Так точно!

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

Следующий шаг

Решить снова

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

1. Введение в криптографию.

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Отличное решение!

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 захешированных 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

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ 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](#).

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

Следующий шаг

Решить снова

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Следующий шаг

Решить снова

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

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Всё правильно.

- ☐ 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

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

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

2. Цифровая подпись.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

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

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Отличное решение!

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

Следующий шаг

Решить снова

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

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

Выберите один вариант из списка

☒ Верно. Так держать!

- ☒ усиленная квалифицированная
- ☐ простая
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

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

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

Выберите один вариант из списка

☒ Верно.

Верно решил
Из всех попы

- ☐ 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

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

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

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

Следующий шаг

Решить снова

3. Электронные платежи. [Вопрос 1](#) из 1

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ 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](#).

- ☐ 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

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

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ 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

Следующий шаг

Решить снова

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Верно.

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

Следующий шаг

Решить снова

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

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Всё получилось!

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

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

Следующий шаг

Решить снова

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Правильно, молодец!

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

Следующий шаг

Решить снова

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

3 Выводы

В результате прохождения курса получил знания в области кибербезопасности.