Общество с ограниченной ответственностью «Ребреин»
ИНН 7727409582, ОГРН 1197746106161
Адрес: 123056, город Москва, Большая Грузинская ул, д. 36а стр. 5а, офис 13

Утверждено
Приказом № ПР-1 от 17.06.2025 г.

Генеральный директор


_____ Фролкина Е.А.
«17» июня 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
– ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«АНАЛИЗ ЛОГОВ И ДИАГНОСТИКА СИСТЕМ В DEVOPS-СРЕДЕ»

Срок реализации: 1 месяц
Количество часов: 37 акад. ч.
Форма обучения: заочная форма
Формат обучения: с применением исключительно дистанционных технологий
Возраст обучающихся: для лиц старше 17 лет, имеющих или получающих среднее профессиональное и (или) высшее образование

Москва, 2025 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая дополнительная профессиональная программа – программа повышения квалификации «Анализ логов и диагностика систем в DevOps-среде» (далее – Программа) разработана в соответствии с:

- Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Постановлением Правительства РФ от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Профессиональным стандартом 06.015 «Специалист по информационным системам», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 13 июля 2023 г. № 586н;
- ФГОС высшего образования – бакалавриат по направлению 09.03.03 Прикладная информатика, утв. приказом Минобрнауки России от 19.09.2017 №922.

В данной программе учтены основные идеи формирования универсальных учебных действий учащихся и соблюдена преемственность с программами высшего и/или среднего профессионального образования.

Направленность программы: Программа имеет техническую направленность.

Адресат:
Программа ориентирована на специалистов, работающих с эксплуатацией и поддержкой IT-инфраструктуры, а также тех, кто стремится улучшить процессы мониторинга и диагностики в DevOps-среде. Курс будет полезен:

- DevOps-инженерам, желающим систематизировать и углубить знания в области сбора, хранения и анализа логов.
- Системным администраторам, которым важно быстро находить и устранять неисправности в системах на основе логов.
- Инженерам по наблюдаемости (Observability Engineers), отвечающим за стабильность и предсказуемость поведения сервисов.
- Разработчикам, стремящимся лучше понимать жизненный цикл приложений в продуктивной среде и быстро находить причины ошибок.
- IT-специалистам, переходящим в DevOps-сферу, и желающим освоить стек инструментов для логирования и диагностики.

Требования к входным знаниям обучающегося:
Для успешного освоения программы слушателям необходимо:

- Иметь базовые знания системного администрирования и принципов работы операционных систем (Linux);
- Понимать архитектуру современных распределённых приложений и микросервисов;
- Владеть начальными навыками работы с контейнерами (например, Docker) и знанием DevOps-подходов;
- Иметь базовое представление о логировании и мониторинге в IT-инфраструктуре.

Актуальность реализации:

Современные IT-системы становятся всё более распределёнными и сложными. Эффективная диагностика инцидентов, устранение сбоев и обеспечение надёжности сервисов невозможны без налаженного процесса централизованного сбора, хранения и анализа логов. DevOps-инженеры, системные администраторы и специалисты по наблюдаемости сталкиваются с необходимостью быстро интерпретировать логи и извлекать из них ключевую информацию для принятия технических решений.

Программа позволяет системно подойти к теме логирования, разобраться в архитектуре инструментов (Fluentd, rsyslog, Elasticsearch, Graylog, Vector), и научиться выстраивать отказоустойчивые и масштабируемые цепочки логирования, что критически важно для обеспечения стабильности современных инфраструктур.

Отличительные особенности программы:

- Фокус на практику: каждый инструмент и подход рассматриваются через реальные кейсы из DevOps-практики, а обучение сопровождается заданиями по настройке и отладке логирования;
- Полный стек инструментов: охватываются как классические, так и современные решения для логирования, включая Fluentd, Elasticsearch, Graylog, Kibana и Vector;
- Внимание к продвинутым конфигурациям: слушатели научатся настраивать фильтрацию, буферизацию, сетевое взаимодействие и безопасность логов;
- Подход DevOps-инженера: в центре внимания — обеспечение наблюдаемости, отказоустойчивости и быстрой диагностики сбоев;
- Актуальность: программа учитывает современные практики и архитектуры логирования в контейнерных и облачных средах.

Объем и срок освоения программы: 37 академ. ч. в течение 1 мес.

Доступ к материалам Программы у обучающихся остаётся и после окончания периода обучения. Это позволяет повторять изученный материал в удобное время, восполнять пробелы в знаниях, а также возвращаться к практическим заданиям при решении рабочих задач. Такой формат способствует более глубокому закреплению навыков и поддерживает профессиональное развитие выпускников даже после завершения обучения.

Выдаваемый документ о квалификации: удостоверение о повышении квалификации и/или сертификат об успешном освоении программы.

Цели и задачи программы:

Сформировать у слушателей системное понимание процесса сбора, обработки и анализа логов в современных IT-инфраструктурах, а также обучить применению инструментов логирования (rsyslog, Fluentd, Elasticsearch, Graylog, Vector) для диагностики, мониторинга и повышения отказоустойчивости сервисов.

Программа направлена на решение следующих основных задач:

Обучающие:

- Объяснить архитектуру логирования в Linux и контейнерных средах;
- Научить использовать инструменты сбора логов: rsyslog, Fluentd, Vector;
- Познакомить с системами хранения и визуализации логов: Elasticsearch, Kibana, Graylog;
- Показать приёмы диагностики и анализа на основе логов.

Развивающие:

- Развить навыки построения устойчивой и масштабируемой системы логирования;

- Способствовать формированию аналитического подхода к решению инцидентов;
- Углубить понимание связей между логами, мониторингом и безопасностью.

Воспитательные:
- Сформировать ответственное отношение к качеству мониторинга и наблюдаемости;
- Воспитать культуру технической аккуратности при работе с продакшн-инфраструктурой;
- Подчеркнуть важность логирования как основы стабильной работы сервисов и принятия обоснованных решений.

Планируемые результаты:
Знания:
- Принципы логирования в Linux и контейнерных средах;
- Назначение и архитектура инструментов: rsyslog, Fluentd, Vector, Elasticsearch, Kibana, Graylog;
- Возможности визуализации логов и создания дашбордов;
- Особенности настройки потоков логов, фильтрации, буферизации и доставки;
- Типовые сценарии использования логов для диагностики и мониторинга.

Умения:
- Настраивать сбор логов с помощью rsyslog и Fluentd;
- Реализовывать маршрутизацию и фильтрацию логов;
- Конфигурировать хранение логов в Elasticsearch и Graylog;
- Использовать Kibana и Graylog для анализа и визуализации логов;
- Подключать и отлаживать сбор логов из Docker-контейнеров;
- Выявлять ошибки и аномалии в логах для последующего устранения проблем в инфраструктуре.

Навыки:
- Создание устойчивой цепочки логирования в DevOps-среде;
- Быстрая диагностика системных и прикладных ошибок по логам;
- Внедрение инструментов логирования в существующую инфраструктуру;
- Оптимизация производительности лог-систем (буферы, парсеры, плагины);
- Работа с реальными логами в распределённых и облачных окружениях.

Перечень профессиональных компетенций, на получение которых направлено обучение:
На основе профстандарта 06.015 «Специалист по информационным системам»:
- A/06.4 Исправление дефектов и несоответствий в коде информационной системы и документации к информационной системе в соответствии с трудовым заданием в рамках технической поддержки процессов создания (модификации) и сопровождения информационной системы.

Таким образом, в результате освоения программы у обучающихся формируются следующие профессиональные компетенции:
- ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности
- ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

Организационно-педагогические условия реализации программы дополнительного профессионального образования

Язык реализации образовательной программы: обучение проводится на русском языке.

Форма обучения: заочная форма.

Особенности реализации программы: программа реализуется с использованием электронного обучения и исключительно дистанционных образовательных технологий.

Условия набора: на обучение принимаются все желающие лица, оплатившие обучение и заключившие договор об образовании. Обучение проходит в индивидуальном формате без формирования учебных групп. Обучающийся самостоятельно определяет время освоения Программы.

Формы проведения занятий:

- занятия в текстовом формате;
- практическая работа;
- самостоятельная работа с литературой;
- индивидуальные вопросы.

Материально-техническое оснащение

Материальное обеспечение программы

Занятия проводятся в системе дистанционного обучения «Rebrain». Каждый обучающийся и педагог оснащены доступом к системе дистанционного обучения: https://rebrainme.com/.

У педагога дополнительного профессионального образования имеется необходимое оборудование средства для реализации программы: ноутбук с подключением к интернету, программное обеспечение.

Методическое обеспечение программы

Программа обеспечена:

- учебно-методическими материалами (текстовые занятия, полезными материалами);
- практическими заданиями.

Кадровое обеспечение:

К реализации программы в качестве педагогов дополнительного образования допускаются лица:

1) отвечающее одному из требований:

а) имеющее высшее образование или среднее профессиональное образование в рамках укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования «Образование и педагогические науки»;

б) имеющее высшее образование либо среднее профессиональное образование в рамках иных укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования при условии его соответствия дополнительной общеобразовательной общеразвивающей программе, реализуемой ООО «Ребреин», и получение при необходимости дополнительного профессионального образования педагогической направленности;

в) успешно прошедшее промежуточной аттестации не менее чем за два года обучения по образовательным программам высшего образования по специальностям и

направлениям подготовки, соответствующей направленности дополнительной общеобразовательной общеразвивающей программе;

2) не имеющее ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации;

3) прошедшее обязательный предварительный (при поступлении на работу) и периодические медицинские осмотры (обследования), а также внеочередные медицинские осмотры (обследования) в порядке, установленном законодательством Российской Федерации.

Реализация Программы также возможна лицами, привлекаемыми на условиях гражданско-правового договора в соответствии с действующим законодательством РФ.

2. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модуля	Количество часов			Формы контроля / аттестация
		Всего	Теория	Практика	
1	Модуль 1 “Онбординг”	1	0,5	0,5	Входное тестирование
2	Модуль 2 “Logs”	32	12	20	Практическое задание
3	Модуль 3 “Финальная работа”	4		4	Итоговое практическое задание

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование модуля	1 неделя	2 неделя	3 неделя	4 неделя
1	Модуль 1 “Онбординг”	1			
2	Модуль 2 “Logs”	8	9	9	6
3	Модуль 3 “Финальная работа”				4 | А

4. РАБОЧАЯ ПРОГРАММА

Модуль 1. Онбординг
Теория 0,5 академ. ч. Практика 0,5 академ. ч.
Модуль состоит из следующих тем:

Тема 1: Онбординг

В модуле обучающемуся предоставляется вводный конспект, содержащий общую информацию о программе, структуре курса, форматах взаимодействия с материалами и ожидаемых результатах обучения.

Предусмотрено прохождение входного тестирования, включающего 7 вопросов, направленных на закрепление информации из онбординга. В рамках блока обучающийся выполняет задание по целеполаганию: формулирует свою цель прохождения программы, указывает желаемые навыки по окончании обучения, а также оценивает текущий уровень своих знаний.

Модуль 2. Logs
Теория 12 академ. ч. Практика 20 академ. ч.
Модуль состоит из следующих тем:

Тема 1: Как и куда приложения пишут логи
Содержание: Краткая сводка о логах. Способы записи логов. Формат логов. Практическое задание.

Тема 2: Rsyslog и его основные настройки
Содержание: Сервис управления логами RSyslog. Настройка сервера. Секция Modules. Секция Global directives. Секция Rules. Создание правил. Язык скриптов RainerScript. Шаблоны. Практическое задание.

Тема 3: Fluentd и его аналоги
Содержание: Четыре системы для сбора, обработки и трансляции логов. Пять этапов работы Fluentd. Базовые настройки Fluentd. Практическое задание.

Тема 4: Fluentd: расширенные настройки
Содержание: Теги. Лейблы. Вложенные секции. Практическое задание.

Тема 5: Fluentd и работа с сетью
Содержание: Секция Buffer. Input & Output Plugins. Практическое задание.

Тема 6: Fluentd и сбор логов из Docker
Содержание: Настройка сервера. Fluentd docker. Fluentd — установка и запуск с помощью DEB-пакета. Запуск docker container с выводом журналов во Fluentd. Работа с плагинами Fluentd. Практическое задание.

Тема 7: Обзор Elasticsearch
Содержание: Ключевые понятия Elasticsearch. Установка и настройка безопасности. Настройка ES в командной строке. Обзор API. Практическое задание.

Тема 8: Настройка кластера Elasticsearch
Содержание: Репликация (replication). Шардирование (sharding). Практическое применение стратегий масштабирования. Шардирование в Elasticsearch. Коэффициент репликации (replication factor) шардов. Разнесение данных по разным индексам. Настройка кластера Elasticsearch. Дополнительные настройки и рекомендации. Практическое задание.

Тема 9: Kibana
Содержание: Скачивание, установка, настройка Kibana. Запросы в Kibana. Визуализатор. Kibana Dashboard. Практическое задание.

Тема 10: Использование буфера для приёмки логов
Содержание: Обзор систем обработки очередей сообщений. Погружение в Kafka. Конфигурация ZooKeeper. Конфигурация Broker. Настройки Topic. Практическое задание.

Тема 11: Graylog — всё в одном
Содержание: Установка. Веб-интерфейс Graylog. Настройка Docker. Практическое задание.

Тема 12: Продвинутая настройка Graylog
Содержание: Graylog streams. Пользователи в Graylog. Роли. Практическое задание.

Тема 13: Vector
Содержание: Обзор инструмента. Сравнение с Fluentd. Особенности и компоненты Vector. Трансформации. Назначения.

Модуль направлен на формирование у обучающихся базовых и продвинутых навыков по настройке и отладке логирования. Каждый блок модуля включает текстовое занятие с теоретическим материалом и пошаговыми инструкциями, после изучения которого предлагается практическое задание.

Практические задания рассчитаны на 2 академических часа. Выполнение заданий предполагает отправку решения на проверку через личный кабинет обучающегося. Критерии оценки прописаны в описании к каждому заданию. В случае корректного выполнения выставляется зачёт. Если работа содержит ошибки, задание возвращается на доработку. При повторной неудачной попытке (после двух доработок) обучающийся получает «незачёт».

Модуль 3. Финальная работа

Блок посвящён выполнению финального практического задания без предварительного теоретического блока.

5. МЕТОДИЧЕСКИЕ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Программа обеспечена системой дистанционного обучения https://rebrainme.com/.

Педагогические технологии:
- технология дифференцированного обучения;
- технология разноуровневого обучения;
- технология развивающего обучения;
- технология проблемного обучения;
- технология дистанционного обучения.

Методы обучения:
- словесный, наглядный практический;
- объяснительно – иллюстративный;
- частично-поисковый, исследовательский проблемный;
- игровой, дискуссионный.

Электронно-библиотечные ресурсы и системы, информационно-справочные системы:

1. Научная электронная библиотека eLIBRARY.RU.
2. Собственные учебные материалы: https://rebrainme.com/logs/
3. Официальная документация Docker [Электронный ресурс]: https://docs.docker.com/engine/logging/configure/#supported-logging-drivers
4. Официальная документация Rsyslog [Электронный ресурс]: rsyslog documentation
5. Официальная документация Fluentd [Электронный ресурс]: https://docs.fluentd.org/quickstart
6. Официальная документация Elasticsearch [Электронный ресурс]: https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-elasticsearch-from-archive-on-linux-macos
7. Язык запросов Kibana [Электронный ресурс]: https://www.elastic.co/docs/explore-analyze/query-filter/languages/kql

6. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценочные материалы:
Для отслеживания результатов освоения программы среди слушателей проводится текущий контроль и итоговое оценивание.

Текущий контроль
Осуществление текущего контроля проводится после занятий в виде написания практических заданий или тестирований. Тематика и условия выполнения практических заданий расписаны в личном кабинете обучающегося в СДО. Педагог проверяет решение и принимает решение о принятии решения (зачет), о необходимости доработать решение или о незачете. Если промежуточный контроль представлен в виде тестирования, подсчет верных ответов и выставление оценки «зачёт» и «незачёт» происходят в автоматическим решиме в СДО.

Как отрыть, сделать и сдать задание

1. Нажмите кнопку «Создать окружение». Начнётся создание окружения, состоящего из одной или более виртуальных машин с Ubuntu Linux, к которым выдаются IP, логин и пароль для доступа по SSH. Создание окружения занимает до 5 минут.
2. По необходимости вам станут доступны переменные, которые указаны в фигурных скобках, например, ${base_domain}. Подставьте их при выполнении задания.
3. После выполнения нажмите кнопку «Проверить задание», и в течение ближайших 3-5 минут скрипт проверит выполнение всех условий и выдаст обратную связь.
4. Если вы что-то забыли или сделали неверно, можно исправить ошибки и отправить задание на проверку повторно через кнопку «Проверить задание».
5. Если время на таймере истекло, окружение автоматически уничтожится и вам придётся начать задание заново.
6. После получения удовлетворительной оценки нажмите кнопку «Удалить окружение», чтобы созданное окружение уничтожилось и вы могли приступить к следующему заданию.
7. Если вы успешно выполнили задание, но у вас остались вопросы, задайте их ментору через кнопку «?» или в канале практикума в Mattermost. Менторы проверяют вопросы в течение 24 часов.

Тема 3: Fluentd и его аналоги

1. Установите Fluentd как сервис (fluentd.service).
2. Сконфигурируйте Fluentd на чтение логов из файла /var/log/app.log. Помните про формат логов (apache2).
3. Сконфигурируйте отправку лога в syslog с помощью плагина fluent-plugin-remote_syslog. Отправленные логи пометьте тегом apache, используйте плагин remote_syslog для записи сообщений в файл syslog. Помните о протоколе UDP по умолчанию.
4. Сгенерируйте файл лога (/var/log/app.log) с помощью проекта flog.

wget
https://github.com/mingrammer/flog/releases/download/v0.4.3/flog_0.4.3_linux_amd64.tar.gz
tar -xzvf flog_0.4.3_linux_amd64.tar.gz
mv flog /usr/bin/
flog -t log -f apache_common -o /var/log/app.log # вариант с разной генерацией логов
tail -f /var/log/app.log
for _ in $(seq 1 100); do sudo flog -t log -w -f apache_common -o /var/log/app.log; done # вариант генерации логов в цикле

5. Проверьте наличие логов приложения в syslog.

6. После выполнения настроек смело нажимайте «Проверить выполнение».

Итоговое оценивание
В конце программы обучающиеся сдают итоговую аттестацию.

Заказчик без сисадмина

Итак, представьте. Вы работаете в компании, которая оказывает услуги по администрированию систем и проектов. Ваша команда специализируется на обработке и анализе логов.

В среду к вам обратился новый заказчик. У него уволился единственный системный администратор, и теперь никто не знает, что и как настроено на серверах. Известно только, что веб-серверы проксировали запросы к контейнерам.

Вам предстоит разобрать старый конструктор и найти все рабочие детали. Рекомендуем начать с анализа сохранившихся логов, но для этого необходимо их распарсить и обработать.

Задание

1. Настроить Elasticsearch кластер из трех нод, на серверах es0[1-3].
2. Настроить на сервере logs-aggregator:
- kibana - таким образом, что бы даже при отсутствии связи с одной или двумя нодами Elasticsearch, данные для поиска и отображения были доступны.
- apache.kafka - для временного хранения сообщений лога, до их обработки и отправки в кластер elasticsearch.
- fluentd - вычитывать сообщения из kafka обробатывать и отправлять в соответствующий index в elasticsearch.
3. Настроить на серверах app[1-3]:
- вычитывание всех текущих и исторических системных логов.
- вычитывание всех текущих и исторических логов приложений.
- отправка всех вычитанных сообщений в kafka.
- чем и как вы будете вычитывать сообщения, мы вас не ограничиваем, но вам надо будет аргументировать и объяснить ваш выбор, а так же приложить к ответу соответствующие конфигурационные файлы. Желательно в виде текста оформленного в кодовый блок, а не в качестве архива с файлами.

Результаты текущего контроля и итогового оценивания отображаются в личном кабинете слушателя в системе дистанционного обучения https://rebrainme.com/.
По результатам сдачи текущего контроля и итогового оценивания педагог даёт обратную связь слушателям, отмечает их сильные стороны и обращает внимание на зоны для развития. При необходимости педагог может повторить пройденные темы со слушателями, если установлен факт плохого закрепления и усвоения темы у слушателей.