Отчёт по прохождению внешнего курса

Основы кибербезопасности

Городянский Фёдор Николаевич

Содержание

1	Цел	ь и задание работы	5
2	Вып	олнение лабораторной работы	6
	2.1	Выполнение заданий из раздела "Безопасноть в сети"	7
	2.2	Выполнение заданий из раздела "Защита ПК/Телефона"	21
	2.3	Выполнение заданий из раздела "Криптография на практике"	31
3	Выв	ОДЫ	39

Список иллюстраций

Список таблиц

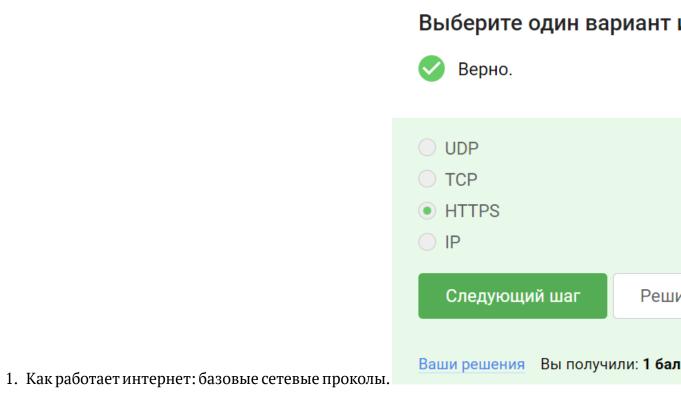
1 Цель и задание работы

Пройти курс по основам кибербезопасности.

2 Выполнение лабораторной работы

2.1 Выполнение заданий из раздела "Безопасноть в сети".

Выберите протокол прикладног



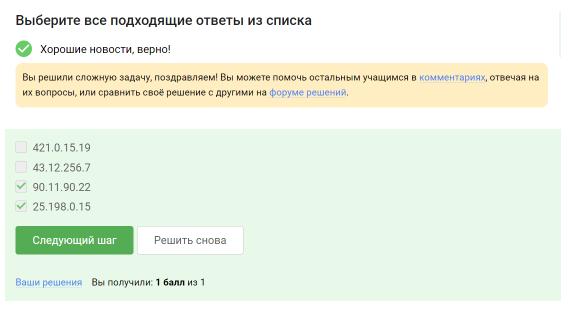
Выберите один вариант из списка

Следующий шаг

На каком уровне работает протокол ТСР?

Абсолютно точно.
Транспортном
Прикладном
Канальном
Сетевом

Решить снова



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

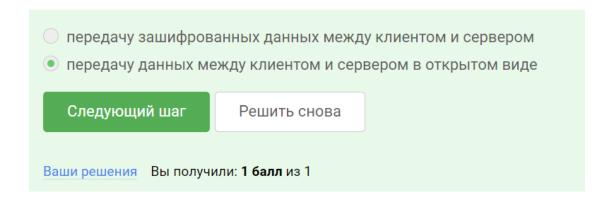


сетевой прикладно	ой канальный тр	ранспортный	
прикладной транс	портный канальнь	ый сетевой	
транспортный – сете	евой прикладной	канальный	
• прикладной транс	портный сетевой	канальный	
Следующий шаг	Решить снова		
Ваши решения Вы получи	или: 1 балл из 1		

Протокол http предполагает

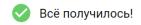
Выберите один вариант из списка

🗸 Хорошие новости, верно!



Протокол https состоит из

Выберите один вариант из списка

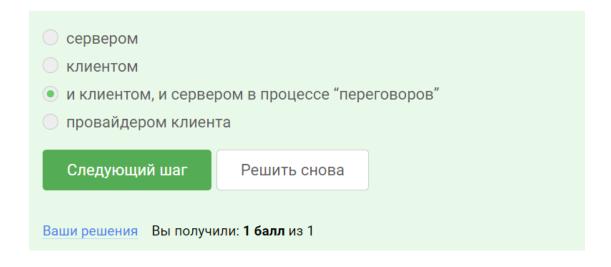


	гия и передачи данні Ікация клиента и сер	ых вера и шифрования данных ятификация сервера, генерация общего ключа
Следующий шаг	Решить снова	
Ваши решения Вы получ	или: 1 балл из 1	

Версия протокола TLS определяется

Выберите один вариант из списка

Верно.



В фазе "рукопожатия" протокола TLS не предусмотрено

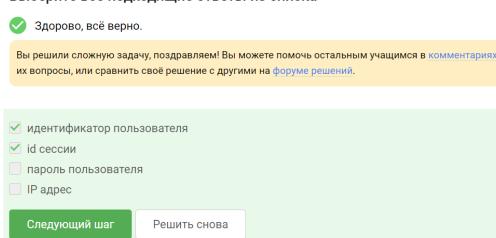
Выберите один вариант из списка

Отличное решение!

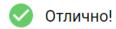
формирование общ	его секретного ключ	а между клиентом и сервером
🔾 аутентификация (ка	к минимум одной из	сторон)
🔾 выбираются алгори	тмы шифрования/ау	тентификации
• шифрование данны	X	
Следующий шаг	Решить снова	
Ваши решения Вы получ	1 / 1	

Куки хранят:

Выберите все подходящие ответы из списка

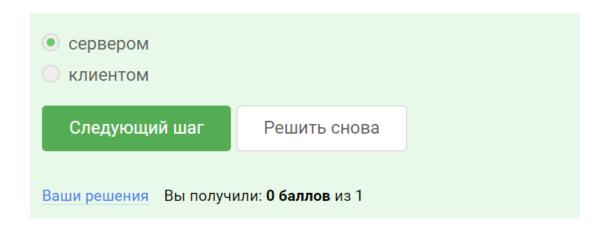


2. Персонализация сети. Ваши решения Вы получили: 1 балл из 1



аутентификации пол	пьзователя	
персонализации веб	б-страниц	
отслеживания инфо	рмации о пользователе	
сборе статистики по	осещаемости сайта	
• улучшения надежно	ости соединения	
Следующий шаг	Решить снова	
Ваши решения Вы получ	или: 1 балл из 1	

🗸 Верно. Так держать!

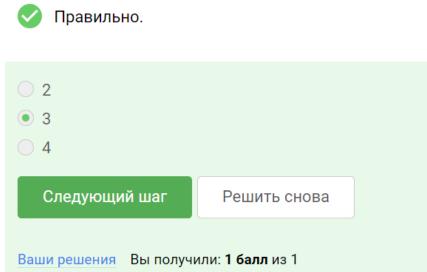


Сессионные куки хранятся в браузере?

Выберите один вариант из списка

🗸 Верно. Так держать!

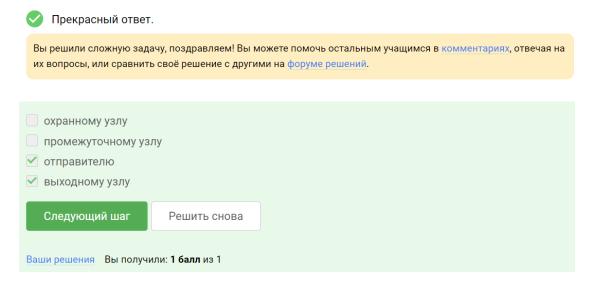
Да, на некоторое вре Нет Да, на время пользо		вером
Следующий шаг	Решить снова	
Ваши решения Вы получи	или: 1 балл из 1	



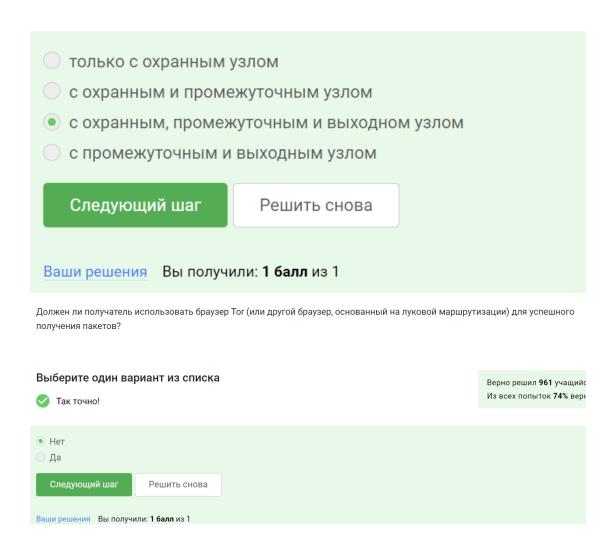
3. Браузер TOR: Анонимизация.

ІР-адрес получателя известен

Выберите все подходящие ответы из списка







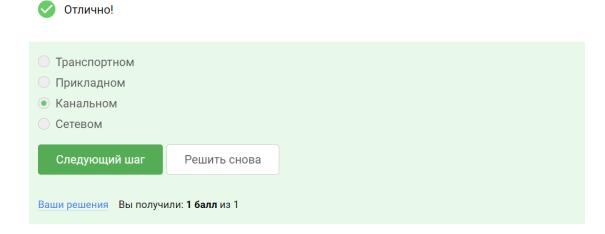
Ваши решения Вы получили: 1 балл из 1



4. Беспроводные сети Wi-fi.

На каком уровне работает протокол WiFi?

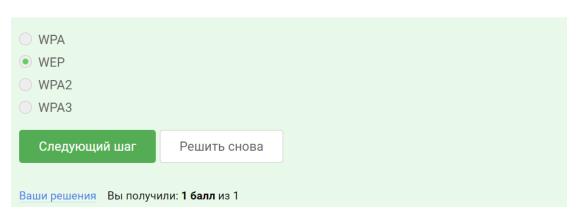
Выберите один вариант из списка



Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

🗸 Верно. Так держать!



Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

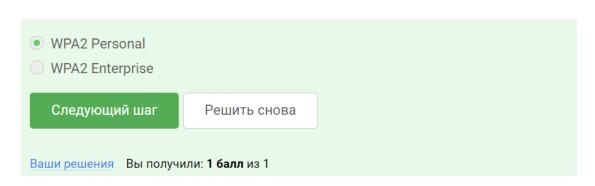
Здорово, всё верно.

передаются в заши	фрованном виде	
🔾 передаются в откры	том виде после аутентификации устройств	
• передаются в заши	фрованном виде после аутентификации устройств	
🔾 передаются в откры	том виде	
Следующий шаг	Решить снова	
Ваши решения Вы получ	или: 1 балл из 1	

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

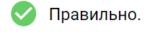


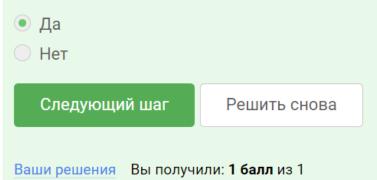


2.2 Выполнение заданий из раздела "Защита ПК/Телефона"

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка





1. Шифрование диска.

Шифрование диска основано на

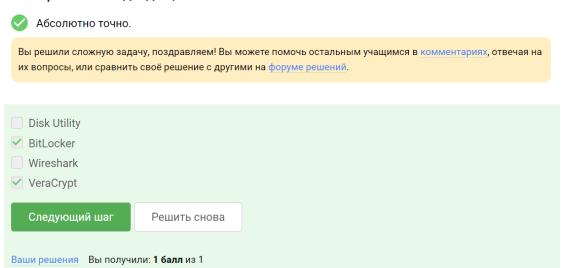
Выберите один вариант из списка

🗸 Хорошая работа.

хэшировании симметричном шифасимметричном шиф		
Следующий шаг	Решить снова	
Ваши решения Вы получи	или: 1 бал<u>й</u> ј из 1	

С помощью каких программ можно зашифровать жесткий диск?

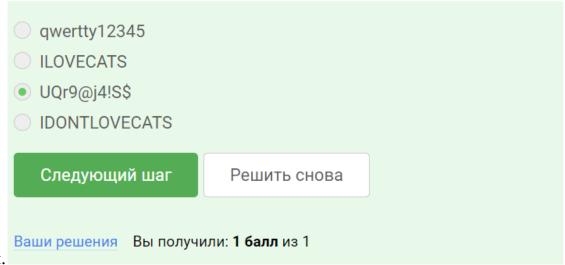
Выберите все подходящие ответы из списка



Какие пароли можно отнести с стойким?

Выберите один вариант из списка





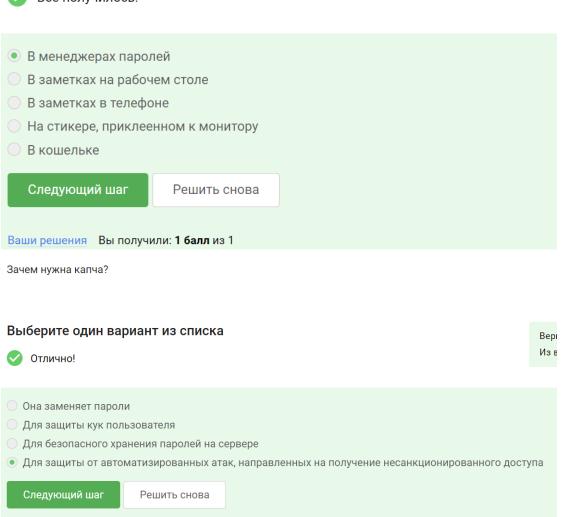
2. Пароли.

Где безопасно хранить пароли?

Выберите один вариант из списка

Всё получилось!

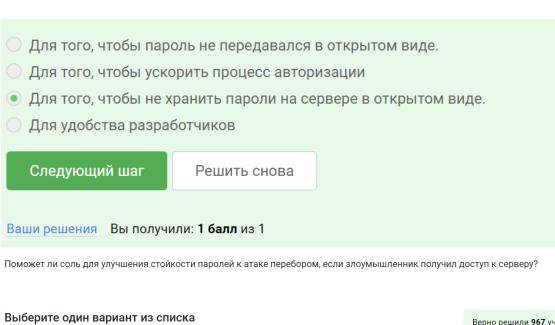
Ваши решения Вы получили: 1 балл из 1



Для чего применяется хэширование паролей?

Выберите один вариант из списка





Выберите один вариант из списка

✓ Верно. Так держаты!

✓ Да

✓ Нет

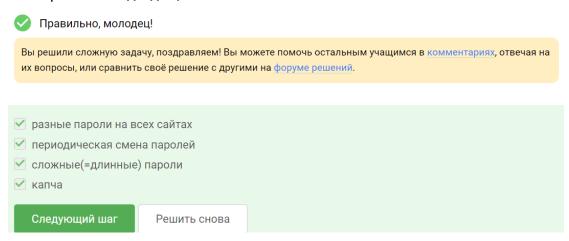
Следующий шаг

Решить снова

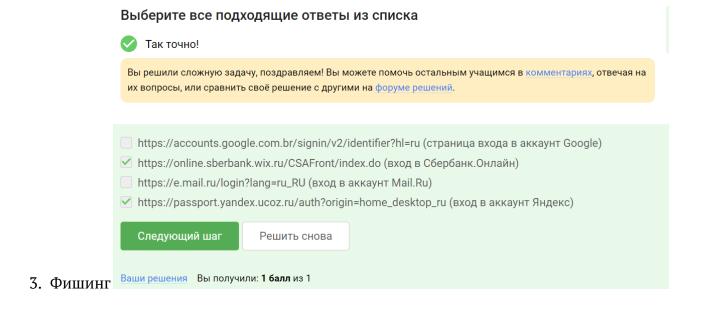
Ваши решения Вы получили: 1 балл из 1

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка



Какие из следующих ссылок являются фишинговыми?



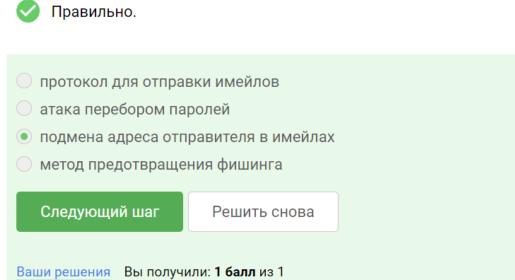
26

Может ли фишинговый имейл прийти от знакомого адреса?

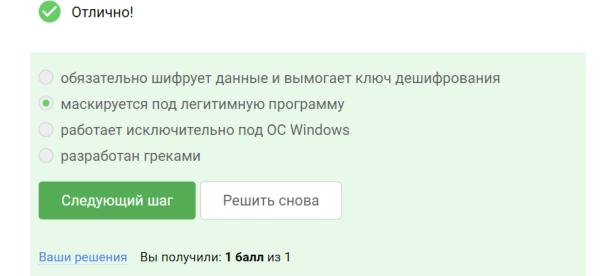
Выберите один вариант из списка

Отличное решение!

ДаНет	
Следующий шаг	Решить снова
Ваши решения Вы получ	или: 1 балл из 1

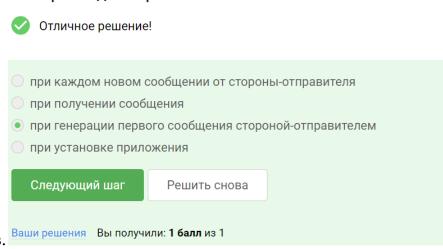


4. Вирусы.Примеры.



На каком этапе формируется ключ шифрования в протоколе мессенджеро

Выберите один вариант из списка



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 секрет

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 захэшированных данных
 ✓ эффективно вычисляется
 ✓ дает на выходе фиксированное число бит независимо от объема входных данных
 Следующий шаг
 Решить снова
 Вы получили: 1 балл из 1

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. АЕЅ SHA2 RSA € CCDSA ГОСТ Р 34.10-2012

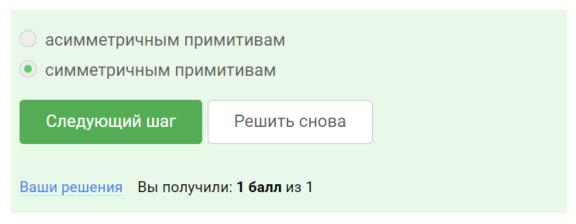
Код аутентификации сообщения относится к

Решить снова

Выберите один вариант из списка

Здорово, всё верно.

Следующий шаг

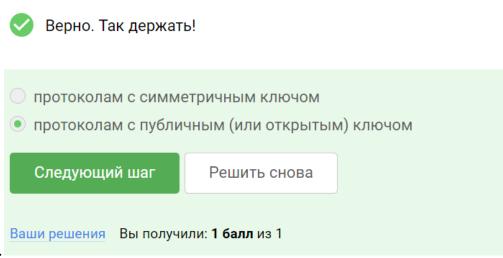


Всё правильно.

Симметричный прим	иитив генерации обц	цего секретного ключа
асимметричный при	имитив генерации об	щего открытого ключа
• асимметричный при	имитив генерации об	щего секретного ключа
🔾 асимметричный алг	оритм шифрования	
Следующий шаг	Решить снова	
Ваши решения Вы получи	или: 1 балл из 1	

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



2. Цифровая подпись.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Абсолютно точно.подпись, открытый ключ, сообщ

• подпись, открытый	ключ, сообщение
подпись, секретный	ключ
подпись, открытый	ключ
подпись, секретный	ключ, сообщение
, .	, .
Следующий шаг	Решить снова

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

Отличное решение!

аутентификацию	
неотказ от авторства	
целостность	
• конфиденциальность	
Следующий шаг	Решить снова
Ваши решения Вы получ	или: 1 балл из 1

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

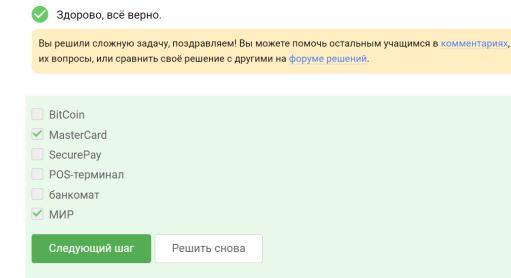
Выберите один вариант из списка

Ваши решения Вы получили: 1 балл из 1

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 решилі Из всех попы 🕜 Верно. 🗎 в любой организации, имеющей соответствующую лицензию ФСБ в минкомсвязи РФ • в удостоверяющем (сертификационном) центре в любой организации по месту работы Следующий шаг Решить снова

Выберите из списка все платежные системы.

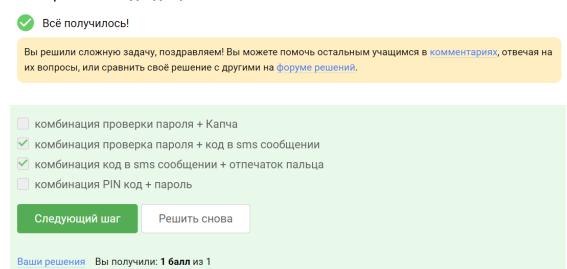
Выберите все подходящие ответы из списка



3. Электронные платежи.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка



При онлайн платежах сегодня используется

Выберите один вариант из списка



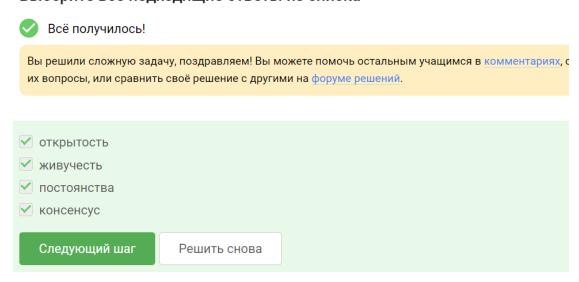
Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Верно. О 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



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.