Платформа Радар

Руководство по установке и обновлению

Версия 4.2.3

ООО «Пангео Радар»

Оглавление

1. Общие сведения о «Платформе Радар»

Специализированное программное обеспечение «**Платформа Радар**» (далее – **СПО РАДАР**, **Платформа Радар**, платформа) является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и предназначено для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности (далее – ИБ) с целью выявления инцидентов и организации реагирования на них.

СПО РАДАР поставляется в виде дистрибутива, предназначенного для установки на сервер или группу серверов.

СПО РАДАР может быть расположено как локально для работы исключительно внутри контура Заказчика, так и у внешнего оператора, оказывающего услуги мониторинга информационной безопасности.

СПО РАДАР после внедрения функционирует в автоматизированном режиме под управлением администратора Заказчика.

СПО РАДАР в вычислительной сети Заказчика не накладывает ограничений на функционирование серверов и рабочих станций Заказчика, подключаемых к системе в качестве источников событий ИБ.

Платформа обеспечивает решение следующих задач:

- сбор информации об активах, их учет и управление записями об активах;
- сбор событий ИБ от активов и/или от установленного на активах ПО;
- автоматическая обработка поступивших событий (нормализация, обогащение);
- загрузка и анализ результатов работы сканеров уязвимостей;
- корреляция событий, создание записей об инцидентах и управление ими;
- автоматизированный контроль реагирования на инциденты, контроль устранения;
- получение, обновление и использование информации об угрозах;
- ручной анализ событий ИБ при расследовании инцидентов;
- формирование отчетов, в том числе в графическом виде (рабочие столы).

СПО РАДАР имеет сертификат соответствия ФСТЭК России № 4210 от 05 февраля 2020 г. (переоформлен 22 марта 2022 г.), срок действия: пять лет.

2. Лицензирование

2.1 Лицензирование Платформы Радар

Лицензионное соглашение – это юридически обязывающий договор об использовании **Платформы Радар** между пользователями и компанией ООО "Пангео Радар".

Перед установкой **Платформы Радар** необходимо внимательно ознакомиться с лицензионным соглашением. Этот документ включен в комплект поставки.

Лицензия – это переданное лицензиаром неисключительное право на использование **Платформы Радар** лицензиату на определенный в лицензии срок, предоставляемое на основании лицензионного соглашения.

Стандартные условия лицензионного соглашения предусматривают:

- установленный срок (или отсутствие срока в случае бессрочной лицензии) действия лицензии и использования **Платформы Радар**;
- оказание технической поддержки в течение года после получения лицензии. Срок может быть продлен по соглашению лицензиара и лицензиата;
- обновление **Платформы Радар** до актуальной версии в течение года после получения лицензии. Срок может быть продлен по соглашению лицензиара и лицензиата.

2.2 Ограничения лицензии

Стандартные ограничения лицензии включают в себя:

- установленный срок лицензии, если это предусмотрено лицензионным соглашением;
- установленный средний поток событий (EPS). Определяется договором и лицензионным соглашением. Может быть изменен по соглашению лицензиара и лицензиата;
- установленное максимально возможное для добавления количество лог-коллекторов (агентов сбора);
- наличие или отсутствие режима Мультиарендности и установленное максимальное количество экземпляров **Платформы Радар**;
- наличие подключенных интеграций.

Лицензия соотносится с системным окружением, на которое была выполнена установка **Платформы Радар**.

Внимание: *При копировании **Платформы Радар** в другое системное окружение (физическую или виртуальную машину) лицензия прекращает свое действие*.

Для сменившегося системного окружения требуется заново получить лицензию в службе технической поддержки **Платформы Радар**.

При превышении среднего потока событий, более установленного лицензией, будет отображено сообщение о превышении, но все функции продолжат свою работу.

При дальнейшем превышении среднего потока событий более 1000 EPS в течение 7 дней будет отображено сообщение о введении следующих ограничений:

- о добавлении новых компонентов сбора и обработки событий;
- о подключении новых источников.

Остальные функции **Платформы Радар** продолжат работать в штатном режиме.

При окончании срока лицензии будет отображено соответствующее сообщение. Все функции **Платформы Радар** продолжат свою работу, но будет доступен только раздел **Администрирование → Лицензия**.

3. Функционирование

3.1 Структура

СПО РАДАР состоит из сервисов, каждый из которых предназначен для выполнения определенных функций. Сервисы могут объединяться в подсистемы (наборы сервисов) в зависимости от их функционального назначения.

СПО РАДАР включает в себя основные подсистемы:

- **PANGEORADAR-CORE** – подсистема управления **Платформой Радар**;
- **PANGEORADAR-WORKER** – подсистема обработки событий;
- **PANGEORADAR-CORRELATOR** – подсистема корреляции событий;
- **PANGEORADAR-EVENT-STORAGE** – подсистема хранения событий;
- **PANGEORADAR-LOG-COLLECTOR** – подсистема сбора событий.

Помимо основных подсистем в состав **СПО РАДАР** входят подсистемы, которые можно установить, как самостоятельные, в случае распределенной установки, или в составе подсистемы **PANGEORADAR-CORE**:

- **PANGEORADAR-MONITORING** – подсистема мониторинга работоспособности платформы;
- **PANGEORADAR-BALANCER** – подсистема балансировки событий;
- **PANGEORADAR-TI** – подсистема справочной информации об угрозах.

Перечень сервисов СПО РАДАР приведены в «Табл. 1».

Табл. 1 – Перечень сервисов в составе подсистем Платформы Радар

№	Подсистема	Сервис	Описание
1	PANGEORADAR-MONITORING	Alert-manager	Менеджер уведомлений. Отвечает за пересылку уведомлений от PANGEORADAR-MONITORING в PANGEORADAR-CORE
2	PANGEORADAR-BALANCER	Beaver	Балансировщик обработчика событий. Отвечает за балансировку приходящего потока события из сервиса **Kafka** и направляет их в базу данных **OpenSearch**
3	PANGEORADAR-CORE	Cerberus	Межсервисный шлюз. Выступает посредником между клиентами и сервисами, выполняя различные функции, связанные с маршрутизацией запросов к API
4	PANGEORADAR-CORE	ClusterAgent	Агент управления узлом кластера. Отвечает за управление состоянием узла, на котором он установлен
5	PANGEORADAR-CORE	Cm	Менеджер кластера. Отвечает за управление кластером, а именно распределение нагрузки, регистрацию процессов и мониторинг состояния узлов
6	PANGEORADAR-CORE	Cruddy	Центр управления API. Обрабатывает и отвечает на все запросы, выполняемые по API
7	PANGEORADAR-CORE	DatasApi	Отчетность. Отвечает за формирование отчетов о работе платформы
8	PANGEORADAR-CORE	Docs	Документация. Обеспечивает доступ к документации на продукт

№	Подсистема	Сервис	Описание
9	PANGEORADAR-WORKER	Enricher	Обогащение событий. Отвечает за процесс заполнения полей нормализованных событий дополнительной информацией
10	PANGEORADAR-CORE	EventAnt	Менеджер обмена информацией с центрами реагирования на компьютерные инциденты
11	PANGEORADAR-CORRELATOR	FlowBalancer	Балансировщик коррелятора. Отвечает за балансировку результатов корреляции и пересылку их в базу данных.
12	PANGEORADAR-MONITORING	Grafana	Визуализация метрик работы платформы. Предоставляет пользователям набор виджетов для визуализации метрик.
13	PANGEORADAR-MONITORING	KafkaExporter	Экспорт метрик с сервиса Kafka
14	PANGEORADAR-WORKER	Kafka	Передача данных и событий между сервисами платформы
15	PANGEORADAR-CORE	Karaken	Провайдер мультиарендности. Предоставляет возможности для реализации архитектуры мултитенант или мультиарендность
16	PANGEORADAR-CORE	KeyCloak	Аутентификация. Отвечает за управление доступом пользователей к платформе
17	PANGEORADAR-LOG-COLLECTOR	Logcollector	Сбор событий от источников и их передача в платформу. За сбор отвечают агенты сбора лог-коллектора: - agent - отвечает за сбор событий с ОС Linux - agent win - отвечает за сбор событий с ОС Windows
18	PANGEORADAR-CORRELATOR	Logmule	Коррелятор событий. Отвечает за корреляцию событий согласно правилам корреляции
19	PANGEORADAR-WORKER	Logproxy	Пересылка событий от лог-коллектора в сервис Kafka. Замена сервиса Rsyslog
20	PANGEORADAR-MONITORING	NodeExporter	Сбор метрик с узлов кластера
21	PANGEOEVENT-STORAGE	Opensearch	Хранение и поиск обработанных событий
22	PANGEORADAR-MONITORING	Opensearch-exporter	Сбор метрик с хранилища событий
23	RADAR-CORE	Pg	База данных
24	PANGEORADAR-MONITORING	Prometheus	Сбор и хранение метрик работы **Платформы Радар**
25	PANGEORADAR-CORE	Sonar	Сканирование активов
26	PANGEORADAR-WORKER	Termit	Отвечает за процедуру разбора и нормализации событий
27	PANGEORADAR-TI (RADAR-CORE)	Ti	Обновление информации об угрозах
28	PANGEORADAR-CORE	Toller	Оповещения. Отвечает за формирование уведомлений от **Платформы Радар** и пересылки сформированных уведомлений пользователям и администраторам
29	PANGEORADAR-CORE	Ui	Главный интерфейс. Отвечает за предоставление пользователям веб-интерфейса платформы
30	PANGEORADAR-CORE	Wal-listener	Интеграционный слой. Отвечает за управление интеграциями со сторонними системами

3.2 Обработка и корреляция событий

Схема взаимодействия подсистем, отвечающих за сбор, обработку и корреляцию событий приведена на «Рис. 1».

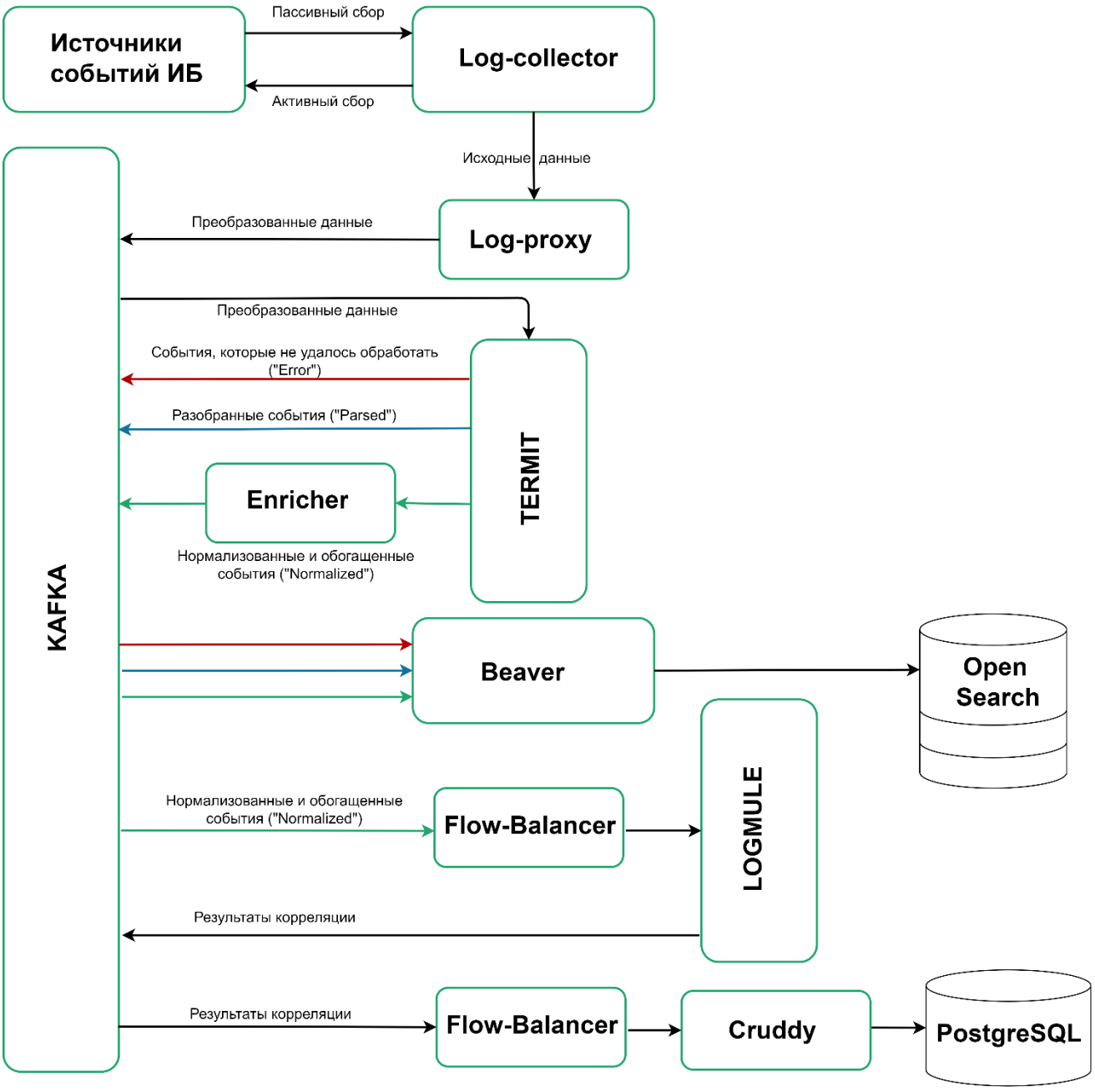

Рис. 1 – Схема обработки и корреляции событий

Принцип работы:

1. **Источники событий ИБ** – это любой актив, устройство, программное обеспечение в инфраструктуре организации, которое может создавать журналы работы.
2. **Log-Collector** (лог-коллектор) осуществляет сбор событий от источников. Сбор может выполняться двумя способами:
    - Активный сбор – лог-коллектор обращается к источнику для сбора событий;
    - Пассивный сбор – источник самостоятельно отправляет события в лог-коллектор.

3. **Log-proxy** обрабатывает полученные события и оптимизирует их для быстрой пересылки в сервис **Kafka**.
4. **Kafka** направляет полученный поток событий в обработчик **Termit**.
5. **Termit** обрабатывает события согласно правилам разбора и распределяет их по трем топикам:
    - **Error** – в ходе разбора события возникли ошибки и его не удалось разобрать;
    - **Parsed** – событие разобрано на пары **«Ключ-Значение»**;
    - **Normalized** – полученные пары **«Ключ-Значение»** подготовлены для передачи в таксономию.
6. Топики **Error**, **Parsed** и **Normalized** возвращаются в **Kafka**. При этом топик **Normalized** дополнительно проходит процедуру обогащения сервисом **Enricher**.
7. Балансировщик **Beaver** забирает все топики из сервиса **Kafka** и направляет их в базу данных **OpenSearch**. При этом **Beaver** по меткам времени раскладывает события в индексы **OpenSearch**.
8. Балансировщик **FlowBalancer** работает параллельно **Beaver** и забирает из сервиса **Kafka** только события из топика **Normalized**. Затем фильтрует их согласно фильтрам потока событий и если событие подходит под условие, то оно пересылается в коррелятор (сервис **Logmule**).
9. **Logmule** осуществляет корреляцию событий согласно правилам корреляции. Результаты корреляции возвращаются в сервис **Kafka**.
10. Балансировщик **FlowBalancer** забирает результаты корреляции и через центр управления API они отправляются в базу данных платформы.

3.3 Серверные роли

Наборам сервисов или подсистемам (установленным на сервере и выполняющим определенные функции для пользователей или других серверов), присваиваются серверные роли.

Серверная роль определяет основную функцию сервера, при этом одному серверу могут быть назначены несколько ролей, и одна роль может исполняться несколькими серверами. Перечень используемых ролей приведён в «Табл. 2».

Табл. 2 – Серверные роли СПО РАДАР

Наименование роли	Ролевой состав
MASTER	Включает подсистемы **RADAR-CORE** и **RADAR-TI**
BALANCER	Включает подсистему **RADAR-BALANCER**
WORKER	Включает подсистему **RADAR-TERMITE**
CORRELATOR	Включает подсистему **RADAR-LOGMULE**

Наименование роли	Ролевой состав
MONITORING	Включает подсистему **RADAR-MONITORING**. Часто устанавливается вместе с ролью **MASTER**
DATA	Включает подсистему **RADAR-EVENT-STORAGE**
BACKUP	Отвечает за резервное копирование платформы
AGENT/AGENT WIN	Включает подсистему **PANGEORADAR-LOG-COLLECTOR**, которая состоит из сервиса **logcollector-agent** и соответствующих агентов сбора

Важно! *Сервис **logcollector-manager** устанавливается в составе роли **MASTER**.*

Управление серверными ролями происходит через веб-интерфейс **Платформы Радар** в разделе **Администрирование → Кластер**.

3.4 Масштабирование

Каждая подсистема или сервис **СПО РАДАР** может масштабироваться следующим образом:

- «вертикально» — путем наращивания мощности конфигурации серверов;
- «горизонтально» — путем увеличения количества параллельно работающих единиц аппаратного обеспечения с копией масштабируемого сервиса или подсистемы.

В случае необходимости увеличения производительности конкретной подсистемы **Платформы Радар** можно оперировать как отдельно взятыми сервисами и/или подсистемами, так и серверными ролями.

4. Требования к ПО

4.1 Общие требования к ПО

Основной вариант поставки СПО РАДАР подразумевает что следующие элементы среды функционирования входят в состав комплекта поставки:

- **СУБД PostgreSQL** — система хранения данных.
- **OpenSearch** — поисковая система для работы с системами управления базами данных (СУБД).
- **Apache Kafka** — распределённый программный брокер сообщений.

Требование к ОС: **ОС Debian Linux 12.11 (amd64) / Astra Linux 1.8.3.2 и выше**.

Для работы с графическим интерфейсом **СПО РАДАР** на АРМ пользователя должен быть установлен один из следующих браузеров:

- **Microsoft Edge**;
- **Google Chrome**;
- **Яндекс.Браузер**.

4.2 Требования к СУБД, используемой как хранилище событий

СУБД для организации хранилища данных должна обеспечивать выполнение следующих задач:

- обработка параллельных запросов СУБД;
- сжатие хранимых данных;
- индексирование данных;
- репликация и распределенное хранение данных.

СУБД не имеет программных ограничений на срок online-хранения событий. Срок online-хранения зависит только от аппаратных ресурсов серверов СУБД.

Платформа Радар поддерживает сжатие данных при хранении журналов событий со средней степенью сжатия до 30-50% для оперативного хранения и до 80% для архивного хранения событий.

Платформа Радар позволяет использовать для хранения событий как локальные хранилища, так и внешние (сетевые). В случае необходимости масштабирования долгосрочного хранилища событий не потребуется глобальных изменений архитектуры решения.

5. Требования к ТО

Технические требования для работы **Платформы Радар** рассчитываются для обеспечения штатного функционирования в случае одновременной работы всех пользователей Заказчика.

5.1 Требования к АРМ оператора

Параметр	**Требование**
Процессор	1 процессор, не менее 4 ядер с тактовой частотой 2.1 ГГц
Жесткий диск	50 ГБ свободного пространства
Оперативная память	8 ГБ
Дополнительные устройства	Монитор (или несколько) с разрешением 1920x1080, Мышь, Клавиатура

5.2 Требования к конфигурации сервера

При подборе оптимальной конфигурации сервера для развертывания платформы следует учитывать следующие факторы:

1. Установка ПО будет централизованной или распределенной?

   Примеры конфигураций для установки на один сервер и для распределенной установки можно посмотреть в разделе «Примеры конфигурации аппаратного обеспечения».

2. Будут ли на сервере работать какие-либо приложения, не относящиеся к **Платформе Радар**?
3. Сколько событий в секунду должен обрабатывать сервер? Сколько событий в день должен обрабатывать сервер? Оба фактора являются переменными, при этом дневная цифра более важна для определения параметров сервера.
4. Какой средний размер события?
5. Сколько источников будет подключено к **Платформе Радар**?
6. Какие требования предъявляются к обеспечению отказоустойчивости?
7. Длительность хранения события?
8. Есть ли необходимость хранить исходное сообщение или достаточно только нормализованного варианта?

Перечисленные выше факторы (а также, при необходимости, дополнительные факторы) прорабатываются во время разработки проектного внедрения.

Также вопросы по подбору оптимальной конфигурации оборудования можно адресовать в службу технической поддержки, когда требуется определить размер и параметры оборудования "с нуля" или оценить возможности уже существующей потенциальной конфигурации.

Пример требований к серверу при централизованной установке:

Параметр	Требование
Процессор	1 процессор, 4 ядра, с тактовой частотой 2.1 ГГц
Жесткий диск	80 ГБ
Оперативная память	24 ГБ
Сетевые интерфейсы	1 серверный сетевой адаптер со скоростью передачи данных не менее 100 Мб/с|

Пример требований к серверу при распределенной установке:

Параметр	Требование
Процессор	1 процессор, 4 ядра, с тактовой частотой 2.1 ГГц
Жесткий диск	80 ГБ
Оперативная память	24 ГБ
Сетевые интерфейсы	1 серверный сетевой адаптер со скоростью передачи данных не менее 100 Мб/с|

5.3 Подбор параметров серверного оборудования

В данном разделе рассматриваются особенности подбора серверного оборудования для установки **Платформы Радар** по следующим критериям:

- производительность процессора;
- объём ОЗУ;
- объем и производительность дисковой подсистемы;
- требования к сети.

Дисковая подсистема является наиболее частым узким местом.

Производительность ЦП - второе по популярности узкое место.

Производительность сети обычно является узким местом только в случае установки распределенной инсталляции.

5.3.1 Подбор Процессора по производительности

При подборе серверного оборудования следует учитывать следующую информацию:

- Все модули **Платформы Радар** поддерживают 64-разрядные процессоры;
- Так как большинство модулей **Платформы Радар**, чувствительных к производительности, являются многопоточными, то ресурсы ЦП сервера можно представить как умножение количества ядер ЦП на скорость каждого ядра.

Два значения, которые часто включаются в спецификации ЦП (сервера), - это количество ядер ЦП и количество потоков ЦП. Например, ЦП может иметь 4 ядра и 8 потоков.

При выборе сервера рекомендуется рассматривать производительность ЦП с точки зрения количества потоков, так как данная метрика более актуальна для производительности **Платформы Радар**, чем физическое кол-во ядер ЦП.

5.3.2 Подбор объема ОЗУ

Разработчик **СПО ПР** рекомендует для каждого сервера **Платформы Радар** минимум **16 Гб** оперативной памяти. Дополнительная оперативная память может потребоваться в зависимости от требований к производительности **Платформы Радар**.

Увеличение объема установленной ОЗУ - эффективный способ снизить накладные расходы на операции дискового ввода-вывода.

Следующие компоненты являются основными пользователями оперативной памяти **Платформы Радар**:

- **PostgreSQL** - в идеальном случае оперативная память должна обеспечивать буферизацию всей базы данных. В большинстве случаев это невозможно, но чем выше процент базы данных, которая может быть буферизована в ОЗУ, тем лучше с точки зрения производительности. Объем дискового пространства, потребляемого PostgreSQL, рассмотрен в разделе «Требования к дисковому пространству»;
- **Kafka** - в большинстве случаев Kafka может работать с пространством кучи (heap) 6 Гб памяти. При таком режиме требуется кэш-память файловой системы размером до 28–30 Гб на машине с 32 Гб. Для повышенных производственных нагрузок рекомендуется использовать машины 32 Гб ОЗУ и выше. В этом случае дополнительная оперативная память будет использоваться для поддержки кеширования страниц ОС и повышения пропускной способности клиентов. Kafka также может работать и с меньшим объемом оперативной памяти, но при этом его способность справляться с нагрузкой затрудняется. Для нормальной работы Kafka потребуется достаточно много памяти для буферизации активных процессов чтения и записи. Можно сделать предварительную оценку потребностей в памяти, исходя из необходимости иметь возможность буферизования в течение 30 секунд. Тогда потребность в памяти вычисляется как write_throughput * 30. Менее 32 Гб ОЗУ, как правило, непродуктивно (в конечном итоге понадобится много маленьких машин);
- **RADAR TERMITE** - оптимальный размер оперативной памяти для сервиса 16 Гб;
- **RADAR LOGMULE** - объем ОЗУ определяется характером правил корреляции. Общая рекомендация - не менее 8Гб ОЗУ на инстанс;
- **OpenSearch** - стандартная рекомендация для производительных кластеров - 32 Гб на ноду кластера OpenSearch;
- **Буферы файловой системы** - ОС обычно выделяет большую часть оставшейся оперативной памяти в этой области. Основная область, в которой буферы файловой системы могут улучшить производительность, - это балансировщик событий, очередь обмена сообщениями и хранилище событий.

Объем дискового пространства, который занимает балансировщик, очередь и хранилище очередей рассмотрены в разделе «Требования к дисковому пространству».

5.3.3 Подбор дисковой подсистемы

5.3.3.1 Рекомендации по вводу-выводу дисковой подсистемы

Для **Платформы Радар** в большинстве ситуаций производительность произвольного ввода-вывода дисковой подсистемы более важна, чем производительность последовательного чтения и записи, и может оказаться узким местом до ЦП или ОЗУ. Особенно это характерно для централизованной установки **Платформы Радар**, при которой происходит много операций записи и чтения разными модулями **Платформы Радар**, установленными на один сервер.

До определенного уровня производительности можно использовать накопители на магнитных дисках. Но для максимальной производительности рекомендуется использовать твердотельные накопители (SSD).

Один из ключевых показателей, на который следует обратить внимание при выборе дисковой подсистемы для использования, - это производительность в IOPS (операций ввода-вывода в секунду) как для случайного чтения, так и для произвольной записи.

5.3.3.2 Рекомендации по подбору файловой системы

Рекомендуется использовать файловые системы XFS и избегать EXT4.

- XFS - это высокопроизводительная масштабируемая файловая система, которая обычно развертывается в самых требовательных приложениях. RHEL 7 является файловой системой по умолчанию и поддерживается на всех архитектурах. XFS имеет свои преимущества, но при настройке JBOD она не дает особых преимуществ;
- EXT4 не масштабируется до того же размера, что и XFS.

5.3.3.3 Рекомендации по использованию твердотельного накопителя

Платформа Радар в настоящее время использует два разных уровня SSD-накопителей для собственных стендов:

- На серверах, для которых требуется скорость обработки до 10K событий в секунду или меньше, используются стандартные твердотельные накопители;
- На серверах, которым требуется скорость обработки более 10K событий в секунду, используются SSD-диски корпоративного класса. Желательно использование SSD с поддержкой технологии Write intensive.

Рекомендуется включать TRIM на SSD-дисках (если это возможно в конкретной модели) и использовать правильное выравнивание разделов.

В некоторых случаях уязвимым местом дисковой подсистемы становится диск или RAID-контроллер, поэтому при использовании твердотельных накопителей также рекомендуется проверить производительность диска или RAID-контроллера, к которому будут подключены твердотельные накопители.

5.3.3.4 Рекомендации по использованию магнитного накопителя

Если SSD-накопители не подходят, то рекомендуется использовать самую быструю доступную конфигурацию магнитного накопителя. Например:

- Использовать накопитель с не менее 10K оборотов, желательно 15K оборотов в минуту;
- Использовать диски SAS, так как они обычно быстрее, чем диски SATA;
- Использовать объединение несколько магнитных жестких дисков в один массив RAID 10. Даже если в конкретном случае не нужна совокупная емкость хранилища, то это один из способов увеличения производительности доступного дискового ввода-вывода.

Внимание! **Платформа Радар** не позволяет использовать магнитные накопители со скоростью оборотов менее 10K RPM.

5.3.3.5 Рекомендации по комбинированию твердотельных накопителей и магнитных дисков

Можно использовать комбинацию твердотельных накопителей и магнитных накопителей, чтобы воспользоваться преимуществами каждого из них:

- Компоненты, интенсивно использующие дисковый ввод-вывод, такие как база данных PostgreSQL, Kafka, OpenSeach, могут храниться на SSD;
- Компоненты с низким объемом операций ввода-вывода, такие как операционная система, журналы и резервные копии, могут храниться на магнитных дисках;
- Также рекомендуется переносить неиспользуемые индексы OpenSearch при длительном хранении на магнитные диски.

5.3.3.6 Рекомендации по использованию RAID-массивов

Чтобы оптимизировать производительность и обеспечить избыточность в случае отказа жесткого диска, рекомендуется использовать массивы RAID 1 и/или RAID 10.

Не рекомендуется использовать массивы RAID 5 и RAID 0.

При прочих равных условиях надежность **Платформы Радар** с использованием массива RAID 10 обычно превосходит надежность с использованием массивов RAID 5 и RAID 0.

5.3.3.7 Рекомендации по кэшированию чтения и записи на контроллерах RAID

Некоторые контроллеры RAID имеют возможность включить кэш чтения и/или записи.

Для **кэша записи** рекомендуется выполнить следующие действия:

- Отключить кэш записи RAID-контроллера, если нет заведомо исправного BBU (блока резервного питания от батареи). Это связано с тем, что кэш записи создает риск потери данных, когда нет работающего BBU;
- Если установлен заведомо исправный BBU, часто имеет смысл включить кэш записи RAID-контроллера. Выполнение этого на массиве RAID, который использует магнитные диски, почти всегда повысит производительность. Выполнение этого на RAID-массиве, в котором используются SSD-диски, часто, но не всегда, улучшает производительность. Это связано с тем, что SSD-диски достаточно быстры и используют собственное кэширование,

поэтому иногда дополнительные накладные расходы на выполнение кэширования записи оказывают влияние на производительность;

- Некоторые контроллеры RAID также имеют параметр конфигурации для отключения кэширования записи в случае отказа BBU. При наличии данного параметра конфигурации рекомендуется его включить.

Статья "Диски с точки зрения файловой системы" на ACM.org содержит более подробную информацию о том, как работает кэширование записи.

Для **кэша чтения** рекомендуется выполнить следующие действия:

- Перед включением кэша записи RAID-контроллера рекомендуется отключить его кэш чтения, чтобы для записи можно было выделить больше ресурсов кэша;
- Если кэш записи RAID-контроллера отключается, то имеет смысл включить кэш чтения RAID-контроллера.

Выполнение вышеприведенных действий по включению/отключению кэш на массиве RAID, который использует магнитные диски, в большинстве случаев улучшит производительность.

Выполнение вышеприведенных действий на массиве RAID, в котором используются SSD-диски, часто, но не всегда, улучшит производительность. Это связано с тем, что SSD-диски достаточно быстрые, поэтому иногда дополнительные накладные расходы на выполнение кэширования чтения влияют на производительность.

Мы рекомендуем отключить кэш чтения RAID-контроллера.

Оперативная память операционной системы может служить кэшем чтения и более доступна для ЦП, чем кэш RAID-контроллера.

5.3.4 Требования к дисковому пространству

Требования к дисковому пространству определяются следующими характеристиками:

- длительность хранения событий;
- количество событий в секунду, которые необходимо обработать **Платформе Радар**.

Вопросы по подбору оптимального дискового пространства или запросы для оценки существующего дискового пространства можно адресовать в службу технической поддержки.

5.4 Требования к параметрам сети

Быстрая и надежная сеть - важный компонент производительности в распределенной системе. Низкая задержка гарантирует, что узлы могут легко обмениваться данными, а высокая пропускная способность помогает перемещению и восстановлению сегментов. Современные сети центров обработки данных (1 GbE, 10 GbE) достаточны для подавляющего большинства кластеров.

Высокой пропускной способности при работе **Платформы Радар** не получится достичь при использовании сетевой подсистемы ниже, чем 1GbE.

5.5 Совместимость Платформы Радар с технологиями виртуализации

Платформа Радар совместима с некоторыми технологиями виртуализации, которые обеспечивают 64-разрядный процессор и установку ОС Debian 12 / Astra Linux 1.8.

Ниже приведены технологии виртуализации, совместимые с **Платформой Радар**:

- VMware ESX (i) и vSphere;
- Сервер VMware, использующий Linux или Windows в качестве ОС хоста;
- KVM;
- Xen;
- Сервер Microsoft Hyper-V;
- Виртуализация "Горизонт-ВС".

С точки зрения производительности рекомендуется с осторожностью использовать мощности облачного провайдера для установки **Платформы Радар**.

5.6 Примеры конфигурации аппаратного обеспечения

5.6.1 Конфигурация 1

Параметр	Значение
Период хранения в днях	30 (оперативного 30)
EPS	1000
Кол-во правил корреляции	700+

Серверные роли	Кол-во	CPU ядра	RAM GB	Хранилище GB	Сеть	ОС
MASTER	1	24	32	1000 (SSD)	1Gbps	DEBIAN 12
DATA-COLD	1	4	16	2200	1Gbps	DEBIAN 12
Суммарно	2	28	48	HDD 2200 Gb		
				SSD 1000 Gb		

5.6.2 Конфигурация 2

Параметр	Значение
Период хранения в днях	365 (оперативного 90)

Параметр	Значение
EPS	30000
Кол-во правил корреляции	700+

Серверные роли	Кол-во	CPU ядра	RAM GB	Хранилище GB	Сеть	ОС
MASTER	1	16	32	1000	1Gbps	DEBIAN 12 / Astra Linux 1.8
WORKER	2	16	32	500	1Gbps	DEBIAN 12 / Astra Linux 1.8
BALANCER	1	8	16	1000 (SSD)	1Gbps	DEBIAN 12 / Astra Linux 1.8
CORRELATOR	1	24	24	500	1Gbps	DEBIAN 12 / Astra Linux 1.8
Data-HOT	3	8	54	1600 (SSD)	1Gbps	DEBIAN 12 / Astra Linux 1.8
Data-COLD	2	4	44	90000	1Gbps	DEBIAN 12 / Astra Linux 1.8
Data-COORDINATOR	1	12	16	500	1Gbps	DEBIAN 12 / Astra Linux 1.8
Data-Archive	1	2	2	47000	1Gbps	DEBIAN 12 / Astra Linux 1.8
LOG-COLLECTOR	3	4	16	500 (SSD)	1Gbps	DEBIAN 12 / Astra Linux 1.8
Суммарно	15	138	454	HDD 230000		
				SSD 7300		

6. Подготовка к установке

6.1 Подготовка к установке на один сервер

6.1.1 Подготовка оборудования

Перед началом процесса необходимо выбрать наиболее подходящую конфигурацию оборудования (см. «Примеры конфигурации аппаратного обеспечения»).

Сервера, на которых разворачивается ПО **Платформы Радар**, далее именуются целевыми системами.

6.1.2 Подготовка дисковой системы

Подготовка к установке и запуску **Платформы Радар** должна осуществляться с учетом требований, представленных в разделах «Требования к ПО» и «Требования к ТО».

При разметке дисковой подсистемы необходимо учитывать следующие требования:

- корневой раздел (/) - все свободное пространство;
- раздел /home - 10 Гб;
- раздел swap - не менее 10% от общего объема оперативной памяти, исходя из требований к ресурсам для конкретного модуля **Платформы Радар** (см. раздел «Требования к ТО»);
- тип файловой системы - XFS (при необходимости можно использовать EXT4).

6.1.3 Подготовка аппаратной части

Подготовка как физического сервера, так и виртуальной машины выполняются по одинаковому сценарию и включают следующую последовательность операций:

1. Организация доступа к выбранным физическим серверам/виртуальным машинам, удовлетворяющих системным требованиям (см. «Требования к ТО»);
2. На физических серверах должна быть проведена разметка дисков (форматирование);
3. Установка ОС Debian 12 / Astra Linux 1.8 (процесс не рассматривается в данном документе);
4. Первичная настройка операционной системы (сетевая конфигурация, DNS, NTP).

6.1.4 Настройка сетевой конфигурации

1. Для доступа к веб-интерфейсам управления **Платформой Радар** инсталлятор откроет порты:
    - 443
    - 9000
    - 8080
    - 8180

2. Для корректного взаимодействия между сервисами платформы рекомендуется открыть следующие порты:
    - 9092
    - 9200
    - 5672
    - 15672
    - 5432
    - 2092
    - 8080
    - 8086
    - 9000
    - 8180
    - 6677
    - 6630
    - 1100
    - 22

Подробное описание сетевого взаимодействия приведено в разделе «Межсетевое взаимодействие».

6.1.5 Подготовка к установке

Подготовка для установки **Платформы Радар** включает обеспечение следующих условий:

- доступ к целевой системе по SSH (необходимо для копирования образов системы, файлов конфигурации и настройки системы);
- наличие учётной записи с правами привилегированного пользователя (администратора) ОС в целевой системе;
- при необходимости закомментировать репозитории ОС Debian Linux 12 (amd64), которые могут вызвать конфликты при установке.

6.1.5.1 Настройка SSH-сервера на Debian 12

1. Откройте терминал.
2. При необходимости обновите списки пакетов и установленные пакеты с помощью команд:

```
# sudo apt update
# sudo apt upgrade
```

3. Установить пакет OpenSSH сервера, если он ещё не установлен. Для этого нужно выполнить команду:

```
# sudo apt-get install openssh-server
```

4. OpenSSH сервер по умолчанию использует порт 22 для удаленных подключений. Если вы используете службу UFW, нужно разрешить удаленное подключение к порту 22. Для этого выполните команду:

   ```
   # sudo ufw allow ssh
   ```

5. Удостоверьтесь, что в конфигурации OpenSSH сервера разрешен **root-логин**. Для этого откройте конфигурационный файл /etc/ssh/sshd_config и проверьте настройки следующих параметров:

   ```
   PasswordAuthentication yes
   PermitRootLogin yes
   ```

6. Проверьте работу SSH-сервера с помощью команды:

   ```
   # sudo systemctl status ssh
   ```

6.1.5.2 Комментирование репозиториев на Debian 12

Чтобы избежать возможность загрузки не подходящих пакетов во время установки платформы и исключить конфликты и проблемы совместимости, характерные для сложных сценариев установки, необходимо закомментировать следующие репозитории:

```
# deb http://deb.debian.org/debian/ bookworm main
# deb-src http://deb.debian.org/debian/ bookworm main
# deb http://security.debian.org/debian-security bookworm-security main
# deb-src http://security.debian.org/debian-security bookworm-security main
```

Для этого откройте файл `/etc/apt/sources.list.d/pangeoradar.list` (ранее использовался `/etc/apt/sources.list`), закомментируйте в нем все строки и выполните команду:

```
# sudo apt update
```

6.2 Подготовка к распределенной установке

6.2.1 Подготовка оборудования

Подготовка оборудования для распределенной установки **Платформы Радар** производится аналогично подготовке оборудования для централизованной установки (см. раздел «Подготовка к установке на один сервер»), кроме задач подготовки дисковой системы и настройки сетевых конфигураций.

6.2.1.1 Подготовка дисковой системы к распределенной установке

Для распределенной установки при разметке дисковой подсистемы для всех серверных ролей, кроме серверной роли DATA, необходимо учитывать следующие (стандартные) требования:

- корневой раздел (/) - все свободное пространство;
- раздел /home - 10 Гб;
- раздел swap - не менее 10% от общего объема оперативной памяти, из требований к ресурсам для конкретного модуля **Платформы Радар** (см. раздел «Требования к ТО»);
- тип файловой системы - XFS (при необходимости можно использовать EXT4).

6.2.1.2 Настройка сетевой конфигурации при распределенной установке

1. Для доступа к веб-интерфейсам управления **Платформой Радар** нужно открыть порты:
    - 443
    - 9000
    - 8080
    - 8180
2. Между узлами кластера необходимо разрешить взаимодействие в обе стороны по следующим портам:
    - 9092
    - 9200
    - 5672
    - 15672
    - 5432
    - 2092
    - 8080
    - 8086
    - 9000
    - 8180
    - 6677
    - 6630
    - 1100
    - 22

В «Табл. 3» приведены необходимые сетевые настройки при распределенной установке **Платформы Радар** (независимо от вариантов распределенной установки).

Табл. 3 – Сетевые настройки для распределенной установки Платформы Радар

Исходящий	Входящий	Порты	Описание
Correlator	Master	5672	Чтение нормализованных событий из очереди для корреляции
Correlator	Master	8086	Передача результатов корреляции
Log-Collector	Balancer	1500-5000, 9997-9999, 15403, 15404TCP/UDP	Передача данных от сборщика в балансировщик и менеджер очередей
Log-Collector	Источники событий	21, 22, 135, 445, 1443, 3306, 5432, 5601	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками

Исходящий	Входящий	Порты	Описание
Log-Collector	Master	9000	Запрос конфигурационных данных
Master	Data	9200	Работа с сырыми событиями
Master	Correlator	2092	Управление правилами корреляции
Master	Log-Collector	4805 4806	Мониторинг и сбор статистики. Управление сборщиком событий API
Master	Balancer Correlator Data Worker	6676	Управление агентами кластера
Master	Balancer Correlator Data Worker	9100	Мониторинг и сбор статистики
Master	Balancer	9292, 9308	Мониторинг и сбор статистики
Master	Data	9114	Мониторинг и сбор статистики
Worker	Balancer	9092	Чтения событий из менеджера очередей для их обработки
Worker	Master	5672	Передача нормализованных событий в очередь на корреляцию
Worker	Data	9200	Передача событий на хранение
Источники событий	Log-Collector	162 SNMP trap; 4807 UDP receiver; 4808 TCP receiver; 4809 TCP receiver SSL/TLS; 4810 HTTP receiver; 4811 HTTPS receiver; 4812 NetFlow reciever	Пассивный сбор событий
Пользователи **Платформы Радар**	Master	8080 9000 6676 6677	Доступ к интерфейсу **Платформы Радар**, проверка API ключей
Data (с ролью Master)	Data (с ролью Data)	9300	Взаимодействие между нодами в кластере хранилища данных

Также подробное описание сетевого взаимодействия для различных вариантов установки приведено в разделе «Межсетевое взаимодействие».

6.2.2 Подготовка узлов

6.2.2.1 Настройка SSH-сервера на Debian 12

Аналогично с «Настройка SSH-сервера на Debian 12».

6.2.2.2 Настройка службы синхронизации времени в ОС Debian (NTP)

Примечание: *все команды выполняются от имени привилегированного пользователя*.

На всех узлах кластера необходимо настроить службу синхронизации времени.

Для настройки службы синхронизации времени необходимо выполнить следующие настройки:

1. Добавить адрес NTP сервера в файл конфигурации службы:

   ```
   echo 'NTP=<адрес NTP сервера>’>> /etc/systemd/timesyncd.conf
   ```

2. Перезапустить службу:

   ```
   systemctl restart systemd-timesyncd.service
   ```

3. Проверка синхронизации:

   ```
   timedatectl status
   ```

4. Проверка состояния службы:

   ```
   systemctl status systemd-timesyncd.service
   ```

5. Добавление службы в автозапуск:

   ```
   systemctl enable --now systemd-timesyncd.service
   ```

6.2.3 Комментирование репозиториев на Debian 12

Чтобы избежать возможность загрузки не подходящих пакетов во время установки платформы и исключить конфликты и проблемы совместимости, характерные для сложных сценариев установки, необходимо закомментировать следующие репозитории:

```
# deb http://deb.debian.org/debian/ bookworm main
# deb-src http://deb.debian.org/debian/ bookworm main
# deb http://security.debian.org/debian-security bookworm-security main
# deb-src http://security.debian.org/debian-security bookworm-security main
```

Для этого откройте файл `/etc/apt/sources.list.d/pangeoradar.list` (ранее использовался `/etc/apt/sources.list`), закомментируйте в нем все строки и выполните команду:

```
# sudo apt update
```

7. Установка

7.1 Установка Платформы Радар на один сервер

Внимание! *Установка должна выполняться с учетной записи с правами суперпользователя*.

Внимание! *Для корректной установки Платформы Радар в ОС Debian должна быть задана переменная PATH, содержащая полный список необходимых путей:* `/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin`. *В случае, если переменная PATH не содержит путей* `/usr/sbin` *и* `/sbin`, *их следует добавить вручную*.

Перечень шагов для выполнения установки платформы:

- Шаг 1. Распаковка дистрибутива и запуск скрипта для установки;
- Шаг 2. Получение лицензии;
- Шаг 3. Установка в веб-интерфейсе платформы;
- Шаг 4. Завершение установки.

7.1.1 Шаг 1. Распаковка дистрибутива и запуск скрипта для установки

Дистрибутив системы представляет собой архив **pgr-x.x.x.tar.gz**, где **x.x.x** – номер версии платформы.

1. Создайте каталог для размещения файлов платформы. Например, `/var/tmp/pgr-x.x.x/`:

   ```
   # cd /var/tmp/
   # mkdir pgr-x.x.x
   ```

   Где `x.x.x` - номер версии платформы.

2. Перейдите в созданный каталог и извлеките содержимое архива **pgr-x.x.x.tar.gz**.

   ```
   # tar -xvf <наименование установочного архива>
   ```

3. Запустите файл `install.sh` с правами суперпользователя:

   ```
   # sudo ./install.sh
   ```

4. Начнется процесс установки платформы. Установка занимает некоторое время, в течение которого загружаются и устанавливаются модули **Платформы Радар**.

5. После загрузки основных модулей инсталлятор попросит указать IP-адрес и доменное имя сервера (необязательно), на котором будет установлена **Платформа Радар**.

   Внимание! *Если вы хотите работать в DNS инфраструктуре, то на данном этапе установки необходимо указать доменное имя сервера (FQDN) и по завершению установки переключить режим подключения к платформе с IP на FQDN. Подробнее см.*

«Руководство администратора» → раздел «Настройка платформы для работы в DNS инфраструктуре».

6. Дождитесь окончания установки, после чего на экране появится сообщение об успешном завершении первого этапа:

```
Продолжите установку по адресу: https://<IP-адрес платформы>/install
Логин/Пароль по умолчанию - admin/admin
```

7.1.2 Шаг 2. Получение лицензии

Внимание! *В случае, если в инфраструктуре, куда устанавливается платформа, работает **Kaspersky Security Center (KSC)** и на машине, с которой будет проходить установка платформы через web-интерфейс, установлен **Kaspersky Endpoint Security (KES)**, то при установке, он подменит сертификаты на свои, что приведет к ошибкам. Необходимо отключить **KES** на соответствующей машине.*

1. Перейдите по адресу, указанному в конце работы инсталлятора: `http://<IP-адрес платформы>/install`.
2. Пройдите процедуру входа и смены пароля (по умолчанию: `admin/admin`). Откроется мастер установки на вкладке "Лицензия" (см. «Рис. 2»).

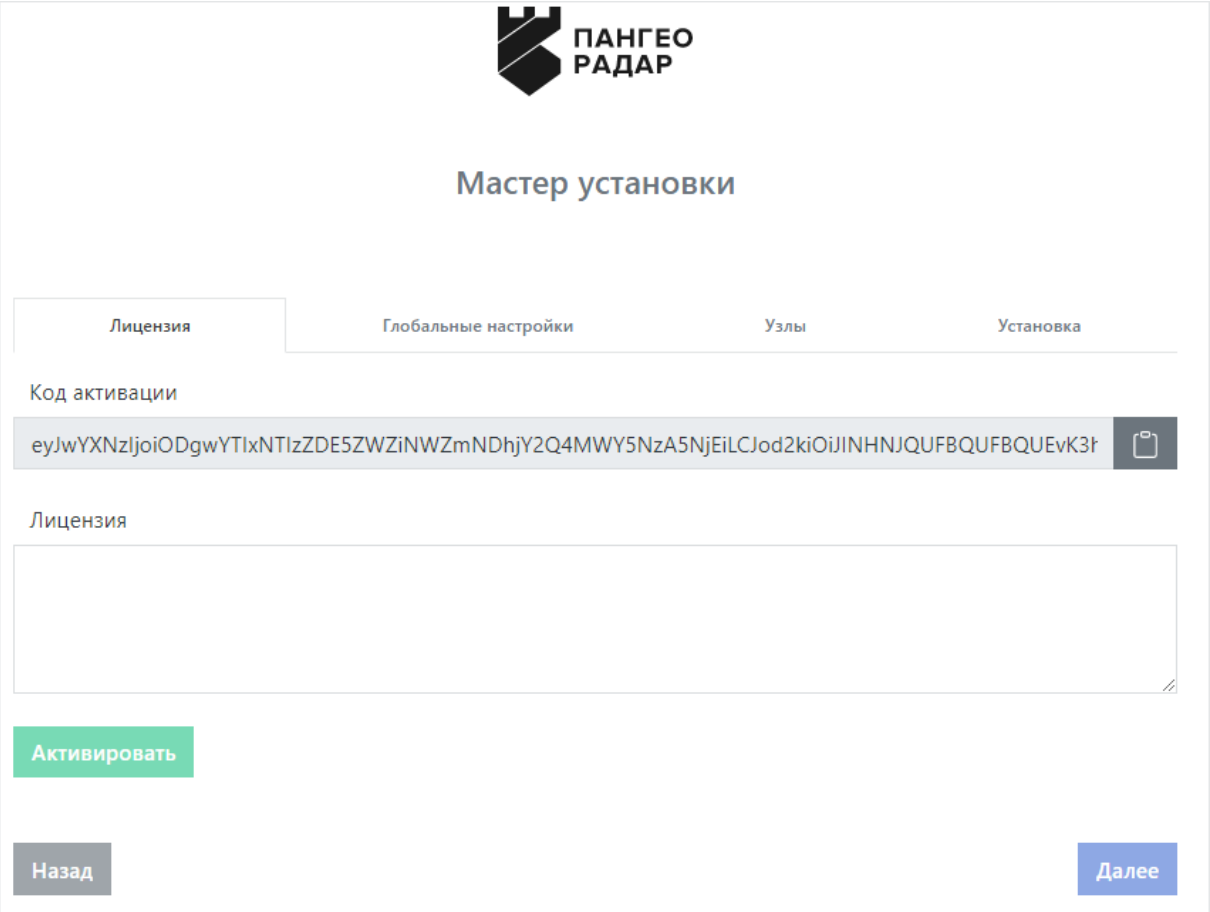

Рис. 2 – Мастер установки. Вкладка "Лицензия"

3. В поле **Код активации** отображается ваш код активации для получения. Скопируйте его с помощью кнопки . Рекомендуется сохранить скопированный код в текстовый файл.

4. Перейдите в личный кабинет клиентского портала **Платформы Радар** (см. «Рис. 3»).

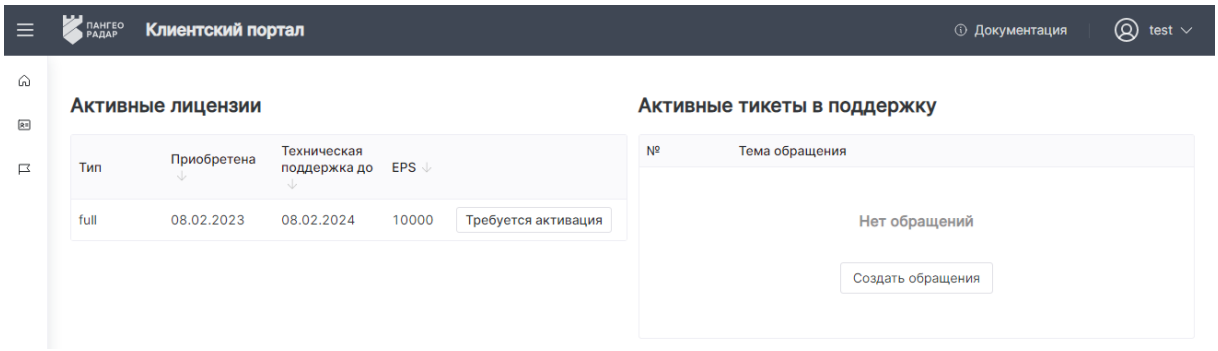

Рис. 3 – Клиентский портал Платформы Радар

5. Нажмите на кнопку **Требуется активация** и в открывшемся окне укажите, скопированный ранее, код активации. Будет выполнена активация лицензии, кнопка **Требуется активация** будет заменена на кнопку **Лицензия** (см. «Рис. 4»).

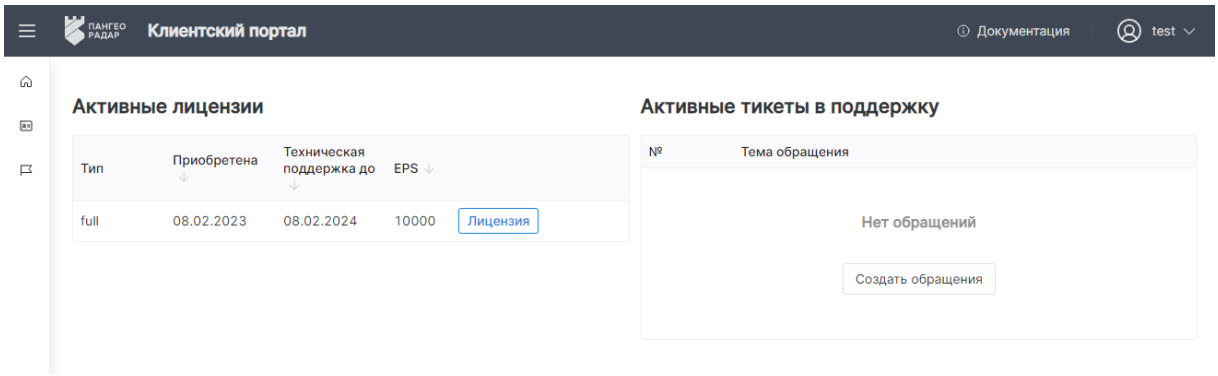

Рис. 4 – Клиентский портал. Кнопка получения лицензии

6. Нажмите на кнопку **Лицензия**. Откроется окно "Скачать лицензию" (см. «Рис. 5»).

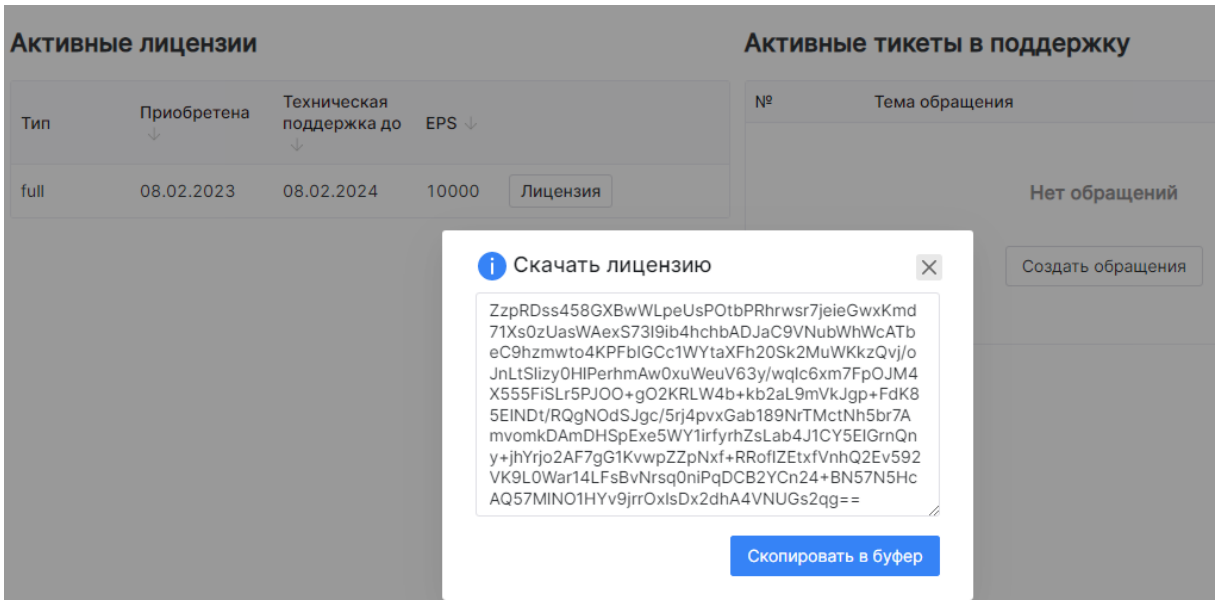

Рис. 5 – Окно "Скачать лицензию"

7. Скопируйте лицензию. Рекомендуется сохранить скопированное значение в текстовый файл.

8. Перейдите в мастер установки платформы на вкладку "Лицензия" (см. «Рис. 2»), в поле **Лицензия** укажите значение лицензии и нажмите кнопку **Активировать**. Лицензия будет активирована, а на экране будут отображены ее параметры (см. «Рис. 6»).

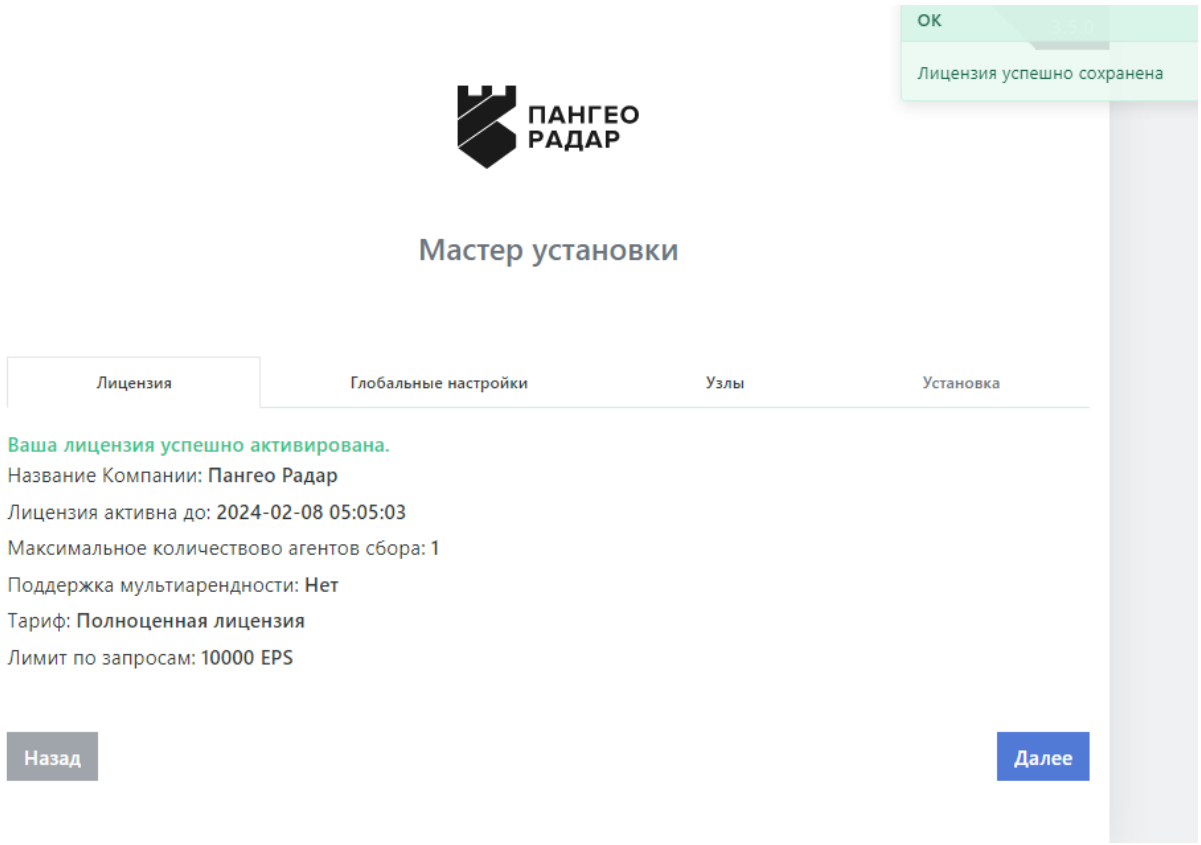

Рис. 6 – Параметры лицензии

7.1.3 Шаг 3. Установка в веб-интерфейсе платформы

1. После активации лицензии нажмите кнопку **Далее**. Откроется вкладка "Глобальные настройки" (см. «Рис. 7»).

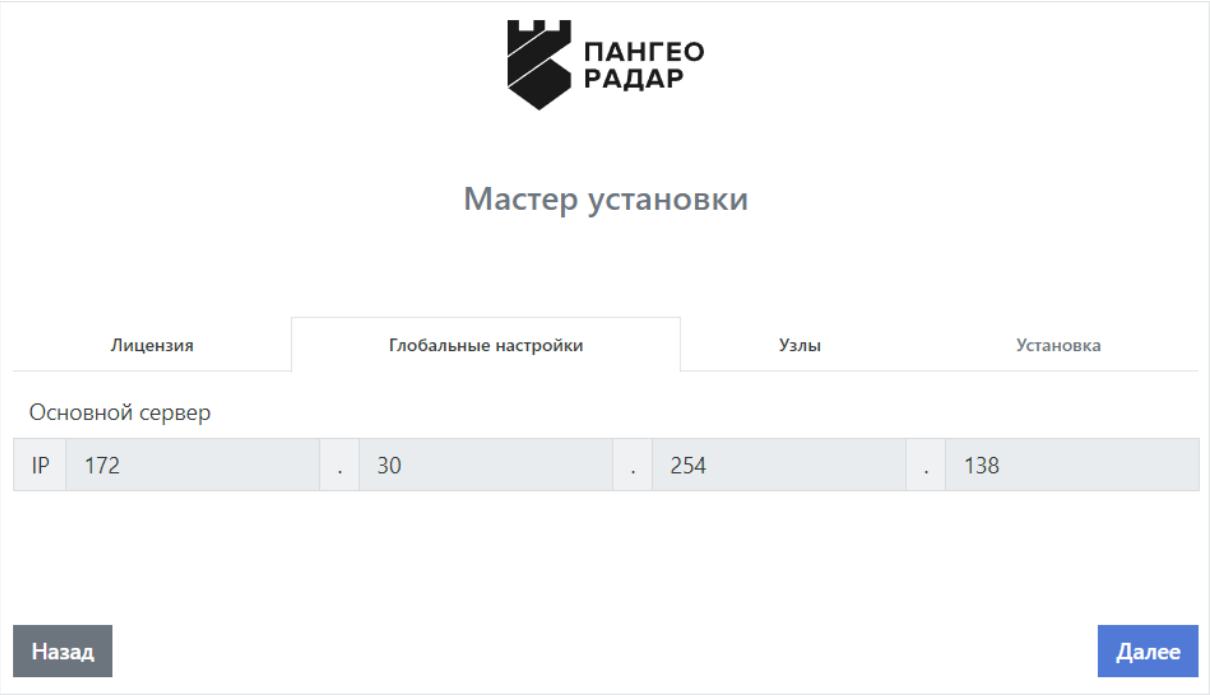

Рис. 7 – Мастер установки. Вкладка "Глобальные настройки"

2. На вкладке "Глобальные настройки" проверьте параметры основного сервера, указанные на первом шаге, и нажмите кнопку **Далее**. Откроется вкладка "Узлы" (см. «Рис. 8»).

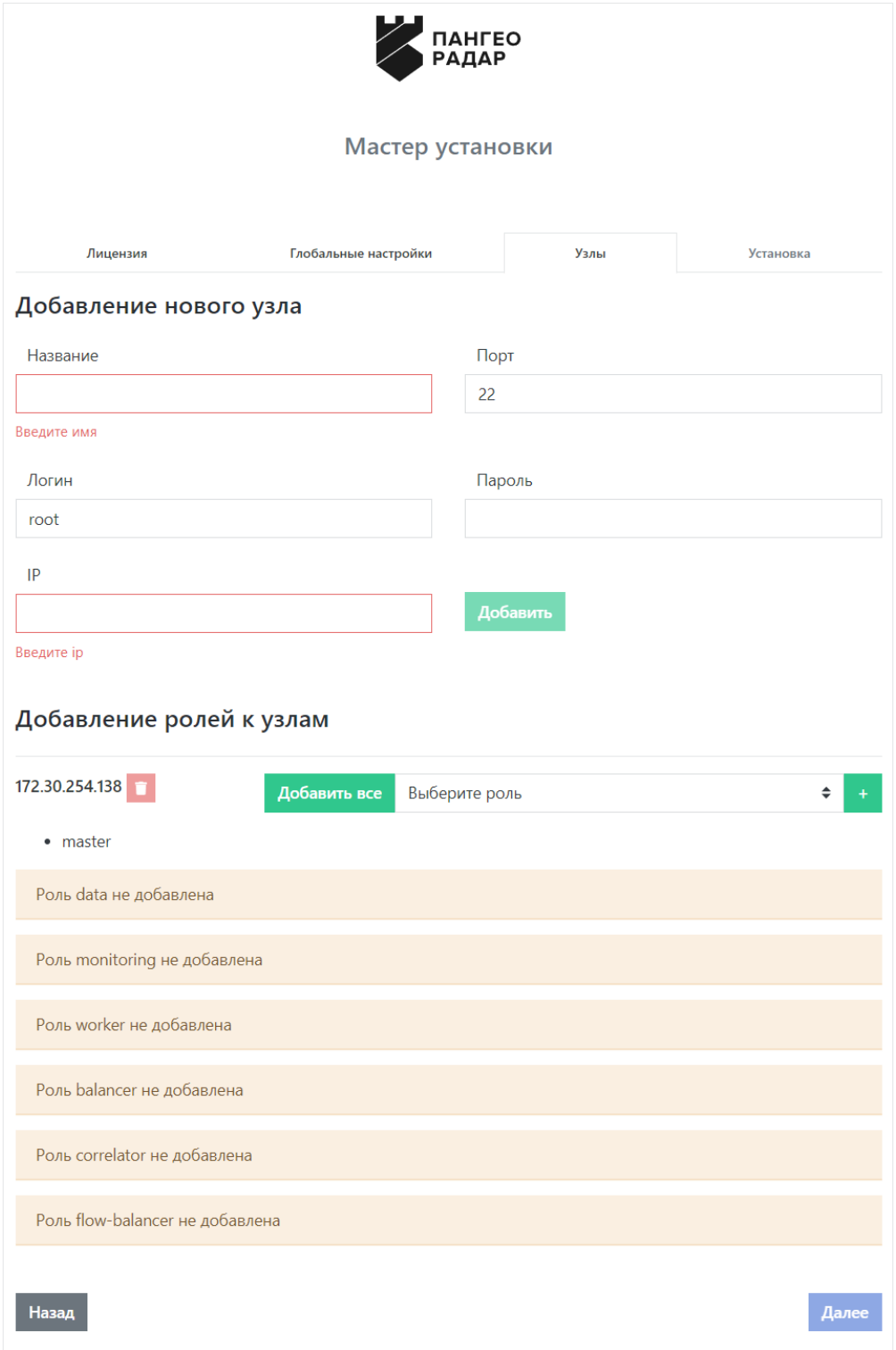

Рис. 8 – Мастер установки. Вкладка "Узлы"

3. На вкладке **Узлы** выполните следующие действия:
    - назначьте все возможные серверные роли на основной сервер. Для этого нажмите кнопку **Добавить все**.
    - из выпадающего списка **Выберите роль** выберите значение "*agent*".

Роли будут назначены на основной сервер (см. «Рис. 9»).

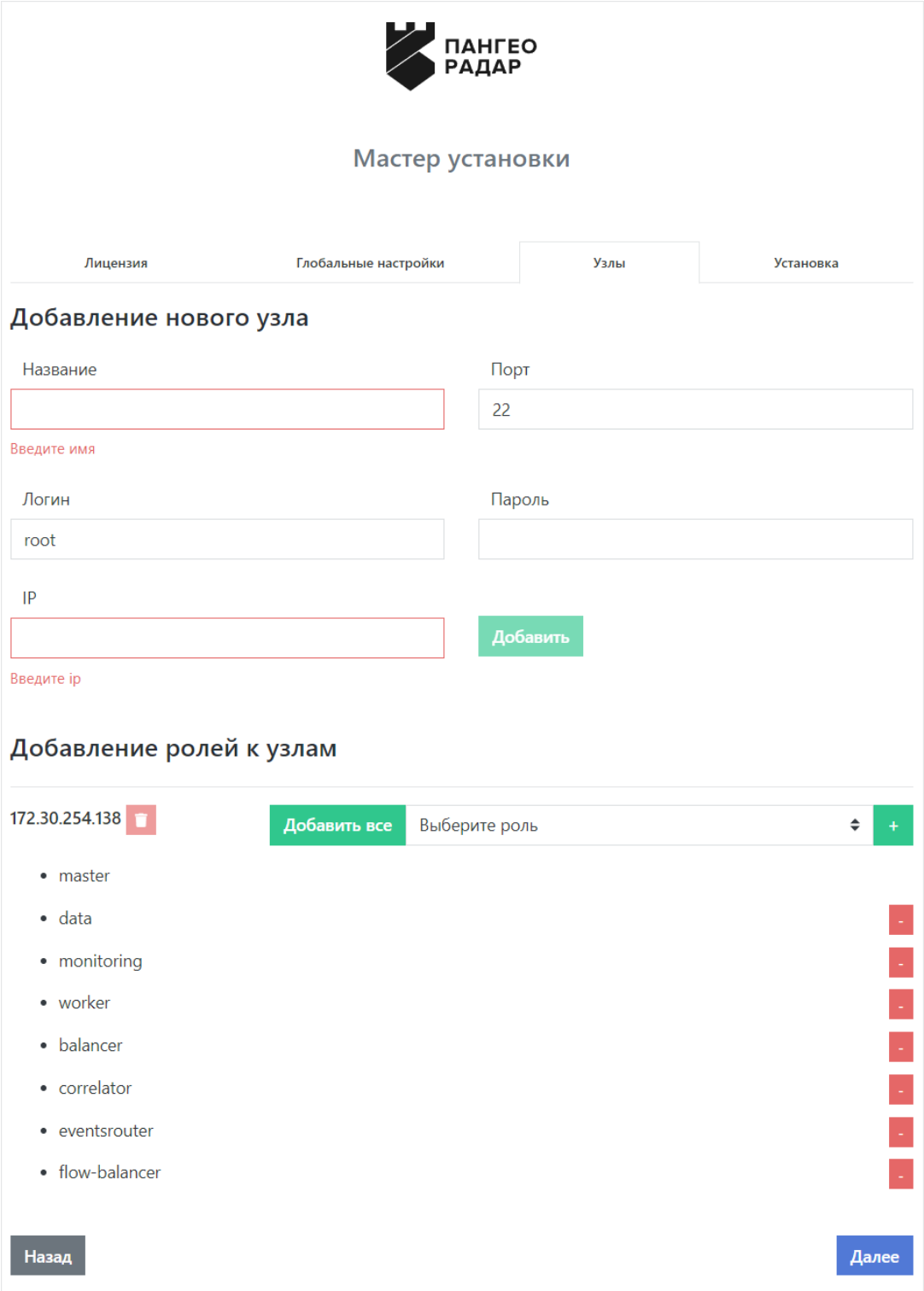

Рис. 9 – Мастер установки. Добавление всех ролей на один сервер

4. Нажмите кнопку **Далее**. Откроется вкладка "Установка" (см. «Рис. 10»).

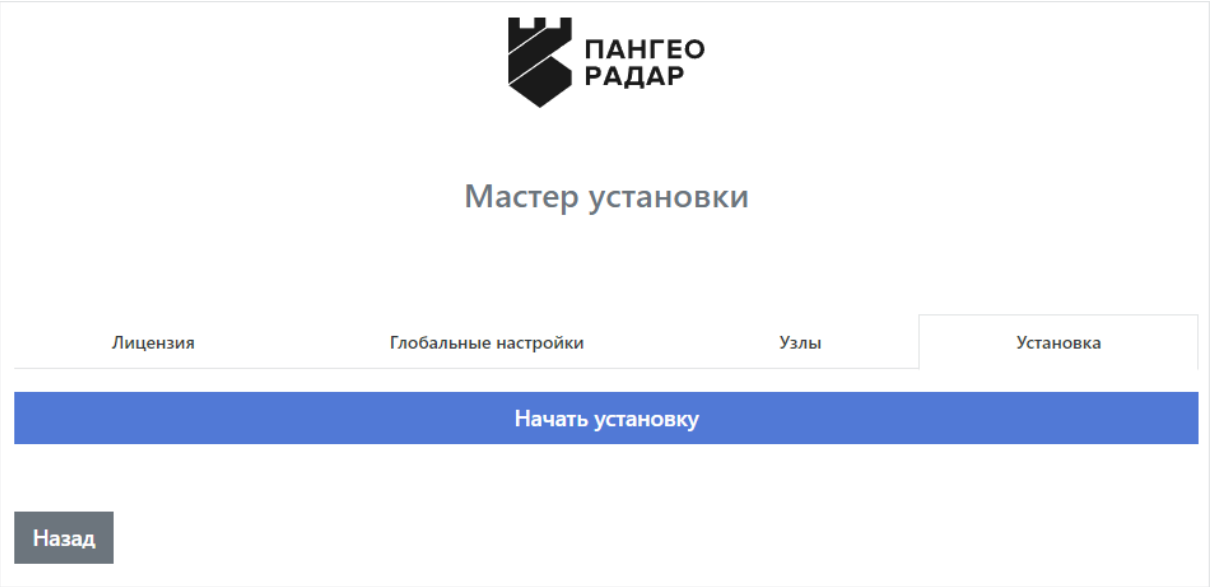

Рис. 10 – Мастер установки. Вкладка "Установка"

5. Нажмите кнопку **Начать установку**. Начнется процесс установки платформы (см. «Рис. 11»).

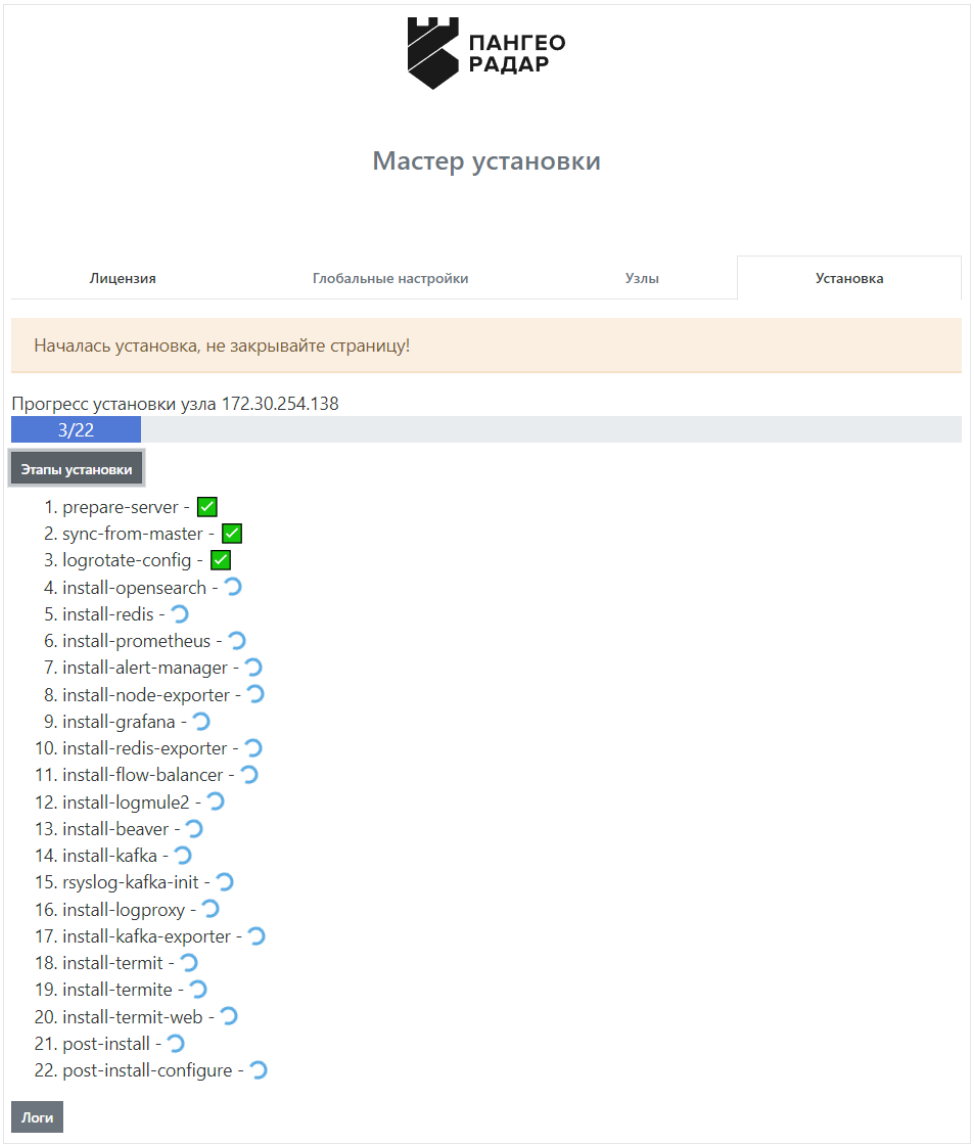

Рис. 11 – Процесс установки

6. При необходимости вы можете посмотреть журнал установки, нажав на кнопку **Логи** (см. «Рис. 12»).

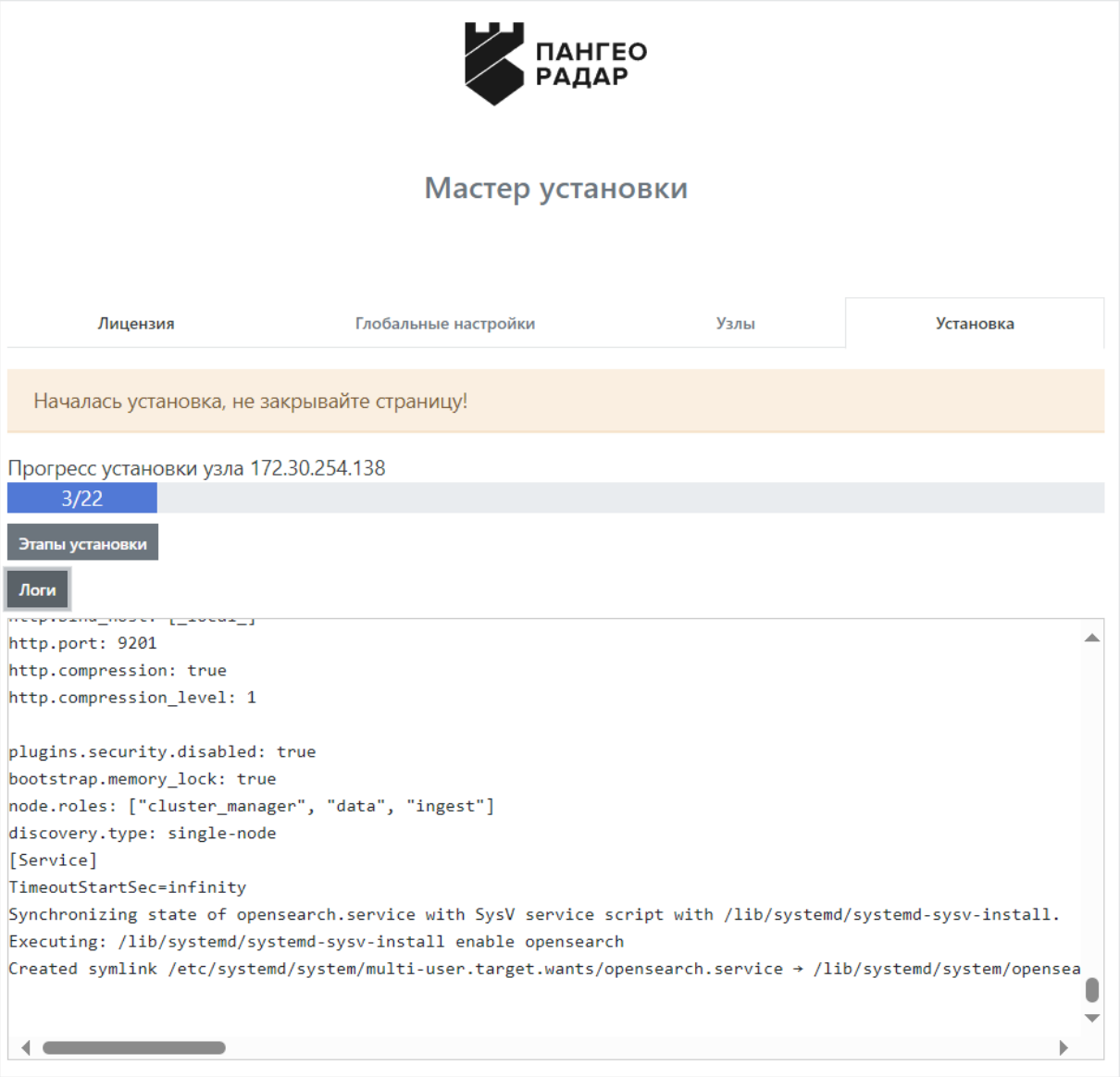

Рис. 12 – Журнал процесса установки

7. Установка займет некоторое время. После завершения установки отобразится окно "Обновление конфигурационных файлов" (см. «Рис. 13»).

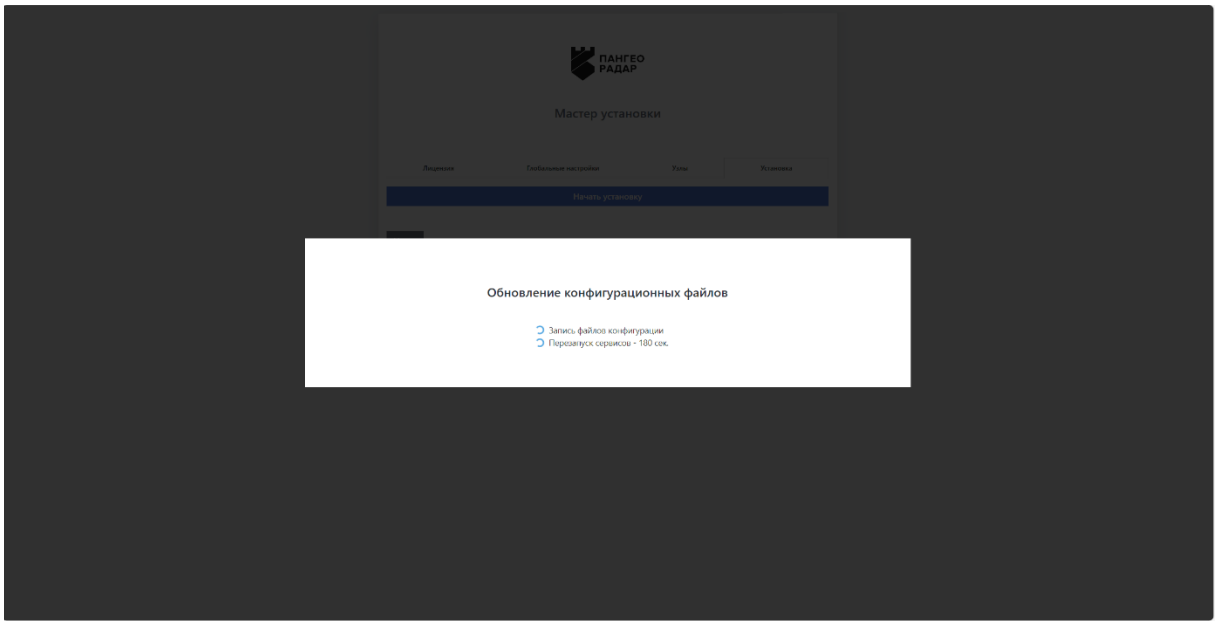

Рис. 13 – Окно "Обновление конфигурационных файлов"

8. По завершению перезапуска сервисов откроется **Платформа Радар** в разделе **Администрирование → Кластер → Узлы системы** (см. «Рис. 14»).

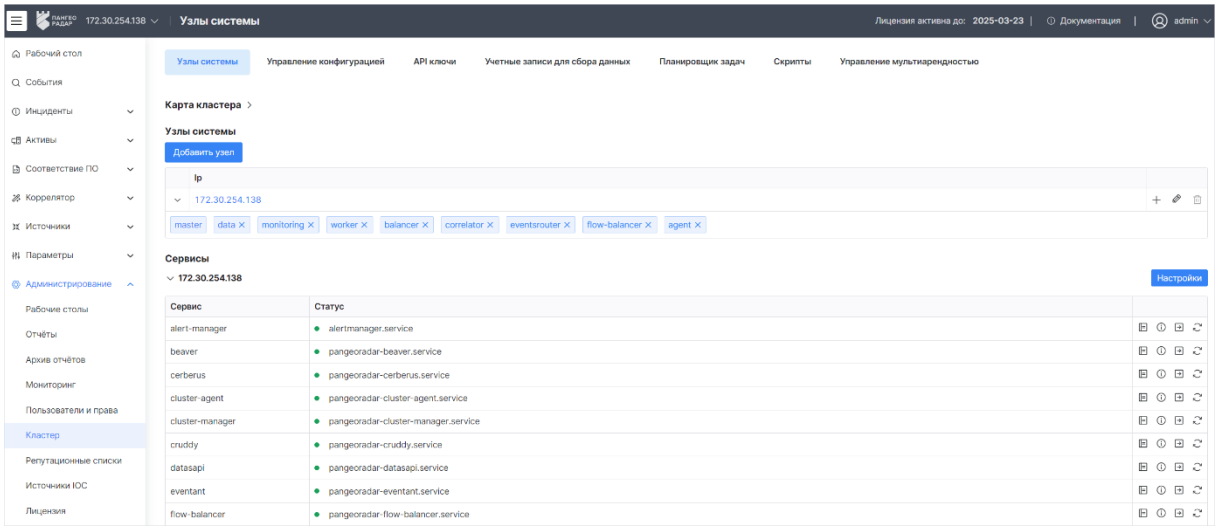

Рис. 14 – Проверка установки сервисов

7.1.4 Шаг 4. Завершение установки

Для полного завершения установки необходимо выполнить первичную настройку платформы. См. раздел «Шаг 4. Завершение установки

Для полного завершения установки необходимо выполнить первичную настройку платформы. См. раздел «**Ошибка! Неверная ссылка закладки.**».

Первичная настройка платформы».

7.2 Особенности распределенной установки

Внимание! *Установка должна выполняться с учетной записи с правами суперпользователя*.

Внимание! *Для корректной установки Платформы Радар в ОС Debian должна быть задана переменная PATH, содержащая полный список необходимых путей:*

`/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin`. В случае, если переменная PATH не содержит путей `/usr/sbin` и `/sbin`, их следует добавить вручную.

7.2.1 Шаг 1. Распаковка дистрибутива и запуск скрипта для установки

Дистрибутив системы представляет собой архив **pgr-x.x.x.tar.gz**, где **x.x.x** – номер версии платформы.

1. Создайте каталог для размещения файлов платформы. Например, `/var/tmp/pgr-x.x.x/`:

   ```
   # cd /var/tmp/
   # mkdir pgr-x.x.x
   ```

   Где `x.x.x` - номер версии платформы.

2. Перейдите в созданный каталог и извлеките содержимое архива **pgr-x.x.x.tar.gz**.

   ```
   # tar -xvf <наименование установочного архива>
   ```

3. Запустите файл `install.sh` с правами суперпользователя:

   ```
   # sudo ./install.sh
   ```

4. Начнется процесс установки платформы. Установка занимает некоторое время, в течение которого загружаются и устанавливаются модули **Платформы Радар**.

5. После загрузки основных модулей инсталлятор попросит указать IP-адрес и доменное имя сервера (необязательно), на котором будет установлена **Платформа Радар**.

   Внимание! *Если вы хотите работать в DNS инфраструктуре, то на данном этапе установки необходимо указать доменное имя сервера (FQDN) и по завершению установки переключить режим подключения к платформе с IP на FQDN. Подробнее см. «Руководство администратора» → раздел «Настройка платформы для работы в DNS инфраструктуре».*

6. Дождитесь окончания установки, после чего на экране появится сообщение об успешном завершении первого этапа:

   ```
   Продолжите установку по адресу: https://<IP-адрес платформы>/install
   Логин/Пароль по умолчанию - admin/admin
   ```

7.2.2 Шаг 2. Получение лицензии

Внимание! *В случае, если в инфраструктуре, куда устанавливается платформа, работает **Kaspersky Security Center (KSC)** и на машине, с которой будет проходить установка платформы через web-интерфейс, установлен **Kaspersky Endpoint Security (KES)**, то при установке, он подменит сертификаты на свои, что приведет к ошибкам. Необходимо отключить **KES** на соответствующей машине.*

1. Перейдите по адресу, указанному в конце работы инсталлятора: `http://<IP-адрес платформы>/install`.

2. Пройдите процедуру входа и смены пароля (по умолчанию: `admin/admin`). Откроется мастер установки на вкладке "Лицензия" (см. «Рис. 15»).

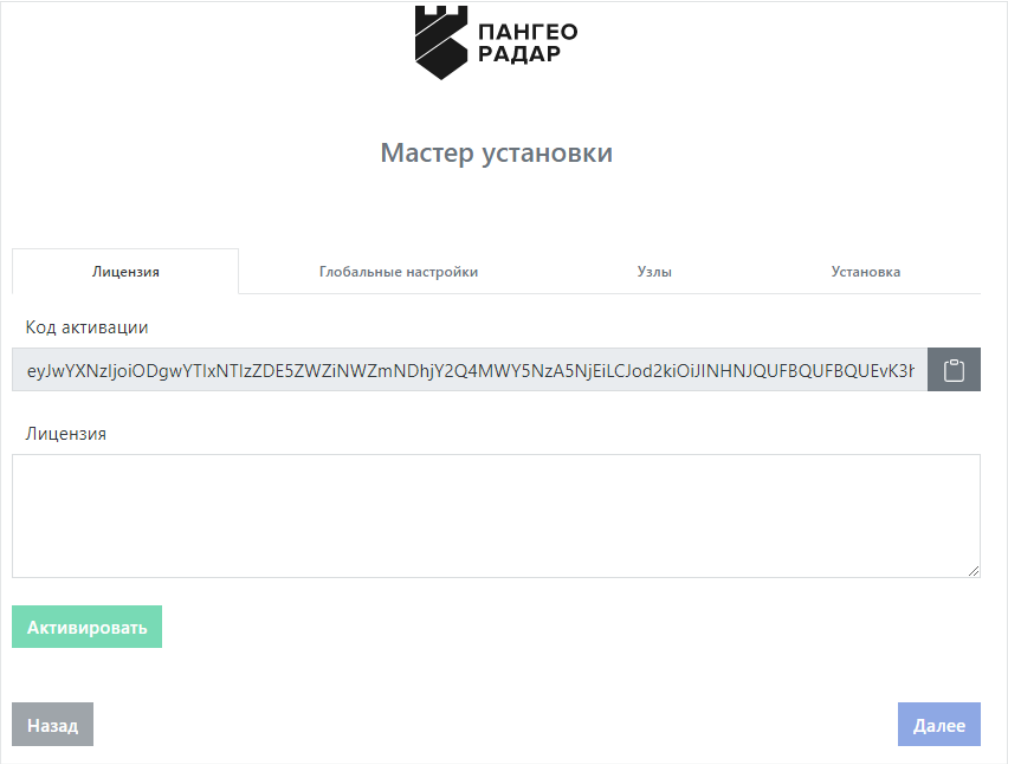

Рис. 15 – Мастер установки. Вкладка "Лицензия"

3. В поле **Код активации** отображается ваш код активации для получения. Скопируйте его с помощью кнопки  . Рекомендуется сохранить скопированный код в текстовый файл.
4. Перейдите в личный кабинет клиентского портала **Платформы Радар** (см. «Рис. 16»).

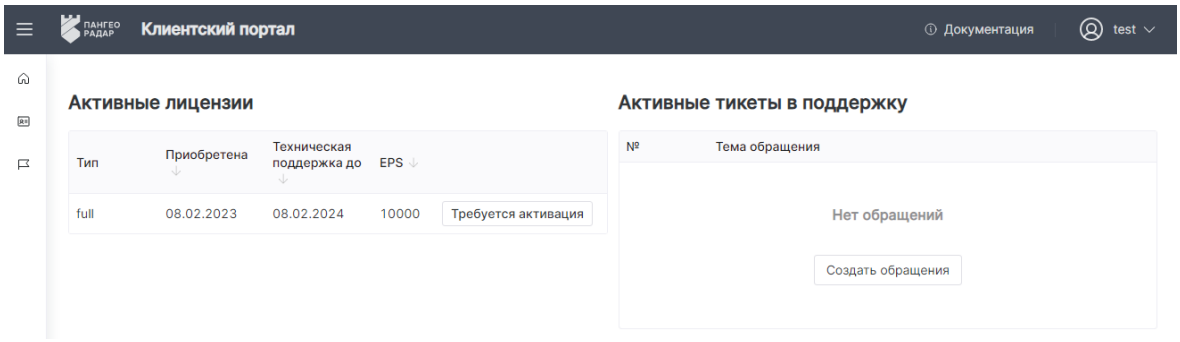

Рис. 16 – Клиентский портал Платформы Радар

5. Нажмите на кнопку **Требуется активация** и в открывшемся окне укажите, скопированный ранее, код активации. Будет выполнена активация лицензии, кнопка **Требуется активация** будет заменена на кнопку **Лицензия** (см. «Рис. 17»).

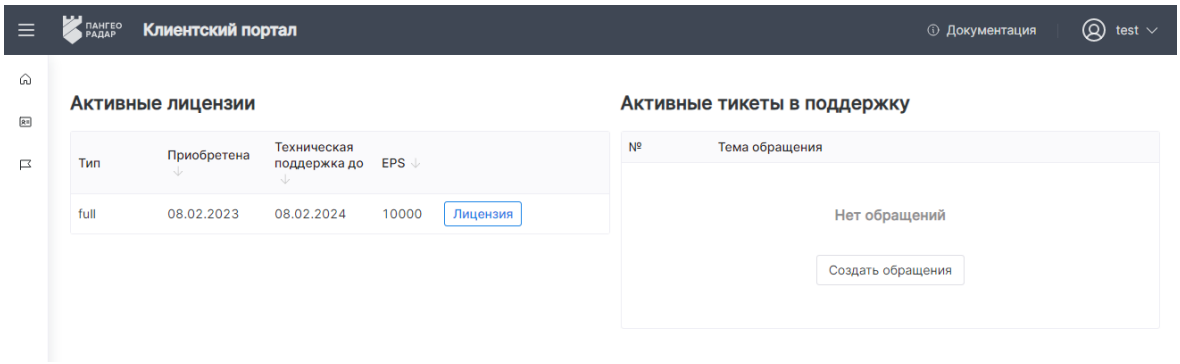

Рис. 17 – Клиентский портал. Кнопка получения лицензии

6. Нажмите на кнопку **Лицензия**. Откроется окно "Скачать лицензию" (см. «Рис. 18»).

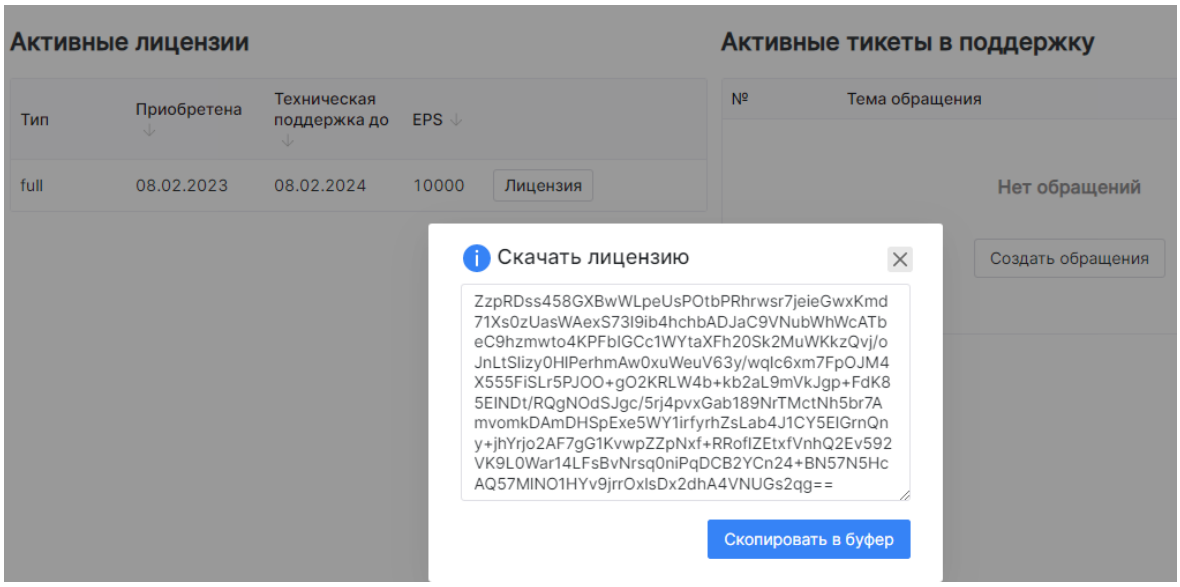

Рис. 18 – Окно "Скачать лицензию"

7. Скопируйте лицензию. Рекомендуется сохранить скопированное значение в текстовый файл.

8. Перейдите в мастер установки платформы на вкладку "Лицензия" (см. «Рис. 15»), в поле **Лицензия** укажите значение лицензии и нажмите кнопку **Активировать**. Лицензия будет активирована, а на экране будут отображены ее параметры (см. «Рис. 19»).

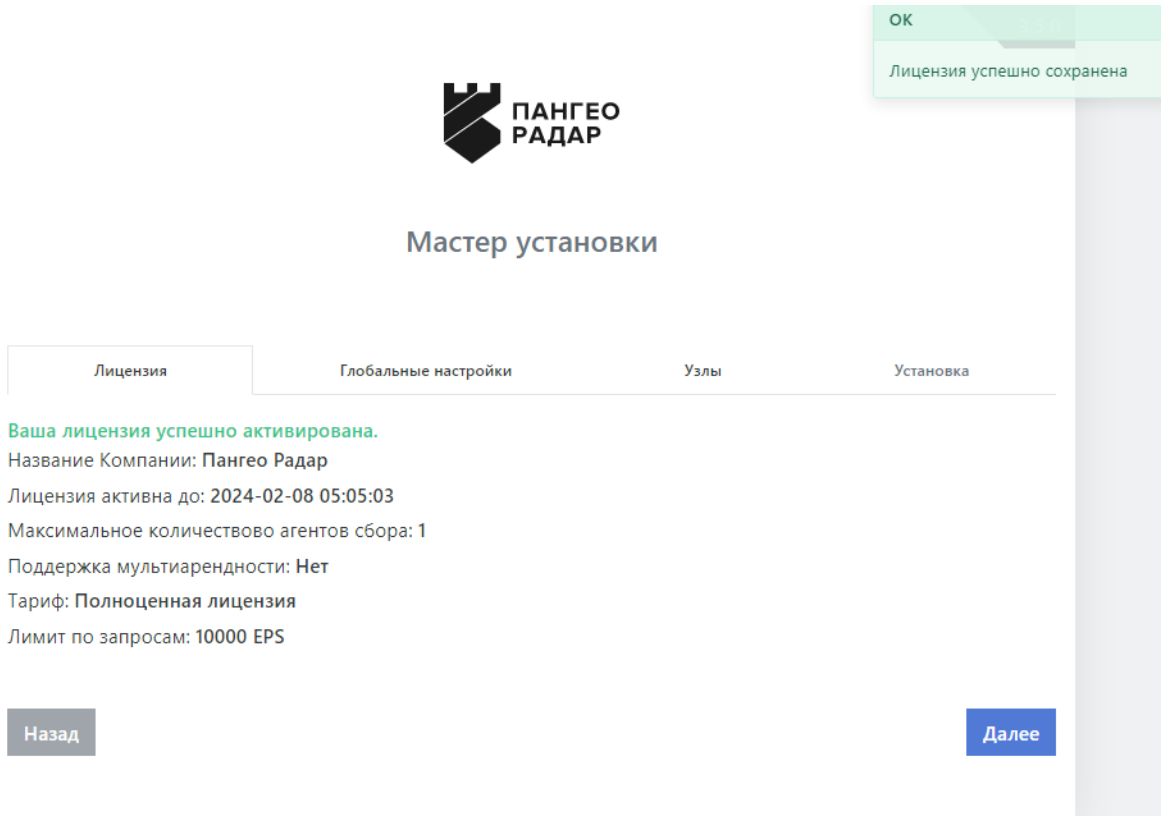

Рис. 19 – Параметры лицензии

7.2.3 Шаг 3. Установка в веб-интерфейсе платформы

1. После активации лицензии нажмите кнопку **Далее**. Откроется вкладка "Глобальные настройки" (см. «Рис. 20»).

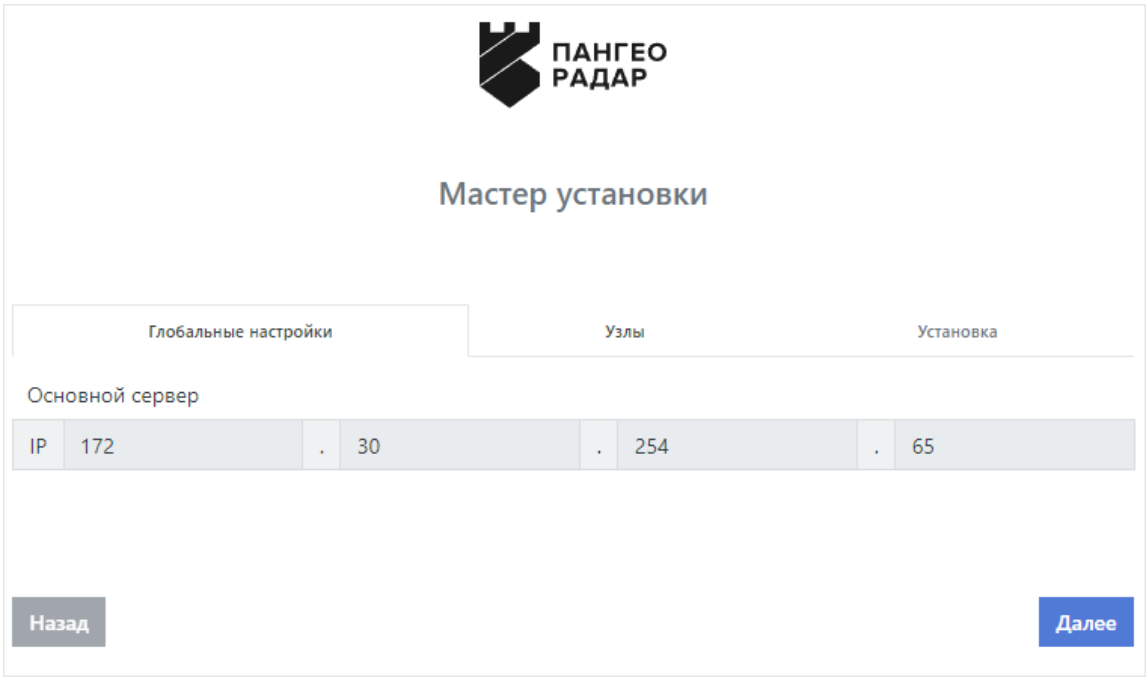

Рис. 20 – Экран продолжения установки Платформы Радар

2. На вкладке "Глобальные настройки" проверьте параметры основного сервера, указанные на первом шаге, и нажмите кнопку **Далее**. Откроется вкладка "Узлы" (см. «Рис. 21»).

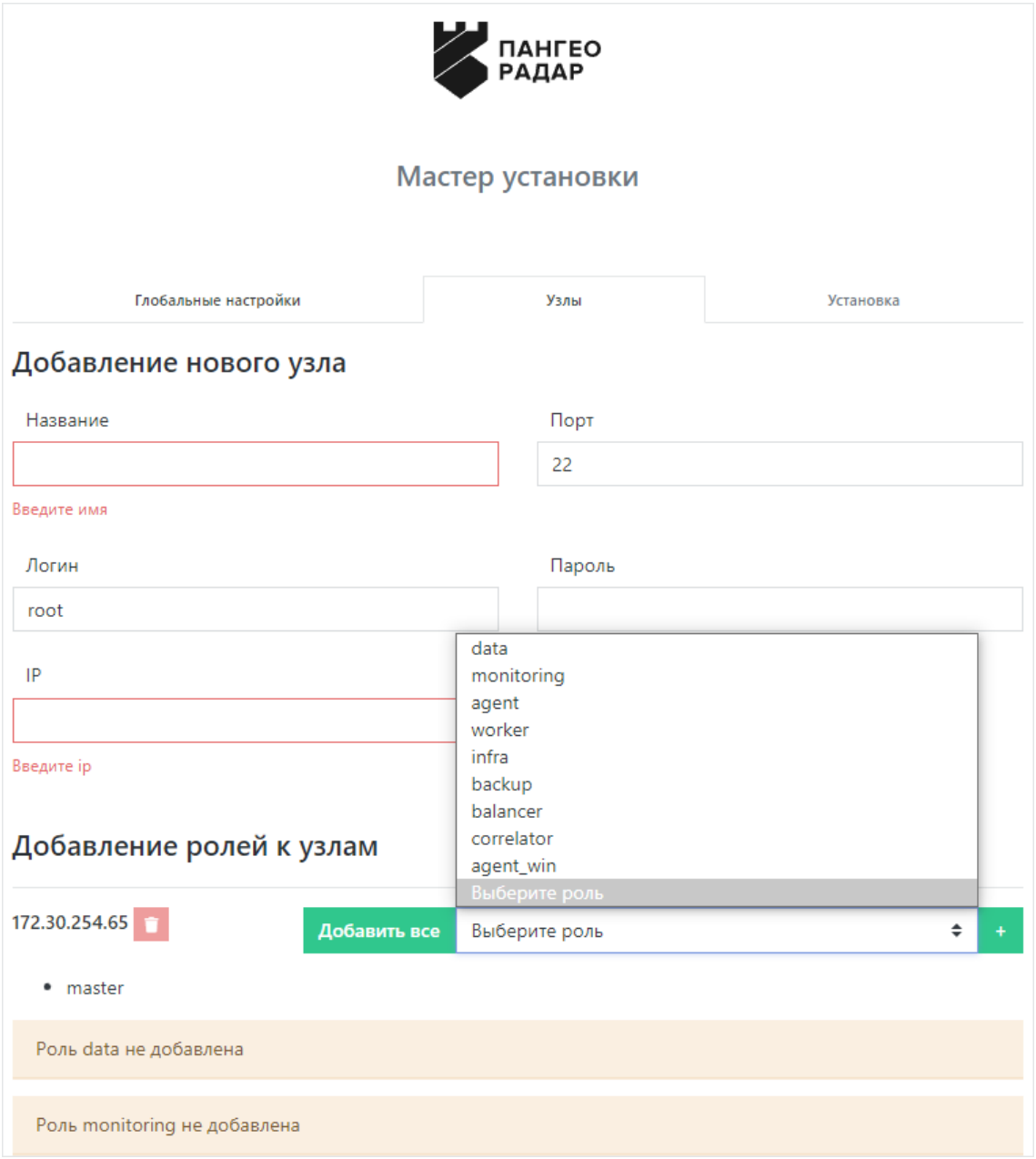

Рис. 21 – Экран настройки узлов Платформы Радар

3. Добавьте необходимые узлы кластера, указав в форме "Добавление нового узла" (см. «Рис. 22») следующие данные:
   - в поле **Название** укажите название узла;
   - в полях **Логин** и **Пароль** укажите аутентификационные данные, по которым будет происходить подключение к узлу;
   - в поле **IP** укажите IP-адрес узла;
   - в поле **Порт** укажите значение "*22*";
   - нажмите кнопку **Добавить**.

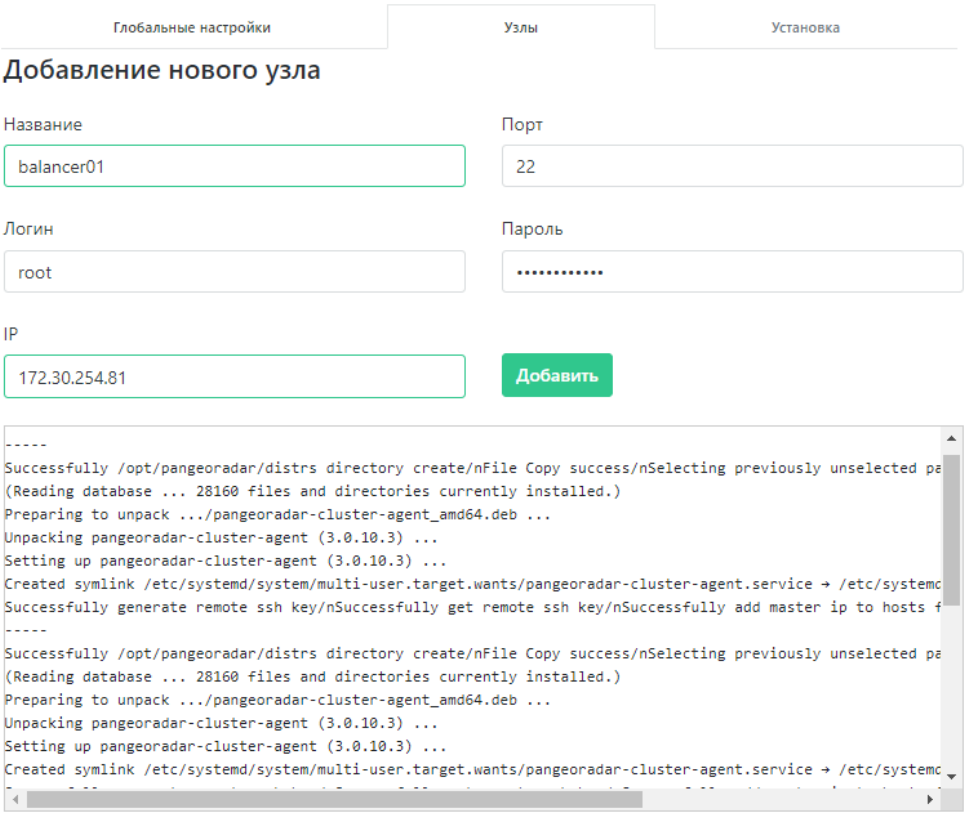

Рис. 22 – Добавление нового узла

4. Назначьте добавленным узлам необходимые серверные роли. Для этого выберите узел и из выпадающего списка **Выберите роль** назначьте узлу нужную роль (см. «Рис. 23»).

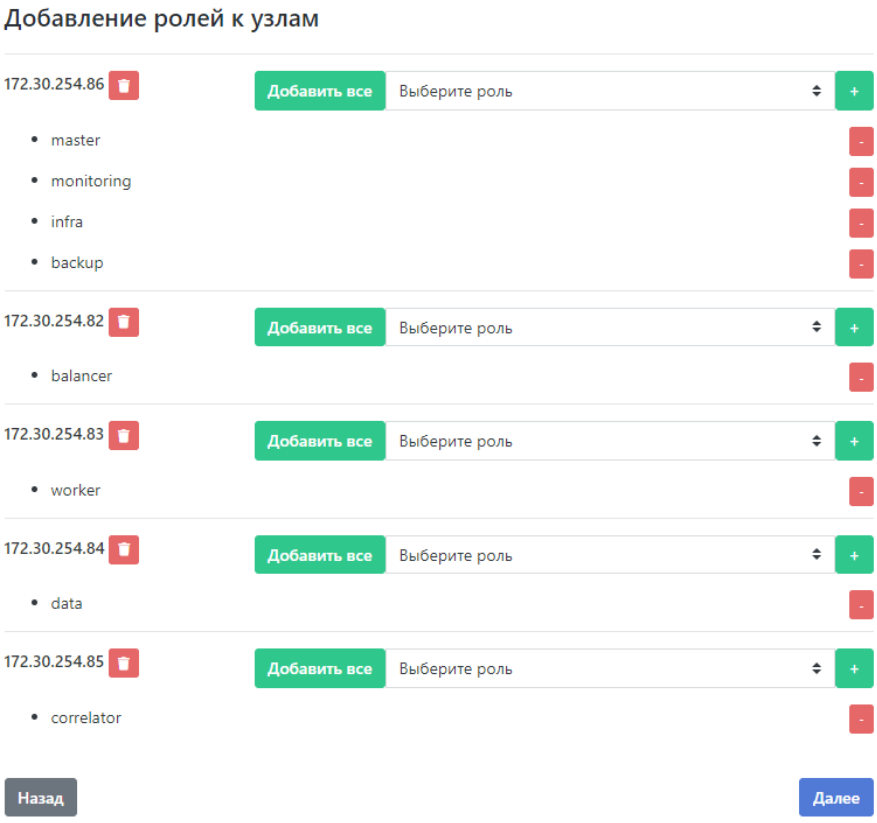

Рис. 23 – Добавление ролей к узлам

5. Нажмите кнопку **Далее**. Откроется вкладка "Установка" (см. «Рис. 24»).

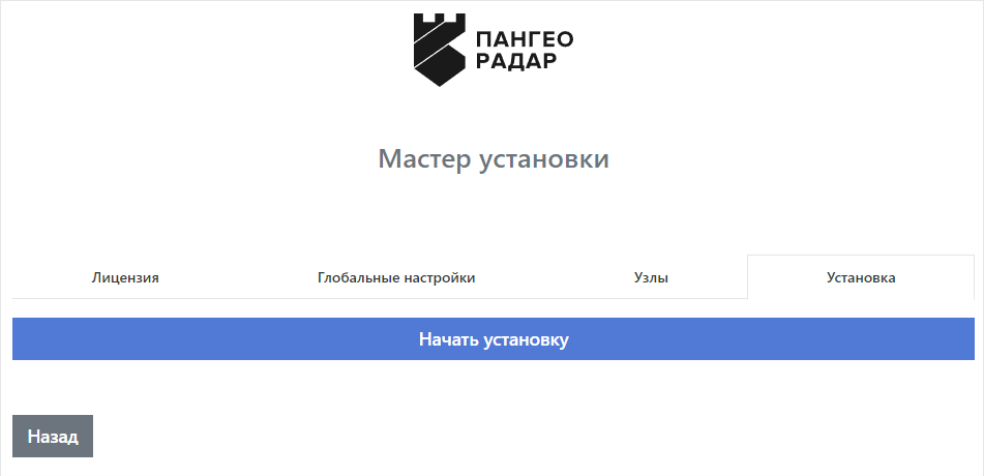

Рис. 24 – Мастер установки. Вкладка "Установка"

6. Нажмите кнопку **Начать установку**. Начнется процесс установки платформы (см. «Рис. 25»).

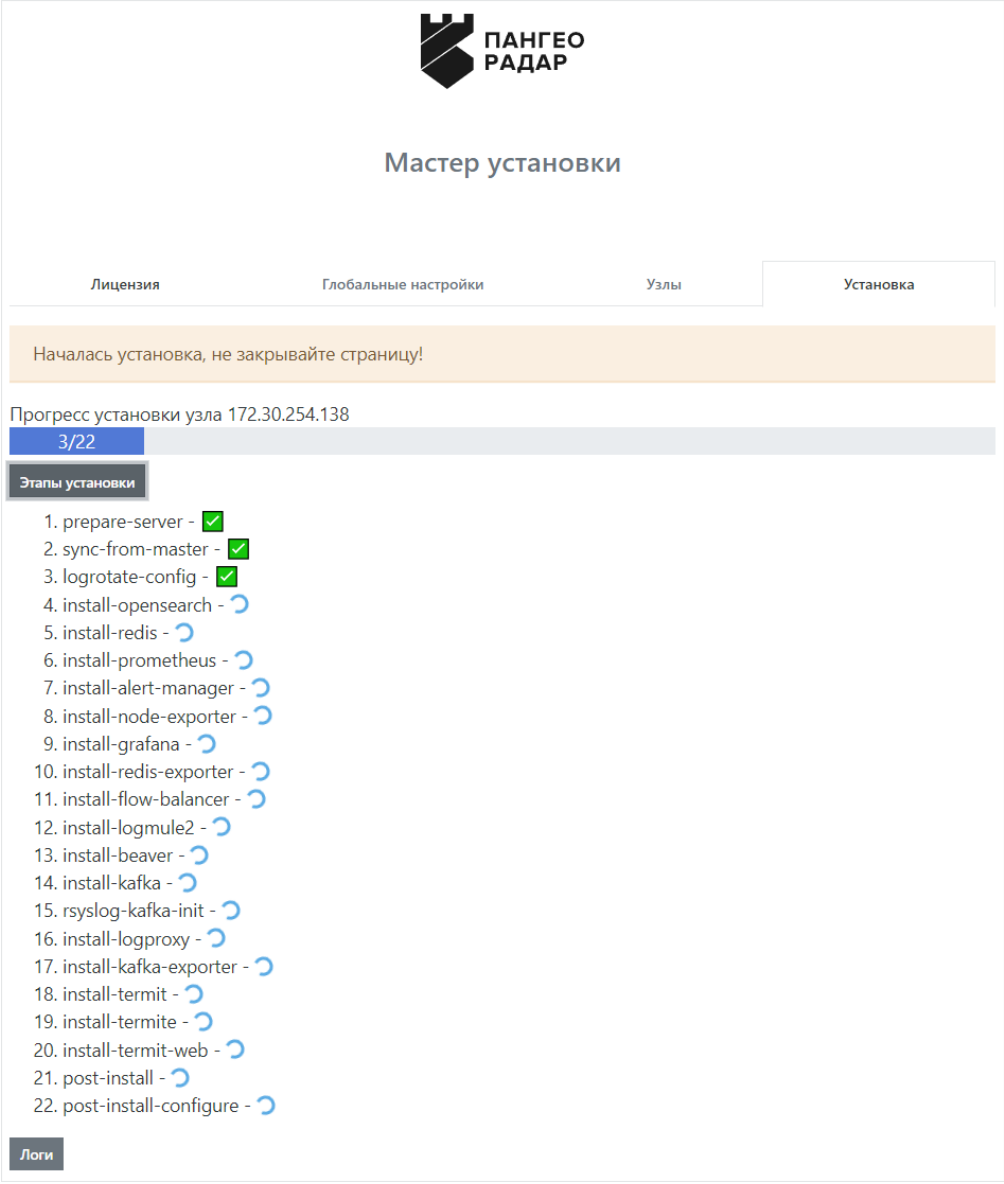

Рис. 25 – Процесс установки

7. При необходимости вы можете посмотреть журнал установки, нажав на кнопку **Логи** (см. «Рис. 26»).

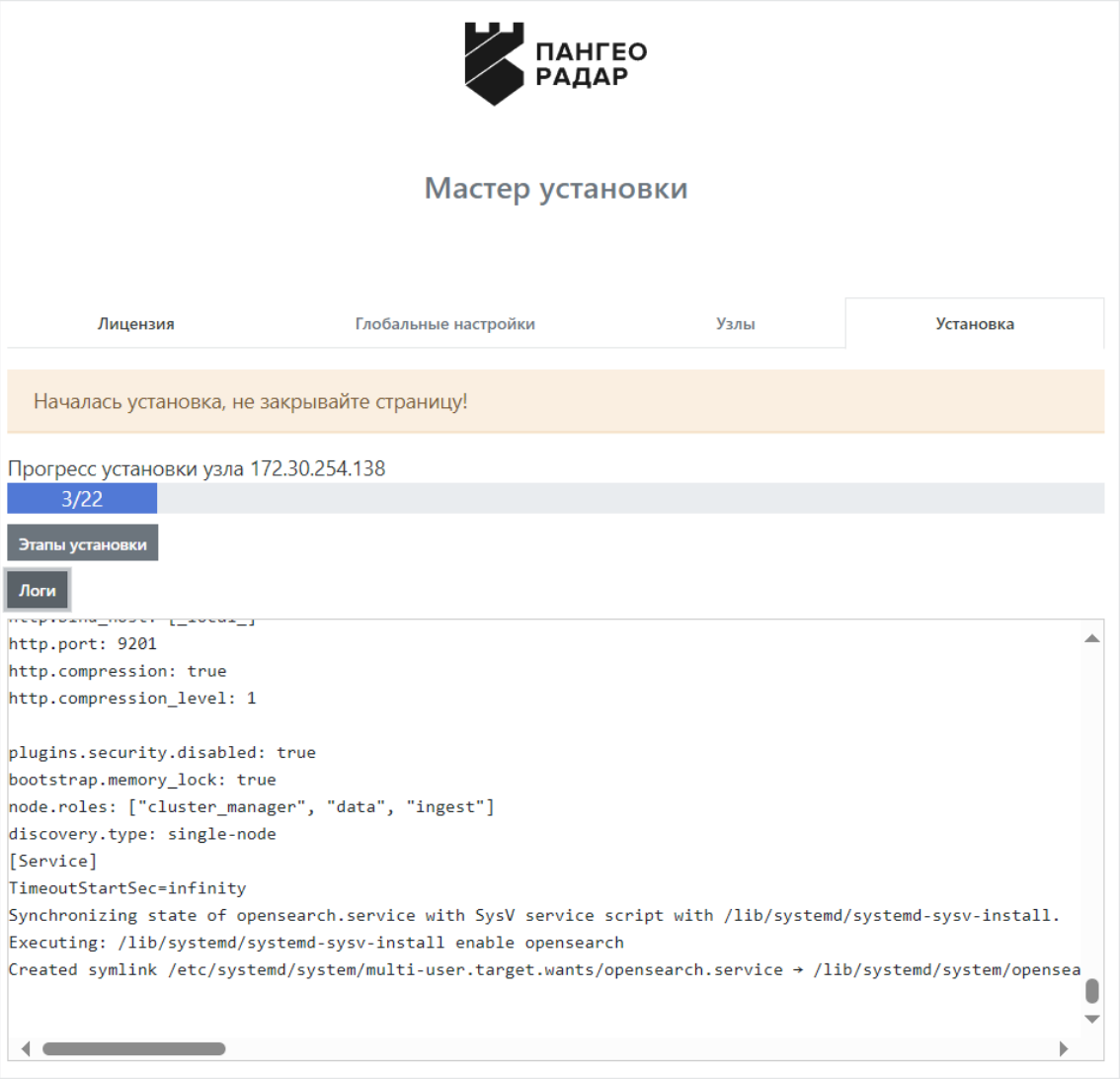

Рис. 26 – Журнал процесса установки

8. Установка займет некоторое время. После завершения установки отобразится окно "Обновление конфигурационных файлов" (см. «Рис. 27»).

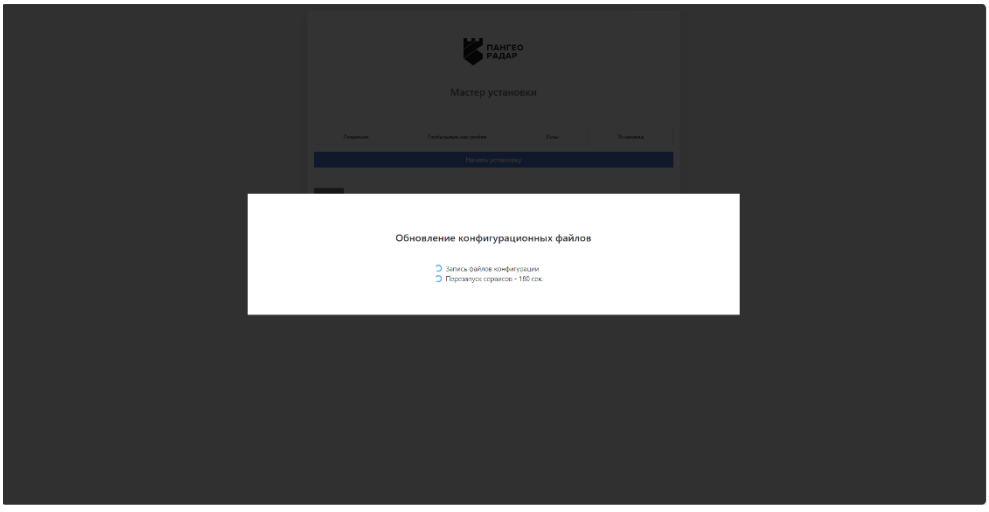

Рис. 27 – Окно "Обновление конфигурационных файлов"

9. По завершению перезапуска сервисов откроется раздел **Администрирование → Кластер →** вкладка **Узлы системы** (см. «Рис. 28»).

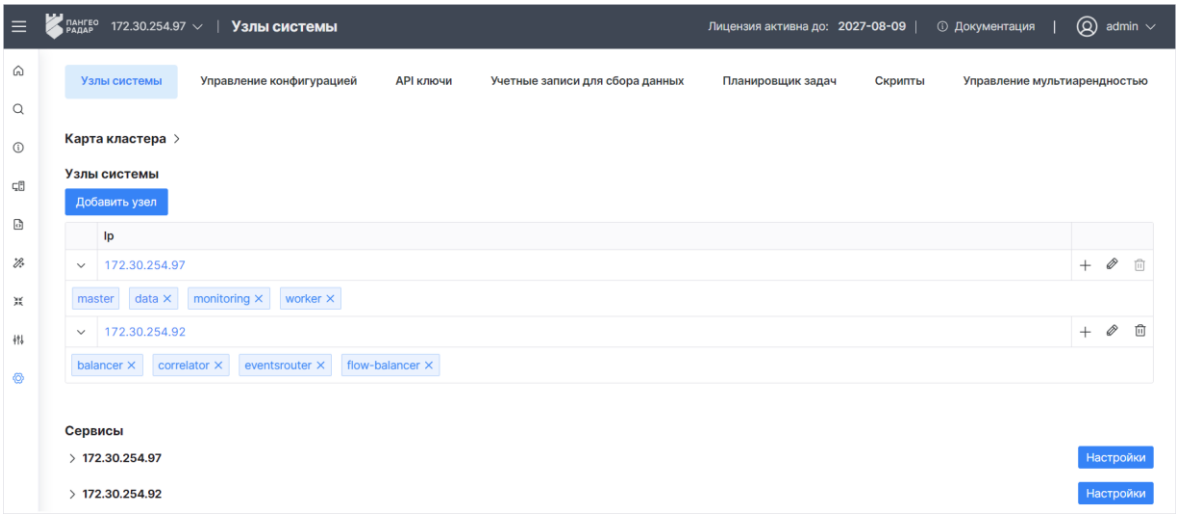

Рис. 28 – Раздел "Кластер". Список узлов платформы

7.2.4 Шаг 4. Завершение установки

Для полного завершения установки необходимо выполнить первичную настройку платформы. См. раздел «**Ошибка! Неверная ссылка закладки.**».

8. Первичная настройка платформы

Перечень действий, которые необходимо выполнить главному администратору после установки платформы, приведен в «Табл. 4».

Табл. 4 – Действия после установки платформы

№	Действие	Ожидаемый результат
1	Проверить работу сервисов платформы.	- все сервисы платформы работают в штатном режиме (индикатор ●); - журналы служб не имеют ошибок после установки.
2	Настроить конфигурацию кластера в соответствии с инфраструктурой.	- настроен глобальный ключ авторизации; - выполнена настройка сервисов платформы; - переопределены параметры узлов (при необходимости).
3	Установить контент, предоставляемый вендором.	Контент успешно установлен. В платформу добавились следующие данные: - правила корреляции; - фильтры потока событий; - макросы; - табличные списки; - источники; - правила разбора и обогащения; - типы инцидентов.
4	Настроить локальные сети.	- необходимое кол-во локальных сетей добавлено в платформу; - изменения опубликованы; - информация о локальных сетях автоматически передается сервисам при изменении конфигурации платформы.
5	Установить и настроить лог-коллектор.	- установлено необходимое количество агентов сбора на соответствующие ОС; - созданы учетные записи для подключения к лог-коллектору; - настроены необходимые компоненты сбора и отправки событий; - запущены сборщики и отправители агентов сбора.
6	Настроить источники для подключения к платформе.	На стороне источника выполнены необходимые настройки для подключения к платформе.
7	Включить источники в платформе.	- источник добавлен в платформу (вручную или из эксперт пака); - для источника настроены безусловные и условные правила разбора; - для источника настроены правила обогащения; - опубликованы все изменения, внесенные в источники; - проверено наличие потока событий, поступающего от источника (разделы **Мониторинг** и **События**);
8	Проверка работы правил корреляции.	- для соответствующих правил есть результаты "сработок"; - в логах правила отсутствуют ошибки.
9	Подключить подчиненные инстансы.	Действие выполняется в случае, если планируется использовать платформу в инфраструктуре мультитенант. Результат действия: - подключены необходимые инстансы; - возможно переключение между инстансами; - возможно конфигурировать подчиненные инстансы.
10	Настроить доступ пользователей к платформе: - Пользователи; - Группы пользователей; - Роли; - Доступ к данным.	- добавлены пользователи; - добавлены группы пользователей; - пользователям и группам пользователей выданы необходимые роли; - пользователям и группам пользователей выданы права на доступ к соответствующим данным.
11	Настроить рабочие столы.	- настроены рабочие столы и соответствующие виджеты; - пользователям и группам пользователей выданы доступы к рабочим столам.
12	Настроить отчеты.	- настроен внешний вид отчетов; - настроена периодичность формирования отчетов.

№	Действие	Ожидаемый результат
13	Выполнить поиск и первоначальную настройку активов: - Настроить политики идентификации активов; - Обнаружить хосты; - Обнаружить сервисы; - Выполнить сбор данных с активов.	- настроены политики идентификации активов; - выполнено сканирование подсетей; - информация об обнаруженных активах добавлена в платформу; - собраны данные о сервисах на выбранных активах; - созданы учетные записи для сбора данных с активов; - собраны данные об аппаратном и программном обеспечении активов.
14	Настроить группы активов.	- настроены группы активов; - пользователям и группам пользователей выданы права на работу с группами активов.
15	Настроить оповещения.	- настроены оповещения о внештатном и штатном изменении конфигурации платформы; - настроены оповещения для пользователей.

Внимание! *Для выполнения настройки **Платформы Радар** воспользуйтесь инструкциями, которые приведены в следующих документах:*

- *Руководство Администратора;*
- *Руководство Оператора;*
- *Руководство по работе с источниками событий информационной безопасности.*

Для обеспечения бесперебойной и безотказной работы платформы, рекомендуется ознакомиться с Руководством Администратора. Раздел 16.5 Возможные проблемы при эксплуатации платформы.

9. Обновление Платформы Радар

В данном разделе приняты следующие обозначения:

- `UPDATE_HOME` – временный каталог, который используется для выполнения обновления. Название и расположение каталога могут быть произвольными.

9.1 Подготовка к обновлению

Для выполнения обновления необходим дистрибутив новой версии **Платформы Радар**, который представляет собой архив **pgr-x.x.x.tar.gz**, где **x.x.x** – номер версии платформы.

1. Удостоверьтесь, что аппаратное и программное обеспечение удовлетворяет требованиям новой версии платформы. Актуальные требования указаны в следующих разделах:
   - «Требования к ПО»;
   - «Требования к ТО».
2. Если для работы платформы применены средства виртуализации, то сделайте снимок (snapshot) всех машин, используемых платформой.
3. Сделайте резервную копию пользовательского контента (см. «Руководство Администратора. Раздел 16.7 Резервное копирование пользовательского контента»).
4. Создайте временный каталог UPDATE_HOME.
5. Извлеките содержимое архива **pgr-x.x.x.tar.gz** в каталог `UPDATE_HOME`:

   ```
   # tar -xvf <наименование установочного архива>
   ```

6. Проверьте корректность работы репозитория:

   ```
   # apt update
   ```

7. Проверьте сетевую доступность всех узлов платформы.

Особенности обновления платформы с различных версий:

- при обновлении платформы с версии 3.4.0 лицензия будет сброшена;
- при обновлении платформы с версии 3.5.0 выдача лицензии производится через клиентский портал;
- начиная с версии 3.6.0 на платформе обновляется сервис `logmule` и добавляется новый сервис `flow-balancer`;
- начиная с версии 3.7.0 поисковая система `ElasticSearch` заменяется на `OpenSearch`;
- начиная с версии 3.7.0 и выше скрипт обновления запускается файлом `install.sh`.

9.2 Выполнение обновления

1. Запустите скрипт обновления в зависимости от версии платформы:
   - если версия ниже 3.7.0, то запустите следующий файл:

     ```
     # sudo bash update_<версия релиза>.sh
     ```

- если версия 3.7.0 и выше, то запустите следующий файл:

  ```
  # sudo ./install.sh
  ```

2. Дождитесь окончания процесса обновления, отслеживая все возникающие ошибки.
3. Обновите контент (эксперт пак) на версию из дистрибутива.

   Примечание: *если при выполнении обновления возникли ошибки, то обратитесь в службу технического сопровождения по электронному адресу support@pangeoradar.ru*.

10. Межсетевое взаимодействие

10.1 Централизованная установка Платформы Радар

Ниже приведен перечень используемых портов при централизованной установке **Платформы Радар**:

Исходящий	Входящий	Порты	Описание
Log-Collector	Master	9009	Взаимодействие с Мастером
Master	Log-Collector	8085/tcp, 22/tcp (Linux-версия), 6677/tcp (Linux-версия), 9100/tcp (Linux-версия)	Управление коллектором с мастера и сбор статистики
Источники событий	Log-Collector	1500-5000/tcp, 500-5000/udp	Пассивный сбор событий
Log-Collector	Источники событий	22/tcp 135/tcp, 135/udp, 445/tcp 1433/tcp, Динамический диапазон портов Microsoft RPC (49152-65535/tcp)	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками
АРМ администратора	IP-адрес лог-коллектора	22/tcp (Linux-версия), 3389/tcp (Windows-версия), 3389/udp (Windows-версия)	Администрирование
Log-Collector	Log-proxy	1100/tcp 1100/udp	Отправка событий в сервис **Kafka**
Пользователи **Платформы Радар**	Master	443 8080 9000 6676 6677	Доступ к интерфейсу **Платформы Радар**, проверка API ключей

10.2 Распределенная установка Платформы Радар

Ниже приведён перечень используемых портов при распределенной установке **Платформы Радар** (независимо от вариантов распределенной установки):

Исходящий	Входящий	Порты	Описание
Correlator	Master	5672	Чтение нормализованных событий из очереди для корреляции
Correlator	Master	8086	Передача результатов корреляции
Log-Collector	Balancer	1500-5000, 9997-9999, 15403, 15404TCP/UDP	Передача данных от сборщика в балансировщик и менеджер очередей

Исходящий	Входящий	Порты	Описание
Log-Collector	Источники событий	21, 22, 135, 445, 1443, 3306, 5432, 5601	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками
Log-Collector	Master	9000	Запрос конфигурационных данных
Master	Data	9200	Работа с сырыми событиями
Master	Correlator	2092	Управление правилами корреляции
Master	Log-Collector	4805 4806	Мониторинг и сбор статистики. Управление сборщиком событий API
Master	Balancer Correlator Data Worker	6676	Управление агентами кластера
Master	Balancer Correlator Data Worker	9100	Мониторинг и сбор статистики
Master	Balancer	9292, 9308	Мониторинг и сбор статистики
Master	Data	9114	Мониторинг и сбор статистики
Worker	Balancer	9092	Чтения событий из менеджера очередей для их обработки
Worker	Master	5672	Передача нормализованных событий в очередь на корреляцию
Worker	Data	9200	Передача событий на хранение
Источники событий	Log-Collector	162 SNMP trap; 4807 UDP receiver; 4808 TCP receiver; 4809 TCP receiver SSL/TLS; 4810 HTTP receiver; 4811 HTTPS receiver; 4812 NetFlow reciever	Пассивный сбор событий
Пользователи **Платформы Радар**	Master	8080 9000 6676 6677	Доступ к интерфейсу **Платформы Радар**, проверка API ключей
Data (с ролью Master)	Data (с ролью Data)	9300	Взаимодействие между нодами в кластере хранилища данных

10.3 Порты сервисов Платформы Радар

Ниже приведен перечень портов сервисов **Платформы Радар** по умолчанию. При необходимости их можно изменить в управлении конфигурацией кластера.

№	Сервис	Описание	Порт	Внешний порт на сервере nginx
1	Beaver	Балансировщик обработчика событий	9201	9200

№	Сервис	Описание	Порт	Внешний порт на сервере nginx
2	Cerberus	Межсервисный шлюз	9900	9000
3	ClusterAgent	Агент управления узлом кластера.	6678	6677
4	Cm	Менеджер кластера	6676	
5	Cruddy	Центр управления API	8089	
6	DatasApi	Отчетность	8083	
7	Enrich	Обогащение событий		
8	ESExporter	Экспорт метрик с сервиса, отвечающего за хранение событий	9115	9114
9	EventAnt	Менеджер обмена информацией	8780	
10	FlowBalancer	Балансировщик коррелятора		
11	Grafana	Визуализация метрик	6631	6630
12	KafkaExporter	Экспорт метрик с сервиса Kafka	9309	9308
13	Kafka	Передача данных и событий между модулями		
14	Karaken	Провайдер мультиарендности	8000	9009
15	KeyCloak	Аутентификация	8181	8180
16	Logmule2	Коррелятор событий	18567	
17	Logproxy	Пересылка событий от лог-коллектора в сервис Kafka	1100	
18	Nginx	Веб-сервер		
19	NodeExporter	Сбор метрик с узлов кластера	9101	9100
20	Opensearch	Хранение и поиск обработанных событий	9201	9200
21	Pg	База данных	5432	
22	Prometheus	Сбор и хранение метрик работы **Платформы Радар**	9090	
23	Sonar	Сканирование активов	9666	
24	Termit	Разбор, нормализация событий		

№	Сервис	Описание	Порт	Внешний порт на сервере nginx
25	Ti	Обновление информации об угрозах	8082	
26	Toller	Оповещения	6699	
27	Ui	Отладка интерфейса пользователя	8081	

10.4 Список портов для доступа к веб-интерфейсу Платформы Радар

- 8180/tcp (аутентификация/вход);
- 6630/tcp (API);
- 443/tcp (веб-интерфейс);
- 9009/tcp (взаимодействие с мастером);
- 1234/tcp (межсервисный шлюз);
- 8097/tcp (документация);
- 9000/tcp (мультитенанс/мультиарендность).