

Программный комплекс
«Система мониторинга и управления
событиями безопасности
Ankey SIEM Next Generation» v 4.1.2

Руководство по инсталляции

© ООО «Газинформсервис» с 2004 года

При инсталляции ПК Ankey SIEM NG необходимо ознакомиться с условиями лицензионного соглашения на использование конечным пользователем программы*, согласно которому весь функционал программного комплекса, в том числе отдельные его модули (составляющие)**, носители и документация, предоставляются на условиях «как есть»***.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ООО «Газинформсервис».

Ankey SIEM NG® является зарегистрированным товарным знаком ООО «Газинформсервис».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, ООО «Газинформсервис» ответственности не несет.

Дата редакции документа: 3 квартал 2023 года.

* Использование ПК Ankey SIEM NG означает согласие со всеми пунктами лицензионного соглашения.

** ПК Ankey SIEM NG включает в свой состав компоненты платформы, коннекторы (модули сбора и обработки данных) и контент (модули выявления нарушений ИБ (корреляционной обработки данных)).

*** Выполнение основных функций программы (функциональные возможности), предусмотренных (-е) действующей релизной версией. Комплектность, предусмотренная действующей релизной версией изделия. Документация, предусмотренная действующей релизной версией изделия.

Содержание

1 Об этом документе	7
2 О ПК Ankey SIEM NG	10
2.1 Архитектура ПК Ankey SIEM NG	10
2.1.1 Компонент Ankey SIEM Next Generation Core	11
2.1.2 Компонент Ankey SIEM Next Generation Server.....	11
2.1.3 Компонент Ankey SIEM Next Generation Events Storage.....	11
2.1.4 Компонент Ankey SIEM Next Generation Agent.....	11
2.1.5 Компонент Ankey SIEM Next Generation Management and Configuration	12
2.1.6 Компонент Ankey SIEM Next Generation Knowledge Base	12
2.1.7 Компонент Ankey SIEM Next Generation Retro Correlator.....	12
2.2 Схема взаимодействия компонентов	12
3 Развертывание ПК Ankey SIEM NG.....	16
3.1 Типовые схемы развертывания Ankey SIEM NG	16
3.1.1 Рекомендации по выбору конфигурации Ankey SIEM NG.....	16
3.1.2 Схема развертывания конфигурации для низконагруженных систем .	17
3.1.3 Схема развертывания конфигурации для средненагруженных систем	19
3.1.4 Схема развертывания конфигураций для высоконагруженных и	21
3.1.5 Об установке конвейеров обработки событий	23
3.2 Аппаратные и программные требования	25
3.2.1 Требования к аппаратному обеспечению конфигурации для	25
3.2.2 Требования к аппаратному обеспечению конфигурации для	27
3.2.3 Требования к аппаратному обеспечению конфигурации для	29
3.2.4 Требования к аппаратному обеспечению конфигурации для	32
3.2.5 Аппаратные требования к серверу облегченной версия Ankey SIEM NG	35
3.2.6 Аппаратные требования к серверу сбора событий с компонентом	36
3.2.7 Рекомендации по расчету объема и выбору накопителей для хранения	38
3.2.8 Требования к программному обеспечению	39
3.2.9 Рекомендации по развертыванию Ankey SIEM NG в виртуальной среде	39
3.2.10 Взаимодействие с внешними системами	40
3.3 Подготовка к установке Ankey SIEM NG	41
3.3.1 Подготовка к установке Ankey SIEM NG на ОС Astra Linux SE	41
3.4 Об установке компонентов на Linux-like с помощью ролей	42

3.5	Сценарий развертывания Ankey SIEM NG	45
3.6	Установка роли Deployer	47
3.7	Установка компонента Ankey SIEM NG MC на Linux-like	48
3.7.1	Установка роли SqlStorage	48
3.7.2	Установка роли JatobaStorage и онлайн активация лицензии.....	49
3.7.3	Установка роли JatobaStorage и офлайн активация лицензии.....	51
3.7.4	Установка роли Management and Configuration.....	52
3.8	Установка компонента Knowledge Base на Linux-like	53
3.9	Установка компонента Ankey SIEM NG Core на Linux-like	55
3.9.1	Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core ...	55
3.9.2	Установка роли Core	56
3.10	Установка компонента Ankey SIEM NG Events Storage на Linux-like	58
3.10.1	Установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage	58
3.10.2	Установка роли SIEM Storage с хранилищем событий Elasticsearch .	59
3.10.3	Установка роли SIEM Storage с хранилищем событий LogSpace	61
3.11	Установка компонента Ankey SIEM NG Server на Linux-like	62
3.11.1	Установка модуля Salt Minion на сервер Ankey SIEM NG Server.....	63
3.11.2	Установка роли RMQ Message Bus на сервер Ankey SIEM NG Server	64
3.11.3	Установка роли SIEM Server	65
3.12	Установка компонента Ankey SIEM NG Agent	66
3.12.1	Установка модуля Salt Minion на сервер Ankey SIEM NG Agent.....	67
3.12.2	Установка роли Agent	67
3.12.3	Установка компонента Ankey SIEM NG Agent на Windows Server	69
3.13	Установка облегченной версии компонента Ankey SIEM NG Server на Linux-like	70
3.13.1	Установка модуля Salt Minion на сервер облегченной версии Ankey SIEM NG Server	70
3.13.2	Установка роли RMQ Message Bus на сервер облегченной версии Ankey SIEM NG Server	71
3.13.3	Установка роли SIEM Server для облегченной версии компонента ...	72
3.14	Установка облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows	73
3.15	Установка правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server	75
3.16	Активация лицензии Ankey SIEM NG	76
3.16.1	Активация лицензии на Linux-like при наличии доступа к интернету .	76
3.16.2	Активация лицензии на Linux-like при отсутствии доступа к интернету	77
3.17	Удаление лицензионного ключа	78
3.18	Установка стандартной базы данных в ОС Astra Linux и Debian	78
3.19	Установка дополнительного компонента Ankey SIEM NG RC	86
3.19.1	Установка модуля Salt Minion на сервер Ankey SIEM NG RC	86

3.19.2	Установка роли RMQ Message Bus на сервер Ankey SIEM NG RC	87
3.19.3	Установка роли Retro Correlator	88
3.20	Установка доверенного сертификата для сайта Ankey SIEM NG	89
3.21	Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Agent	90
3.22	Настройка Ankey SIEM NG для обеспечения его безопасной работы	92
3.22.1	Настройка Ankey SIEM NG в конфигурации для низконагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like	92
3.22.2	Настройка Ankey SIEM NG в конфигурации для средненагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like	95
3.22.3	Настройка Ankey SIEM NG в конфигурации для высоконагруженных и сверхнагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like	98
4	Обновление ПК Ankey SIEM NG	102
4.1	Обновление с помощью дистрибутивов	102
4.1.1	Обновление облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows	103
4.1.2	Обновление компонента Ankey SIEM NG Agent на Windows Server	104
4.1.3	Обновление правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server	105
4.1.4	Обновление роли Deployer	106
4.1.5	Обновление компонента Ankey SIEM NG MC на Linux-like	106
4.1.6	Обновление компонента Knowledge Base на Linux-like	108
4.1.7	Обновление компонента Ankey SIEM NG Core на Linux-like	108
4.1.8	Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG ES на Linux-like	110
4.1.9	Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG Server на Linux-like	112
4.1.10	Обновление версии 4.0 компонента Ankey SIEM NG ES на Linux-like	114
4.1.11	Обновление версии 4.0 компонента Ankey SIEM NG Server на Linux-like	116
4.1.12	Обновление облегченной версии компонента Ankey SIEM NG Server на Linux-like	118
4.1.13	Обновление компонента Ankey SIEM NG Agent на Linux-like	120
4.1.14	Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG RC	121
4.1.15	Обновление версии 4.0 компонента Ankey SIEM NG RC	122
5	Удаление компонентов из ОС Windows Server	125
6	Просмотр и изменение параметров конфигурации Ankey SIEM NG	126
6.1	Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux-like	126
6.1.1	Просмотр конфигурации роли	126

6.1.2	Изменение конфигурации роли.....	126
6.1.3	Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch	127
6.1.4	Изменение степени сжатия данных в Elasticsearch.....	127
6.2	Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Microsoft Windows	128
6.2.1	Просмотр конфигурации.....	129
6.2.2	Изменение конфигурации вручную.....	129
6.2.3	Изменение конфигурации с помощью XML-файла.....	129
7	Диагностика и решение проблем	130
	Перечень сокращений.....	131
	Приложение А Порядок установки ПК Ankey SIEM NG.....	134
	Приложение Б Параметры конфигурации компонентов Ankey SIEM NG на Linux- like.....	137
	Приложение В Параметры конфигурации компонентов Ankey SIEM NG на Microsoft Windows	160
	Приложение Г Рекомендуемые конфигурации для систем хранения событий информационной безопасности	169
	Приложение Д Установка модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных)	170
Д.1	Установка дополнительных модулей сбора и обработки данных	170
Д.2	Установка дополнительных модулей выявления нарушений ИБ (корреляционной обработки данных).....	171
Д.2.1	Установка и удаление дополнительного пакета контента в Ankey SIEM NG	172
Д.2.2	Работа с ресурсами в пользовательской ветке	176

1 Об этом документе

Руководство по внедрению содержит информацию для планирования и выполнения развертывания Ankey SIEM Next Generation (далее также – ПК Ankey SIEM NG) в инфраструктуре организации. В руководстве вы найдете типовые схемы развертывания ПК Ankey SIEM NG, а также инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

Руководство адресовано руководителям и специалистам IT-подразделения организации, которые планируют и выполняют развертывание ПК Ankey SIEM NG.

Комплект документации ПК Ankey SIEM NG включает в себя документы, представленные в таблице 1.1.

Таблица 1.1 – Комплект документации ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
Сведения о релизе	Обзор новых возможностей Ankey SIEM NG	Содержит описание изменений между выпускаемой и предыдущей версиями ПК Ankey SIEM NG
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию и инструкции по настройке и администрированию продукта
	Руководство оператора Ankey SIEM NG	Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности
	Руководство по инсталляции Ankey SIEM NG	Содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
	Руководство администрирования Ankey SIEM NG Management and Configuration	Содержит справочную информацию и инструкции по настройке и администрированию компонента Ankey SIEM NG Management and Configuration
	Руководство по настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker
Подключение источников	Руководство по интеграции с источниками Ankey SIEM NG	Содержит рекомендации по интеграции элементов IT-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников и аудита активов

Каталог	Наименование документа	Описание
	Руководство по интеграции с источниками Ankey SIEM NG. Приложение А	Содержит перечни регистрируемых событий, маппинг событий и результаты обработки для поддерживаемых источников пакета стандартных коннекторов ПК Ankey SIEM NG
	Руководство по интеграции с источниками Ankey SIEM NG. Список изменений	Содержит список изменений пакета стандартных коннекторов ПК Ankey SIEM NG
Настройка корреляции	Пакет общих ресурсов контента <Номер версии пакета>. Описание	Содержит справочную информацию и инструкции по установке и настройке пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет общих ресурсов контента <Номер версии пакета>. Приложение А	Содержит списки применимых правил корреляции из состава пакета общих ресурсов контента ПК Ankey SIEM NG для поддерживаемых источников
	Пакет общих ресурсов контента <Номер версии пакета>. Список изменений	Содержит список изменений пакета общих ресурсов контента ПК Ankey SIEM NG
Дополнительно	Руководство разработчика Ankey SIEM NG	Содержит рекомендации по созданию правил нормализации, корреляции, агрегации и обогащения событий, описание утилит Ankey SIEM NG SDK для их отладки, а также информацию о доступных в Ankey SIEM NG функциях сервиса REST API
	Синтаксис языка запроса PDQL	Содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с Ankey SIEM NG
	PDQL-запросы для анализа активов	Содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в Ankey SIEM NG

В документе приняты условные обозначения.

Таблица 1.2 – Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия

Пример текста с условным обозначением	Описание
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
❖ Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду Stop-Service	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2 О ПК Ankey SIEM NG

Ankey SIEM Next Generation (далее также – Ankey SIEM NG) – это система управления событиями и информацией о безопасности, которая предназначена для сбора, хранения и анализа данных о событиях, которые генерируют различные источники в IT-инфраструктуре организаций. Ankey SIEM NG позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

ПК Ankey SIEM NG предоставляет следующие основные возможности:

- **Инвентаризация активов.** Система регулярно собирает данные о сетевых узлах и связях между ними;
- **Сбор данных о событиях.** В качестве источника событий может выступать любое поддерживаемое оборудование или ПО;
- **Анализ событий для выявления инцидентов ИБ.** Набор специальных правил, на основе которых выполняется анализ;
- **Управление инцидентами ИБ.** Система помогает организовать работу по расследованию инцидентов информационной безопасности и устранению их последствий;
- **Визуализация данных.** Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.

ПК Ankey SIEM NG предоставляет также дополнительные возможности:

- **Пакеты экспертизы.** Использование базы знаний. База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки;
- **Автоматизация работы с активами.** Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования IT-инфраструктуры;
- **Повторная проверка событий.** Ретроспективная корреляция полученных ранее событий после добавления новых правил или обновления данных табличных списков, ретроспективный поиск индикаторов компрометации;
- **Отправка уведомлений.** Оповещение ответственных об изменениях в IT-инфраструктурах организаций, о работе задач сбора данных Ankey SIEM NG, собираемых событиях, а также о выявляемых инцидентах ИБ.

2.1 Архитектура ПК Ankey SIEM NG

Ankey SIEM NG состоит из программных компонентов, которые возможно размещать как на одном сервере, так и на нескольких. Гибкая архитектура позволяет масштабировать и внедрять Ankey SIEM NG в организации с IT-инфраструктурами разных масштабов. Если поток событий в Ankey SIEM NG

превышает 3000 событий в секунду, то требуется распределенная установка компонентов ПК Ankey SIEM NG.

2.1.1 Компонент Ankey SIEM Next Generation Core

Компонент Ankey SIEM Next Generation Core (далее также – Ankey SIEM NG Core) является основным компонентом системы, ее управляющим сервером. Ankey SIEM NG Core устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях и выполняет следующие функции:

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- оперативное реагирование на инциденты информационной безопасности;
- обеспечение взаимодействия подразделений организации при расследовании инцидентов;
- поддержку веб-интерфейса системы.

2.1.2 Компонент Ankey SIEM Next Generation Server

Компонент Ankey SIEM Next Generation Server (далее также – Ankey SIEM NG Server) выполняет основные функции по обработке событий безопасности:

- агрегацию, фильтрацию, нормализацию и корреляцию событий;
- автоматическое создание инцидентов;
- привязку событий к активам.

2.1.3 Компонент Ankey SIEM Next Generation Events Storage

Компонент Ankey SIEM Next Generation Events Storage (далее также – Ankey SIEM NG Events Storage) обеспечивает централизованное хранение информации о событиях безопасности.

2.1.4 Компонент Ankey SIEM Next Generation Agent

Компонент Ankey SIEM Next Generation Agent (далее также – Ankey SIEM NG Agent) сканирует активы ИТ-инфраструктуры организации и собирает события с источников. Ankey SIEM NG Agent имеет модульную структуру. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и проводить специализированные проверки в режиме теста на проникновение.

Ankey SIEM NG Agent собирает следующую информацию об активах:

- название;
- версию и производителя операционной системы;
- установленные обновления ОС;
- список установленного ПО;
- параметры ОС и ПО;
- учетные записи пользователей и их привилегии;
- данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС;
- параметрах сети и средств защиты.

Ankey SIEM NG Agent управляет модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом Ankey SIEM NG Server.

К одному компоненту Ankey SIEM NG Server можно подключать несколько компонентов Ankey SIEM NG Agent. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

2.1.5 Компонент Ankey SIEM Next Generation Management and Configuration

Компонент Management and Configuration (далее также – Ankey SIEM NG MC) обеспечивает:

- сервис единого входа в продукты ПК Ankey SIEM NG, развернутые в инфраструктуре организации;
- управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;
- журналирование действий пользователей.

2.1.6 Компонент Ankey SIEM Next Generation Knowledge Base

Компонент Ankey SIEM NG Knowledge Base – это единая база знаний ПК, которая содержит схему полей событий, пакеты экспертизы (наборы правил и табличных списков), макросы (фильтры). Вместе с Ankey SIEM NG Knowledge Base устанавливаются утилиты (Software Development Kit или SDK) для разработки правил, макросов, табличных списков, валидации и управления установочными базами данных.

Создание, редактирование и хранение пакетов экспертизы и табличных списков для последующей установки в компонент Ankey SIEM NG Server осуществляется в приложении Ankey SIEM NG Knowledge Base.

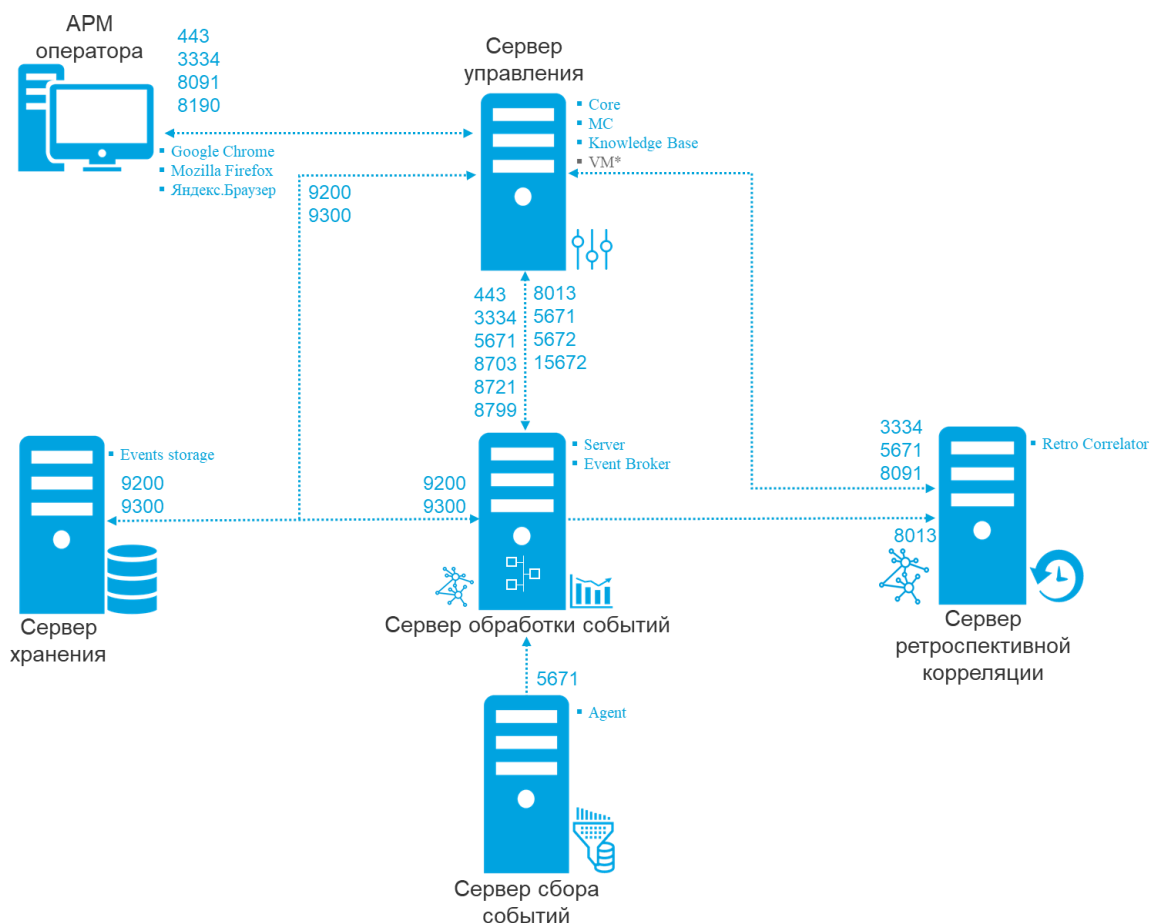
Примечание. Описание дополнительных модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных) представлено в приложении Д.

2.1.7 Компонент Ankey SIEM Next Generation Retro Correlator

Компонент Ankey SIEM Next Generation Retro Correlator (далее также – Ankey SIEM NG RC) выполняет повторную проверку полученных ранее событий при помощи правил корреляции. В состав компонента входят службы agent.service и siemserver-retrocontroller.service.

2.2 Схема взаимодействия компонентов

Взаимодействие компонентов ПК Ankey SIEM NG отражено на рисунке 2.1.



*Компонент Ankey SIEM NG VM является опциональным дополнительным модулем и лицензируется отдельно

Рисунок 2.1 – Схема взаимодействия компонентов ПК Ankey SIEM NG¹

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Agent сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и события с источников. Собранные данные агенты передают в Ankey SIEM NG Core и Ankey SIEM NG Server.
2. Компонент Ankey SIEM NG Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочими сведениями об узлах и связях между ними. Также компонент хранит параметры задач на сбор данных, профилей сканирования и транспортов, данные и сценарии справочников и осуществляет контроль доступа к этим данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов. Собранные события передаются на Ankey SIEM NG Server для нормализации, агрегации, обогащения и корреляции.

¹ При наличии дополнительного модуля Ankey SIEM NG VM для обновления базы данных уязвимостей может использоваться дополнительный компонент Ankey SIEM NG UCS. Для обновления баз данных модули Salt Minion иницируют подключение к модулю Salt Master на сервере Ankey SIEM NG UCS, используя TCP-порты 4505 и 4506. Для подключения к модулю Salt Master с помощью REST-интерфейса (без участия модуля Salt Minion) используется TCP-порт 9035.

3. Компонент Ankey SIEM NG Server обрабатывает входящий поток событий, приводит их к единому формату (нормализует). Затем выполняет корреляцию событий по заданным правилам. В результате этого процесса поток событий может обогатиться новыми событиями, полученными в результате действия правил корреляции. Ankey SIEM NG Server передает компоненту Ankey SIEM NG Events Storage поступившие события в исходном (необработанном) и в нормализованном виде для хранения.

Примечание. Нормализация событий может выполняться на сервере Ankey SIEM NG Agent. Для этого необходимо установить на сервер Ankey SIEM NG Agent облегченную версию Ankey SIEM NG Server – «SIEM на агенте». События, нормализованные на таком сервере Ankey SIEM NG Agent, передаются для хранения компоненту Ankey SIEM NG Events Storage.

4. Компонент Knowledge Base содержит базу знаний, необходимых Ankey SIEM NG для структурирования сведений, собранных от источников событий и объектов инфраструктуры.
5. Компонент Ankey SIEM NG обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
6. Для управления системой, просмотра данных, построения отчетов и мониторинга пользователь подключается к компоненту Ankey SIEM NG Core через веб-интерфейс в соответствии с правами, которые назначены в Ankey SIEM NG MC.
7. Компонент Ankey SIEM NG RC обеспечивает возможность ретроспективной проверки полученных ранее событий, используя новые правила корреляции и данные из табличных списков.

Для обеспечения сетевого взаимодействия компонентов ПК Ankey SIEM NG должны быть доступны для входящих соединений порты, которые представлены в таблице 2.1.

Таблица 2.1 – Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя, ПО для загрузки данных уведомлений	Ankey SIEM NG Core	443
Ankey SIEM NG Server	Ankey SIEM NG Core	443, 3334, 5671, 8703, 8721,8799
Ankey SIEM NG RC	Ankey SIEM NG Core	5671
Рабочая станция пользователя	Knowledge Base	8091, 8190
Ankey SIEM NG RC	Knowledge Base	8091
Рабочая станция пользователя, компонент Ankey SIEM NG RC	Ankey SIEM NG MC	3333, 3334
Ankey SIEM NG Core	Ankey SIEM NG Server	5671, 5672, 8013, 15672
Knowledge Base, Ankey SIEM NG RC	Ankey SIEM NG Server	8013

Источник	Получатель	TCP-порт
Ankey SIEM NG Agent	Ankey SIEM NG Server	5671
Ankey SIEM NG Core, Ankey SIEM NG Server	Ankey SIEM NG ES	9200, 9300

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов ПК Ankey SIEM NG рекомендуется разрешить соединения от рабочих станций администраторов:

- через порт 3389/TCP (протокол RDP) – к серверу под управлением ОС Windows Server с установленным компонентом Ankey SIEM NG Agent;
- через порт 22/TCP – к серверам под управлением ОС Linux-like с установленными компонентами ПК Ankey SIEM NG.

3 Развертывание ПК Ankey SIEM NG

В этом разделе приведены инструкции по установке компонентов Ankey SIEM NG, активации лицензии и первоначальной настройке ключевых функций системы, даны рекомендации по выбору конфигурации, а также описаны типовые схемы развертывания, аппаратные и программные требования к серверам.

3.1 Типовые схемы развертывания Ankey SIEM NG

В этом подразделе приведены рекомендации по выбору конфигурации Ankey SIEM NG, описаны типовые схемы развертывания.

3.1.1 Рекомендации по выбору конфигурации Ankey SIEM NG

В зависимости от сложности IT-инфраструктуры организации могут применяться следующие конфигурации Ankey SIEM NG:

- **для низконагруженных систем.** Рекомендуется для развертывания в организациях, которые рассчитывают выполнять периодическое сканирование узлов не чаще одного раза в месяц и получать поток событий от источников, не превышающий 3000 событий в секунду, и не планируют расширение своей IT-инфраструктуры;

Внимание! Если поток событий, который принимает ПК Ankey SIEM NG, превышает 70 % от допустимого потока для низконагруженной конфигурации, а также планируется установка или создание дополнительных правил корреляции помимо встроенных, то рекомендуется применять конфигурацию для средненагруженных или высоконагруженных систем (в зависимости от потока событий). Применение конфигурации для средненагруженных или высоконагруженных систем позволяет расширить возможности горизонтального или вертикального масштабирования SIEM-системы (включая новые функциональные возможности), а также увеличить общую пропускную способность и производительность.

- **для средненагруженных систем.** Рекомендуется для развертывания в организациях, которые рассчитывают получать поток событий от источников, не превышающий 10 000 событий в секунду, и планируют расширение своей IT-инфраструктуры;
- **для высоконагруженных систем.** Рекомендуется для развертывания в организациях, которые планируют получать поток событий от источников, не превышающий 30 000 событий в секунду;
- **для сверхнагруженных систем.** Рекомендуется для развертывания в организациях, которые планируют

получать поток событий от источников, не превышающий 60 000 событий в секунду.

Развертывание ПК Ankey SIEM NG на нескольких площадках

В крупных организациях вы можете развернуть в каждом подразделении одну из конфигураций ПК Ankey SIEM NG – локальную площадку. Каждая площадка имеет свой управляющий сервер – компонент Ankey SIEM NG Core и свою базу активов и инцидентов. С помощью компонентов Ankey SIEM NG MC площадки связываются между собой, в результате чего синхронизируются учетные записи их пользователей, становятся доступными распределенный поиск событий и их репликация между площадками.

Установка дополнительных конвейеров обработки событий

Конвейер обработки событий в общем случае состоит из компонентов Ankey SIEM NG Server и Ankey SIEM NG ES и нескольких агентов. По умолчанию ПК Ankey SIEM NG содержит только один конвейер. Вы можете добавить один или несколько конвейеров в существующую систему (например, в случае расширения IT-инфраструктуры) или изначально развернуть систему на нескольких конвейерах. Количество дополнительных конвейеров ограничено лицензией.

Конвейер можно установить в каждом территориально удаленном филиале организации для сбора, обработки и хранения событий, произошедших на активах этого филиала. Работой всех конвейеров управляет единый сервер – компонент Ankey SIEM NG Core, установленный в центральном офисе. Кроме того, каждый конвейер отправляет на управляющий сервер сведения об активах своего филиала. В центральном офисе также может быть установлен свой конвейер для обработки событий, произошедших в IT-инфраструктуре этого офиса.

Развертывание системы на нескольких конвейерах позволяет равномерно распределить нагрузку между ними и в то же время использовать единый сервер для хранения сведений обо всех активах и инцидентах, для управления задачами сканирования IT-инфраструктуры и сбора событий, а также для просмотра и анализа событий.

3.1.2 Схема развертывания конфигурации для низконагруженных систем

Для развертывания конфигурации потребуется один сервер. На него необходимо установить основные компоненты Ankey SIEM NG Core, Ankey SIEM NG Knowledge Base, Ankey SIEM NG MC, Ankey SIEM NG Server, Ankey SIEM NG Events Storage и Ankey SIEM NG Agent.

Если потребуется функционал ретроспективной корреляции, то на отдельном сервере возможно развернуть дополнительный компонент Ankey SIEM NG RC. Установка этого компонента необязательна, однако его рекомендуется устанавливать для использования дополнительных возможностей Ankey SIEM NG.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.9).

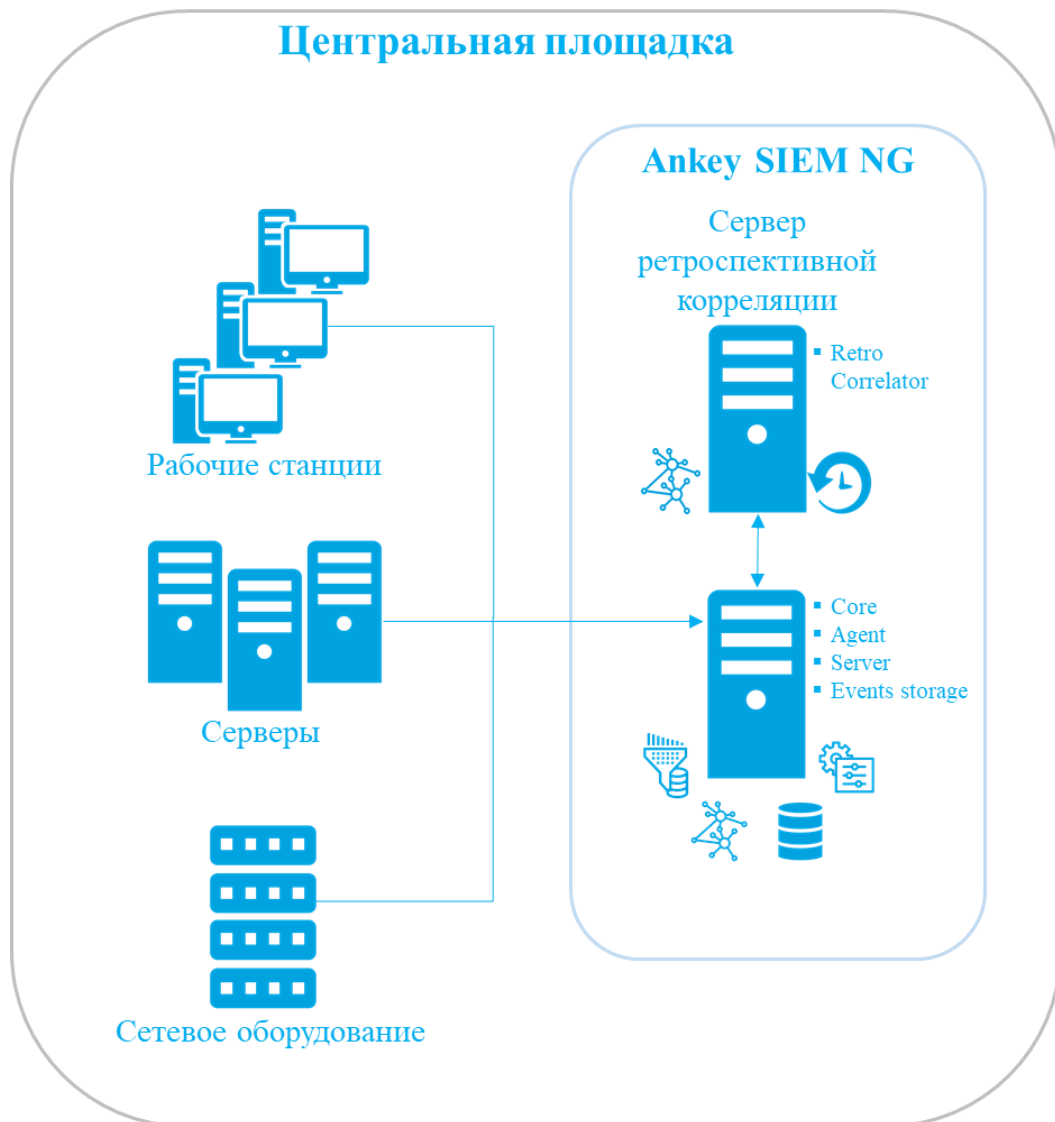


Рисунок 3.1 – Развертывание конфигурации для низконагруженных систем на одной площадке

В зависимости от физической или логической топологии IT-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный агент².

Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных агентов.

² **Внимание!** Рекомендуется не нагружать один агент большим количеством CustomEventCollector ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

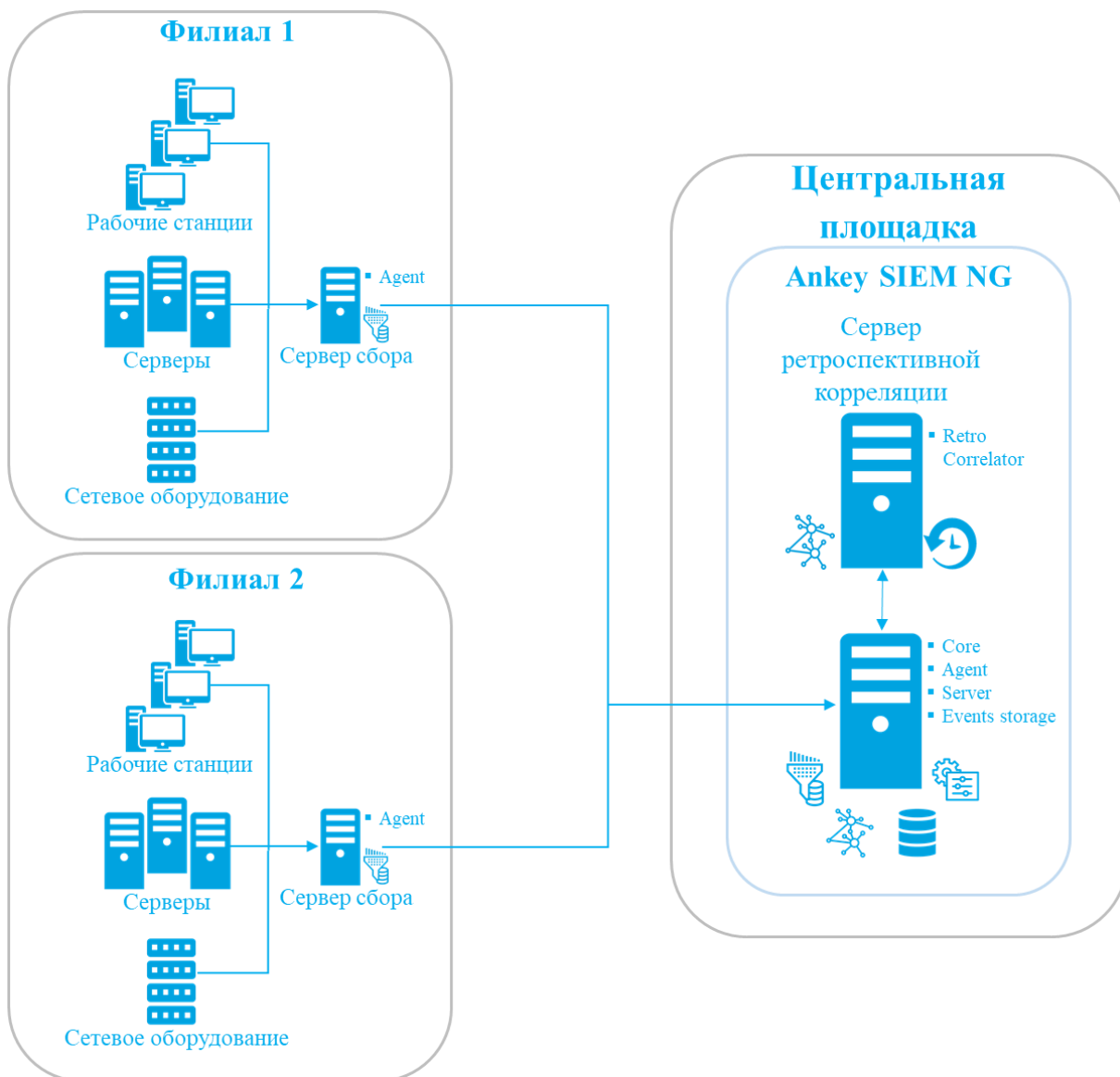


Рисунок 3.2 – Развертывание конфигурации для низконагруженных систем на филиальной сети

3.1.3 Схема развертывания конфигурации для средненагруженных систем

Для развертывания ПК Ankey SIEM NG в средненагруженной конфигурации потребуются минимум три сервера. На первый сервер необходимо установить основные компоненты Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и Ankey SIEM NG Agent, на второй – основные компоненты Ankey SIEM NG Server и Ankey SIEM NG Events Storage, на третий – дополнительный компонент Ankey SIEM NG Agent. Количество дополнительных компонентов Ankey SIEM NG Agent будет зависеть от общего потока событий на весь ПК Ankey SIEM NG. При потоке 10 000 событий в секунду всего потребуется четыре компонента Ankey SIEM NG Agent с распределением потока между ними (не более 3000 событий в секунду на один Ankey SIEM NG Agent).

На отдельный сервер возможно установить дополнительный компонент Ankey SIEM NG RC. Установка этого компонента необязательна, однако его

рекомендуется устанавливать для использования дополнительных возможностей Ankey SIEM NG.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.9).

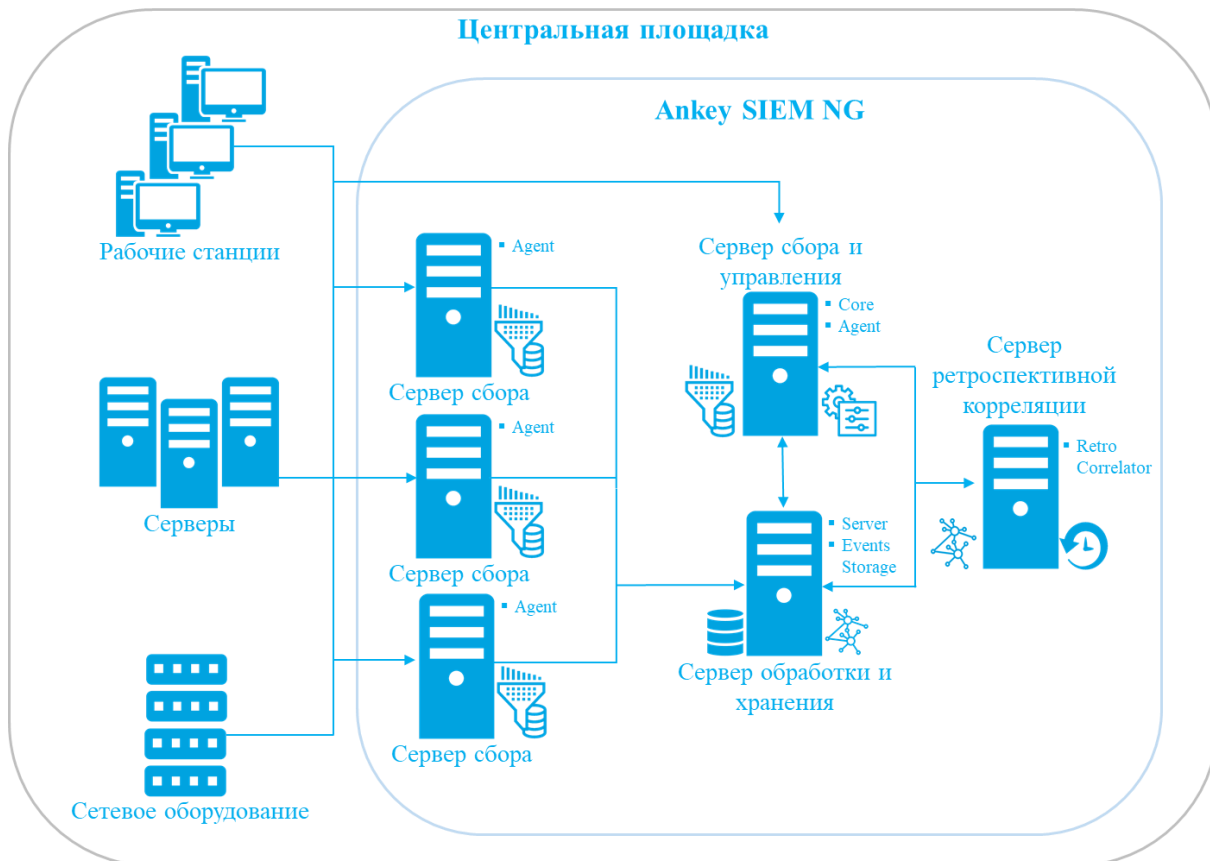


Рисунок 3.3 – Развертывание конфигурации для средненагруженных систем на одной площадке

В зависимости от физической или логической топологии IT-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный агент³.

Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных агентов.

³ **Внимание!** Рекомендуется не нагружать один агент большим количеством CustomEventCollector ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

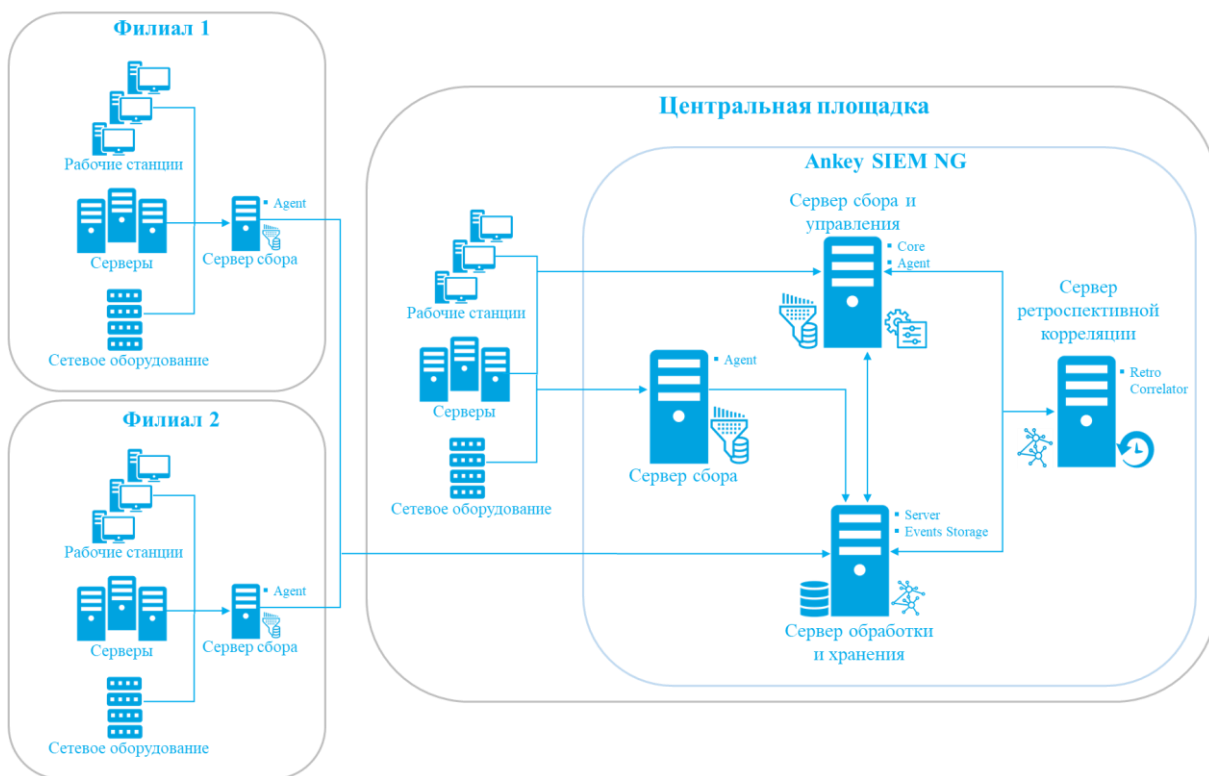


Рисунок 3.4 – Развертывание конфигурации для средненагруженных систем на филиальной сети

3.1.4 Схема развертывания конфигураций для высоконагруженных и сверхнагруженных систем

Для развертывания конфигураций вам потребуются:

- сервер для компонентов Ankey SIEM NG Core, Ankey SIEM NG Knowledge Base и Ankey SIEM NG MC;
- сервер для компонента Ankey SIEM NG Server;
- сервер для компонента Ankey SIEM NG Events Storage;
- серверы для компонентов Ankey SIEM NG Agent.

Количество серверов для компонентов Ankey SIEM NG Agent⁴ зависит от планируемой нагрузки на агенты, а также от физической и логической топологии ИТ-инфраструктуры организации. В конфигурации:

- для высоконагруженных систем при потоке до 30 000 событий в секунду потребуется распределить весь поток событий между 10 серверами с компонентом Ankey SIEM NG Agent (не более 3 000 событий в секунду на 1 Ankey SIEM NG Agent);
- для сверхнагруженных систем при потоке до 60 000 событий в секунду потребуется распределить весь поток событий между 20 серверами с компонентом Ankey SIEM

⁴ **Внимание!** Рекомендуется не нагружать один агент большим количеством CustomEventCollector ввиду потребления большого количества оперативной памяти, что требуется учитывать при выборе архитектуры программного комплекса с учетом распределения компонентов в инфраструктуре.

NG Agent (не более 3 000 событий в секунду на 1 Ankey SIEM NG Agent).

Если требуется сканировать узлы, расположенные в отдельных сетевых сегментах, рекомендуется устанавливать отдельный агент на каждый сегмент.

На отдельный сервер возможно установить дополнительный компонент Ankey SIEM NG RC. Установка этого компонента необязательна, однако его рекомендуется устанавливать для использования дополнительных возможностей Ankey SIEM NG.

Компоненты системы могут быть установлены в виртуальной среде (см. пункт 3.2.9).

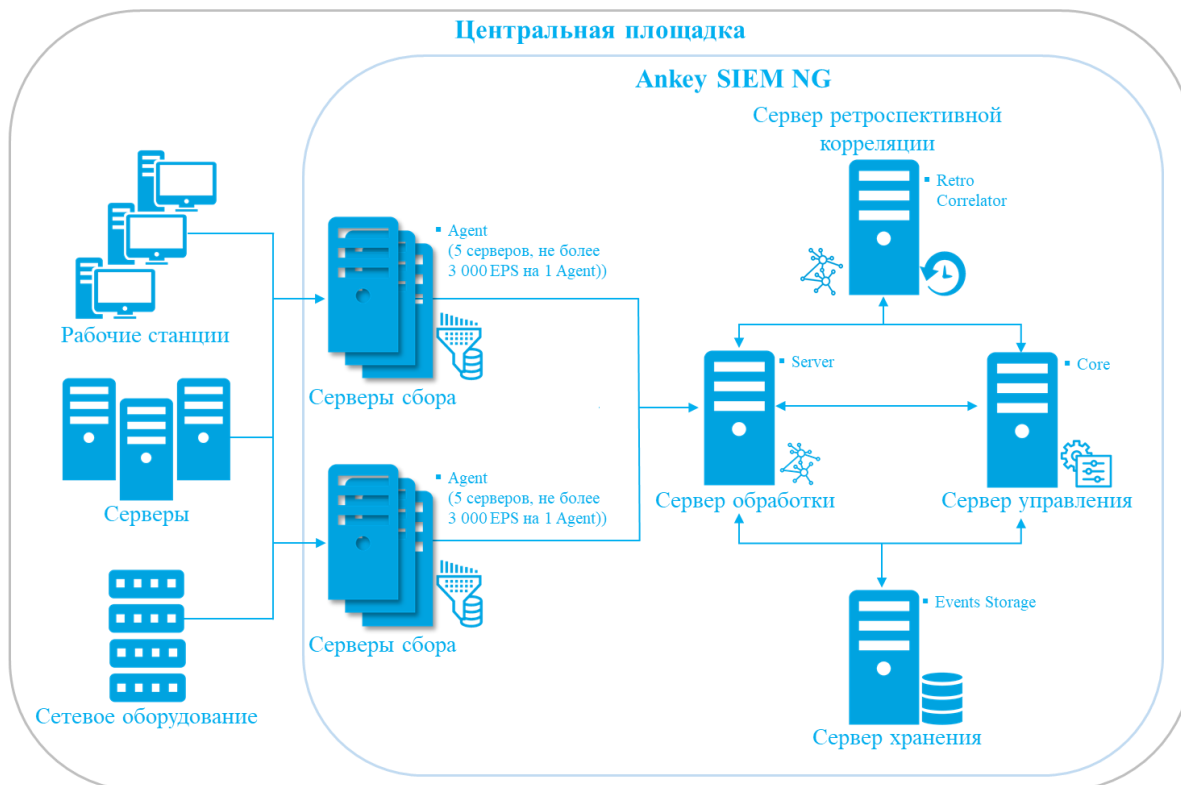


Рисунок 3.5 – Развертывание конфигурации для высоконагруженных систем (не более 3 000 событий в секунду на 1 Ankey SIEM NG Agent)

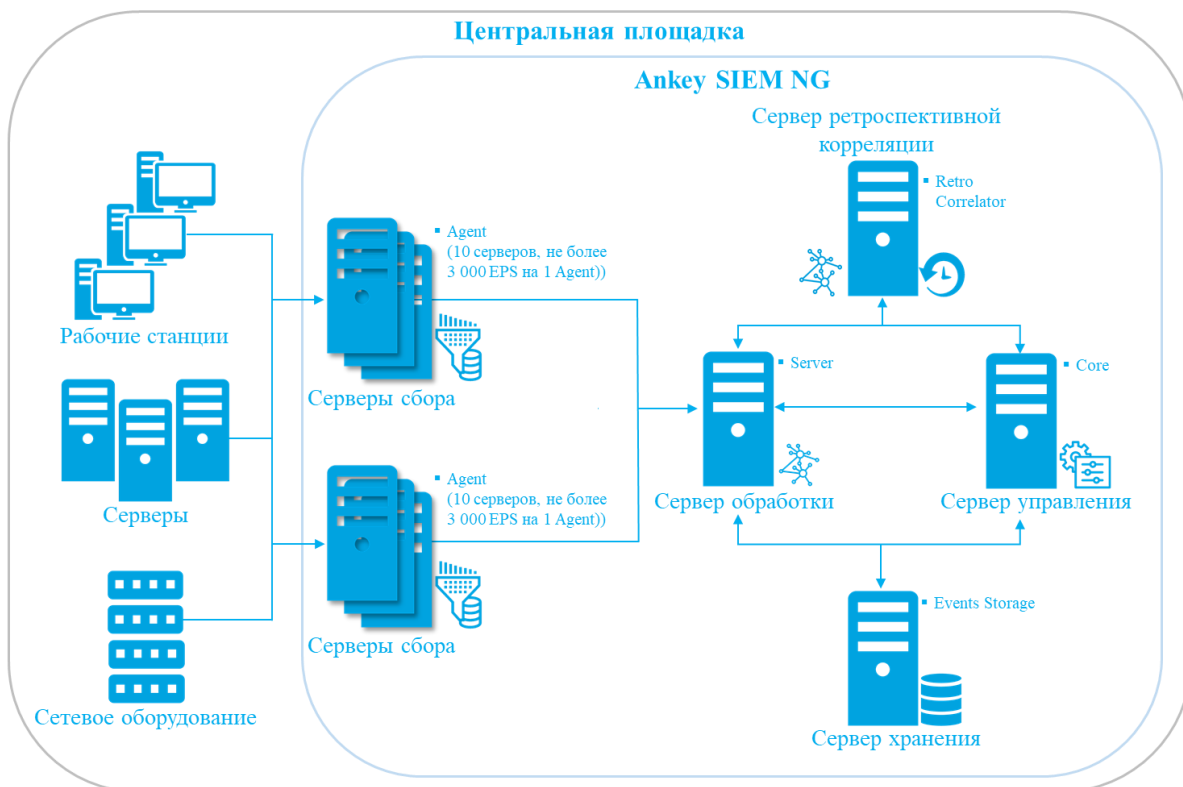


Рисунок 3.6 – Развертывание конфигурации для сверхнагруженных систем (не более 3 000 событий в секунду на 1 Ankey SIEM NG Agent)

3.1.5 Об установке конвейеров обработки событий

По умолчанию в состав ПК Ankey SIEM NG входит только один конвейер обработки событий. В конфигурациях для средненагруженных, высоконагруженных и сверхнагруженных систем вы можете установить один или несколько дополнительных конвейеров. Не рекомендуется устанавливать дополнительные конвейеры в конфигурации для низконагруженных систем (такая схема развертывания не поддерживается производителем).

Аппаратное обеспечение серверов каждого конвейера должно соответствовать потоку собираемых и обрабатываемых им событий. Компоненты конвейера необходимо устанавливать в следующем порядке: Ankey SIEM NG ES → Ankey SIEM NG Server → агенты (Ankey SIEM NG Agent, Ankey SIEM NG RC). Компоненты Ankey SIEM NG Server и Ankey SIEM NG ES могут быть установлены как на один сервер (в конфигурации для средненагруженных систем), так и на отдельные серверы (в конфигурациях для высоконагруженных и сверхнагруженных систем). Агенты рекомендуется устанавливать на отдельные серверы⁵.

Один из конвейеров является главным, поскольку через компонент Ankey SIEM NG ES этого конвейера выполняются все запросы по фильтрации событий, в том числе хранящихся в других конвейерах (кросс-кластерный поиск). По умолчанию главным является первый установленный конвейер.

⁵ **Внимание!** Установка агента на один сервер с компонентами Ankey SIEM NG Server, Ankey SIEM NG ES и Event Broker не рекомендуется, так как такая инсталляция не предусмотрена архитектурно, что может привести к затруднению в работе модуля Salt при установке, а также Event Broker при эксплуатации.

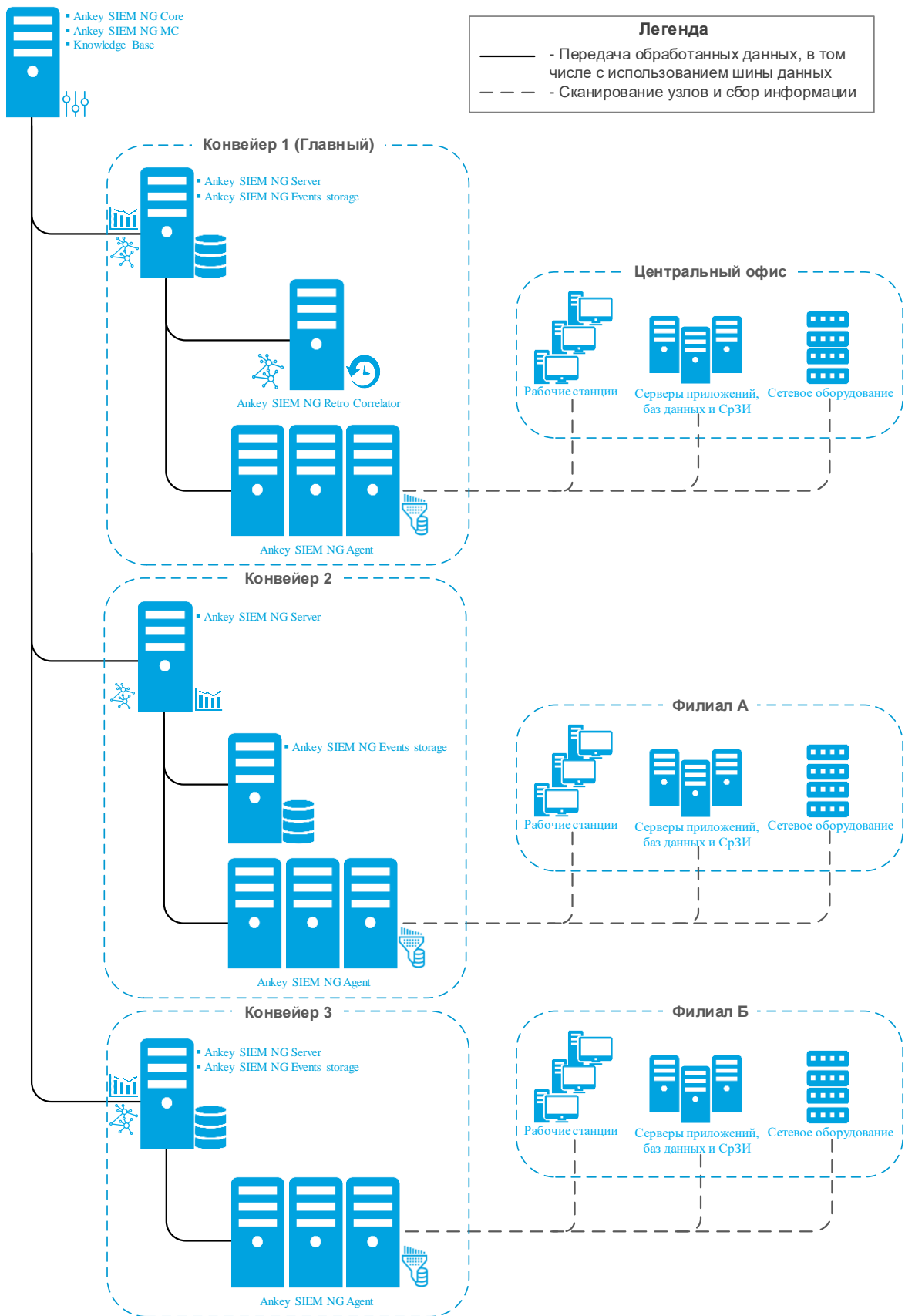


Рисунок 3.7 – Пример конфигурации ПК Ankey SIEM NG, развернутой на трех конвейерах

3.2 Аппаратные и программные требования

В этом подразделе приведены требования к аппаратному и программному обеспечению серверов Ankey SIEM NG.

3.2.1 Требования к аппаратному обеспечению конфигурации для низконагруженных систем

Компоненты системы необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3.1 – Аппаратные требования к серверу сбора, управления, обработки и хранения событий с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC, Ankey SIEM NG Knowledge Base, Ankey SIEM NG Server, Ankey SIEM NG Events Storage и Ankey SIEM NG Agent

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 56 логических ядер)
Память (ОЗУ)	128 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
Компонент сервера	Минимальное требование
	<p><i>Для хранения данных²:</i> Для определения требуемого объема свободного дискового пространства и выбора накопителей для хранения событий следуйте инструкциям в пункте 3.2.7</p> <p><i>Расчетные значения³:</i></p> <p>250 EPS</p> <ul style="list-style-type: none"> – в оперативном доступе: не менее 483 ГБ; – в архивах⁴: не менее 1448 ГБ. <p>1000 EPS</p> <ul style="list-style-type: none"> – в оперативном доступе: не менее 1932 ГБ; – в архивах⁴: не менее 5794 ГБ. <p>2500 EPS</p> <ul style="list-style-type: none"> – в оперативном доступе: не менее 4828 ГБ; – в архивах⁴: не менее 14484 ГБ
<p>¹Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы</p>	

ОС (корневым каталогом / на Linux-like) и объемом 1000 ГБ для работы компонентов и баз данных (каталогом /var на Linux-like).

² Рекомендуется использовать отдельный RAID-массив (RAID1+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).

³ При сроках хранения событий в оперативном доступе – 30 дней рекомендуется рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях.

Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.

⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше чем хранилище для событий в оперативном доступе минимум в два раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Таблица 3.2 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	1 процессор с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многоядерности (не менее 8 логических ядер)
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство ²	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹

¹Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.

² Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт).

3.2.2 Требования к аппаратному обеспечению конфигурации для средненагруженных систем

Компоненты системы необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3.3 – Аппаратные требования к серверу сбора и управления с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC, Ankey SIEM NG Knowledge Base и Ankey SIEM NG Agent

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 32 логических ядер)
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	<i>Для ОС и установки ПО:</i> диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
<p>¹Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом / на Linux-like) и объемом 2200 ГБ для работы компонентов и баз данных (каталогом /var на Linux-like).</p>	

Таблица 3.4 – Аппаратные требования к серверу обработки и хранения с компонентами Ankey SIEM NG Server, Ankey SIEM NG Events Storage

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 56 логических ядер)
Память (ОЗУ)	256 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый

Компонент сервера	Минимальное требование
Жесткие диски и свободное дисковое пространство	<p><i>Для ОС и установки ПО:</i> диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве¹</p>
	<p><i>Для хранения данных²:</i> Для определения требуемого объема свободного дискового пространства и выбора накопителей для хранения событий следуйте инструкциям в пункте 3.2.7</p>
	<p><u>Расчетные значения³:</u></p> <p>3000 EPS – в оперативном доступе: не менее 5794 ГБ; – в архивах⁴: не менее 17381 ГБ.</p> <p>5000 EPS – в оперативном доступе: не менее 9656 ГБ; – в архивах⁴: не менее 28968 ГБ.</p> <p>10000 EPS – в оперативном доступе: не менее 19312 ГБ; – в архивах⁴: не менее 57936 ГБ</p>
<p>¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на три логических раздела – корневой каталог объемом 200 ГБ для работы ОС, каталог /var объемом 400 ГБ для файлов журналов ОС и RabbitMQ, каталог /opt объемом 400 ГБ для файлов журналов и кэша Ankey SIEM NG.</p> <p>² Рекомендуется использовать отдельный RAID-массив (RAID1+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).</p> <p>³ При сроках хранения событий в оперативном доступе – 30 дней необходимо рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях.</p> <p>Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.</p> <p>⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен</p>	

быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше чем хранилище для событий в оперативном доступе минимум в два раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Таблица 3.5 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	1 процессор с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 8 логических ядер)
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство ²	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
¹ Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. ² Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт).	

3.2.3 Требования к аппаратному обеспечению конфигурации для высоконагруженных систем

Компоненты системы необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3.6 – Аппаратные требования к серверу управления с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Knowledge Base

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 32 логических ядер)
Память (ОЗУ)	128 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый

Компонент сервера	Минимальное требование
Жесткие диски и свободное дисковое пространство	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
<p>¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом / на Linux-like) и объемом 2200 ГБ для работы компонентов и баз данных (каталогом /var на Linux-like).</p>	

Таблица 3.7 – Аппаратные требования к серверу обработки с компонентом Ankey SIEM NG Server

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 56 логических ядер)
Память (ОЗУ)	128 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый, 2 порта со скоростью 10 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
<p>¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на три логических раздела – корневой каталог объемом 200 ГБ для работы ОС, каталог /var объемом 1000 ГБ для файлов журналов ОС и RabbitMQ, каталог /opt объемом 1000 ГБ для файлов журналов и кэша Ankey SIEM NG.</p>	

Таблица 3.8 – Аппаратные требования к серверу хранения с компонентом Ankey SIEM NG Events Storage

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 56 логических ядер)
Память (ОЗУ)	256 ГБ

Компонент сервера	Минимальное требование
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый, 2 порта со скоростью 10 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	<i>Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве¹</i>
	<i>Для хранения данных²: Для определения требуемого объема свободного дискового пространства и выбора накопителей для хранения событий следуйте инструкциям в пункте 3.2.7</i>
	<i>Расчетные значения³: 15000 EPS – в оперативном доступе: не менее 28968 ГБ; – в архивах⁴: не менее 86904 ГБ. 20000 EPS – в оперативном доступе: не менее 38624 ГБ; – в архивах⁴: не менее 115872 ГБ. 30000 EPS – в оперативном доступе: не менее 57936 ГБ; – в архивах⁴: не менее 173808 ГБ</i>
<p>¹ Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на два логических раздела – корневой каталог объемом 200 ГБ для работы ОС и каталог /es_logs объемом 1000 ГБ для файлов журналов Ankey SIEM NG Events Storage.</p> <p>² Рекомендуется использовать отдельный RAID-массив (RAID10+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).</p> <p>³ При сроках хранения событий в оперативном доступе – 30 дней необходимо рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях.</p> <p>Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуются восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.</p> <p>⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен</p>	

быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше чем хранилище для событий в оперативном доступе минимум в два раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Таблица 3.9 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	1 процессор с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 8 логических ядер)
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство ²	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
¹ Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. ² Преобразовать файловую систему в ext4 (размер блока 4096 байт).	

3.2.4 Требования к аппаратному обеспечению конфигурации для сверхнагруженных систем

Компоненты системы необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3.10 – Аппаратные требования к серверу управления с компонентами Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Knowledge Base

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 32 логических ядер)
Память (ОЗУ)	128 ГБ

Компонент сервера	Минимальное требование
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	<i>Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве¹</i>
¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (для Linux-like, размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом / на Linux-like) и объемом 2200 ГБ для работы компонентов и баз данных (каталогом /var на Linux-like).	

Таблица 3.11 – Аппаратные требования к серверу обработки с компонентом Ankey SIEM NG Server

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 64 логических ядер)
Память (ОЗУ)	128 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый, 2 порта со скоростью 10 Гбит/с каждый
Жесткие диски и свободное дисковое пространство ²	<i>Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве¹</i>
¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на три логических раздела – корневой каталог объемом 200 ГБ для работы ОС, каталог /var объемом 1000 ГБ для файлов журналов ОС и RabbitMQ, каталог /opt объемом 1000 ГБ для файлов журналов и кэша Ankey SIEM NG.	

Таблица 3.12 – Аппаратные требования к серверу хранения с компонентом Ankey SIEM NG Events Storage

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (суммарно не менее 56 логических ядер)
Память (ОЗУ)	256 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый, 2 порта со скоростью 10 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	<i>Для ОС и установки ПО:</i> диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
	<i>Для хранения данных²:</i> Для определения требуемого объема свободного дискового пространства и выбора накопителей для хранения событий следуйте инструкциям в пункте 3.2.7
	<i>Расчетные значения³:</i> 35000 EPS – в оперативном доступе: не менее 67592 ГБ; – в архивах ⁴ : не менее 202776 ГБ. 50000 EPS – в оперативном доступе: не менее 95560 ГБ; – в архивах ⁴ : не менее 289679 ГБ

¹Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. Преобразовать файловую систему в ext4 (размер блока 4096 байт) и разделить дисковое пространство на два логических раздела – корневой каталог объемом 200 ГБ для работы ОС и каталог /es_logs объемом 1000 ГБ для файлов журналов Ankey SIEM NG Events Storage.

²Рекомендуется использовать отдельный RAID-массив (RAID10+1HS) для дисков типа SSD. Поддерживаемые конфигурации RAID-массивов приведены в Приложении Г и зависят от применяемых типов дисков. Рекомендуется при выборе конфигурации хранилища данных учитывать критерии масштабирования решений класса SIEM, такие как постепенное увеличение потока событий и увеличение сроков хранения событий в различном формате, что сказывается на расширении объема хранилища данных (конфигурация хранилища должна иметь возможность расширения сформированного объема с учетом выполнения требований по IOPS).

³При сроках хранения событий в оперативном доступе – 30 дней необходимо рассчитывать объем дискового пространства для архивных событий – 90 дней. Сроки хранения могут быть изменены, определяются условиями применения ПК Ankey SIEM NG и описываются в проектных решениях.

Внимание! Не следует превышать максимальный срок (90 суток) хранения событий в оперативном доступе Elasticsearch, т.к. если потребуется восстановить в оперативный доступ события из архивов, то максимальный срок в 90 суток будет превышен, что приведет к сбоям в работе Elasticsearch. На регулярной основе рекомендуется хранить в оперативном доступе события не более чем за 30 суток.

⁴ Архивные события должны храниться обязательно для восстановления, в случае необходимости, в оперативном доступе (срок хранения архивных событий не должен быть менее срока хранения событий, находящихся в оперативном доступе). Архивные данные могут быть размещены на выделенном дисковом RAID-массиве с дисками HDD (SAS/SATA от 7200 об./мин. и выше) или в RAID-массиве с SSD в случае выполнения требований по скорости восстановления систем (в зависимости от требований RTO для соответствующих объемов восстанавливаемых данных). Хранилище для архивных событий должно быть больше чем хранилище для событий в оперативном доступе минимум в два раза.

Примечание. Сроки хранения определяются проектными решениями: необходимо рассчитывать конфигурацию дискового хранилища в зависимости от сроков хранения пропорционально текущим значениям либо в зависимости от поступающего потока событий и среднего размера события (в расчет берутся как необработанные (RAW), так и нормализованные события).

Таблица 3.13 – Аппаратные требования к серверу ретроспективной корреляции с компонентом Ankey SIEM NG Retro Correlator

Компонент сервера	Минимальное требование
Центральный процессор	1 процессор с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 8 логических ядер)
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство ²	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
¹ Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями. ² Преобразовать файловую систему в ext4 (размер блока 4096 байт).	

3.2.5 Аппаратные требования к серверу облегченной версия Ankey SIEM NG Server («SIEM на агенте»)

Компоненты Ankey SIEM NG Agent и Ankey SIEM NG Server в конфигурации облегченная версия Ankey SIEM NG Server («SIEM на агенте») необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям. Данные аппаратные требования актуальны для всех типов конфигураций системы.

Таблица 3.14 – Аппаратные требования к серверу сбора и обработки событий с компонентами Ankey SIEM NG Agent и Ankey SIEM NG Server («SIEM на агенте»)

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 56 логических ядер)
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Для ОС и установки ПО: диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве ¹
¹ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.	

3.2.6 Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Agent, размещенному в отдельном сегменте сети

Компонент Ankey SIEM NG Agent, размещенный в отдельном сегменте сети, необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям. Данные аппаратные требования актуальны для всех типов конфигураций системы.

Таблица 3.15 – Аппаратные требования к серверу сбора событий с компонентом Ankey SIEM NG Agent, размещенному в отдельном сегменте сети

Компонент сервера	Минимальное требование		
	Конфигурации для низконагруженных систем ⁴ . До 1000 событий\сек, не более чем с 1000 узлов	Конфигурации для средненагруженных систем ⁴ . До 3000 событий\сек, не более чем с 1000 узлов	Конфигурации для высоконагруженных или сверхнагруженных систем ⁴ . До 3000 событий\сек, не более чем с 1000 узлов ⁵
Центральный процессор	1 процессор с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 32 логических	2 процессора с тактовой частотой не менее 2,2 ГГц, поддержка инструкций SSE4.2 и AVX, поддержка технологии многопоточности (не менее 56 логических ядер)

Компонент сервера	Минимальное требование		
	Конфигурации для низконагруженных систем ⁴ . До 1000 событий\сек, не более чем с 1000 узлов	Конфигурации для средненагруженных систем ⁴ . До 3000 событий\сек, не более чем с 1000 узлов	Конфигурации для высоконагруженных или сверхнагруженных систем ⁴ . До 3000 событий\сек, не более чем с 1000 узлов ⁵
	менее 8 логических ядер)	ядер)	
Память (ОЗУ)	32 ГБ	64 ГБ	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый		
Жесткие диски и свободное дисковое пространство ²	<i>Для ОС и установки ПО:</i> диски HDD (10000 об./мин.) SAS или SSD не менее 1000 ГБ эффективного объема дискового пространства в RAID-массиве ¹		<i>Для ОС и установки ПО:</i> диски HDD (10000 об./мин.) SAS или SSD не менее 2000 ГБ эффективного объема дискового пространства в RAID-массиве ³

¹ Для установки ПО требуется не менее 1000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID1+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.

² Рекомендуется преобразовать файловую систему в ext4 (для Linux, размер блока 4096 байт).

³ Для установки ПО требуется не менее 2000 ГБ свободного места на дисковом пространстве. Для повышения отказоустойчивости рекомендуется использовать отдельный RAID на HDD (10000 об./мин.) SAS (рекомендуемая конфигурация RAID10+1HS), а также устанавливать компоненты ОС на отдельный RAID-массив. Возможно использование других конфигураций RAID-массивов в соответствии с проектными решениями. Объем дискового массива для ОС также может быть увеличен в соответствии с проектными решениями.

⁴ Максимальное количество одновременно функционирующих задач с модулями опроса конфигураций (аудита) активов ограничено. На одном агенте не рекомендуется одновременно запускать: более 4 задач с каждым модулем **audit**, **pentest**, **customeventcollector**, **vshperevenetcollector**; более 100 задач с модулями **syslog**, **wineventlog**, **filemonitor**, **netflow**, **odbclog**, **networkwatch**, **ssheventcollector**, **snmpeventcollector**; более 1 задачи с каждым модулем **hostdiscovery**, **batcheventsearch**, **dpicollector**, **mp8scanimporter**.

⁵ Максимальный поток событий в секунду для компонента Ankey SIEM NG Agent может быть увеличен в конфигурациях для высоконагруженных и сверхнагруженных систем с учетом развития функциональных возможностей (по потоку событий) компонентов платформы. Рекомендуется использовать данные вычислительные ресурсы для сервера компонента Ankey SIEM NG Agent в тех случаях, когда невозможно развернуть несколько серверов сбора событий на одном объекте и общий поток на объекте может превысить 3000 событий в секунду (с учетом возникновения всплесков событий от среднего потока).

3.2.7 Рекомендации по расчету объема и выбору накопителей для хранения событий

Для определения требуемого объема свободного дискового пространства необходимо выполнить расчеты.

Примечание. Расчеты выполняются для определения объема необработанных и нормализованных событий.

Вы можете рассчитать приблизительный объем (в байтах), необходимый для хранения суточного объема данных о событиях, по формуле:

$V_{hdd} = R * T * EPS$, где

V_{hdd} – объем свободного дискового пространства;

EPS – (events per second) суммарное количество событий ИБ в секунду от всех источников событий;

R – средний размер события ИБ в байтах (800 байт);

T – количество секунд в сутках (86400 секунд);

Например, при средней скорости 1000 событий в секунду система запишет за сутки $800 \times 86400 \times 1000 \approx 65$ ГБ данных.

Объем требуемого дискового пространства для хранения событий ИБ на определенном периоде времени рассчитывается по формуле:

$V_{hdd} = EPS * R * T / (1024 * 1024 * 1024) * D$, где

V_{hdd} – объем свободного дискового пространства;

EPS – (events per second) суммарное количество событий ИБ в секунду от всех источников событий;

R – средний размер события ИБ в байтах (800 байт);

T – количество секунд в сутках (86400 секунд);

$1024 * 1024 * 1024$ – перевод из байтов в Гигабайты;

D – общее количество дней, в течение которых требуется хранить события ИБ.

Пример расчета объема дискового пространства для хранения событий в течение 30 дней при суммарном потоке 30 000 событий в секунду:

$V_{hdd} = 30000 \times 800 \times 86400 / (1024 \times 1024 \times 1024) \times 30 \approx 57\,936$ ГБ

Реальное потребление свободного места зависит от типа событий и может быть как меньше, так и больше значений, рассчитанных по формуле.

В низконагруженной конфигурации рекомендуется объединить жесткие диски или твердотельные диски в массив RAID 10 и выделить на отдельном логическом диске каталог /data для хранения индексов в оперативном доступе с событиями информационной безопасности. Для организации хранения архивных индексов необходимо выделить дополнительный логический диск для каталога /es_backup⁶ (описание создания хранилища индексов представлено в Руководстве администратора Ankey SIEM NG 4.1.2).

В средненагруженной и высоконагруженной конфигурациях рекомендуется объединить жесткие диски или твердотельные диски в массив RAID 10 и выделить в отдельную файловую систему каталог /data для хранения индексов в оперативном доступе с событиями информационной безопасности. Для организации хранения архивных индексов необходимо выделить в отдельную

⁶ При инсталляции можно задать пользовательское наименование каталога (например: /data_archive). Подробнее см. пункт 3.10.2.

файловую систему каталог `/es_backup`⁷. Объем дискового пространства для архивных индексов зависит от объема индексов в оперативном доступе и необходимого срока хранения.

В сверхнагруженной конфигурации необходимо использовать два типа накопителей данных: жесткие диски и твердотельные накопители. Рекомендуется объединить жесткие диски в массив RAID 10 и подключить к ним каталог `/data` для хранения индексов, находящихся в «теплой» стадии, твердотельные накопители – объединить в массив RAID 6 и подключить к ним каталог `/datahot` для хранения индексов, находящихся в «горячей» стадии.

Примечание. Подробное описание стадий жизненного цикла индексов приведено на сайте elastic.co.

3.2.8 Требования к программному обеспечению

Все компоненты Ankey SIEM NG поддерживают установку на ОС семейства Linux-like – Astra Linux Special Edition 1.7⁸ или Debian 10. Кроме того, вы можете установить компонент Ankey SIEM NG Agent и облегченную версию Ankey SIEM NG Server («SIEM на агенте») на Windows Server 2012, 2012 R2, 2016, 2019 или 2022.

Перед развертыванием Ankey SIEM NG необходимо настроить DNS серверов, на которые будут устанавливаться компоненты системы

Внимание! Перед развертыванием Ankey SIEM NG на Astra Linux Special Edition 1.7 необходимо на серверах компонентов выполнить действия, указанные в бюллетенях производителя № 2021-1126SE17 и № 2022-0318SE17MD (подробнее см. [в справочном центре Astra Linux](#)).

Примечание. При развертывании компонента Ankey SIEM NG Agent устанавливается драйвер WinPcap 4.1.3. Не рекомендуется дополнительно устанавливать другие версии драйвера WinPcap, поскольку работа другой версии драйвера может привести к некорректной работе модуля `hostdiscovery`.

Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Поддерживаемые браузеры – Google Chrome версий 49 и выше, Mozilla Firefox версий 45 и выше, Яндекс.Браузер версий 22 и выше.

3.2.9 Рекомендации по развертыванию Ankey SIEM NG в виртуальной среде

Рекомендуется использовать версию 11 виртуальной машины VMware vSphere и версию 6.0 гипервизора VMware ESXi с приведенными ниже

⁷ При инсталляции можно задать пользовательское наименование каталога (например: `/data_archive`). Подробнее см. пункт 3.10.2.

⁸ Рекомендуется при установке операционной системы Astra Linux 1.7.x SE применять уровень защищенности «Максимальный» («Смоленск»), т.к. уровень безопасности и надежности выше.

параметрами распределения ресурсов.

Настройка гипервизора

Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы.

Настройка центрального процессора

В аппаратных требованиях к центральному процессору указано минимальное количество логических ядер. Если сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить вдвое меньше физических ядер. Если технология Hyperthreading не используется, количество выделенных физических ядер должно быть равно количеству логических. Например, если виртуальной машине требуется 56 логических ядер и сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить два процессора по 14 ядер каждый.

Для повышения производительности виртуальной машины рекомендуется в блоке параметров **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**.

Настройка оперативной памяти

Объем оперативной памяти, выделяемой каждой виртуальной машине, не должен быть меньше значения, указанного в аппаратных требованиях. Также необходимо учитывать, что часть оперативной памяти сервера (до 8% от общего объема) должна быть зарезервирована для работы гипервизора.

Для работы виртуальной машины рекомендуется зарезервировать постоянный объем оперативной памяти, установив в блоке параметров **Resources Allocation** флажок **Reserve all guest memory (All locked)**.

Настройка виртуальных жестких дисков

Объем и производительность виртуальных жестких дисков не должны быть меньше значений, указанных в аппаратных требованиях.

При создании виртуального жесткого диска на шаге **Create a Disk** в блоке параметров **Disk Provisioning** рекомендуется выбрать вариант **Thick Provision Eager Zeroed**, на шаге **Advanced Options** в блоке параметров **Mode** рекомендуется установить флажок **Independent**, а затем выбрать вариант **Persistent**.

3.2.10 Взаимодействие с внешними системами

Средства обеспечения безопасности могут оказывать влияние на работу Ankey SIEM NG. Поэтому на этапе планирования и развертывания рекомендуется провести тестовые сканирования и при необходимости принять меры для снижения негативных последствий. Например, может потребоваться отключить средства межсетевого экранирования, антивирусную защиту или специализированные средства контроля аппаратного оборудования на серверах, где установлены компоненты Ankey SIEM NG.

Большинство сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (stateful inspection, application firewall), которые могут вмешиваться в процесс сканирования, снижая достоверность полученных результатов. Так, например, результат сканирования веб-

приложения через межсетевой экран, поддерживающий функции защиты веб-приложений (web application firewall), не будет достоверным, поскольку межсетевой экран заблокирует ряд потенциально опасных запросов, используемых сканером. В некоторых средствах защиты нельзя отключить фильтрацию прикладных протоколов для отдельных узлов, и в таких случаях рекомендуется выносить Ankey SIEM NG Agent за межсетевой экран.

Системы обнаружения и предотвращения атак часто реагируют на процесс сканирования как на потенциальную атаку. Получение списка открытых портов, проверка стойкости паролей, доступ к протоколам удаленного управления – все это может привести к срабатыванию средств защиты. В случае если механизм предотвращения атак не задействован, множественные срабатывания сигнатур приведут только к увеличению объема журналов системы обнаружения атак. Если механизм предотвращения атак включен, то система может вмешаться в процесс сканирования и исказить результаты работы. В связи с этим рекомендуется вносить узлы, на которых установлены компоненты Ankey SIEM NG, в список исключений системы обнаружения атак.

3.3 Подготовка к установке Ankey SIEM NG

3.3.1 Подготовка к установке Ankey SIEM NG на ОС Astra Linux SE

В процессе установки операционных систем Astra Linux, на этапе дополнительных настроек, необходимо убедиться, что не включен параметр **Запрос пароля для команды sudo**, как представлено на рисунке 3.8.

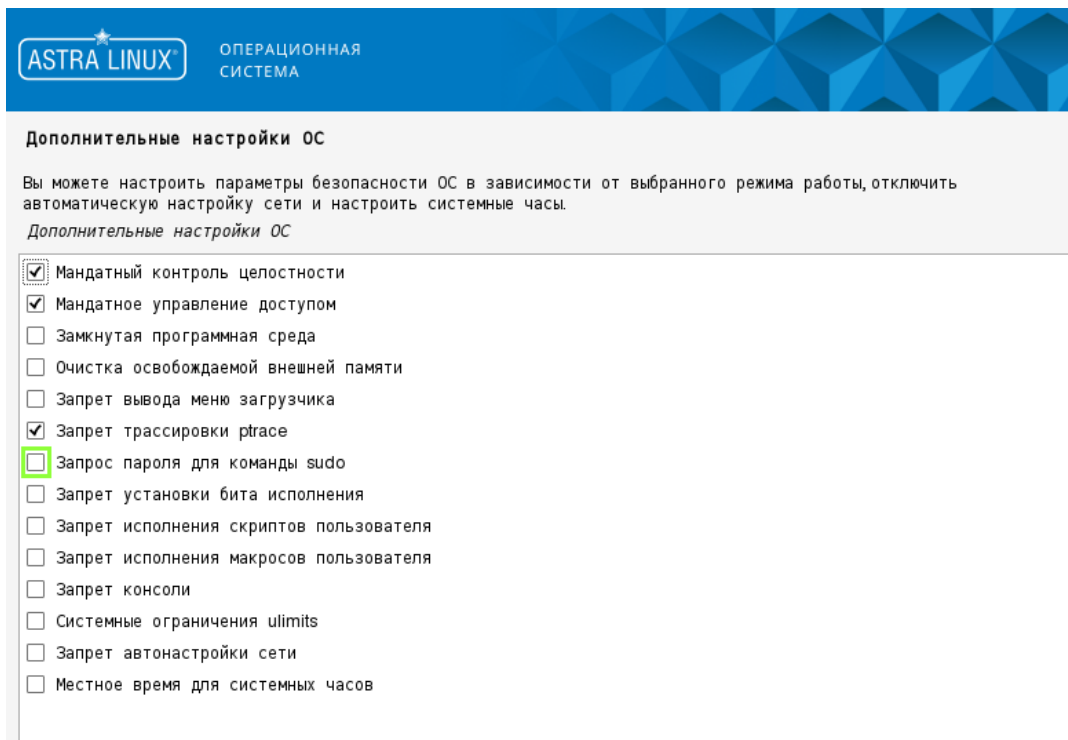


Рисунок 3.8 – Дополнительные настройки ОС Astra Linux

Если операционная система Astra Linux была установлена с активированным параметром **Запрос пароля для команды sudo**, то его

возможно отключить с помощью команды `sudo astra-sudo-control disable` в интерфейсе командной строки операционной системы.

После установки всех компонентов ПК, в случае необходимости, запрос пароля для команды `sudo` возможно включить в уже установленной операционной системе с помощью команды `sudo astra-sudo-control enable`, которую следует выполнить в интерфейсе командной строки с правами суперпользователя.

Перед началом установки ПК Ankey SIEM NG необходимо обеспечить для всех хостов, куда планируется установка компонентов ПК, доступность корректно настроенного DNS-сервера. В DNS-сервере должны быть настроены зоны прямого и обратного просмотра.

Если планируется в ПК Ankey SIEM NG использовать функционал для отправки уведомлений пользователям SIEM-системы по электронной почте, то в почтовом сервере ИТ-инфраструктуры, где внедряется ПК Ankey SIEM NG, необходимо создать сервисную учетную запись, например, `ak_siem_ng`.

Внимание! Перед началом установки ролей ПК необходимо корректно настроить репозитории для ОС Linux-like.

Например, для ОС Astra Linux SE следует выполнить команду `sudo nano /etc/apt/sources.list`.

Если есть доступ к глобальной сети Интернет, то в файле `sources.list` следует проверить наличие или добавить адреса репозитория для ОС Astra Linux SE:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-  
64 main contrib non-free
```

Все остальные ссылки следует закомментировать или удалить.

Если нет доступа к глобальной сети Интернет, то необходимо настроить локальный репозиторий ОС Astra Linux SE. Для этого необходимо создать каталог и распаковать в него архив с пакетами локального репозитория. Далее в файл `/etc/apt/sources.list` следует добавить ссылку на каталог, в котором содержатся пакеты локального репозитория. Например, `deb [trusted=yes] file:<Полный путь до каталога с локальным репозиторием> main non-free`.

Все остальные ссылки следует закомментировать или удалить.

3.4 Об установке компонентов на Linux-like с помощью ролей

Роль является базовой единицей развертывания на Linux-like и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые

распределяются по приложениям определенного типа (Management and Configuration, Knowledge Base или Ankey SIEM NG). Такая архитектура позволяет гибко и удобно развертывать систему, а также обновлять и настраивать ее в дальнейшем. Тип приложения определяется составом входящих в него экземпляров ролей:

- приложение Management and Configuration содержит только роли SqlStorage/JatobaStorage и Management and Configuration;
- приложение Knowledge Base – только роль Knowledge Base;
- приложение Ankey SIEM NG – только роли Core, SIEM Server, Events Storage Elasticsearch, Events Storage LogSpace, Agent, RMQ Message Bus и Retro Correlator.

Примечание. При развертывании системы можно создать несколько приложений одного типа (например, несколько приложений Knowledge Base), однако такие конфигурации не поддерживаются производителем.

Управление развертыванием обеспечивается ролью Deployer, которая построена на базе системы управления конфигурациями SaltStack. Ее модуль Salt Master обеспечивает общее управление установкой (созданием экземпляров) ролей, модули Salt Minion – установку ролей на каждый сервер системы.

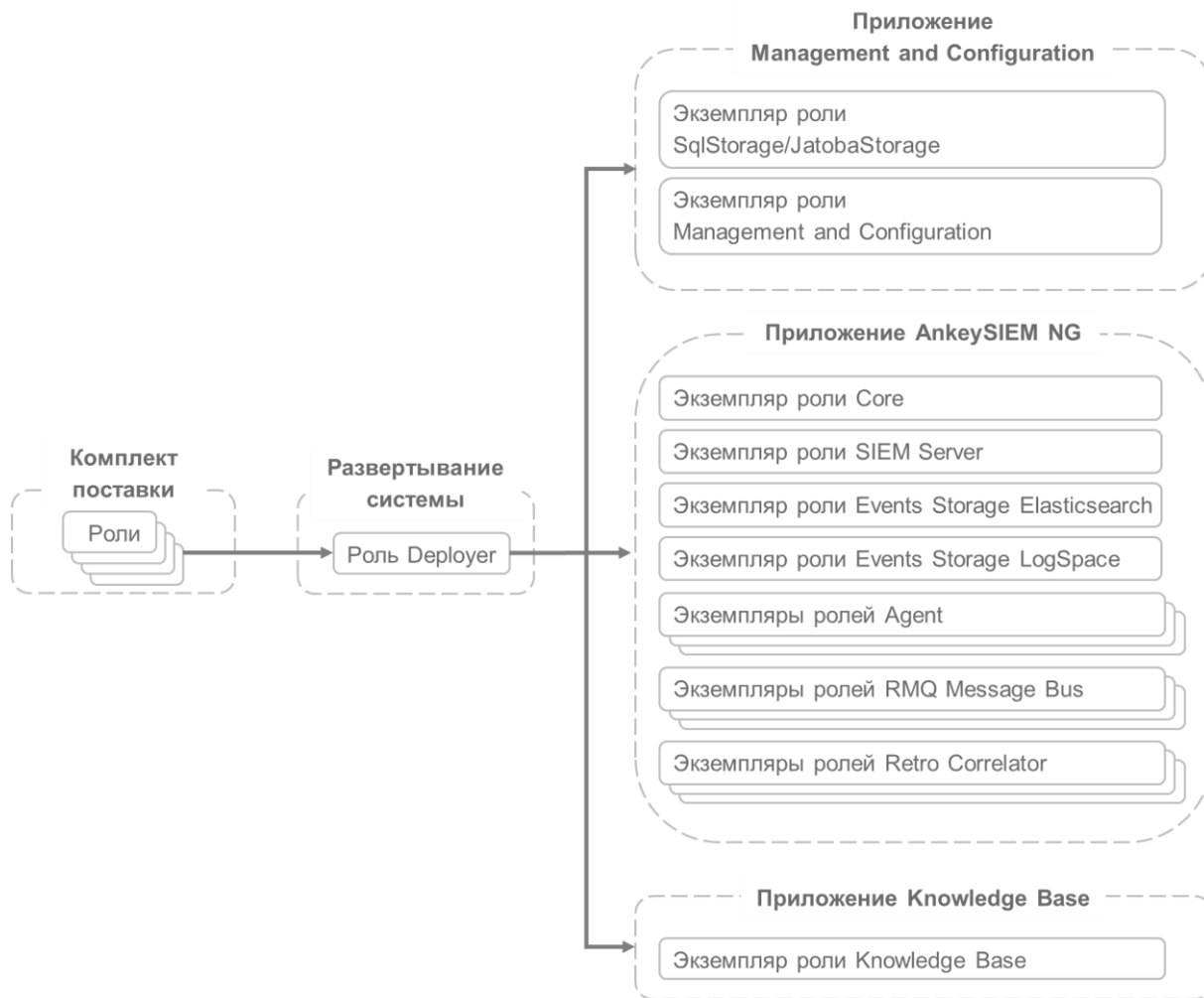


Рисунок 3.9 – Развертывание системы с помощью ролей

Для установки компонента может потребоваться установка как одной, так и нескольких ролей. В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.
2. Выбор приложения для установки роли. Вам потребуется или выбрать ранее созданное приложение необходимого типа, или создать новое, если приложение необходимого типа отсутствует. При создании приложения нужно ввести его идентификатор, который среди прочего будет использоваться в качестве имени каталога для размещения файлов всех экземпляров ролей, входящих в состав данного приложения.

Примечание. Вы можете использовать идентификаторы, предлагаемые системой по умолчанию. Например, если для приложения Management and Configuration использовать предлагаемый по умолчанию идентификатор mc-application, файлы всех экземпляров ролей этого приложения будут размещены в каталоге /var/lib/deployedroles/mc-application.

3. Ввод названия экземпляра роли и выбор сервера для ее установки. Введенное название среди прочего будет использоваться в качестве имени каталога для размещения файлов создаваемого экземпляра роли (например, файлов журналов и файлов конфигурации).

Примечание. Вы можете использовать названия, предлагаемые системой по умолчанию. Например, если для роли SqlStorage использовать предлагаемое по умолчанию название `sqlstorage`, файлы этого экземпляра ролей будут размещены в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли %Компонент%>`. Например: `/var/lib/deployed-roles/mc-applicaton/sqlstorage`.

4. Проверка и изменение параметров конфигурации.
Запуск установки.

3.5 Сценарий развертывания Ankey SIEM NG

Порядок установки компонентов зависит от конфигурации Ankey SIEM NG и от операционных систем, выбранных для серверов Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG Event Storage. При установке компонентов на Linux-like базовыми единицами развертывания являются роли (см. подраздел 3.4).

Внимание! Все установочные файлы ПК Ankey SIEM NG⁹ следует разместить в соответствии со структурой и порядком каталогов на хосте, где планируется установка компонента Core. После копирования установочных файлов ПК Ankey SIEM NG необходимо убедиться, что каталогу с установочными файлами и всем архивам с установочными файлами назначены максимальные права доступа `sudo chmod 777 /opt` или `KB_21.0.5549-LinuxBuild-Ankey.tar.gz`. Весь процесс установки ролей компонентов ПК Ankey SIEM NG необходимо выполнять с хоста, где планируется установка компонента Core.

⁹ Если реализована поставка ПК Ankey SIEM NG на нескольких носителях (например, в виде компакт-дисков), то необходимо перенести установочные файлы со всех носителей в среду функционирования для последующего запуска установки ПО в соответствующей конфигурации. При копировании дополнительного ПО на хост следует выполнять копирование архивов, а не каталогов. Копирование каталогов с дополнительным ПО может привести к перезаписи содержимого уже существующих каталогов на хосте. Т.е. в уже готовую структуру каталогов с основным ПО Ankey SIEM NG на хосте необходимо добавить только архивы с дополнительным ПО.

Компоненты Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG Event Storage устанавливаются на Linux-like

Этот вариант развертывания поддерживают все конфигурации Ankey SIEM NG.

Внимание! Примеры распределения ролей и порядка действий по серверам ПК Ankey SIEM NG в зависимости от выбранной конфигурации представлены в приложении А.

При развертывании необходимо придерживаться следующего порядка действий¹⁰:

1. Установить и настроить ОС Astra Linux Special Edition 1.7 или Debian 10. Подробнее см. инструкцию по установке ОС Astra Linux Special Edition 1.7 или инструкцию по установке Debian 10, а также подраздел 3.3.
2. Установка роли Deployer (см. подраздел 3.6).
3. Установка компонента Ankey SIEM NG MC (см. подраздел 3.7):
 - 3.1 Установка роли SqlStorage (см. пункт 3.7.1) или JatobaStorage (см. пункты 3.7.2 или 3.7.3).
 - 3.2 Установка роли Management and Configuration (см. пункт 3.7.4).
4. Установка компонента Knowledge Base (см. подраздел 3.8):
 - 4.1 Установка роли Knowledge Base.
5. Установка компонента Ankey SIEM NG Core (см. подраздел 3.9):
 - 5.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core (см. пункт 3.9.1).
 - 5.2 Установка роли Core (см. пункт 3.9.2).
6. Установка компонента Ankey SIEM NG ES (см. подраздел 3.10):
 - 6.1 Установка модуля Salt Minion на сервер Ankey SIEM NG ES¹¹ (см. пункт 3.10.1).
 - 6.2 Установка роли Event Storage с хранилищем событий Elasticsearch (см. пункт 3.10.2).
 - 6.3 Установка роли Event Storage с хранилищем событий LogSpace (опционально) (см. пункт 3.10.3).
7. Установка компонента Ankey SIEM NG Server (см. подраздел 3.11):
 - 7.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Server¹² (см. пункт 3.11.1).
 - 7.2 Установка роли RMQ Message Bus¹³ (см. пункт 3.11.2).

¹⁰ Все команды далее в терминале необходимо выполнять с правами суперпользователя root. Для этого можно перейти в учетную запись суперпользователя с помощью команды `sudo -s` или выполнять команды под учетной записью текущего пользователя используя команду `sudo` (например, `sudo ./install.sh`).

¹¹ В конфигурации для низконагруженных систем установка модуля Salt Minion на сервер Ankey SIEM NG ES не требуется.

¹² Данный шаг необходимо выполнить, если Ankey SIEM NG Core установлен на Linux в конфигурации для высоконагруженных или сверхнагруженных систем. В конфигурации для средненагруженных систем модуль Salt Minion устанавливается на сервер Ankey SIEM NG Server при установке компонента Ankey SIEM NG ES.

¹³ Данный шаг необходимо выполнить, если Ankey SIEM NG Server устанавливается в

- 7.3 Установка роли SIEM Server (см. пункт 3.11.3).
8. Установка компонента Ankey SIEM NG Agent (см. подраздел 3.12):
 - 8.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Agent¹⁴ (см. пункт 3.12.1).
 - 8.2 Установка роли Agent (см. пункт 3.12.2).
 9. Установка облегченной версии Ankey SIEM NG Server и правил нормализации и агрегации для нее (опционально):
 - 9.1 Установка модуля Salt Minion (см. пункт 3.13.1).
 - 9.2 Установка роли RMQ Message Bus (см. пункт 3.13.2).
 - 9.3 Установка роли SIEM Server (см. пункт 3.13.3).
 10. Активация лицензии (см. подраздел 3.16).
 11. Установка стандартной базы данных (см. подраздел 3.18).
 12. Установка и первоначальная настройка компонента Ankey SIEM NG RC (опционально) (см. подраздел 3.19):
 - 12.1 Установка модуля Salt Minion (см. пункт 3.19.1).
 - 12.2 Установка роли RMQ Message Bus (см. пункт 3.19.2).
 - 12.3 Установка роли Retro Correlator (см. пункт 3.19.3).
 13. Настройка Ankey SIEM NG для обеспечения его безопасной работы (см. подраздел 3.22).

3.6 Установка роли Deployer

Для установки роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

Роль необходимо устанавливать:

- если компоненты Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG Event Storage устанавливаются на Linux-like – на сервер Ankey SIEM NG Core.

Внимание! Перед установкой роли Deployer необходимо синхронизировать время на серверах, на которые будут установлены роли Deployer и Core.

Для установки роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. Если на сервере Ankey SIEM NG MC есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
2. Распакуйте архив `Deployer_<Номер версии>.tar.gz`:
`tar -xf Deployer_<Номер версии>.tar.gz`
3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
4. В открывшемся окне нажмите кнопку **Yes**.

конфигурации для средненагруженных, высоконагруженных или сверхнагруженных систем.

¹⁴ Данный шаг необходимо выполнить, если Ankey SIEM NG Agent устанавливается на отдельный сервер.

- Начнутся распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.
5. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
Откроется окно для проверки и изменения параметров установки.
 6. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
 7. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера, на который устанавливается роль `Deployer`.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

8. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **ОК**.
Роль установлена.

3.7 Установка компонента Ankey SIEM NG MC на Linux-like

Компонент Ankey SIEM NG MC устанавливается с помощью ролей `SqlStorage` или `JatobaStorage` и `Management and Configuration` в следующем порядке: сначала устанавливается роль `SqlStorage` или `JatobaStorage`, затем роль `Management and Configuration`.

Перед установкой компонента Ankey SIEM NG MC необходимо принять решение, какая именно роль будет установлена `SqlStorage` (СУБД PostgreSQL) или `JatobaStorage` (СУБД Jatoba).

Для установки роли `JatobaStorage` потребуется:

- доступ к глобальной сети Интернет (для получения лицензии в режиме онлайн или офлайн);
- действующий ключ активации для СУБД Jatoba.

3.7.1 Установка роли SqlStorage

Для установки роли вам потребуется архив `SqlStorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `SqlStorage_<Номер версии>.tar.gz`:
`tar -xvf SqlStorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.

Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.

4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли SqlStorage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
13. Нажмите кнопку **OK**.

Роль установлена.

3.7.2 Установка роли JatobaStorage и онлайн активация лицензии

Для установки роли вам потребуется архив JatobaStorage_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив JatobaStorage_<Номер версии>.tar.gz:
tar -xf JatobaStorage_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.

4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли JatobaStorage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Для выполнения онлайн активации СУБД Jatoba следует выбрать вариант **Basic configuration**.
Откроется список основных параметров для настройки установки СУБД.
11. Необходимо убедиться, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выбрать значение online.
13. В поле **LicenceKey** удалить значение по умолчанию XXXXX-XXXXX-XXXXX-XXX и вручную ввести ключ для активации СУБД Jatoba.
14. Если устанавливается роль JatobaStorage с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение `https://licence.gaz-is.ru`.
16. Значения в других полях следует оставить по умолчанию.
17. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
18. Выберите **OK** и нажмите на клавиатуре клавишу Enter.
Роль установлена.

Внимание! Перед установкой других ролей ПК Ankey SIEM NG необходимо проверить работоспособность docker-контейнера с СУБД Jatoba. После установки роли JatobaStorage выполнить команду: `docker ps -a`
В результате вывода команды должны содержаться данные обо всех установленных docker-контейнерах и их состоянии. Название docker-контейнера с СУБД Jatoba будет зависеть от названия роли (например: storage-jatoba). В колонке STATUS должно быть значение UP <количество времени>, в течение которого docker-контейнер с СУБД Jatoba активен.

3.7.3 Установка роли JatobaStorage и офлайн активация лицензии

Для установки роли вам потребуется архив `JatobaStorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `JatobaStorage_<Номер версии>.tar.gz`:
`tar -xf JatobaStorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения **Management and Configuration** и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли **JatobaStorage** и нажмите кнопку **OK**. Откроется окно для проверки и изменения параметров установки.
10. Для выполнения онлайн активации СУБД **Jatoba** следует выбрать вариант **Basic configuration**. Откроется список основных параметров для настройки установки СУБД.
11. Необходимо убедиться, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выбрать значение `offline`.
13. В поле **LicenceKey** удалить значение по умолчанию `XXXXX-XXXXX-XXXXX-XXX` и вручную ввести ключ для активации СУБД **Jatoba**.
14. Если устанавливается роль **JatobaStorage** с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение `https://licence.gaz-is.ru`.
16. Значения в других полях следует оставить по умолчанию.

17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
18. Выберите **ОК** и нажмите на клавиатуре клавишу **Enter**.

Роль установлена.

❖ Для офлайн активации лицензии:

1. После установки роли `JatobaStorage` перейдите в каталог `/var/lib/deployed-roles/<Название приложения Ankey SIEM NG MC, например: mc-application-ankey>/<Название роли СУБД Jatoba, например: jatobastorage>/config/license/` и проверьте наличие файла `request.dat`.
2. Перенесите файл `request.dat` на хост с доступом к глобальной сети Интернет.
3. В веб-браузере хоста с доступом к глобальной сети интернет необходимо перейти на сайт `https://license.gaz-is.ru/offlineActivate/`. В веб-браузере должна отобразиться страница **Офлайн-активация**.
4. Для формирования запроса на офлайн активацию лицензии СУБД `Jatoba` скопируйте в окно ввода активационный запрос для получения файла лицензии или скопируйте и вставьте запрос из файла `request.dat`.
В ответ на запрос из файла `request.dat` будет предоставлен файл лицензии `license.bin`.
5. Сохраните на хосте файл `license.bin` и переименуйте с соблюдением регистра в `jatoba.cer`.
6. Перенесите файл `jatoba.cer` в каталог `/var/lib/deployed-roles/<Название приложения Ankey SIEM NG MC, например: mc-application-ankey>/<Название роли СУБД Jatoba, например: jatobastorage>/config/license/`.

Лицензия для СУБД `Jatoba` активирована.

Примечание. Подробнее о получении лицензии с активацией офлайн вы можете прочитать в Руководстве по установке СУБД `Jatoba` [на сайте производителя](#).

Внимание! Перед установкой других ролей ПК `Ankey SIEM NG` необходимо проверить работоспособность `docker`-контейнера с СУБД `Jatoba`. После установки роли `JatobaStorage` выполнить команду: `docker ps -a`
В результате вывода команды должны содержаться данные обо всех установленных `docker`-контейнерах и их состоянии. Название `docker`-контейнера с СУБД `Jatoba` будет зависеть от названия роли (например: `storage-jatoba`). В колонке `STATUS` должно быть значение `UP` «количество времени», в течение которого `docker`-контейнер с СУБД `Jatoba` активен.

3.7.4 Установка роли **Management and Configuration**

Для установки роли вам потребуется архив `ManagementAndConfiguration_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив ManagementAndConfiguration_<Номер версии>.tar.gz:
tar -xf ManagementAndConfiguration_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли Management and Configuration и нажмите кнопку **OK**. Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
10. Убедитесь, что в качестве значения параметров HostAddress и PostgreHost указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. В качестве значения параметра DefaultLocale выберите язык веб-интерфейса приложения Management and Configuration.
12. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
13. Нажмите кнопку **OK**.

Роль установлена.

3.8 Установка компонента Knowledge Base на Linux-like

Компонент Knowledge Base устанавливается с помощью роли Knowledge Base. Для установки роли вам потребуется архив KB_<Номер версии>.tar.gz из комплекта поставки.

- ❖ Чтобы установить роль:
 1. На сервере Ankey SIEM NG Core распакуйте архив KB_<Номер версии>.tar.gz:
tar -xf KB_<Номер версии>.tar.gz
 2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
 3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
 4. Выберите вариант **Create New Application**.
 5. В открывшемся окне введите идентификатор приложения Knowledge Base и нажмите кнопку **OK**.
 6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли Knowledge Base и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. В качестве значения параметра **DefaultLocale** выберите желаемый язык интерфейса приложения Knowledge Base.

Внимание! Укажите значения параметров:

SiemAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
MCAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334
CoreAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:443

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение **Deployment configuration successfully applied**.
13. Нажмите кнопку **OK**.
Роль установлена.

3.9 Установка компонента Ankey SIEM NG Core на Linux-like

Компонент Ankey SIEM NG Core устанавливается с помощью ролей RMQ Message Bus и Core в следующем порядке: сначала устанавливается роль RMQ Message Bus, затем роль Core.

Внимание! Для установки компонента Ankey SIEM NG Core необходимо, чтобы TCP-порт 80 был свободен. Если этот порт занят каким-либо веб-сервером, выключите этот веб-сервер, удалите его или перенесите на другой порт.

3.9.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core

Для установки роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**. Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **ОК**.

Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

13. Нажмите кнопку **ОК**.

Роль установлена.

3.9.2 Установка роли Core

Для установки роли вам потребуется архив `Core_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `Core_<Номер версии>.tar.gz`:
`tar -xf Core_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли Core и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
10. В качестве значения параметра `DefaultLocale` выберите желаемый язык интерфейса приложения Ankey SIEM NG.

Внимание! Укажите корректные значения основных параметров:

HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
MCAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334
KBAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
SiemFrontendAddress: http://<FQDN или IPv4-адрес сервера Ankey SIEM NG Server>:8013>

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Если требуется настройка отправки уведомлений из компонента Ankey SIEM NG Core по электронной почте, то выберите вариант **Advanced configuration**.
Откроется страница со списком основных и дополнительных параметров для настройки роли Core.
12. В качестве значения параметра **DefaultLocale** выберите желаемый язык веб-интерфейса приложения Ankey SIEM NG.
13. Укажите значения дополнительных параметров для настройки отправки уведомлений из компонента Ankey SIEM NG Core по электронной почте на почтовый сервер:
 - EmailNotificationRetryPeriodSeconds: <указать значение в секундах, по умолчанию 60>;
 - Smtphost: <IP-адрес или FQDN SMTP-сервера, по умолчанию localhost>;
 - Smtppassword: <Пароль служебной учетной записи для подключения Ankey SIEM NG CORE к SMTP-серверу>;
 - Smtpport: <Порт SMTP-сервера для входящих подключений от Ankey SIEM NG CORE, по умолчанию 25>;
 - Smtpsender: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте от компонента Ankey SIEM NG Core, по умолчанию Notification System<NoReply@SiemNotifications.com>>;
 - Smtpssestablished: <Для подключения к SMTP-серверу службы Ankey SIEM NG CORE используют защищенное (True) или незащищенное (False) соединение, по умолчанию False>;
 - Smtpluser: <Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу. Служебная учетная запись для Core должна быть создана и настроена на почтовом сервере заранее, до установки роли Core >;
 - Smtplusedefaultcredentials: <Режим аутентификации SMTP-сервера:
True - для аутентификации используются логин и пароль

служебной учетной записи Network Service (необходимо очистить значения параметров SmtпUser и SmtпPassword); False - для аутентификации используются логин и пароль, указанные в параметрах SmtпUser и SmtпPassword, по умолчанию True».

14. Нажмите кнопку **ОК**.

Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.

15. Нажмите кнопку **ОК**.

Роль установлена.

3.10 Установка компонента Ankey SIEM NG Events Storage на Linux-like

Компонент Ankey SIEM NG ES устанавливается с помощью одной из ролей – с хранилищем событий Elasticsearch или с хранилищем событий LogSpace¹⁵.

Внимание! Хранилище событий LogSpace имеет ряд следующие ограничений функциональных возможностей:

- нет горячих и холодных индексов для хранения событий ИБ;
- нет поддержки работы ПК Ankey SIEM NG с несколькими конвейерами, связанными с одним ядром (компонентом Ankey SIEM NG Core);
- нет поддержки распределенного поиска событий ИБ между площадками, которые объединены в одну иерархию.

Перед установкой роли необходимо установить модуль Salt Minion на сервер Ankey SIEM NG ES в конфигурациях для высоконагруженных и сверхнагруженных систем, а также если Ankey SIEM NG Core установлен на Linux-like – в конфигурации для средненагруженных систем. В конфигурации для низконагруженных систем установка модуля Salt Minion на сервер Ankey SIEM NG ES не требуется.

Для хранения событий доступны два типа хранилищ – Elasticsearch и LogSpace. Выбранное хранилище будет установлено при установке соответствующей роли.

3.10.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Events Storage

❖ Чтобы установить модуль Salt Minion:

1. Если на сервере Ankey SIEM NG ES есть файл /etc/salt/pki/minion/minion_master.pub, удалите его:
rm /etc/salt/pki/minion/minion_master.pub

¹⁵ Дистрибутив роли LogSpace является опциональным хранилищем ПК Ankey SIEM NG и предоставляется по запросу к производителю с учетом принятия действующих ограничений по функциональным возможностям. Полная функциональность доступна в хранилище событий Elasticsearch.

2. Если Ankey SIEM NG ES устанавливается на Astra Linux, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
3. Если Ankey SIEM NG ES устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
4. На сервере с установленной ролью `Deployer` запустите сценарий:
`/var/lib/deploer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
5. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG ES и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

6. В открывшемся окне введите логин учетной записи с правами суперпользователя¹⁶ на сервере Ankey SIEM NG ES и нажмите кнопку **ОК**.
7. В открывшемся окне **Info** нажмите кнопку **ОК**.
8. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG ES.
Запустится установка модуля Salt Minion.
9. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.10.2 Установка роли SIEM Storage с хранилищем событий Elasticsearch

Для установки роли вам потребуется архив `EventsStorage_elasticsearch_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `EventsStorage_elasticsearch_<Номер версии>.tar.gz`:
`tar -xf EventsStorage_elasticsearch_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.

¹⁶ В ОС Astra Linux не предусмотрена работа под учетной записью суперпользователя `root`. Для выполнения установки компонентов ПК Ankey SIEM NG необходимо переключаться в учетную запись суперпользователя из текущей учетной записи (например, `administrator`). Для переключения в учетную запись суперпользователя `root` возможно использовать команду `sudo -s`.

Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.

4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG ES.
9. В открывшемся окне введите название экземпляра роли SIEM Storage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите набор параметров:
 - если Ankey SIEM NG развертывается в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**¹⁷;
 - если Ankey SIEM NG развертывается в конфигурации для низконагруженных, высоконагруженных или сверхнагруженных систем, выберите вариант **Advanced configuration**.Откроется страница с перечнем параметров конфигурации.
11. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG ES.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Укажите значение параметра **ClusterConfigurationProfile**:
 - если Ankey SIEM NG развертывается в конфигурации для низконагруженных систем, выберите вариант **AIO**;

¹⁷ Можно выбрать **Advanced configuration** для развертывания средненагруженных систем, потому что данный вариант предоставляет возможность гибкой настройки под любые условия.

- если для средненагруженных систем – выберите вариант **SIEMandStorage**;
 - если для высоконагруженных – вариант **Standalone**¹⁸;
 - если для сверхнагруженных – вариант **ManagedStorage**.
13. Укажите каталоги для хранения данных Ankey SIEM NG ES:
- если Ankey SIEM NG развертывается в конфигурации для низконагруженных, средненагруженных или высоконагруженных систем, измените значения параметров:
PathData: <Каталог для хранения индексов>
PathRepo: <Каталог для хранения резервных копий индексов>
PathLog: <Каталог для хранения файлов журналов>
 - если Ankey SIEM NG развертывается в конфигурации для сверхнагруженных систем, измените значения параметров:
PathData: <Каталог для хранения индексов, находящихся в "теплой" стадии, а также для хранения счетчиков всех индексов>
PathDataHot: <Каталог для хранения индексов, находящихся в "горячей" стадии>
PathRepo: <Каталог для хранения резервных копий индексов>
PathLog: <Каталог для хранения файлов журналов>

Примечание. Подробное описание жизненного цикла индексов приведено на сайте elastic.co.

14. Если Ankey SIEM NG развертывается в конфигурации для высоконагруженных или сверхнагруженных систем и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, установите флажок **HighLoad**.

Примечание. В случае установки флажка **HighLoad** кластер Elasticsearch будет содержать четыре узла данных.

15. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

16. Нажмите кнопку **ОК**.

Роль установлена.

3.10.3 Установка роли SIEM Storage с хранилищем событий LogSpace

Для установки роли вам потребуется архив `EventsStorage_LogSpace_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `EventsStorage_LogSpace_<Номер версии>.tar.gz`:
`tar -xf EventsStorage_LogSpace_<Номер версии>.tar.gz`

¹⁸ Для более тонко настроить ресурсы можно выбирать **Manual**.

2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG ES.
9. В открывшемся окне введите название экземпляра роли SIEM Storage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница с перечнем параметров конфигурации.
11. В качестве значения параметра `PathData` укажите каталог для установки хранилища событий LogSpace.
12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.
14. На сервере с установленным хранилищем событий LogSpace откройте TCP-порты 8123 и 9000 для входящих соединений.
Роль установлена.

3.11 Установка компонента Ankey SIEM NG Server на Linux-like

Установка компонента Ankey SIEM NG Server делится на следующие этапы:

1. Если Ankey SIEM NG Core установлен на Linux-like в конфигурации для высоконагруженных или сверхнагруженных систем – установка модуля Salt Minion.

Примечание. В конфигурации для средненагруженных систем модуль Salt Minion устанавливается (см. пункт 3.11.1) на сервер Ankey SIEM NG Server при установке компонента Ankey SIEM NG ES.

2. Если Ankey SIEM NG Server устанавливается в конфигурации для средненагруженных, высоконагруженных или сверхнагруженных систем – установка роли RMQ Message Bus.
3. Если выполняется установка Ankey SIEM NG Server в конфигурации для низконагруженных систем, то устанавливается только роль SIEM Server. Второй экземпляр роли RMQ Message Bus не требуется устанавливать.

3.11.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Server

- ❖ Чтобы установить модуль Salt Minion:
 1. Если на сервере Ankey SIEM NG Server есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
 2. Если Ankey SIEM NG Server устанавливается на Astra Linux, на сервере Ankey SIEM NG Server отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
 3. Если Ankey SIEM NG Server устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
 4. На сервере с установленной ролью Deployer запустите сценарий установки:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
 5. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

6. В открывшемся окне введите логин учетной записи с правами суперпользователя¹⁹ на сервере Ankey SIEM NG Server и нажмите кнопку **ОК**.
7. В открывшемся окне **Info** нажмите кнопку **ОК**.

¹⁹ В ОС Astra Linux не предусмотрена работа под учетной записью суперпользователя `root`. Для выполнения установки компонентов ПК Ankey SIEM NG необходимо переключаться в учетную запись суперпользователя из текущей учетной записи (например, `administrator`). Для переключения в учетную запись суперпользователя `root` возможно использовать команду `sudo -s`.

8. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Server.
Запустится установка модуля Salt Minion.
9. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.11.2 Установка роли **RMQ Message Bus** на сервер **Ankey SIEM NG Server**

Для установки роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения `Ankey SIEM NG`.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с FQDN или IPv4-адрес сервера `Ankey SIEM NG Server`.
8. В открывшемся окне введите название экземпляра роли `RMQ Message Bus` и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите набор параметров:
 - если `Ankey SIEM NG` развертывается в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
 - если `Ankey SIEM NG` развертывается в конфигурации для высоконагруженных или сверхнагруженных систем, выберите вариант **Advanced configuration**.
Откроется страница с перечнем основных параметров (если был выбран вариант **Basic configuration**) или всех доступных параметров конфигурации (если был выбран вариант **Advanced configuration**).

10. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

12. Нажмите кнопку **ОК**.

Роль установлена.

3.11.3 Установка роли SIEM Server

Для установки роли вам потребуется архив `SiemServer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `SiemServer_<Номер версии>.tar.gz`:

```
tar -xf SiemServer_<Номер версии>.tar.gz
```
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Server.
8. В открывшемся окне введите название экземпляра роли SIEM Server и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение Б).

Внимание! Укажите значения параметров:

`CoreAddress`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
`HostAddress`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
`RMQHost`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

10. Укажите значение параметра **StorageBackendType**:
 - если для хранения событий используется Elasticsearch, выберите вариант **elasticsearch**;
 - если используется LogSpace – выберите вариант **logspace**.
11. Если Ankey SIEM NG развертывается в конфигурации для высоконагруженных или сверхнагруженных систем, измените значение параметра ElasticsearchHost:
ElasticsearchHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>
12. Если Ankey SIEM NG развертывается в конфигурации для сверхнагруженных систем, укажите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG ES:
 - если для хранения событий используется Elasticsearch, измените значение параметра ElasticsearchHost:
ElasticsearchHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>;
 - если для хранения событий используется LogSpace, измените значение параметра LogSpaceHost:
LogSpaceHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>.
13. Если Ankey SIEM NG развертывается в конфигурации для сверхнагруженных систем, установите флажок **ManagedStorage**.
14. Если предполагаемый поток событий от источников будет превышать 20 000 событий в секунду и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, установите флажок **HighLoad**.

Примечание. В случае установки флажка **HighLoad** для службы SIEM server storage будет выделено шесть потоков операционной системы (вместо четырех, когда флажок снят).

15. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
16. Нажмите кнопку **ОК**.
Роль установлена.

3.12 Установка компонента Ankey SIEM NG Agent

В этом подразделе приведены инструкции по установке компонента Ankey SIEM NG Agent на Linux-like и на Windows Server.

Внимание! Если Ankey SIEM NG Agent установлен на Linux-like, Ankey SIEM NG не сможет проводить аудит активов с Windows Server и собирать любые данные в режиме пентеста.

Установка компонента на Linux-like выполняется с помощью роли Agent. Если Ankey SIEM NG Agent устанавливается на отдельный сервер, перед установкой роли необходимо установить на этот сервер модуль Salt Minion.

3.12.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Agent

- ❖ Чтобы установить модуль Salt Minion:
 1. Если на сервере Ankey SIEM NG Agent есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
 2. Если Ankey SIEM NG Agent устанавливается на Astra Linux, на сервере Ankey SIEM NG Agent отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
 3. Если Ankey SIEM NG Agent устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
 4. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
 5. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Agent и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

6. В открывшемся окне введите логин учетной записи с правами суперпользователя²⁰ на сервере Ankey SIEM NG Agent и нажмите кнопку **ОК**.
7. В открывшемся окне **Info** нажмите кнопку **ОК**.
8. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Agent.
9. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.12.2 Установка роли Agent

Для установки роли вам потребуется архив `AgentLinux_<Номер`

²⁰ В ОС Astra Linux не предусмотрена работа под учетной записью суперпользователя `root`. Для выполнения установки компонентов ПК Ankey SIEM NG необходимо переключаться в учетную запись суперпользователя из текущей учетной записи (например, `administrator`). Для переключения в учетную запись суперпользователя `root` возможно использовать команду `sudo -s`.

версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив AgentLinux_<Номер версии>.tar.gz:
tar -xf AgentLinux_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Agent.
9. В открывшемся окне введите название экземпляра роли Agent и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров.
11. В качестве значения параметра AgentName введите название агента, которое будет отображаться в веб-интерфейсе приложения **Ankey SIEM NG**.
12. Убедитесь, что в качестве значения параметра AgentRMQHost указано полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии Ankey SIEM NG Server – в зависимости от того, для какой версии компонента предназначен Ankey SIEM NG Agent.

Внимание! Если в параметре AgentRMQHost указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

13. В качестве значения параметра AgentRMQVirtualHost выберите **SIEM**.

14. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
15. Нажмите кнопку **ОК**.
Роль установлена.

Примечание. Для корректной работы Ankey SIEM NG Agent в ОС Linux-like требуется отдельно скачать и установить ODBC-драйвер (версия для 64-разрядной архитектуры) для требуемых источников, которые будут подключаться к ПК Ankey SIEM NG. Драйвер вы можете скачать с официальных сайтов производителей источников.

3.12.3 Установка компонента Ankey SIEM NG Agent на Windows Server

Для установки компонента Ankey SIEM NG Agent на Windows Server вам потребуется файл `AnkeyAgentSetup_<Номер версии>.exe` из комплекта поставки.

Если мастер установки предложит перезагрузить операционную систему, вам необходимо подтвердить перезагрузку. После перезагрузки установка будет продолжена автоматически.

- ❖ Чтобы установить компонент Ankey SIEM NG Agent:
 1. Запустите файл `AnkeyAgentSetup_<Номер версии>.exe`.
Откроется окно мастера установки.
 2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
 3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
 4. Укажите пути для установки.

Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.

5. Нажмите кнопку **Продолжить**.
6. В поле **Имя агента** введите имя агента, которое будет отображаться в интерфейсе Ankey SIEM NG.
7. В блоке параметров **Адрес обработчика данных** в раскрывающемся списке выберите значение **SIEM** и укажите в поле полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии Ankey SIEM NG Server – в зависимости от того, для какой версии компонента предназначен Ankey SIEM NG Agent.

Внимание! Если в поле указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

8. Нажмите кнопку **Продолжить**.
Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. Вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.

9. Нажмите кнопку **Установить**.
10. По завершении установки нажмите кнопку **Заккрыть**.
11. Если устанавливается первый компонент Ankey SIEM NG Agent и компонент Ankey SIEM NG Server установлен на Linux-like, на сервере с установленной ролью Deployer выполните команды:
 1. `cp /opt/deployer/pki/legacy_ca/windows-selfsigned-default.pem /opt/deployer/pki/trusted_ca/`
 2. `dpkg-reconfigure deployer`
 3. `/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId RmqMessageBus`

Компонент Ankey SIEM NG Agent установлен.

3.13 Установка облегченной версии компонента Ankey SIEM NG Server на Linux-like

Перед установкой облегченной версии Ankey SIEM NG Server необходимо установить компонент Ankey SIEM NG Agent. Также необходимо убедиться, что в качестве значения параметра `AgentRMQHost` компонента Ankey SIEM NG Agent указан FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server, а параметру `AgentRMQVirtualHost` присвоено значение `siem`.

Внимание! Не предусмотрено развертывание облегченной версии Ankey SIEM NG Server на том же сервере, где установлен компонент Ankey SIEM NG Core.

Установка облегченной версии компонента Ankey SIEM NG Server делится на следующие этапы:

1. Установка модуля Salt Minion.
2. Установка роли RMQ Message Bus.
3. Установка роли SIEM Server.

3.13.1 Установка модуля Salt Minion на сервер облегченной версии Ankey SIEM NG Server

- ❖ Чтобы установить модуль Salt Minion:
 1. Если на сервере облегченной версии Ankey SIEM NG Server есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
 2. Если облегченная версия Ankey SIEM NG Server устанавливается на сервер на Astra Linux, отключите на этом сервере обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
 3. Если облегченная версия Ankey SIEM NG Server устанавливается на Debian, на сервере компонента отключите обязательный ввод

пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:

```
<Логин учетной записи, от имени которой устанавливается компонент>  
ALL=(ALL:ALL) NOPASSWD: ALL
```

4. На сервере с установленной ролью `Deployer` запустите сценарий:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
5. В открывшемся окне введите FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

6. В открывшемся окне введите логин учетной записи с правами суперпользователя²¹ (`root`) на сервере облегченной версии Ankey SIEM NG Server и нажмите кнопку **ОК**.
7. В окне **Info** нажмите кнопку **ОК**.
8. Введите пароль учетной записи с правами суперпользователя (`root`) на сервере облегченной версии Ankey SIEM NG Server. Запустится установка модуля Salt Minion.
9. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.13.2 Установка роли RMQ Message Bus на сервер облегченной версии Ankey SIEM NG Server

Для установки роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.

²¹ В ОС Astra Linux не предусмотрена работа под учетной записью суперпользователя `root`. Для выполнения установки компонентов ПК Ankey SIEM NG необходимо переключаться в учетную запись суперпользователя из текущей учетной записи (например, `administrator`). Для переключения в учетную запись суперпользователя `root` возможно использовать команду `sudo -s`.

5. В окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне выберите вариант с доменным именем сервера облегченной версии Ankey SIEM NG Server.
7. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
9. Укажите в качестве значения параметра `HostAddress` **FQDN** или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать **FQDN** или IPv4-адрес сервера.

10. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.

Роль установлена.

3.13.3 Установка роли SIEM Server для облегченной версии компонента

Для установки роли вам потребуется архив `SiemServer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `SiemServer_<Номер версии>.tar.gz`:
`tar -xf SiemServer_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Server.
7. В открывшемся окне введите название экземпляра роли SIEM Server и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
8. Выберите набор параметров **Advanced configuration**.

Откроется страница с перечнем всех доступных параметров конфигурации.

Внимание! Укажите значения параметров:

HostAddress: <FQDN или IPv4-адрес сервера облегченной версии компонента Ankey SIEM NG Server>

TargetSiemRabbitHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server, который будет получать данные о событиях от облегченной версии компонента>

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

9. Установите флажок **SiemOnAgent**.
10. Если Ankey SIEM NG развертывается в конфигурации для сверхнагруженных систем, установите флажок **ManagedStorage**.
11. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
12. Нажмите кнопку **ОК**.

Роль установлена.

3.14 Установка облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows

Перед установкой облегченной версии компонента Ankey SIEM NG Server необходимо установить на том же сервере компонент Ankey SIEM NG Agent.

Внимание! Не предусмотрено развертывание облегченной версии Ankey SIEM NG Server на том же сервере, где установлен компонент Ankey SIEM NG Core.

- ❖ Чтобы установить облегченную версию Ankey SIEM NG Server:
 1. Запустите файл `AnkeySiemSetup_<Номер версии>.exe`.
Откроется окно мастера установки.
 2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
 3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
 4. Выберите вариант установки облегченной версии Ankey SIEM NG Server и нажмите кнопку **Продолжить**.
 5. Укажите пути для установки.

Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.

6. Нажмите кнопку **Продолжить**.
Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. В этом случае вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.

7. Нажмите кнопку **Установить**.
8. По завершении установки нажмите кнопку **Заккрыть**.
9. В адресной строке браузера введите: `http://<FQDN> или IPv4-адрес облегченной версии SIEM Server>:15672/#/dynamic-shovels`
Откроется страница входа в RabbitMQ.
10. Введите логин `siem` и пароль.

Примечание. По умолчанию пароль служебной учетной записи – `P@ssword`.

11. Нажмите кнопку **Login**.
Откроется вкладка **Admin** с таблицей **Dynamic Shovels**.
12. В таблице **Dynamic Shovels** в столбце **Name** нажмите ссылку.
13. В открывшемся окне нажмите кнопку **Delete this shovel**.
14. Повторите шаги 12–13 для всех строк таблицы **Dynamic Shovels**.
15. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файл `/opt/deployer/pki/CABundle.crt` с сервера, на котором установлена роль `Deployer`, на сервер облегченной версии Ankey SIEM NG Server.
16. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файлы `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.crt` и `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.key` с сервера стандартной версии Ankey SIEM NG Server на сервер облегченной версии Ankey SIEM NG Server.

На сервере облегченной версии Ankey SIEM NG Server в интерфейсе командной строки Windows от имени администратора выполните команды:

```
coreagentcfg set -p AgentRMQVirtualHost siem RMQHost localhost
rabbitmqcfg set -p CACertFile <Путь к файлу CABundle.crt> -v
siemcfg set -p TargetSiemRabbitHost <FQDN или IPv4-адрес стандартной версии Ankey SIEM NG Server> RMQHost <FQDN или IPv4-адрес стандартной версии Ankey SIEM NG Server> RMQ_SSL_CA_CERTIFICATE <Путь к файлу CABundle.crt> RMQ_SSL_CERTIFICATE <Путь к файлу RMQ_SIEM_Client.crt> RMQ_SSL_KEY <Путь к файлу RMQ_SIEM_Client.key>
```


Облегченная версия компонента Ankey SIEM NG Server установлена.

После установки облегченной версии компонента Ankey SIEM NG Server необходимо установить правила нормализации и агрегации (см. раздел 3.15).


3.15 Установка правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server

Перед установкой правил необходимо убедиться, что в Ankey SIEM NG установлена стандартная база данных (см. подраздел 3.18).


❖ Чтобы установить правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Knowledge Base**.
Откроется страница **Статистика**.

Примечание. Если вы используете браузер Mozilla Firefox и на странице **Статистика** отображается сообщение "Отключен", необходимо проверить, что адреса `https://<FQDN>` или IPv4-адрес компонента `Ankey SIEM NG Core>:8091` добавлены в исключения безопасности браузера.

2. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.
Откроется страница **Базы данных / <Название БД>**.
3. В панели **Базы данных** выберите родительскую базу данных, которая содержит устанавливаемые правила.
4. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
5. В панели **Папки** выберите **Все объекты**.
6. В панели **Наборы для установки** выберите **Все объекты**.
7. В панели со списком объектов нажмите .
Появится строка с названиями фильтров.
8. По ссылке **Объекты: все** установите флажки **Агрегация** и **Нормализация**.
9. Повторно нажмите на ссылку.
10. В списке правил выберите те правила, которые требуется установить для облегченной версии Ankey SIEM NG Server.

Примечание. Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов – клавишу Ctrl, для выбора всех объектов в списке – комбинацию клавиш Ctrl+A.

11. Нажмите .
12. Выберите вариант **Для установки в SIEM Lite**.
13. Нажмите кнопку **Экспортировать**.
Браузер сохранит архив `knowledgebase_<Дата экспорта>.zip` в папку загрузки.
14. Переместите файл архива на сервер облегченной версии Ankey SIEM NG Server в любую папку.

15. Если облегченная версия Ankey SIEM NG Server установлена на Windows Server , запустите установку правил нормализации и агрегации:
"C:\Program Files\Gazinformservice\Ankey SIEM NG Server\siemlight-kb" -u
<Путь к файлу архива>
16. Если облегченная версия Ankey SIEM NG Server установлена на Linux-like, запустите установку правил нормализации и агрегации:
"/opt/siem/bin/siemlight-kb" -u <Путь к файлу архива>

Правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server установлены.

3.16 Активация лицензии Ankey SIEM NG

Для активации лицензии вам потребуются следующие файлы из комплекта поставки:

- шаблон ключа <Номер лицензии>.grdvd;
- текстовый файл с серийным номером Ankey SIEM NG <Идентификатор ключа>.txt;
- мастер активации лицензий GuardantActivationWizard.exe.

Активация лицензии выполняется на сервере компонента Ankey SIEM NG Core.

Если активировать несколько лицензий, система будет использовать только одну из них – имеющую самую раннюю дату окончания. Поэтому в случае приобретения продукта, который может быть развернут на базе уже установленного Ankey SIEM NG необходимо активировать объединенную лицензию на оба продукта (ее можно запросить в службе технической поддержки ООО «Газинформсервис»). В противном случае после активации отдельной лицензии на второй продукт в системе будет доступен набор функций только одного продукта.

После изменения аппаратной конфигурации сервера Ankey SIEM NG Core (например, по причине замены центрального процессора) необходимо повторно активировать лицензию. Количество таких повторных активаций ограничено – не более пяти раз. Дальнейшие попытки активации приведут к ошибке мастера активации «Количество активаций для введенного серийного номера исчерпано». Для получения нового шаблона ключа и нового серийного номера необходимо обратиться в службу технической поддержки (см. раздел 7).

Если вы повторно активировали лицензию (например, после переустановки ОС или компонента Ankey SIEM NG Core) и при этом не изменяли аппаратную конфигурацию сервера, счетчик активаций не уменьшается (количество таких повторных активаций не ограничено).

Информация о лицензии доступна на странице **Система → Управление системой**.

3.16.1 Активация лицензии на Linux-like при наличии доступа к интернету

❖ Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing скопируйте шаблон ключа <Номер

лицензии>.grdvd и текстовый файл с серийным номером <Идентификатор ключа>.txt.

2. **Запустите активацию лицензии от имени суперпользователя (root):**

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор  
ключа>.txt
```

По завершении активации появится сообщение License activation Succeeded.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов Ankey SIEM NG Core и Knowledge Base с помощью команды `docker restart $(docker ps | awk '/ core-|kb-/ {print $NF}')`, а затем выйти из системы и заново войти.

Кроме того, если Ankey SIEM NG развертывается в средненагруженной, высоконагруженной или сверхнагруженной конфигурации, после активации лицензии необходимо перезапустить службу Core Events Aggregator на сервере Ankey SIEM NG Server с помощью команды `docker restart $(docker ps | awk '/core-events-aggregator/ {print $NF}')`.

3.16.2 Активация лицензии на Linux-like при отсутствии доступа к интернету

Для активации лицензии вам потребуется рабочая станция с доступом в интернет и файл `GuardantActivationWizard.exe` из комплекта поставки.

❖ Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.

2. Выполните команду от имени суперпользователя (root):

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор  
ключа>.txt /offline
```

Мастер активации лицензий создаст в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` файл `<Номер лицензии>.grdvd.toserver`.

3. На рабочей станции с доступом в интернет разместите в одной папке файлы `GuardantActivationWizard.exe` и `<Номер лицензии>.grdvd.toserver`.
4. Запустите файл `GuardantActivationWizard.exe`.
Откроется окно мастера активации лицензий.
5. Нажмите кнопку **Указать файл лицензии**.
6. В открывшемся окне выберите файл `<Номер лицензии>.grdvd.toserver` и нажмите кнопку **Открыть**.
7. Нажмите кнопку **Далее**.

- Мастер активации лицензий создаст файл <Номер лицензии>.grdvd.fromserver. Папка с файлом откроется автоматически.
8. Нажмите кнопку **Готово**.
 9. Скопируйте файл <Номер лицензии>.grdvd.fromserver на сервер Ankey SIEM NG Core в каталог /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing.
 10. Выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd.fromserver
```

По завершении активации появится сообщение License activation Succeeded.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов Ankey SIEM NG Core и Knowledge Base с помощью команды `docker restart $(docker ps | awk '/ core-|kb-/ {print $NF}')`, а затем выйти из системы и заново войти.

Кроме того, если Ankey SIEM NG развертывается в средненагруженной, высоконагруженной или сверхнагруженной конфигурации, после активации лицензии необходимо перезапустить службу Core Events Aggregator на сервере Ankey SIEM NG Server с помощью команды `docker restart $(docker ps | awk '/core-events-aggregator/ {print $NF}')`.

3.17 Удаление лицензионного ключа

❖ Чтобы удалить ключ на Linux-like, выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /delete=<Идентификатор ключа>
```

Ключ удален.

3.18 Установка стандартной базы данных в ОС Astra Linux и Debian

Для работы с контентом в веб-интерфейсе ПК Ankey SIEM NG 4.1.2 необходимо:

- создать корневую базу данных **GIS_DB**;
- установить в корневую базу данных пакет только с актуальной²² таксономией **Taxonomy_4.x.x.kb**;
- установить в корневую базу данных пакет стандартных коннекторов, который содержится в архиве **<название пакета с коннекторами><версия пакета>.kb**, например **GIS_KB_ConnectorsStd_A.B.C.kb**;

²² Необходимо поставить версию пакета с таксономией согласно мажорной версии релиза. Например, для релиза ПК Ankey SIEM NG 3.x.x необходимо поставить соответствующую версию пакета с таксономией 3.x.x.

- установить в корневую базу данных пакет стандартного контента, который содержится в архиве **<название пакета контента><версия пакета>.kb**, например **GIS_KB_ContentStd_A.B.C.kb**;

Внимание! Необходимо сначала установить пакет стандартных коннекторов, а после пакет стандартного контента. Установка пакетов по отдельности или в другом порядке не рекомендуется, т.к. пакет стандартных коннекторов является основой для работы стандартного пакета контента.

Примечание. Создание и удаление корневой базы данных в Knowledge Base выполняется с помощью утилиты **kbtools**, которая устанавливается вместе с компонентом Ankey SIEM NG Core.

- создать ветку корневой базы данных **GIS_DB**. Например, **Customer_Data**. Дождаться завершения процесса создания ветки **Customer_Data**.
- ❖ Чтобы установить системную базу знаний требуется:





1. Создание корневой базы данных **GIS_DB**. Следует запустить от имени администратора интерфейс командной строки операционной системы Linux-like и выполнить команду:

```
/var/lib/deployed-roles/<Название приложения Knowledge Base>/<Название экземпляра роли приложения Knowledge Base, например kb-83dspxbudksxc1mdooung>/tools/kbtools/kbtools createRootdb --db GIS_DB --db_name "GIS_DB" --kbHost <FQDN или IPv4 адрес сервера с компонентом Core> --iamHost <FQDN или IPv4-адрес сервера с компонентом Core> --login <Логин учетной записи с правами администратора> --password <Пароль от учетной записи с правами администратора>
```

Корневая база данных **GIS_DB** предназначена для хранения коннекторов и контента в исходном состоянии. Контент в базе данных следует устанавливать/обновлять²³ в полуавтоматическом режиме, используя функционал веб-интерфейса управления ПК Ankey SIEM NG.

Примечание. Для того чтобы была возможность импортировать контент в базы данных ПК с помощью функционала веб-интерфейса необходимо установить корректную таксономию полей с помощью утилиты **kbtools**. Функционал веб-интерфейса не позволяет импортировать **схему полей событий**. После импорта **схемы полей событий** в новую базу данных возможно использовать функционал веб-интерфейса для импорта пакетов коннекторов и контента.

²³ Алгоритм обновления ресурсов в базах данных представлен в документе «Руководство администратора Ankey SIEM NG 4.1.2».

2. Для импорта пакета с актуальной таксономией **Taxonomy_4.x.x.kb** в корневую базу данных **GIS_DB** следует запустить интерфейс командной строки операционной системы Linux-like, переключиться на учетную запись суперпользователя (**root**) и выполнить команду:
`/var/lib/deployed-roles/<Название приложения Knowledge Base>/<название экземпляра роли приложения Knowledge Base, например kb-83dspxbudksxc1mdooulng>/tools/kbtools/kbtools importPackage --db GIS_DB --kbHost <FQDN или IPv4 сервера с компонентом Core> --iamHost <FQDN или IPv4-адрес сервера с компонентом Core> --login <Логин учетной записи с правами администратора> --password <Пароль от учетной записи с правами администратора> --source "/opt/<название пакета><версия пакета с таксономией>.kb" --mode Upsert --ImportTaxonomy`
3. Для импорта пакета стандартных коннекторов **GIS_KB_Connectors_Std_A.B.C.kb** можно воспользоваться функцией веб-интерфейса  **Импорт**:
 - в адресной строке браузера введите ссылку для входа в интерфейс ПК Ankey SIEM NG.
Откроется страница входа в сервис Ankey SIEM NG MC;
 - указать логин и пароль учетной записи и нажать **Войти**;
 - в веб-интерфейсе Ankey SIEM NG откройте выпадающий список компонентов, нажав на графический элемент 
 - в раскрывшемся меню выберите пункт **Knowledge Base**.
Откроется веб-страница **Knowledge Base**.
 - в веб-интерфейсе Ankey SIEM NG откройте выпадающий список компонентов, нажав на графический элемент 
 - в раскрывшемся меню выберите пункт Knowledge Base.
Откроется веб-страница Knowledge Base.
 - в главном меню выберите пункт с корневой базой данных **GIS_DB**;
 - в главном меню в разделе SIEM выберите пункт **Пакеты экспертизы**.
Откроется страница **Пакеты экспертизы**;
 - в верхнем правом углу вкладки **Пакеты экспертизы** на панели инструментов выберите  **Импорт**;
 - в открывшемся диалоговом окне нажмите ссылку выберите, где будет предложено указать файл для загрузки, или переместите с помощью манипулятора типа **мышь** файл пакета стандартных коннекторов **GIS_KB_Connectors_Std_A.B.C.kb** в специальное окно. После этого появится окно **Импорт объектов**;
 - выполните импорт с параметрами, указанными на рисунке 3.10.

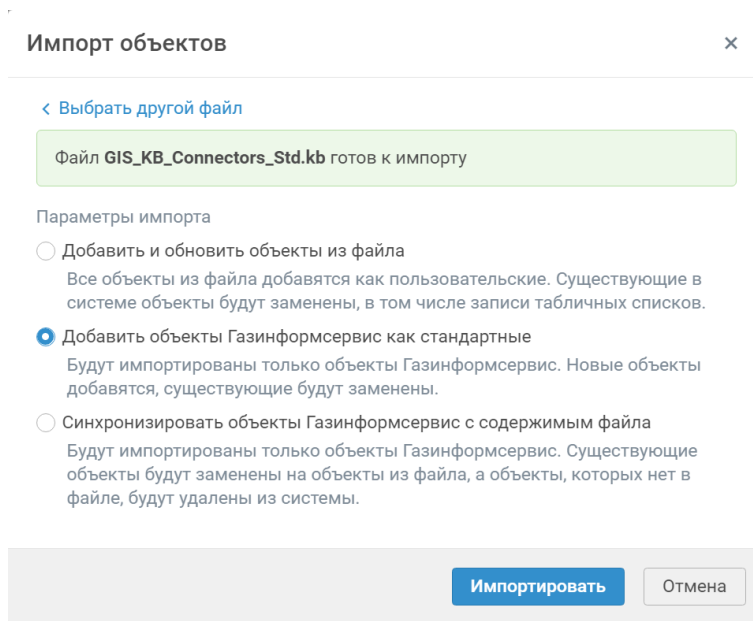





Рисунок 3.10 – Пример настройки параметров импорта коннекторов без возможности редактирования

- После импорта пакета стандартных коннекторов в базу данных **GIS_DB** они будут недоступны для редактирования.
4. Для импорта пакета стандартного контента **GIS_KB_ContentStd_A.B.C.kb** можно воспользоваться функцией веб-интерфейса  **Импорт**:
- в адресной строке браузера введите ссылку для входа в интерфейс ПК Ankey SIEM NG.
Откроется страница входа в сервис Ankey SIEM NG MC;
 - указать логин и пароль учетной записи и нажать **Войти**;
 - в веб-интерфейсе Ankey SIEM NG откройте выпадающий список компонентов, нажав на графический элемент ;
 - в раскрывшемся меню выберите пункт **Knowledge Base**.
Откроется веб-страница **Knowledge Base**.
 - в главном меню выберите пункт с корневой базой данных **GIS_DB**;
 - в главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
Откроется страница **Пакеты экспертизы**;
 - в верхнем правом углу вкладки **Пакеты экспертизы** на панели инструментов выберите  **Импорт**;
 - в открывшемся диалоговом окне нажмите ссылку **выберите**, где будет предложено указать файл для загрузки, или перетащите файл пакета стандартного контента **GIS_KB_ContentStd_A.B.C.kb** в диалоговое окно.
После этого появится окно **Импорт объектов**;
 - выполните импорт с параметрами, указанными на рисунке 3.11.

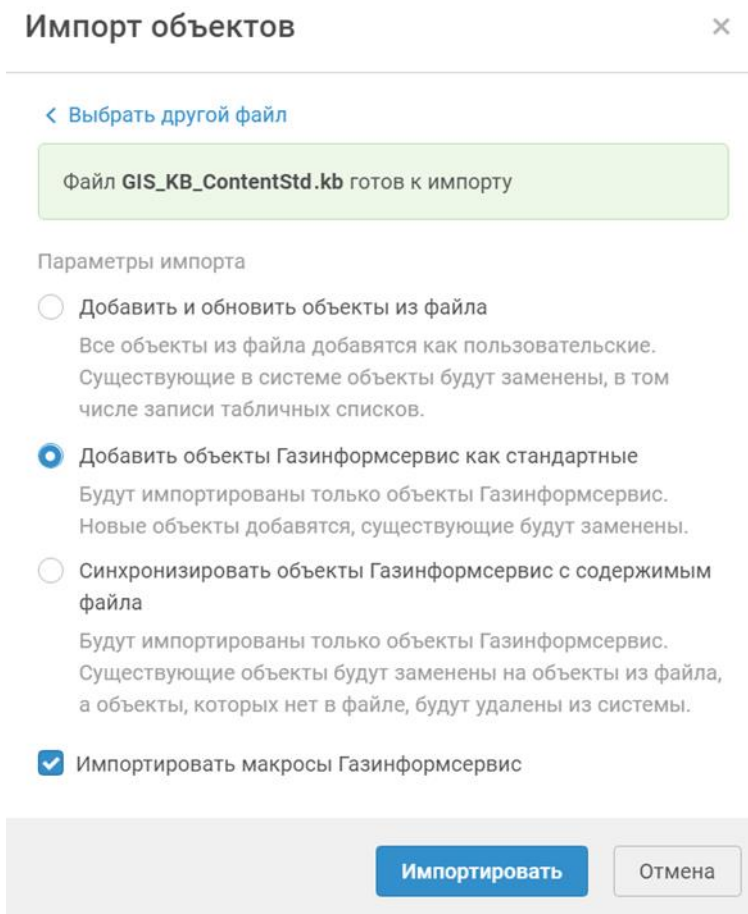


Рисунок 3.11 – Пример настройки параметров импорта контента без возможности редактирования и с добавлением макросов

Примечание. Все последующие пакеты рекомендуется импортировать через веб-интерфейс по аналогичному сценарию.

После импорта пакета стандартного контента в базу данных **GIS_DB** он будет недоступен для редактирования.

5. Далее необходимо создать ветку **Customer_Data** от корневой базы данных **GIS_DB**:
 - в приложении **Knowledge Base** в главном меню в разделе **<Название БД>** выберите пункт **Базы данных**. Откроется страница **Базы данных / <Название БД>**;
 - в панели **Базы данных** выберите корневую базу данных **GIS_DB**;

Внимание! Перед созданием ветки проверьте, что все необходимые наборы ресурсов (см. пункты 2 и 3) загружены в корневую базу данных.

- в панели инструментов нажмите кнопку **+ Создать ветку**;
- в открывшемся окне **Создание ветки** в поле **Имя** введите название **Customer_Data**;

- в поле **Идентификатор** введите идентификатор **Customer_Data**;
- в блоке параметров **Модификаторы доступа** настройте параметры:
 - **разрешить просмотр контента** – разрешение для пользователей на просмотр объектов в БД;
 - **разрешить редактирование контента** – разрешение на изменение объектов в БД;
 - **разрешить редактирование параметров базы данных** – разрешение на изменение параметров БД;
 - **разрешить слияние в базу данных** – разрешение на импорт объектов из родительской БД.

Внимание! Параметры **Разрешить слияние в базу данных** и **Разрешить редактирование параметров базы данных** необходимо оставить неотмеченными.

Пример настройки параметров в блоке **Модификаторы доступа** представлен на рисунке 3.12;

Рисунок 3.12 – Настройка параметров в блоке **Модификаторы доступа**

- нажмите кнопку **Сохранить**;
Начнется процесс создания ветки корневой базы данных.


Примечание. Процесс создания ветки занимает некоторое время в связи с копированием в нее ресурсов из родительской корневой базы данных.

После завершения создания ветка будет доступна для выбора;





- в главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.

Откроется страница **Пакеты экспертизы**, где будет видно, что набор ресурсов в ветке установочной базы данных полностью идентичен набору ресурсов в корневой базе данных **GIS_DB**.

Внимание! Ресурсы сохранили свои свойства и являются стандартными, т.е. недоступными к изменению. Работа с пользовательскими ресурсами описана в документе «Руководство оператора Ankey SIEM NG 4.1.2».

6. Ветку **Customer_Data** выбрать в качестве установочной. Для это следует в веб-интерфейсе перейти в **Knowledge Base**, открыть выпадающий список баз данных, нажав на графический элемент , и выбрать пункт **Базы данных**. В качестве текущей базы данных выбрать ветку **Customer_Data** и нажать на **Сделать установочной**.


Внимание! Базу данных **GIS_DB** нельзя использовать в качестве установочной, т.к. не гарантируются правильные дальнейшие обновления, а также сохранение пользовательских ресурсов.

7. Перед валидацией и установкой контента необходимо выполнить установку программных инструментов разработки контента (SDK) для валидации контента (SDK). Для этого следует в веб-интерфейсе открыть выпадающий список **SIEM**  и выбрать **Выбор версии SDK**. Далее следует выбрать SDK определенной версии, например, 25.x.xxxx, а затем нажать на  **Установить SDK для валидации** для установки.
8. После установки SDK следует открыть выпадающий список **SIEM**  и выбрать **Пакеты экспертизы**.
9. Выделить в веб-интерфейсе весь контент и выполнить валидацию, нажав на графическую кнопку . Валидация должна завершиться без ошибок.

❖ Чтобы корректно установить все необходимые ресурсы в компонент **Server** следует:

1. В главном меню в разделе **<Название базы данных>** выбрать **Customer_Data**.

Внимание! Ветка **Customer_Data** является установочной БД, ресурсы, расположенные в родительской **GIS_DB**, доступны только для валидации и не устанавливаются в компонент **Server**.

2. В главном меню в разделе **SIEM** выберите **Пакеты экспертизы**. Откроется страница **Пакеты экспертизы**.
3. В панели **Наборы для установки** нажать . Откроется окно **Создание набора для установки**.

4. В поле **Системное название** ввести название набора. Рекомендуется указать системное название на латинице.
5. В поле **Название (русский)** возможно внести любое значение, оно будет отображаться в веб-интерфейсе. Например, «Ресурсы для конвейера в администрации».
6. В поле **Входит в набор** выбрать **Все объекты** или любой другой корректно сформированный набор для установки.
7. В поле **Устанавливать в конвейер** выбрать один или несколько конвейеров, в который будут установлены ресурсы из набора установки. Выбрать конвейеры для установки возможно только в том случае, если корректно выполнена установка всех основных компонентов Ankey SIEM NG.

Примечание. Наборы установки для конвейеров следует формировать с учетом того, что при установке новых ресурсов из приложения **Knowledge Base** в компонент **Server** ресурсы, которые были установлены ранее, автоматически и принудительно удаляются, а новые устанавливаются. Т.е. набор установки для конвейеров должен содержать все необходимые правила нормализации, правила корреляции, правила обогащения, правила агрегации и табличные списки.

8. Нажмите кнопку **Создать**. Набор для установки создан.
9. В панели **Наборы для установки** выберите **Все объекты**.
10. В панели **Папки** выберите пакет экспертизы (или папку). Появится список объектов пакета экспертизы (папки).
11. Выберите объекты.
12. Нажмите на графическую кнопку . Откроется окно **Наборы для установки**.
13. Установите флажок напротив названия набора для установки, в который нужно добавить объекты.

Примечание. Место ресурса в иерархической структуре не поменяется, наборы для установки представляют собой группы, которые объединяют объекты по некоторому признаку.

14. Нажмите кнопку **Сохранить**. Объекты добавлены в набор для установки.
15. Из набора установки необходимо удалить все родительские ресурсы, с которых были созданы копии в ветке **Customer_Data** чтобы не было конфликтов в работе SIEM-системы после установки. Найти родительский ресурс, выделив скопированный, возможно, перейдя к нему по ссылке из описания скопированного ресурса.
16. Установить контент в компонент **Ankey SIEM NG Server**, нажав на графическую кнопку . Начнется установка контента.

Примечание. При наведении курсора на значок ► во всплывающей подсказке отображается статус установки.

17. После завершения установки в рабочей области появится сообщение **Установка успешно завершена**. Контент установлен из Knowledge Base в **Ankey SIEM NG Server**.

3.19 Установка дополнительного компонента Ankey SIEM NG RC

Внимание! Компонент Ankey SIEM NG RC необходимо устанавливать на отдельный сервер.

Установка компонента Ankey SIEM NG RC делится на следующие этапы:

1. Установка модуля Salt Minion.
2. Установка роли RMQ Message Bus.
3. Установка роли Retro Correlator.

3.19.1 Установка модуля Salt Minion на сервер Ankey SIEM NG RC

- ❖ Чтобы установить модуль Salt Minion:
 1. Если на сервере Ankey SIEM NG RC есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
 2. Если Ankey SIEM NG RC устанавливается на Astra Linux, на сервере Ankey SIEM NG RC отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
 3. Если Ankey SIEM NG RC устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
 4. На сервере с установленной ролью `Deployer` запустите сценарий:
`/var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh`
 5. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

6. В открывшемся окне введите логин учетной записи с правами суперпользователя²⁴ на сервере Ankey SIEM NG RC и нажмите кнопку **ОК**.

²⁴ В ОС Astra Linux не предусмотрена работа под учетной записью суперпользователя `root`. Для

7. В открывшемся окне **Info** нажмите кнопку **OK**.
8. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG RC.
Запустится установка модуля Salt Minion.
9. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **OK**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера >' successfully installed..`

Модуль Salt Minion установлен.

3.19.2 Установка роли RMQ Message Bus на сервер Ankey SIEM NG RC

Для установки роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
8. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.

выполнения установки компонентов ПК Ankey SIEM NG необходимо переключаться в учетную запись суперпользователя из текущей учетной записи (например, `administrator`). Для переключения в учетную запись суперпользователя `root` возможно использовать команду `sudo -s`.

10. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
12. Нажмите кнопку **ОК**.

Роль установлена.

3.19.3 Установка роли Retro Correlator

Для установки роли вам потребуется архив `RetroCorrelator_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RetroCorrelator_<Номер версии>.tar.gz`:

```
tar -xf RetroCorrelator_<Номер версии>.tar.gz
```
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
7. В открывшемся окне введите название экземпляра роли `Retro Correlator` и нажмите кнопку **ОК**.
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.

Внимание! Укажите значения параметров:

```
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
InternalRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
KBAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091  
SiemServerAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG  
Server>
```

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

9. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **ОК**.
11. На сервере Ankey SIEM NG RC в файле `/opt/core-agent/config.json` измените значение параметров `rmq` → `host` и `rmq` → `vhost`:

```
"host": "<FQDN или IPv4-адрес сервера Ankey SIEM NG Server>" "vhost":  
"siem"
```
12. Перезапустите службу: `systemctl restart core-agent.service`
Роль установлена.

3.20 Установка доверенного сертификата для сайта Ankey SIEM NG

При развертывании Ankey SIEM NG для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Extended Key Usage (EKU) содержать записи `serverAuth` и `clientAuth`;
- в расширении Subject Alternative Name (SAN) содержать запись об FQDN или IPv4-адрес сервера компонента в зависимости от значения параметра `HostAddress`.

- ❖ Чтобы установить доверенный сертификат на Linux-like:
 1. На сервере Ankey SIEM NG Core разместите файлы сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название`

экземпляра роли>/certs для каждой роли Core, Management and Configuration и Knowledge Base.

2. Измените конфигурации (см. пункт 6.1.2) ролей Core, Management and Configuration и Knowledge Base.

SSLCertificatePemFileName: <Имя файла сертификата>

SSLKeyFileName: <Имя файла закрытого ключа>

Например:

SSLCertificatePemFileName: website.crt

SSLKeyFileName: website.key

Сертификат установлен.

Внимание! Имена файлов сертификата и ключа не должны совпадать с именами файлов, которые уже находятся в папке сертификатов: замена содержимого стандартных файлов приведет к некорректной работе системы.

3.21 Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Agent

Для RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Agent вы можете установить пользовательский сертификат безопасности, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- использовать отдельные файлы для хранения сертификата центра сертификации (ЦС), пользовательского сертификата и закрытого ключа;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Extended Key Usage (EKU) записи аутентификации сервера `serverAuth` и аутентификации клиента `clientAuth`;
- содержать в поле Common Name значения `core`, `siem` или `agent` для компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Agent соответственно.

Примечание. Если компонент Ankey SIEM NG Agent установлен на Windows Server, а другие компоненты в ОС Linux-like – необходимо установить пользовательский сертификат от одного центра сертификации для всех компонентов. Для компонента Ankey SIEM NG Agent установлен в Windows Server используются команды, указанные в инструкции для Windows Server. Для компонентов на Linux-like – параметры из инструкции для Linux-like.

❖ Чтобы установить пользовательский сертификат для RMQ Message Bus и компонента Ankey SIEM NG Agent на Windows Server:

1. Разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа на сервере Ankey SIEM NG Core в постоянной папке, к которой есть доступ у пользователя Network Service.
2. Установите сертификат для RMQ Message Bus, выполнив команду:
rabbitmqcfg set -p CACertFile <Путь к файлу сертификата ЦС> CertFile <Путь к файлу пользовательского сертификата> KeyFile <Путь к файлу закрытого ключа>
3. Установите сертификат для Ankey SIEM NG Agent, выполнив команду:
agentcfg set -p RMQ_SSL_CA_CERTIFICATE <Путь к файлу сертификата ЦС> RMQ_SSL_CERTIFICATE <Путь к файлу пользовательского сертификата> RMQ_SSL_KEY <Путь к файлу закрытого ключа>

Сертификат установлен.

❖ Чтобы установить пользовательский сертификат RMQ Message Bus и компонентов Ankey SIEM NG Core, Ankey SIEM NG Server и Ankey SIEM NG Agent на Linux-like:

1. Разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей RMQ Message Bus, Core, SIEM Server и Agent.
2. Измените конфигурацию роли RMQ Message Bus:
CACertFile: <Имя файла сертификата ЦС>
CertFile: <Имя файла пользовательского сертификата>
KeyFile: <Имя файла закрытого ключа>
3. Измените конфигурацию роли Core:
CACertificateFileName: <Имя файла сертификата ЦС>
RMQsslCertificateFileName: <Имя файла пользовательского сертификата>
RMQsslKeyFileName: <Имя файла закрытого ключа>
4. Измените конфигурацию роли SIEM Server:
RMQ_SSL_CA_CERTIFICATE: <Полный путь к файлу сертификата ЦС>
RMQ_SSL_CERTIFICATE: <Полный путь к файлу пользовательского сертификата>
RMQ_SSL_KEY: <Полный путь к файлу закрытого ключа>
5. Измените конфигурацию роли Agent:
Agent_RMQ_SSL_CA_Certificate: <Полный путь к файлу сертификата ЦС>
Agent_RMQ_SSL_Certificate: <Полный путь к файлу пользовательского сертификата>
Agent_RMQ_SSL_Key: <Полный путь к файлу закрытого ключа>

Сертификат установлен.

3.22 Настройка Ankey SIEM NG для обеспечения его безопасной работы

В этом подразделе приводятся инструкции по настройке развернутой конфигурации Ankey SIEM NG для обеспечения его безопасной работы.

Компоненты системы рекомендуется разместить в доверенном сегменте сети. Доступ к ним из других сегментов рекомендуется ограничить с помощью межсетевого экрана.

3.22.1 Настройка Ankey SIEM NG в конфигурации для низконагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like

❖ Чтобы настроить Ankey SIEM NG:

1. На серверах под управлением Linux-like разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m  
conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-  
адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m  
conntrack --ctstate NEW -m comment --comment "SSH admin access" -j  
ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `-s 198.51.100.0,198.51.100.1,192.0.2.0/24`.

2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:

```
iptables -F DOCKER-USER
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-m conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --  
dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --  
comment "Web user access" -j ACCEPT
```

3. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed/roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin/config/`, добавьте параметры:

```
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
```

```
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
```

4. Перезапустите службы компонентов Ankey SIEM NG Core и Knowledge Base:

```
docker restart $(docker ps | awk '!/core-|kb-/{print $NF}')
```

5. **Разрешите входящие соединения от агентов:**
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Agent> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Agent to Ankey SIEM NG Server" -j ACCEPT`
6. **Разрешите входящие соединения от Ankey SIEM NG RC:**
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports 3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT`
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Server" -j ACCEPT`
7. **На серверах под управлением Linux-like заблокируйте все входящие соединения, кроме разрешенных:**
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP`
`iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT`
8. **Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent:** `apt-get install iptables-persistent`

Примечание. Порядок сохранения правил на серверах под управлением Astra Linux описан в [справочном центре производителя операционной системы](#).

9. Сохраните правила межсетевого экрана: `netfilter-persistent save`
10. **На серверах агентов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:**
`netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389`
`netsh advfirewall firewall delete rule name=all protocol=udp localport=3389`
11. **Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:**
`netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`
`netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24.

12. Если для сбора событий по стандарту syslog и протоколу Netflow агенты на Windows Server не использует порты по умолчанию, на серверах агентов удалите правила для входящих соединений с этих портов:
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp localport=%P)
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp localport=%P)
13. Смените пароли служебных учетных записей в Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 4.1.2).
14. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.
15. Установите собственные доверенные сертификаты (см. подраздел 3.20) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.
16. На серверах под управлением Linux-like для каждого администратора Ankey SIEM NG создайте отдельную учетную запись:
adduser <Логин администратора>
17. На рабочих станциях администраторов Ankey SIEM NG сгенерируйте ключевую пару.

Примечание. Для генерации ключевой пары на Linux-like вы можете использовать утилиту ssh-keygen, на Windows Server – PuTTYgen.

18. На серверах под управлением Linux-like добавьте открытый ключ в файл /home/<Логин администратора>/.ssh/authorized_keys.
19. В файле /etc/ssh/sshd_config раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):
PubkeyAuthentication yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
PasswordAuthentication no
20. В файле /etc/sudoers измените значение параметра:
<Логин администратора> ALL=(ALL) ALL
21. Для каждого пользователя Ankey SIEM NG создайте отдельную учетную запись.

22. Смените пароль учетной записи Administrator²⁵.
Ankey SIEM NG настроен.

3.22.2 Настройка Ankey SIEM NG в конфигурации для средненагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like

❖ Чтобы настроить Ankey SIEM NG:

1. На серверах под управлением Linux-like разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m  
conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-  
адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m  
conntrack --ctstate NEW -m comment --comment "SSH admin access" -j  
ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `-s 198.51.100.0,198.51.100.1,192.0.2.0/24`.

2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:

```
iptables -F DOCKER-USER
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-m conntrack --ctstate
```

```
ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --  
dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --  
comment "Web user access" -j ACCEPT
```

3. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed/roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin/config/`, добавьте параметры:

```
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
```

```
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
```

4. Перезапустите службы компонентов Ankey SIEM NG Core и Knowledge Base:

```
docker restart $(docker ps | awk '/core-|kb-/{print $NF}')
```

5. Разрешите входящие соединения от Ankey SIEM NG Server:

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса>  
-s <IP-адрес сервера Ankey SIEM NG Server> -p tcp -m multiport --dports
```

²⁵ По умолчанию P@ssw0rd.

- 443,3334,5671,8703,8721,8799 -m conntrack -ctstate NEW -m comment --comment "From Ankey SIEM NG Server to Ankey SIEM NG Core" -j ACCEPT
6. **Разрешите входящие соединения от Ankey SIEM NG RC:**
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports 3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT
7. **На сервере Ankey SIEM NG Server разрешите входящие соединения от Ankey SIEM NG Core:**
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m multiport --dports 5671,5672,8013,15672 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey SIEM NG Server" -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Core> -p tcp --dport 9200 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey SIEM NG ES" -j ACCEPT
8. **Разрешите входящие соединения от агентов:**
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Agent> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Agent to Ankey SIEM NG Server" -j ACCEPT
9. **Разрешите входящие соединения от Ankey SIEM NG RC:**
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Server" -j ACCEPT
10. **На серверах под управлением Linux-like заблокируйте все входящие соединения, кроме разрешенных:**
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT
11. **Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent:** apt-get install iptables-persistent

Примечание. Порядок сохранения правил на серверах под управлением Astra Linux-like описан в [справочном центре производителя операционной системы](#).

12. **Сохраните правила межсетевого экрана:** netfilter-persistent save
13. **На серверах агентов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:**
netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389
netsh advfirewall firewall delete rule name=all protocol=udp localport=3389

14. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:

```
netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in  
action=allow  
protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций  
администраторов>  
netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in  
action=allow  
protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций  
администраторов>
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24.

15. Если для сбора событий по стандарту syslog и протоколу Netflow агенты на Windows Server не использует порты по умолчанию, на серверах агентов удалите правила для входящих соединений с этих портов:

```
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all  
protocol=tcp localport=%P)  
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all  
protocol=udp localport=%P)
```

16. Смените пароли служебных учетных записей в Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 4.1.2).
17. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.
18. Установите собственные доверенные сертификаты (см. подраздел 3.20) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.
19. На серверах под управлением Linux-like для каждого администратора Ankey SIEM NG создайте отдельную учетную запись:
- ```
adduser <Логин администратора>
```
20. На рабочих станциях администраторов Ankey SIEM NG сгенерируйте ключевую пару.

**Примечание.** Для генерации ключевой пары на Linux-like вы можете использовать утилиту ssh-keygen, на Windows Server – PuTTYgen.

21. На серверах под управлением Linux-like добавьте открытый ключ в файл /home/<Логин администратора>/.ssh/authorized\_keys.

22. В файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):  
PubkeyAuthentication yes  
RhostsRSAAuthentication no  
HostbasedAuthentication no  
PermitEmptyPasswords no  
PasswordAuthentication no
  23. В файле `/etc/sudoers` измените значение параметра:  
<Логин администратора> ALL=(ALL) ALL
  24. Для каждого пользователя Ankey SIEM NG создайте отдельную учетную запись.
  25. Смените пароль учетной записи Administrator<sup>26</sup>.
- Ankey SIEM NG настроен.

### 3.22.3 Настройка Ankey SIEM NG в конфигурации для высоконагруженных и сверхнагруженных систем: Ankey SIEM NG Core и Ankey SIEM NG Server установлены на Linux-like

- ❖ Чтобы настроить Ankey SIEM NG:
  1. На серверах под управлением Linux-like разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT
  2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:  
iptables -F DOCKER-USER  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --dports 443,3334,8091,8190 -m conntrack -ctstate NEW -m comment --comment "Web user access" -j ACCEPT
  3. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed/roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin/config/`, добавьте параметры:  
PGADMIN\_CONFIG\_MASTER\_PASSWORD\_REQUIRED=True

<sup>26</sup> По умолчанию P@ssw0rd.

- PGADMIN\_DEFAULT\_PASSWORD=<Пароль PGAdmin>
4. **Перезапустите службы компонентов Ankey SIEM NG Core и Knowledge Base:**  
docker restart \$(docker ps | awk '/core-|kb-/{print \$NF}')
  5. **Разрешите входящие соединения от Ankey SIEM NG Server:**  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Server> -p tcp -m multiport --dports 443,3334,5671,8703,8721,8799 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Server to Ankey SIEM NG Core" -j ACCEPT
  6. **Разрешите входящие соединения от Ankey SIEM NG RC:**  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m multiport --dports 3334,5671,8091 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Core" -j ACCEPT
  7. **На сервере Ankey SIEM NG Server разрешите входящие соединения от Ankey SIEM NG Core:**  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Core> -p tcp -m multiport --dports 5671,5672,8013,15672 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey SIEM NG Server" -j ACCEPT
  8. **Разрешите входящие соединения от агентов:**  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Agent> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Agent to Ankey SIEM NG Server" -j ACCEPT
  9. **Разрешите входящие соединения от Ankey SIEM NG RC:**  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG RC> -p tcp -m tcp --dport 8013 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG RC to Ankey SIEM NG Server" -j ACCEPT
  10. **На сервере Ankey SIEM NG ES разрешите входящие соединения от Ankey SIEM NG Core и Ankey SIEM NG Server:**  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Core> -p tcp --dport 9200 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Core to Ankey SIEM NG ES" -j ACCEPT  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Server> -p tcp --dport 9200 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Server to Ankey SIEM NG ES" -j ACCEPT
  11. **На серверах под управлением Linux-like заблокируйте все входящие соединения, кроме разрешенных:**  
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP  
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT
  12. **Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent: apt-get install iptables-persistent**

**Примечание.** Порядок сохранения правил на серверах под управлением Astra Linux описан в [справочном центре производителя операционной системы](#).

13. Сохраните правила межсетевого экрана: netfilter-persistent save
14. На серверах агентов под управлением Windows Server удалите все правила удаленного доступа по протоколу RDP:  

```
netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389
netsh advfirewall firewall delete rule name=all protocol=udp localport=3389
```
15. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:  

```
netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
```
16. Если для сбора событий по стандарту syslog и протоколу Netflow агенты на Windows Server не использует порты по умолчанию, на серверах агентов удалите правила для входящих соединений с этих портов:  

```
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp localport=%P)
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp localport=%P)
```
17. Смените пароли служебных учетных записей в Ankey SIEM NG (подробнее см. Руководство администратора Ankey SIEM NG 4.1.2).
18. На серверах под управлением Windows Server убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.
19. Установите собственные доверенные сертификаты (см. подраздел 3.20) для Ankey SIEM NG Core, Knowledge Base, Ankey SIEM NG MC и RabbitMQ.
20. На серверах под управлением Linux-like для каждого администратора Ankey SIEM NG создайте отдельную учетную запись:  

```
adduser <Логин администратора>
```
21. На рабочих станциях администраторов Ankey SIEM NG сгенерируйте ключевую пару.

**Примечание.** Для генерации ключевой пары на Linux-like вы можете использовать утилиту ssh-keygen, на Windows Server – PuTTYgen.

22. На серверах под управлением Linux-like добавьте открытый ключ в файл /home/<Логин администратора>/.ssh/authorized\_keys.

23. В файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):  
PubkeyAuthentication yes  
RhostsRSAAuthentication no  
HostbasedAuthentication no  
PermitEmptyPasswords no  
PasswordAuthentication no
  24. В файле `/etc/sudoers` измените значение параметра:  
<Логин администратора> ALL=(ALL) ALL
  25. Для каждого пользователя Ankey SIEM NG создайте отдельную учетную запись.
  26. Смените пароль учетной записи Administrator<sup>27</sup>.
- Ankey SIEM NG настроен.

---

<sup>27</sup> По умолчанию P@ssw0rd.

## 4 Обновление ПК Ankey SIEM NG

Вы можете обновлять компоненты ПК Ankey SIEM NG на серверах под управлением Linux-like – с помощью дистрибутивов.

А также можете обновлять компонент Ankey SIEM NG Agent на серверах под управлением ОС Windows Server – с помощью дистрибутива.

Для обновления каждого компонента Ankey SIEM NG требуется не менее 50 ГБ свободного места на жестком диске сервера. Если компоненты Ankey SIEM NG установлены на одном сервере, требуется не менее 60 ГБ свободного места.

Прежде чем приступать к обновлению Ankey SIEM NG, рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

Перед началом обновления необходимо убедиться в отсутствии ошибок в работе системы (индикатор состояния системы не красный), а также рекомендуется создать резервную копию данных компонентов.

Если вы используете удаленное подключение к серверам компонентов, рекомендуется не прерывать сессию удаленного подключения до завершения обновления. Для удаленного подключения к серверам на Linux-like рекомендуется использовать утилиту `screen`.

Иерархическую инсталляцию Ankey SIEM NG необходимо обновлять в следующем порядке: сначала обновить компоненты, расположенные на главной площадке, и только затем – компоненты, расположенные на подчиненных площадках.

В версии 3.0 обновлены SSL-сертификаты, поставляемые в составе Ankey SIEM NG. Во время обновления системы с версии 2.1 (после обновления Ankey SIEM NG Core и до обновления агентов) будут недоступны как сами агенты, так и работа с задачами на сбор данных.

### 4.1 Обновление с помощью дистрибутивов

Для обновления Ankey SIEM NG необходимо обратиться в техническую поддержку ООО «Газинформсервис» и получить дистрибутивы с новыми версиями компонентов.

Начиная с версии 3.0 компоненты Ankey SIEM NG на Debian поддерживают только Debian 10. Обновление Debian (инструкцию см. на сайте [debian.org](http://debian.org)) необходимо выполнять в следующем порядке:

1. Обновить список пакетов с помощью команды `apt-get update`.
2. Выполнить минимальное обновление Debian с помощью команды `apt-get upgrade`. Будут обновлены только те пакеты, обновление которых не требует удаления или установки других пакетов.
3. Обновить компоненты Ankey SIEM NG ES, Ankey SIEM NG Server и Ankey SIEM NG RC с помощью дистрибутивов для Debian 10.
4. Выполнить полное обновление Debian с помощью команды `apt-get full-upgrade`. Будут установлены последние доступные версии пакетов и разрешены изменившиеся зависимости. При необходимости будут установлены новые пакеты и удалены все устаревшие пакеты, которые вызывают конфликты.

Начиная с версии 4.0 базовыми единицами развертывания компонентов на ОС семейства Linux-like являются роли, каждая из которых представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Архитектурно роли распределены между приложениями (Management and Configuration, Knowledge Base и Ankey SIEM NG) и поставляются в виде отдельных архивов. Для обновления того или иного компонента системы может потребоваться обновление как одной, так и нескольких ролей.

Управление развертыванием компонентов на Linux-like обеспечивает роль Deployer, которая построена на базе программного обеспечения SaltStack. Его модуль Salt Master обеспечивает общее управление обновлением компонентов Ankey SIEM NG, модули Salt Minion – обновление компонентов на каждом сервере системы.

Порядок обновления компонентов зависит от выбранных конфигурации Ankey SIEM NG и операционных систем для серверов Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG ES.

### **Компоненты Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Server и Ankey SIEM NG ES установлены на Linux-like**

Ankey SIEM NG необходимо обновлять в следующем порядке:

1. Обновление роли Deployer.
2. Обновление компонента Ankey SIEM NG MC.
3. Обновление компонента Knowledge Base.
4. Обновление компонента Ankey SIEM NG Core.
5. Обновление компонента Ankey SIEM NG ES.
6. Обновление компонента Ankey SIEM NG Server (как стандартной, так и облегченной версии).
7. Обновление компонентов Ankey SIEM NG Agent.
8. Обновление компонента Ankey SIEM NG RC.

#### **4.1.1 Обновление облегченной версии компонента Ankey SIEM NG Server на Microsoft Windows**

**Внимание!** В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.

Для обновления вам потребуется файл AnkeySiemSetup\_<Номер версии>.exe из комплекта поставки.

❖ Чтобы обновить облегченную версию компонента Ankey SIEM NG Server:

1. Запустите файл AnkeySiemSetup\_<Номер версии>.exe. Откроется окно мастера обновления.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Обновить**.
4. По завершении обновления нажмите кнопку **Закреть**.

5. В адресной строке браузера введите: `http://<FQDN или IPv4-адрес облегченной версии SIEM Server>:15672/#/dynamic-shovels`  
Откроется страница входа в RabbitMQ.
6. Введите логин `siem` и пароль.

**Примечание.** По умолчанию пароль служебной учетной записи – `P@ssword`.

7. Нажмите кнопку **Login**.  
Откроется вкладка **Admin** с таблицей **Dynamic Shovels**.
8. В таблице **Dynamic Shovels** в столбце **Name** нажмите ссылку.
9. В открывшемся окне нажмите кнопку **Delete this shovel**.
10. Повторите шаги 8–9 для всех строк таблицы **Dynamic Shovels**.
11. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файл `/opt/deployer/pki/CABundle.crt` с сервера, на котором установлена роль `Deployer`, на сервер облегченной версии Ankey SIEM NG Server.
12. Если стандартная версия Ankey SIEM NG Server установлена на Linux, скопируйте файлы `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.crt` и `/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG Server>/<Название экземпляра роли SIEM Server>/certs/RMQ_SIEM_Client.key` с сервера стандартной версии Ankey SIEM NG Server на сервер облегченной версии Ankey SIEM NG Server.

На сервере облегченной версии Ankey SIEM NG Server в интерфейсе командной строки Windows от имени администратора выполните команды:

```
coreagentcfg set -p AgentRMQVirtualHost siem RMQHost localhost
rabbitmqcfg set -p CACertFile <Путь к файлу CABundle.crt> -v
siemcfg set -p TargetSiemRabbitHost <FQDN или IPv4-адрес стандартной версии Ankey SIEM NG Server> RMQHost <FQDN или IPv4-адрес стандартной версии Ankey SIEM NG Server> RMQ_SSL_CA_CERTIFICATE <Путь к файлу CABundle.crt> RMQ_SSL_CERTIFICATE <Путь к файлу RMQ_SIEM_Client.crt> RMQ_SSL_KEY <Путь к файлу RMQ_SIEM_Client.key>
```

Облегченная версия компонента Ankey SIEM NG Server обновлена.

После обновления облегченной версии Ankey SIEM NG Server необходимо обновить компонент Ankey SIEM NG Agent и правила нормализации и агрегации (см. раздел 4.1.3), установленные с этой версией.

### 4.1.2 Обновление компонента Ankey SIEM NG Agent на Windows Server

**Внимание!** В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.



Для обновления вам потребуется файл AnkeyAgentSetup\_<Номер версии>.exe из комплекта поставки.


❖ Чтобы обновить компонент Ankey SIEM NG Agent:

1. Запустите файл AnkeyAgentSetup\_<Номер версии>.exe. Откроется окно мастера обновления.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Обновить**.
4. По завершении обновления нажмите кнопку **Заккрыть**.

Компонент Ankey SIEM NG Agent обновлен.

### 4.1.3 Обновление правил нормализации и агрегации для облегченной версии Ankey SIEM NG Server

❖ Чтобы обновить правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Knowledge Base**.  
Откроется страница **Статистика**.

**Примечание.** Если вы используете браузер Mozilla Firefox и на странице **Статистика** отображается сообщение "Отключен", необходимо проверить, что адреса `https://<FQDN>` или IPv4-адрес компонента Ankey SIEM NG Core:>:8091 добавлены в исключения безопасности браузера.

2. В главном меню в разделе <Название БД> выберите пункт **Базы данных**.  
Откроется страница **Базы данных / <Название БД>**.
3. В панели **Базы данных** выберите родительскую базу данных, которая содержит устанавливаемые правила.
4. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
5. В панели **Папки** выберите **Все объекты**.
6. В панели **Наборы для установки** выберите **Все объекты**.
7. В панели со списком объектов нажмите .
8. По ссылке **Объекты: все** установите флажки **Агрегация** и **Нормализация**.
9. Повторно нажмите на ссылку.
10. В списке правил выберите те правила, которые требуется обновить для облегченной версии Ankey SIEM NG Server.

**Примечание.** Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов – клавишу Ctrl, для выбора всех объектов в списке – комбинацию клавиш Ctrl+A.

11. Нажмите .
- Откроется окно **Экспорт объектов**.

12. Выберите вариант **Для установки в SIEM Lite**.
13. Нажмите кнопку **Экспортировать**.  
Браузер сохранит архив `knowledgebase_<Дата экспорта>.zip` в папку загрузки.
14. Переместите файл архива на сервер облегченной версии Ankey SIEM NG Server в любую папку.
15. Если облегченная версия Ankey SIEM NG Server установлена на Linux-like, запустите установку правил нормализации и агрегации:  
`"/opt/siem/bin/siemlight-kb" -u <Путь к файлу архива>`

Правила нормализации и агрегации для облегченной версии Ankey SIEM NG Server обновлены.

#### 4.1.4 Обновление роли Deployer

Для обновления роли вам потребуется архив `Deployer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. Распакуйте архив `Deployer_<Номер версии>.tar.gz`:  
`tar -xf Deployer_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов. По завершении подготовки откроется окно для проверки и изменения параметров обновления.
4. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
5. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера, на который установлена роль Deployer.
6. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
7. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.5 Обновление компонента Ankey SIEM NG MC на Linux-like

Компонент Ankey SIEM NG MC необходимо обновлять в следующем порядке: сначала обновить роль `SqlStorage` или `JatobaStorage`, затем – роль `Management and Configuration`.

##### 4.1.5.1 Обновление роли SqlStorage

Для обновления роли вам потребуется архив `SqlStorage_<Номер версии>.tar` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `SqlStorage_<Номер версии>.tar`:  
`tar -xf SqlStorage_<Номер версии>.tar`

2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения **Management and Configuration**.
5. В открывшемся окне выберите вариант с названием экземпляра роли `SqlStorage`. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
7. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера **Ankey SIEM NG Core**.
8. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.5.2 Обновление роли **Management and Configuration**

Для обновления роли вам потребуется архив `ManagementAndConfiguration_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере **Ankey SIEM NG Core** распакуйте архив `ManagementAndConfiguration_<Номер версии>.tar.gz`:  
`tar -xf ManagementAndConfiguration_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения **Management and Configuration**.
5. В открывшемся окне выберите вариант с названием экземпляра роли **Management and Configuration**. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
7. Убедитесь, что в качестве значения параметров `HostAddress` и `PostgreHost` указано полное доменное имя (FQDN) или IPv4-адрес сервера **Ankey SIEM NG Core**.
8. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.

Роль обновлена.

### 4.1.6 Обновление компонента Knowledge Base на Linux-like

Для обновления компонента необходимо обновить роль Knowledge Base. Для обновления роли вам потребуется архив KB\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив KB\_<Номер версии>.tar.gz:  
tar -xf KB\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Knowledge Base.
5. В открывшемся окне выберите вариант с названием экземпляра роли Knowledge Base. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
7. Проверьте значения параметров:  
SiemAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
MCAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334  
CoreAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:443
8. Нажмите кнопку **OK**. Запустится установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
9. Нажмите кнопку **OK**.

Роль обновлена.

### 4.1.7 Обновление компонента Ankey SIEM NG Core на Linux-like

Компонент необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль Core.

#### 4.1.7.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG Core

Для обновления роли вам потребуется архив RmqMessagebus\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив RmqMessagebus\_<Номер версии>.tar.gz:  
tar -xf RmqMessagebus\_<Номер версии>.tar.gz

2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер Ankey SIEM NG Core. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
7. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.
8. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.7.2 Обновление роли Core

Для обновления роли вам потребуется архив `Core_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `Core_<Номер версии>.tar.gz`:  
`tar -xf Core_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли Core. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Advanced configuration**. Откроется страница со списком параметров (см. приложение Б).
7. Проверьте значения параметров:  
`HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>`  
`MCAAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334`  
`KBAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091`

PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
SiemFrontendAddress: http://<FQDN или IPv4-адрес сервера Ankey SIEM  
NG Server>:8013>

8. Нажмите кнопку **ОК**.

Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

9. Нажмите кнопку **ОК**.

Роль обновлена.

#### 4.1.8 Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG ES на Linux-like

Перед обновлением компонента Ankey SIEM NG ES необходимо установить роль `Deployer` на сервер Ankey SIEM NG Server. Если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, также перед обновлением компонента Ankey SIEM NG ES необходимо установить на его сервер модуль Salt Minion (см. пункте 3.10.1).

Для обновления компонента необходимо установить роль `SIEM Storage`. Для установки роли вам потребуется архив `EventsStorage_elasticsearch_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Server распакуйте архив `EventsStorage_elasticsearch_<Номер версии>.tar.gz`:  
`tar -xf EventsStorage_elasticsearch_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **ОК**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG ES.
8. В открывшемся окне введите название экземпляра роли `SIEM Storage` и нажмите кнопку **ОК**.  
Откроется окно для проверки и изменения параметров установки.
9. Выберите набор параметров:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
  - если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, выберите вариант **Advanced configuration**.

Откроется страница с перечнем параметров конфигурации.

10. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG ES.
11. Проверьте значение параметра **ClusterConfigurationProfile**:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных систем, проверьте, что выбран вариант **AIO**;
  - если для средненагруженных систем – выбран вариант **SIEMandStorage**;
  - если для высоконагруженных – вариант **Standalone**;
  - если для сверхнагруженных – вариант **ManagedStorage**.
12. Проверьте пути для хранения данных Ankey SIEM NG ES:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных, средненагруженных или высоконагруженных систем, проверьте значения параметров:
    - PathData: <Каталог для хранения индексов>
    - PathRepo: <Каталог для хранения резервных копий индексов>
    - PathLog: <Каталог для хранения файлов журналов>
  - если Ankey SIEM NG развернут в конфигурации для сверхнагруженных систем, проверьте значения параметров:
    - PathData: <Каталог для хранения индексов, находящихся в "теплой" стадии, а также для хранения счетчиков всех индексов>
    - PathDataHot: <Каталог для хранения индексов, находящихся в "горячей" стадии>
    - PathRepo: <Каталог для хранения резервных копий индексов>
    - PathLog: <Каталог для хранения файлов журналов>

**Примечание.** Подробное описание стадий жизненного цикла индексов приведено на сайте [elastic.co](https://www.elastic.co). Если вы хотите, чтобы данные хранились в каталогах по умолчанию, – не изменяйте значения параметров.

13. Если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, проверьте, что установлен флажок **HighLoad**.

**Примечание.** В случае установки флажка **HighLoad** кластер Elasticsearch будет содержать четыре узла данных.

14. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
15. Нажмите кнопку **OK**.

Роль установлена.

## 4.1.9 Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG Server на Linux-like

Компонент необходимо обновлять в следующем порядке: сначала установить роль RMQ Message Bus, затем – роль SIEM Server.

### 4.1.9.1 Обновление Ankey SIEM NG Server: установка роли RMQ Message Bus

Для установки роли вам потребуется архив RmqMessagebus\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Server распакуйте архив RmqMessagebus\_<Номер версии>.tar.gz:  
tar -xf RmqMessagebus\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Server.
7. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.  
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
9. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server.
10. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
11. Нажмите кнопку **OK**.

Роль установлена.

### 4.1.9.2 Обновление Ankey SIEM NG Server: установка роли SIEM Server

Для установки роли вам потребуется архив SiemServer\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Server распакуйте архив SiemServer\_<Номер версии>.tar.gz:  
tar -xf SiemServer\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.



3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Server.
7. В открывшемся окне введите название экземпляра роли SIEM Server и нажмите кнопку **OK**.  
Откроется окно для проверки и изменения параметров установки.
8. Выберите набор параметров:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
  - если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, выберите вариант **Advanced configuration**.Откроется страница с перечнем параметров конфигурации.
9. Укажите значения параметров:  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>  
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
10. Если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, проверьте значение параметра ElasticsearchHost:  
ElasticsearchHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>
11. Если Ankey SIEM NG развернут в конфигурации для сверхнагруженных систем, убедитесь, что установлен флажок **ManagedStorage**.
12. Если предполагаемый поток событий от источников будет превышать 20 000 событий в секунду и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, убедитесь, что установлен флажок **HighLoad**.

**Примечание.** После установки флажка **HighLoad** для службы SIEM server storage будет выделено шесть потоков операционной системы (вместо четырех, когда флажок снят).

13. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
14. Нажмите кнопку **OK**.  
Роль установлена.

## 4.1.10 Обновление версии 4.0 компонента Ankey SIEM NG ES на Linux-like

**Внимание!** Перед обновлением компонента необходимо обновить роль Deployer.

Для обновления компонента необходимо обновить роль SIEM Storage. Порядок действий при обновлении зависит от типа установленного хранилища событий.

### 4.1.10.1 Обновление роли Event Storage с хранилищем событий LogSpace

Для обновления роли вам потребуется архив EventsStorage\_LogSpace\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив EventsStorage\_LogSpace\_<Номер версии>.tar.gz:  
`tar -xf EventsStorage_LogSpace_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли Event Storage. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**. Откроется страница с перечнем параметров конфигурации.
7. В качестве значения параметра `Database` укажите название хранилища событий LogSpace.
8. В качестве значения параметра `PathData` укажите каталог хранилища событий LogSpace.
9. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.

Роль обновлена.

### 4.1.10.2 Обновление роли SIEM Storage с хранилищем событий Elasticsearch

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив EventsStorage\_elasticsearch\_<Номер версии>.tar.gz:  
`tar -xf EventsStorage_elasticsearch_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.

Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.

4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Storage.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите набор параметров:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных или средненагруженных систем, выберите вариант **Basic configuration**;
  - если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, выберите вариант **Advanced configuration**.

Откроется страница с перечнем параметров конфигурации.

7. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG ES.
8. Проверьте значение параметра **ClusterConfigurationProfile**:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных систем, проверьте, что выбран вариант **AIO**;
  - если для средненагруженных систем – выбран вариант **SIEMandStorage**;
  - если для высоконагруженных – вариант **Standalone**;
  - если для сверхнагруженных – вариант **ManagedStorage**.
9. Проверьте пути для хранения данных Ankey SIEM NG ES:
  - если Ankey SIEM NG развернут в конфигурации для низконагруженных, средненагруженных или высоконагруженных систем, проверьте значения параметров:  
PathData: <Каталог для хранения индексов>  
PathRepo: <Каталог для хранения резервных копий индексов>  
PathLog: <Каталог для хранения файлов журналов>
  - если Ankey SIEM NG развернут в конфигурации для сверхнагруженных систем, проверьте значения параметров:  
PathData: <Каталог для хранения индексов, находящихся в "теплой" стадии, а также для хранения счетчиков всех индексов>  
PathDataHot: <Каталог для хранения индексов, находящихся в "горячей" стадии>  
PathRepo: <Каталог для хранения резервных копий индексов>  
PathLog: <Каталог для хранения файлов журналов>

**Примечание.** Подробное описание стадий жизненного цикла индексов приведено на сайте [elastic.co](https://www.elastic.co). Если вы хотите, чтобы данные хранились в каталогах по умолчанию, – не изменяйте значения параметров.

10. Если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, проверьте, что установлен флажок **HighLoad**.

**Примечание.** В случае установки флажка **HighLoad** кластер Elasticsearch будет содержать четыре узла данных.

11. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

12. Нажмите кнопку **ОК**.

Роль обновлена.

### 4.1.11 Обновление версии 4.0 компонента Ankey SIEM NG Server на Linux-like

**Внимание!** Перед обновлением компонента необходимо обновить роль Deployer.

Если Ankey SIEM NG развернут в конфигурации для средненагруженных, высоконагруженных или сверхнагруженных систем, Ankey SIEM NG Server необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль SIEM Server. Если Ankey SIEM NG развернут в конфигурации для низконагруженных систем, необходимо обновить только роль SIEM Server.

#### 4.1.11.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG Server

Для обновления роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:  
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер Ankey SIEM NG Server.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.

7. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Server.
8. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **ОК**.

Роль обновлена.

#### 4.1.14.2. Обновление роли SIEM Server

Для обновления роли вам потребуется архив `SiemServer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `SiemServer_<Номер версии>.tar.gz`:  
`tar -xf SiemServer_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Server.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
7. Укажите значения параметров:  
`CoreAddress`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
`HostAddress`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>  
`RMQHost`: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
8. Проверьте значение параметра **StorageBackendType**:
  - если для хранения событий используется `Elasticsearch`, убедитесь, что выбран вариант **elasticsearch**;
  - если используется `LogSpace` – выбран вариант **logspace**.
9. Если Ankey SIEM NG развернут в конфигурации для высоконагруженных или сверхнагруженных систем, проверьте значение параметра, указывающего расположение сервера Ankey SIEM NG ES в сети:
  - если для хранения событий используется `Elasticsearch`, проверьте значение параметра `ElasticsearchHost`:  
`ElasticsearchHost`: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>
  - если используется `LogSpace` – проверьте значение параметра `LogSpaceHost`:  
`LogSpaceHost`: <FQDN или IPv4-адрес сервера Ankey SIEM NG ES>

10. Если Ankey SIEM NG развернут в конфигурации для сверхнагруженных систем, убедитесь, что установлен флажок **ManagedStorage**.
11. Если предполагаемый поток событий от источников будет превышать 20 000 событий в секунду и сервер Ankey SIEM NG ES имеет емкость ОЗУ 256 ГБ или более, убедитесь, что установлен флажок **HighLoad**.

**Примечание.** В случае установки флажка **HighLoad** для службы SIEM server storage будет выделено шесть потоков операционной системы (вместо четырех, когда флажок снят).

12. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.12 Обновление облегченной версии компонента Ankey SIEM NG Server на Linux-like

Облегченную версию Ankey SIEM NG Server необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль SIEM Server.

##### 4.1.12.1 Обновление роли RMQ Message Bus на сервере облегченной версии Ankey SIEM NG Server

Для обновления роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:  
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнутся распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер облегченной версии Ankey SIEM NG Server.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
7. Укажите в качестве значения параметра `HostAddress` FQDN или IPv4-адрес сервера облегченной версии Ankey SIEM NG Server.

8. Нажмите кнопку **ОК**.
9. Начнется установка пакетов.  
По завершении установки появится сообщение `Deployment configuration successfully applied.`
10. Нажмите кнопку **ОК**.

Роль обновлена.

#### 4.1.12.2 Обновление роли SIEM Server для облегченной версии компонента

Для обновления роли вам потребуется архив `SiemServer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. В адресной строке браузера введите:  
`http://<FQDN или IPv4-адрес облегченной версии SIEM Server>:15672/#/dynamic-shovels`  
Откроется страница входа в RabbitMQ.
2. Введите логин `siem` и пароль.

**Примечание.** По умолчанию пароль служебной учетной записи – `P@ssword`.

3. Нажмите кнопку **Login**.  
Откроется вкладка **Admin** с таблицей **Dynamic Shovels**.
4. В таблице **Dynamic Shovels** в столбце **Name** нажмите ссылку.
5. В открывшемся окне нажмите кнопку **Delete this shovel**.
6. Повторите шаги 4–5 для всех строк таблицы **Dynamic Shovels**.
7. На сервере с установленной ролью **Deployer** распакуйте архив `SiemServer_<Номер версии>.tar.gz`:  
`tar -xf SiemServer_<Номер версии>.tar.gz`
8. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
9. Начнутся распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
10. Выберите вариант с идентификатором приложения **Ankey SIEM NG**.
11. В открывшемся окне выберите название экземпляра роли **SIEM Server** облегченной версии компонента и нажмите кнопку **ОК**.  
Откроется окно для проверки и изменения параметров установки.
12. Выберите набор параметров **Advanced configuration**.  
Откроется страница с перечнем всех доступных параметров конфигурации.
13. Укажите значения параметров:  
`HostAddress: <FQDN или IPv4-адрес сервера облегченной версии компонента Ankey SIEM NG Server>`  
`TargetSiemRabbitHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server, который получает данные о событиях от облегченной версии компонента>`
14. Установите флажок **SiemOnAgent**.

15. Если Ankey SIEM NG развернут в конфигурации для сверхнагруженных систем, установите флажок **ManagedStorage**.
16. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
17. Нажмите кнопку **ОК**.

Роль обновлена

#### 4.1.13 Обновление компонента Ankey SIEM NG Agent на Linux-like

**Внимание!** Для обновления версий 2.1 и 3.0 компонента до версии 4.0 или выше необходимо удалить существующую роль Agent и установить роль Agent из комплекта поставки в соответствии с инструкцией (см. пункт 3.12.2).

Для обновления компонента необходимо обновить роль Agent. Для обновления роли вам потребуется архив `AgentLinux_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `AgentLinux_<Номер версии>.tar.gz`:  
`tar -xf AgentLinux_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне выберите вариант с названием экземпляра роли Agent.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров.
7. Убедитесь, что в качестве значения параметра `AgentRMQHost` указано полное доменное имя (FQDN) или IPv4-адрес стандартной или облегченной версии Ankey SIEM NG Server – в зависимости от того, для какой версии компонента предназначен Ankey SIEM NG Agent.
8. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **ОК**.

Роль обновлена.



#### 4.1.14 Обновление версий 2.1 и 3.0 компонента Ankey SIEM NG RC

Обновление компонента Ankey SIEM NG RC делится на следующие этапы:

1. Установка модуля Salt Minion (см. пункт 3.19.1).
2. Установка роли RMQ Message Bus.
3. Установка роли Retro Correlator.

##### 4.1.14.1 Обновление компонента Ankey SIEM NG RC: установка роли RMQ Message Bus

Для установки роли вам потребуется архив RmqMessagebus\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив RmqMessagebus\_<Номер версии>.tar.gz:  
tar -xf RmqMessagebus\_<Номер версии>.tar.gz
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
  - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG – выберите этот вариант;
  - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG отсутствует – выберите вариант **Create New Application**.
5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
8. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**. Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**. Откроется страница со списком основных параметров.
10. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG RC.
11. Нажмите кнопку **OK**. Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
12. Нажмите кнопку **OK**.

Роль установлена.

#### 4.1.14.2 Обновление компонента Ankey SIEM NG RC: установка роли Retro Correlator

Для установки роли вам потребуется архив RetroCorrelator\_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив RetroCorrelator\_<Номер версии>.tar.gz:  
`tar -xf RetroCorrelator_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
7. В открывшемся окне введите название экземпляра роли Retro Correlator и нажмите кнопку **OK**.  
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
9. Укажите значения параметров:  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
InternalRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
KBAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091  
SiemServerAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
10. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.  
На сервере Ankey SIEM NG RC в файле `/opt/core-agent/config.json` измените значение параметров `rmq → host` и `rmq → vhost`:  
`"host": "<FQDN или IPv4-адрес сервера Ankey SIEM NG Server>" "vhost": "siem"`
12. Перезапустите службу: `systemctl restart core-agent.service`  
Роль установлена.

#### 4.1.15 Обновление версии 4.0 компонента Ankey SIEM NG RC

Компонент необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем – роль Retro Correlator.

#### 4.1.15.1 Обновление роли *RMQ Message Bus* на сервере *Ankey SIEM NG RC*

Для обновления роли вам потребуется архив `RmqMessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RmqMessagebus_<Номер версии>.tar.gz`:  
`tar -xf RmqMessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения `Ankey SIEM NG`.
5. В открывшемся окне выберите вариант с названием экземпляра роли `RMQ Message Bus`, который установлен на сервер `Ankey SIEM NG RC`.  
Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
7. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера `Ankey SIEM NG RC`.
8. Нажмите кнопку **OK**.  
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.

Роль обновлена.

#### 4.1.15.2 Обновление роли *Retro Correlator*

Для обновления роли вам потребуется архив `RetroCorrelator_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `RetroCorrelator_<Номер версии>.tar.gz`:  
`tar -xf RetroCorrelator_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.  
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения `Ankey SIEM NG`.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

6. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG RC.
7. В открывшемся окне введите название экземпляра роли Retro Correlator и нажмите кнопку **ОК**.  
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.  
Откроется страница со списком основных параметров.
9. Проверьте значения параметров:  
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
InternalRMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG RC>  
CoreAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>  
KBAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091  
SiemServerAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Server>
10. Нажмите кнопку **ОК**.  
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
11. Нажмите кнопку **ОК**.  
Роль обновлена.

## 5 Удаление компонентов из ОС Windows Server

Для удаления компонентов ПК Ankey SIEM NG вы можете использовать стандартные средства Windows Server. При удалении компонентов ПК Ankey SIEM NG вы можете также удалить пользовательские данные.

### *Удаление компонента Ankey SIEM NG стандартными средствами Windows Server*

- ❖ Чтобы удалить компонент Ankey SIEM NG:
  1. В контекстном меню кнопки **Пуск** выберите пункт **Программы и компоненты**.
  2. В списке установленных программ выберите компонент Ankey SIEM NG и нажмите кнопку **Удалить/Изменить**.  
Откроется окно мастера удаления компонента Ankey SIEM NG.
  3. Нажмите кнопку **Удалить**.
  4. Если требуется удалить пользовательские данные, установите флажок **Удалить данные приложений**.
  5. Нажмите кнопку **Удалить**.  
Запустится процесс удаления компонента Ankey SIEM NG.
  6. По завершении удаления нажмите кнопку **Заккрыть**.Компонент Ankey SIEM NG удален.

## 6 Просмотр и изменение параметров конфигурации Ankey SIEM NG

В этом разделе приведены инструкции по просмотру и изменению параметров конфигурации компонентов Ankey SIEM NG. Описания параметров приведены в приложениях Б и В.

### 6.1 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux-like

Конфигурация компонента включает в себя параметры конфигураций ролей, помощью которых компонент был установлен. Для просмотра и изменения конфигурации компонента необходимо просмотреть и изменить конфигурацию той или иной роли.

#### 6.1.1 Просмотр конфигурации роли

- ❖ Чтобы просмотреть конфигурацию роли:
  1. На сервере с установленной ролью Deployer запустите сценарий:  
`/var/lib/deployer/role_packages/<Название роли>/install.sh`
  2. В открывшемся окне нажмите кнопку **Yes**.
  3. В открывшемся окне выберите вариант с идентификатором приложения роли.
  4. В открывшемся окне выберите вариант с названием экземпляра роли.  
Откроется окно для выбора набора параметров.
  5. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
  6. По завершении просмотра нажмите кнопку **Cancel**.
  7. В окне для выбора набора параметров нажмите кнопку **Cancel**.

#### 6.1.2 Изменение конфигурации роли

- ❖ Чтобы изменить конфигурацию роли:
  1. На сервере с установленной ролью Deployer запустите сценарий:  
`/var/lib/deployer/role_packages/<Название роли>/install.sh`
  2. В открывшемся окне нажмите кнопку **Yes**.
  3. В открывшемся окне выберите вариант с идентификатором приложения роли.
  4. В открывшемся окне выберите вариант с названием экземпляра роли.  
Откроется окно для выбора набора параметров.
  5. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
  6. Измените значения параметров.
  7. Нажмите кнопку **OK**.  
Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
  8. Нажмите кнопку **OK**.  
Конфигурация роли изменена.

### 6.1.3 Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch

- ❖ Чтобы изменить объем оперативной памяти:
  1. На сервере с установленной ролью Deployer запустите сценарий:  
`/var/lib/deployer/role_packages/<Название роли SIEM Storage>/install.sh`
  2. В открывшемся окне нажмите кнопку **Yes**.
  3. В открывшемся окне выберите вариант с идентификатором приложения роли.
  4. В открывшемся окне выберите вариант с названием экземпляра роли.  
Откроется окно для выбора набора параметров.
  5. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
  6. Измените значение параметра `ClusterConfigurationProfile` на `Manual`.
  7. В качестве значений параметров `MasterNodeHeapSize`, `ClientNodeHeapSize` и `DataNodeHeapSize` введите объем оперативной памяти, выделяемый для главного узла, клиентского узла и узла данных соответственно.

**Примечание.** Суммарный объем оперативной памяти всех узлов кластера, умноженный на коэффициент 1,7, не должен превышать объем оперативной памяти сервера Ankey SIEM NG ES.

8. Нажмите кнопку **OK**.  
Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.  
Объем оперативной памяти изменен.

### 6.1.4 Изменение степени сжатия данных в Elasticsearch

Elasticsearch позволяет изменять степень сжатия сохраняемых данных за счет использования одного из алгоритмов – LZ4 (по умолчанию) или DEFLATE.

- ❖ Чтобы выбрать алгоритм сжатия данных:
  1. На сервере с установленной ролью Deployer запустите сценарий:  
`/var/lib/deployer/role_packages/<Название роли SIEM Storage>/install.sh`
  2. В открывшемся окне нажмите кнопку **Yes**.
  3. В открывшемся окне выберите вариант с идентификатором приложения роли.
  4. В открывшемся окне выберите вариант с названием экземпляра роли.  
Откроется окно для выбора набора параметров.
  5. Выберите вариант **Advanced configuration**.  
Откроется страница со списком параметров (см. приложение Б).
  6. Измените значение параметра `ElasticsearchCompression`:
    - если вы хотите использовать для сжатия сохраняемых данных алгоритм LZ4, выберите значение `default`;

- если вы хотите использовать для сжатия сохраняемых данных алгоритм DEFLATE, выберите значение best\_compression.
- 7. Нажмите кнопку **ОК**.  
Начнется изменение конфигурации роли.  
По его завершении появится сообщение Deployment configuration successfully applied.
- 8. Нажмите кнопку **ОК**.  
Алгоритм сжатия данных выбран и будет применен к новым индексам.

## 6.2 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Microsoft Windows

Для просмотра и изменения конфигурации компонентов вам потребуются утилиты, которые входят в комплект поставки и включены в дистрибутивы компонентов. После развертывания системы путь к исполняемому файлу утилиты добавляется в переменную окружения PATH.

Таблица 6.1 – Список компонентов и поставляемых с ними утилит

| Компонент            | Утилита          |
|----------------------|------------------|
| Ankey SIEM NG Server | siemcfg.exe      |
| Ankey SIEM NG Agent  | coreagentcfg.exe |

С помощью утилит вы можете просматривать краткое описание параметров конфигурации и их текущие значения. Также вы можете изменять значения параметров двумя способами: вручную вводя названия параметров и их новые значения или указывая путь к XML-файлу с новыми значениями. Утилиты необходимо запускать в интерфейсе командной строки Microsoft Windows от имени администратора.

Таблица 6.2 – Команды утилит Ankey SIEM NG

| Команда | Действие                                                                        |
|---------|---------------------------------------------------------------------------------|
| set     | Ввод значений параметров (соответствующие службы перезапускаются автоматически) |
| get     | Вывод значений параметров (значения выводятся в одинарных кавычках)             |
| list    | Вывод описания параметров                                                       |
| version | Вывод версии компонента                                                         |
| start   | Запуск остановленных служб компонента                                           |
| stop    | Остановка служб компонента                                                      |
| restart | Перезапуск служб компонента                                                     |



### 6.2.1 Просмотр конфигурации

❖ Чтобы просмотреть конфигурацию, выполните команду:  
<Название утилиты> get -p <Название параметра 1> <Название параметра 2> ...  
<Название параметра N>

Например:

```
corecfg get -p PtkbFeatureEnabled PtkbFeatureHost
```

### 6.2.2 Изменение конфигурации вручную

❖ Чтобы изменить конфигурацию вручную, выполните команду:  
<Название утилиты> set -p <Название параметра 1> <Значение параметра 1>  
<Название параметра 2> <Значение параметра 2> ... <Название параметра N>  
<Значение параметра N>

Например:

```
corecfg set -p PtkbFeatureEnabled true PtkbFeatureHost core.example.com
```

### 6.2.3 Изменение конфигурации с помощью XML-файла

❖ Чтобы изменить конфигурацию с помощью XML-файла:

1. Создайте XML-файл в кодировке UTF-8:

```
<?xml version="1.0" encoding="utf-8"?>
<params>
 <param id="Название параметра 1" value="Значение параметра 1" />
 <param id="Название параметра 2" value="Значение параметра 2" />

 <param id="Название параметра N" value="Значение параметра N" />
</params>
```

2. Выполните команду:

```
<Название утилиты> set -f <Путь к XML-файлу>
```

Конфигурация изменена.

## 7 Диагностика и решение проблем

Инструкции по диагностике и решению проблем, возникающих при работе с ПК Ankey SIEM NG, представлены в документе «Руководство администратора Ankey SIEM NG 4.1.2».

Если выполнение указанных в документе шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис».

**Примечание.** Порядок обращения в службу технической поддержки, а также особенности и ограничения услуг технической поддержки представлены в документе «Руководство администратора Ankey SIEM NG 4.1.2».

## Перечень сокращений

AIO	–	All in One – конфигурация ПК Ankey SIEM NG для низконагруженных систем. Все компоненты устанавливаются на одном сервере
API	–	Application Programming Interface – протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого
AVX	–	Advanced Vector Extensions (AVX) – расширение системы команд x86 для микропроцессоров Intel и AMD
CIDR	–	Classless Inter-Domain Routing – бесклассовая адресация
CSV	–	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
DNS	–	Domain Name System – компьютерная распределённая система для получения информации о доменах
EB	–	Модуль Ankey SIEM Next Generation Event Broker
EPS	–	Events Per Second – количество событий в секунду
ES	–	Компонент Ankey SIEM Next Generation Events Storage
FQDN	–	Fully Qualified Domain Name – имя домена, не имеющее неоднозначностей в определении
HDD	–	Hard disk drive – запоминающее устройство
HTTP	–	HyperText Transfer Protocol – протокол передачи гипертекста
HTTPS	–	HyperText Transfer Protocol Secure – расширение протокола HTTP в целях повышения уровня безопасности
ILM	–	Information Lifecycle Management – перемещение информации различного рода и ценности в системе хранения данных (СХД) на основании модифицирующихся требований бизнеса к критериям защищенности и доступности информации с учетом ее ценности, актуальности и оптимизации расходов на ее хранение
IOPS	–	Input/output operations per second – количество операций ввода-вывода в секунду

IP	–	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
KB	–	Knowledge Base – это единая база знаний ПК Ankey SIEM NG
LDAP	–	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегченный вариант разработанного ITU-T протокола DAP
MC	–	Компонент Ankey SIEM NG Management and Configuration
PDQL	–	Язык, разработанный для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в ПК Ankey SIEM NG
PEM	–	Privacy Enhanced Mail Certificate – сертификат, зашифрованный в Base64, широко применяемый как формат категории интернет-файлов
RC	–	Компонент Ankey SIEM NG Retro Correlator
RDP	–	Remote Desktop Protocol – протокол удаленного рабочего стола
RSA	–	Rivest, Shamir и Adleman – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел
RTO	–	Recovery Time Objective – допустимое время восстановления данных
SAN	–	Subject Alternative Name – расширение X.509, позволяющее связать различные значения с сертификатом безопасности с помощью поля subjectAltName
SAS	–	Serial Attached SCSI – последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных
SATA	–	Serial ATA – последовательный интерфейс обмена данными с накопителями информации
SCADA	–	Supervisory Control And Data Acquisition – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления

SHA	–	Secure Hash Algorithm – семейство криптографических хеш-функций
SIEM	–	Security information and event management – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности
SMTP	–	Simple Mail Transfer Protocol – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SOC	–	Security operations center – центр управления безопасностью отвечает за защиту организации от киберугроз
SSD	–	Solid-State Driv – компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти
SSH	–	Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	–	Secure Sockets Layer – криптографический протокол, который подразумевает более безопасную связь
TCP	–	Transmission Control Protocol – протоколов передачи данных интернета
UDP	–	User Datagram Protocol – протокол транспортного уровня
АСУ ТП	–	Автоматизированная система управления технологическим процессом
БД	–	База данных
ИБ	–	Информационная безопасность
ИТ	–	Информационные технологии
ОЗУ	–	Оперативное запоминающее устройство
ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных
ЦС	–	Центр сертификации

## Приложение А Порядок установки ПК Ankey SIEM NG

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в низконагруженной конфигурации представлен на рисунке А.1.

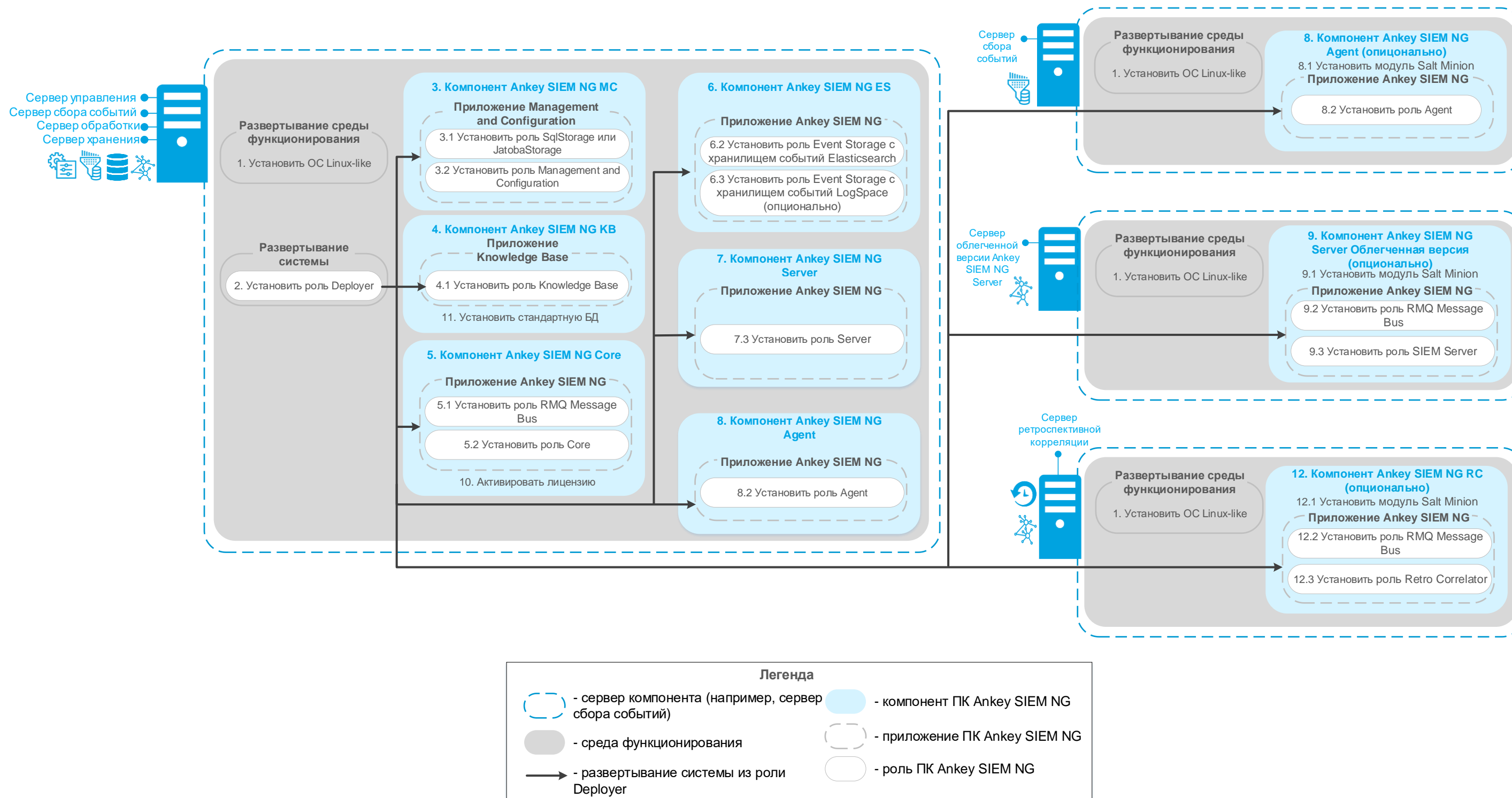


Рисунок А.1 – Алгоритм инсталляции ПК Ankey SIEM NG в низконагруженной конфигурации

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в средненагруженной конфигурации представлен на рисунке А.2.

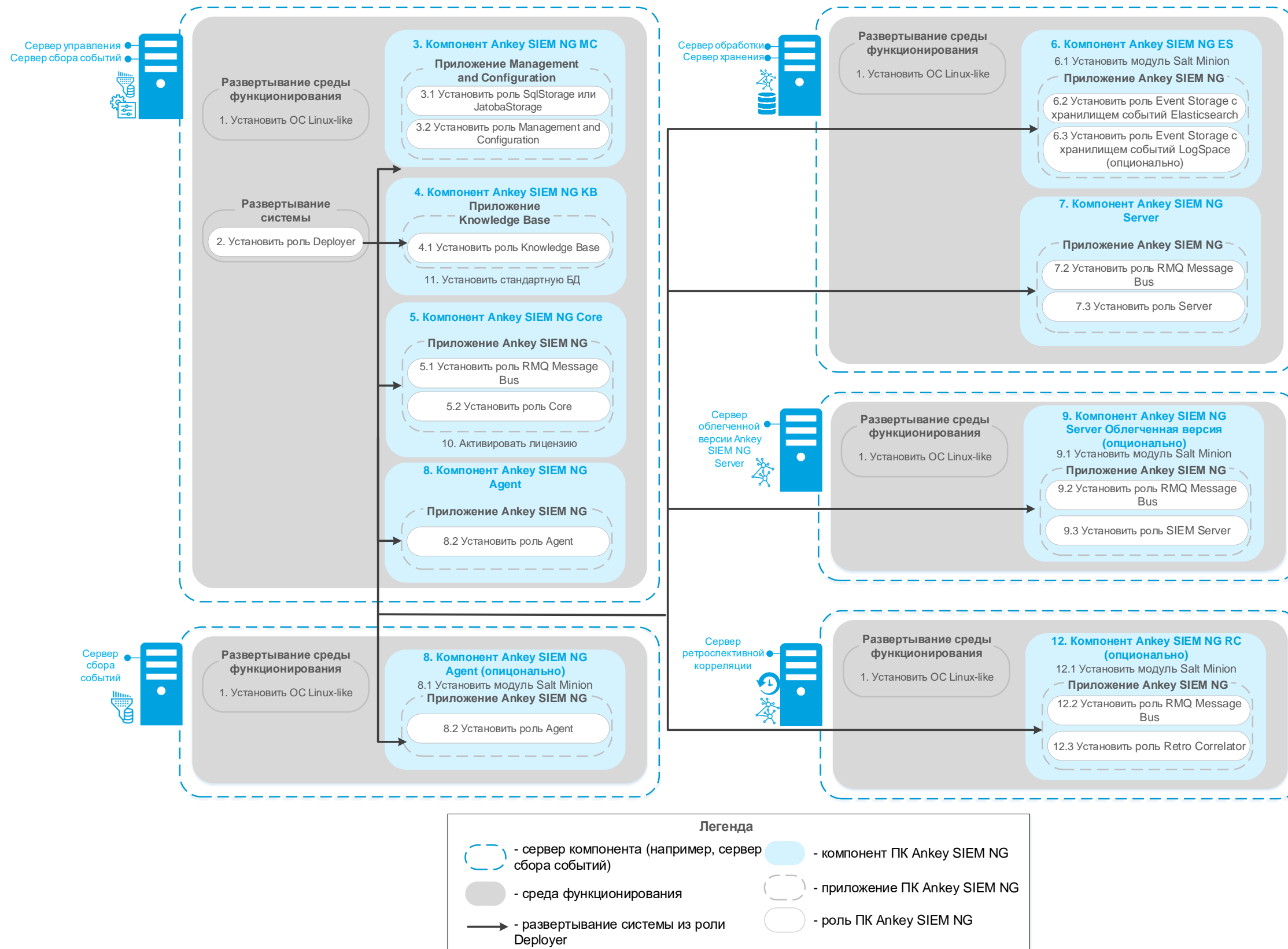


Рисунок А.2 – Алгоритм инсталляции ПК Ankey SIEM NG в средненагруженной конфигурации

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG в высоконагруженной и сверхнагруженной конфигурации представлен на рисунке А.3.

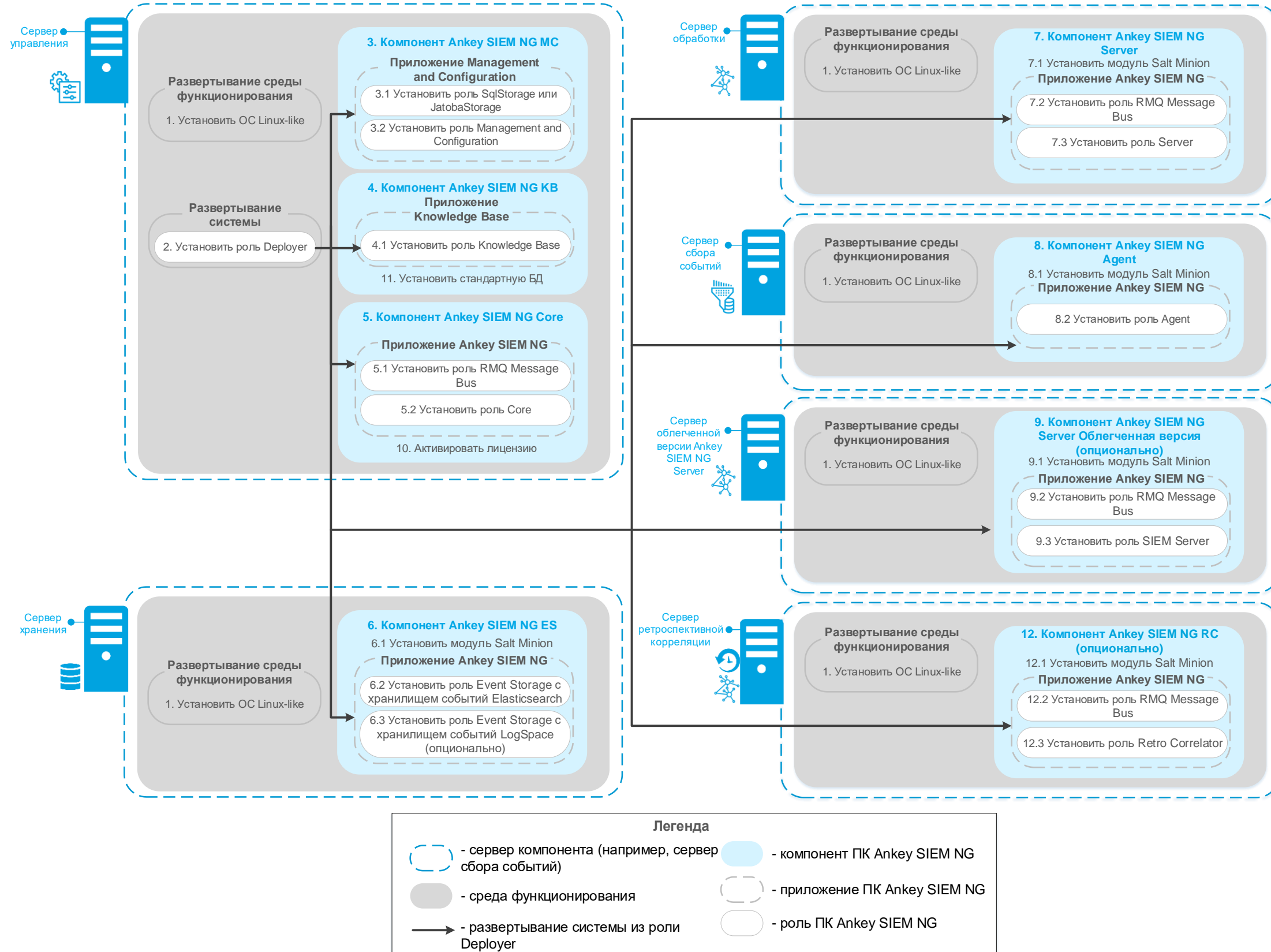


Рисунок А.3 – Алгоритм инсталляции ПК Ankey SIEM NG в высоконагруженной и сверхнагруженной конфигурации



## Приложение Б

### Параметры конфигурации компонентов Ankey SIEM NG на Linux-like

В этом приложении приведены описания параметров и их значения по умолчанию.

Таблица Б.1 – Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	–
RegistryPort	Номер порта для доступа к локальному реестру docker-образов	5000

Таблица Б.2 – Параметры конфигурации роли SqlStorage и JatobaStorage

Параметр	Описание	Значение по умолчанию
<b>Параметры конфигурации роли SqlStorage</b>		
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage	–
PgAdminPort	Порт для доступа к PgAdmin	9001
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
<b>Параметры конфигурации роли JatobaStorage</b>		
HostAddress	IP-адрес или FQDN сервера с установленной ролью JatobaStorage	–
JatobaLicenseActivationType	Тип активации лицензии	online
LicenseEmail	Адрес электронной почты, указанный при получении лицензии	email@email.com

Параметр	Описание	Значение по умолчанию
LicenceKey	Ключ активации лицензии	XXXXX-XXXXX-XXXXX-XXX
LicenceServerUri	Адрес сервера лицензирования Jatoba	https://license.gaz-is.ru/
PgPassword	Пароль служебной учетной записи для доступа к СУБД Jatoba	P@sswordP@ssword
PgPort	Порт для доступа к СУБД Jatoba	5432
PgUser	Логин служебной учетной записи для доступа к СУБД Jatoba	pt_system

Таблица Б.3 – Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service одновременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DefaultLocale	Интерфейс Ankey SIEM NG MC отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG MC	–
IamCookieLifetime	Продолжительность жизни неактивной сессии в Ankey SIEM NG (в часах)	168
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000

Параметр	Описание	Значение по умолчанию
MasterRedirectEnabled	В случае иерархической установки аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
PostgreHost	IP-адрес или FQDN сервера с установленной ролью SqlStorage или JatobaStorage	–
PostgrePassword	Пароль служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	P@sswordP@ssword
PostgreUserName	Логин служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	pt_system
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	–
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	–

**Таблица Б.4 – Параметры конфигурации роли Knowledge Base**

Параметр	Описание	Значение по умолчанию
ClientId	Идентификатор для регистрации приложения Knowledge Base в Ankey SIEM NG MC	ptkb
ClientSecret	Ключ для регистрации приложения Knowledge Base в Ankey SIEM NG MC	secret
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
DefaultLocale	Интерфейс Knowledge Base отображается на русском (ru-RU) или английском (en-US) языке	–
DeploymentType	Тип развертывания Knowledge Base	–
DetectOutOfSyncWithSIEM	Knowledge Base определяет (флажок установлен) или не определяет (флажок снят) отсутствие синхронизации с Ankey	Флажок установлен

Параметр	Описание	Значение по умолчанию
	SIEM NG Server	
DisplayName	Название приложения Knowledge Base в Ankey SIEM NG MC	Knowledge Base
EditableOrigins	Поставщик, атрибуты объектов которого можно изменять	Local
HostAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
ShowDiffObjectId	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
SiemAddress	IP-адрес или FQDN сервера Ankey SIEM NG Server	localhost

Параметр	Описание	Значение по умолчанию
SiemPort	Порт сервера Ankey SIEM NG Server для входящих подключений от Knowledge Base	8013
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	–
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25
SmtpSender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtpUseDefaultCredentials	Режим аутентификации SMTP-сервера: флажок установлен – для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtpUser и SmtpPassword); флажок снят – для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword	Флажок установлен
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	–
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Таблица Б.5 – Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
ConsiderEventsImportance	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)	Флажок установлен
DefaultAssetTtl	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	90.00:00:00

Параметр	Описание	Значение по умолчанию
DefaultLocale	Интерфейс Ankey SIEM NG отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на SMTP-сервер	10
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
IncidentAggregationTimeout	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	00:01:00
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	P@sswordP@ssword
PostgreUserName	Логин служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	–
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в Ankey SIEM NG Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O

Параметр	Описание	Значение по умолчанию
RMQsslCertPath	Путь к файлу SSL-сертификата RabbitMQ	RMQ_Core_Client.p12
RMQsslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	mpx_core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SaltMasterHost	IP-адрес или FQDN сервера с модулем Salt Master	–
SaltMasterPort	Порт сервера с модулем Salt Master для входящих подключений от Ankey SIEM NG Core	9035
Smtphost	IP-адрес или FQDN SMTP-сервера	localhost
Smtppassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу	–
Smtpport	Порт SMTP-сервера для входящих подключений от Ankey SIEM NG Core	25
Smtpsender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
Smtuser	Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу	–
Ttlcheckperiod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00

Таблица Б.6 – Параметры конфигурации роли Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	–
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode1	–



Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Agent
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ. <b>Примечание.</b> Брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG	localhost
AgentRMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
AgentRMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt
Agent_RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен

Параметр	Описание	Значение по умолчанию
Agent_RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key

Таблица Б.7 – Параметры конфигурации роли SIEM Storage

Параметр	Описание	Значение по умолчанию
BindHost	IP-адрес или FQDN сетевых интерфейсов сервера Ankey SIEM NG ES. <b>Примечание.</b> Elasticsearch обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы	0.0.0.0
ClientNodeHeapSize	Объем оперативной памяти, выделяемый для клиентского узла (в гигабайтах). <b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант <i>Manual</i> в качестве значения параметра <i>ClusterConfigurationProfile</i>	16g
ClusterConfigurationProfile	Объем оперативной памяти, выделяемый каждому типу узлов кластера Elasticsearch. Для выбора доступны следующие варианты: – <i>AIO</i> – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для низконагруженных систем; – <i>SIEMandStorage</i> – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для средненагруженных систем;	Standalone

Параметр	Описание	Значение по умолчанию
	<p>– Standalone – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для высоконагруженных систем;</p> <p>– ManagedStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для сверхнагруженных систем;</p> <p>– Manual – ввод значений вручную (параметры DataNodeHeapSize, ClientNodeHeapSize, MasterNodeHeapSize)</p>	
DataNodeHeapSize	<p>Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах).</p> <p><b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile</p>	30g
HighLoad	Кластер Elasticsearch содержит два (флажок снят) или четыре (флажок установлен) узла данных	Флажок снят
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG ES	–
MasterNodeHeapSize	<p>Объем оперативной памяти, выделяемый для главного узла (в гигабайтах).</p> <p><b>Примечание.</b> Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile</p>	16g
PathData	Путь к индексам Elasticsearch. Если Ankey SIEM NG развернут для сверхнагруженных систем – путь к индексам, находящимся в "теплой" стадии	/data
PathDataHot	Путь к индексам, находящимся в "горячей" стадии	/datahot
PathLog	Путь к файлам журналов	/es_logs

Параметр	Описание	Значение по умолчанию
PathRepo	Путь к резервным копиям индексов	/es_backup <sup>28</sup>
RotateCount	Максимальное количество файлов журналов для компонентов сторонних производителей	10
RotateSize	Максимальный размер файла журнала для компонентов сторонних производителей (G для гигабайтов, M для мегабайтов, k для килобайтов)	200M
SetRecomendedDiskScheduler	Для операций ввода-вывода ядро Debian использует планировщик по умолчанию (флажок снят) или планировщик deadline (флажок установлен)	Флажок установлен
TailcutterDbSPACE	Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)	92%
TailcutterLog	Путь к файлу журнала утилиты tailcutter	/opt/estools/log/tailcutter.log
TailcutterLogLevel	Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)	WARNING
TailcutterTtl	Срок хранения индексов для событий (в днях)	365
TailcutterTtlc	Срок хранения индексов для счетчиков событий (в днях)	7

Таблица Б.8 – Параметры конфигурации роли SIEM Server

Параметр	Описание	Значение по умолчанию
AssetResolverPort	Порт сервера Ankey SIEM NG Core для подключения службы SIEM Server assets resolution	8721
AUTH_KEY	Путь к файлу закрытого ключа сертификата для аутентификации Ankey SIEM NG Server в Ankey SIEM NG MC	/opt/siem/etc/authKey.pem

<sup>28</sup> При инсталляции можно задать пользовательское наименование каталога (например: /data\_archive). Подробнее см. пункт 3.10.2.

Параметр	Описание	Значение по умолчанию
ClusterSeedHost	IP-адрес или FQDN сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	–
ClusterSeedPort	Порт сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	9300
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CorePort	Порт сервера Ankey SIEM NG Core для подключения Ankey SIEM NG Server	8799
CoreRabbitAuthMethod	Аутентификация Ankey SIEM NG Server в брокере RabbitMQ выполняется с помощью логина и пароля (plain) или с помощью сертификатов безопасности (ssl).  <b>Примечание.</b> Этот брокер устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG	ssl
CoreTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)	16384
CorrTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых данными об активах, справочной информацией (в мегабайтах)	4096
CounterRefreshInterval	Период обновления данных о счетчиках производительности (в секундах)	60
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG Server (возможные значения – fatal, error, warn, info, debug или trace)	info

Параметр	Описание	Значение по умолчанию
ElasticsearchAggregationQuery Timeout	Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)	600
ElasticsearchAggregationResponse Timeout	Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)	600
ElasticsearchAggregationSize	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	1000
ElasticsearchAPIVersion	Версия API, используемая для взаимодействия с Elasticsearch	7.4
ElasticsearchCompression	Алгоритм сжатия данных, используемый в Elasticsearch	default
ElasticsearchCountersLimit	Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (0 – количество получаемых записей не ограничено)	0
ElasticsearchDefaultQueryTimeout	Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)	600
ElasticsearchDefaultResponse Timeout	Тайм-аут выполнения запроса фильтрации событий (в секундах)	600
ElasticsearchHost	IP-адрес или FQDN сервера Ankey SIEM NG ES	localhost
ElasticsearchMaxReplySize	Максимальный размер ответа от Elasticsearch (в байтах)	524288000
EnriTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)	8192
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	0.0.0.0

Параметр	Описание	Значение по умолчанию
GlobalRabbitHost	IP-адрес или FQDN сервера RabbitMQ. <b>Примечание.</b> Этот брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Server и обеспечивает обмен сообщениями между службами Ankey SIEM NG Server	127.0.0.1
GlobalRabbitPort	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Core	5672
HighLoad	Для службы SIEM server storage выделено шесть (флажок установлен) или четыре (флажок снят) потока операционной системы	Флажок снят
LogCount	Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов Ankey SIEM NG Server	2
LogSize	Максимальный размер файла журнала Ankey SIEM NG Server (в байтах)	104857600
LogSpaceHost	IP-адрес или FQDN сервера Ankey SIEM NG ES	localhost
ManagedStorage	Для управления жизненным циклом индексов Elasticsearch используется (флажок установлен) или не используется (флажок снят) технология ILM	Флажок снят
MonitoringOomEnabled	Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)	Флажок установлен
MonitoringOomMemoryLimit	Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)	60
MonitoringOvertriggerEnabled	Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)	Флажок установлен

Параметр	Описание	Значение по умолчанию
MonitoringOvertriggerPeriod	Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)	3600
MonitoringOvertriggerThreshold	Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила	300
ProtectedRulesPath	Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)	–
RemoteEventsSkipAggregator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) агрегацию реплицированных событий	Флажок установлен
RemoteEventsSkipCorrelator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) корреляцию реплицированных событий	Флажок установлен
RemoteEventsSkipEnricher	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) обогащение реплицированных событий	Флажок установлен
RemoteEventsSkipResolver	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) привязку реплицированных событий к активам	Флажок установлен
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	/opt/siem/etc/rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	/opt/siem/etc/ RMQ_SIEM_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	/opt/siem/etc/ RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохраняются (флажок установлен) или не сохраняются (флажок снят) после перезагрузки брокера	Флажок установлен



Параметр	Описание	Значение по умолчанию
RMQHost	IP-адрес или FQDN сервера RabbitMQ. <b>Примечание.</b> Этот брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Server к брокеру RabbitMQ	P@ssword
RMQPort	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Server при аутентификации с помощью логина и пароля (plain)	5672
RMQPortSSL	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG Server при аутентификации с помощью сертификатов безопасности (ssl)	5671
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Server к брокеру RabbitMQ	siem
RMQVirtualHost	Имя виртуального узла RabbitMQ для подключения Ankey SIEM NG Server	mpx
RowBatchSize	Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM Server frontend из службы (в службу) SIEM Server commander	5000
SiemOnAgent	Установлена облегченная (флажок установлен) или стандартная (флажок снят) версия Ankey SIEM NG Server	Флажок снят
StatsPublishPeriod	Период обновления данных, отображаемых в рабочей области главной страницы Ankey SIEM NG (в секундах)	30
StorageBackendType	В качестве хранилища событий используется Elasticsearch или LogSpace	elasticsearch
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (флажок установлен) или без него (флажок снят)	Флажок установлен

Параметр	Описание	Значение по умолчанию
StoreUnnormalizedRaw	Ненормализованные события хранятся (флажок установлен) или не хранятся (флажок снят) в системе	Флажок установлен
TableListsRestorePolicy	Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestorер. Для выбора доступны следующие варианты: <ul style="list-style-type: none"> <li>– disabled – автоматическое восстановление выключено;</li> <li>– fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери;</li> <li>– best_effort – в процессе восстановления допустима потеря одной-двух последних записей;</li> <li>– robust – в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы)</li> </ul>	best_effort
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица Б.9 – Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
CACertFile	Путь к файлу корневого сертификата	rootCA.crt
CertFile	Путь к файлу публичного сертификата	RMQ_Server.crt
HostAddress	IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus	–
KeyFile	Путь к файлу закрытого ключа сертификата	RMQ_Server.pem
MEMORY_HIGH_WATERMARK	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах).  <b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10

Параметр	Описание	Значение по умолчанию
RMQAdminPassword	Пароль служебной учетной записи администратора RabbitMQ	P@ssword
RMQAdminUser	Логин служебной учетной записи администратора RabbitMQ	Administrator
RMQAgentPassword	Пароль служебной учетной записи для доступа агентов к RabbitMQ	P@ssword
RMQAgentUser	Логин служебной учетной записи для доступа агентов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671
RMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSiemPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ	P@ssword
RMQSiemUser	Логин служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ	siem
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
RMQ_DISK_FREE_LIMIT	<p>Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах).</p> <p><b>Примечание.</b> Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений</p>	20

Параметр	Описание	Значение по умолчанию
WATERMARK_PAGING_RATIO	<p>Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK).</p> <p><b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск</p>	0.5

Таблица Б.10 – Параметры конфигурации роли Retro Correlator

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	–

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG RC
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
AgentRMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
AgentRMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	rootCA.crt
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt

Параметр	Описание	Значение по умолчанию
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG RC (возможные значения – fatal, error, warn, info, debug или trace)	info
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG RC	localhost
InternalRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
InternalRMQPassword	Пароль служебной учетной записи для доступа к RabbitMQ	P@ssword
InternalRMQPort	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью логина и пароля (plain)	5672
InternalRMQPortSSL	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью сертификатов безопасности (ssl)	5671
InternalRMQUser	Логин служебной учетной для доступа к RabbitMQ	siem
InternalRMQVirtualHost	Имя виртуального узла RabbitMQ	/
KBAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
LogCount	Максимальное количество файлов журналов Ankey SIEM NG RC (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов Ankey SIEM NG RC	2

Параметр	Описание	Значение по умолчанию
LogSize	Максимальный размер файла журнала Ankey SIEM NG RC (в байтах)	104857600
MaxTableListsSize	Максимальный объем оперативной памяти, выделяемый для хранения табличных списков (в мегабайтах)	8192
RetroControllerHost	IP-адрес для входящих подключений от агента на Debian	0.0.0.0
SiemServerAddress	IP-адрес или FQDN сервера Ankey SIEM NG Server	localhost

## Приложение В

### Параметры конфигурации компонентов Ankey SIEM NG на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов Ankey SIEM NG на Microsoft Windows.

Таблица В.1 – Параметры конфигурации компонента Ankey SIEM NG Server

Параметр	Описание	Значение по умолчанию
AUTH_KEY	Путь к файлу закрытого ключа сертификата для аутентификации Ankey SIEM NG Server в Ankey SIEM NG MC	C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\config\Pk\authKey.pem
ClusterSeedHost	IP-адрес или FQDN сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	–
ClusterSeedPort	Порт сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	9300
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CorePort	Порт сервера Ankey SIEM NG Core для входящих подключений от Ankey SIEM NG Server	8799
CoreRabbitAuthMethod	Аутентификация Ankey SIEM NG Server в RabbitMQ выполняется с помощью логина и пароля (plain) или с помощью сертификатов безопасности (ssl)	ssl
CoreTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)	16384
CorrRegister	Служба SIEM Server correlator запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)	True
CorrTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых данными об активах, справочной информацией и данными от репутационных сервисов (в мегабайтах)	4096
CounterRefreshInterval	Период обновления данных о счетчиках производительности (в секундах)	60



Параметр	Описание	Значение по умолчанию
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG Server (возможные значения – fatal, error, warn, info, debug или trace)	info
ElasticsearchAggregationQueryTimeout	Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)	600
ElasticsearchAggregationResponseTimeout	Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)	600
ElasticsearchAggregationSize	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	1000
ElasticsearchAPIVersion	Версия API, используемая для взаимодействия с Elasticsearch	7.4
ElasticsearchCompression	Алгоритм сжатия данных, используемый в Elasticsearch	default
ElasticsearchCountersLimit	Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (0 – количество получаемых записей не ограничено)	0
ElasticsearchDefaultQueryTimeout	Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)	600
ElasticsearchDefaultResponseTimeout	Тайм-аут выполнения запроса фильтрации событий (в секундах)	600
ElasticsearchHost	IP-адрес или FQDN сервера Ankey SIEM NG ES	localhost
ElasticsearchMaxReplySize	Максимальный размер ответа от Elasticsearch (в байтах)	524288000
EnriTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)	8192
EnrRegister	Служба SIEM Server enricher запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)	True
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60

Параметр	Описание	Значение по умолчанию
EventsCaseSensitiveSearch	<p>Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False).</p> <p><b>Примечание.</b> Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения</p>	False
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	127.0.0.1
GlobalRabbitHost	<p>IP-адрес или FQDN сервера RabbitMQ.</p> <p><b>Примечание.</b> В конфигурации для низконагруженных систем брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG, а также между службами Ankey SIEM NG Server</p>	127.0.0.1
GlobalRabbitPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Core	5672
LogCount	Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов Ankey SIEM NG Server	2
LogSize	Максимальный размер файла журнала Ankey SIEM NG Server (в байтах)	104857600
MonitoringOomEnabled	Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (True) или не выполняется (False)	True
MonitoringOomMemoryLimit	Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)	60

Параметр	Описание	Значение по умолчанию
MonitoringOvertriggerEnabled	Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (True) или не выполняется (False)	True
MonitoringOvertriggerPeriod	Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)	3600
MonitoringOvertriggerThreshold	Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила	300
ProtectedRulesPath	Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)	-
RemoteEventsSkipAggregator	Площадка-получатель выполняет (False) или не выполняет (True) агрегацию реплицированных событий	True
RemoteEventsSkipCorrelator	Площадка-получатель выполняет (False) или не выполняет (True) корреляцию реплицированных событий	True
RemoteEventsSkipEnricher	Площадка-получатель выполняет (False) или не выполняет (True) обогащение реплицированных событий	True
RemoteEventsSkipResolver	Площадка-получатель выполняет (False) или не выполняет (True) привязку реплицированных событий к активам	True
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey SIEMNGServer\install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey SIEM NGServer\install\scripts\Certificates\RMQ_SIEM_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey

Параметр	Описание	Значение по умолчанию
		SIEM NG Server\install\scripts\Certificates\RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохраняются (True) или не сохраняются (False) после перезагрузки брокера	True
RMQHost	IP-адрес или FQDN сервера RabbitMQ.  <b>Примечание.</b> В конфигурации для низконагруженных систем брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG, а также между службами Ankey SIEM NG Server	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Server к RabbitMQ	P@ssword
RMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Server при аутентификации с помощью логина и пароля (plain)	5672
RMQPortSSL	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Server при аутентификации с помощью сертификатов безопасности (ssl)	5671
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Server к RabbitMQ	siem
RMQVirtualHost	Имя виртуального узла RabbitMQ для подключения Ankey SIEM NG Server	mpx
RoutRegister	Служба SIEM Server router запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)	True
RowBatchSize	Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM Server frontend из службы (в службу) SIEM Server commander	5000

Параметр	Описание	Значение по умолчанию
SiemOnAgent	Установлена облегченная (True) или стандартная (False) версия Ankey SIEM NG Server	False
StatsPublishPeriod	Период обновления данных, отображаемых в рабочей области главной страницы Ankey SIEM NG	30
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (True) или без него (False)	True
StoreUnnormalizedRaw	Ненормализованные события хранятся (True) или не хранятся (False) в системе	True
TableListsRestorePolicy	Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestorer. Вы можете указать следующие значения: – disabled – автоматическое восстановление выключено; – fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери; – best_effort – в процессе восстановления допустима потеря одной-двух последних записей; – robust – в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы)	best_effort
TailcutterDbSPACE	Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)	92%
TailcutterLog	Путь к файлу журнала утилиты tailcutter	C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\log\tailcutter.log
TailcutterLogLevel	Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)	WARNING
TailcutterTtl	Срок хранения индексов для событий (в днях)	365

Параметр	Описание	Значение по умолчанию
TailcutterTtlc	Срок хранения индексов для счетчиков событий (в днях)	7
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица В.2 – Параметры конфигурации компонента Ankey SIEM NG Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	20480M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	-

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Agent
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\Program Files (x86)\Gazinformservice\Ankey SIEM NGAgent\install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\Program Files (x86)\Gazinformservice\Ankey SIEM NGAgent\install\scripts\Certificates\RMQ_Agent_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\Program Files(x86)\Gazinformservice\Ankey SIEM NG Agent\install\scripts\Certificates\RMQ_Agent_Client.key
RMQHost	IP-адрес или FQDN сервера RabbitMQ. Примечание. Брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	P@ssword

Параметр	Описание	Значение по умолчанию
RMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	mpx_agent
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SSLEnabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение	True



## Приложение Г

### Рекомендуемые конфигурации для систем хранения событий информационной безопасности

Для размещения данных может использоваться одновременно несколько систем долговременного хранения. Рекомендуется отделить хранилище для событий в оперативном доступе от хранилища для архивных событий. Для обработки и хранения событий в оперативном доступе требуются высокопроизводительные твердотельные накопители. Для обработки и хранения архивных событий допустимо использовать менее производительные жесткие диски.

Для оперативного хранилища событий критичными параметрами являются:

- скорость операций случайной записи;
- скорость операций случайного чтения.

Для архивного хранилища событий критичным параметром является скорость операций последовательного чтения.

Поддерживаемые конфигурации при взаимодействии с внешними системами/устройствами хранения представлены в таблице Г.1.

Таблица Г.1 – Поддерживаемые конфигурации при взаимодействии с внешними системами/устройствами хранения

Тип массивов данных	Тип файловых систем для хранения	Тип жестких дисков	Возможные конфигурации и RAID	Рекомендуемый резерв дисков
Direct Attached Storage; Network Attached Storage; Storage Area Network	ext4	HDD (10000 об./мин.)/ (15000 об./мин.)	RAID 10 RAID 6***	1 Hot Spare**
		SSD*	RAID 5 RAID 6 RAID 1	
<p>* Рекомендуемая конфигурация RAID6+1HS. При необходимости могут применяться массивы RAID 10, RAID 50, RAID 60 аналогично HDD для обеспечения повышенной производительности в соответствии с проектными решениями.</p> <p>** Количество дисков в горячем резерве может быть увеличено в соответствии с проектными решениями.</p> <p>*** Применять RAID 6 HDD только для хранения архивных событий ПК. Для событий в оперативном доступе необходимо использовать HDD RAID 10.</p>				

Порядок подключения, отключения и эксплуатации определяется в документации, поставляемой совместно с оборудованием определенного типа в виде системы либо устройства хранения.

## Приложение Д

### Установка модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных)

**Примечание.** Номер версии<sup>29</sup> дополнительных коннекторов Ankey SIEM NG и пакетов контента Ankey SIEM NG имеет формат А.В.С, где А – минимально поддерживаемая версия платформы Ankey SIEM NG, В – мажорная версия изделия, С – минорная версия изделия. Например: 4.2.1.

**Примечание.** Дополнительные контент и коннекторы версии 3.x совместимы с платформой ПК Ankey SIEM NG 4.x.

#### Д.1 Установка дополнительных модулей сбора и обработки данных

Модули сбора и обработки данных (далее также – коннекторы ПК Ankey SIEM NG) предназначены для интеграции ПК Ankey SIEM NG с источниками событий. Посредством коннекторов обеспечивается предварительная обработка событий на сервере обработки Ankey SIEM NG с помощью правил нормализации. Предварительная обработка осуществляется в целях приведения структуры событий источников к единому формату ПК Ankey SIEM NG. Правила нормализации выполняют первичную обработку событий (парсинг, маппинг) и категоризацию (обогащение сведений категориями для последующей корреляционной и аналитической обработки). После обработки события передаются на сервер хранения Ankey SIEM NG.

В ПК Ankey SIEM NG предусмотрены следующие типы коннекторов:

- стандартные коннекторы, предназначенные для интеграции ПК Ankey SIEM NG со стандартными источниками событий<sup>30</sup>;

**Внимание!** Установка стандартных коннекторов Ankey SIEM NG описана в «Руководстве по установке Ankey SIEM NG 4.1.2» в подразделе 3.18. Настройка сбора событий от стандартных источников в Ankey SIEM NG описана в «Руководстве по интеграции с источниками Ankey SIEM NG 4.1.2».

- дополнительные коннекторы, предназначенные для интеграции ПК Ankey SIEM NG с нестандартными источниками событий<sup>31</sup>, которые не поддерживаются

<sup>29</sup> Для определения версии установленного коннектора и контента см. документ «Руководство администратора Ankey SIEM NG 4.1.2».

<sup>30</sup> Список поддерживаемых стандартных источников приведен в документе «Обзор новых возможностей Ankey SIEM NG 4.1.2».

<sup>31</sup> Список поддерживаемых нестандартных источников приведен в документе «Руководство по интеграции с источниками Ankey SIEM NG 4.1.2».

платформой Ankey SIEM NG (не являются «коробочным» решением).

Для установки дополнительного коннектора Ankey SIEM NG необходимо:

- импортировать в систему файл дополнительного коннектора Ankey SIEM NG;
- установить коннектор Ankey SIEM NG в папке **Пакет дополнительных коннекторов**;
- выполнить настройку профиля;
- создать задачу для организации сбора событий.

**Внимание!** Детализация и особенности установки и настройки сбора событий от нестандартных источников в Ankey SIEM NG описана в документации на использование дополнительных коннекторов, которая поставляется в рамках приобретения таких изделий.

## Д.2 Установка дополнительных модулей выявления нарушений ИБ (корреляционной обработки данных)

Модули выявления нарушений ИБ (корреляционной обработки данных) (далее также – контент ПК Ankey SIEM NG) – это набор взаимосвязанных инструментов ПК Ankey SIEM NG (правила обогащения, правила агрегации, правила локализации, правила корреляции, макросы и табличные списки), предназначенный для автоматизации процесса предупреждения, обнаружения и реагирования на инциденты ИБ.

В ПК Ankey SIEM NG предусмотрены следующие пакеты контента:

1. Стандартные пакеты контента, которые входят в комплект поставки ПК Ankey SIEM NG:
  - пакет общих ресурсов контента – коробочный набор ресурсов для корреляции и анализа данных, содержит общие макросы, общие табличные списки, общие правила обогащения и набор корреляционных правил для всех типов источников, необходимых для работы верхнеуровневых пакетов контента;

**Внимание!** Установка пакета общих ресурсов контента Ankey SIEM NG описана в «Руководстве по установке Ankey SIEM NG 4.1.2» в подразделе 3.18. Настройка пакета общих ресурсов контента Ankey SIEM NG в Ankey SIEM NG описана в документе «Пакет общих ресурсов контента <Номер версии пакета>. Описание».

2. Дополнительные пакеты контента (не являются «коробочным» решением):
  - инфраструктурный пакет контента – наборы инструментов мониторинга и выявления инцидентов для различных типов источников;

- пакет мониторинга ПО SCADA – наборы инструментов мониторинга и выявления инцидентов для источников событий типа АСУ ТП;
- пакет мониторинга SOC – наборы инструментов мониторинга и выявления инцидентов для выявления распределенных атак на различные дочерние общества, функционирует на верхнем уровне иерархии ПК Ankey SIEM NG;
- пакет мониторинга SIEM – наборы инструментов мониторинга и выявления инцидентов для автоматизации процесса обнаружения подозрений на инциденты ИБ. Пакет функционирует на событиях внутреннего аудита ПК Ankey SIEM NG и предназначен для выявления воздействия на ключевые ресурсы платформы со стороны пользователей и системы.

Для установки дополнительного пакета контента Ankey SIEM NG необходимо выполнить действия из подраздела Д.2.1.

## Д.2.1 Установка и удаление дополнительного пакета контента в Ankey SIEM NG

После создания корневой базы данных и пользовательской ветки, создание которых представлено в подразделе 3.18, пункт **Пакеты экспертизы** раздела **SIEM** приложения **Knowledge Base** примет вид<sup>32</sup>, представленный на рисунке Д.1.

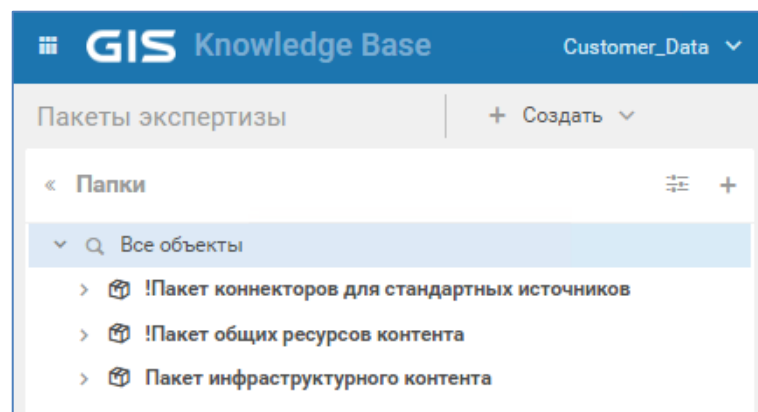


Рисунок Д.1 – Облик пользовательской ветки Customer\_Data


Для нормализации и последующей корреляции событий, объекты Knowledge Base необходимо:

- валидировать;
- установить в SIEM.

Валидация – это проверка объекта на предмет соответствия синтаксису языка XPR, а также наличия всех необходимых зависимостей от других ресурсов (например, табличных списков и макросов). О том, что объект не валидирован




<sup>32</sup> Состав пакетов может отличаться.

свидетельствует значок .

Объекты Knowledge Base не задействуются в процессах нормализации и корреляции событий автоматически. Для применения правил к потоку событий с источников необходимо произвести их установку в SIEM. О том, что объект не установлен в SIEM свидетельствует красный значок  или его отсутствие.

Пример не валидированного и не установленного в конвейер объекта приведен на рисунке Д.2.

Правило предназначено для обнаружения событий удаления файлов, которые запрещены к удалению. Табличный список конфигурации: "COMMON\_Files\_Forbidden". Табличный список исключений: "COMMON\_Tracking\_Exceptions".

Системное название	TTS_35_Deleting_Files_Prohibited_For_Deletion
Идентификатор	GIS-CR-100800193
Тип	 Стандартный
Поставщик	GIS
Папка	!Пакет общих ресурсов контента/Правила корреляции и/Подмена или фальсификация информации
Наборы для установки	Актуальный набор ресурсов SIEM
Статус валидации	
Статус установки	





№...	С...	Идентификатор	Системное название	Описание	Тип	
1		GIS-CR-100800193	TTS_35_Deleting_Files_Prohibited_For_Deletion	Правило предназначено для обнаружения событий удал...		

Рисунок Д.2 – Пример не установленного и не валидированного объекта

Для валидации и установки объектов в конвейер необходимо использовать функционал наборов для установки. Наборы для установки – это особый метод группировки объектов Knowledge Base, созданный чтобы упростить процессы валидации и установки. В наборы могут входить любые стандартные и пользовательские ресурсы из разных пакетов экспертизы и папок.

Процесс создания наборов для установки подробно описан в документе «Руководство оператора Ankey SIEM NG 4.1.2».

❖ Для валидации объектов необходимо выполнить следующие действия:

1. В правом верхнем углу на панели инструментов выбрать инструмент **Валидация**, как показано на рисунке Д.3.

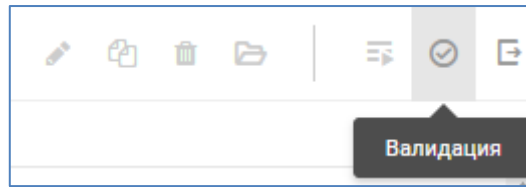


Рисунок Д.3 – Инструмент Валидация


2. В открывшемся окне выбрать **Все объекты из Knowledge Base** (или **Объекты из набора для установки**, или **Только <название\_объекта>**) и запустить процесс валидации нажатием кнопки **Запустить валидацию**.
  3. После успешного завершения процесса, статус валидации всех объектов изменится. О том, что объект валидирован свидетельствует значок .
- ❖ Для установки объектов в конвейер необходимо выполнить следующие действия:
1. В верхней части страницы на панели инструментов выбрать инструмент **Установить в SIEM**, как показано на рисунке Д.4.



Рисунок Д.4 – Инструмент Установить в SIEM

2. В открывшемся окне отметить галочкой необходимый конвейер и запустить процесс установки нажатием кнопки **Запустить установку**, как показано на рисунке Д.5

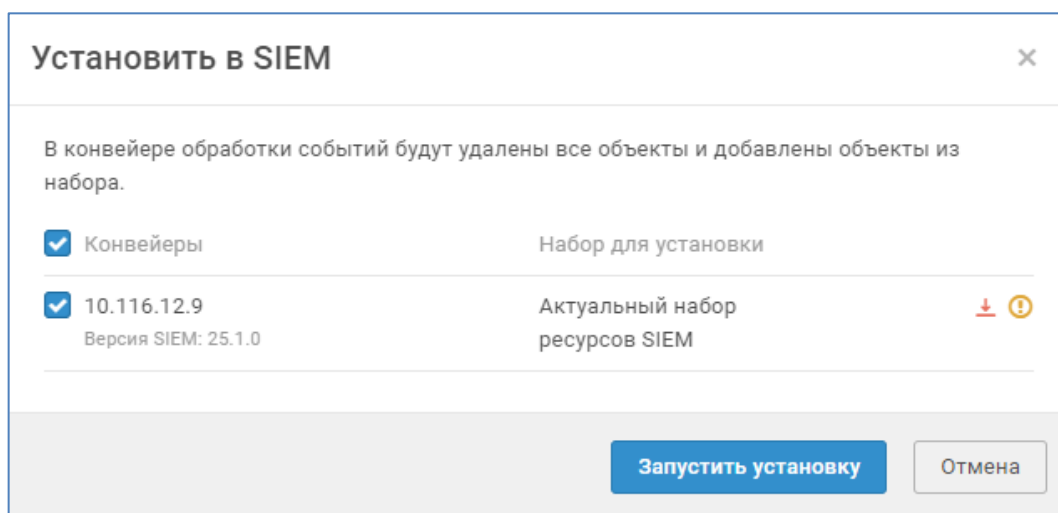



Рисунок Д.5 – Окно установки объектов в конвейер

3. После успешного завершения процесса, статус установки объектов изменится. О том, что объект установлен в конвейер свидетельствует значок .

**Внимание!** При выполнении указанных действий для объектов из набора для установки валидации и установке подвергается именно состав ресурсов в наборе. В случае ошибок, связанных с отсутствием необходимых объектов, следует убедиться, что в наборе для установки учтены все зависимости между ресурсами.

❖ Для удаления объектов из конвейера необходимо выполнить следующие действия:

1. Выбрать необходимые ресурсы и в правом верхнем углу на панели инструментов выбрать инструмент **Наборы для установки**, как показано на рисунке Д.6.

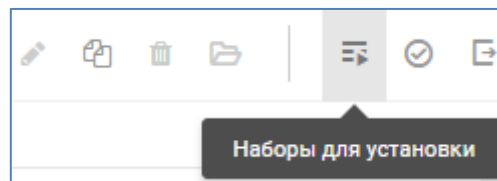


Рисунок Д.6 – Инструмент Наборы для установки

2. В открывшемся окне снять галочку принадлежности к набору для установки, который привязан к конвейеру, из которого следует удалить объекты, как показано на рисунке Д.7.

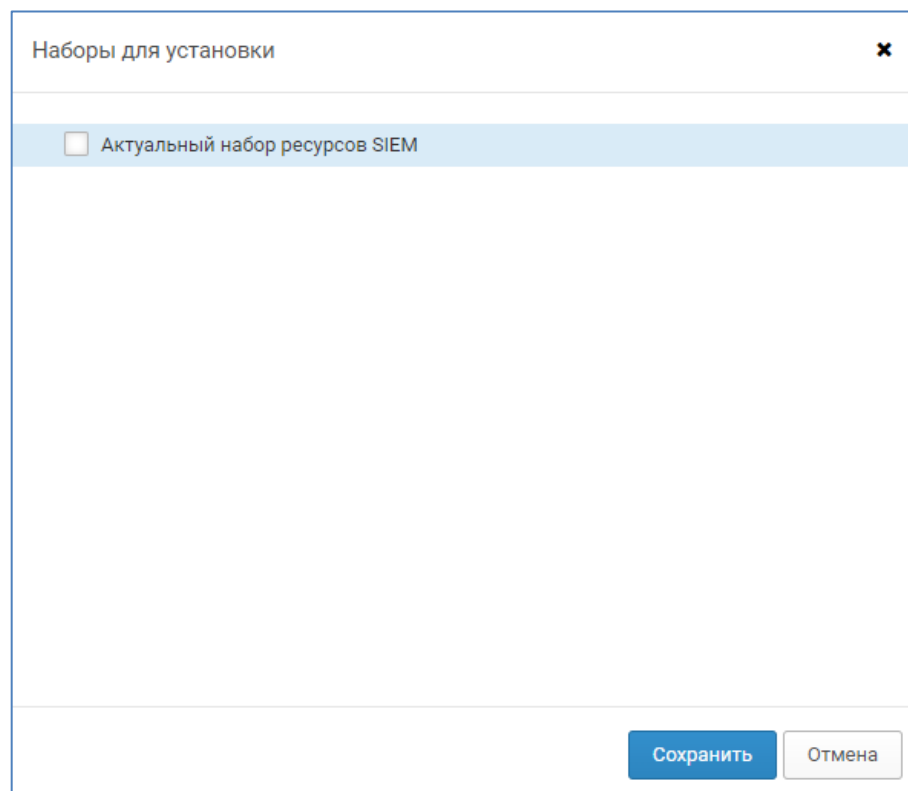


Рисунок Д.7 – Окно выбора наборов для установки

3. Установить объекты в конвейер, как было описано ранее.

**Внимание!** Удаление из конвейера не подразумевает удаление объектов из Knowledge Base.

## Д.2.2 Работа с ресурсами в пользовательской ветке

Пользовательская ветка подразумевает наличие в ней стандартных (эталонных) копий объектов, которые недоступны для редактирования и удаления. Но в ходе эксплуатации ПК Ankey SIEM NG может потребоваться изменить параметры правил, например, пороговые значения срабатываний правил корреляции, заполнение полей правил нормализации или тексты правил локализации.

Модификация стандартных объектов может быть выполнена только посредством копирования объекта. При копировании новый объект появляется в Knowledge Base как пользовательский и доступен для дальнейшего редактирования и удаления.

**Внимание!** На модифицированные пользователем ресурсы пакетов экспертизы не распространяется техническая поддержка.

После копирования объекта необходимо учитывать, что наличие двух идентичных по логике работы правил, установленных в SIEM, приведет к ложным срабатываниям, поэтому оригинальный объект, на основе которого делалась копия, должен быть удален из SIEM, а новый, скопированный, установлен в соответствии с инструкцией, приведенной в разделе Д.2.1.

Ограничения на создание новых объектов в пользовательской ветке отсутствуют.

**Внимание!** Создание новых объектов в эталонной корневой базе данных GIS\_DB запрещено!

Процесс работы с ресурсами подробно описан в документе «Руководство оператора Ankey SIEM NG 4.1.2».