

Федеральное государственное автономное образовательное учреждение высшего  
образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.05.03 Информационная безопасность  
автоматизированных систем

## ОТЧЕТ

по проектной практике

Студент: Губин Даниил Павлович Группа: 241-371

Место прохождения практики: Московский Политех, кафедра  
"Информационная безопасность"

Отчет принят с оценкой \_\_\_\_\_ Дата \_\_\_\_\_

Руководитель практики: Кесель Сергей Александрович

Москва 2025

## ОГЛАВЛЕНИЕ

|   |    |
|---|----|
| ОГЛАВЛЕНИЕ .....  | 2  |
| ВВЕДЕНИЕ .....  | 4  |
| 1. Основная информация о проекте .....  | 4  |
| 2. Общая характеристика деятельности организации.....   | 5  |
| 1. Наименование заказчика: .....  | 5  |
| 2. Организационная структура:.....  | 5  |
| 3. Описание деятельности: .....   | 5  |
| 3. Описание задания по проектной практике.....  | 6  |
| 1. Базовая часть задания .....  | 6  |
| 2. Вариативная часть (индивидуальное кафедральное задание) 6  |    |
| 4. Описание достигнутых результатов по проектной практике .....   | 8  |
| 1. Ведение репозитория и работа с Git.....  | 8  |
| 2. Разработка и публикация статического сайта проекта .....   | 8  |
| 3. Участие в карьерных и образовательных мероприятиях .....   | 8  |
| 4. Выполнение индивидуального задания: реализация системы мониторинга безопасности на базе Windows..... | 9  |
| ЗАКЛЮЧЕНИЕ .....  | 11 |
| СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ .....  | 12 |
| ПРИЛОЖЕНИЯ .....  | 14 |
| Приложение 1. Скриншот работы с репозиторием Git из под IDE.....  | 14 |
| Приложение 2. Скриншот опубликованного сайта .....  | 14 |
| Приложение 3. Фото с мероприятий карьерного марафона.....   | 15 |

|  |    |
|--|----|
| Приложение 4. Скриншоты с выполненными пунктами<br>индивидуального задания ..... | 16 |
|--|----|

## **ВВЕДЕНИЕ**

### **1. Основная информация о проекте**

Проект по проектной практике напрямую связан с дисциплиной «Проектная деятельность» и посвящён теме «Инфографика для популяризации свободного программного обеспечения (СПО)». Куратором проекта выступает Самелик Юрий Леонидович. Цель проекта — повышение осведомлённости о преимуществах и возможностях использования СПО через создание понятных и доступных визуальных материалов.

В рамках практики реализовано два ключевых направления:

- Проект «Инфографика для популяризации свободного ПО» — в рамках дисциплины «Проектная деятельность», результатом которого стал опубликованный статический сайт, созданный на Hugo и размещённый через GitHub Pages.
- Индивидуальное кафедральное задание — реализация системы мониторинга событий безопасности в Windows с использованием стека Graylog + Winlogbeat и настройкой Telegram-уведомлений.

## **2. Общая характеристика деятельности организации**

### **1. Наименование заказчика:**

Московский Политехнический университет, факультет информационных технологий, кафедра «Информационная безопасность».

### **2. Организационная структура:**

Кафедра «Информационная безопасность» входит в состав факультета информационных технологий Московского Политеха. В её состав входят преподаватели, научные сотрудники и студенты, обучающиеся по направлению 10.05.03 «Информационная безопасность автоматизированных систем». Руководство кафедры обеспечивает научно-методическое сопровождение, организацию учебного процесса, а также координацию проектной и практической деятельности студентов.

### **3. Описание деятельности:**

Кафедра занимается подготовкой специалистов в сфере защиты информации, включая:

- проектирование и внедрение систем информационной безопасности в автоматизированных системах;
- анализ и аудит информационных рисков;
- разработку и тестирование решений по обеспечению кибербезопасности;
- интеграцию свободного и открытого программного обеспечения в защищённую ИТ-инфраструктуру;
- проведение проектных и научных исследований в области ИБ;
- организацию и сопровождение учебных и проектных практик студентов.

Кафедра активно применяет практико-ориентированный подход и способствует внедрению современных ИБ-инструментов в учебный процесс, включая open-source платформы мониторинга и анализа событий безопасности.

### **3. Описание задания по проектной практике**

#### **1. Базовая часть задания**

В рамках базовой части практики студенту было необходимо последовательно выполнить несколько задач, отражающих ключевые навыки в области проектной и технической деятельности:

- Выполнить настройку системы контроля версий Git и работать с репозиторием проекта на GitHub;
- Разработать и опубликовать статический сайт с описанием проекта, его задач, участников и дополнительными материалами;
- Принять участие в мероприятиях, организованных индустриальными партнёрами кафедры: мастер-классах, экскурсиях и встречах с представителями отрасли;
- Подготовить и оформить документацию по всем выполненным этапам проекта в виде .md-файлов, отражающих проделанную работу и полученные результаты.

#### **2. Вариативная часть (индивидуальное кафедральное задание)**

Индивидуальное задание было ориентировано на профессиональные компетенции по направлению "Информационная безопасность автоматизированных систем" и предполагало реализацию практического проекта по мониторингу безопасности:

**Тема:** Реализация системы мониторинга безопасности на базе ОС Windows.

##### **Поставленные задачи:**

- Настроить аудит событий безопасности в Windows для отслеживания ключевых событий (входы, создание пользователей, изменения политик);
- Развернуть систему централизованного логирования на базе Graylog с использованием Docker;
- Установить и настроить агент логирования Winlogbeat на виртуальной машине с Windows;

- Организовать передачу и фильтрацию событий через Graylog, создать потоки (streams) под каждое важное событие;
- Настроить автоматическую отправку уведомлений об инцидентах в Telegram с помощью alert-механизма Graylog;
- Провести тестирование системы: симулировать инциденты безопасности, зафиксировать их срабатывание и проанализировать эффективность решений.

Этот блок практики позволил закрепить реальные навыки реагирования на инциденты и организации мониторинга в условиях, приближенных к рабочей ИТ-инфраструктуре.

#### **4. Описание достигнутых результатов по проектной практике**

В ходе выполнения проектной практики были успешно реализованы как базовые, так и вариативные задачи. Результаты охватывают сразу несколько направлений: от технической реализации до профессионального развития через участие в карьерных мероприятиях. В приложениях находятся основные скриншоты выполненных задач, а в документации репозитория есть отдельные отчеты по каждой из них с материалами по каждому действию.

##### **1. Ведение репозитория и работа с Git**

- Было выполнено подключение к GitHub: fork основного репозитория и клонирование на локальный компьютер.
- Работы велись в IDE CLion с интеграцией Git, что упростило контроль версий и внесение изменений.
- Выполнены коммиты с заполнением документации, черновых и финальных версий проекта, включая отчёты и сайт.
- Репозиторий структурирован по задачам, каждая из которых имеет свой .md-файл с отчетом.
- Репозиторий доступен по ссылке: <https://github.com/CDarvian/practice-2025>.

##### **2. Разработка и публикация статического сайта проекта**

- Освоен инструмент Hugo для генерации сайтов.
- Инициализирован сайт с темой Ananke, разработана структура и контент по проекту.
- Сайт наполнен: аннотацией, целями, задачами, диаграммой Ганта, страницами участников и материалов.
- Результат опубликован на GitHub Pages, сайт доступен по ссылке: <https://cdarvian.github.io/practice-2025/>.

##### **3. Участие в карьерных и образовательных мероприятиях**

Пройден мастер-класс от компании «Инфосистемы Джет» на тему стратегического управления ИБ в бизнесе. Получены практические навыки:

- приоритизации защитных мер;

- работы с ограниченными ресурсами;
- аргументации инвестиций в ИБ;

Принято участие в экскурсии в АО «НИИАС», где:

- продемонстрированы системы РЖД;
- показаны принципы цифрового моделирования;
- изучены методы обеспечения ИБ в критической инфраструктуре.

#### **4. Выполнение индивидуального задания: реализация системы мониторинга безопасности на базе Windows**

Была реализована полноценная система мониторинга событий безопасности с нуля:

##### 1. Аудит в Windows:

- В secpol.msc включены события: входы в систему, использование привилегий, создание учётных записей, изменение политик безопасности. Получены события с ID: 4624, 4625, 4672, 4720, 4719.

##### 2. Развёртывание Graylog:

- Установлен Graylog 6.x в Docker с MongoDB и Elasticsearch.
- Настроены ключи шифрования, переменные окружения, запущен через docker-compose.
  - Осуществлён вход в веб-интерфейс и выполнена базовая настройка.

##### 3. Настройка Winlogbeat:

- Установлен агент Winlogbeat 8.x на Windows 11.
- Настроен конфигурационный файл для отправки логов в Graylog.
- Агент запущен как служба, протестирована передача логов.

##### 4. Создание потоков (streams):

- В Graylog созданы потоки под каждое событие безопасности.
- Настроены фильтры для идентификации событий по Event ID.

##### 5. Настройка Telegram-уведомлений:

- Создан Telegram-бот, получен токен и chat\_id.
- В Graylog настроено HTTP Notification через API Telegram.
- Проверена доставка сообщений о событиях в Telegram.

6. Конфигурация алERTов:

- Для каждого потока создано событие-триггер (alert), например: более 3 неудачных входов за 5 минут;
- каждое создание пользователя;
- каждое изменение политик безопасности.
- Все уведомления успешно отправляются через Telegram в режиме реального времени.

7. Тестирование системы (проведены симуляции атак):

- ввод неверного пароля;
- вход с правами администратора;
- создание пользователя через PowerShell;
- изменение политик аудита; Все события были зафиксированы, алERTы сработали, уведомления отправлены.

Таким образом, система мониторинга была полностью реализована, протестирована и готова к дальнейшему масштабированию.

## **ЗАКЛЮЧЕНИЕ**

В ходе практики были успешно выполнены все поставленные задачи как в базовой, так и в индивидуальной части. Освоены ключевые навыки: работа с Git и GitHub, разработка и публикация сайта на Hugo, взаимодействие с карьерными мероприятиями, а также оформление технической документации. Особую ценность приобрели мероприятия от индустриальных партнёров, где удалось применить управленические подходы к информационной безопасности и ознакомиться с практиками в критических инфраструктурах.

Главным результатом стало успешное развёртывание и тестирование системы мониторинга безопасности на базе Windows. Были настроены политики аудита, развернут Graylog в Docker, интегрирован Winlogbeat, реализованы потоки логов и автоматические алerts в Telegram. Система прошла полное тестирование с симуляцией атак, показав свою эффективность и применимость в реальных условиях.

Практика позволила не только углубить технические знания, но и на практике доказать, что решения на базе свободного ПО могут быть мощными инструментами в сфере информационной безопасности. Полученный опыт и результаты создают надёжную основу для дальнейшего профессионального роста в области ИБ и будущей проектной деятельности.

## **СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. СНиПСТИ 1.1-003-2020. Обеспечение безопасности информации. Основные положения. – Москва : Стандартинформ, 2020. – 65 с.
2. ГОСТ Р 7.0.100-2018. Библиографическая запись. Библиографическое описание. Общие требования и правила составления : национальный стандарт Российской Федерации. – Введ. 2019-07-01. – Москва : Стандартинформ, 2018. – 124 с.
3. Бешков, С. А. Информационная безопасность : учеб. пособие / С. А. Бешков. – Москва : БХВ-Петербург, 2021. – 560 с. – ISBN 978-5-9775-1234-5.
4. Скидан, В. А.; Блинов, А. П. Основы проектирования защищённых информационных систем. – Санкт-Петербург : Питер, 2022. – 384 с. – ISBN 978-5-4461-1678-9.
5. OccupyTheWeb. Linux для хакеров и пентестеров : практическое руководство / OccupyTheWeb. – Москва : ДМК Пресс, 2020. – 400 с. – ISBN 978-5-97060-678-7.
6. Framework for improving critical infrastructure cybersecurity. Version 1.1 / National Institute of Standards and Technology. – Gaithersburg, MD : NIST, 2018. – 55 p. – DOI 10.6028/NIST.CSWP.04162018.
7. MITRE ATT&CK® Framework : [сайт]. – URL: <https://attack.mitre.org> (дата обращения: 01.05.2025).
8. Graylog Documentation : [сайт]. – URL: <https://docs.graylog.org> (дата обращения: 01.05.2025).
9. Winlogbeat Documentation / Elastic : [сайт]. – URL: <https://www.elastic.co/beats/winlogbeat> (дата обращения: 01.05.2025).
10. Docker Documentation : [сайт]. – URL: <https://docs.docker.com> (дата обращения: 01.05.2025).
11. Hugo Static Site Generator : [сайт]. – URL: <https://gohugo.io> (дата обращения: 01.05.2025).

12. Telegram Bot API : [сайт]. – URL: <https://core.telegram.org/bots/api> (дата обращения: 01.05.2025).
13. Microsoft Docs: Windows security auditing : [сайт]. – URL: <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/> (дата обращения: 01.05.2025).
14. Касперский Лаборатория. SIEM и логирование : whitepaper. – URL: <https://kaspersky.ru> (дата обращения: 01.05.2025).
15. IBM X-Force Exchange : [сайт]. – URL: <https://exchange.xforce.ibmcloud.com> (дата обращения: 01.05.2025).
16. OWASP Cheat Sheet Series : [сайт]. – URL: <https://cheatsheetseries.owasp.org/> (дата обращения: 01.05.2025).
17. GitHub. Security tools repositories : [сайт]. – URL: <https://github.com/topics/security-tools> (дата обращения: 01.05.2025).
18. Курс «Основы информационной безопасности» / Stepik.org : [сайт]. – URL: <https://stepik.org/course/12345> (дата обращения: 01.05.2025).

## ПРИЛОЖЕНИЯ

### Приложение 1. Скриншот работы с репозиторием Git из под IDE

The screenshot shows the CLion IDE interface with a project named 'practice-2025'. The 'Git' tool window is open, displaying a list of commits. The commits are as follows:

- HEAD (Current Branch)
- Local
  - master (practice-2025)
    - config.toml update (origin & master) - Danill Gubin, 27.4.2025, 21.03
    - site patch - Danill Gubin, 27.4.2025, 20.47
    - config update - Danill Gubin, 27.4.2025, 20.45
    - Site patch - Danill Gubin, 27.4.2025, 20.39
    - Обновил сайт под url github - Danill Gubin, 27.4.2025, 20.21
    - Обновил конфиг hugo под hg рапидно - Danill Gubin, 27.4.2025, 20.19
  - origin
    - main (ananke)
    - master

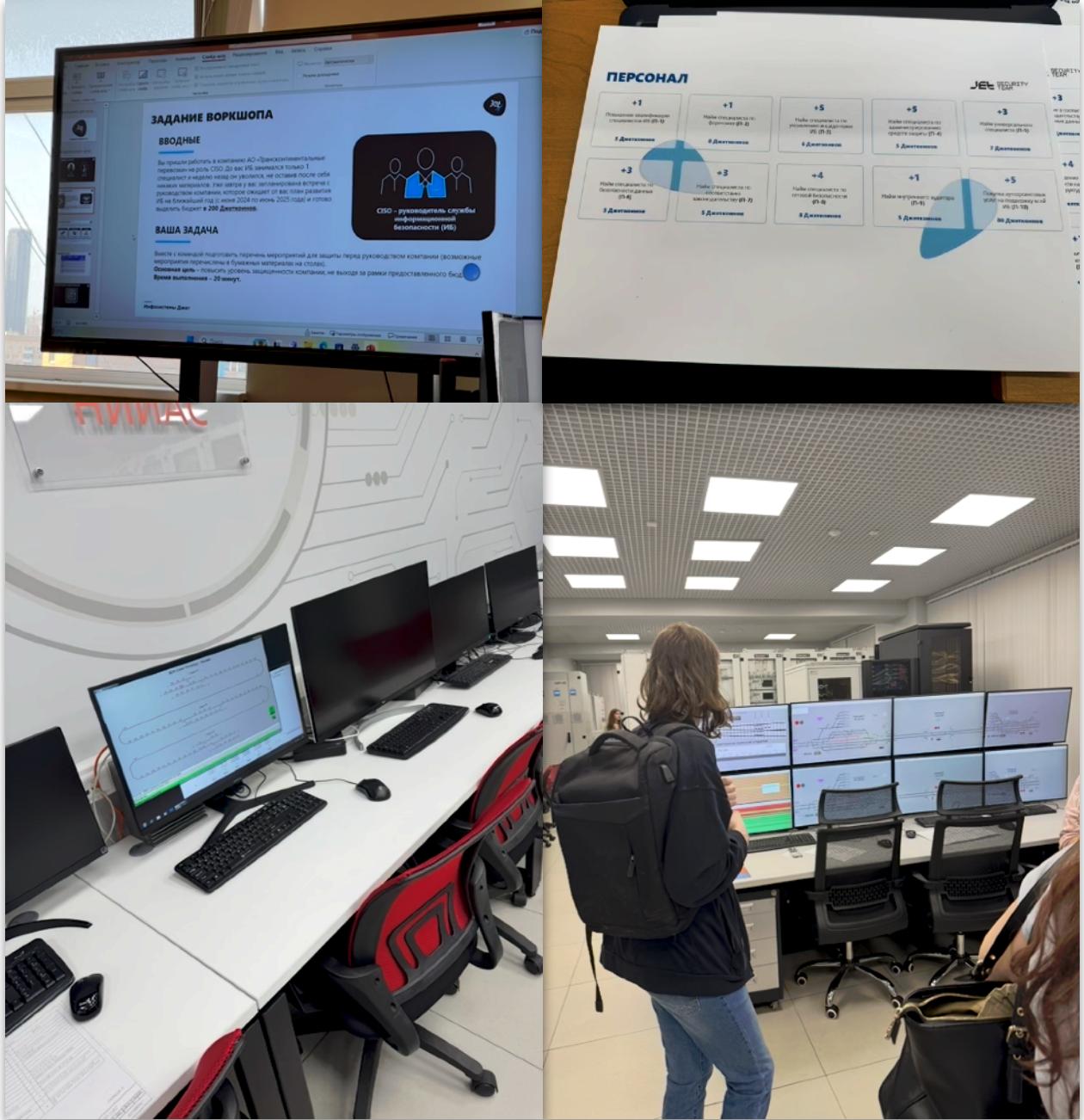
On the right side of the IDE, there is a terminal window showing the command `git clone https://github.com/CBarvian/practice-2025.git`. A tooltip above the terminal says: 'Для продолжения работы над репозиторием на локальном компьютере с привычным инструментарием, необходимо было клонировать созданный fork.' Below the terminal, another tooltip says: 'Ранее git уже был установлен на компьютер и настроен для работы из терминала.'

### Приложение 2. Скриншот опубликованного сайта

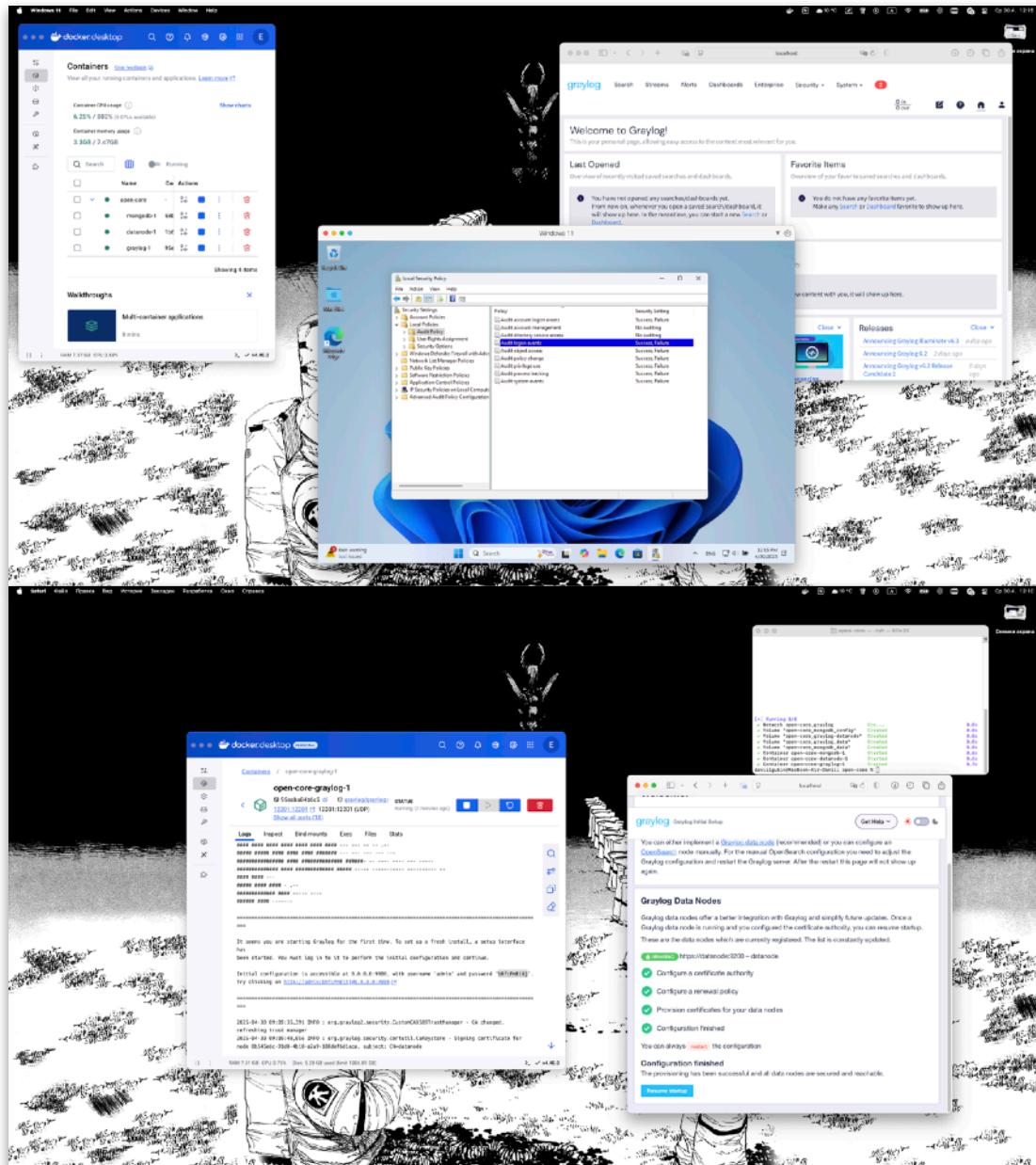
The screenshot shows a GitHub project page for 'oscarvan.github.io'. The page has the following sections:

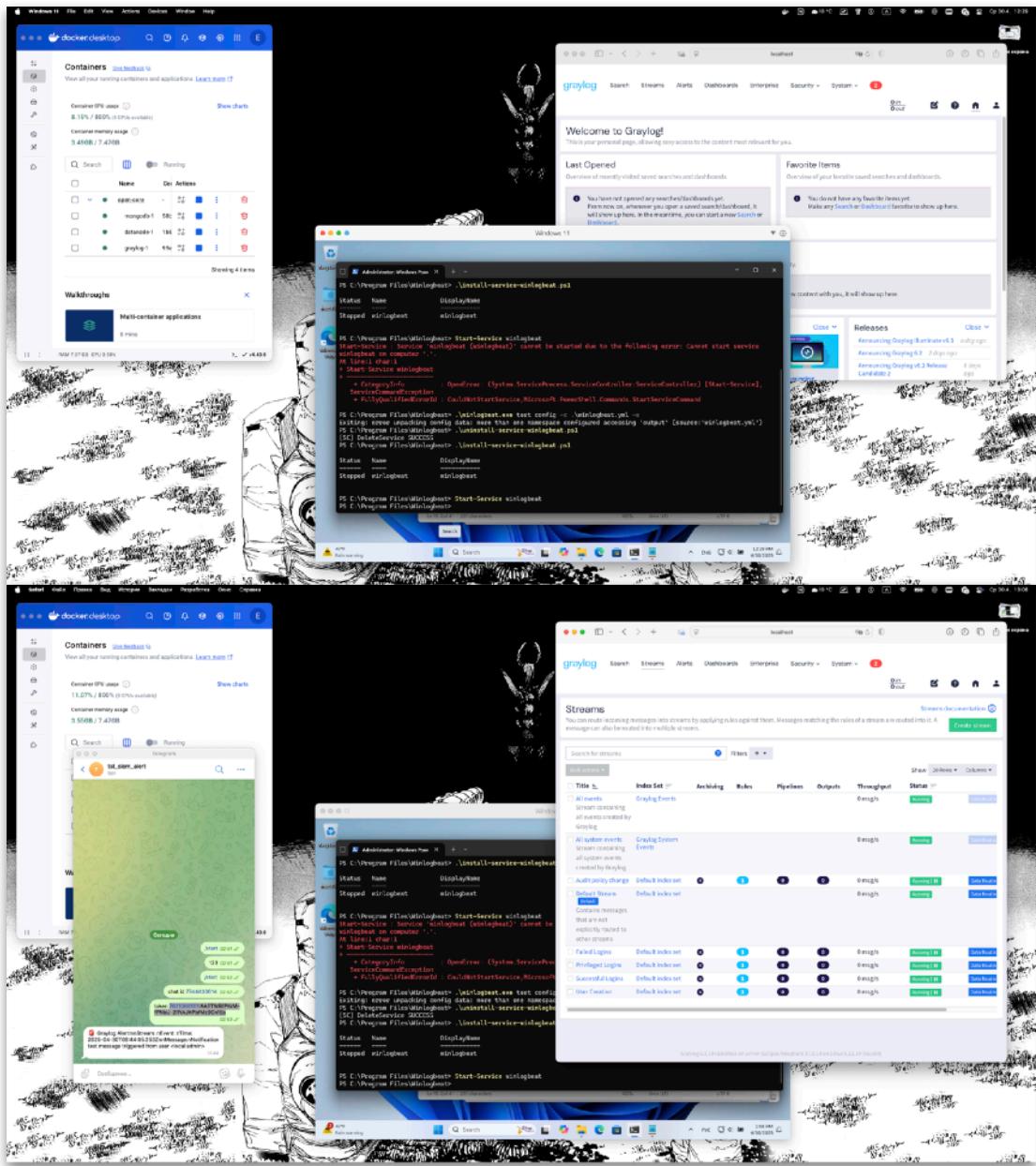
- Инфографика для популяризации свободного ПО**: A section with the title 'Главная'.
- Аннотация к проекту**:
  - Проект направлен на популяризацию свободного программного обеспечения (СПО) – через создание серии информативных и визуально привлекательных инфографик. В рамках работы команда разрабатывает дизайн-макеты, печатные и цифровые прототипы, а также взаимодействует с партнёрами для экспертной оценки.
  - Цель проекта – создать и напечатать набор наглядных текстово-графических материалов (листовки, плакаты, буклеты) для популяризации свободного программного обеспечения.
- Актуальность проекта**:
  - Свободное программное обеспечение с открытым кодом бесплатно, безопасно и широко применяется – от госструктур до личного использования, а возможность его свободного редактирования раздвигает информационную среду России, давая переход на СПО важным как для граждан, так и для государства.
- Аннотация к практике**:
  - Участники
  - ФИО   Учебная  
группа   Код  
направления   Профиль  
образовательной

### Приложение 3. Фото с мероприятий карьерного марафона



## Приложение 4. Скриншоты с выполненными пунктами индивидуального задания





The image consists of three vertically stacked screenshots of a Windows desktop environment.

**Top Screenshot:**

- Left Panel:** Shows the Docker Desktop interface with a container named "test\_start\_alert". It displays resource usage (CPU 6.42%, Memory 3.54GB / 7.47GB) and a list of running containers.
- Middle Panel:** A PowerShell window titled "Administrator Windows PowerShell" runs the command `Install-Service -Name \$logbeat` in the directory `C:\Program Files\WindowsPowerShell\`. The output shows the service being created and started.
- Right Panel:** A browser window for "graylog" shows the "API Key (Optional)" configuration page. It includes fields for "API Key (Optional)", "API Secret (Optional)", and "Headers (Optional)". Below these are dropdowns for "HTTP Method" (POST), "Content Type" (application/json), and "Time zone for data/time" (UTC). A "Body Template" section contains a JSON template for a POST/PUT body. A success message at the bottom indicates "Logbeats are created successfully."

**Middle Screenshot:**

- Left Panel:** Shows the Docker Desktop interface with a container named "test\_start\_alert". Resource usage is shown.
- Middle Panel:** A PowerShell window titled "Administrator Windows PowerShell" runs the command `Install-Service -Name \$logbeat` in the directory `C:\Program Files\WindowsPowerShell\`. The output shows the service being created and started.
- Right Panel:** A browser window for "graylog" shows the "Event Definitions" page. It lists several event definitions with their descriptions, priorities, last matched times, and statuses. One entry is highlighted with a green checkmark: "Event definition 'defn\_audit\_policy\_change' was created successfully." The status is "Success".

**Bottom Screenshot:**

- Left Panel:** Shows the Docker Desktop interface with a container named "test\_start\_alert". Resource usage is shown.
- Middle Panel:** A PowerShell window titled "Administrator Windows PowerShell" runs the command `Install-Service -Name \$logbeat` in the directory `C:\Program Files\WindowsPowerShell\`. The output shows the service being created and started.
- Right Panel:** A browser window for "graylog" shows the "Search" interface. It includes a search bar, a histogram for "MessageCount" over time, and a list of log entries. One entry is highlighted: "The Windows Filtering Platform has permitted a connection." The timestamp is 2025-04-19T14:33:48Z.