
Основы информационной безопасности. Обучение в записи

Урок 8. Семинар: Основы криптографической защиты информации

Оглавление

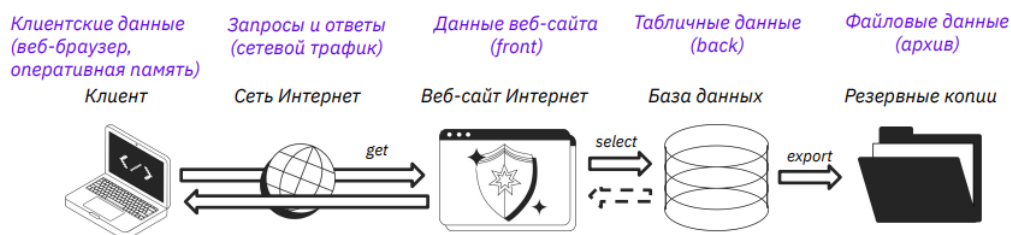
Задание 1.....	2
Задание 2.....	3
Задание 3.....	5
Домашнее задание:	7

Задание 1

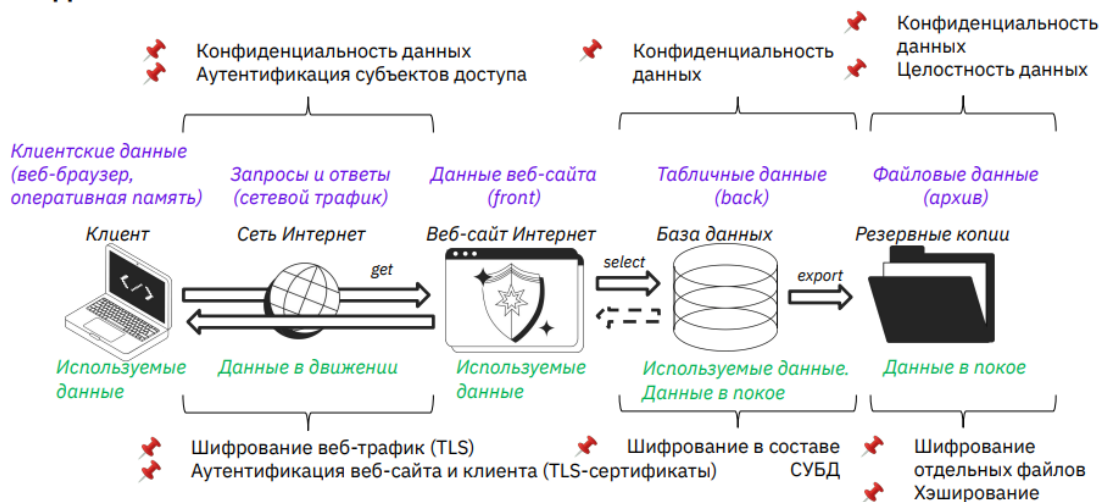


Задание №1. Выбор СКЗИ

- Вам как ИБ-специалисту компании «Самый лучший образовательный сайт» пришла пора выбрать СКЗИ для вашей информационной системы:
- Какие свойства информации (данных) вы можете обеспечить за счёт применения СКЗИ?
- Какие варианты применения СКЗИ?



Задание №1. Ответ



* Возможны авторские варианты ответов

Задание 2



Задание №2. Проверка TLS-сертификатов.

- Вам как ИБ-специалисту пришла пора проверить состояние TLS-сертификат для вашего веб-сайта.
- Проверить TLS-сертификаты*:
 - Домена, где у вас электронная почта или т.п.
 - Домена вашего работодателя или ВУЗ-а
 - 94.156.189[.]28 (убирая квадратные скобки)
- Сделать скриншоты (Google Docs).

LeaderSSL

Проверка SSL

Домен:

* https://www.leaderssl.ru/tools/ssl_checker

LeaderSSL

SSL БРЕНДЫПРОДУКТЫПОМОЩЬУТИЛИТЫ SSLПАРТНЕРАМО КОМПАНИИ

8 (495) 225-22358 (800) 555-5737

Домен:

✓ Сертификат проверен и установлен правильно

Специальное предложение: получите wildcard SSL сертификат мгновенно всего за 18 000,00 руб. в год без предоплаты!

⚠ Сервер поддерживает устаревший (менее безопасный) протокол SSL v2. Настоятельно рекомендуем отключить его

GlobalSign Root CA

GlobalSign

GlobalSign RSA OV SSL CA 2018

*.mail.ru

Информация о сервере

IP адрес(а)

- 217.69.139.215
- 217.69.139.216
- 94.100.180.215
- 94.100.180.216

DNS серверы

- ns1.mail.ru
- ns2.mail.ru

Сервер

- nginx

Не применимо

Домен		*.mail.ru
Сертификат	Альтернативные имена (SANs)	*.mail.ru mail.ru
	Организация	VK LLC
	Город	Moscow
	Область	Moscow
	Страна	RU
	Тип сертификата	Подтверждение организации (OV)
Подлинность	Действителен с	✓ 24 октября 2024
	Истекает	✓ 25 ноября 2025 (Истекает через 172 дней)
	OSCP статус	Не применимо
	CLR статус	
Подробности	Алгоритм	2048 bit RSA key
	Подпись	sha256WithRSAEncryption
Подписи	MD5	ce4678e823a1979a8d84368a4d976fc9
	SHA1	f642829c557ad5d32c379a9e8ad303ac3799cf
	Серийный номер	4736764119409679704278763460

LeaderSSL

SSL БРЕНДЫПРОДУКТЫПОМОЩЬУТИЛИТЫ SSLПАРТНЕРАМО КОМПАНИИ

8 (495) 225-22358 (800) 555-5737

Домен:

✓ Сертификат проверен и установлен правильно

Специальное предложение: получите SSL сертификат мгновенно всего от 459,12 руб./год без предоплаты!

Срок действия SSL сертификата закончится менее чем через 90 дней. Получите SSL сертификат в течение 5 минут без предоплаты

⚠ Сервер поддерживает устаревший (менее безопасный) протокол SSL v2. Настоятельно рекомендуем отключить его

GlobalSign Root CA

GTS Root R4

WE2

mail.google.com

Информация о сервере

IP адрес(а)

- 142.250.203.197
- 2a00:1450:401b:810::2005

DNS серверы

- ns3.google.com
- ns4.google.com
- ns2.google.com
- ns1.google.com

Сервер

- GSE

✓

Домен		mail.google.com
Сертификат	Альтернативные имена (SANs)	mail.google.com inbox.google.com
	Тип сертификата	Проверка домена (DV)
Подлинность	Действителен с	✓ 12 мая 2025
	Истекает	✓ 4 августа 2025 (Истекает через 59 дней)
	OSCP статус	Не применимо
	CLR статус	
Подробности	Алгоритм	256 bit id-ecPublicKey key
	Подпись	ecdsa-with-SHA256
Подписи	MD5	8130e17787a7b1762b154b55262d9154
	SHA1	5869aef54714065492776637f09ed10431c3aca
	Серийный номер	51803443555993538516408170848958433194

LeaderSSL

SSL БРЕНДЫПРОДУКТЫПОМОЩЬУТИЛИТЫ SSLПАРТНЕРАМО КОМПАНИИ

8 (495) 225-22358 (800) 555-5737

Домен:

gb.ru

ПРОВЕРИТЬ

✓Сертификат проверен и установлен правильно

Специальное предложение: получите wildcard SSL сертификат мгновенно всего за 18 000,00 руб. в год без предоплаты!

⚠Сервер поддерживает устаревший (менее безопасный) протокол SSL v2. Настоятельно рекомендуем отключить его

GlobalSign Root CA

GlobalSign

GlobalSign RSA OV SSL CA 2018

*.gb.ru

Информация о сервере

IP адрес(а)

- 178.248.232.209

DNS серверы

- dns01.skillbox.pro
- dns02.skillbox.pro
- dns03.skillbox.pro
- dns04.skillbox.pro
- dns05.skillbox.pro

Сервер

- QRATOR

Не применимо

Домен		*.gb.ru
Сертификат	Альтернативные имена (SANs)	*.gb.ru gb.ru
	Организация	VK LLC
	Город	Moscow
	Область	Moscow
	Страна	RU
Подлинность	Тип сертификата	Подтверждение организации (OV)
	Действителен с	✓ 12 мая 2025
	Истекает	✓ 13 июня 2026 (Истекает через 372 дней)
	OCSP статус	Не применимо
	CLR статус	
Подробности	Алгоритм	2048 bit RSA key
	Подпись	sha256WithRSAEncryption
Подписи	MD5	0b2ee7690a17a851bf4d771bfbcfa6f9
	SHA1	71bb4ee4c570f7b9007cb86d01d8f721879aef6d
	Серийный номер	7665087177257453178651265403

LeaderSSL

SSL БРЕНДЫПРОДУКТЫПОМОЩЬУТИЛИТЫ SSLПАРТНЕРАМО КОМПАНИИ

8 (495) 225-22358 (800) 555-5737

Домен:

lk.rosreestr.ru

ПРОВЕРИТЬ

✗Самоподписанный сетификат в цепочке сертификатом

⚠Сервер поддерживает устаревший (менее безопасный) протокол SSL v2. Настоятельно рекомендуем отключить его

Russian Trusted Root CA

Russian Trusted Sub CA

*.rosreestr.ru

Информация о сервере

IP адрес(а)

- 217.77.104.136

DNS серверы

- ns2.rtcomm.ru
- ns.rt-comm.ru
- ns.rtcomm.ru

✓

Домен		*.rosreestr.ru
Сертификат	Альтернативные имена (SANs)	rosreestr.ru www.rosreestr.ru *.rosreestr.ru *.r03.rosreestr.ru *.r07.rosreestr.ru *.r13.rosreestr.ru *.r41.rosreestr.ru *.r49.rosreestr.ru *.r53.rosreestr.ru *.r64.rosreestr.ru *.r76.rosreestr.ru *.r80.rosreestr.ru *.r81.rosreestr.ru *.r84.rosreestr.ru *.r85.rosreestr.ru *.r86.rosreestr.ru *.u82.rosreestr.ru *.u82.rosreestr.ru
	Организация	Rosreestr
	Город	Moscow
	Область	Moscow
	Страна	RU
Подлинность	Тип сертификата	Подтверждение организации (OV)
	Действителен с	✓ 28 января 2025
	Истекает	✓ 28 января 2026 (Истекает через 236 дней)
	OCSP статус	Не применимо
	CLR статус	

Задание 3

Семинар 4. Выбор средств криптографической защиты информации

Задание №3. Расчет и проверка хэшей. Файл

Вам, как ИБ-специалисту, необходимо рассчитать хэш-значения для файлов резервных копий.

- Рассчитать хэш SHA-2 (длина хэша 256) для файла с использованием встроенных средств Windows:
 - в командной строке: `certutil -hashfile "путь к файлу" SHA256`
 - в PowerShell-оболочке: `get-filehash -Algorithm SHA256 "путь к файлу"`
- Рассчитать хэш SHA-2 (длина хэша 256) для файла с использованием встроенных средств Linux:
 - `sha256sum "путь к файлу"`.
- Проверить полученные значения хэшей на веб-ресурсах: <https://hash-file.online/> и/или https://www.strerr.com/ru/sha256_file.html
- Сделать скриншоты (Google Docs).

Select a file to hash

Select a file to hash from your system

Выберите файл

hashtest.txt

Семинар 4. Выбор средств криптографической защиты информации

md5decrypt.net/en/Sha256/#answer

Sha256 Decrypt & Encrypt

paste one or several hashes (up to 100)

Encrypt

Decrypt

Для операционной системы Windows:

PowerShell 7 Preview

PS C:\Users\user> get-filehash -Algorithm SHA256 C:\Users\user\Desktop\Календарь.docx

Algorithm	Hash	Path
SHA256	DD335913492254df8e7b06771cdfccbddfb1d1c2640c8b7aa8b6c6392bff4da6	C:\Users\user\Desktop\Календарь.docx

Командная строка

Microsoft Windows [Version 10.0.26100.4202]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\user>certutil -hashfile C:\Users\user\Desktop\Календарь.docx SHA256
Хэш SHA256 C:\Users\user\Desktop\Календарь.docx:
dd335913492254df8e7b06771cdfccbddfb1d1c2640c8b7aa8b6c6392bff4da6
CertUtil: -hashfile - команда успешно выполнена.
C:\Users\user>

Семинар Основы криптог... | Обучение | GeekBrains - обр... | Основы ИБ. Семинар 4. Осно... | Онлайн-расчет файла SHA256

strerr.com/ru/sha256_file.html

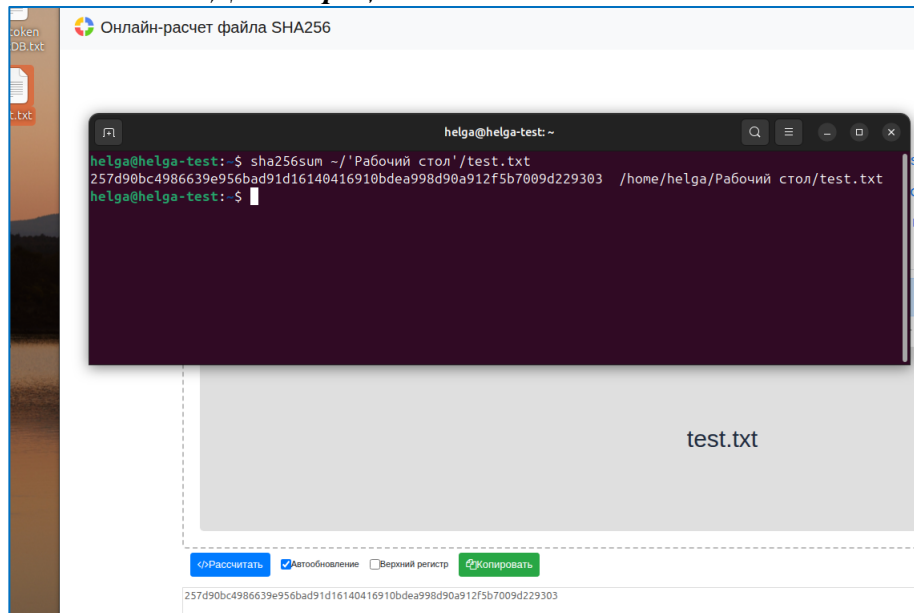
Добро пожаловать в онлайн-расчет файла SHA256

Календарь.docx

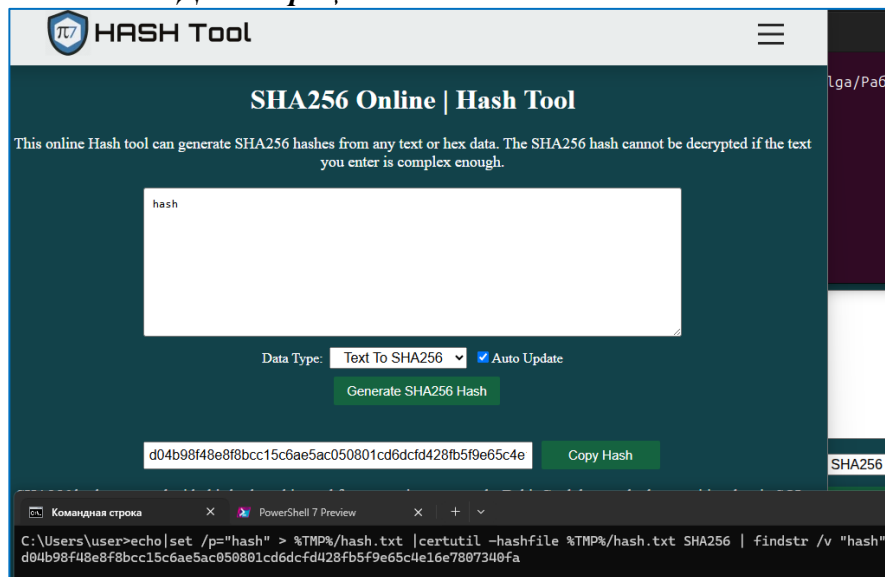
☐ Рассчитать ☒ Автообновление ☐ Верный регистр

dd335913492254df8e7b06771cdfccbddfb1d1c2640c8b7aa8b6c6392bff4da6

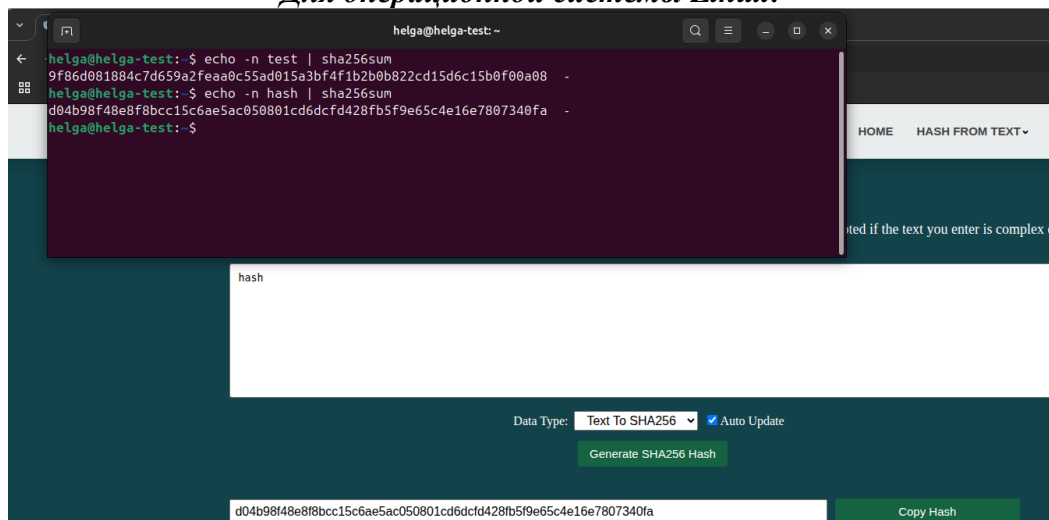
Для операционной системы Linux:



Для операционной системы Windows:




Для операционной системы Linux:




Домашнее задание:

Семинар 4. Выбор средств криптографической защиты информации



Домашнее задание

- Самостоятельно выполнить задание № 3 сегодняшнего семинара с операционными системами, которые не были доступны студенту во время занятия (скриншоты в Google Docs)
- *Напишите программу на Python, которая будет вычислять хэш-значения (файл формата .py или .ipynb)

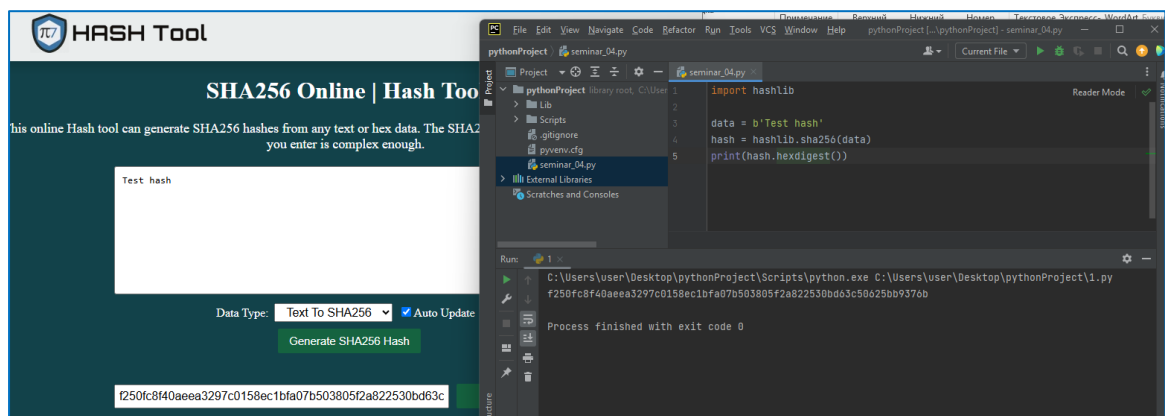


1.1. [Скриншот выполненного Задания № 3](#)

1.2. *Напишите программу на Python, которая будет вычислять хэш-значения):*

```
import hashlib
```

```
data = b'Test hash'  
hash = hashlib.sha256(data)  
print(hash.hexdigest())
```



Ссылка на репозиторий:

<https://github.com/olgashenkel/GeekBrains-specialization-ELECTIVES/tree/main/13.%20Fundamentals%20of%20Information%20Security>