
Основы информационной безопасности. Обучение в записи

*Урок 6. Семинар: Основные технологии и инструменты обеспечения ИБ
(некриптографические)*

Оглавление

Задание 1.....	2
Задание 2.....	3
Задание 3.....	5
Задание 4.....	7

Задание 1

Семинар 3. Основные технологии и инструменты обеспечения ИБ (некриптографические)

Задание №1 “Выбор пароля”

Вам как ИБ-специалисту пришла пора сменить свой пароль:

- Выберите несколько паролей.
- Проверьте их в сервисе *password.kaspersky.com**
- Сделайте скриншот итогового варианта.
- Расскажите, почему именно он.

password

✗

Пароль пора срочно менять!

- Плохая новость
- Часто используемое слово
- Этот пароль засветился в базах утечек паролей 9659365 раз.

* Возможные альтернативы: <https://2ip.ru/passcheck/> и <https://www.passwordmonster.com/>

Проверьте и усильте свой пароль

Ваш пароль в безопасности? Проверьте его прямо сейчас и создайте надежный пароль за считанные секунды. Мы не собираем и не храним ваши пароли! [Подробнее](#)

.....

✕

👁

✔

Содержит цифры

✔

Содержит заглавные буквы

✔

Не найдено в базе данных

✔

Содержит специальные символы

✔

Никаких шаблонов

!

Пароль слишком короткий

Ваш пароль не встречается в базах утечек паролей. Пароль не достаточно сильный, потому что не хватает специальных символов, длины.

🔄

Сгенерировать надежный пароль?

Проверьте и усильте свой пароль

Ваш пароль в безопасности? Проверьте его прямо сейчас и создайте надежный пароль за считанные секунды. Мы не собираем и не храним ваши пароли! [Подробнее](#)

.....

✕

👁

✔

Содержит цифры

✔

Содержит заглавные буквы

✔

Не найдено в базе данных

✔

Содержит специальные символы

✔

Никаких шаблонов

✔

Хорошая новость: у вас стойкий ко взлому пароль.

🔄

Сгенерировать надежный пароль?

Задание 2

Семинар 3. Основные технологии и инструменты обеспечения ИБ (некриптографические)

Задание №2 “Дискреционное управление доступом”

Вам как ИБ-специалисту необходимо настроить дискреционный доступ к каталогу с файлами «Recovery», куда помещаются резервные копии (выгрузки) из базы данных:

- Один каталог «Recovery» (место размещения на усмотрение студента).
- Права только на чтение каталога для отдельного пользователя (выбор пользователя на усмотрение студента).

Для операционной системы Windows:

Учетная запись Майкрософт

Создать пользователя для этого компьютера

Если эта учетная запись предназначена для ребенка или подростка, выберите **Создать и резервную копию**; и создайте учетную запись Майкрософт. Когда младшие члены семьи входят с учетной записью Microsoft, они получают защиту конфиденциальности, ориентированную на их возраст.

Если вы хотите использовать пароль - выберите что-то, что вам запомнится легко, а другим будет сложно угадать.

Кто будет использовать данный компьютер?

Test

Разрешения для группы "Recovery"

Безопасность

Имя объекта: C:\Users\Public\Recovery

Группы или пользователи:

СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ

СИСТЕМА

Test (DESKTOP-929P2AG\Test)

ПАКЕТНЫЕ ФАЙЛЫ

Администраторы (DESKTOP-929P2AG\Администратор)

Добавить... Удалить

Разрешения для группы "Test"	Разрешить	Запретить
Чтение и выполнение	<input type="checkbox"/>	<input type="checkbox"/>
Список содержимого папки	<input type="checkbox"/>	<input type="checkbox"/>
Чтение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Запись	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Особые разрешения	<input type="checkbox"/>	<input type="checkbox"/>

OK Отмена Применить

Сохранение документа

« Локальный диск (C:) » Пользователи » Общие » Recovery

Поиск в: Recovery

Имя: Илья

Дата изменения: 03.06.2025 22:05

Тип: Документ Microsoft Word

Размер: 0 KB

Имя файла: Документ Microsoft Word

Тип файла: Документ Word

Авторы: Test

Тег: Добавьте ключевое с...

Название: Добавьте название

Сохранять эскизы

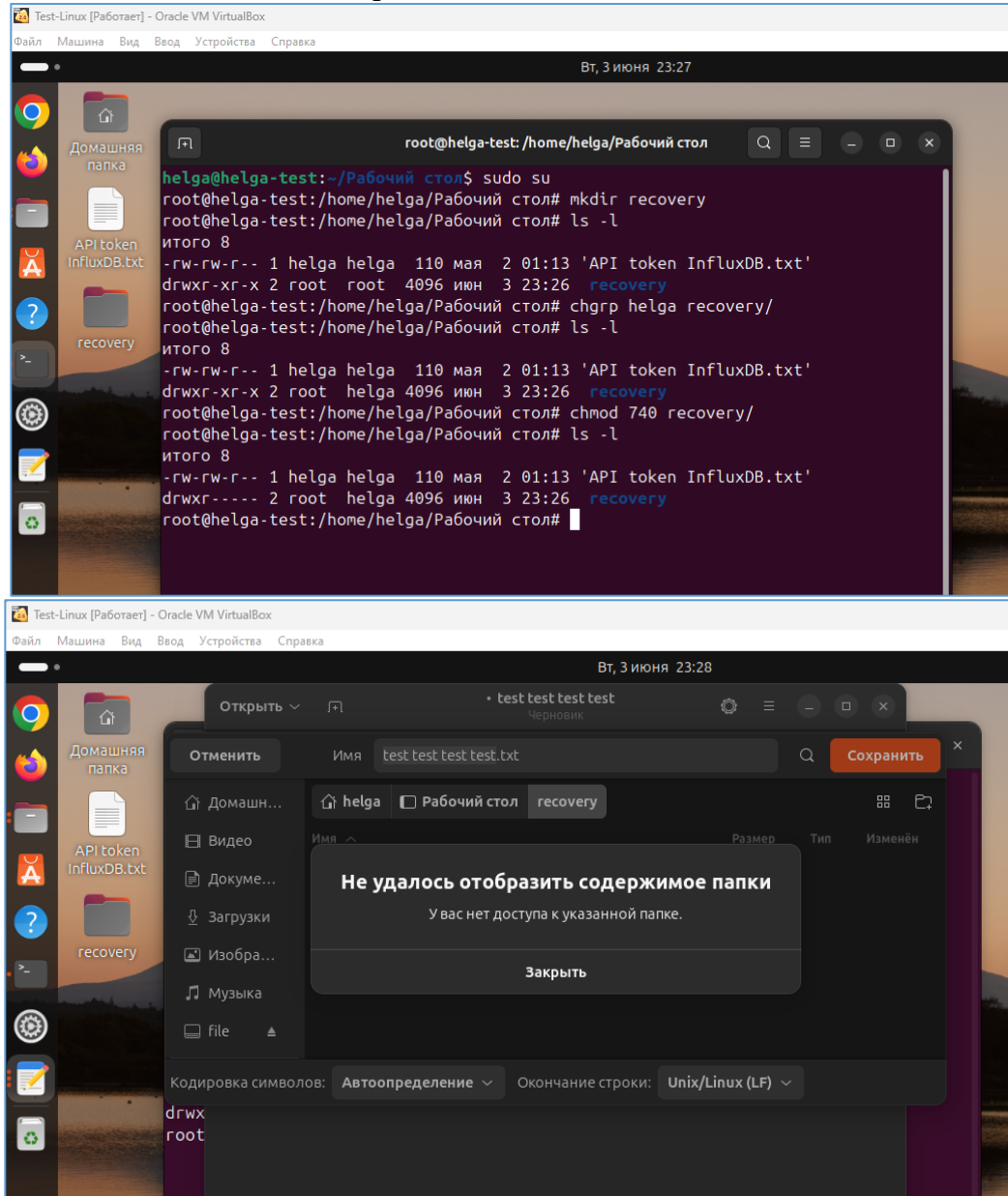
Microsoft Word

Не удается сохранить этот файл, так как он доступен только для чтения. Чтобы не потерять изменения, сохраните документ под новым именем или в другом расположении. (C:\...Документ Microsoft Word.docx)

Показать справку >>

OK

Для операционной системы Linux:



Задание 3



Задание №3 “Просмотр событий” (вопрос для Windows)

Вам как ИБ-специалисту необходимо проанализировать историю входов в операционную систему Windows.

- Вызвать MSC-оснастку «Просмотр событий» (Event Viewer) в Windows разными способами:
 - Комбинация WIN + R (или приложение «Командная строка») и ввести `eventvwr.exe` или `eventvwr.msc`, или `eventvwr`.
 - Комбинация Windows + X и выбрать «Просмотр событий».
 - Найти в каталоге `%SystemRoot%\System32 eventvwr.exe` или `eventvwr.msc`
- Найти события успешного входа: id 4624.
- Выйти из операционной системы, повторно войти, сначала введя неверный пароль, найти событие неуспешного входа: id 4625.
- Ознакомиться с другими событиями и возможностями по фильтрации событий.

Для операционной системы Windows:

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Security' log. The main pane shows a list of events, including successful logons (4624) and failed logons (4625). The details pane on the right shows the properties of a selected event, such as the user name, domain, and logon type.

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	4672	Special Logon
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	4624	Login
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	4624	Login
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	4648	Login
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	4738	User Account Management
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:20	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:18	Microsoft Windows s...	4625	Login
Аудит успеха	04.06.2025 19:07:18	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:18	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:14	Microsoft Windows s...	4625	Login
Аудит успеха	04.06.2025 19:07:14	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:14	Microsoft Windows s...	5059	Other System Events
Аудит успеха	04.06.2025 19:07:10	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:10	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management
Аудит успеха	04.06.2025 19:07:09	Microsoft Windows s...	4798	User Account Management

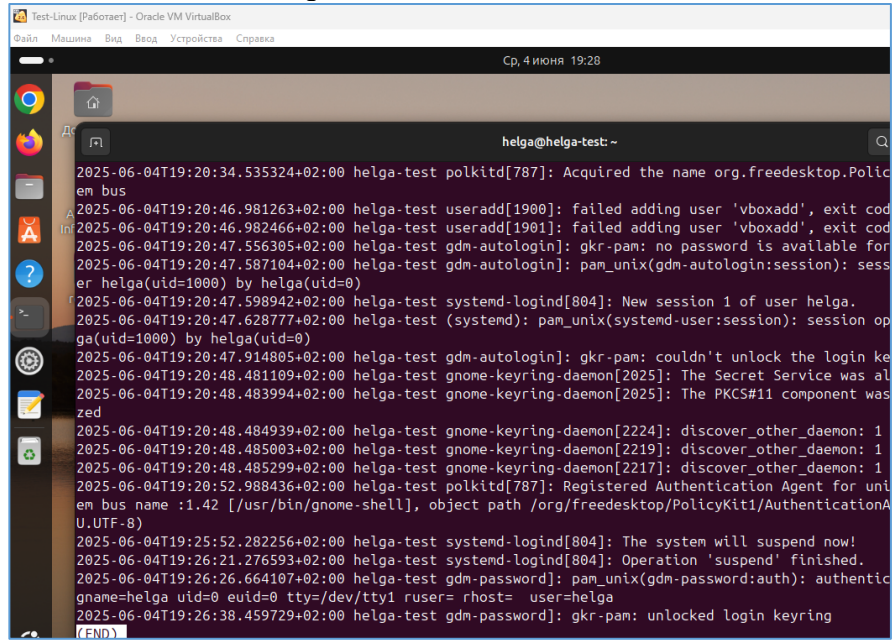
Событие 4624, Microsoft Windows security auditing.

Вход в учетную запись выполнен успешно.

Субъект: Идентификатор безопасности: СИСТЕМА
Имя учетной записи: DESKTOP-929P2AGS
Домен учетной записи: WORKGROUP

Имя журнала: Безопасность
Источник: Microsoft Windows security
Дата: 04.06.2025 19:07:20
Код: 4624
Категория задачи: Logon
Уровни: Сведения
Ключевые слова: Аудит успеха
Пользов.: Н/Д
Компьютер: DESKTOP-929P2AG
Код операции: Сведения

Для операционной системы Linux:



The screenshot shows a terminal window titled 'Test-Linux [Работает] - Oracle VM VirtualBox'. The window has a menu bar with 'Файл', 'Машина', 'Вид', 'Ввод', 'Устройства', and 'Справка'. The top status bar shows 'Ср, 4 июня 19:28'. The terminal prompt is 'helga@helga-test: ~'. The output consists of system logs with timestamps and messages from various daemons and services.

```
2025-06-04T19:20:34.535324+02:00 helga-test polkitd[787]: Acquired the name org.freedesktop.PolicyKit1:AuthenticationAuthority1
2025-06-04T19:20:46.981263+02:00 helga-test useradd[1900]: failed adding user 'vboxadd', exit code 1
2025-06-04T19:20:46.982466+02:00 helga-test useradd[1901]: failed adding user 'vboxadd', exit code 1
2025-06-04T19:20:47.556305+02:00 helga-test gdm-autologin]: gkr-pam: no password is available for user helga(uid=1000) by helga(uid=0)
2025-06-04T19:20:47.587104+02:00 helga-test gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user helga(uid=1000) by helga(uid=0)
2025-06-04T19:20:47.598942+02:00 helga-test systemd-logind[804]: New session 1 of user helga.
2025-06-04T19:20:47.628777+02:00 helga-test (systemd): pam_unix(systemd-user:session): session opened for user helga(uid=1000) by helga(uid=0)
2025-06-04T19:20:47.914805+02:00 helga-test gdm-autologin]: gkr-pam: couldn't unlock the login keyring for user helga(uid=1000)
2025-06-04T19:20:48.481109+02:00 helga-test gnome-keyring-daemon[2025]: The Secret Service was already running
2025-06-04T19:20:48.483994+02:00 helga-test gnome-keyring-daemon[2025]: The PKCS#11 component was not loaded
2025-06-04T19:20:48.484939+02:00 helga-test gnome-keyring-daemon[2224]: discover_other_daemon: 1
2025-06-04T19:20:48.485003+02:00 helga-test gnome-keyring-daemon[2219]: discover_other_daemon: 1
2025-06-04T19:20:48.485299+02:00 helga-test gnome-keyring-daemon[2217]: discover_other_daemon: 1
2025-06-04T19:20:52.988436+02:00 helga-test polkitd[787]: Registered Authentication Agent for unix user helga name :1.42 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAuthority1
2025-06-04T19:25:52.282256+02:00 helga-test systemd-logind[804]: The system will suspend now!
2025-06-04T19:26:21.276593+02:00 helga-test systemd-logind[804]: Operation 'suspend' finished.
2025-06-04T19:26:26.664107+02:00 helga-test gdm-password]: pam_unix(gdm-password:auth): authentication successful for user helga uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=helga
2025-06-04T19:26:38.459729+02:00 helga-test gdm-password]: gkr-pam: unlocked login keyring
(END)
```

Задание 4

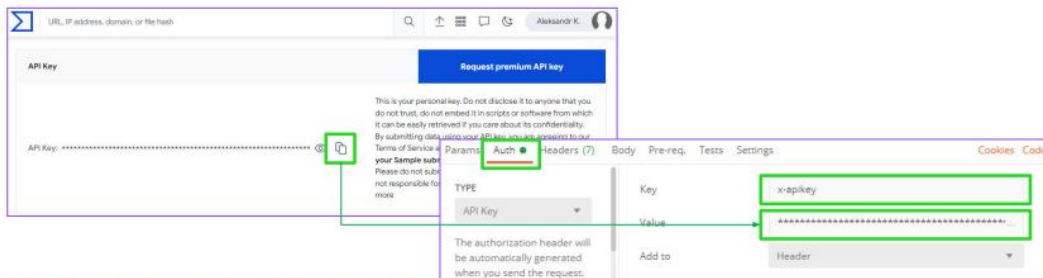
Семинар 3. Основные технологии и инструменты обеспечения ИБ (некриптографические)



Задание №4 “Работа с VirusTotal” (вопрос + инструкция)

Проверка объектов с использованием сервиса VirusTotal:

- Скопировать API Key из личного кабинета VirusTotal*
- Установить приложение Postman**



* https://www.virustotal.com/gui/user/<user_name>/apikey

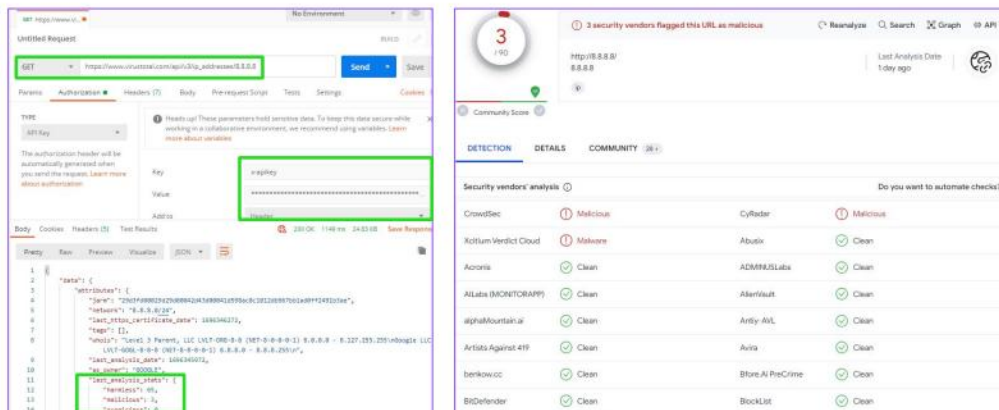
** <https://www.postman.com/downloads/>

Семинар 3. Основные технологии и инструменты обеспечения ИБ (некриптографические)



Задание №4 “Работа с VirusTotal” (инструкция)

Для IP-адреса GET-запрос

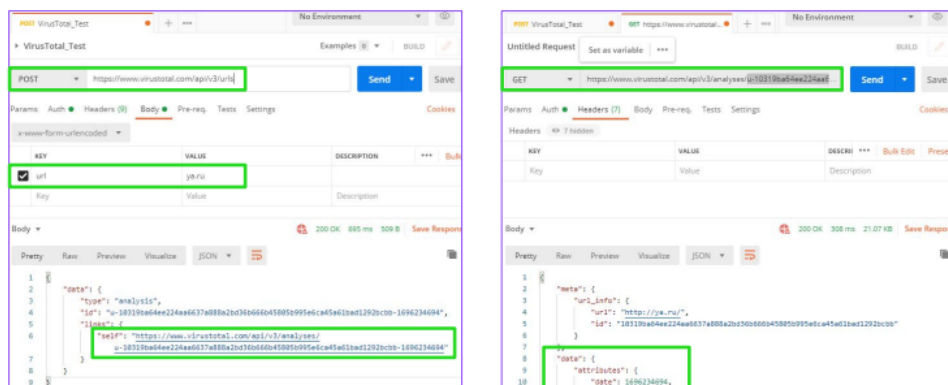


Семинар 3. Основные технологии и инструменты обеспечения ИБ (некриптографические)



Задание №4 “Работа с VirusTotal” (инструкция)

- Для URL-адреса сначала POST-запрос, чтобы получить «id»
- Затем GET-запрос с использованием полученного «id», чтобы получить данные





Задание №4 “Работа с VirusTotal” (объекты проверки)

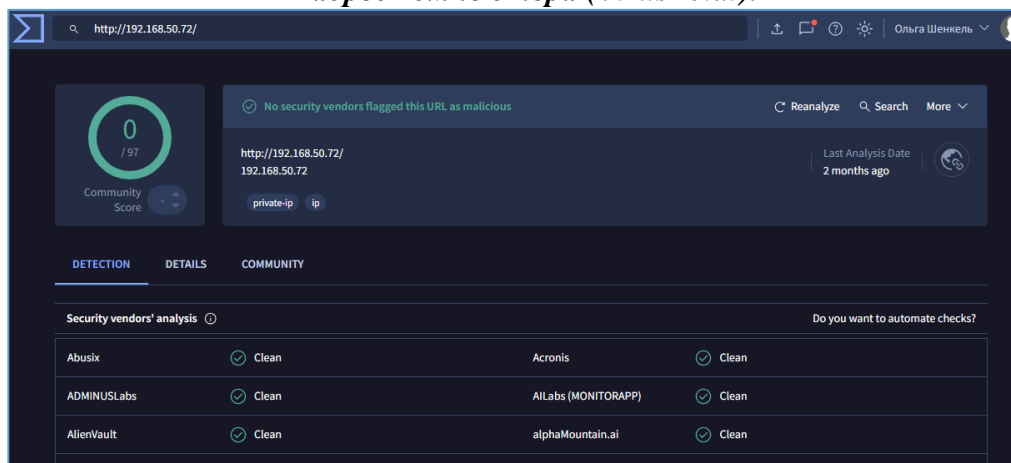
Проверить:

- ✖ IP-адрес вашего компьютера
- ✖ URL-адрес сервиса, где у вас электронная почта или т.п.
- ✖ URL-адрес вашего работодателя или ВУЗ-а
- ✖ 94.156.189[.]28 (убирая квадратные скобки)
- ✖ cheapdealnow[.]top (убирая квадратные скобки)

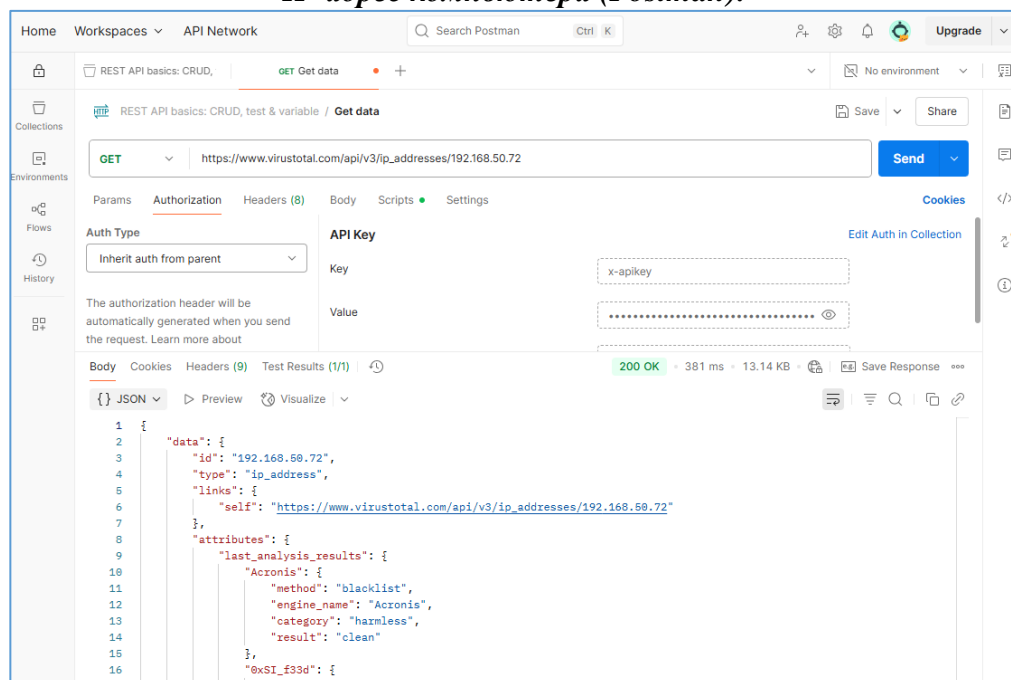
Сделать отдельные вкладки в Postman и веб-браузере на каждый объект проверки (не менее 5 шт.)

* Описание API: <https://developers.virustotal.com/reference/ip-info>

IP-адрес компьютера (VirusTotal):



IP-адрес компьютера (Postman):



URL-адрес mail.ru (VirusTotal):

The screenshot shows the VirusTotal interface for the IP address 217.69.139.215. The top section displays a Community Score of 1/94 and a warning that 1/94 security vendors flagged this IP address as malicious. Below this, the IP address is listed as 217.69.139.215 (217.69.128.0/20) with AS 47764 (LLC VK) and a last analysis date of 1 hour ago. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis	Do you want to automate checks?
Webroot	Malicious
Abusix	Clean
Acronis	Clean
ADMINUSLabs	Clean
AlLabs (MONITORAPP)	Clean
AlienVault	Clean
alphaMountain.ai	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BitDefender	Clean

URL-адрес mail.ru (Postman):

The screenshot shows the Postman interface with a GET request to the VirusTotal API. The request is saved and has a status of 200 OK. The response body is displayed in JSON format, showing details about the IP address 217.69.139.215, including its reputation, whois date, continent, and total votes.

```
{  "data": {    "id": "217.69.139.215",    "type": "ip_address",    "links": {      "self": "https://www.virustotal.com/api/v3/ip_addresses/217.69.139.215"    },    "attributes": {      "reputation": 0,      "whois_date": 1747138294,      "continent": "EU",      "tags": [],      "total_votes": {        "benkow.cc": 0      }    }  }
```

URL-адрес gmail.com (VirusTotal):

The screenshot shows the VirusTotal interface for the IP address 172.217.21.165. The top section displays a Community Score of 0/94 and a warning that 7 detected files communicating with this IP address. Below this, the IP address is listed as 172.217.21.165 (172.217.0.0/19) with AS 15169 (GOOGLE) and a last analysis date of 5 months ago. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis	Do you want to automate checks?
Abusix	Clean
Acronis	Clean
ADMINUSLabs	Clean
AlLabs (MONITORAPP)	Clean
AlienVault	Clean
alphaMountain.ai	Clean
Antiy-AVL	Clean
benkow.cc	Clean

URL-адрес gmail.com (Postman):

Home Workspaces API Network Search Postman Ctrl K Upgrade

REST API basics: CRUD, GET Get data GET https://www.virustotal.com/api/v3/ip_addresses/172.217.21.165

GET https://www.virustotal.com/api/v3/ip_addresses/172.217.21.165

Params Authorization Headers (8) Body Scripts Settings Cookies

Inherit auth from parent

The authorization header will be automatically generated when you send the request. Learn more about [authorization](#).

Key Value Add to

x-apikey

Header

Body Cookies Headers (9) Test Results (1/1) 200 OK 405 ms 14.59 KB Save Response

JSON Preview Visualize

```
1 {
2   "data": {
3     "id": "172.217.21.165",
4     "type": "ip_address",
5     "links": {
6       "self": "https://www.virustotal.com/api/v3/ip_addresses/172.217.21.165"
7     },
8     "attributes": {
9       "whois_date": 1733596622,
10      "tags": [
11        "self-signed"
12      ],
13      "last_modification_date": 1733596624,
14      "total_votes": {
15        "harmless": 0,
16        "malicious": 0
17      }
18    }
19  }
20 }
```

URL-адрес gb.ru (VirusTotal):

178.248.232.209

Did you intend to search across the file corpus instead? [Click here](#)

0 / 94 Community Score

No security vendor flagged this IP address as malicious

Reanalyze Similar More

178.248.232.209 (178.248.232.0/21)
AS 51115 (HLL LLC)

RU Last Analysis Date 5 months ago

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AlienVault	Clean

URL-адрес gb.ru (Postman):

Home Workspaces API Network Search Postman Ctrl K Upgrade

REST API basics: CRUD, GET Get data GET https://www.virustotal.com/api/v3/ip_addresses/178.248.232.209

GET https://www.virustotal.com/api/v3/ip_addresses/178.248.232.209

Params Authorization Headers (8) Body Scripts Settings Cookies

Inherit auth from parent

The authorization header will be automatically generated when you send the request. Learn more about [authorization](#).

Key Value Add to

x-apikey

Header

Body Cookies Headers (9) Test Results (1/1) 200 OK 410 ms 14.7 KB Save Response

JSON Preview Visualize

```
1 {
2   "data": {
3     "id": "178.248.232.209",
4     "type": "ip_address",
5     "links": {
6       "self": "https://www.virustotal.com/api/v3/ip_addresses/178.248.232.209"
7     },
8     "attributes": {
9       "continent": "EU",
10      "last_analysis_stats": {
11        "malicious": 0,
12        "suspicious": 0,
13        "undetected": 33,
14        "harmless": 61,
15        "timeout": 0
16      }
17    }
18  }
19 }
```

94.156.189.28

9

/ 94

Community Score

9/94 security vendors flagged this IP address as malicious

Reanalyze

Similar

More

94.156.189.28 (94.156.189.0/24)

CY

Last Analysis Date

AS 44901 (Belcloud LTD)

9 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CRDF	Malicious	CyRadat	Malicious
Dr.Web	Malicious	G-Data	Malware
Kaspersky	Malware	Lionic	Malware
SOCRadat	Phishing	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean

The screenshot shows the Postman REST client interface. At the top, there are tabs for 'Home', 'Workspaces', and 'API Network'. Below these, there's a search bar and a 'REST API basics: CRUD,' tab. The main area displays a GET request to the URL 'https://www.virustotal.com/api/v3/ip_addresses/94.156.189.28'. The 'Authorization' tab is selected, showing 'Inherit auth from parent'. The 'Body' tab is also visible, showing a JSON response with details about the IP address, including its ID, type, and links.

REST API basics: CRUD, test & variable / **Get data**

GET https://www.virustotal.com/api/v3/ip_addresses/94.156.189.28 Send

Params Authorization Headers (8) Body Scripts Settings Cookies

Inherit auth from parent

Key: x-apikey

Value:

Add to: Header

The authorization header will be automatically generated when you send the request. Learn more about [authorization](#).

Body Cookies Headers (9) Test Results (1/1) 200 OK • 417 ms • 23.7 KB Save Response

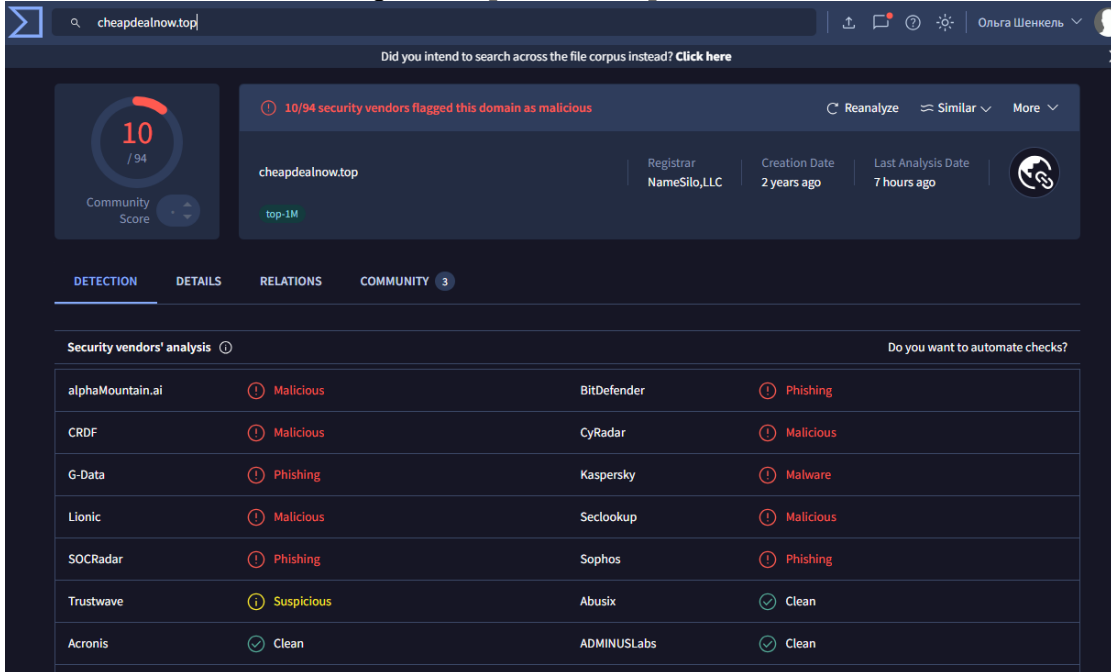
{ } JSON Preview Visualize

```

1  {
2    "data": {
3      "id": "94.156.189.28",
4      "type": "ip_address",
5      "links": {
6        "self": "https://www.virustotal.com/api/v3/ip_addresses/94.156.189.28"
7      },
8      "attributes": {
9        "last_https_certificate": {
10          "cert_signature": {
11            "signature_algorithm": "sha256RSA",
12            "signature":
13              "43b81e621cd984988306af2266b03e3d199ca9abf44798db65e647846d69d27b0143c3227b109bb945c3
14              f7e9388910ac2d483c21e7d89cc330c5b6fdb2ae285da1ab1371fa0bd50d65d2b76a5b99733f57666d1f59
15              373abdc9c4b37a78fe346a499279b283b001e6eb331c99740b6fcc40ddea549a4ae2f59b63eb33b35e09b
16              238085359a747325cafe8a5e380834a07cd601244921df1a309785fe5e6c023108d9b5f418b6b8dca690
17              98ab0974e1712c6968ac2bfa8266e5283125c4e25cac40afc451541f240e3d3b9b996ee3037c57ede0a58
18              61a06ceb9dec90037bba70876927f5b3b1cff755b77bef100aa992505c72740fd0d1682eff5f00d569be2
19              6bf"
20            }
21          }
22        }
23      }
24    },
25    "extensions": {
26      "subject_key_identifier": "Aaf0a7c8d3664c310360731d68c555f54b0468569"
27    }
28  }

```

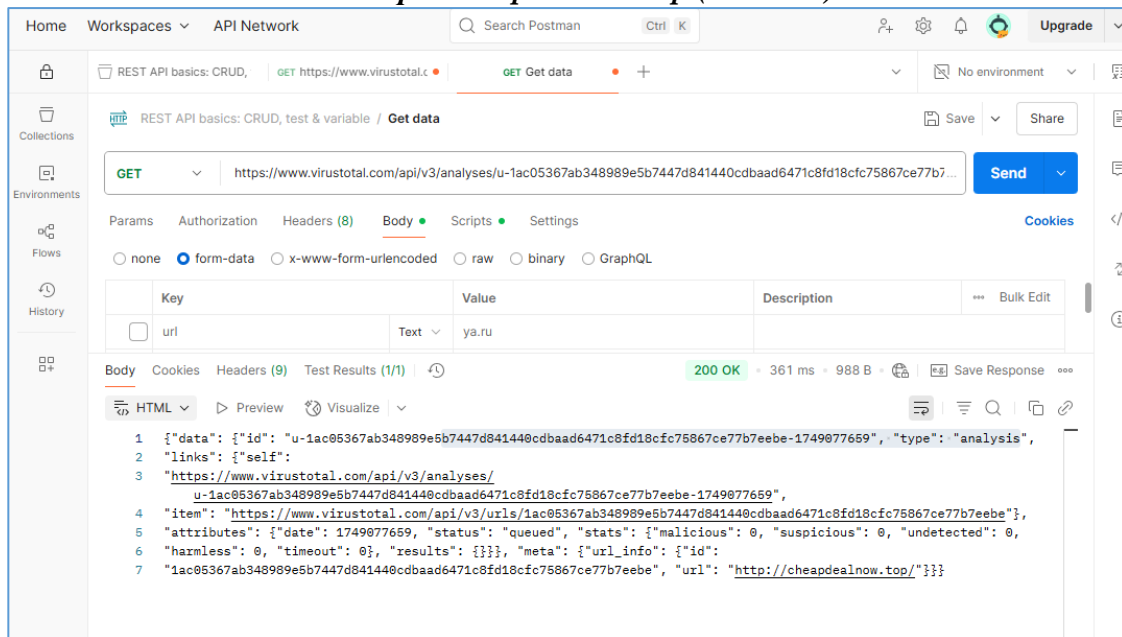
URL-адрес cheapdealnow.top (VirusTotal):



The screenshot shows the VirusTotal interface for the domain cheapdealnow.top. At the top, a search bar contains the domain name. Below it, a summary card displays a community score of 10/94 and a status of '10/94 security vendors flagged this domain as malicious'. The card also shows the registrar as NameSilo, LLC, creation date as 2 years ago, and last analysis date as 7 hours ago. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Vendor	Verdict	Vendor	Verdict
alphaMountain.ai	Malicious	BitDefender	Phishing
CRDF	Malicious	CyRadar	Malicious
G-DATA	Phishing	Kaspersky	Malware
Lionic	Malicious	Seclookup	Malicious
SOCradar	Phishing	Sophos	Phishing
Trustwave	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

URL-адрес cheapdealnow.top (Postman):



The screenshot shows the Postman interface with a GET request to the VirusTotal API. The request is configured with the URL `https://www.virustotal.com/api/v3/analyses/u-1ac05367ab348989e5b7447d841440cdbaad6471c8fd18cfc75867ce77b7eebe-1749877659`. The response is a 200 OK status, and the body is displayed in JSON format.

```
1 {
2   "data": {
3     "id": "u-1ac05367ab348989e5b7447d841440cdbaad6471c8fd18cfc75867ce77b7eebe-1749877659",
4     "type": "analysis",
5     "links": {
6       "self": "https://www.virustotal.com/api/v3/analyses/u-1ac05367ab348989e5b7447d841440cdbaad6471c8fd18cfc75867ce77b7eebe-1749877659",
7       "item": "https://www.virustotal.com/api/v3/urls/1ac05367ab348989e5b7447d841440cdbaad6471c8fd18cfc75867ce77b7eebe",
8       "attributes": {
9         "date": "1749877659",
10        "status": "queued",
11        "stats": {
12          "malicious": 0,
13          "suspicious": 0,
14          "undetected": 0,
15          "harmless": 0,
16          "timeout": 0,
17          "results": {},
18          "meta": {
19            "url_info": {
20              "id": "1ac05367ab348989e5b7447d841440cdbaad6471c8fd18cfc75867ce77b7eebe",
21              "url": "http://cheapdealnow.top/"
22            }
23          }
24        }
25      }
26    }
27  }
```

Ссылка на репозиторий:

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