

Основы кибербезопасности

Внешний курс на Stepik

Аскеров Александр Эдуардович

Содержание

1 Раздел 1	5
1.1 Пункт 2.1	5
1.2 Пункт 2.2	10
1.3 Пункт 2.3	14
1.4 Пункт 2.4	16
2 Раздел 2	20
2.1 Пункт 3.1	20
2.2 Пункт 3.2	22
2.3 Пункт 3.3	25
2.4 Пункт 3.4	26
2.5 Пункт 3.5	28
3 Раздел 3	29
3.1 Пункт 4.1	29
3.2 Пункт 4.2	31
3.3 Пункт 4.3	33
3.4 Пункт 4.4	34
4 Курс завершён	37

Список иллюстраций

1.1	Протокол прикладного уровня	5
1.2	Протокол TCP работает на транспортном уровне	6
1.3	Адреса IPv4	7
1.4	Определение DNS сервера	8
1.5	Последовательность протоколов в модели TCP/IP	8
1.6	Протокол http	9
1.7	Составляющие протокола https	9
1.8	Версия протокола TLS	10
1.9	Фаза “рукопожатия” протокола TLS	10
1.10	Куки	11
1.11	Использование куки	12
1.12	Сервер генерирует куки	13
1.13	Хранение куки	13
1.14	Число промежуточных узлов в луковой сети Tor	14
1.15	IP-адрес получателя	15
1.16	Общий секретный ключ	16
1.17	Получение пакетов через Tor	16
1.18	Определение Wi-Fi	17
1.19	Протокол работы Wi-Fi	17
1.20	Методы обеспечения шифрования и аутентификации в сети Wi-Fi	18
1.21	Передача данных между хостом сети и роутером	18
1.22	Метод аутентификации для домашней сети	19
2.1	Шифрование загрузочного сектора диска	20
2.2	Шифрование диска	21
2.3	Программы для шифрования жёсткого диска	21
2.4	Стойкие пароли	22
2.5	Безопасное место для хранения паролей	23
2.6	Смысл капчи	23
2.7	Хэширование паролей	24
2.8	Атака перебором	24
2.9	Меры защиты от атаки перебором	25
2.10	Фишинговые ссылки	25
2.11	Фишинговый имейл от знакомого адреса	26
2.12	Email Спупинг	27
2.13	Вирус-тロян	27
2.14	Этап формирования ключа шифрования в протоколе в Signal	28

2.15 Сквозное шифрование	28
3.1 Ключи в асимметричных криптографических примитивах	29
3.2 Свойства криптографической хэш-функции	29
3.3 Алгоритмы цифровой подписи	30
3.4 Код аутентификации сообщения	30
3.5 Обмен ключами Диффи-Хэллмана	31
3.6 Протокол электронной цифровой подписи	31
3.7 Алгоритм верификации электронной цифровой подписи	32
3.8 Характеристики электронной цифровой подписи	32
3.9 Типы сертификата электронной цифровой подписи	33
3.10 Организации по выдаче квалифицированного сертификата ключа проверки электронной подписи	33
3.11 Платёжные системы	33
3.12 Многофакторная аутентификация	34
3.13 Онлайн платежи	34
3.14 Криптографическая хэш-функция	35
3.15 Системы блокчейн	35
3.16 Секретные ключи	36
4.1 Результат завершённого курса	37

1 Раздел 1

1.1 Пункт 2.1

Выберем протокол прикладного уровня.

Выберите протокол прикладного уровня

Выберите один вариант из списка



Верно. Так держать!

- UDP
- TCP
- HTTPS
- IP

Рис. 1.1: Протокол прикладного уровня

Укажем уровень, на котором работает протокол TCP.

На каком уровне работает протокол TCP?

Выберите один вариант из списка



Всё получилось!

- Транспортном
- Прикладном
- Канальном
- Сетевом

Рис. 1.2: Протокол TCP работает на транспортном уровне

Выберем все корректные адреса IPv4.

Выберите все корректные адреса IPv4

Выберите все подходящие отв



Отлично!

Вы решили сложную задачу, поздравляем!
их вопросы, или сравнить своё решение с д

<input type="checkbox"/> 421.0.15.19
<input type="checkbox"/> 43.12.256.7
<input checked="" type="checkbox"/> 90.11.90.22
<input checked="" type="checkbox"/> 25.198.0.15

Рис. 1.3: Адреса IPv4

Первые два варианта не подходят, так как в них есть числа, превышающие 255.

Дадим определение DNS серверу.

DNS сервер

Выберите один вариант из списка

 Прекрасный ответ.

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

Рис. 1.4: Определение DNS сервера

Выберем корректную последовательность протоколов в модели TCP/IP.

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

Рис. 1.5: Последовательность протоколов в модели TCP/IP

Выберем, что предполагает протокол http.

Протокол http предполагает

Выберите один вариант из списка

Всё правильно.

- передачу зашифрованных данных между клиентом и сервером
- передачу данных между клиентом и сервером в открытом виде

Рис. 1.6: Протокол http

Выберем, из чего состоит протокол https.

Протокол https состоит из

Выберите один вариант из списка

Хорошая работа.

- 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

Рис. 1.7: Составляющие протокола https

Выберем, чем определяется версия протокола TLS.

Версия протокола TLS определяется

Выберите один вариант из списка

 Так точно!

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

Рис. 1.8: Версия протокола TLS

Выберем, что не предусмотрено в фазе “рукопожатия” протокола TLS.

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

 Верно. Так держать!

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

Рис. 1.9: Фаза “рукопожатия” протокола TLS

1.2 Пункт 2.2

Выберем, что хранят куки.

Куки хранят:

Выберите все подходящие



Абсолютно точно.

Вы решили сложную задачу, поздравляю! Проверьте правильность ваших вопросы, или сравнить своё решение с ответом.



пароль пользователя



IP адрес



id сессии



идентификатор пользователя

Рис. 1.10: Куки

Выберем, для чего не используются куки.

Куки не используются для

Выберите один вариант из списка

 Хорошие новости, верно!

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

Рис. 1.11: Использование куки

Выберем, что генерируют куки.

Куки генерируются

Выберите один вариант из списка

 Прекрасный ответ.

- сервером
- клиентом

Рис. 1.12: Сервер генерирует куки

Скажем, хранятся ли сессионные куки в браузере.

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

 Отличное решение!

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

Рис. 1.13: Хранение куки

1.3 Пункт 2.3

Укажем, сколько промежуточных узлов в луковой сети Tor.

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

 Отлично!

- 2
- 3
- 4

Рис. 1.14: Число промежуточных узлов в луковой сети Tor

Укажем, кому известен IP-адрес получателя.

IP-адрес получателя известен

Выберите все подходящие



Всё правильно.

Вы решили сложную задачу, поздравляю! Вы можете задать мне новые вопросы, или сравнить своё решение с моим.



охранному узлу



промежуточному узлу



отправителю



выходному узлу

Рис. 1.15: IP-адрес получателя

Укажем, как отправитель генерирует общий секретный ключ.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

 Здорово, всё верно.

Only one variant is correct:

- только с охранным узлом
- с охранным и промежуточным узлом
- с охранным, промежуточным и выходном узлом
- с промежуточным и выходным узлом

Рис. 1.16: Общий секретный ключ

Укажем, должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов.

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

Only one variant is correct:

Верно решил 961 учащийся
Из всех попыток 74% верных

- Да
- Нет

Рис. 1.17: Получение пакетов через Tor

1.4 Пункт 2.4

Дадим определение Wi-Fi.

Wi-Fi - это

Выберите один вариант из списка

 Прекрасный ответ.

- 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

Рис. 1.18: Определение Wi-Fi

Выберем, на каком уровне работает протокол Wi-Fi.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

 Всё правильно.

- Транспортном
- Прикладном
- Канальном
- Сетевом

Рис. 1.19: Протокол работы Wi-Fi

Выберем небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

 Верно. Так держать!

- WPA
- WEP
- WPA2
- WPA3

Рис. 1.20: Методы обеспечения шифрования и аутентификации в сети Wi-Fi

Укажем, как передаются данные между хостом сети и роутером.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

 Всё правильно.

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

Рис. 1.21: Передача данных между хостом сети и роутером

Выберем метод аутентификации для домашней сети.

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

 Прекрасный ответ.

- WPA2 Personal
- WPA2 Enterprise

Рис. 1.22: Метод аутентификации для домашней сети

2 Раздел 2

2.1 Пункт 3.1

Укажем, можно ли зашифровать загрузочный сектор диска.

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

 Всё получилось!

- Да
- Нет

Рис. 2.1: Шифрование загрузочного сектора диска

Выберем, на чём основано шифрование диска.

Шифрование диска основано на

Выберите один вариант из списка



Прекрасный ответ.



хэшировании



симметричном шифровании



асимметричном шифровании

Рис. 2.2: Шифрование диска

Укажем, с помощью каких программ можно зашифровать жёсткий диск.

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка



Здорово, всё верно.

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



Wireshark



BitLocker



VeraCrypt



Disk Utility

Рис. 2.3: Программы для шифрования жёсткого диска

2.2 Пункт 3.2

Выберем пароли, которые можно отнести к стойким.

Какие пароли можно отнести с стойким?

Выберите один вариант из списка



Здорово, всё верно.

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

Рис. 2.4: Стойкие пароли

Нам подходит только тот пароль, в котором присутствуют буквы, символы, цифры, разный регистр, а также он должен быть достаточно длинным.

Выберем, где безопасно хранить пароли.

Где безопасно хранить пароли?

Выберите один вариант из списка



Всё получилось!

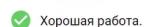
- В менеджерах паролей
- В заметках на рабочем столе
- В заметках в телефоне
- На стикере, приклеенном к монитору
- В кошельке

Рис. 2.5: Безопасное место для хранения паролей

Укажем, зачем нужна капча.

Зачем нужна капча?

Выберите один вариант из списка



Хорошая работа.

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

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

Рис. 2.6: Смысл капчи

Укажем, для чего применяется хэширование паролей.

Для чего применяется хэширование паролей?

Выберите один вариант из списка

 Отлично!

- 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

Рис. 2.7: Хэширование паролей

Скажем, поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу.

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

Выберите один вариант из списка

 Отличное решение!

Верно решили 967 учащихся
Из всех попыток 66% верных

- Нет
- Да

Рис. 2.8: Атака перебором

Скажем, какие меры защищают от утечек данных атакой перебором.

Какие меры защищают от утечек данных атакой перебором?

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](#)

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

Рис. 2.9: Меры защиты от атаки перебором

2.3 Пункт 3.3

Выберем, какие из следующих ссылок являются фишинговыми.

Какие из следующих ссылок являются фишинговыми?

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](#).

- <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)

Рис. 2.10: Фишинговые ссылки

Эти ссылки являются фишинговыми, так как их доменные имена отличаются от настоящих доменных имён сайтов, на которые хочет зайти пользователь.

Скажем, может ли фишинговый имейл прийти от знакомого адреса.

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

 Правильно.

- Да
- Нет

Рис. 2.11: Фишинговый имейл от знакомого адреса

2.4 Пункт 3.4

Скажем, что такое Email Спупинг.

Email Спурфинг – это

Выберите один вариант из списка

 Так точно!

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

Рис. 2.12: Email Спурфинг

Выберем, как работает вирус-троян.

Вирус-троян

Выберите один вариант из списка

 Отличное решение!

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

Рис. 2.13: Вирус-троян

2.5 Пункт 3.5

Скажем, на каком этапе формируется ключ шифрования в протоколе в Signal.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

 Отличное решение!

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

Рис. 2.14: Этап формирования ключа шифрования в протоколе в Signal

Выберем суть сквозного шифрования.

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
- сообщения передаются от отправителя к получателю без участия сервера

Рис. 2.15: Сквозное шифрование

3 Раздел 3

3.1 Пункт 4.1

Укажем, какие ключи имеют стороны в асимметричных криптографических примитивах.

В асимметричных криптографических примитивах

Выберите один вариант из списка

Хорошая работа.

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

Рис. 3.1: Ключи в асимметричных криптографических примитивах

Выберем свойства криптографической хэш-функции.

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно. Так держать!

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](#).

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

Рис. 3.2: Свойства криптографической хэш-функции

Выберем алгоритмы цифровой подписи.

К алгоритмам цифровой подписи относятся

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](#).

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

Рис. 3.3: Алгоритмы цифровой подписи

Выберем, к чему относится код аутентификации сообщения.

Код аутентификации сообщения относится к

Выберите один вариант из списка

Всё правильно.

- асимметричным примитивам
- симметричным примитивам

Рис. 3.4: Код аутентификации сообщения

Дадим определение обмену ключами Диффи-Хэллмана.

Обмен ключами 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

Рис. 3.5: Обмен ключами Диффи-Хэллмана

3.2 Пункт 4.2

Выберем, к чему относится протокол электронной цифровой подписи.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

 Отличное решение!

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

Рис. 3.6: Протокол электронной цифровой подписи

Выберем, что требует на вход алгоритм верификации электронной цифровой подписи.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

 Прекрасный ответ.

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

Рис. 3.7: Алгоритм верификации электронной цифровой подписи

Укажем, что не обеспечивает электронная цифровая подпись.

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

 Абсолютно точно.

- неотказ от авторства
- аутентификацию
- целостность
- конфиденциальность

Рис. 3.8: Характеристики электронной цифровой подписи

Выберем тип сертификата электронной цифровой подписи для отправки налоговой отчётности в ФНС.

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

Выберите один вариант из списка

Отлично!

простая
 усиленная неквалифицированная
 усиленная квалифицированная

Верно решили 904 учащихся
Из всех попыток 67% верных

Рис. 3.9: Типы сертификата электронной цифровой подписи

Выберем, в какой организации можно получить квалифицированный сертификат ключа проверки электронной подписи.

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

Выберите один вариант из списка

Хорошая работа.

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

Верно решили 902 учащихся
Из всех попыток 60% верных

Рис. 3.10: Организации по выдаче квалифицированного сертификата ключа проверки электронной подписи

3.3 Пункт 4.3

Выберем все платёжные системы в списке.

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Всё 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](#).

- BitCoin
 MasterCard
 SecurePay
 POS-терминал
 банкомат
 МИР

Рис. 3.11: Платёжные системы

Выберем из списка примеры многофакторной аутентификации.

Примером многофакторной аутентификации является

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](#).

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

Рис. 3.12: Многофакторная аутентификация

Мы выбрали те варианты, в которых используются факторы разных категорий аутентификации.

Выберем, что используется при онлайн платежах.

При онлайн платежах сегодня используется

Выберите один вариант из списка

Правильно, молодец!

- 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

Рис. 3.13: Онлайн платежи

3.4 Пункт 4.4

Выберем, какое свойство криптографической хэш-функции используется в доказательстве работы.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Прекрасный ответ.

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

Рис. 3.14: Криптографическая хэш-функция

Выберем, какими свойствами обладает консенсус в некоторых системах блокчейн.

Консенсус в некоторых системах блокчейн обладает свойствами

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](#).

- консенсус
- открытость
- постоянства
- живучесть

Рис. 3.15: Системы блокчейн

Выберем, секретные ключи какого криптографического примитива хранят участники блокчейна.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

 Хорошая работа.

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

Рис. 3.16: Секретные ключи

4 Курс завершён

Курс завершён.

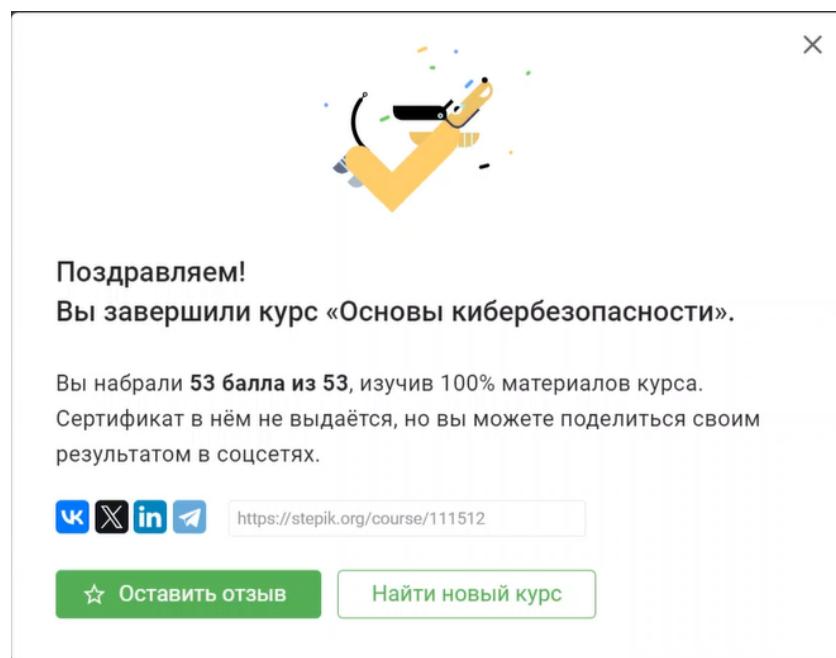


Рис. 4.1: Результат завершённого курса