GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс

«Система мониторинга и управления событиями безопасности Ankey SIEM Next Generation» v 5.2.3

Руководство администратора

Ankey SIEM NG®

© 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: 4 квартал 2024 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 10
2 О ПК Ankey SIEM NG 14
2.1 Варианты исполнения ПК Ankey SIEM NG 14
2.2 Архитектура ПК Ankey SIEM NG 17
2.2.2 Компонент Ankey SIEM Next Generation Core 18
2.2.3 Компонент Ankey SIEM Next Generation Management and Configuration 19
2.2.4 Компонент Ankey SIEM Next Generation Collector 20
2.2.5 Компонент Ankey SIEM Next Generation Server 21
2.2.6 Компонент Ankey SIEM Next Generation Events Storage 22
2.2.7 Компонент Ankey SIEM Next Generation Knowledge Base 22
2.2.8 Компонент Ankey SIEM Next Generation Retro Correlator 23
2.3 Схема взаимодействия компонентов 23
2.3.1 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG 23
2.3.2 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG VM 26
2.3.3 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG с дополнительным компонентом VM 28
3 Пользователи и права доступа 31
3.1 Вход в Ankey SIEM NG 31
3.2 Управление учетными записями 32
3.2.1 Создание учетной записи 33
3.2.2 Изменение данных пользователя 33
3.2.3 Блокирование и разблокирование учетной записи 33
3.2.4 Экспорт данных пользователей в текстовый файл 34
3.2.5 Создание LDAP-подключения 34
3.2.6 Настройка синхронизации с Microsoft Active Directory 36
3.2.7 Запуск вручную синхронизации с Microsoft Active Directory 36
3.2.8 Изменение параметров LDAP-подключения 37
3.2.9 Проверка LDAP-подключения 37
3.2.10 Удаление LDAP-подключения 37
3.3 Управление ролями и правами доступа 38
3.3.1 Создание роли 38
3.3.2 Создание роли на основе существующей роли 38
3.3.3 Изменение роли 38
3.3.4 3Удаление роли 39
3.3.5 Назначение ролей в одном приложении 39
3.3.6 Назначение ролей в нескольких приложениях 39
3.4 Просмотр записей о действиях пользователей 40
3.5 Смена пароля служебной учетной записи администратора 40
3.6 Предоставление доступа к событиям 41

3.7 Предоставление доступа к активам, инцидентам и источникам....41
4 Площадки и связи между ними....42
4.1 Регистрация площадки....42
4.2 Изменение параметров площадки....43
4.3 Отключение площадки....43
5 Распределенный поиск и репликация событий....44
5.1 Распределенный поиск событий....44
5.2 Репликация событий....45
5.3 Добавление связей для распределенного поиска....46
5.4 Удаление связи для распределенного поиска....46
5.5 Добавление правила репликации событий....47
5.6 Изменение правила репликации событий....47
5.7 Удаление правила репликации событий....48
6 Управление приложениями....49
6.1 Переименование приложения....49
6.2 Удаление приложения....49
7 Управление политиками....51
7.1 Страница Политики....52
7.2 Создание правила для значимости активов....53
7.3 Создание правила для сроков актуальности данных....54
7.4 Создание правила для соответствия стандартам....54
7.5 Создание правила для статусов несоответствий....55
7.6 Создание правила для статусов уязвимостей....55
7.7 Создание правила для отметки «важная»....56
7.8 Изменение правила....57
7.9 Копирование правила....57
7.10 Включение и отключение правила....57
7.11 Удаление правила....58
7.12 Применение изменений в политиках....58
7.13 Отмена изменений в черновике политики....58
8 Мониторинг источников событий....59
8.1 Просмотр списка источников и списка потоков событий от источника....60
8.2 Просмотр списка форвардеров и списка источников форвардера....61
8.3 Создание предупреждения для отслеживания наличия событий....62
8.4 Создание предупреждения для отслеживания средней скорости потока событий....62
8.5 Создание предупреждения для отслеживания задержки в получении события коллектором....63
8.6 Остановка и повторный запуск отслеживания потока событий....64
8.7 Удаление источника (форвардера) из списка....64
8.8 Экспорт списка источников (форвардеров) в текстовый файл....65
8.9 Обновление списка источников (форвардеров)....66
9 Мониторинг состояния ПК Ankey SIEM NG....67
9.1 Страница Управление системой....67

9.2 Удаление коллектора сбора событий из списка 69
9.3 Мониторинг работы правил корреляции....70
10 Резервное копирование данных....71
10.1 Создание резервной копии данных роли на Linux 71
10.2 Создание резервной копии индексов Elasticsearch на Linux....72
10.3 Создание резервной копии данных хранилища LogSpace....73
10.4 О резервном копировании данных о площадках и их связях....73
11 Восстановление данных из резервной копии....74
11.1 Восстановление данных компонентов Ankey SIEM NG на Linux из резервной копии 74
11.2 Восстановление индексов Elasticsearch из резервной копии на Linux 76
11.2.1 Восстановление всех индексов Elasticsearch из резервной копии на Linux 77
11.2.2 Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux 78
11.3 Восстановление данных хранилища LogSpace из резервной копии 78
11.4 О восстановлении резервной копии данных о площадках и их связях ...79
12 Индексы Elasticsearch: ротация, архивация, перемещение, удаление и использование политик ILM....80
12.1 Просмотр списка индексов 81
12.2 Настройка ротации индексов....81
12.3 Архивация индексов....82
12.3.1 Создание хранилища для архивных индексов....82
12.3.2 Архивация индексов на Linux 82
12.3.3 Настройка архивации индексов по расписанию 82
12.4 Восстановление индекса из архива....83
12.5 Удаление архивных индексов 83
12.5.1 Удаление архивных индексов на Linux....83
12.5.2 Удаление архивных индексов по расписанию 83
12.6 Удаление индекса без архивации....84
12.7 Перемещение индексов на Linux 84
13 Разделы LogSpace: ротация, резервное копирование и восстановление 86
13.1.2 Просмотр списков разделов и архивов LogSpace 88
13.1.3 Удаление разделов и архивов LogSpace 88
14 Смена паролей служебных учетных записей....89
14.1 Смена пароля служебной учетной записи в PostgreSQL 89
14.2 Смена пароля служебной учетной записи в СУБД Jatoba 89
14.3 Смена паролей служебных учетных записей в RabbitMQ....90
14.3.1 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Core на Linux....90
14.3.2 RabbitMQ: смена паролей служебных учетных записей компонента Ankey SIEM NG Server на Linux....90
14.3.3 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Collector на Microsoft Windows....92

14.3.4 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Collector на Linux 93
15 Настройка журналирования работы ПК Ankey SIEM NG 94
15.1 Настройка журналирования работы компонента Ankey SIEM NG Core на Linux 94
15.2 Настройка журналирования работы компонента Ankey SIEM NG Server 94
15.3 Настройка журналирования работы компонента Ankey SIEM NG Events Storage с Elasticsearch версии 7 95
15.4 Настройка журналирования работы компонента Ankey SIEM NG Collector на Microsoft Windows 96
16 Просмотр и изменение параметров конфигурации Ankey SIEM NG 97
16.1 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux 97
16.1.1 Просмотр конфигурации роли 97
16.1.2 Изменение конфигурации роли 97
16.1.3 Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch 98
16.1.4 Изменение степени сжатия данных в Elasticsearch 99
16.1.5 Регистрация событий при нарушении и восстановлении параметров источников 99
16.1.6 Настройка SMTP-сервера для отправки уведомлений по электронной почте 100
16.2 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Microsoft Windows 101
16.2.2 Просмотр конфигурации 102
16.2.3 Изменение конфигурации вручную 102
16.2.4 Изменение конфигурации с помощью XML-файла 102
17 Отключение отправки ненормализованных событий облегченной версией компонента Ankey SIEM NG Server («SIEM на коллекторе») 103
18 Настройка обогащения событий данными геолокации 104
19 Пользовательские поля в модели актива 106
19.1 Добавление пользовательских полей в модель актива 106
19.2 Добавление описания пользовательских полей 108
19.3 Изменение имен пользовательских полей 109
19.4 Удаление пользовательских полей из модели актива 110
20 Настройка категоризации 112
21 Управление модулями сбора и обработки данных, модулями выявления нарушений ИБ (корреляционной обработки данных) 114
21.1 Рекомендации по обновлению ресурсов 116
21.2 Алгоритм обновления ресурсов в эталонной базе данных до новой версии 117
21.3 Алгоритм обновления ресурсов в ветке Customer_Data 120
21.4 Алгоритм обновления отдельных ресурсов, полученных в рамках технической поддержки (hotfix) 120

21.5 Алгоритм обновления схемы полей событий и SDK после обновления компонентов Ankey SIEM NG ... 122
22 Работа с инфраструктурами ... 124
22.1 Создание инфраструктуры ... 124
22.2 Изменение названия инфраструктуры ... 124
22.3 Удаление инфраструктуры ... 124
23 Изменение проверок по чек-листу ... 126
24 Диагностика и решение проблем ... 127
24.1 Уведомления о состоянии системы ... 127
24.2 Обмен данными между компонентами системы ... 127
1.1.1 Вход в RabbitMQ ... 129
24.2.2 Мониторинг потока событий в RabbitMQ ... 129
24.2.3 Очередь storageq не уменьшается ... 130
24.2.4 Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается 130
24.2.5 Очередь storageq растет и начинает уменьшаться только после появления ошибки ... 131
24.2.6 Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки ... 132
24.3 Мониторинг состояния RabbitMQ и Elasticsearch ... 133
24.3.1 Параметры конфигурации службы SIEM Server health monitor ... 133
24.4 Ошибка "Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога" ... 136
24.5 Ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен» ... 136
24.6 Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога» ... 137
24.7 Ошибка "Объем свободного места на диске, выделенном для SIEM Messaging Service, достиг критического порога ... 138
24.8 Ошибка "Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога" ... 138
24.9 Ошибка "Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем" ... 139
24.10 Предупреждение "Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога" ... 140
24.11 Индексы Elasticsearch находятся в состоянии red ... 140
24.12 Служба Elasticsearch останавливается через некоторое время после запуска ... 142
24.13 Система не получает данные от задачи ... 142
24.14 Отсутствуют события от источников ... 144
24.15 Задача аудита не собирает сведения об активах ... 145
24.16 Не приходят уведомления, отправляемые по электронной почте ... 145
24.17 Ошибка "Sdk пакет <Номер версии> поврежден. Необходимо

восстановление"....146
24.18 Не удается импортировать отчет из MaxPatrol 8....146
24.19 Настройка компонентов после изменения IP-адресов или FQDN их серверов....147
24.20 Подсеть Docker-контейнера Ankey SIEM NG совпадает с одной из подсетей предприятия....148
24.20.1 Изменение подсети Docker-контейнера при обновлении компонентов....149
24.21 Диагностика коннекторов по сбору данных с источников событий....150
24.21.1 Диагностика источника событий (журналирование данных)....151
24.21.2 Проверка функционирования ПК Ankey SIEM NG....153
24.21.3 Диагностика работы коннектора....153
24.21.4 Включение расширенного режима логирования (debug-режим)....156
24.21.5 Версия дополнительного коннектора....158
24.22 Диагностика пакетов контента....159
24.22.1 Начальная проверка правила корреляции....160
24.22.2 Проверка корректности обработки события....173
24.22.3 Проверка корректности использования табличного списка....176
24.22.4 Корректность проверки правила....179
24.22.5 Возможность уменьшения срабатываний правил корреляции....183
24.22.6 Дополнительная информация....185
24.22.7 Версия пакета контента....185
24.23 Не все зависимые ресурсы импортированы в систему и/или добавлены в набор установок....186
24.24 Справочная информация....188
24.24.1 Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки....188
24.24.2 Сбор информации о нагрузке на файловую систему и запущенных процессах....188
24.24.3 Просмотр статуса службы....189
24.24.4 Проверка доступности сетевого порта сервера....189
24.24.5 Просмотр состояния индексов Elasticsearch....189
24.24.6 Просмотр состояния Elasticsearch....190
24.24.7 Создание дампа памяти процесса....190
24.24.8 Расположение индексов Elasticsearch....190
24.24.9 Расположение файлов журналов....190
24.24.10 Параметры мониторинга обработки активов....192
24.24.11 Просмотр данных о политиках ILM....194
24.24.12 Экспорт конфигурационных параметров ролей в файл....194
25 Обращение в службу технической поддержки....196
25.1 Требования к содержанию заявки....196
25.2 Порядок регистрации и учета заявок....197
25.3 В техническую поддержку входит....199
25.4 Ограничения в предоставлении услуг технической поддержки....200

Перечень сокращений 204
Приложение А Параметры конфигурации компонентов Ankey SIEM NG на Linux 209
Приложение Б Параметры конфигурации компонентов Ankey SIEM NG на Microsoft Windows 233
Приложение В Параметры проверок по чек-листу 242
Приложение Г Управление нормализацией событий с помощью команды drop 246
Приложение Д Структурная схема проверки работоспособности правила корреляции 249
Приложение Е Формы обращения в техническую поддержку 250

1 Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию программного комплекса Ankey SIEM Next Generation (далее также − ПК Ankey SIEM NG). Руководство не содержит инструкций по установке ПК Ankey SIEM NG и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим 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
	Актуальные версии прикладных модулей ПК Ankey SIEM NG	Содержит список актуальных версий сборок всех поддерживаемых ресурсов к ПК Ankey SIEM NG, разработанных ООО "Газинформсервис"
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию о ПК Ankey SIEM NG и вариантах его исполнения, а также 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 настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker
Инсталляция	Руководство по инсталляции Часть 1. Инсталляция ПК Ankey SIEM NG в исполнениях Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM	Содержит информацию для внедрения вариантов исполнения Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта

Каталог	Наименование документа	Описание
	Руководство по инсталляции Часть 2. Инсталляция ПК Ankey SIEM NG в исполнении Ankey SIEM NG VM	Содержит информацию для внедрения варианта исполнения Ankey SIEM NG VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
Подключение инфраструктуры	Руководство по настройке аудита активов Ankey SIEM NG (AM+VM+HCC)	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для аудита активов
	Руководство по интеграции с источниками событий Ankey SIEM NG.	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников
	Руководство по интеграции с источниками событий 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 событий Ankey SIEM NG. Список изменений	Содержит список изменений пакета стандартных коннекторов ПК Ankey SIEM NG
Настройка корреляции	Пакет общих ресурсов контента. Описание пакета экспертизы <Номер версии пакета>.	Содержит справочную информацию и инструкции по установке и настройке пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет общих ресурсов контента Приложение А <Номер версии пакета>.	Содержит списки применимых правил корреляции из состава пакета общих ресурсов контента ПК Ankey SIEM NG для поддерживаемых источников
	Пакет общих ресурсов контента Список изменений <Номер версии пакета>	Содержит список изменений пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет мониторинга SIEM Описание пакета экспертизы <Номер версии пакета>	Содержит списки применимых правил корреляции из состава пакета мониторинга SIEM для ПК Ankey SIEM NG
	Пакет мониторинга SIEM Список изменений <Номер версии пакета>	Содержит список изменений пакета мониторинга SIEM к ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
Инструкции к разработке	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 ПК 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 ПК Ankey SIEM NG
	PDQL-запросы для анализа активов	Содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в ПК Ankey SIEM NG
Дополнительно	Инструкция по обновлению Ankey SIEM NG с версии 4.x на версию 5.x	Содержит шаги, необходимые для обновления ПК Ankey SIEM NG с версии 4.1 до версии 5.2
	Инструкция по установке и настройке Ankey Update Mirror	Содержит информацию об установке и настройке локального сервера обновлений для получения обновлений экспертных данных компонента Ankey SIEM NG VM
	Инструкция по обновлению пакетов ресурсов с версии 3.x.x на версию 4.x.x	Содержит информацию, необходимую для обновления пакетов ресурсов ПК Ankey SIEM NG с версии 3.x.x на версию 4.x.x

В документе приняты условные обозначения.

Таблица 1.2 − Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
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 **ОК**	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 ИТ-инфраструктуре организаций. Ankey SIEM NG позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

2.1 Варианты исполнения ПК Ankey SIEM NG

ПК Ankey SIEM NG поддерживает несколько вариантов исполнения. Варианты исполнения ПК Ankey SIEM NG определяются приобретенной лицензией и влияют на состав, функции и взаимодействие компонентов системы.

Существуют следующие варианты исполнения ПК Ankey SIEM NG:

- Ankey SIEM NG;
- Ankey SIEM NG VM;
- Ankey SIEM NG с дополнительным компонентом VM.

ПК Ankey SIEM NG предоставляет следующие возможности в зависимости от варианта исполнения, который определяется приобретенной лицензией. Для получения информации о лицензиях необходимо сформировать запрос в службу технической поддержки ООО «Газинформсервис».

Внимание! Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

Таблица 2.1 – Возможности ПК Ankey SIEM NG в трёх вариантах исполнения

Возможности ПК Ankey SIEM NG	Ankey SIEM NG	Ankey SIEM NG VM[1]	Ankey SIEM NG с дополнительным компонентом VM
Инвентаризация активов	+	+	+
Сбор данных о событиях	+	-	+
Анализ событий для выявления инцидентов ИБ	+	-	+
Управление инцидентами ИБ	+	-	+
Сбор данных об уязвимостях на активах	-	+	+
Анализ уязвимостей на активах	-	+	+

1 Ankey SIEM NG VM возможно развернуть и использовать как самостоятельно, так и в рамках единой интегрированной системы обеспечения информационной безопасности предприятия. В этом случае Ankey SIEM NG VM поддерживает взаимодействие с ПК Ankey SIEM NG, что позволяет полнее и своевременнее актуализировать модель ИТ-инфраструктуры предприятия, более точно оценивать защищенность предприятия и использовать эти данные при работе с сетевым трафиком.

Возможности ПК Ankey SIEM NG	Ankey SIEM NG	Ankey SIEM NG VM[1]	Ankey SIEM NG с дополнительным компонентом VM
Предоставление информации об уязвимостях на активах при помощи базы знаний	-	+	+
Визуализация данных	+	+	+
Дополнительные возможности:			
Оценка соответствия стандартам безопасности[2]	-	+	+
Пакеты экспертизы	+	-	+
Автоматизация работы с активами	+	+	+
Повторная проверка событий	+	-	+
Отправка уведомлений	+	+	+

- **Инвентаризация активов.** Система регулярно собирает данные о сетевых узлах и связях между ними;
- **Сбор данных о событиях.** Система собирает данные о событиях с источников событий. 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;
- **Информация об уязвимостях на активах.** На основе постоянно обновляемой базы знаний Ankey SIEM NG предоставляет пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах. Ankey SIEM NG определяет способы устранения уязвимостей и позволяет настраивать политики контроля.
- **Оценка уязвимостей на активах**. Система выбирает среди уязвимостей те, которые необходимо устранять в первую очередь, и отображает степень защищенности активов.
- **Визуализация данных.** Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.
- **Пакеты экспертизы.** Использование базы знаний, разработанной экспертами ООО «Газинформсервис». База

[2] Оценка соответствия стандартам безопасности осуществляется при помощи дополнительного модуля НСС.

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 ИТ-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 ИТ-инфраструктурах организаций, о работе задач сбора данных Ankey SIEM NG, собираемых событиях, а также о выявляемых инцидентах ИБ.

При активации дополнительного модуля Host Compliance Control (далее также – HCC) с помощью лицензии обеспечивается выполнение следующих функций:

- **Сбор информации о параметрах безопасности.** Дополнительный модуль HCC получает полную информацию о составе ИТ-инфраструктуры и собирает сведения о параметрах безопасности.
- **Оценка соответствия стандартам безопасности.** Дополнительный модуль HCC отслеживает соответствие ИТ-инфраструктуры готовым стандартам, отдельным требованиям и может приоритизировать обнаруженные риски.

2.2 Архитектура ПК Ankey SIEM NG

ПК 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 ИТ-инфраструктурами разных масштабов. Если поток событий в Ankey SIEM NG превышает 5000 событий в секунду[3], то требуется распределенная установка компонентов ПК Ankey SIEM NG.

В состав Ankey SIEM NG входят компоненты, которые представлены в таблице 2.2. Состав компонентов определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.2 – Компоненты ПК Ankey SIEM NG

Компоненты ПК Ankey SIEM NG	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Ankey SIEM Next Generation Core	+	+	+
Ankey SIEM Next Generation Management and Configuration	+	+	+
Ankey SIEM Next Generation Collector	+	+	+
Ankey SIEM Next Generation Server	+	-	+
Ankey SIEM Next Generation Events Storage	+	-	+
Ankey SIEM Next Generation Knowledge Base	+	-	+
Ankey SIEM Next Generation Retro Correlator	+	-	+

[3] более 5 000 событий в секунду при использовании модуля syslog, более 3 000 событий в секунду при смешанном сборе событий.

2.2.2 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 функции, которые представлены в таблице 2.3. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.3 – Функции компонента Ankey SIEM Next Generation Core

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Централизованное хранение конфигурации активов	+	+	+
Централизованное управление всеми компонентами системы	+	+	+
Оперативное реагирование на инциденты информационной безопасности	+	+	+
Обеспечение взаимодействия подразделений организации при расследовании инцидентов	+	+	+
Автоматизация процесса управления уязвимостями	-	+	+
Поддержка веб-интерфейса системы	+	+	+

2.2.3 Компонент Ankey SIEM Next Generation Management and Configuration

Компонент Ankey SIEM Next Generation Management and Configuration (далее также − Ankey SIEM NG MC) обеспечивает функции, представленные в таблице 2.4. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.4 – Функции компонента Ankey SIEM Next Generation Management and Configuration

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Сервис единого входа в продукты ПК Ankey SIEM NG, развернутые в инфраструктуре организации	+	+	+
Управление пользователями системы: – создание учетных записей; – назначение прав; – блокирование и активация учетных записей	+	+	+
Интеграция с Microsoft Active Directory, включая аутентификацию пользователей и синхронизацию прав доступа	+	+	+
Управление иерархией продуктов Ankey SIEM NG	+	+	+
Журналирование действий пользователей	+	+	+
Хранение: – сведений об уязвимостях (об условиях их возникновения и способах устранения); – сведений о бюллетенях безопасности и возможном ПО на активах.	+	+	+

2.2.4 Компонент Ankey SIEM Next Generation Collector

Компонент Ankey SIEM Next Generation Collector (далее также − Ankey SIEM NG Collector) обеспечивает функции, представленные в таблице 2.5. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.5 – Функции компонента Ankey SIEM Next Generation Collector

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Сканирование и сбор информации об активах	+	+	+
Управление модулями сканирования и мониторинг их состояния	+	+	+
Сбор событий с источников	+	-	+
Передача данных между модулями и компонентом Ankey SIEM NG Server	+	-	+
Передача данных между модулями и компонентом Ankey SIEM NG Core	+	+	+

Ankey SIEM NG Collector имеет модульную структуру. Модули сканирования позволяют сканировать активы системы в режимах черного и белого ящика, обнаруживать узлы и их открытые сетевые сервисы, а также проводить специализированные проверки в режиме теста на проникновение.

Ankey SIEM NG Collector в режиме активного и пассивного сканирования 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 Collector управляет модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и:

- компонентом Ankey SIEM NG Server и Ankey SIEM NG Core для вариантов исполнения ПК Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM;
- компонентом Ankey SIEM NG Core для варианта исполнения Ankey SIEM NG VM;

К одному компоненту Ankey SIEM NG Server[4] или Ankey SIEM NG Core можно подключать несколько компонентов Ankey SIEM NG Collector. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты). Количество серверов Ankey SIEM NG Collector зависит от планируемой нагрузки на коллекторы, а также от физической и логической топологии ИТ-инфраструктуры организации. Максимально возможное количество коллекторов для одного экземпляра Ankey SIEM NG Core – 50.

2.2.5 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, которые представлены в таблице 2.6. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.6 – Функции компонента Ankey SIEM Next Generation Server

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Обработка событий безопасности: – нормализация; – агрегация; – обогащение; – корреляция.	+	Компонент отсутствует в поставке	+
Автоматическое создание инцидентов;	+		+
Создание активов из событий	+		+
Привязка событий к активам	+		+

[4] для вариантов исполнения ПК Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM.

2.2.6 Компонент Ankey SIEM Next Generation Events Storage

Компонент Ankey SIEM Next Generation Events Storage (далее также − Ankey SIEM NG Events Storage) обеспечивает функции, представленные в таблице 2.7. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.7 – Функции компонента Ankey SIEM Next Generation Events Storage

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Централизованное хранение информации о событиях безопасности	+	Компонент отсутствует в поставке	+

2.2.7 Компонент Ankey SIEM Next Generation Knowledge Base

Компонент Ankey SIEM NG Knowledge Base – это единая база знаний ПК, которая обеспечивает функции, представленные в таблице 2.8. Состав доступных функций определяется вариантом исполнения в зависимости от приобретенной лицензии.

Таблица 2.8 – Функции компонента Ankey SIEM Next Generation Knowledge Base

Функции компонента	Ankey SIEM NG	Ankey SIEM NG VM	Ankey SIEM NG с дополнительным компонентом VM
Хранение: – схемы полей событий; – пакетов экспертизы (наборов правил и табличных списков); – макросов (фильтров)	+	Компонент отсутствует в поставке	+

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 модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных) представлено в разделе 21.

2.2.8 Компонент Ankey SIEM Next Generation Retro Correlator

Компонент Ankey SIEM NG 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.

2.3 Схема взаимодействия компонентов

Состав компонентов и их взаимодействие определяется вариантом исполнения в зависимости от приобретенной лицензии.

2.3.1 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG

Взаимодействие компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG отражено на рисунке 2.1.

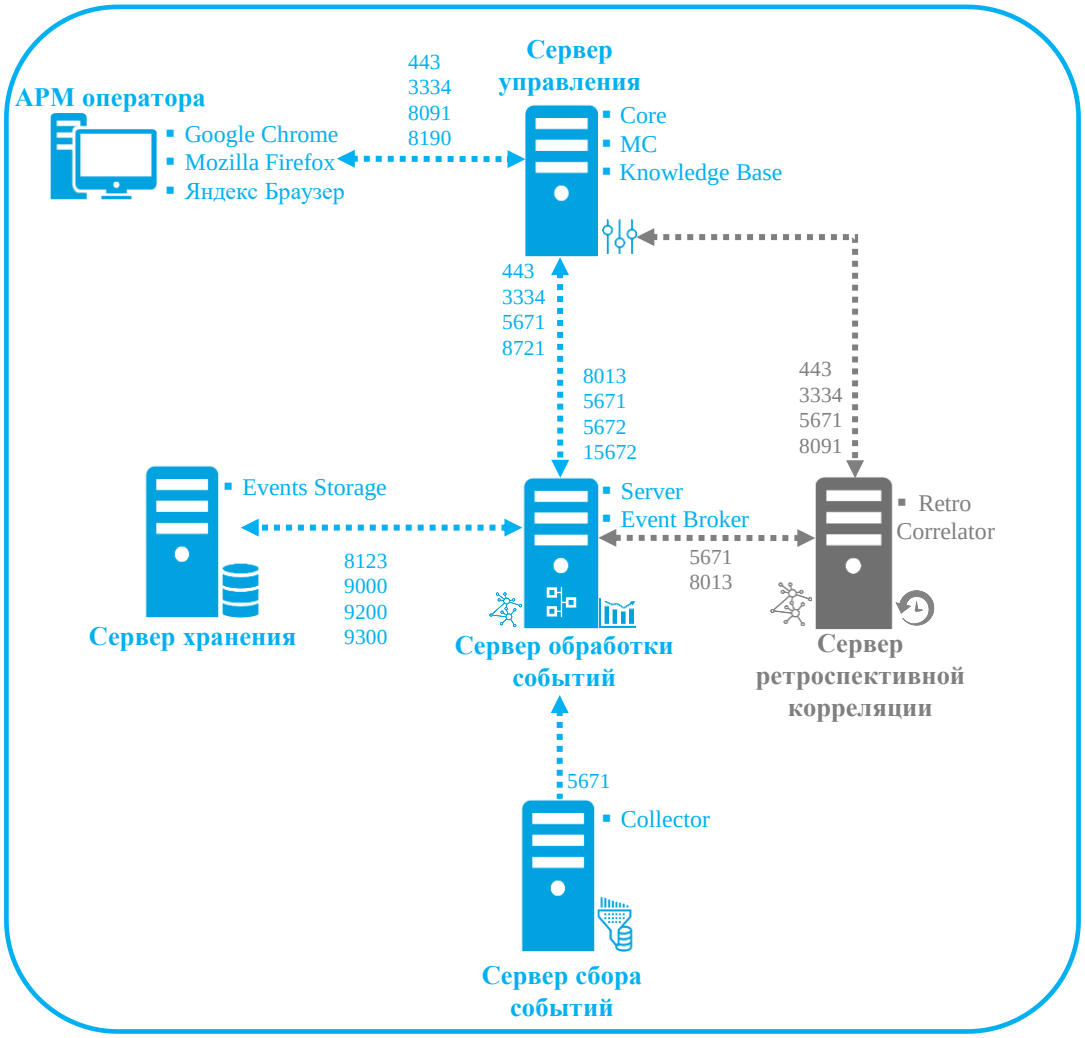


Рисунок 2.1 – Схема взаимодействия компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Collector сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и события с источников. Собранные данные коллекторы передают в Ankey SIEM NG Server и Ankey SIEM NG Core. Переданные события используются в Ankey SIEM NG Server для нормализации, агрегации, обогащения и корреляции.
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.
3. Компонент Ankey SIEM NG Server обрабатывает входящий поток событий, приводит их к единому формату в соответствии с правилами нормализации и группирует их согласно правилам агрегации. Он также связывает события с активами и, при необходимости, создает новые активы на основе событий. Затем дополняет данные о событиях, используя правила обогащения или табличные списки, и анализирует поток нормализованных событий по правилам корреляции для выявления и регистрации событий информационной безопасности. Ankey SIEM NG Server передает компоненту Ankey SIEM NG ES поступившие события в исходном (необработанном) и в нормализованном виде для хранения.

> **Примечание.** Нормализация событий может выполняться на сервере Ankey SIEM NG Collector. Для этого необходимо установить на сервер Ankey SIEM NG Collector облегченную версию Ankey SIEM NG Server – «SIEM на коллекторе». События, нормализованные на таком сервере Ankey SIEM NG Collector, передаются для агрегации, обогащения и корреляции на основной Ankey SIEM NG Server.

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 MC 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 2.9.

Таблица 2.9 − Компоненты и порты взаимодействия ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG

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, 5672, 8721
Ankey SIEM NG RC	Ankey SIEM NG Core	443, 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	3334
Ankey SIEM NG Core	Ankey SIEM NG Server	5671, 5672, 5672
Knowledge Base	Ankey SIEM NG Server	8013
Ankey SIEM NG RC	Ankey SIEM NG Server	8013, 5671
Ankey SIEM NG Collector	Ankey SIEM NG Server	5671
Ankey SIEM NG Server	Ankey SIEM NG ES	8123, 9000, 9200, 9300

Внимание! Для корректной работы SaltStack на сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.
Для средненагруженных и высоконагруженных систем на серверах, на которые устанавливаются компоненты Ankey SIEM NG Server, Ankey SIEM NG ES, Ankey SIEM NG Core, Ankey SIEM NG Collector, Ankey SIEM NG RC, порт 22/TCP должен быть открыт для входящих соединений от сервера с ролью Deployer.

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP – к серверам на Linux.

2.3.2 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG VM

Взаимодействие компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG VM отражено на рисунке 2.3.

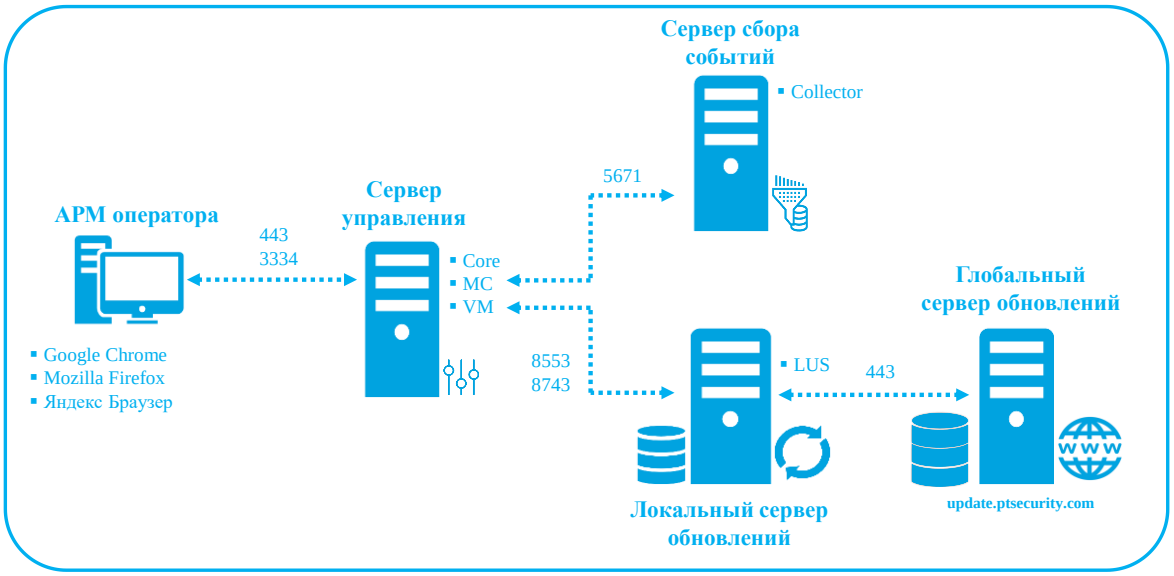


Рисунок 2.2 − Схема взаимодействия компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG VM

1. Модули компонента Ankey SIEM NG Collector сканируют ИТ-инфраструктуру предприятия и собирают сведения о сетевых узлах. Собранные данные коллекторы передают в Ankey SIEM NG Core.
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.
3. Используя данные базы уязвимостей Ankey SIEM NG, компонент Ankey SIEM NG Core рассчитывает уязвимости на активах.
4. Компонент Ankey SIEM NG MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
5. 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.

Для обеспечения сетевого взаимодействия компонентов ПК Ankey SIEM NG VM должны быть доступны для входящих соединений порты, которые представлены в таблице 2.10.

Таблица 2.10 − Компоненты и порты взаимодействия ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG VM

Источник	Получатель	TCP-порт
Рабочая станция пользователя	Ankey SIEM NG Core	443
Ankey SIEM NG Collector	Ankey SIEM NG Core	5671
Рабочая станция пользователя	Ankey SIEM NG MC	3334
Ankey SIEM NG Core	Ankey SIEM NG Update Mirror (LUS)	8553, 8743
Ankey SIEM NG Update Mirror (LUS)	Глобальный сервер обновлений	443

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP – к серверам на Linux.

2.3.3 Схема взаимодействия компонентов для варианта исполнения Ankey SIEM NG с дополнительным компонентом VM

Взаимодействие компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG с дополнительным компонентом VM отражено на рисунке 2.3.

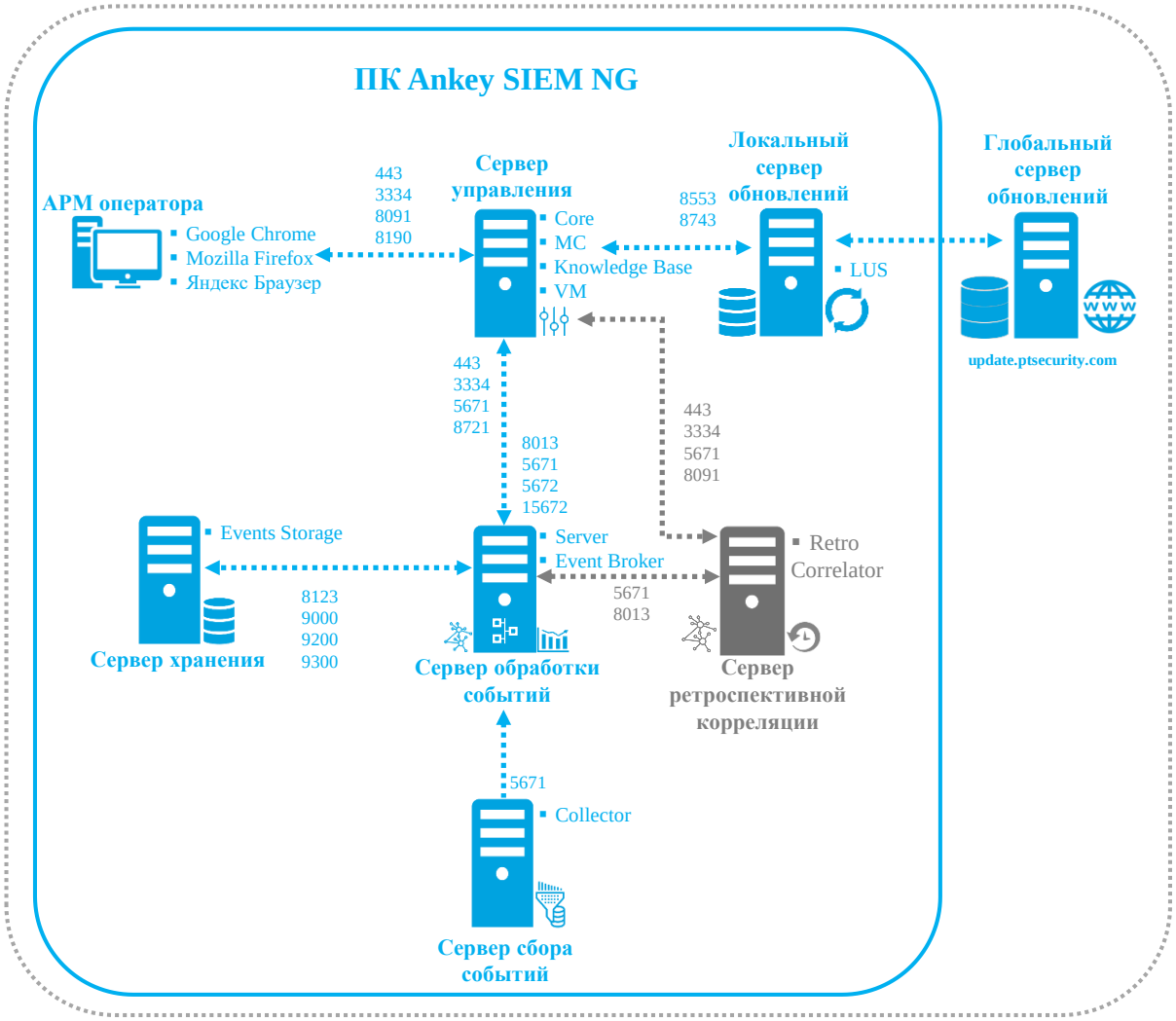


Рисунок 2.3 − Схема взаимодействия компонентов ПК Ankey SIEM NG для варианта исполнения Ankey SIEM NG с дополнительным компонентом VM

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Collector сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и события с источников. Собранные данные коллекторы передают в Ankey SIEM NG Server и Ankey SIEM NG Core. Переданные события используются в Ankey SIEM NG Server для нормализации, агрегации, обогащения и корреляции.
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.

3. Компонент Ankey SIEM NG Server обрабатывает входящий поток событий, приводит их к единому формату в соответствии с правилами нормализации и группирует их согласно правилам агрегации. Он также связывает события с активами и, при необходимости, создает новые активы на основе событий. Затем дополняет данные о событиях, используя правила обогащения или табличные списки, и анализирует поток нормализованных событий по правилам корреляции для выявления и регистрации событий информационной безопасности. Ankey SIEM NG Server передает компоненту Ankey SIEM NG ES поступившие события в исходном (необработанном) и в нормализованном виде для хранения.

Примечание. Нормализация событий может выполняться на сервере Ankey SIEM NG Collector. Для этого необходимо установить на сервер Ankey SIEM NG Collector облегченную версию Ankey SIEM NG Server – «SIEM на коллекторе». События, нормализованные на таком сервере Ankey SIEM NG Collector, передаются для агрегации, обогащения и корреляции на основной Ankey SIEM NG Server.

4. Компонент Ankey SIEM NG MC обеспечивает доступ к системе через сервис единого входа, журналирует действия пользователей и хранит информацию об уязвимостях.
5. Компонент Knowledge Base содержит базу знаний, необходимых Ankey SIEM NG для структурирования сведений, собранных от источников событий и объектов инфраструктуры.
6. Компонент Ankey SIEM NG MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
7. 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.
8. 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 2.11.

Таблица 2.11 − 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, 8721
Ankey SIEM NG RC	Ankey SIEM NG Core	443, 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	3334
Ankey SIEM NG Core	Ankey SIEM NG Server	5671, 5672, 15672
Knowledge Base	Ankey SIEM NG Server	8013
Ankey SIEM NG RC	Ankey SIEM NG Server	8013, 5671
Ankey SIEM NG Collector	Ankey SIEM NG Server	5671
Ankey SIEM NG Server	Ankey SIEM NG ES	8123, 9000, 9200, 9300
Ankey SIEM NG Core	Ankey SIEM NG Update Mirror (LUS)	8553, 8743
Ankey SIEM NG Update Mirror (LUS)	Глобальный сервер обновлений	443

Внимание! Для корректной работы SaltStack на сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.
Для средненагруженных и высоконагруженных систем на серверах, на которые устанавливаются компоненты Ankey SIEM NG Server, Ankey SIEM NG ES, Ankey SIEM NG Core, Ankey SIEM NG Collector, Ankey SIEM NG RC, порт 22/TCP должен быть открыт для входящих соединений от сервера с ролью Deployer.

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP – к серверам на Linux.

3 Пользователи и права доступа

В ПК Ankey SIEM NG реализована ролевая модель управления доступом. В общем случае пользователю могут быть назначены одна или несколько ролей. Каждая роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в системе (например, доступность работы с активами). Также для роли можно определить активы, источники, события и инциденты, доступ к которым получат пользователи с этой ролью.

При развертывании системы ее компоненты передают в Ankey SIEM NG Management and Configuration данные о доступных привилегиях и стандартных ролях. Роли и привилегии распределены по приложениям, которым соответствует определенный набор функций системы. Если пользователь имеет несколько ролей в приложении, права доступа суммируются.

При развертывании Ankey SIEM NG в Ankey SIEM NG Management and Configuration регистрируются следующие приложения:

- **Management and Configuration.** Приложение предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления площадками и связями между ними. По умолчанию приложение содержит стандартные роли **Администратор** и **Пользователь**;
- **Ankey SIEM NG.** Приложение предназначено для настройки сбора данных об ИТ-инфраструктуре предприятия и работы с активами, источниками, событиями и инцидентами. По умолчанию приложение содержит стандартные роли **Администратор** и **Оператор**;
- **Knowledge Base.** Приложение предназначено для работы с пакетами экспертизы, макросами и схемой полей событий. По умолчанию приложение содержит стандартную роль **Администратор**.

Описание интерфейса приложений, зарегистрированных в Ankey SIEM NG MC, представлено в документе «Руководство оператора Ankey SIEM NG 5.2.3»

3.1 Вход в Ankey SIEM NG

Ankey SIEM NG Management and Configuration обеспечивает механизм единого входа (технология single sign-on), поэтому другие продукты Ankey SIEM NG в случае их интеграции с Ankey SIEM NG также могут быть зарегистрированы в Ankey SIEM NG Management and Configuration, а их роли и привилегии будут доступны для назначения пользователям.

При развертывании Ankey SIEM NG автоматически создается учетная запись (логин – Administrator, пароль – P@ssword), имеющая все возможные стандартные роли. Эту учетную запись невозможно заблокировать, также невозможно изменить ее логин. После входа в систему рекомендуется сменить пароль этой учетной записи на более сложный.

Для обеспечения выполнения пользователем производственных задач

необходимо:

1. Создать для пользователя учетную запись.
2. Если набор привилегий стандартных ролей не подходит для выполнения производственных задач – создать пользовательские роли с нужным набором привилегий.
3. Назначить пользователю необходимые роли.
4. Настроить для ролей доступ к активам, источникам, событиям и инцидентам в соответствии с производственными задачами пользователя.

В этом разделе даны инструкции по предоставлению доступа к активам, источникам, событиям и инцидентам.

3.2 Управление учетными записями

Управление учетными записями различается в зависимости от типа аутентификации пользователей.

В случае локальной аутентификации необходимо вручную создавать учетные записи (см. раздел 3.2.1), аутентификация пользователей выполняется в Ankey SIEM NG MC. Администратор указывает в приложении **Management and Configuration** логин, пароль, статус пользователя, персональную и организационную информацию, а также роли пользователя. Эти параметры доступны для изменения и хранятся только в Ankey SIEM NG MC.

Для использования LDAP-аутентификации необходимо настроить LDAP-подключение перед созданием учетных записей (см. раздел 3.2.1). Администратор указывает в приложении **Management and Configuration** логин, статус и роли пользователя. Пароль учетной записи хранится в Microsoft Active Directory и не может быть изменен в приложении **Management and Configuration**. Персональная и организационная информация по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Учетная запись может автоматически создаваться в Ankey SIEM NG MC при первом входе пользователя. Для этого необходимо настроить LDAP-подключение и синхронизацию с Microsoft Active Directory (см. раздел 3.2.6). Логин, пароль, а также группы пользователя, соответствующие его ролям, хранятся в Microsoft Active Directory и не могут быть изменены в приложении **Management and Configuration**. Персональная и организационная информация также по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Система может содержать учетные записи пользователей с разными типами аутентификации. Вы можете сменить пользователю тип аутентификации в системе.

Список пользователей и назначенных им ролей приведен на странице **Пользователи**, список LDAP-подключений − на странице **Настройка LDAP-подключений**.

3.2.1 Создание учетной записи

Если аутентификация пользователя будет выполняться через LDAP, перед созданием учетной записи необходимо настроить этот тип аутентификации.

После создания учетная запись не может быть удалена. Если требуется запретить пользователю вход в систему, необходимо заблокировать его учетную запись (см. раздел 3.2.3).

❖ Чтобы создать учетную запись пользователя:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. В блоке параметров **Учетные данные** выберите тип аутентификации.
3. Если вы выбрали локальную аутентификацию, введите логин и пароль пользователя.

   Примечание. Если требуется, чтобы пользователь сменил пароль при первом входе в систему, установите флажок.

4. Если вы выбрали LDAP-аутентификацию, введите доменное имя пользователя и по ссылке **Выбрать домен** выберите LDAP-подключение.
5. Нажмите кнопку **Создать**.

Учетная запись пользователя создана.

3.2.2 Изменение данных пользователя

❖ Чтобы изменить данные пользователя:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. Выберите учетную запись пользователя, данные которого необходимо изменить.
3. Внесите изменения и нажмите кнопку **Сохранить**.

Данные пользователя изменены.

3.2.3 Блокирование и разблокирование учетной записи

❖ Чтобы заблокировать учетную запись:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. В списке выберите пользователя, учетную запись которого необходимо заблокировать.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

3. Нажмите кнопку **Заблокировать**.

Учетная запись пользователя заблокирована.

❖ Чтобы разблокировать учетную запись:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. В списке выберите пользователя, учетную запись которого необходимо разблокировать.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

3. Нажмите кнопку **Разблокировать**.

Учетная запись пользователя разблокирована.

3.2.4 Экспорт данных пользователей в текстовый файл

❖ Чтобы экспортировать данные пользователей:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. Выберите учетные записи пользователей для экспорта.

   Примечание. Вы можете выбирать несколько учетных записей подряд, нажимая клавишу **Shift**, или несколько отдельных учетных записей, нажимая клавишу **Ctrl**.

3. Нажмите кнопку **Экспорт**.
4. В открывшемся окне выберите вариант экспорта выбранных учетных записей и подтвердите экспорт.
   Браузер загрузит текстовый файл с данными пользователей.

Данные пользователей экспортированы.

3.2.5 Создание LDAP-подключения

Если вы планируете использовать защищенное соединение по протоколу SSL, перед созданием LDAP- подключения нужно установить на узле с Ankey SIEM NG Management and Configuration корневой сертификат центра сертификации. Файл корневого сертификата вы можете получить у администратора LDAP-сервера.

❖ Чтобы установить корневой сертификат на узел с Ankey SIEM NG Management and Configuration:

1. Скопируйте файл сертификата в хранилище /usr/local/share/ca-certificates.
2. Обновите список доверенных сертификатов в операционной системе:
   sudo update-ca-certificates
3. Перезагрузите узел с Ankey SIEM NG Management and Configuration.

Корневой сертификат установлен.

❖ Чтобы создать LDAP-подключение:

1. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.
   Откроется страница **Настройка LDAP-подключений**.
2. В панели инструментов нажмите кнопку **Добавить подключение**.
   Откроется страница **Новое LDAP-подключение**.
3. Введите название LDAP-подключения.
4. В блоке параметров **Серверы** в поле **Адрес** введите IP-адрес или полное доменное имя (FQDN) имя LDAP-сервера.

> **Примечание.** Если требуется устанавливать защищенное соединение с LDAP-сервером, адрес необходимо вводить в зависимости от типа доверенного сертификата (он выпускается или для IP-адреса, или для полного доменного имя).

5. В поле **Порт** введите номер порта.
6. Если требуется устанавливать защищенное соединение с LDAP-сервером, установите флажок **SSL**.

> **Примечание.** Вы можете добавлять дополнительные серверы, нажимая +. При потере соединения с одним сервером запрос аутентификации может быть обработан другим сервером. После заполнения полей вы можете проверить соединение (см. раздел 3.2.9) с LDAP-серверами.

7. В поле **Домены** введите DNS-имя домена, NetBIOS-имя домена или UPN-суффикс.
8. В поле **База поиска пользователей** введите имя записи каталога, начиная с которой выполняется поиск учетных записей пользователей.

> **Примечание.** Вы можете автоматически загрузить имена доменов и параметры базы поиска, нажав кнопку **Запросить данные с сервера** и указав данные учетной записи с правами доступа на чтение данных о пользователях.

9. Если требуется, настройте синхронизацию с Microsoft Active Directory (см. раздел 3.2.6).
10. Нажмите кнопку **Добавить**.
    LDAP-подключение создано.

3.2.6 Настройка синхронизации с Microsoft Active Directory

Вы можете настраивать синхронизацию при создании LDAP-подключения на странице **Новое LDAP-подключение** или при его изменении (см. раздел 3.2.8) на странице **Изменение параметров LDAP-подключения**. Перед настройкой синхронизации необходимо создать в Microsoft Active Directory учетную запись с правами на чтение данных о пользователях и группах пользователей.

❖ Чтобы настроить синхронизацию с Microsoft Active Directory:

1. Включите синхронизацию с Microsoft Active Directory.
2. В секции **Синхронизация с Active Directory** введите логин и пароль служебной учетной записи с правами на чтение данных о пользователях и группах пользователей Active Directory.
3. Если необходимо осуществлять поиск групп пользователей по базе, отличной от указанной при создании LDAP-подключения, в блоке параметров **Синхронизация с Active Directory** выберите вариант **Другая база** и в поле под ним укажите нужное значение.
4. Если необходимо, включите синхронизацию по расписанию и по ссылке настройте расписание.

> **Примечание.** Синхронизация также может быть запущена вручную (см. раздел 3.2.7) на странице Настройка LDAP-подключений.

5. В блоке параметров **Соответствие ролей и групп** нажмите кнопку **Получить список групп** и в раскрывающихся списках выберите группы Microsoft Active Directory, соответствующие ролям пользователей.
6. Нажмите кнопку **Сохранить**.
   Синхронизация с Microsoft Active Directory настроена.

3.2.7 Запуск вручную синхронизации с Microsoft Active Directory

❖ Чтобы вручную запустить синхронизацию с Microsoft Active Directory:

1. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.
   Откроется страница **Настройка LDAP-подключений**.
2. Выберите LDAP-подключение.
3. Нажмите кнопку **Запустить синхронизацию**.
4. В таблице отобразится значок .
   Синхронизация с Microsoft Active Directory запущена вручную.

По завершении синхронизации:

- если синхронизация была выполнена успешно − значок статуса пропадет, в панели **<Название подключения>** время последней синхронизации изменится на актуальное;
- если синхронизация была выполнена с предупреждениями − значок статуса сменится на , в панели **<Название подключения>** отобразится текст предупреждения;

– если синхронизация была выполнена с ошибками − значок статуса сменится на , в панели **<Название подключения>** отобразится текст ошибки.

3.2.8 Изменение параметров LDAP-подключения

❖ Чтобы изменить параметры LDAP-подключения:

1. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.
   Откроется страница **Настройка LDAP-подключений**.
2. Выберите LDAP-подключение.
3. В панели инструментов нажмите кнопку **Изменить подключение**.
   Откроется страница **Изменение параметров LDAP-подключения**.
4. Внесите изменения.

> **Примечание.** После внесения изменений рекомендуется проверить подключение (см. раздел 3.2.9).

5. Нажмите кнопку **Сохранить**.

Параметры LDAP-подключения изменены.

3.2.9 Проверка LDAP-подключения

При проверке LDAP-подключения устанавливается пробное соединение с LDAP-серверами.

Вы можете проверять подключение при его создании на странице **Новое LDAP-подключение** или изменении его параметров (см. раздел 3.2.8) на странице **Изменение параметров LDAP-подключения**.

❖ Чтобы проверить LDAP-подключение:

1. Нажмите кнопку **Проверить соединение**.
   Откроется окно **Проверка соединения**.
2. Введите логин и пароль пользователя с правами доступа на чтение данных о пользователях.
3. Нажмите кнопку **Проверить**.
   Результаты проверки отобразятся в окне **Проверка соединения**.
4. Нажмите кнопку **Закрыть**.

LDAP-подключение проверено.

3.2.10 Удаление LDAP-подключения

❖ Чтобы удалить LDAP-подключение:

1. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.
   Откроется страница **Настройка LDAP-подключений**.
2. Выберите LDAP-подключение.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

LDAP-подключение удалено.

3.3 Управление ролями и правами доступа

Роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в продуктах.

Если аутентификация пользователей выполняется локально или через LDAP без синхронизации с Microsoft Active Directory, вы можете назначать:

- роли в одном приложении (см. раздел 3.3.5) нескольким пользователям − на странице Роли и права доступа;
- роли в нескольких приложениях (см. раздел 3.3.6) нескольким пользователям − на странице **Пользователи**.

Если учетные записи пользователей синхронизируются с Microsoft Active Directory, назначение им ролей в приложении **Management and Configuration** недоступно. Назначать роли таким пользователям необходимо в Microsoft Active Directory, добавляя их в группы, соответствующие требуемых ролям.

3.3.1 Создание роли

❖ Чтобы создать роль:

1. В главном меню выберите раздел **Роли**.
   Откроется страница **Роли и права доступа**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание роли**.
3. В раскрывающемся списке выберите приложение, для которого необходимо создать роль.
4. Введите название роли.
5. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.
6. Нажмите кнопку **Создать**.

Роль создана.

3.3.2 Создание роли на основе существующей роли

❖ Чтобы создать роль на основе существующей:

1. В главном меню выберите раздел **Роли**.
   Откроется страница **Роли и права доступа**.
2. Выберите роль, на основе которой будет создана новая роль.
3. В панели инструментов нажмите кнопку **Создать копию**.
   Откроется окно **Создание роли**.
4. Введите название роли.
5. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.
6. Нажмите кнопку **Создать**.

Роль создана.

3.3.3 Изменение роли

❖ Чтобы изменить роль:

1. В главном меню выберите раздел **Роли**.
   Откроется страница **Роли и права доступа**.
2. В панели **Роли** выберите роль пользователя.

> **Примечание.** Вы можете выбирать несколько ролей подряд, нажимая клавишу **Shift**, или несколько отдельных ролей, нажимая клавишу **Ctrl**.

3. В панели инструментов нажмите кнопку **Редактировать**.
4. Откроется страница **Редактирование роли <Название роли>**.
5. Внесите изменения и нажмите кнопку **Сохранить**.

Роль изменена.

3.3.4 ЗУдаление роли

❖ Чтобы удалить роль:

1. В главном меню выберите раздел **Роли**.
   Откроется страница **Роли и права доступа**.
2. В панели **Роли** выберите роль пользователя.

> **Примечание.** Вы можете выбирать несколько ролей подряд, нажимая клавишу **Shift**, или несколько отдельных ролей, нажимая клавишу **Ctrl**.

3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Роль удалена.

3.3.5 Назначение ролей в одном приложении

❖ Чтобы назначить роли:

1. В главном меню выберите раздел **Роли**.
   Откроется страница **Роли и права доступа**.
2. В панели **Роли** выберите роли, которые необходимо назначить пользователям.

> **Примечание.** Вы можете выбрать роли только одного приложения.

3. В панели инструментов нажмите кнопку **Назначить**.
4. Во всплывающем окне установите флажки для тех пользователей, которым необходимо назначить выбранные роли.
5. Нажмите кнопку **Назначить выбранные роли пользователям**.

Роли назначены.

3.3.6 Назначение ролей в нескольких приложениях

❖ Чтобы назначить роли:

1. В главном меню в разделе **Пользователи** выберите пункт **Пользователи**.
   Откроется страница **Пользователи**.
2. Выберите учетные записи пользователей, которым необходимо назначить роли.

Примечание. Вы можете выбирать несколько учетных записей подряд, нажимая клавишу Shift, или несколько отдельных учетных записей, нажимая клавишу Ctrl.

3. В панели инструментов нажмите кнопку **Роли в приложениях**. Откроется окно **Роли пользователей**.
4. В раскрывающемся списке **<Название приложения>** установите флажки для назначаемых пользователям ролей.
5. Нажмите кнопку **Сохранить**.

Роли назначены.

3.4 Просмотр записей о действиях пользователей

❖ Чтобы просмотреть записи о действиях пользователя:

1. В главном меню выберите раздел **Журнал действий**.
2. В панели **Пользователи** выберите пользователя, записи о действиях которого необходимо просмотреть.
3. В панели **Действия** выберите группу действий, записи о которых необходимо просмотреть.
4. Если требуется, выберите период для просмотра записей, нажав .
5. В панели **Действия пользователей** отобразится список записей о действиях пользователя.

3.5 Смена пароля служебной учетной записи администратора

В случае невозможности сменить пароль служебной учетной записи Administrator через веб-интерфейс (например, при утере пароля), вы можете сменить пароль в терминале Linux. Новый пароль должен быть не короче 8 символов и содержать как минимум одну строчную и одну прописную латинскую букву, одну цифру и один спецсимвол.

❖ Чтобы сменить пароль на Linux:

1. Выполните команды:
   cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли Management and Configuration>/tools/ ;
   chmod +x reset-password.sh ;
   ./reset-password.sh .
2. В интерфейсе терминала появится сообщение:
   Please enter new password
3. Введите новый пароль.
   Начнется процесс смены пароля.
   По его завершении в интерфейсе терминала появится сообщение:
   Password successfully changed

Пароль изменен.

3.6 Предоставление доступа к событиям

❖ Чтобы предоставить доступ к событиям:

1. В главном меню в разделе **Система** выберите пункт **Права доступа**.
   Откроется страница **Права доступа**.
2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к событиям.
3. В панели **<Название роли>** по ссылке **Редактировать** откройте окно **Доступ к событиям**.
4. В раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ к событиям, введите условия фильтрации.

> **Примечание.** Вы можете скопировать условия фильтрации, нажав ссылку **Вставить условие из сохраненного запроса** и выбрав условия фильтрации из списка.

6. Нажмите кнопку **Сохранить**.

Доступ к событиям предоставлен.

3.7 Предоставление доступа к активам, инцидентам и источникам

После получения доступа к активам также будут доступны связанные с активами инциденты и источники.

❖ Чтобы предоставить доступ к активам:

1. В главном меню в разделе **Система** выберите пункт **Права доступа**.
   Откроется страница **Права доступа**.
2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к активам.
3. В панели **<Название роли>** по ссылке **Редактировать** откройте окно **Доступ к активам, инцидентам и источникам**.
4. В раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы активов, к которым необходимо предоставить доступ.

> **Примечание.** Вы можете искать группы активов с помощью поля поиска и выбирать группы активов, устанавливая флажки напротив них.

6. Нажмите кнопку **Сохранить**.

Доступ к активам предоставлен.

4 Площадки и связи между ними

Компоненты ПК Ankey SIEM NG, интегрированные с одним и тем же сервером Ankey SIEM NG MC, используют единую среду для аутентификации пользователей, управления их учетными записями и правами доступа. Совокупность таких продуктов называется площадкой.

Связи между площадками отображаются на схеме площадок в виде двухуровневого дерева. На одном уровне дерева находится главная площадка, на другом − одна или несколько площадок, связанных с главной. Создание связей между главной площадкой и остальными площадками (регистрацию площадок) нужно выполнять в интерфейсе главной площадки. Подчиненная площадка может быть зарегистрирована только на одной главной площадке.

Учетные записи пользователей Ankey SIEM NG MC постоянно синхронизируются между всеми площадками. Пользователи каждой площадки при наличии прав доступа могут через главное меню Ankey SIEM NG MC войти в приложения других площадок.

Внимание! По умолчанию учетные записи не имеют прав доступа на другие площадки, поэтому для входа от их имени необходимо назначить им подходящие роли для удаленных площадок (см. раздел 3.3).

Также необходимо обеспечить сетевое взаимодействие через TCP-порт 3334 между рабочими станциями пользователей и серверами Ankey SIEM NG всех площадок.

При аутентификации с главной площадки в подчиненные необходимо к логину учетной записи на удаленной площадке добавлять @SITE. Например, Auditor@SITE.

Перед регистрацией площадок необходимо:

- синхронизировать по протоколу NTP время между серверами Ankey SIEM NG MC всех площадок;
- убедиться, что на всех площадках развернуты одинаковые версии Ankey SIEM NG MC;
- обеспечить сетевое взаимодействие через TCP-порт 3334 между сервером Ankey SIEM NG MC главной площадки и серверами Ankey SIEM NG MC остальных площадок;
- убедиться, что значения параметров HostAddress в конфигурациях Ankey SIEM NG MC на всех площадках имеют один и тот же тип: в качестве значения параметра должен быть указан или IP-адрес сервера, или его FQDN в одинаковом для всех параметров регистре.

4.1 Регистрация площадки

Для выполнения инструкции вам потребуются логин и пароль учетной записи с привилегией **Подключение локальной площадки к иерархии** на регистрируемой площадке.

❖ Чтобы зарегистрировать площадку:

1. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.

2. В панели инструментов нажмите кнопку **Зарегистрировать площадку**.
   Откроется окно **Регистрация площадки**.
3. Введите название площадки и ее псевдоним.

> **Примечание.** После регистрации площадки ее название будет отображаться на схеме и в раскрывающемся списке при нажатии . Псевдоним площадки может содержать только буквы латинского алфавита, цифры, дефис и знак подчеркивания и должен быть уникальным.

4. В поле **Адрес** введите значение параметра HostAddress конфигурации Ankey SIEM NG MC.
5. Нажмите кнопку **Подключиться**.
   Откроется страница входа на регистрируемую площадку.
6. Введите логин и пароль учетной записи с привилегией **Подключение локальной площадки к иерархии** на регистрируемой площадке и нажмите кнопку **Войти**.
   Откроется окно **Подтвердить подключение к площадке <Название площадки>**.
7. Нажмите кнопку **Подтвердить**.
8. Нажмите кнопку **Зарегистрировать**.
   Новая площадка появится на схеме.

Площадка зарегистрирована.

4.2 Изменение параметров площадки

❖ Чтобы изменить параметры:

1. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
2. На схеме выберите площадку.
3. В панели инструментов нажмите кнопку **Изменить**.
4. Откроется окно **Изменение площадки <Название площадки>**.
5. Внесите изменения.
6. Если вы изменили адрес площадки, нажмите кнопку **Подключиться** и разрешите подключение.
7. Нажмите кнопку **Сохранить**.
8. Параметры площадки изменены.

4.3 Отключение площадки

❖ Чтобы отключить площадку:

1. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
2. На схеме выберите площадку.
3. В панели инструментов нажмите кнопку **Отключить** и подтвердите отключение.

Площадка отключена.

5 Распределенный поиск и репликация событий

После создания связей между площадками вы сможете настроить связи между приложениями Ankey SIEM NG, предназначенные для выполнения следующих задач.

5.1 Распределенный поиск событий

Связь обеспечивает в интерфейсе локального приложения работу с событиями, собранными в других приложениях. Эти события будут доступны для поиска и фильтрации, группировки и агрегации, отображения на виджетах и выпуска по ним отчетов. Вместе с тем данные об этих событиях не реплицируются между хранилищами связанных приложений.

Для работы с распределенным поиском вы можете предоставить пользователю следующие привилегии:

- **распределенный поиск событий.** Разрешает просмотр полученных распределенным поиском событий на странице **События** и на виджетах, а также выпуск отчетов по таким событиям. Привилегия доступна для ролей в приложении Ankey SIEM NG;

> Внимание! Пользователю с привилегией **Распределенный поиск событий** будут доступны все события, собранные как на локальной площадке, так и на площадках связанных приложений. Права доступа к событиям, указанные для ролей пользователя на странице **Система** → **Права доступа**, будут проигнорированы.

- **просмотр правил репликации и связей для распределенного поиска.** Разрешает просмотр созданных связей распределенного поиска на странице **Площадки**. Привилегия доступна для ролей в приложении Ankey SIEM NG Management and Configuration;
- **добавление, изменение и удаление правил репликации и связей для распределенного поиска.** Разрешает управление связями распределенного поиска на странице **Площадки**. Привилегия доступна для ролей в приложении Ankey SIEM NG Management and Configuration.

Перед настройкой связей для распределенного поиска на каждой площадке необходимо:

1. Обеспечить сетевое взаимодействие через TCP-порты 9200 и 9300 между серверами Ankey SIEM NG Server и Ankey SIEM NG Events Storage связываемых приложений.

2. В качестве значения параметра ClusterSeedHost[5] компонента Ankey SIEM NG Server указать IP-адрес или FQDN сервера Ankey SIEM NG Events Storage главного конвейера на данной площадке.
3. Повторно запустить настройку компонента Ankey SIEM NG Core: /opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId Core.

Не рекомендуется создавать связи для распределенного поиска между приложениями в низконагруженной конфигурации Ankey SIEM NG.

5.2 Репликация событий

Связь обеспечивает репликацию данных о событиях из одного приложения в другое согласно установленному правилу. После репликации эти события будут доступны в приложении-получателе независимо от сетевой доступности приложения-отправителя.

Для работы с правилами репликации вы можете предоставить пользователю следующие привилегии:

- **просмотр правил репликации и связей для распределенного поиска.** Разрешает просмотр правил репликации на странице **Площадки**. Привилегия доступна для ролей в приложении Ankey SIEM NG Management and Configuration;
- **добавление, изменение и удаление правил репликации и связей для распределенного поиска.** Разрешает управление правилами репликации на странице **Площадки**. Привилегия доступна для ролей в приложении Ankey SIEM NG Management and Configuration.

Перед добавлением правила, а также для его дальнейшей работы необходимо обеспечить сетевое взаимодействие через TCP-порт 443 между серверами Ankey SIEM NG Core связываемых приложений.

При работе с правилами репликации событий необходимо учитывать ряд ограничений:

- между двумя приложениями можно создать только одно правило;
- правила не должны формировать направленный цикл;
- по умолчанию приложение-получатель не выполняет агрегацию, обогащение, корреляцию и привязку реплицированных событий к активам.

Примечание. Вы можете разрешить агрегацию (параметр RemoteEventsSkipAggregator), обогащение (параметр RemoteEventsSkipEnricher), корреляцию (параметр RemoteEventsSkipCorrelator) и привязку реплицированных событий к активам (параметр RemoteEventsSkipResolver) в приложении-получателе.

[5] Параметры конфигурации компонентов представлены в приложениях А и Б.

5.3 Добавление связей для распределенного поиска

❖ Чтобы добавить связи:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
3. На схеме выберите приложение.
4. В панели **Приложение Ankey SIEM NG** выберите вкладку **Распределенный поиск**.
5. В панели инструментов нажмите кнопку **Добавить связи**.
   Откроется окно **Новые связи для распределенного поиска**.
6. Укажите связанные приложения:
   – если требуется, чтобы в выбранном приложении были доступны события из других приложений, выберите эти приложения в раскрывающемся списке По другим приложениям;
   – если требуется, чтобы события выбранного приложения были доступны в других приложениях, − выберите эти приложения в раскрывающемся списке **По этому приложению**.
7. Нажмите кнопку **Добавить**.
8. Новые связи появятся на схеме и в панели **Приложение Ankey SIEM NG**.

Связи добавлены.

5.4 Удаление связи для распределенного поиска

❖ Чтобы удалить связь:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
3. На схеме выберите приложение.
4. В панели **Приложение Ankey SIEM NG** выберите вкладку **Распределенный поиск**.
5. Выберите связь.

> **Примечание.** Вы можете выбрать несколько связей подряд с помощью клавиши **Shift** или нескольких отдельных связей с помощью клавиши **Ctrl**.

6. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Связь удалена.

5.5 Добавление правила репликации событий

Перед добавлением правила необходимо убедиться, что в приложении-отправителе вам доступны страница **События** и группы активов, события на которых нужно реплицировать.

❖ Чтобы добавить правило:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
3. На схеме выберите приложение, которое будет отправлять реплицированные события.
4. В панели **Приложение Ankey SIEM NG** выберите вкладку **Репликация событий**.
5. В панели инструментов нажмите кнопку **Добавить правило репликации**.
   Откроется окно **Новое правило репликации**.
6. В поле **Получатель** укажите приложение, которое будет получать реплицированные события.
7. Нажмите кнопку **Настроить репликацию событий**.
   Откроется страница **События**.
8. В панели **Группы** выберите группы активов, события которых нужно реплицировать.
9. Если требуется, в панели **Фильтры** выберите фильтр событий.
10. Нажмите кнопку **Завершить настройку**.
11. Нажмите кнопку **Добавить**.
12. Новое правило репликации появится на схеме и в панели **Приложение Ankey SIEM NG**.

Правило добавлено.

5.6 Изменение правила репликации событий

Перед изменением правила необходимо убедиться, что в приложении-отправителе вам доступны страница **События** и группы активов, репликацию событий которых нужно изменить.

❖ Чтобы изменить правило:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
3. На схеме выберите приложение.
4. В панели **Приложение Ankey SIEM NG** выберите вкладку **Репликация событий**.
5. Выберите правило.
6. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется окно **Правило репликации**.
7. Нажмите кнопку **Настроить репликацию событий**.
   Откроется страница **События**.
8. Внесите изменения.
9. Нажмите кнопку **Завершить настройку**.

10. Нажмите кнопку **Сохранить**.

Правило изменено.

5.7 Удаление правила репликации событий

❖ Чтобы удалить правило:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню выберите раздел **Площадки**.
3. Откроется страница **Площадки**.
4. На схеме выберите приложение.
5. В панели **Приложение Ankey SIEM NG** выберите вкладку **Репликация событий**.
6. Выберите правило.
7. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Правило удалено.

6 Управление приложениями

Ankey SIEM NG MC предоставляет пользователю возможность переименовывать и удалять приложения, зарегистрированные на выбранной площадке. Для этого роль пользователя (см. раздел 3) должна содержать соответствующие привилегии − **Переименование приложений** и **Удаление приложений**. Переименовать или удалить приложение можно только с площадки, на которой оно зарегистрировано. Для перехода к нужной площадке необходимо в главном меню нажать ⁞⁞⁞ и выбрать площадку.

6.1 Переименование приложения

❖ Чтобы переименовать приложение:

1. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
2. На схеме выберите приложение.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется окно **Приложение <Название приложения> (<Псевдоним приложения>)**.
4. Если вы хотите изменить псевдоним приложения, в поле **Псевдоним** укажите новое значение.
5. Если вы хотите изменить название приложения, нажмите **Изменить название** и в поле **Название** укажите новое значение.

> **Примечание.** Вы можете вернуть приложению системное название. Для этого необходимо нажать **Изменить название**, удалить из поля **Название** существующее значение и оставить поле пустым.

6. Нажмите кнопку **Сохранить**.

Приложение переименовано.

6.2 Удаление приложения

> Внимание! После удаления приложение нельзя будет восстановить.

❖ Чтобы удалить приложение:

1. В главном меню выберите раздел **Площадки**.
   Откроется страница **Площадки**.
2. На схеме выберите приложение.

> **Примечание.** Удаление приложения Management and Configuration недоступно, потому что в нем зарегистрированы остальные приложения площадки.

3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

4. В открывшемся окне введите псевдоним удаляемого приложения с точностью до символа и нажмите **Удалить**.
5. Приложение удалено.

При удалении приложения Ankey SIEM NG MC сохраняет его идентификатор (ClientID), но удаляет связи, псевдоним и название, если оно было задано. При необходимости, вы можете повторно зарегистрировать приложение на площадке с использованным ранее идентификатором.

7 Управление политиками

Примечание. Работа с требованиями и стандартами доступна только при наличии соответствующей лицензии.

Специалистам по ИБ часто требуется анализировать состояние ИТ-инфраструктуры предприятия. При большом количестве сетевых узлов анализ, выполняемый вручную, может занимать значительное время, что замедлит реакцию на угрозы ИБ.

В Ankey SIEM NG предусмотрен механизм для автоматизации процессов устранения уязвимостей и контроля за регулярностью сканирования активов – политики. Политика состоит из совокупности правил, которые автоматически изменяют параметры объектов системы (например, сроки актуальности данных об активах или статусы экземпляров уязвимостей).

Политики содержат стандартные правила, которые по умолчанию отключены. Также вы можете создавать свои правила. Применение условий правила зависит от его номера по порядку внутри политики. Если объект системы может быть изменен несколькими правилами (например, один и тот же актив подходит под условия фильтрации нескольких правил), применятся условия первого по порядку правила. Вы можете менять порядок, перетаскивая правила в таблице.

При создании, удалении, включении и отключении правил, а также при изменении их параметров или порядка система не изменяет политику сразу: она создает черновик политики и вносит в него все изменения. Пока изменения не применены, система работает с двумя версиями политики: измененная версия (черновик) отображается в веб-интерфейсе и не применяется к объектам системы, исходная версия (чистовик) применяется к объектам и недоступна для просмотра в веб-интерфейсе. При большом количестве объектов применение изменений может занимать продолжительное время (до нескольких суток).

Если политику изменяют одновременно несколько пользователей, они работают с одним черновиком. В результате применятся изменения, внесенные тем пользователем, который последним работал с черновиком.

В Ankey SIEM NG доступны следующие политики.

Для значимости активов

Правила политики автоматически изменяют значимость активов. Определение значимости активов позволяет упорядочить работу с ними, выделить значимые активы, уязвимости на которых могут нанести больше всего вреда ИТ-инфраструктуре организации, и уделять им повышенное внимание. Необходимо стремиться к тому, чтобы для всех активов была указана значимость.

Для сроков актуальности данных

Правила политики автоматически устанавливают сроки актуальности и устаревания данных об активах, полученных в результате сканирования ИТ-инфраструктуры методами аудита и пентеста. Опасные уязвимости на активах, данные о которых редко обновляются, могут быть выявлены слишком поздно. Вы можете оценить количество активов, данные о которых не были получены вовремя, с помощью виджета **Актуальность данных об активах**, а также найти

их с помощью PDQL-запроса.

Для соответствия стандартам

Правила политики автоматически проверяют выбранные активы или группы активов на соответствие стандартам. Это позволяет вовремя выявлять активы, требующие внимания и устранять обнаруженные несоответствия. Вы можете оценить количество активов, соответствующих стандартам с помощью виджетов **Стандарты на активах** или **Соответствие активов стандартам**, а также найти их с помощью PDQL-запроса.

Для статусов несоответствий

Правила политики автоматически изменяют статус несоответствий активов требованиям, определяют срок их устранения или откладывают обработку на определенный срок. Вы можете оценить количество несоответствий с определенными статусами с помощью виджета **Активы по статусам несоответствий**, а также найти их с помощью PDQL-запроса.

Для статусов уязвимостей

Правила политики автоматически изменяют статус экземпляров уязвимостей, определяют срок их устранения или откладывают их обработку на определенный срок. Перечень запланированных к устранению уязвимостей можно выпускать в виде отчета по расписанию и отправлять по электронной почте системному администратору.

Для отметки «важная»

Правила политики автоматически отмечают отдельные экземпляры уязвимостей как важные. Например, в качестве важных могут быть отмечены наиболее опасные для ИТ-инфраструктуры уязвимости. Вы можете найти активы с важными уязвимостями с помощью PDQL-запроса.

Для работы с политиками предназначена страница **Система** → **Политики**.

7.1 Страница Политики

Страница предназначена для работы с политиками. В панели инструментов находятся следующие кнопки:

- **Создать правило** − для создания правила;
- **Редактировать** − для изменения параметров правила (см. подраздел 7.8);
- **Копировать** − для создания правила на основе имеющегося правила (см. подраздел 7.9);
- **Удалить** − для удаления правила (см. подраздел 7.11);
- **Включить** − для включения правила в работу (см. подраздел 7.10);
- **Отключить** − для приостановки работы правила (см. подраздел 7.10).

В рабочей области страницы расположены:

- панель **Список политик**. Содержит список политик и предназначена для выбора политики, применения изменений (см. подраздел 7.12, а также отмены не

примененных изменений (см. подраздел 7.13). При выборе политики составляющие ее правила отобразятся в центральной панели. Если политика имеет не примененные изменения, на левой границе строки с названием политики отобразится желтая полоска, в правой части строки − кнопка  для отмены изменений, а в нижней части панели − кнопка **Применить изменения**. Если выполняется применение изменений, слева от названия политики отобразится значок ;

– центральная панель. Содержит таблицу с правилами и предназначена для выбора правила и изменения порядка применения правил. При выборе правила сведения о нем отобразятся в правой части страницы в панели **<Название правила>**. В таблице отображаются следующие состояния правил:
   − правило работает;
   − правило остановлено;
   − правило работает с предупреждением;
   − правило не работает из-за ошибки. Такой же значок отобразится слева от названия политики с этим правилом.
– панель **<Название правила>**. Содержит сведения о правиле, а также отображает сообщения о его работе.

7.2 Создание правила для значимости активов

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для значимости активов.
3. Нажмите кнопку **Создать правило**. Откроется страница **Создание правила**.
4. Введите название правила.
5. В раскрывающемся списке выберите группы активов, для которых необходимо указывать значимость.

> **Примечание.** Вы также можете отфильтровать активы с помощью PDQL-запроса.

6. В раскрывающемся списке выберите значимость актива.
7. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.3 Создание правила для сроков актуальности данных

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для сроков актуальности данных.
3. Нажмите кнопку **Создать правило**. Откроется страница **Создание правила**.
4. Введите название правила.
5. В раскрывающемся списке выберите группы активов, для которых необходимо указывать сроки актуальности данных.

> **Примечание.** Вы также можете отфильтровать активы с помощью PDQL-запроса.

6. Если требуется, измените значения по умолчанию для сроков актуальности данных.
7. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.4 Создание правила для соответствия стандартам

Для выполнения инструкции требуется учетная запись с правами администратора.

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для соответствия стандартам.
3. Нажмите кнопку **Создать правило**. Откроется страница **Создание правила**.
4. Введите название правила.
5. В раскрывающемся списке выберите группы активов, которые необходимо проверять на соответствие стандарту.

> **Примечание.** Вы можете отфильтровать активы с помощью PDQL-запроса.

6. В раскрывающемся списке выберите стандарт, на соответствие которому необходимо проверять активы.
7. Нажмите кнопку **Сохранить**.
   Правило создано.
   Система начнет использовать правило только после применения изменений в политике (см. раздел 7.12).

7.5 Создание правила для статусов несоответствий

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.
   Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для статусов несоответствий.
3. Нажмите кнопку **Создать правило**.
   Откроется страница **Создание правила**.
4. Введите название правила.
5. В раскрывающемся списке **Группы активов** выберите группы активов, которые необходимо проверять на соответствие требованиям.

   Примечание. Вы можете ввести условие фильтрации активов на языке PDQL в поле **Фильтр активов**.

6. В поле **Фильтр требований** введите запрос на языке PDQL для поиска тех экземпляров требований, статусы которых необходимо изменять.
7. В панели **Результат применения правила** в раскрывающемся списке **Действие** выберите действие, которое необходимо выполнять при несоответствии актива требованиям.
8. Если требуется запланировать устранение несоответствия актива требованиям, в поле **Срок исправления** укажите срок выполнения этой задачи.
9. Если требуется исключать несоответствия требованиям из мониторинга, в раскрывающемся списке **Уточнение к статусу** выберите причину исключения.

   Примечание. По истечении срока исключения несоответствия требованиям будут снова проверены правилами политики. Если требуется вручную устранять выявленные в результате повторной проверки несоответствия требованиям, нужно в раскрывающемся списке **Устранение** выбрать **Вручную**.

10. Нажмите кнопку **Сохранить**.
    Правило создано.
11. Система начнет использовать правило только после применения изменений в политике (см. раздел 7.12).

7.6 Создание правила для статусов уязвимостей

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.
   Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для статусов уязвимостей.
3. Нажмите кнопку **Создать правило**.

Откроется страница **Создание правила**.

4. Введите название правила.
5. В поле Фильтр уязвимостей введите запрос на языке PDQL для поиска тех экземпляров уязвимостей, статусы которых необходимо изменять.

> **Примечание.** Для уточнения результатов поиска вы можете указать группы активов, а также отфильтровать активы с помощью условия на языке PDQL.

6. В раскрывающемся списке выберите действие, которое необходимо выполнять с экземплярами уязвимостей.
7. Если требуется исключать из мониторинга экземпляры уязвимостей, в раскрывающемся списке **Уточнение к статусу** выберите причину исключения.

> **Примечание.** По истечении срока исключения экземпляры уязвимостей будут по умолчанию запланированы к устранению в течение семи дней. Если требуется устранять экземпляры уязвимостей вручную, необходимо выбрать это действие в раскрывающемся списке **Устранение**.

8. Нажмите кнопку **Сохранить**.
   Правило создано.
   Система начнет использовать правило только после применения изменений в политике (см. раздел 7.12).

7.7 Создание правила для отметки «важная»

❖ Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.
   Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для отметки «важная».
3. Нажмите кнопку **Создать правило**.
   Откроется страница **Создание правила**.
4. Введите название правила.
5. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска экземпляров уязвимостей, которые необходимо отмечать как важные.

> **Примечание.** Для уточнения результатов поиска вы можете указать группы активов, а также отфильтровать активы с помощью условия на языке PDQL.

6. Нажмите кнопку **Сохранить**.
7. Правило создано.
8. Система начнет использовать правило только после применения изменений в политике (см. раздел 7.12).

7.8 Изменение правила

Вы можете изменять только пользовательские правила, стандартные правила недоступны для изменения.

❖ Чтобы изменить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Редактировать**. Откроется окно **Редактирование правила <Название правила>**.
5. Внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило изменено.

Система начнет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.9 Копирование правила

❖ Чтобы скопировать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Копировать**. Откроется окно **Создание правила**.
5. Если требуется, внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило скопировано.

Система начнет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.10 Включение и отключение правила

❖ Чтобы включить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Включить**.

Правило включено. Система начнет использовать правило только после применения изменений в политике (см. подраздел 7.12).

❖ Чтобы отключить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Отключить**.

Правило отключено. Система перестанет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.11 Удаление правила

Вы можете удалять только пользовательские правила, стандартное правило удалить невозможно.

❖ Чтобы удалить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**. Откроется страница **Политики**.
2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Удалить**.

Правило удалено.

Система перестанет использовать правило только после применения изменений в политике (см. подраздел 7.12).

7.12 Применение изменений в политиках

Приведенная инструкция описывает применение изменений, внесенных в несколько политик. Если изменения внесены только в одну политику, для их применения необходимо в панели **Список политик** нажать кнопку **Применить изменения**.

❖ Чтобы применить изменения, внесенные в несколько политик:

1. В панели Список политик нажмите кнопку **Применить изменения**.
2. Откроется окно **Применение изменений**.
3. Установите флажки с названиями политик, изменения в которых необходимо применить.
4. Нажмите кнопку **Применить**.

Изменения применены.

7.13 Отмена изменений в черновике политики

❖ Чтобы отменить изменения:

1. В панели **Список политик** наведите курсор на строку с названием политики и нажмите ⋮.
2. В открывшемся меню выберите пункт **Сбросить изменения**.

Изменения отменены.

8 Мониторинг источников событий

Для уменьшения вероятности пропуска инцидентов ИБ необходимо своевременно отслеживать состояние источников событий и потока данных от них. Качество и непрерывность сбора данных с источников влияют на оперативность выявления инцидентов и принятия решений.

Данные от источников передаются в ПК Ankey SIEM NG напрямую (без посредников) или через промежуточный актив − форвардер (например, через контроллер домена). Форвардер, кроме пересылки данных от других активов, также может отправлять данные от находящихся в нем источников.

Источники и форвардеры появляются в системе автоматически, по мере сбора событий с активов и их идентификации. На странице **Мониторинг источников** пользователь системы может просмотреть состояние источников и параметры потока данных от них или состояние форвардеров и параметры находящихся в них источников. Ссылка для выбора типа элементов (источников или форвардеров) находится в верхней части рабочей области страницы.

Если вы выбрали по ссылке работу с источниками, рабочая область страницы **Мониторинг источников** содержит:

- панель **Источники** для поиска источников, которые находятся на активах выбранной группы и вложенных в нее групп;
- панель **Фильтры** для фильтрации источников по условию наличия или отсутствия предупреждений;
- панель управления с возможностью настраивать, отключать или включать предупреждения для источника, удалять источники из списка, экспортировать и обновлять список источников, искать источники в списке;
- центральную панель с таблицей источников, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от источника).

Если вы выбрали по ссылке работу с форвардерами, рабочая область страницы **Мониторинг источников** содержит:

- панель **Форвардеры** для поиска форвардеров, которые содержатся в выбранной группе активов и вложенных в нее группах;
- панель **Фильтры** для фильтрации форвардеров по условию наличия или отсутствия предупреждений;
- панель управления с возможностью настраивать, отключать или включать предупреждения для форвардера, удалять форвардеры из списка, экспортировать и обновлять список форвардеров, искать форвардеры в списке;
- центральную панель с таблицей форвардеров, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от форвардера).

Примечание. По умолчанию на странице **Мониторинг источников** отображаются все источники (форвардеры), связанные с группами активов, к которым оператору предоставлен доступ.

8.1 Просмотр списка источников и списка потоков событий от источника

❖ Чтобы просмотреть список источников:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт Ankey SIEM NG.
   Откроется главная страница.
2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.
   Откроется страница **Мониторинг источников**.

В центральной панели отображена таблица со списком источников.

Для каждого источника в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

Примечание. Срок хранения данных, полученных от источника, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров вы можете создавать предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события коллектором. Состояние предупреждения отображается в столбце **Контроль** соответствующим значком:

- – параметры потока событий находятся в пределах допустимых значений;
- – параметры потока событий вышли за пределы допустимых значений;
- – предупреждение отключено.

При наведении курсора мыши на значок предупреждения во всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

Примечание. Источник автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от источника.

Также вы можете настраивать отправку уведомлений для получения по электронной почте информации о потоке событий от источника или форвардера.

❖ Чтобы просмотреть список потоков событий от источника, откройте страницу со списком потоков событий двойным щелчком мыши на строке с названием источника.

8.2 Просмотр списка форвардеров и списка источников форвардера

❖ Чтобы просмотреть список форвардеров:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт Ankey SIEM NG.
   Откроется главная страница.
2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.
   Откроется страница **Мониторинг источников**.

В центральной панели отображена таблица со списком форвардеров.

Для каждого форвардера в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

Примечание. Срок хранения данных, полученных от форвардера, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров вы можете создавать предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события коллектором. Состояние предупреждения отображается в столбце **Контроль** соответствующим значком:

- – параметры потока событий находятся в пределах допустимых значений;
- – параметры потока событий вышли за пределы допустимых значений;
- – предупреждение отключено.

При наведении курсора мыши на значок предупреждения во всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

Примечание. Форвардер автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от форвардера.

❖ Чтобы просмотреть список источников форвардера, откройте страницу со списком источников двойным щелчком мыши на строке с названием форвардера.

8.3 Создание предупреждения для отслеживания наличия событий

❖ Чтобы создать предупреждение для отслеживания наличия событий:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. В панели инструментов нажмите кнопку **Настроить предупреждения**.
   Откроется страница **Настройка предупреждений для источника <Название источника>**.
3. Включите отслеживание наличия событий.
4. По ссылкам укажите период, в котором необходимо отслеживать наличие событий, с учетом часового пояса.
5. Нажмите кнопку **Добавить**.

> **Примечание.** Вы можете добавлять до десяти периодов. Периоды не должны пересекаться.

6. Нажмите кнопку **Сохранить**.

Предупреждение создано. Отслеживание наличия событий запущено.

8.4 Создание предупреждения для отслеживания средней скорости потока событий

❖ Чтобы создать предупреждение для отслеживания средней скорости потока событий:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. В панели инструментов нажмите кнопку **Настроить предупреждения**.
   Откроется страница **Настройка предупреждений для источника <Название источника>**.
3. Включите отслеживание средней скорости потока событий.
4. По ссылке выберите, какие значения средней скорости необходимо отслеживать (абсолютные или относительные).
5. По ссылкам укажите интервал, в котором необходимо отслеживать среднюю скорость, с учетом часового пояса.

6. В поле правее введите продолжительность периода для вычисления средней скорости.

> **Примечание.** Продолжительность периода для вычисления средней скорости не должна превышать продолжительность интервала, в котором необходимо отслеживать среднюю скорость.

7. Если вы выбрали отслеживание абсолютного значения средней скорости потока событий, в полях **Минимум** и **Максимум** введите пороговые значения средней скорости.
8. Если вы выбрали отслеживание относительного значения средней скорости потока событий, в полях **Уменьшение** и **Увеличение** введите пороговые значения в процентах относительно средней скорости.
9. Нажмите кнопку **Добавить**.

> **Примечание.** Вы можете добавлять до десяти периодов. Периоды не должны пересекаться.

10. Нажмите кнопку **Сохранить**.

Предупреждение создано. Отслеживание средней скорости потока событий запущено.

8.5 Создание предупреждения для отслеживания задержки в получении события коллектором

❖ Чтобы создать предупреждение для отслеживания задержки в получении события коллектором:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. В панели инструментов нажмите кнопку **Настроить предупреждения**.
   Откроется страница **Настройка предупреждений для источника <Название источника>**.
3. Включите отслеживание задержки в получении события коллектором.
4. Введите значение задержки и по ссылке укажите единицу измерения времени (минуты или часы).
5. Нажмите кнопку **Сохранить**.

Предупреждение создано. Отслеживание задержки в получении события коллектором запущено.

8.6 Остановка и повторный запуск отслеживания потока событий

Вы можете остановить отслеживание потока событий от источника или форвардера (например, на время проведения плановых работ по техническому обслуживанию актива).

❖ Чтобы остановить отслеживание потока событий:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

6. В панели инструментов нажмите кнопку **Отключение предупреждения**.
7. Слева от названия источника (форвардера) отобразится значок ✔.

Отслеживание потока событий остановлено.

❖ Чтобы запустить отслеживание потока событий:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. В панели инструментов нажмите кнопку **Включение предупреждения**.
3. Слева от названия источника (форвардера) отобразится значок ✔.

Отслеживание потока событий запущено.

8.7 Удаление источника (форвардера) из списка

Источник (форвардер) автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Вы также можете удалить источник (форвардер) из списка вручную.

❖ Чтобы удалить источник (форвардер) из списка вручную:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. Нажмите кнопку **Настроить предупреждения**.

Откроется страница **Настройка предупреждений для источника <Название источника>**.

3. Убедитесь, что отключено отслеживание наличия событий, средней скорости потока событий и задержки в получении события коллектором.
4. Нажмите кнопку **Сохранить**.
5. Нажмите кнопку **Удалить источник** или кнопку **Удалить форвардер** и подтвердите удаление.

Источник (форвардер) удален из списка.

8.8 Экспорт списка источников (форвардеров) в текстовый файл

Вы можете экспортировать в текстовый файл список всех источников (форвардеров) или список выбранных источников (форвардеров).

❖ Чтобы экспортировать список всех источников (форвардеров):

1. На странице **Мониторинг источников** в панели инструментов нажмите кнопку **Экспортировать список**.
2. В открывшемся окне выберите вариант экспорта списка всех источников (форвардеров).
3. Нажмите кнопку **Экспортировать**.
   Браузер загрузит текстовый файл со списком источников (форвардеров).

Список всех источников (форвардеров) экспортирован в текстовый файл.

❖ Чтобы экспортировать список выбранных источников (форвардеров):

1. На странице **Мониторинг источников** в центральной панели выберите строки с названиями источников (форвардеров).

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

2. Нажмите кнопку **Экспортировать список**.
3. В открывшемся окне выберите вариант экспорта выбранных источников (форвардеров).
4. Нажмите кнопку **Экспортировать**.
   Браузер загрузит текстовый файл со списком источников (форвардеров).

Список выбранных источников (форвардеров) экспортирован в текстовый файл.

8.9 Обновление списка источников (форвардеров)

Вы можете обновлять список источников (форвардеров) вручную или настраивать автоматическое обновление списка.

❖ Чтобы обновить список источников (форвардеров) вручную, в верхней правой части страницы Мониторинг источников нажмите .

❖ Чтобы настроить автоматическое обновление списка источников (форвардеров):

1. В верхней правой части страницы **Мониторинг источников** нажмите .
2. В открывшемся окне установите флажок **Автоматически обновлять** и выберите период обновления.

Автоматическое обновление списка источников (форвардеров) настроено.

9 Мониторинг состояния ПК Ankey SIEM NG

В ПК Ankey SIEM NG реализован автоматический мониторинг параметров жизнеспособности и целостности системы и ее компонентов. Источником для мониторинга служат статистические данные за определенные периоды. Результаты мониторинга отображаются по нажатию индикатора состояния системы. Предусмотрены также цветовые индикаторы уровня опасности события:

- красный – сообщает о неполадке или сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен);
- желтый − сообщает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра);
- зеленый − сообщает о том, что система работает корректно;
- синий − сообщает о каком-либо событии, не нарушающем жизнеспособность и целостность системы или ее компонента.
- белый – сообщает о том, что диагностику системы выполнить не удалось.

9.1 Страница Управление системой

Страница **Управление системой** предназначена для просмотра состояния лицензии, управления коллекторами сбора данных, а также для просмотра информации об используемой базе знаний по уязвимостям и обновления этой базы вручную.

В рабочей области страницы расположены центральная панель и панель **Компоненты**, в которой доступны следующие разделы.

О системе

Раздел предназначен для просмотра информации о лицензии, версиях системы и компонента Ankey SIEM NG Core. На странице доступна информация об истечении срока действия лицензии, отсутствии лицензии или валидного ключа. Также система уведомляет о том, что срок действия лицензии заканчивается, за 14 дней до ее окончания.

Конвейеры

Раздел предназначен для просмотра подробной информации о конвейерах обработки событий, для их переименования и удаления. При выборе раздела в центральной панели отобразится таблица с конвейерами. Для каждого конвейера в таблице указаны статус, псевдоним, доменное имя и IP-адреса сервера Ankey SIEM NG Server, версии Ankey SIEM NG Server и установленной на нем схемы полей событий, семейство ОС сервера.

Вы можете сортировать список, нажимая на названия колонок таблицы, а также обновлять список с помощью значка в правой верхней части таблицы.

При выборе конвейера подробная информация о нем появится в боковой панели, в том числе перечень подключенных к нему коллекторов.

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). В боковой панели для него в качестве значения поля **Тип** отображается значок и отметка Главный конвейер.

В таблице отображаются следующие статусы конвейера:

- **Доступен** − конвейер работает в нормальном режиме;
- **Недоступен** − Ankey SIEM NG Core не получает отклика от компонента Ankey SIEM NG Server конвейера.

В панели инструментов находятся следующие кнопки:

- **Переименовать** − для изменения псевдонима конвейера.
- **Удалить** − для удаления конвейера из списка.

> **Примечание.** Невозможно удалить конвейер, к которому подключены коллекторы, а также единственный конвейер в списке.

Коллекторы

Раздел предназначен для просмотра подробной информации об коллекторах, для обновления их версий и удаления недоступных коллекторов. При выборе раздела в центральной панели отобразится таблица с коллекторами. Для каждого коллектора в таблице указаны название, версия, статус, роли, а также имя, IP-адреса и семейство ОС сервера.

Вы можете сортировать список, нажимая на названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая в правой верхней части таблицы.

Для поиска коллектора в списке вы можете нажать и ввести в поле поиска параметр коллектора.

При выборе коллектора система отображает подробную информацию о нем в боковой панели, в том числе перечень модулей коллектора.

В таблице отображаются следующие статусы коллектора:

- **Доступен** – коллектор работает в нормальном режиме;
- **С ограничениями** – коллектор работает в режиме ограниченной функциональности по причине нехватки свободного места на жестком диске;
- **Недоступен** – Ankey SIEM NG Core не получает отклика от коллектора более 10 минут;
- **Обновляется** – коллектор обновляется;
- **Удаляется** – коллектор удаляется из списка.

В панели инструментов находятся следующие кнопки:

- **удалить** – для удаления недоступного коллектора (см. подраздел 9.2). Если после удаления коллектор начнет присылать данные, он снова будет отображаться в списке;
- **обновить версию** – для обновления версии коллектора.

База уязвимостей

Раздел предназначен для просмотра информации о базе уязвимостей, используемой в Ankey SIEM NG Core, а также для обновления базы уязвимостей вручную. По умолчанию система автоматически проверяет наличие обновлений каждые пять минут.

Обработка активов

Раздел предназначен для просмотра информации о работе служб Ankey SIEM NG Core на различных этапах обработки данных об активах.

Для каждого этапа в таблице указаны название используемой службы, длина очереди, время ожидания обработки, номера пакетов в очереди, номера последних обработанных пакетов и средняя скорость обработки пакетов за 5 минут.

9.2 Удаление коллектора сбора событий из списка

Коллектор, который был установлен в системе, а затем выведен из ее состава (например, по причине неисправности сервера коллектора), автоматически не удаляется из списка коллекторов и продолжает отображаться в интерфейсе со статусом **Недоступен**. После удаления коллектора будут автоматически остановлены:

- если удаленный коллектор был выбран в задаче автоматически − использующие его подзадачи сбора событий;
- если удаленный коллектор был выбран вручную − использующие его задачи.

❖ Чтобы удалить коллектор сбора событий из списка:

1. В главном меню в разделе **Система** выберите пункт **Управление системой**.
   Откроется страница **Управление системой**.
2. В панели **Компоненты** выберите пункт **Коллекторы**.
   В рабочей области страницы отобразится таблица со списком коллекторов.
3. Выберите коллектор со статусом **Недоступен**, который необходимо удалить.

> **Примечание.** Вы можете выбирать несколько строк подряд, нажимая клавишу **Shift**, или несколько отдельных строк, нажимая клавишу **Ctrl**.

4. В панели управления нажмите кнопку **Удалить из списка** и подтвердите удаление.

> **Примечание.** Окно подтверждения удаления появляется в случае, когда удаляемый коллектор используется запущенными задачами сбора событий.

Статус удаляемого коллектора изменится на **Удаляется**. По завершении удаления коллектор не будет отображаться в списке.

Коллектор сбора событий удален из списка.

9.3 Мониторинг работы правил корреляции

ПК Ankey SIEM NG отслеживает объем оперативной памяти, занимаемой правилами корреляции, и количество срабатываний для каждого правила. На основании результатов мониторинга система приостанавливает работу правила корреляции в следующих случаях:

- если все правила занимают более 95% от объема оперативной памяти, выделенной для их работы (по умолчанию 60 ГБ). В этом случае система начинает последовательно приостанавливать работу отдельных правил до тех пор, пока не освободится 20% от объема выделенной памяти;
- если отдельное правило срабатывает слишком часто (по умолчанию более 300 раз за час).

Система автоматически не запускает приостановленные правила − их необходимо запускать вручную. Также приостановленные правила запустятся в случае перезапуска службы SIEM Server correlator.

Отдельные правила можно добавлять в список исключений. Система не приостанавливает работу этих правил, если они срабатывают слишком часто, и приостанавливает их работу в последнюю очередь, когда освобождает выделенную для работы правил оперативную память. Для включения правил в список исключений необходимо добавить их системные названия в текстовый файл (каждое название в отдельной строке) и указать путь к файлу в качестве значения параметра ProtectedRulesPath.

Вы можете изменять объем оперативной памяти, выделенной для работы правил корреляции (параметр MonitoringOomMemoryLimit), или вовсе отключить отслеживание объема оперативной памяти, занимаемой правилами (параметр MonitoringOomEnabled).

Также вы можете изменять период для подсчета количества срабатываний правил корреляции (параметр MonitoringOvertriggerPeriod), максимальное количество срабатываний за этот период, которое не приведет к остановке правила (параметр MonitoringOvertriggerThreshold), или вовсе отключить отслеживание количества срабатываний для всех правил (параметр MonitoringOvertriggerEnabled).

10 Резервное копирование данных

Вы можете создавать резервные копии данных компонентов Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base и Ankey SIEM NG Server с помощью сценариев. Также вы можете создавать резервные копии индексов Elasticsearch и данные хранилища LogSpace. При создании резервной копии данных и при их последующем восстановлении из резервной копии должны совпадать конфигурации Ankey SIEM NG, версии компонента Ankey SIEM NG и языки интерфейса ОС.

Во время создания резервной копии сценарий останавливает службы компонентов, поэтому веб-интерфейс системы будет недоступен. Данные, собираемые коллекторами во время создания копии, не отправляются другим компонентам системы и накапливаются на серверах коллекторов. По завершении создания копии эти данные будут отправлены одновременно всеми коллекторами, что создаст повышенную нагрузку на систему и может привести к появлению ошибок в ее работе. Поэтому перед созданием резервной копии рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период создания резервной копии не запланирован запуск задач по расписанию.

Для резервного копирования данных компонентов на Linux необходимо создать резервные копии данных ролей в следующем порядке: **SIEM Server** → **Core** → **Knowledge Base** → **SqlStorage** или **JatobaStorage** → **Deployer**. Для резервного копирования данных каждой роли вам потребуется отдельный сценарий backup.sh, который после установки роли находится в каталоге /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/. Сценарий необходимо запускать в интерфейсе терминала Linux от имени суперпользователя (root).

Сценарии резервного копирования не создают копию индексов Elasticsearch, копию цифрового сертификата, заверенного подписью удостоверяющего центра, а также не сохраняют пароли служебных учетных записей, отличные от паролей по умолчанию.

10.1 Создание резервной копии данных роли на Linux

Внимание! Перед созданием резервной копии необходимо сохранить копию файлов цифровых сертификатов роли. После восстановления данных роли из резервной копии необходимо добавить файлы сертификатов в каталог /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs.

❖ Чтобы создать резервную копию данных, запустите сценарий резервного копирования данных:

/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/backup.sh <Путь к каталогу для размещения архива с резервной копией данных>

Например:

/var/lib/deployed-roles/mc-application-ankey/sqlstorage/backup.sh /backup

Архив backup.tar с резервной копией данных будет сохранен в каталоге /backup/mc-application-ankey/sqlstorage.

10.2 Создание резервной копии индексов Elasticsearch на Linux

Если в системе запущена задача архивации индексов по расписанию, перед созданием резервной копии необходимо ее остановить.

Для регистрации хранилища резервной копии индексов в Elasticsearch используется утилита es_initrepo, которую необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

❖ Чтобы создать резервную копию индексов Elasticsearch на Linux:

1. Укажите путь к каталогу для хранения резервной копии индексов:
   /opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу для хранения резервной копии индексов>"

> Внимание! Резервную копию индексов и копии индексов, создаваемые при архивации по расписанию, необходимо хранить в разных каталогах. Во избежание переполнения корневой файловой системы рекомендуется для хранения резервной копии смонтировать к каталогу отдельное дисковое устройство.

Утилита es_initrepo зарегистрирует в Elasticsearch хранилище резервной копии индексов и свяжет его с указанным каталогом. После регистрации хранилища интерфейс терминала Linux выведет сообщение:
Repository <Название хранилища> created successfully.

> **Примечание.** Команда также перезапустит службы Elasticsearch. После перезапуска Elasticsearch начнет восстанавливать индексы и будет некоторое время недоступен.

2. Создайте резервную копию индексов:
   – если требуется выполнить резервное копирование индексов, созданных за определенный период, выполните команду:
     /opt/estools/bin/es_backup_tool -cmd backup -from <Дата начала периода> -to <Дата окончания периода> -host 127.0.0.1 -port 9200 -di false

     Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

   – если требуется выполнить резервное копирование индексов, с момента создания которых прошло не меньше определенного количества дней, выполните команду:
     /opt/estools/bin/es_backup_tool -cmd backup -t <Количество дней> -host 127.0.0.1 –port 9200 -di false

     > **Примечание.** Значение параметра -t должно быть больше нуля.

– если требуется создать резервную копию всех индексов, выполните команду:
/opt/estools/bin/es_backup_tool -cmd full_backup -host 127.0.0.1 -port 9200
Утилита es_backup_tool сформирует из индексов, созданных системой за каждые сутки, отдельные файлы резервной копии. После создания каждого из этих файлов интерфейс терминала Linux отобразит сообщение: snapshot_<Дата создания индексов> created successfully

Резервная копия индексов Elasticsearch на Linux создана.

Если задача архивации индексов по расписанию была остановлена, после создания резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

10.3 Создание резервной копии данных хранилища LogSpace

Резервное копирование данных из хранилища LogSpace осуществляется с помощью утилиты backup_tool. Утилита входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

Внимание! Утилита поддерживает только полное резервное копирование данных. Инкрементальное резервное копирование невозможно.

❖ Чтобы создать резервную копию данных, на сервере с ролью Event Storage выполните команду:

/opt/dbtools/bin/backup_tool --cmd full_backup --repopath /<Каталог для резервной копии данных>

Например:

/opt/dbtools/bin/backup_tool --cmd full_backup --repopath /backup_dir

Резервная копия данных будет сохранена в каталоге /backup_dir.

Примечание. При выполнении команды full_backup без ключа --repopath резервная копия данных будет сохранена в каталоге /db_backup.

10.4 О резервном копировании данных о площадках и их связях

После регистрации всех площадок и добавления необходимых связей рекомендуется создать резервную копию данных компонентов Ankey SIEM NG Core и Ankey SIEM NG MC, расположенных на всех площадках. При последующих изменениях в схеме площадок (например, после регистрации новой площадки или добавления связей) рекомендуется создавать резервные копии данных компонентов Ankey SIEM NG Core и Ankey SIEM NG MC, расположенных на главной площадке, на зарегистрированной площадке, а также на тех площадках, связи с которыми были изменены, удалены или добавлены.

11 Восстановление данных из резервной копии

Вы можете восстанавливать данные Ankey SIEM NG Deployer и компонентов Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base и Ankey SIEM NG Server из резервных копий с помощью сценариев. Также вы можете восстанавливать из резервных копий индексы Elasticsearch и данные хранилища LogSpace. При создании резервной копии данных и при их последующем восстановлении из резервной копии должны совпадать конфигурации ПК Ankey SIEM NG, версии компонента ПК Ankey SIEM NG и языки интерфейса ОС.

Данные компонентов на Linux необходимо восстанавливать в следующем порядке: **Deployer** → **SqlStorage** или **JatobaStorage** → **Knowledge Base** → **Core** → **SIEM Server**. Для восстановления данных каждой роли вам потребуется отдельный сценарий restore.sh, который после установки роли находится в каталоге /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземляра роли>/. Сценарий необходимо запускать в интерфейсе терминала Linux от имени суперпользователя (root).

Инструкции по восстановлению данных содержат шаги по установке компонентов. Поэтому данные компонентов необходимо восстанавливать на сервере с чистой операционной системой.

11.1 Восстановление данных компонентов Ankey SIEM NG на Linux из резервной копии

Внимание! После восстановления компонентов ПК Ankey SIEM NG из резервных копий дополнительно требуется переустановка компонента Ankey SIEM NG Collector и повторная активация лицензии, подробнее см. документ Руководство по инсталляции Ankey SIEM NG 5.2.3 (с компонентом VM).

Для восстановления данных вам потребуются архивы с дистрибутивами ролей. Их версии должны совпадать с версиями дистрибутивов, которые были использованы при создании резервной копии.

Если при создании резервной копии компоненты Ankey SIEM NG Server и Ankey SIEM NG ES находились на отдельных серверах, при восстановлении данных необходимо также выделить для этих компонентов отдельные серверы.

Перед восстановлением данных необходимо разместить резервную копию на сервере роли Deployer, а также распаковать на этом сервере архивы с дистрибутивами ролей.

❖ Чтобы восстановить данные компонентов на Linux:

1. Установите роль Deployer.
2. Если при создании резервной копии компоненты Ankey SIEM NG Server и Ankey SIEM NG ES были установлены на отдельных серверах, установите на сервера этих компонентов модули Salt Minion.

3. Для каждой роли в следующей последовательности **SqlStorage** или **JatobaStorage** → **Knowledge Base** → **RMQ Message Bus** → **Core** → **SIEM Storage** → **SIEM Server**→ **Collector** выполните сценарий:
   cd /opt/deployer/bin
   ./Install-RolePackage.ps1 -ManifestPath <Путь к файлам дистрибутива роли>/package.yaml
   Например:
   cd /opt/deployer/bin
   ./Install-RolePackage.ps1 -ManifestPath /home/Roles/ SqlStorage_<номер версии> /package.yaml
4. Восстановите данные роли Deployer:
   /var/lib/deployed-roles/<Идентификатор приложения Deployer>/<Название экземпляра роли Deployer>/restore.sh /backup

> Внимание! Файл с резервными копиями backup.tar должен лежать по пути:
> /backup/<Идентификатор приложения Deployer>/<Название экземпляра роли Deployer>/backup.tar

5. Для каждой роли в каталоге /var/lib/deployer/role_instances/<Название роли> в файле instance.yaml в качестве значения параметра HostId укажите идентификатор Salt Minion.
6. Для каждой роли в каталоге /var/lib/deployer/role_instances/<Название роли> в файлах params.yaml и params.default.yaml в качестве значений параметров, содержащих FQDN, укажите FQDN серверов, на которые будут установлены соответствующие роли.

> **Примечание.** Для быстрой замены значений параметров можно использовать команду find /var/lib/deployer/ -name "params*.yaml" -exec sed -i 's/<FQDN сервера, на который была установлена роль>/<FQDN сервера, на который будет установлена роль>/' {} \;

7. Установите роль SqlStorage или JatobaStorage.
8. Восстановите данные роли SqlStorage или JatobaStorage:
   /var/lib/deployed-roles/<Идентификатор приложения SqlStorage/JatobaStorage>/<Название экземпляра роли SqlStorage/JatobaStorage>/restore.sh /backup

> Внимание! Файл с резервными копиями backup.tar должен лежать по пути:
> /backup/<Идентификатор приложения SqlStorage/JatobaStorage>/<Название экземпляра роли SqlStorage/JatobaStorage>/backup.tar

9. Установите роли Management and Configuration и Knowledge Base.

10. Восстановите данные роли Knowledge Base:
/var/lib/deployed-roles/<Идентификатор приложения Knowledge Base>/<Название экземпляра роли Knowledge Base>/restore.sh /backup

> Внимание! Файл с резервными копиями backup.tar должен лежать по пути:
> /backup/<Идентификатор приложения Knowledge Base>/<Название экземпляра роли Knowledge Base>/backup.tar

11. Установите роли RMQ Message Bus и Core.
12. Восстановите данные роли Core:
/var/lib/deployed-roles/<Идентификатор приложения Core>/<Название экземпляра роли Core>/restore.sh /backup

> Внимание! Файл с резервными копиями backup.tar должен лежать по пути:
> /backup/<Идентификатор приложения Core>/<Название экземпляра роли Core>/backup.tar

13. Установите роль SIEM Storage.
14. Установите роли RMQ Message Bus и SIEM Server.
15. Восстановите данные роли SIEM Server:
/var/lib/deployed-roles/<Идентификатор приложения SIEM Server>/<Название экземпляра роли SIEM Server>/restore.sh /backup

> Внимание! Файл с резервными копиями backup.tar должен лежать по пути:
> /backup/<Идентификатор приложения SIEM Server>/<Название экземпляра роли SIEM Server>/backup.tar

16. Установите роль Collector.

> **Примечание.** При резервном копировании данные роли Collector не сохраняются, поэтому роль необходимо устанавливать заново.

Данные компонентов восстановлены.

17. После восстановления данных необходимо для каждой из ролей добавить файлы сертификатов, сохраненные на этапе резервного копирования (см. раздел 10.1), в каталоги /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs.

11.2 Восстановление индексов Elasticsearch из резервной копии на Linux

При восстановлении индексов Elasticsearch из резервной копии на Linux

вы можете восстановить как все индексы, так и индексы, созданные за определенный период.

Внимание! Восстановление индексов, созданных за определенный период, возможно только на том сервере, где была создана резервная копия этих индексов.

Если в системе запущена задача архивации индексов по расписанию, перед восстановлением индексов из резервной копии необходимо ее остановить.

Вы можете просмотреть список архивных индексов с помощью соответствующей команды (см. раздел 12.1)

11.2.1 Восстановление всех индексов Elasticsearch из резервной копии на Linux

❖ Чтобы восстановить индексы Elasticsearch из резервной копии на Linux:

1. На сервере Ankey SIEM NG Server остановите службу SIEM Server storage и все службы Elasticsearch:
   systemctl stop -a elasticsearch* siemserver-storage.service
2. Удалите каталог с индексами:
   rm -rf /<Путь к каталогу индексов>/*
3. Запустите все службы Elasticsearch:
   systemctl start -a elasticsearch*
4. Запустите службу SIEM Server storage для загрузки шаблона индекса:
   systemctl start siemserver-storage.service
5. Остановите службу SIEM Server storage:
   systemctl stop siemserver-storage.service
6. Восстановите индексы из файла резервной копии:
   /opt/estools/bin/es_backup_tool -cmd full_restore
   После восстановления данных из файла интерфейс терминала отобразит сообщение:
   restored snapshot: snapshot_<Дата создания индексов>
7. Запустите службу SIEM Server storage:
   systemctl start siemserver-storage.service
   Индексы Elasticsearch восстановлены из резервной копии на Linux.
   Если задача архивации индексов по расписанию была остановлена, после восстановления данных из резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

11.2.2 Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux

❖ Чтобы восстановить индексы Elasticsearch, созданные за определенный период, из резервной копии на Linux, выполните команду:

/opt/estools/bin/es_backup_tool -cmd restore -host 127.0.0.1 -port 9200 -arc snapshot_<Дата создания индексов>

После восстановления данных из файла интерфейс терминала отобразит сообщение:

restored snapshot: snapshot_<Дата создания индексов>

Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) – один отдельный символ.

Индексы Elasticsearch восстановлены из резервной копии на Linux.

Если задача архивации индексов по расписанию была остановлена, после восстановления данных из резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

11.3 Восстановление данных хранилища LogSpace из резервной копии

Вы можете восстановить данных хранилища LogSpace из резервной копии с помощью утилиты backup_tool. Утилита входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

❖ Чтобы восстановить данные из резервной копии:

1. На сервере Ankey SIEM NG Server остановите службу Ankey SIEM NG ES:

   systemctl stop siemserver-storage.service

2. Удалите таблицы events, counters и cp из базы данных, в которую планируете восстанавливать данные:

   logspace-client --query 'truncate table siem.events'
   logspace-client --query 'truncate table siem.counters'
   logspace-client --query 'truncate table siem.cp'
   logspace-client --query 'drop table siem.events'
   logspace-client --query 'drop table siem.counters'
   logspace-client --query 'drop table siem.cp'

3. На сервере с ролью Event Storage выполните команду:

   /opt/dbtools/bin/backup_tool --cmd full_restore -db <Название базы данных> --arc <Название резервной копии > --repopath /<Каталог с резервной копией данных>

   Например:

   /opt/dbtools/bin/backup_tool --cmd full_restore -db logspace_db --arc siem.*.20220512.000001 --repopath /backup_dir

Примечание. При выполнении команды full_restore без ключа -db для базы данных будет использовано название siem. При выполнении команды full_restore без ключа --arc утилита восстановит данные из самой актуальной резервной копии.

4. Запустите службу Ankey SIEM NG ES:
   systemctl start siemserver-storage.service

Данные из резервной копии восстановлены.

11.4 О восстановлении резервной копии данных о площадках и их связях

Восстановление данных необходимо начинать с главной площадки. Данные остальных площадок можно восстанавливать в любом порядке.

Сервер, на котором будут восстановлены данные Ankey SIEM NG MC, должен иметь такое же доменное имя (при его отсутствии − такой же IP-адрес), которое имел сервер Ankey SIEM NG MC на момент создания резервной копии. Также при восстановлении данных компонента Ankey SIEM NG MC главной площадки необходимо до начала восстановления закрыть на его сервере TCP-порт 8703 для входящих соединений, по окончании восстановления открыть этот порт.

12 Индексы Elasticsearch: ротация, архивация, перемещение, удаление и использование политик ILM

Индексы Elasticsearch хранят информацию о событиях информационной безопасности. При продолжительной обработке событий, а также при расширении ИТ-инфраструктуры предприятия (увеличении количества активов и потока событий от них) имеющееся свободное место на жестких дисках сервера Ankey SIEM NG Events Storage будет уменьшаться, что может привести к необходимости подключения новых жестких дисков или отдельной системы хранения данных. С помощью утилит, устанавливаемых при развертывании системы, вы можете:

- просматривать список индексов;
- настраивать ротацию индексов;
- архивировать индексы по расписанию и восстанавливать их из архива;
- удалять архивные индексы по расписанию;
- удалять индексы без архивации.

Также вы можете перемещать индексы в новое хранилище. Утилиты для просмотра, ротации, архивации и удаления индексов находятся на сервере Ankey SIEM NG Events Storage. Указанные в инструкциях команды необходимо выполнять в терминале от имени суперпользователя (root).

Ротация

Максимальный объем дискового пространства, выделяемый для хранения индексов, автоматически вычисляется при установке и обновлении компонента Ankey SIEM NG Events Storage и равен 80% от общего объема дискового пространства. По умолчанию срок хранения индексов − 365 дней. Утилита ротации tailcutter автоматически запускается каждые 30 минут и при превышении этих значений удаляет старые индексы. Вы можете изменить максимальный объем дискового пространства, выделяемый для хранения индексов, и срок их хранения.

Примечание. Утилита ротации доступна с версии системы 2.0. Если ранее для ротации индексов вы создавали задачи для их архивации и последующего удаления по расписанию, необходимо удалить эти задачи и настроить ротацию индексов с помощью утилиты.

Архивация и удаление

Утилита es_backup_tool создает из исходных индексов архивные, сохраняет их в отдельное хранилище, а исходные индексы удаляет из Elasticsearch. Архивные индексы не используются системой, но при необходимости могут быть восстановлены в любой момент. Кроме того, утилита может удалять ставшие ненужными архивные индексы, удалять исходные индексы без архивации.

Вы можете настроить расписание запуска утилиты es_backup_tool с помощью планировщика заданий и указать количество дней с момента создания

индекса до его архивации и удаления. Архивация индексов создает дополнительную нагрузку на Elasticsearch, поэтому ее рекомендуется выполнять в период наименьшей нагрузки на систему. Перед созданием задачи для архивации индексов необходимо создать хранилище архивных индексов.

Перемещение

Перемещение индексов может потребоваться в случае нехватки свободного места на жестких дисках сервера Ankey SIEM NG Events Storage и, как следствие, подключения новых жестких дисков или отдельной системы хранения данных.

Использование политик ILM

В высоконагруженной конфигурации индексы Elasticsearch необходимо хранить на двух типах накопителей данных – жестких дисках и твердотельных накопителях. Объем твердотельных накопителей позволяет хранить индексы хранилища в горячей стадии от нескольких дней до недели. Затем индексы автоматически переходят в теплую стадию и хранятся на жестких дисках. Для разделения индексов на разные типы накопителей в хранилище событий Elasticsearch используются политики ILM.

Настройка политик ILM происходит автоматически после установки системы и запуска компонента Ankey SIEM NG ES. После настройки политик необходимо перезапустить службу **SIEM server storage** с помощью команды systemctl restart siemserver-storage.

Примечание. Время хранения индексов автоматически определяется из расчета 1 час на каждые 250 ГБ. Для горячей стадии учитывается только объем твердотельных накопителей.

Рекомендуется проверить значения параметров политики ILM после переустановки или обновления системы. Для смены или восстановления значений параметров необходимо внести изменения в файл политик /var/lib/storage/siem_*_policy.json по образцу из файла /var/lib/storage/siem_*_policy.json.expample. После сохранения файла необходимо перезапустить службу SIEM server storage.

12.1 Просмотр списка индексов

❖ Чтобы просмотреть список индексов, используемых системой, в интерфейсе терминала Linux выполните команду:

/opt/estools/bin/es_backup_tool -cmd listindex

❖ Чтобы просмотреть список архивных индексов, в интерфейсе терминала Linux выполните команду:

/opt/estools/bin/es_backup_tool -cmd listarchive

12.2 Настройка ротации индексов

Вы можете изменять срок хранения индексов для событий (параметр TailcutterTtl) и для счетчиков событий (параметр TailcutterTtlc), а также максимальный объем дискового пространства, выделяемый для хранения всех индексов (параметр TailcutterDbspace) в конфигурационных параметрах

компонента Ankey SIEM NG ES в соответствии с инструкцией (см. раздел 16.1.2) по изменению конфигурации роли.

12.3 Архивация индексов

Вы можете запускать архивацию индексов вручную или настроить архивацию по расписанию. Перед архивацией индексов необходимо создать для них хранилище (см. пункт 12.3.1).

12.3.1 Создание хранилища для архивных индексов

❖ Чтобы создать хранилище для архивных индексов, в интерфейсе терминала Linux выполните команду:

/opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу для хранения архивных индексов, например, /data_archive >"

По завершении создания хранилища появится сообщение:

Repository siem_backup created successfully.

12.3.2 Архивация индексов на Linux

❖ Чтобы архивировать индексы, созданные за определенный период, выполните команду:

/opt/estools/bin/es_backup_tool -cmd backup -from <Дата начала периода> -to <Дата окончания периода> -di false

Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

❖ Чтобы архивировать индексы, с момента создания которых прошло не меньше определенного количества дней, выполните команду:

/opt/estools/bin/es_backup_tool -cmd backup -t <Количество дней> -di false

Примечание. При выполнении команд архивации без ключа -di false сохраненные индексы будут удалены.

12.3.3 Настройка архивации индексов по расписанию

❖ Чтобы настроить архивацию индексов по расписанию, в планировщике заданий cron на Linux создайте задачу:

<Расписание> /opt/estools/bin/es_backup_tool -cmd backup -t <Дней до архивации> >> /opt/ estools/log/es_backup.log

где:

– <Дней до архивации> – количество дней с момента создания индекса до его архивации;
– <Расписание> – периодичность запуска утилиты для архивации индексов с помощью планировщика заданий.

Примечание. Описание планировщика заданий cron на Debian (параметров команды crontab) приведено на сайте debian.org.

Например, для запуска еженедельной (в каждое воскресенье в 1 час 30 минут) архивации индексов, с момента создания которых прошло 30 дней, необходимо в планировщике заданий cron на Linux создать задачу:

30 1 * * 7 /opt/estools/bin/es_backup_tool -cmd backup -t 30 >> /opt/estools/log/es_backup.log

12.4 Восстановление индекса из архива

Восстановление индекса из архива возможно только на том сервере, где была создана резервная копия этого индекса.

❖ Чтобы восстановить индекс из архива, в интерфейсе терминала Debian выполните команду:

– /opt/estools/bin/es_backup_tool.sh -cmd restore -arc snapshot_<Дата архивации индекса>

Примечание. Дату архивации индекса необходимо указывать в формате <Год-Месяц-День.> (например, snapshot_2022-12-23).

Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) – один отдельный символ.

12.5 Удаление архивных индексов

Вы можете удалять архивные индексы вручную или настроить их удаление по расписанию.

12.5.1 Удаление архивных индексов на Linux

❖ Чтобы удалить архивные индексы, созданные за определенный период, выполните команду:

/opt/estools/bin/es_backup_tool -cmd cleanarchive -from <Дата начала периода> -to <Дата окончания периода>

Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

❖ Чтобы удалить архивные индексы, с момента создания которых прошло не меньше определенного количества дней, выполните команду:

/opt/estools/bin/es_backup_tool -cmd cleanarchive -t <Количество дней>

12.5.2 Удаление архивных индексов по расписанию

❖ Чтобы настроить удаление архивных индексов по расписанию, в планировщике заданий cron на Linux создайте задачу:

– <Расписание> /opt/estools/bin/es_backup_tool -cmd cleanarchive -t <Дней до удаления> >> /opt/estools/log/es_backup.log

где:

– <Дней до удаления> – количество дней с момента создания индекса до его удаления;

– <Расписание> – периодичность запуска утилиты с помощью планировщика заданий.

Примечание. Описание планировщика заданий cron на Debian (параметров команды crontab) представлено на сайте debian.org.

Например, для запуска еженедельного (в каждое воскресенье в 2 часа 30 минут) удаления индексов, с момента создания которых прошло 100 дней, необходимо в планировщике заданий cron на Linux создать задачу:

30 2 * * 7 /opt/estools/bin/es_backup_tool -cmd cleanarchive -t 100 >> /opt/estools/log/es_backup.log

12.6 Удаление индекса без архивации

❖ Чтобы удалить индекс, в интерфейсе терминала Linux выполните команду:

– если Ankey SIEM NG развернут в конфигурации для средненагруженных или высоконагруженных систем с потоком событий до 20000 событий в секунду:
/opt/estools/bin/es_backup_tool -cmd deleteindex --index <Тип индекса>_<Дата создания>

– если для высоконагруженных систем с потоком событий выше 20000 событий в секунду:
/opt/estools/bin/es_backup_tool -cmd deleteindex --index <Тип индекса>_<Дата создания>*

Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) – один отдельный символ.

12.7 Перемещение индексов на Linux

❖ Чтобы переместить индексы:

1. Остановите все задачи сканирования сети и сбора данных.
2. На сервере Ankey SIEM NG Server остановите службу SIEM Server storage:
systemctl stop siemserver-storage
3. На сервере Ankey SIEM NG ES остановите все службы Elasticsearch:
systemctl stop elasticsearch_*
4. Переместите все файлы из каталога с индексами Elasticsearch в каталог нового хранилища, например: mv <Путь к каталогу с индексами Elasticsearch>/* <Путь к каталогу нового хранилища>
Например:
mv /data/* /storage/
5. На сервере с установленной ролью Deployer запустите сценарий:
siemstorage_<Номер версии>/install.sh
6. В открывшемся окне нажмите кнопку **Yes**.

7. В открывшемся окне выберите вариант с идентификатором приложения Ankey SIEM NG.В открывшемся окне выберите вариант с названием экземпляра роли SIEM Storage.
   Откроется окно для проверки и изменения параметров.
8. Выберите вариант **Basic configuration**.
   Откроется страница со списком параметров.
9. Измените значение параметра PathData:
   PathData: <Путь к каталогу нового хранилища>
10. Нажмите кнопку **OK**.
    По завершении изменения конфигурации появится сообщение Deployment configuration successfully applied.
11. Нажмите кнопку **OK**.
12. На сервере Ankey SIEM NG Server запустите службу SIEM Server storage:
    systemctl start siemserver-storage
13. На сервере Ankey SIEM NG ES запустите все службы Elasticsearch:
    systemctl --all start elasticsearch_*
14. Запустите остановленные задачи.

Индексы перемещены.

13 Разделы LogSpace: ротация, резервное копирование и восстановление

Данные в хранилище LogSpace разбиты на разделы. Каждый раздел хранит информацию о событиях информационной безопасности за одни сутки. Для работы с разделами хранилища вы можете использовать набор утилит dbtools, который устанавливается вместе с ролью Event Storage и включает в себя утилиты backup_tool и tailcutter.

Примечание. Хранилище LogSpace не поддерживает распределенный поиск событий.

Ротация

Максимальный объем дискового пространства, выделяемый для хранения разделов, автоматически вычисляется при установке и обновлении роли Event Storage и равен 92% от общего объема дискового пространства. По умолчанию срок хранения разделов – 365 дней. Утилита ротации tailcutter удаляет из хранилища разделы, срок хранения или размер которых превышает значения, указанные в конфигурационных параметрах (см. приложение А) TailcutterTtl, TailcutterTtlc и TailcutterDbspace роли Event Storage. По умолчанию утилита запускается с помощью планировщика **cron** один раз в 30 минут. Задача на запуск создается в **cron** автоматически при установке утилиты. После запуска утилита сначала удаляет разделы таблицы events, срок хранения которых превышает значение параметра TailcutterTtl, затем удаляет разделы таблицы counters, срок хранения которых превышает значение параметра TailcutterTtlc. Далее утилита проверяет наличие свободного дискового пространства и, в случае превышения разделами объема, указанного в параметре **TailcutterDbspace**, удаляет самые старые разделы из таблиц events и counters. Утилита удаляет старые разделы до тех пор, пока занимаемый ими объем не станет меньше значения параметра TailcutterDbspace.

После установки утилита tailcutter хранится в каталоге /opt/dbtools/bin/tailcutter. Вы можете настроить ее параметры, изменяя конфигурацию роли Event Storage согласно инструкции (см. раздел 16.1) или используя соответствующие ключи при запуске утилиты из командной строки.

Таблица 13.1 –Ключи для запуска утилиты tailcutter

Ключ	Описание	Значение по умолчанию
--help	Вывод справочной информации о ключах, с которыми можно запускать утилиту tailcutter	–
--database <Название базы данных>	Название базы данных	siem
--dbspace <Объем дискового пространства в процентах или гигабайтах>	Максимальный объем дискового пространства, выделяемый для разделов хранилища. Обязательный ключ	92%

Ключ	Описание	Значение по умолчанию
--ttl <Количество дней>	Срок хранения разделов таблицы events. Обязательный ключ	365
--ttlc <Количество дней>	Срок хранения разделов таблицы counters. Если значение ключа не указано, оно принимается равным значению ключа --ttl	5
--log <Путь к файлу журнала>	Путь к файлу журнала утилиты tailcutter	/opt/dbtools/log/tailcutter.log
--loglevel <Уровень журналирования>	Уровень журналирования событий утилиты tailcutter. Возможные значения – DEBUG, INFO, WARNING, ERROR или CRITICAL	INFO

Резервное копирование и восстановление

Утилита backup_tool предназначена для резервного копирования (см. раздел 10.3) и восстановления (см. раздел 11.3) данных хранилища LogSpace. Кроме того, утилита может удалять разделы и показывать списки существующих разделов и архивов хранилища.

После установки утилита хранится в каталоге /opt/dbtools/bin. Вы можете настроить ее параметры, используя соответствующие ключи при запуске утилиты из командной строки.

Таблица 13.2 Ключи для запуска утилиты backup_tool

Ключ	Описание	Значение по умолчанию
--help	Вывод справочной информации о ключах, с которыми можно запускать утилиту backup_tool	–
--database <Название базы данных>	Название базы данных	siem
--database_type <Тип базы данных>	Тип хранилища	logspace
-repopath <Путь к каталогу>	Путь к каталогу для сохранения резервной копии данных хранилища	/db_backup
--log <Имя файла>	Путь к файлу журнала утилиты backup_tool	tailcutter.log
--loglevel <Уровень журналирования>	Уровень журналирования событий утилиты backup_tool. Возможные значения – DEBUG, INFO, WARNING, ERROR или CRITICAL	INFO
--time	Допустимый срок хранения разделов, в днях. Разделы, срок хранения которых превышает указанное в ключе значение, будут удалены	–

Ключ	Описание	Значение по умолчанию
--part <Название раздела>	Название раздела, который необходимо удалить с помощью команды deletepart	–
--from	Начало периода, за который необходимо удалить архивы, в формате ГГГГММДД	–
--to	Окончание периода, за который необходимо удалить архивы, в формате ГГГГММДД	–
--cmd deletepart	Команда для удаления раздела. Название раздела необходимо указать после команды с помощью ключа --part	–
--cmd listpart	Вывод списка разделов хранилища	–
--cmd listarchive	Вывод списка архивов хранилища	–
--cmd cleanarchive	Удаление архивов хранилища. После команды необходимо указать в днях срок хранения, при превышении которого необходимо удалять архивы (с помощью ключа --time), или период, за который необходимо удалить архивы (с помощью ключей --from и --to)	–

13.1.2 Просмотр списков разделов и архивов LogSpace

❖ Чтобы просмотреть список разделов хранилища LogSpace, в интерфейсе терминала Linux выполните команду:
/opt/dbtools/bin/backup_tool --cmd listpart

❖ Чтобы просмотреть список архивов хранилища LogSpace, в интерфейсе терминала Linux выполните команду:
/opt/dbtools/bin/backup_tool --cmd listarchive

13.1.3 Удаление разделов и архивов LogSpace

❖ Чтобы удалить раздел хранилища LogSpace, в интерфейсе терминала Linux выполните команду:
/opt/dbtools/bin/backup_tool --cmd deletepart --part <Название раздела>

❖ Чтобы удалить архивы, которые хранятся дольше определенного количества дней, в интерфейсе терминала Linux выполните команду:
/opt/dbtools/bin/backup_tool --cmd cleanarchive --time <Количество дней>

❖ Чтобы удалить архивы хранилища LogSpace за определенный период времени,
в интерфейсе терминала Linux выполните команду:
/opt/dbtools/bin/backup_tool --cmd cleanarchive --from <Нижняя граница периода в формате ГГГГММДД> --to <Верхняя граница периода в формате ГГГГММДД>

14 Смена паролей служебных учетных записей

Для выполнения своих функций компоненты Ankey SIEM NG могут использовать служебные учетные записи. Такие учетные записи не предназначены для выполнения пользователем действий в системе и необходимы для доступа компонентов к ее ресурсам. При развертывании Ankey SIEM NG логины и пароли служебных учетных записей устанавливаются в значения по умолчанию.

Вы можете сменить пароли служебных учетных записей. Команды для смены паролей необходимо вводить в интерфейсе в интерфейсе терминала Linux от имени суперпользователя (root).

14.1 Смена пароля служебной учетной записи в PostgreSQL

При развертывании Ankey SIEM NG в PostgreSQL создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи – pt_system, пароль – P@sswordP@ssword.

❖ Чтобы сменить пароль служебной учетной записи в PostgreSQL на Linux:

1. На сервере с установленной ролью SqlStorage/JatobaStorage выполните команду:
   docker exec -it $(docker ps | awk '/storage-postgres/ {print $NF}') psql -U pt_system -d postgres -c "ALTER USER pt_system WITH PASSWORD '<Новый пароль>'"
2. Измените конфигурацию роли SqlStorage:
   PgPassword: <Новый пароль>
3. Измените конфигурации ролей Management and Configuration, Knowledge Base и Core:
   PostgrePassword: <Новый пароль>

Пароль изменен.

14.2 Смена пароля служебной учетной записи в СУБД Jatoba

При развертывании Ankey SIEM NG в СУБД Jatoba создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи – pt_system, пароль – P@sswordP@ssword.

❖ Чтобы сменить пароль служебной учетной записи в СУБД Jatoba на Linux:

1. На сервере с установленной ролью JatobaStorage выполните команду:
   docker exec -it $(docker ps | awk '/storage-jatoba/ {print $NF}') psql -U pt_system -d postgres -c "ALTER USER pt_system WITH PASSWORD '<Новый пароль>'"
2. Измените конфигурацию роли JatobaStorage:
   PgPassword: <Новый пароль>

3. Измените конфигурации ролей Management and Configuration, Knowledge Base и Core:
   PostgrePassword: <Новый пароль>

Пароль изменен.

14.3 Смена паролей служебных учетных записей в RabbitMQ

Внимание! Приведенные ниже инструкции не предназначены для смены паролей служебных учетных записей компонентов Ankey SIEM NG Server и Ankey SIEM NG Collector, установленных на одном сервере ("SIEM на коллекторе").

Для обмена данными между службами компонентов Ankey SIEM NG используется брокер сообщений RabbitMQ.

В конфигурации для низконагруженных систем используется только один брокер RabbitMQ. В конфигурациях для средненагруженных и высоконагруженных систем используется два брокера RabbitMQ. Один из них устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен данными между службами всех компонентов Ankey SIEM NG, другой – на сервер Ankey SIEM NG Server и обеспечивает обмен данными только между его службами.

14.3.1 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Core на Linux

По умолчанию логин служебной учетной записи компонента Ankey SIEM NG Core на Linux – core, пароль – P@ssword.

❖ Чтобы сменить пароль служебной учетной записи Ankey SIEM NG Core:

1. На сервере Ankey SIEM NG Core измените конфигурации (см. пункт 14.1.2) ролей Core и RMQ Message Bus:
   RMQPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   Cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down docker-compose up -d
4. Пароль изменен.

14.3.2 RabbitMQ: смена паролей служебных учетных записей компонента Ankey SIEM NG Server на Linux

Компонент Ankey SIEM NG Server на Linux для работы в RabbitMQ использует две служебных учетных записи. Одна запись предназначена для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Core, другая – для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Server. По умолчанию обе учетных записи имеют одинаковый логин siem и пароль P@ssword.

Порядок действий по смене паролей зависит от конфигурации Ankey SIEM NG и операционных систем серверов Ankey SIEM NG Server и Ankey SIEM NG Core.

14.3.2.1 *Смена паролей служебных учетных записей Ankey SIEM NG Server на Linux: компоненты Ankey SIEM NG Server и Ankey SIEM NG Core установлены на один сервер*

Если компоненты Ankey SIEM NG Server и Ankey SIEM NG Core установлены на Linux на один сервер, обе учетных записи используются для доступа к одному и тому же брокеру RabbitMQ и по умолчанию имеют одинаковый логин.

❖ Чтобы сменить пароли служебных учетных записей Ankey SIEM NG Server:

1. На сервере Ankey SIEM NG Core измените конфигурации ролей Core и RMQ Message Bus:
   RMQSiemPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   Cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down
   docker-compose up -d
3. Измените конфигурацию роли SIEM Server:
   GlobalRabbitPassword: <Новый пароль>
   RMQPassword: <Новый пароль>

Пароли изменены.

14.3.2.2 *Смена паролей служебных учетных записей Ankey SIEM NG Server на Linux: компоненты Ankey SIEM NG Server и Ankey SIEM NG Core установлены на разные серверы*

Если компоненты Ankey SIEM NG Server и Ankey SIEM NG Core установлены на разные серверы, одна учетная запись используется для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Core, другая – для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Server.

❖ Чтобы сменить пароль служебной учетной записи для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Core под управлением Linux:

1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере Ankey SIEM NG Core:
   RMQSiemPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down
   docker-compose up -d
3. Измените конфигурацию роли SIEM Server:
   RMQPassword: <Новый пароль>

Пароль изменен.

❖ Чтобы сменить пароль служебной учетной записи для подключения к RabbitMQ, установленному на сервер Ankey SIEM NG Server:

1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере Ankey SIEM NG Server:
   RMQSiemPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down
   docker-compose up -d
3. Измените конфигурацию роли SIEM Server:
   GlobalRabbitPassword: <Новый пароль>
4. Если компонент Ankey SIEM NG Core установлен на Linux, измените конфигурацию роли Core:
   RMQSiemPassword: <Новый пароль>

Пароль изменен.

14.3.3 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Collector на Microsoft Windows

По умолчанию логин служебной учетной записи компонента Ankey SIEM NG Collector на Microsoft Windows для доступа к RabbitMQ – mpx_agent, пароль – P@ssword.

❖ Чтобы сменить пароль служебной учетной записи для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Core под управлением Linux:

1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере Ankey SIEM NG Server:
   RMQAgentPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down
   docker-compose up -d
3. На сервере каждого компонента Ankey SIEM NG Collector выполните команду:
   coreagentcfg set -p RMQUser agent RMQPassword <Новый пароль>

Пароль изменен.

14.3.4 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Collector на Linux

По умолчанию логин служебной учетной записи компонента Ankey SIEM NG Collector на Linux для доступа к RabbitMQ – agent, пароль – P@ssword.

❖ Чтобы сменить пароль служебной учетной записи для доступа к RabbitMQ, установленному на сервер Ankey SIEM NG Core под управлением Linux:

1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере Ankey SIEM NG Server:
   RMQAgentPassword: <Новый пароль>
2. Перезапустите Docker-контейнер роли RMQ Message Bus:
   cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземляра роли RMQ Message Bus>/images/messagebus-rabbitmq
   docker-compose down
   docker-compose up -d
3. На сервере каждого компонента Ankey SIEM NG Collector измените конфигурацию роли Collector:
   AgentRMQPassword: <Новый пароль>

Пароль изменен.

15 Настройка журналирования работы ПК Ankey SIEM NG

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

15.1 Настройка журналирования работы компонента Ankey SIEM NG Core на Linux

Настройка выполняется отдельно для каждой службы компонента.

❖ Чтобы настроить журналирование:

1. На сервере Ankey SIEM NG Core в файл **/var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли Core>/images/<Название службы>/config/custom.env** добавьте параметр:
   Logging_Threshold=<Уровень журналирования>

   Примечание. Возможные значения FATAL, ERROR, WARN, INFO, DEBUG и TRACE.

2. Выполните команды:
   cd /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли Core>/images/<Название службы>/
   docker-compose down
   docker-compose up -d

Журналирование настроено.

15.2 Настройка журналирования работы компонента Ankey SIEM NG Server

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию служба SIEM Server health monitor записывает в журнал сообщения уровня debug, все остальные службы − уровня info. Размер каждого файла журнала ограничен 100 МБ, каждая служба хранит последние 10 таких файлов.

Файл siem.conf, используемый для настройки журналирования, находится на сервере Ankey SIEM NG Server в каталоге /opt/siem/etc.

❖ Чтобы настроить журналирование:

1. В файле siem.conf в секции <Название службы> → logger измените значения параметров:
   "level": <Уровень журналирования>

   Примечание. Возможные значения fatal, error, warning, info, debug и trace.

"nfiles": <Максимальное количество сохраняемых файлов журналов>
"size_limit": <Максимальный размер файла журнала (в байтах)>

Примечание. Если требуется сохранять записи обо всех событиях, произошедших за сутки, в один файл журнала, необходимо указать значение параметра size_limit равным нулю.

2. В интерфейсе терминала от имени суперпользователя (root) выполните команду для перезапуска службы, параметры журналирования которой были изменены
   systemctl siemserver-<Название службы>.service restart

Журналирование настроено.

15.3 Настройка журналирования работы компонента Ankey SIEM NG Events Storage с Elasticsearch версии 7

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию в журнал записываются события уровня debug, размер каждого файла журнала ограничен 128 МБ на Linux, общий объем файлов журналов для каждого узла Elasticsearch ограничен 2 ГБ.

Для настройки журналирования вам потребуется файл log4j2.properties, который находится на сервере Ankey SIEM NG Events Storage в каталоге /etc/elasticsearch/<Имя узла Elasticsearch>.

❖ Чтобы настроить журналирование работы компонента Ankey SIEM NG Events Storage:

1. В файле log4j2.properties измените значения параметров:
   logger.action.level = <Уровень журналирования>

Примечание. Возможные значения off, error, warn, info, debug, trace и all.

appender.rolling.policies.size.size = <Максимальный размер файла журнала (в мегабайтах)>MB
appender.rolling.strategy.action.condition.nested_condition.exceeds = <Максимальный общий объем файлов журналов для каждого узла Elasticsearch (в гигабайтах)>GB

2. В интерфейсе терминала от имени суперпользователя (root) выполните команду для перезапуска службы Elasticsearch:
   systemctl --all restart elastic*service

Журналирование настроено.

15.4 Настройка журналирования работы компонента Ankey SIEM NG Collector на Microsoft Windows

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию в журнал записываются события уровня DEBUG. Размер каждого файла журнала ограничен 100 МБ, сохраняются последние 50 файлов. Для настройки журналирования вам потребуется файл C:\Program Files (x86)\Gazinformservice\Ankey SIEM NG Collector\agent.log.xml, который находится на сервере Ankey SIEM NG Collector.

Примечание. Не рекомендуется изменять уровень журналирования без указания службы технической поддержки ПК Ankey SIEM NG.

❖ Чтобы настроить журналирование:

1. В файле agent.log.xml измените значение атрибута level параметра config → root:
   <Название журналируемого компонента коллектора> level="<Уровень журналирования>"

   Примечание. Возможные значения NOTSET, FATAL, ERROR, WARN, INFO, DEBUG и TRACE.

2. Измените значения атрибутов max_file_size и max_backup_index параметра config → params:
   params max_file_size="<Максимальный размер файла журнала (в мегабайтах)>" max_backup_index="<Максимальное количество сохраняемых файлов журналов>"
3. Перезапустите службу Core Agent.

Журналирование настроено.

Эта инструкция не предназначена для настройки журналирования работы модулей Ankey SIEM NG Collector и их компонентов. Оно настраивается с помощью справочников ПК Ankey SIEM NG (подробное описание см. в Руководстве по интеграции с источниками Ankey SIEM NG 5.2.3).

16 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 А и Б.

16.1 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux

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

В результате просмотра или изменения конфигурации роли в каталоге, из которого был запущен сценарий install.sh, формируется каталог /installReports с отчетами. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы изменений.

16.1.1 Просмотр конфигурации роли

❖ Чтобы просмотреть конфигурацию роли:

1. На сервере с установленной ролью Deployer запустите сценарий: <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 А).
6. По завершении просмотра нажмите кнопку **Cancel**.
7. В окне для выбора набора параметров нажмите кнопку **Cancel**.

16.1.2 Изменение конфигурации роли

❖ Чтобы изменить конфигурацию роли:

1. На сервере с установленной ролью Deployer запустите сценарий: <Название роли>_<Номер версии>/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 А).
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**.
9. В открывшемся окне нажмите кнопку **Submit**.
   Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
    Конфигурация роли изменена.

16.1.3 Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch

❖ Чтобы изменить объем оперативной памяти:

1. На сервере с установленной ролью Deployer запустите сценарий: <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 А).
6. Измените значений параметра ClusterConfigurationProfile на Manual.
7. В качестве значения параметров MasterNodeHeapSize, ClientNodeHeapSize и DataNodeHeapSize введите объем оперативной памяти, выделяемый для главного узла, клиентского узла и узла данных соответственно.

> **Примечание.** Минимальное значение параметров MasterNodeHeapSize и ClientNodeHeapSize – 2 ГБ, параметра DataNodeHeapSize – 8 ГБ. Суммарный объем оперативной памяти всех узлов кластера, умноженный на коэффициент 1,5 не должен превышать объем оперативной памяти сервера Ankey SIEM NG ES.

8. Нажмите кнопку **OK**.
9. В открывшемся окне нажмите кнопку **Submit**.
   Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
10. Нажмите кнопку **OK**.
    Объем оперативной памяти изменен.

16.1.4 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: <Название роли SIEM Server>/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 А).
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 **OK**.
8. В открывшемся окне нажмите кнопку **Submit**.
   Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
9. Нажмите кнопку **OK**.
   Алгоритм сжатия данных выбран и будет применен к новым индексам.

16.1.5 Регистрация событий при нарушении и восстановлении параметров источников

❖ Чтобы включить регистрацию событий при нарушении и восстановлении параметров источников:

1. На сервере с установленной ролью Deployer запустите сценарий: <Название роли Core>/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 А).
6. Установите флажок **SendAlertsToSiem**.
7. Нажмите кнопку **OK**.
8. В открывшемся окне нажмите кнопку **Submit**.
   Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
9. Нажмите кнопку **OK**.

Регистрация событий при нарушении и восстановлении параметров источников включена.

16.1.6 Настройка SMTP-сервера для отправки уведомлений по электронной почте

Уведомления Ankey SIEM NG содержат информацию об изменениях в ИТ-инфраструктуре предприятия, о работе задач сбора данных, собираемых событиях и параметрах потока событий, а также о выявляемых инцидентах ИБ и состоянии системы. Вы можете настроить отправку уведомлений по электронной почте, указав при создании задачи адреса получателей уведомления. Подробнее о создании задач для отправки уведомлений см. документ «Руководство оператора Ankey SIEM NG». Перед созданием задачи необходимо настроить SMTP-сервер.

❖ Чтобы настроить SMTP-сервер для отправки уведомлений по электронной почте:

1. На сервере с установленной ролью Deployer распакуйте архив core_<Номер версии>.tar.gz:
   tar -xf core_<Номер версии>.tar.gz
2. Запустите сценарий:
   Core_<Номер версии>/install.sh
3. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли.
   Откроется окно для выбора набора параметров.
6. Выберите вариант **Advanced configuration**.

> **Примечание.** Если требуется включение генерации внутренних событий Ankey SIEM NG в активном канале веб-интерфейса, то выберите вариант **Advanced configuration** и затем включите параметр **SendAlertsToSiem**.

   Откроется страница со списком параметров.
7. Укажите значения параметров:
   - 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>>;

- SmtpSslEnabled: <Для подключения к SMTP-серверу службы Ankey SIEM NG CORE используют защищенное (True) или незащищенное (False) соединение, по умолчанию False>;
- SmtpUser: <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 устанвоки роли Core >;
- SmtpUseDefaultCredentials: <Режим аутентификации SMTP-сервера:
  True - для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtpUser и SmtpPassword);
  False - для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword, по умолчанию True>.

Примечание. Для публичных почтовых сервисов значения параметров SmtpSender и SmtpUser должны совпадать.

8. Чтобы отключить проверку валидности сертификата при подключении к SMTP-серверу, в качестве значения параметра SmtpIgnoreCertificateValidation выберите True.
9. В качестве значения параметра SmtpSecureSocketOptions выберите вариант шифрования при подключении к SMTP-серверу.
10. Нажмите кнопку **OK**.
11. В открывшемся окне нажмите кнопку **Submit**.
    Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
12. Нажмите кнопку **OK**.
13. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

SMTP-сервер настроен

16.2 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 16.1 – Список компонентов и поставляемых с ними утилит

Компонент	Утилита
Ankey SIEM NG Server	siemcfg.exe
Ankey SIEM NG Collector	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 16.2 – 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

16.2.2 Просмотр конфигурации

❖ Чтобы просмотреть конфигурацию, выполните команду:

<Название утилиты> get -p <Название параметра 1> <Название параметра 2> … <Название параметра N>

16.2.3 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>

16.2.4 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.

17 Отключение отправки ненормализованных событий облегченной версией компонента Ankey SIEM NG Server («SIEM на коллекторе»)

По умолчанию компонент Ankey SIEM NG Server, установленный на сервере Ankey SIEM NG Collector, отправляет в основной Ankey SIEM NG Server как нормализованные, так и ненормализованные события. Если требуется, вы можете отключить отправку ненормализованных событий.

❖ Чтобы отключить отправку ненормализованных событий:

1. В конфигурационном файле измените значение параметра normalizer → store_unnormalized_raw:
   - если облегченная версия компонента установлена на сервере Microsoft Wndows, в конфигурационном файле C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\config\siem.conf облегченной версии Ankey SIEM NG Server измените значение параметра normalizer → store_unnormalized_raw:
     "store_unnormalized_raw": false
   - если облегченная версия компонента Ankey SIEM NG Server установлена на сервере Linux, в конфигурационном файле /opt/siem/etc/siem.conf измените значение параметра normalizer → store_unnormalized_raw:
     "store_unnormalized_raw": false
2. Перезапустите службу SIEM Server normalizer облегченной версии Ankey SIEM NG Server:
   - если компонент установлен на Microsoft Windows, используйте для перезапуска стандартные средства операционной системы;
   - если компонент установлен на Linux, используйте для перезапуска команду systemctl restart siemserver-normalizer.service .

Отправка ненормализованных событий отключена.

18 Настройка обогащения событий данными геолокации

Ankey SIEM NG поддерживает обогащение событий данными из базы MaxMind GeoIP для определения местоположения узлов по их IP-адресу.

❖ Чтобы настроить обогащение событий данными геолокации:

1. Скопируйте файлы базы данных MaxMind GeoIP на сервер Ankey SIEM NG Server.
2. На сервере с установленной ролью Deployer распакуйте архив siemserver-linux_<Номер версии>.tar.gz из комплекта поставки.
3. Запустите сценарий:
   siemserver-linux_<Номер версии>/install.sh
4. В открывшемся окне нажмите кнопку **Yes**.
5. В открывшемся окне нажмите кнопку **Yes**.
6. В открывшемся окне выберите вариант с названием экземпляра роли.
   Откроется окно для выбора набора параметров.
7. Выберите вариант **Advanced configuration**.
   Откроется страница со списком параметров (см. приложение А).
8. В параметре GeoIPDBPathASN укажите путь к файлу GeoLite2-ASN.mmdb на сервере Ankey SIEM NG Server.
9. В параметре GeoIPDBPathCity укажите путь к файлу GeoLite2-City.mmdb на сервере Ankey SIEM NG Server.
10. Установите флажок GeoIPEnable.
11. Если требуется, измените параметры обогащения событий данными геолокации.
12. Нажмите кнопку **OK**.
    Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
13. Нажмите кнопку **OK**.
14. Если требуется, исключите подсети из обогащения данными геолокации, добавив их IP-адреса в конфигурационный файл siem.conf в раздел exclude_ip.

> Внимание! Перечень исключенных подсетей сбрасывается до значений, установленных по умолчанию, после каждого запуска сценария install.sh.

15. Если в конфигурационный файл siem.conf были внесены изменения, выполните команду:
    systemctl restart siemserver-enricher.service

Обогащение событий данными геолокации настроено.

Таблица 18.1 – Параметры обогащения событий данными геолокации

Ключ	Описание	Значение по умолчанию
GeoIPFieldDstASN	Заполнять ли поля с номером автономной системы (ASN) узла назначения	GeoIPFieldDstASN
GeoIPFieldDstCity	Формат данных о городе узла назначения. Может принимать значения en, ru, skip	GeoIPFieldDstCity
GeoIPFieldDstCountry	Формат данных о стране узла назначения. Может принимать значения en, ru, iso, skip	GeoIPFieldDstCountry
GeoIPFieldDstOrg	Формат данных об организации узла назначения. Может принимать значения en, skip	GeoIPFieldDstOrg
GeoIPFieldSrcASN	Заполнять ли поля с номером автономной системы (ASN) узла-источника	GeoIPFieldSrcASN
GeoIPFieldSrcCity	Формат данных о городе узла-источника. Может принимать значения en, ru, skip	GeoIPFieldSrcCity
GeoIPFieldSrcCountry	Формат данных о стране узла-источника. Может принимать значения en, ru, iso, skip	GeoIPFieldSrcCountry
GeoIPFieldSrcOrg	Формат данных об организации узла-источника. Может принимать значения en, skip	GeoIPFieldSrcOrg
GeoIPRewriteData	Заменять ли содержимое предзаполненных полей события с данными геолокации на данные MaxMind GeoIP	GeoIPRewriteData

19 Пользовательские поля в модели актива

После развертывания системы в модели актива присутствуют только стандартные поля (например, «Полное имя узла», «Тип устройства», «Операционная система»). Вы можете добавлять в модель актива пользовательские поля (например, «Инвентаризационный номер актива в реестре», «Ответственный за актив») и их описание, изменять имена добавленных ранее полей или удалять их из модели актива.

После добавления полей и ввода их значений пользователи системы смогут:

- просматривать значения добавленных полей в карточке и мини-карточке актива;
- вводить поисковые запросы с учетом добавленных полей;
- осуществлять выборку, группировку и отбор по значениям добавленных полей (PDQL-запрос).

Перед работой с пользовательскими полями необходимо создать файл UserModel.xml в кодировке UTF-8:

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="">
    <Dsl Version="">
      <Entities/>
      <Migrations>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="">
    <Entities>
    </Entities>
  </layer>
</model>
```

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла UserModel.xml не игнорируется регистр символов.

Файл UserModel.xml необходимо разместить на сервере Ankey SIEM NG Core в каталоге /var/lib/deployed-roles/ <Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли Core>/ config/user_model/.

19.1 Добавление пользовательских полей в модель актива

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла UserModel.xml не игнорируется регистр символов.

Если вы добавляете пользовательские поля впервые, вам потребуется файл ModelMigrations.xml, который находится в каталоге /usr/local/share/

microservice/layers/ModelMigrations.xml в Docker-контейнере службы Core Assets Processing.

Примечание. Вы можете войти в Docker-контейнер службы Core Assets Processing с помощью команды docker exec -t -i $(docker ps | awk '/assets-processing/ {print $NF}') /bin/bash.

- Чтобы добавить пользовательские поля в модель актива:
  1. В файле UserModel.xml в качестве значения атрибута Version элементов layer id="UserModel", layer id="UserDescriptions" и значения атрибута Version элемента Dsl укажите версию пользовательской модели.
     - если вы добавляете пользовательские поля впервые, в файле ModelMigrations.xml скопируйте значение атрибута Version элемента Dsl, добавьте единицу к последней цифре скопированного значения и укажите полученное значение в файле UserModel.xml в качестве версии пользовательской модели (например, version="19.0.20206.1");
     - если вы добавляете пользовательские поля повторно, добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, version="19.0.20206.2").

     Например:

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="19.0.20206.1">
    <Dsl Version="19.0.20206.1">
      <Entities/>
      <Migrations>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.1">
    <Entities>
    </Entities>
  </layer>
</model>
```

  2. Для элемента layer id="UserModel" → Dsl → Migrations добавьте дочерний элемент Group с атрибутом Version. В качестве значения атрибута Version укажите версию пользовательской модели, например:

```
<Group Version="19.0.20206.1">
</Group>
```

  3. Для элемента Group добавьте дочерний элемент ChangeEntity с атрибутом Type. В качестве значения атрибута Type укажите Core.Host:

```
<ChangeEntity Type="Core.Host">
</ChangeEntity>
```

4. Для элемента ChangeEntity добавьте дочерние элементы AddProperty (по количеству добавляемых пользовательских полей) с атрибутами Property и PropertyType. В качестве значения атрибута Property укажите имя поля, значения атрибута PropertyType – тип поля.

> **Примечание.** Имена полей должны начинаться с префикса UF_. Допускаются также следующие типы полей: Int, Bool, String, DateTime, Double, Network.IP.

Например:

```
<Group Version="19.0.20206.1">
  <ChangeEntity Type="Core.Host">
    <AddProperty Property="UF_AssetNumber" PropertyType="Int"/>
    <AddProperty Property="UF_AssetOwner" PropertyType="String"/>
    <AddProperty Property="UF_AssetRevisionDate"
PropertyType="DateTime"/>
  </ChangeEntity>
</Group>
```

5. Если необходимо, добавьте описание пользовательских полей (см. подраздел 19.2).
6. Перезапустите службы.

   docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|assetsidentity|assets-projections|assets-scans|core.scanning|core-tables|core-topology|coretopology-analyzer/ {print $NF}')

Пользовательские поля добавлены в модель актива.

19.2 Добавление описания пользовательских полей

> Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла UserModel.xml не игнорируется регистр символов.

❖ Чтобы добавить описание пользовательских полей:

1. В файле UserModel.xml для элемента layer id="UserDescriptions" → Entities добавьте дочерний элемент Entity с атрибутом Name. В качестве значения атрибута Name укажите алиас типа актива. Например, для активов на ОС Microsoft Windows укажите:

   ```
   <Entity Name="OperatingSystem.Windows.WindowsHost">
   </Entity>
   ```

> **Примечание.** Названия алиасов по типу актива содержатся в Docker-контейнере службы Core Assets Processing в файле /usr/local/share/microservice/layers/AssetAliases.xml. Для входа в Docker-контейнер вы можете использовать команду docker exec -t -i $(docker ps | awk '/assetsprocessing/ {print $NF}') /bin/bash.

2. Для элемента Entity добавьте дочерний элемент Properties:
```
<Properties>
</Properties>
```
3. Для элемента Properties добавьте дочерние элементы Property (по числу пользовательских полей с описанием) с атрибутом Name. В качестве значения атрибута Name укажите имя поля, например:
```
<Property Name="UF_AssetNumber">
</Property>
```
4. Для каждого элемента Property добавьте дочерний элемент Title. В качестве значения элемента Title укажите описание пользовательского поля.
Например:
```
<Entity Name="OperatingSystem.Windows.WindowsHost">
  <Properties>
    <Property Name="UF_AssetNumber">
      <Title>Инвентарный номер актива в реестре</Title>
    </Property>
    <Property Name="UF_AssetOwner">
      <Title>Ответственный за актив</Title>
    </Property>
    <Property Name="UF_AssetRevisionDate">
      <Title>Дата последней ревизии актива</Title>
    </Property>
  </Properties>
</Entity>
```

Описание пользовательских полей добавлено.

19.3 Изменение имен пользовательских полей

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла UserModel.xml не игнорируется регистр символов.

❖ Чтобы изменить имена пользовательских полей:

1. В файле UserModel.xml в качестве значения атрибута version элементов layer id="UserModel", layer id="UserDescriptions" и значения атрибута Version элемента Dsl укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, version="19.0.20206.3").
2. Для элемента layer id="UserModel" → Dsl → Migrations добавьте дочерний элемент Group с атрибутом Version. В качестве значения атрибута Version укажите версию пользовательской модели, например:
```
<Group Version="19.0.20206.3">
</Group>
```

3. Для элемента Group добавьте дочерний элемент ChangeEntity с атрибутом Type. В качестве значения атрибута Type укажите Core.Host:
<ChangeEntity Type="Core.Host">
</ChangeEntity>
4. Для элемента ChangeEntity добавьте дочерние элементы RenameProperty (по количеству изменяемых пользовательских полей) с атрибутами Property и NewName. В качестве значения атрибута Property укажите старое имя поля, значения атрибута NewName – новое имя поля.

Примечание. Имена полей должны начинаться с префикса UF_.

Например:
<Group Version="19.0.20206.3">
<ChangeEntity Type="Core.Host">
<RenameProperty Property="UF_AssetNamber" NewName="UF_AssetNumber"/>
<RenameProperty Property="UF_AssetOuner" NewName="UF_AssetOwner"/>
</ChangeEntity>
</Group>
5. Перезапустите следующие службы:
docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|assetsidentity|assets-projections|assets-scans|core.scanning|core-tables|core-topology|coretopology-analyzer/ {print $NF}')

Имена пользовательских полей изменены.

19.4 Удаление пользовательских полей из модели актива

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла UserModel.xml не игнорируется регистр символов.

❖ Чтобы удалить пользовательские поля из модели актива:

1. В файле UserModel.xml в качестве значения атрибута version элементов layer id="UserModel", layer id="UserDescriptions" и значения атрибута Version элемента Dsl укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, version="19.0.20206.4").
2. Для элемента layer id="UserModel" → Dsl → Migrations добавьте дочерний элемент Group с атрибутом Version. В качестве значения атрибута Version укажите версию пользовательской модели, например:

```
<Group Version="19.0.20206.4">
</Group>
```

3. Для элемента Group добавьте дочерний элемент ChangeEntity с атрибутом Type. В качестве значения атрибута Type укажите Core.Host:
```
<ChangeEntity Type="Core.Host">
</ChangeEntity>
```
4. Для элемента ChangeEntity добавьте дочерние элементы RemoveProperty (по количеству удаляемых пользовательских полей) с атрибутом Property. В качестве значения атрибута Property укажите имя удаляемого поля.
Например:
```
<Group Version="19.0.20206.4">
  <ChangeEntity Type="Core.Host">
    <RemoveProperty Property="UF_AssetNumber"/>
    <RemoveProperty Property="UF_AssetOwner"/>
  </ChangeEntity>
</Group>
```
5. Перезапустите следующие службы:
```
docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|assetsidentity|assets-projections|assets-scans|core.scanning|core-tables|core-topology|coretopology-analyzer/ {print $NF}')
```

Пользовательские поля удалены из модели актива.

20 Настройка категоризации

Категоризация представляет собой модель, позволяющую унифицировать однотипные события, которые поступают от различных устройств. Эта модель позволяет создавать аппаратно-независимый контент, помогая сопоставлять события с нормализованными характеристиками.

Категории событий − это набор критериев, помогающих привести поступающие от различных источников события к общему формату, сохранив при этом их первоначальный смысл.

Схема полей событий (см. таблицу 20.1) представляет собой набор полей и их допустимых значений для сохранения информации о событиях на всех этапах их обработки. Столбец «Обязательное заполнение» указывает на необходимость обязательного заполнения поля в правиле нормализации или корреляции.

Таблица 20.1 − Схема полей событий

Название поля	Обязательное заполнение	Тип данных	Описание поля
Поля категоризации событий			
category.generic	Нет	String	Уровень категоризации generic
category.high	Нет	String	Уровень категоризации high
category.low	Нет	String	Уровень категоризации low
Поле, описывающие источник события			
event_src.category	При нормализации	Enum[1]	Категория источника события, например IDS/IPS, Firewall, Mail server
Параметры взаимодействия			
action	Обязательно	Enum[1]	Характер воздействия на объект
status	Обязательно	Enum[1]	Конечный результат воздействия

Название поля	Обязательное заполнение	Тип данных	Описание поля
Поле, описывающие субъект при взаимодействии			
subject	Нет	Enum[1]	Субъект воздействия
Поле, описывающие объект при взаимодействии			
object	Обязательно	Enum[1]	Объект воздействия
[1]Enum – это тип данных, чьё множество значений представляет собой ограниченный список идентификаторов.			

Справочник значений категорий представлен в документе «Руководство разработчика Ankey SIEM NG 5.2.3».

Пример категоризации события Kaspersky Security Center представлен в таблице 20.2.

Таблица 20.2 − Классификация события

Категория	Значение
Category.generic	Error
Subject	account
Action	info
Object	application
Event_src.category	Anti-virus
Status	success
Category.high	Security Software Management
Category.low	Update

Заполнение полей категориями происходит, когда компонент Ankey SIEM NG Server обрабатывает входящий поток событий, приводя их к единому формату. Таким образом, категории могут заполняться не только правилами нормализации, но и формулами обогащения и правилами корреляции. Ознакомиться с проставляемыми категориями можно, обратившись к этим объектам в веб-интерфейсе компонента Ankey SIEM NG Knowledge Base или в .kb-пакете.

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

21 Управление модулями сбора и обработки данных, модулями выявления нарушений ИБ (корреляционной обработки данных)

Примечание. Номер версии[6] дополнительных коннекторов Ankey SIEM NG и пакетов контента Ankey SIEM NG имеет формат A.B.C, где A – минимально поддерживаемая версия таксономии Ankey SIEM NG, B − мажорная версия изделия, C − минорная версия изделия. Например: 4.2.1.

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[7];

  Внимание! Установка стандартных коннекторов Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 5.2.3».
  Настройка сбора событий от стандартных источников в Ankey SIEM NG описана в «Руководстве по интеграции с источниками Ankey SIEM NG 5.2.3».

- дополнительные коннекторы, предназначенные для интеграции ПК Ankey SIEM NG с нестандартными источниками событий[7], которые не поддерживаются платформой Ankey SIEM NG (не являются «коробочным» решением).

[6] Для определения версии установленного коннектора см. пункт 24.21.5, для определения версии пакета контента см. пункт 24.22.7.

[7] Список поддерживаемых стандартных источников приведен в документе «Руководство по интеграции с источниками событий Ankey SIEM NG 5.2.3».

> Внимание! Установка дополнительных коннекторов Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 5.2.3». Настройка сбора событий от нестандартных источников в Ankey SIEM NG описана в документации на использование дополнительных коннекторов, которая поставляется в рамках приобретения таких изделий.

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 инсталляции Ankey SIEM NG 5.2.3». 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.

– пакет обнаружения компьютерных атак (корпоративный сегмент) – наборы инструментов мониторинга и выявления инцидентов, которые предназначены для выявления вредоносной активности в инфраструктуре на основе матрицы MITRE ATT&CK, а также для последующего построения цепочек атак и их обогащения в случае распределенного во времени развития атаки.

Внимание! Установка дополнительных пакетов контента Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 5.2.3». Настройка дополнительных пакетов контента в Ankey SIEM NG описана в документации на использование дополнительного пакета контента, которая поставляется в рамках приобретения такого изделия.

21.1 Рекомендации по обновлению ресурсов

При получении очередного обновления пакета экспертизы, необходимо импортировать его в систему.

Внимание! Импорт пакетов экспертизы производится только в эталонную корневую базу **GIS_DB**, а обновление ресурсов пользовательской ветки происходит через импорт ревизий.

Внимание! Перед проведением обновления необходимо экспортировать все записи из стандартных табличных списков конфигурации. После импорта ревизий все записи в стандартных табличных списках будут удалены.

Пользовательские ресурсы (скопированные и созданные) не затрагиваются обновлением, поэтому записи таких табличных списков экспортировать не требуется.

Для экспорта записей из табличного списка необходимо:

1. Выбрать табличный список в приложении Knowledge Base.
2. При выборе любой записи в табличном списке станет доступна панель инструментов, приведенная на рисунке 21.1.
3. Выбрать инструмент **Экспорт**.

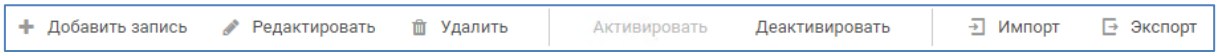


Рисунок 21.1 − Панель инструментов для работы с записями табличного списка

4. В открывшемся окне выбрать **Все <количество> записей** и экспортировать записи нажатием кнопки **Экспортировать**.

Записи табличных списков экспортируются в виде таблицы формата .csv. Обратный импорт доступен, если все названия колонок табличного списка в системе и в файле совпадают. При этом, если в табличный список добавились новые колонки, импорт будет доступен, отсутствующие в файле колонки

приобретут значение null (если колонка поддерживает null значения).

Если колонка табличного списка была переименована (или удалена), то импорт будет завершаться с ошибкой, как показано на рисунке 21.2. В таких случаях можно скорректировать .csv файл, приведя его в соответствие новой структуре табличного списка – переименовав название колонок или удалив лишние. Редактирование следует выполнять с помощью текстового редактора.

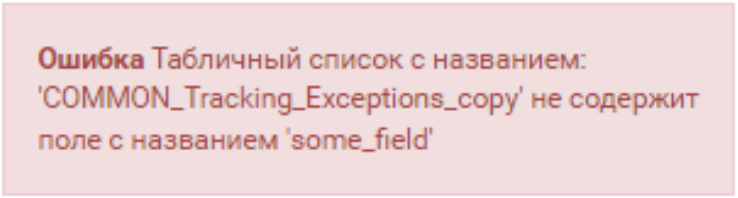


Рисунок 21.2 − Пример ошибки импорта записей в табличный список

Структура .csv файла представлена в виде соответствия названия колонок и всех значений:

“<название_колонки_1>”;…;”<название_колонки_N>”
“<запись_1_колонки_1>”;…;”<запись_1_колонки_N>”
…
“<запись_N_колонки_1>”;…;”<запись_N_колонки_N>”

21.2 Алгоритм обновления ресурсов в эталонной базе данных до новой версии

Внимание! Данный алгоритм предназначен только для обновления ресурсов в эталонной базе данных (**GIS_DB**). Любые попытки его применения к ветке эталонной базы (**Customer_Data**) приведут к потере всех пользовательских наработок, а также невозможности последующих обновлений и, как следствие, необходимости удаления и создания новой пользовательской ветки.

Для обновления ресурсов в эталонной базе данных до новой версии необходимо выполнить следующие действия:

1. В адресной строке браузера введите ссылку для входа в интерфейс ПК Ankey SIEM NG.
   Откроется страница входа в сервис Ankey SIEM NG MC.
2. 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**.
3. Убедившись в необходимости проведения обновления, в компоненте Ankey SIEM NG Core в приложении Knowledge Base разделе с наименованием базы данных выберите эталонную базу данных **GIS_DB** и перейдите к просмотру ее ресурсов.
4. В верхнем правом углу вкладки **Пакеты экспертизы** на панели инструментов выберете **Импорт**.

В открывшемся диалоговом окне нажмите ссылку выберите, где будет предложено указать файл для загрузки, или перетащите файл в диалоговое окно. После этого появится окно **Импорт объектов**. Выполните импорт с параметрами, указанными на рисунке 21.3.

Примечание. Параметр **Импортировать макросы Газинформсервис** присутствует только при импорте пакетов контента ПК Ankey SIEM NG. При импорте коннекторов ПК Ankey SIEM NG данный параметр отсутствует.

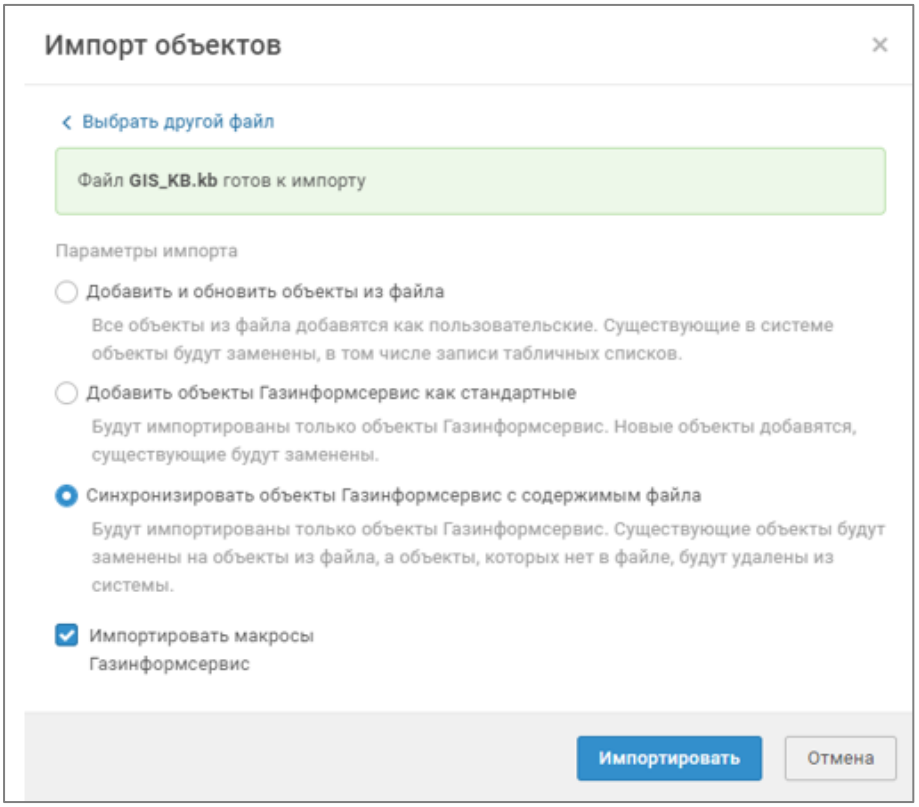


Рисунок 21.3 − Параметры импорта ресурсов для базы данных **GIS_DB**

5. После успешного импорта, все пакеты экспертизы, кроме импортированного, будут удалены из базы данных.
   Для пакета контента убедитесь, что версия импортированного пакета на вкладке **О пакете** изменилась на актуальную и соответствует заявленной в документации и названии файла пакета. Для отображения актуальной информации в разделе **О пакете** необходимо обновить страницу.

Внимание! В случае обновления пакета экспертизы под конкретный источник, при импорте будет унаследовано описание родительского пакета экспертизы (Пакета инфраструктурного контента), и, как следствие, версия останется прежней.

6. Далее необходимо выполнить импорт остальных пакетов экспертизы. Очередность в данном случае не имеет значения.
7. Последующий импорт выполняется аналогично пункту 4 с параметрами, указанными на рисунке 21.4.

Примечание. Параметр **Импортировать макросы Газинформсервис** присутствует только при импорте пакетов контента ПК Ankey SIEM NG. При импорте коннекторов ПК Ankey SIEM NG данный параметр отсутствует.

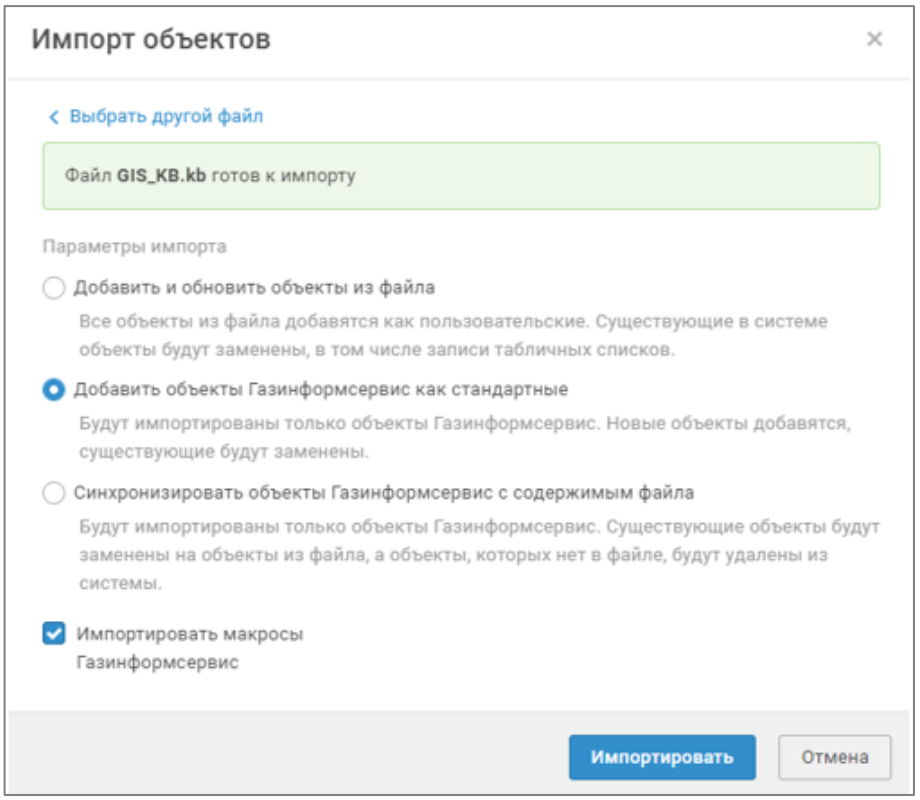


Рисунок 21.4 – Параметры для последующего импорта

Внимание! В случае получения обновления на два и более пакетов экспертизы импорт с параметрами **Синхронизировать объекты Газинформсервис с содержимым файла** достаточно выполнить только для первого импортируемого пакета.

8. Остальные пакеты экспертизы нужно импортировать с параметрами **Добавить объекты Газинформсервис как стандартные**.

Количество изменений (пакетов экспертизы) можно посмотреть в меню в разделе **<Название базы данных>** пункт **Базы данных**.

21.3 Алгоритм обновления ресурсов в ветке Customer_Data

После обновления ресурсов в эталонной базе данных **GIS_DB** до новой версии в пользовательской ветке **Customer_Data** все еще сохраняется старый набор пакетов экспертизы, они прошли валидацию и установлены в SIEM, включая измененные ресурсы.

Внимание! Перед обновлением все записи из табличных списков должны быть экспортированы. В противном случае записи будут удалены.

Для обновления ресурсов в пользовательской ветке **Customer_Data** необходимо выполнить следующие действия:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите ветку **Customer_Data**.
3. В панели инструментов нажмите кнопку **Импорт ревизий**.
   Начнется процесс применения изменений из родительской базы данных в дочернюю, появится индикатор выполнения. По завершении импорта появится сообщение **«Импорт выполнен»**.

   Примечание. Вы можете остановить импорт, нажав кнопку **Отменить**.

4. В строке сообщения нажмите кнопку **Завершить**.

Все изменения ресурсов в базе данных логируются в веб-интерфейсе, что позволяет провести сравнение ревизий и, при необходимости, откатить изменения к предыдущему состоянию. Аналогично можно сравнить состояние до и после обновления пакетов экспертизы, но нужно учитывать, что чем больше ресурсов изменилось в новой версии, тем дольше будет происходить загрузка изменений.

Описание сравнений ревизий представлено в документе «Руководство оператора Ankey SIEM NG 5.2.3».

21.4 Алгоритм обновления отдельных ресурсов, полученных в рамках технической поддержки (hotfix)

В рамках оказания технической поддержки по коннекторам и контенту Ankey SIEM NG могут быть предоставлены исправления критичных багов в отдельных ресурсах или группе ресурсов.

В результате обработки запроса на исправление бага может быть предоставлено исправление (hotfix):

- **для контента**: в виде доработанного ресурса или группы ресурсов отдельным пакетом с постфиксом **fix#**, например: **GIS_KB_Content_Std_3.5.3_fix1.kb**;

– **для коннектора**: в виде доработанного набора ресурсов отдельным пакетом, в наименовании которого содержится приставка **FC_NG_DEV-[НОМЕР_СБОРКИ]**, например: **FC_NG_DEV-34849_acronis_backup_Syslog_2023-08-09_08-24-57.zip**.

Внимание! Перед обновлением дополнительного коннектора необходимо внимательно ознакомиться с документацией, которая поставляется в рамках приобретения таких изделий. Если в рамках обновления до нового релиза потребуется отличная настройка параметров импорта (например, выбор параметра **Синхронизировать объекты Газинформсервис с содержимым файла**), то это будет указано в явном виде в документации дополнительного коннектора.

Примечание. Решение о критичности остается за ООО «Газинформсервис». В случаях, когда баг не будет расценен как критичный, его исправление включается в очередную релизную версию соответствующего пакета экспертизы.

При получении hotfix, необходимо установить его в Knowledge Base посредством импорта содержащихся в нем ресурсов через веб-интерфейс Ankey SIEM NG. Импорт выполняется в эталонную базу аналогично подразделу 21.2 пункту 4 с параметрами приведенными на рисунке 21.5.

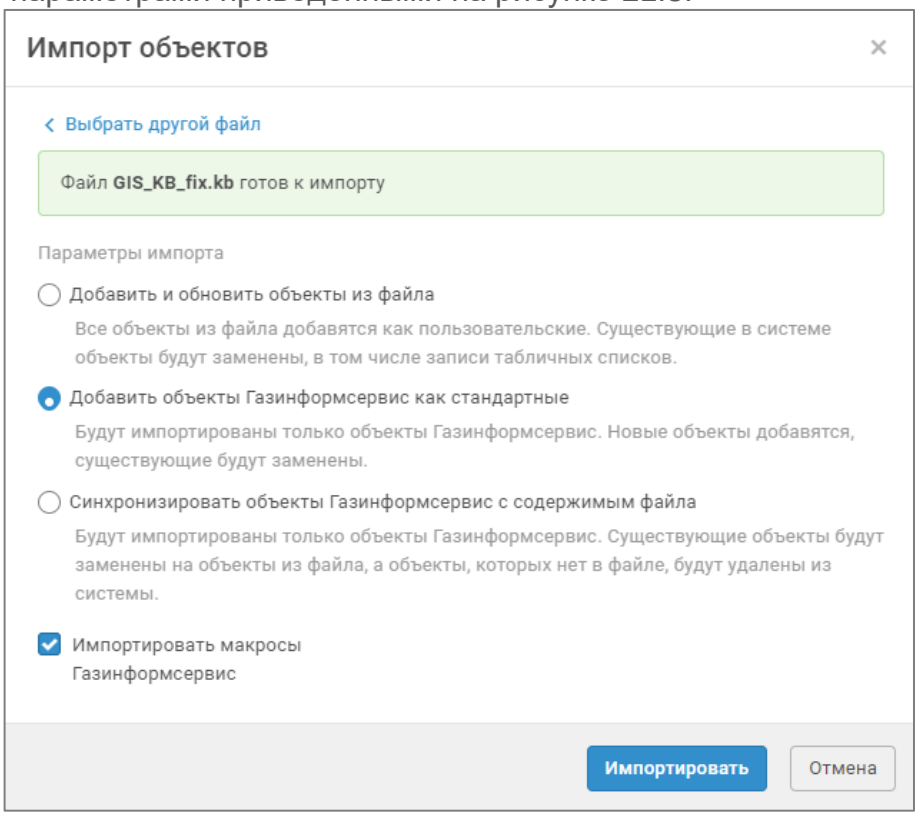


Рисунок 21.5 − Окно импорта hotfix

Примечание. Параметр **Импортировать макросы Газинформсервис** присутствует только при импорте пакетов контента ПК Ankey SIEM NG. При импорте коннекторов ПК Ankey SIEM NG данный параметр отсутствует.

После успешного импорта hotfix в эталонную корневую базу следует выполнить импорт ревизий в пользовательскую ветку, как описано в разделе 21.3.

Результатом обработки запроса на улучшение функционала может быть реализация описанных в запросе улучшений. Улучшение может быть включено только в очередной или последующие релизы пакетов экспертизы и никогда не предоставляется отдельно в виде hotfix. Решение о необходимости и способах реализации, а также сроках реализации улучшений остается за ООО «Газинформсервис».

Подробнее о технической поддержке ПК Ankey SIEM NG представлено в разделе 25.

21.5 Алгоритм обновления схемы полей событий и SDK после обновления компонентов Ankey SIEM NG

Внимание! Настройки необходимо выполнять от имени учетной записи суперпользователя системы.

После каждого обновления компонентов ПК Ankey SIEM NG на новую мажорную версию, например, после обновления с версии 4.1 до версии 5.2, обязательно требуется дополнительно обновить схему полей событий и SDK в эталонной базе ресурсов GIS_DB и пользовательской базе ресурсов Customer_data.

❖ Для обновления схемы полей событий и SDK необходимо:

1. Скопировать в операционную систему, где установлена роль Knowledge Base, пакет с таксономией полей <название пакета><версия пакета с таксономией>.kb, например: Taxonomy_5.2.kb.
2. Установить новую таксономию полей в эталонную базу ресурсов GIS_DB с помощью утилиты kbtools и интерфейса командной строки, выполнив команду: /var/lib/deployed-roles/<Название приложения Knowledge Base>/<название экземпляра роли приложения Knowledge Base, например kb-83dspx6udksxc1md0oulng>/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 true
3. В веб-интерфейсе ПК Ankey SIEM NG перейти в приложение Knowledge Base.
4. Раскрыть выпадающий список **SIEM** и перейти в раздел **Выбор версии SDK**.
5. Проверить значение поля **Версия схемы полей событий**.

В значении поля должна быть указана обновленная версия схемы полей событий. Например: 26.0.220-release-26.0.

6. Нажав кнопку меню **<Название БД>**, раскрыть выпадающий список и выбрать раздел **Базы данных**.
   Откроется меню **Базы данных**.
7. В меню **Базы данных** выбрать пользовательскую базу ресурсов **Customer_data**.
8. Выполнить импорт ревизий из базы данных GIS_DB, нажав кнопку **Импорт ревизий** для того, чтобы обновить схему полей событий в базе ресурсов Customer_data.
9. После успешного импорта новой схемы полей в эталонную базу GIS_DB и Customer_data необходимо установить актуальную версию SDK. Для этого:
   - Раскрыть выпадающий список **SIEM**.
   - Выбрать пункт выпадающего списка **Выбор версии SDK**.
   - Выбрать актуальную версию SDK и нажать на графическую кнопку **Восстановить SDK для валидации**.

Схема полей событий и SDK обновлены.

22 Работа с инфраструктурами

При сканировании ИТ-инфраструктуры предприятия важно правильно идентифицировать активы. Сканирование одним коллектором сетевых сегментов, активы в которых имеют одни и те же IP-адреса, может привести к неверной агрегации активов: вместо нескольких активов система может идентифицировать один актив. Также наличие в списке активов с одинаковым IP-адресом может затруднить оператору поиск необходимого актива.

При наличии в составе площадки таких сегментов сети рекомендуется для каждого из них создать в Ankey SIEM NG отдельную инфраструктуру и сканировать такие инфраструктуры одним коллектором по отдельности.

После развертывания система имеет одну инфраструктуру **Инфраструктура по умолчанию**. Вы можете создавать другие инфраструктуры, изменять их названия и удалять их на странице **Сбор данных** → **Инфраструктура**.

22.1 Создание инфраструктуры

❖ Чтобы создать инфраструктуру:

1. В главном меню в разделе **Сбор данных** выберите пункт **Инфраструктура**.
   Откроется страница **Инфраструктура**.
2. В панели инструментов нажмите кнопку **Добавить инфраструктуру**.
   Откроется страница **Создание инфраструктуры**.
3. Введите название инфраструктуры.
4. Нажмите кнопку **Создать**.

Инфраструктура создана.

22.2 Изменение названия инфраструктуры

❖ Чтобы изменить название инфраструктуры:

1. В главном меню в разделе **Сбор данных** выберите пункт **Инфраструктура**.
   Откроется страница **Инфраструктура**.
2. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Редактирование инфраструктуры <Название инфраструктуры>**.
3. Измените название инфраструктуры.
4. Нажмите кнопку **Сохранить**.

Название инфраструктуры изменено.

22.3 Удаление инфраструктуры

❖ Чтобы удалить инфраструктуру:

1. В главном меню в разделе **Сбор данных** выберите пункт **Инфраструктура**.
   Откроется страница **Инфраструктура**.
2. В списке инфраструктур выберите инфраструктуру, которую необходимо удалить.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

> **Примечание.** Если к удаляемой инфраструктуре привязаны активы, они тоже будут удалены. Задачи, собиравшие данные с активов удаленной инфраструктуры, не будут автоматически остановлены, их необходимо остановить вручную.

Инфраструктура удалена.

23 Изменение проверок по чек-листу

❖ Чтобы изменить проверки на Linux:

1. На сервере Ankey SIEM NG Core в каталоге /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/config/usagemonitoring создайте копию файла check_settings.default.yaml – файл check_settings.yaml.
4. В файле check_settings.yaml измените необходимые параметры (см. приложение В).
5. Перезапустите контейнер core-usage-monitoring:
   docker restart $(docker ps | awk '/core-usage-monitoring/ {print $NF}')

Проверки изменены.

24 Диагностика и решение проблем

В этом разделе приводятся инструкции по диагностике и решению проблем, возникающих при работе с Ankey SIEM NG. Шаги инструкций необходимо выполнять в порядке их перечисления. После того, как один из шагов инструкции привел к решению проблемы, выполнять следующие за ним шаги не нужно.

24.1 Уведомления о состоянии системы

В ПК Ankey SIEM NG реализован автоматический мониторинг параметров жизнеспособности и целостности системы и ее компонентов. Источником для мониторинга служат статистические данные за определенные периоды. Результаты мониторинга отображаются по нажатию индикатора состояния.

Предусмотрены следующие цветовые индикаторы уведомлений:

- красный – сообщает о неполадке или сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен);
- желтый − сообщает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра);
- зеленый − сообщает о том, что система работает корректно;
- синий − сообщает о каком-либо событии, не нарушающем жизнеспособность и целостность системы или ее компонента.
- белый – сообщает о том, что диагностику системы выполнить не удалось.

24.2 Обмен данными между компонентами системы

1. Для обмена данными между службами компонентов Ankey SIEM NG используется брокер сообщений RabbitMQ. В общем случае в системе реализован следующий порядок обмена данными (сообщениями) между службами:
2. При подключении к брокеру службы-отправители создают необходимые точки обмена сообщениями, службы-получатели создают необходимые очереди сообщений и связывают очереди с точками обмена с помощью ключей маршрутизации. Далее службы поддерживают постоянное соединение с брокером.
3. Получив сообщение, брокер уведомляет об этом службу-отправителя и направляет сообщение в точку обмена. Сообщение содержит ключ маршрутизации, поэтому точка обмена пересылает полученное сообщение только в указанную в ключе очередь.

4. Как только сообщение становится первым в очереди, брокер отправляет его службе-получателю. Обработав сообщение, служба-получатель уведомляет об этом брокер.
5. После получения уведомления брокер удаляет из очереди отправленное сообщение. Если брокер не получает уведомление, он не удаляет сообщение из очереди и будет отправлять его до тех пор, пока не получит уведомление.

Примечание. Служба может быть одновременно и отправителем, и получателем сообщений.

В конфигурации для низконагруженных систем используется только один брокер RabbitMQ. Он устанавливается вместе с компонентами (на один сервер) и обеспечивает как обмен данными между службами одного компонента, так и обмен данными между службами разных компонентов Ankey SIEM NG.

В конфигурациях для средненагруженных или высоконагруженных систем используются два брокера. Один из них устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен данными между службами Ankey SIEM NG Core, а также между службами разных компонентов Ankey SIEM NG. Другой брокер устанавливается на сервер Ankey SIEM NG Server и обеспечивает обмен данными только между его службами.

Поскольку события от активов тоже пересылаются между службами в виде сообщений RabbitMQ, проблемы в работе службы-получателя (например, ее незапланированная остановка) при постоянном потоке событий могут привести к существенному росту количества сообщений в очереди. Это уменьшает доступные системе память ОЗУ или свободное место на диске сервера Ankey SIEM NG Server, прежде всего в конфигурациях для средненагруженных или высоконагруженных систем. Для диагностики проблемы важно понимать, откуда очередь получает события и куда их отправляет.

Примечание. Подробное описание процесса обработки событий см. в Руководстве разработчика Ankey SIEM NG 5.2.3.

Таблица 24.1 − Очереди RabbitMQ и связанные с ними службы Ankey SIEM NG Server

Имя очереди	Служба-отправитель	Служба-получатель
pt.mpx.siem.receiver.incoming	Core Agent	SIEM Server receiver
normalizeq	SIEM Server receiver	SIEM Server normalizer
aggregatorq	SIEM Server normalizer	SIEM Server aggregator
event.resolve	SIEM Server aggregator	SIEM Server resolver
enricherq	SIEM Server resolver	SIEM Server enricher
routerq	SIEM Server enricher	SIEM Server router
correlatorq	SIEM Server router	SIEM Server correlator
notifierq	SIEM Server router	SIEM Server correlator

Имя очереди	Служба-отправитель	Служба-получатель
storageq	SIEM Server normalizer, SIEM Server resolver, SIEM Server router	SIEM Server storage

Приведенные в таблице очереди принадлежат брокеру Ankey SIEM NG Server.

24.2.1 Вход в RabbitMQ

Перед входом в RabbitMQ необходимо убедиться, что правила межсетевого экрана разрешают входящее соединение от рабочей станции администратора к серверу RabbitMQ через порт 15672/TCP.

❖ Чтобы войти в RabbitMQ:

1. В адресной строке браузера введите:
   http://<IP-адрес или FQDN сервера RabbitMQ>:15672
   Откроется страница входа в RabbitMQ.
2. Введите логин siem и пароль.

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

3. Нажмите кнопку **Login**.
4. Отобразится страница **Overview**.

Вход в RabbitMQ выполнен.

24.2.2 Мониторинг потока событий в RabbitMQ

Каждое сообщение в RabbitMQ может содержать несколько событий. Среднее количество событий в одном сообщении – 48, максимально возможное – 64.

Вы можете отслеживать обработку системой потока событий на следующих страницах интерфейса RabbitMQ:

1. **Overview**. На странице в раскрывающемся блоке **Totals** отображаются графики количества сообщений, поступивших в брокер за указанный период, и скорости потока сообщений за этот период. В раскрывающемся блоке **Nodes** отображается информация об используемых памяти ОЗУ, месте на диске, а также о количестве используемых брокером дескрипторов файла и сокета.
2. **Exchanges**. На странице отображается таблица точек обмена, в столбцах **Message rate in** и **Message rate out** приводятся входная и, соответственно, выходная скорости потока сообщений, проходящего через точку.
3. **Queues**. На странице отображается таблица очередей сообщений:
   – в столбце **Ready** приводится количество неотправленных, но готовых к отправке сообщений в очереди;
   – в столбце **Unacked** приводится количество отправленных, но не удаленных брокером сообщений. Брокер удалит их из

очереди после получения от службы уведомления об обработке;
- в столбце **Total** приводится общее количество сообщений в очереди.

24.2.3 Очередь storageq не уменьшается

Возможные причины

Возможными причинами проблемы являются неработоспособность компонента Ankey SIEM NG ES или его сетевая недоступность.

Решение

❖ Чтобы решить проблему:

1. На сервере Ankey SIEM NG ES проверьте статус служб (см. пункт 24.24.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. подраздел 24.12).
4. Убедитесь, что параметр ElasticsearchHost компонента Ankey SIEM NG Server равен IP-адресу или FQDN сервера Ankey SIEM NG ES.
5. Убедитесь, что порт 9200/TCP сервера Ankey SIEM NG ES доступен для входящих соединений от сервера Ankey SIEM NG Server.
6. Создайте файл дампа памяти (см. пункт 24.24.7) службы SIEM Server storage.
7. Перезапустите службу SIEM Server storage.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[8], приложив следующую информацию:

- файлы siem.conf, /etc/opt/siem/siem/params.yaml и /etc/opt/siem/siem-server/ params.yaml;
- файл дампа памяти (см. пункт 24.24.7) службы SIEM Server storage;
- файлы журналов Elasticsearch, RabbitMQ, служб SIEM Server storage и SIEM Server frontend.

24.2.4 Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается

Возможные причины

Возможными причинами проблемы являются неработоспособность RabbitMQ или остановка службы Ankey SIEM NG Server, обрабатывающей сообщения очереди.

[8] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

Решение

❖ Чтобы решить проблему:

1. В веб-интерфейсе RabbitMQ на странице **Overview** проверьте наличие ошибок. Если ошибки присутствуют перейдите к их устранению (подробнее см. на сайте rabbitmq.com).
2. Проверьте статус служб (см. пункт 24.24.3) Ankey SIEM NG Server. Если служба остановлена, запустите ее.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[9], приложив следующую информацию:

- снимок экрана, содержащий страницу **Queues** веб-интерфейса RabbitMQ;
- снимок экрана, содержащий параметры очереди и таблицу с получателями сообщений (в раскрывающемся блоке **Consumers)**;
- результат запроса о статусе служб (см. пункт 24.24.3) Ankey SIEM NG Server;
- файлы журналов Ankey SIEM NG Server, RabbitMQ, служб SIEM Server Watchdog (только в конфигурации для низконагруженных систем) и Core Watchdog;
- снимок экрана страницы Система → Мониторинг обработки событий.

24.2.5 Очередь storageq растет и начинает уменьшаться только после появления ошибки

Возможные причины

Возможной причиной проблемы является несоответствие производительности Ankey SIEM NG Server и Ankey SIEM NG ES входящему потоку событий. В этом случае Ankey SIEM NG не успевает обработать события, что приводит к накоплению сообщений в очереди. Последующее срабатывание системы автоматического мониторинга (с появлением ошибки) останавливает отправку и прием событий, очередь начинает уменьшаться. После уменьшения размера очереди до определенного значения система возобновляет отправку и прием событий, что может опять привести к накоплению сообщений в очереди. Такое накопление очереди до появления ошибки и ее последующее уменьшение могут повторяться.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики серверов Ankey SIEM NG Server и Ankey SIEM NG ES соответствуют минимальным требованиям к конфигурации.
2. Убедитесь, что объем раздела подкачки (см. пункт 24.24.1) на сервере Ankey SIEM NG ES равен нулю.
3. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. пункт 24.24.5). Если таких индексов более 900,

[9] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 12).

4. Убедитесь, что центральный процессор, ОЗУ и жесткие диски серверов Ankey SIEM NG Server и Ankey SIEM NG ES не испытывают высокой нагрузки от запущенных процессов (см. пункт 24.24.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки ООО «Газинформсервис»[9], приложив снимки экрана.
5. Убедитесь, что скорость потока событий от источников соответствует развернутой конфигурации системы.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[10], приложив следующую информацию:

- файлы журналов Ankey SIEM NG Server и Ankey SIEM NG ES, RabbitMQ;
- аппаратные характеристики серверов Ankey SIEM NG Server и Ankey SIEM NG ES;
- данные о нагрузке на центральный процессор, ОЗУ и жесткие диски (см. пункт 24.24.2) сервера Ankey SIEM NG ES;
- результат запроса о состоянии индексов (см. пункт 24.24.5);
- снимок экрана страницы Система → Мониторинг обработки событий.

24.2.6 Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки

Возможные причины

Возможной причиной проблемы является несоответствие производительности Ankey SIEM NG Server и Ankey SIEM NG ES входящему потоку событий. В этом случае Ankey SIEM NG не успевает обработать события, что приводит к накоплению сообщений в очереди. Последующее срабатывание системы автоматического мониторинга (с появлением ошибки) останавливает отправку и прием событий, очередь начинает уменьшаться. После уменьшения размера очереди до определенного значения система возобновляет отправку и прием событий, что может опять привести к накоплению сообщений в очереди. Такое накопление очереди до появления ошибки и ее последующее уменьшение могут повторяться.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что скорость потока событий от источников соответствует развернутой конфигурации системы.
2. Убедитесь, что центральный процессор, ОЗУ и жесткие диски серверов Ankey SIEM NG Server и Ankey SIEM NG ES не

[10] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

испытывают высокой нагрузки от запущенных процессов (см. пункт 24.24.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки ООО «Газинформсервис»[10], приложив снимки экрана.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[10], приложив следующую информацию:

- файлы журналов Ankey SIEM NG Server и RabbitMQ;
- файл конфигурации siem.conf;
- снимок экрана страницы Система → Мониторинг обработки событий;
- данные о нагрузке (см. пункт 24.24.2) на центральный процессор, ОЗУ и жесткие диски сервера Ankey SIEM NG Server.

24.3 Мониторинг состояния RabbitMQ и Elasticsearch

Ankey SIEM NG с помощью службы SIEM Server health monitor автоматически отслеживает состояние брокера сообщений RabbitMQ и хранилища событий Elasticsearch. На основании результатов мониторинга поток данных, поступающих в систему, может быть временно ограничен.

Служба содержит модули проверки и модули действия. Модуль проверки отслеживает параметры состояния и при превышении их пороговых значений отправляет предупреждение, сообщение об ошибке или запрашивает выполнение определенного действия. Модуль действия периодически проверяет наличие такого запроса и при его обнаружении может ограничить поток данных, поступающий в RabbitMQ, а также остановить прием данных службой SIEM Server receiver.

Для настройки модулей вам потребуются файлы конфигурации службы SIEM Server health monitor. Файлы содержат JSON-объекты, необходимые для настройки того или иного модуля. Каждый объект состоит из набора параметров (пар «ключ − значение»). После изменения параметров необходимо перезапустить службу. После обновления системы значения параметров возвращаются в используемые по умолчанию.

24.3.1 Параметры конфигурации службы SIEM Server health monitor

Ниже описано назначение JSON-объектов, содержащих параметры модулей проверки (секция checks) и модулей действия, приведен алгоритм работы модулей.

rabbitmq → poll_period

Параметр poll_period определяет частоту запросов для проверки статуса RabbitMQ и свободного места на диске (объект disk_size), для мониторинга длины очереди (объект queues_size) и объема памяти ОЗУ, занимаемой очередями (объект queues_memory). В случае обнаружения статуса «failed» модуль сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

По умолчанию запросы отправляются каждые 30 секунд.

rabbitmq → disk_size

Объект содержит параметры для настройки мониторинга свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ. По умолчанию модуль проверки запрашивает объем свободного места каждые 30 секунд (параметр poll_period).

По результатам запроса модуль:

- если диск содержит меньше 40 ГБ (параметр limits → warn), но больше 30 ГБ (параметр limits → min) свободного места − предупреждает об этом службу SIEM Server health monitor;
- если диск содержит меньше 30 ГБ (параметр limits → min) свободного места − сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

Объем свободного места будет увеличиваться после остановки отправки данных. Если он становится больше 30 ГБ (параметр limits → min), модуль проверки отзывает запросы на остановку.

rabbitmq → queues_size

Объект содержит параметры для настройки мониторинга очереди pt.mpx.siem.receiver.incoming. По умолчанию модуль проверки запрашивает количество сообщений в очереди каждые 30 секунд (параметр poll_period).

По результатам запроса модуль:

- если в очереди находится больше 1000 сообщений (параметр limits → warn), но меньше 2000 сообщений (параметр limits → max) − предупреждает об этом службу SIEM Server health monitor;
- если в очереди находится больше 2000 сообщений (параметр limits → max) − сообщает об ошибке и запрашивает остановку приема данных службой SIEM Server receiver.

Количество сообщений в очереди будет уменьшаться после остановки отправки данных. Если в очереди становится меньше 500 сообщений (параметр limits → min), модуль проверки отзывает запрос на остановку.

rabbitmq → queues_memory

Объект содержит параметры для настройки мониторинга объема памяти ОЗУ, используемого очередями виртуального узла RabbitMQ. По умолчанию модуль проверки запрашивает объем используемой памяти каждые 30 секунд (параметр poll_period).

По результатам запроса модуль:

- если используемый объем больше 4 ГБ (параметр limits → warn), но меньше 6 ГБ (параметр limits → max) − предупреждает об этом службу SIEM Server health monitor;
- если используемый объем больше 6 ГБ (параметр limits → max) − сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

После остановки отправки данных объем используемой памяти будет уменьшаться. Если он становится меньше 4 ГБ (параметр limits → min), модуль проверки отзывает запросы на остановку.

elasticsearch → poll_period

Параметр poll_period определяет частоту запросов для проверки статуса Elasticsearch и свободного места на диске (объект disk_size). В случае обнаружения статуса «red» модуль сообщает об ошибке, а также запрашивает остановку отправки данных от коллекторов и приема данных службой SIEM Server receiver.

По умолчанию запросы отправляются каждые 30 секунд.

elasticsearch → disk_size

Объект содержит параметры для настройки мониторинга свободного места на логическом диске, занимаемом узлами RabbitMQ. По умолчанию модуль проверки запрашивает объем свободного места каждые 30 секунд (параметр poll_period).

По результатам запроса модуль:

- если диск содержит меньше 200 ГБ (параметр limits → warn), но больше 60 ГБ (параметр limits → min) свободного места − предупреждает об этом службу SIEM Server health monitor;
- если диск содержит меньше 60 ГБ (параметр limits → min) свободного пространства − сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

Объем свободного места будет увеличиваться после остановки отправки данных. Если он становится больше 60 ГБ (параметр limits → min), модуль проверки отзывает запросы на остановку.

agent

Объект содержит параметры для управления потоком данных, отправляемых коллектором. По умолчанию модуль действия каждые 30 секунд (параметр check_period) проверяет наличие запроса на остановку отправки данных. При наличии запроса модуль запрещает коллектору отправлять данные в течение 40 секунд (параметр timeout). Если при следующих проверках модуль не обнаруживает ранее существовавший запрос, он снова отправляет коллектору запрет, причем длительность запрета при каждой последующей отправке уменьшается на 5 секунд (параметр timeout_step). Когда длительность запрета станет равна нулю, модуль прекращает его отправку.

receiver

Объект содержит параметры для управления потоком данных, принимаемых службой SIEM Server receiver. По умолчанию модуль действия каждые 30 секунд (параметр check_period) проверяет наличие запроса на остановку приема данных. При наличии запроса модуль запрещает службе принимать данные в течение 40 секунд (параметр timeout). Если при следующих проверках модуль не обнаруживает ранее существовавший запрос, он снова отправляет службе запрет, причем длительность запрета при каждой последующей отправке уменьшается на 5 секунд (параметр timeout_step). Когда длительность запрета станет равна нулю, модуль прекращает его отправку.

24.4 Ошибка "Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога"

Возможные причины

Возможной причиной ошибки является неспособность компонентов Ankey SIEM NG Server и Ankey SIEM NG ES вовремя обрабатывать входящий поток сообщений или неисправность компонентов.

Решение

❖ Чтобы решить проблему:

1. Если присутствует ошибка "Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен", устраните ее.
3. Войдите в RabbitMQ (см. пункт 24.2.1) и проверьте состояние очередей (см. пункт 24.2.2):
   - если количество сообщений не уменьшается, перейдите к решению проблемы "Очередь <Название очереди> не уменьшается";
   - если количество сообщений уменьшается, перейдите к решению проблемы "Очередь <Название очереди> растет и начинает уменьшаться только после появления ошибки".

24.5 Ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен»

Возможные причины

Возможными причинами ошибки являются сетевая недоступность Ankey SIEM NG ES, обработка компонентом сложного запроса или инициализация Elasticsearch после перезагрузки, вызванной срабатыванием системы автоматического мониторинга. Указанные ниже действия по решению проблемы рекомендуется выполнять только в том случае, если ошибка не исчезает в течение 15 минут.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что для Ankey SIEM NG Core задан правильный IP-адрес или FQDN компонента Ankey SIEM NG ES.
2. Убедитесь, что сетевой порт 9200/TCP сервера Ankey SIEM NG ES доступен (см. раздел 24.24.4) для Ankey SIEM NG Core.
3. На сервере Ankey SIEM NG ES проверьте статус служб (см. раздел 24.24.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. раздел 24.12).
4. Проверьте состояние индексов Elasticsearch (см. раздел 24.24.5). Если в Elasticsearch есть индексы в состоянии red, перейдите к решению этой проблемы (см. раздел 24.11).

Если выполнение указанных выше шагов не решило проблему,

необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис», приложив следующую информацию:

- результат выполнения каждого шага инструкции по решению проблемы;
- файлы журналов Elasticsearch;
- данные о нагрузке на центральный процессор, ОЗУ и жесткие диски (см. раздел 19.20.2) серверов Ankey SIEM NG Server и Ankey SIEM NG ES;
- результат запроса о состоянии индексов (см. раздел 24.24.5).

24.6 Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога»

Перед появлением ошибки система отображает предупреждение «Заканчивается свободное место на диске, выделенном для Core Messaging Service».

Возможные причины

Причиной ошибки является уменьшение свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики сервера Ankey SIEM NG Core соответствуют минимальным требованиям к конфигурации.
2. Определите, на какой логический диск установлен RabbitMQ.
   /<Название приложения>/<Название экземпляра роли rmqmessagebus>
   Например:
   df -h /var/lib/deployed-roles/ankey-application/rmqmessagebus/
   Консоль отобразит информацию о диске, на который установлен RabbitMQ.
3. Убедитесь, что этот логический диск занят только файлами, необходимыми для работы ОС и Ankey SIEM NG. Если диск содержит другие файлы и каталоги, удалите их.
4. Перезапустите службу Core Health Monitoring.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис», приложив следующую информацию:

- файл журнала службы Core Health Monitoring;
- снимок экрана, отображающий свободное место на логическом диске.

24.7 Ошибка "Объем свободного места на диске, выделенном для SIEM Messaging Service, достиг критического порога

Перед появлением ошибки система отображает предупреждение "Заканчивается свободное место на диске, выделенном для SIEM Messaging Service".

Возможные причины

Причиной ошибки является уменьшение свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики сервера Ankey SIEM NG Server соответствуют минимальным требованиям к конфигурации.
2. Определите, на какой логический диск установлен RabbitMQ: `df -h /var/lib/rabbitmq`
   Интерфейс терминала отобразит имя диска и его параметры.
3. Убедитесь, что этот логический диск занят только файлами, необходимыми для работы ОС и Ankey SIEM NG. Если диск содержит другие файлы и каталоги, удалите их.
4. Перезапустите службу SIEM Health Monitoring.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[11], приложив следующую информацию:

- файлы журналов служб SIEM Health Monitoring, SIEM Health Monitor;
- снимок экрана, отображающий свободное место на логическом диске.

24.8 Ошибка "Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога"

Перед появлением ошибки система отображает предупреждение "Заканчивается свободное место на диске, выделенном для SIEM Events Storage".

Возможные причины

Причиной ошибки является уменьшение свободного места на логическом диске, занимаемом индексами Elasticsearch.

[11] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики сервера Ankey SIEM NG ES соответствуют минимальным требованиям к конфигурации.
2. Убедитесь, что логический диск с индексами (см. пункт 24.24.8) занят только файлами, необходимыми для работы ОС и Ankey SIEM NG. Если диск содержит другие файлы и папки, удалите их.
3. Проверьте свободное место на логическом диске с индексами Elasticsearch (см. пункт 24.24.8). Если на диске менее 40 ГБ свободного места, настройте архивацию индексов по расписанию (см. подраздел 12.3).
4. Проверьте свободное место на логическом диске с архивными индексами (см. пункт 24.24.8). Если на диске отсутствует свободное место, настройте удаление архивных индексов по расписанию (см. пункт 12.5.2).
5. На сервере Ankey SIEM NG Core перезапустите службу Core Health Monitoring.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[12], приложив следующую информацию:

– файлы журнала службы Core Health Monitoring;
– снимок экрана, отображающий свободное место на логическом диске.

24.9 Ошибка "Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем"

Возможные причины

Причиной ошибки является прекращение работы RabbitMQ.

Решение

❖ Чтобы решить проблему:

1. Проверьте состояние службы RabbitMQ (см. пункт 24.24.3). Если служба остановлена, запустите ее вручную.
2. Проверьте доступность страницы входа в RabbitMQ (см. пункт 24.24.1). Если страница недоступна, сообщите об этом в службу технической поддержки ООО «Газинформсервис», приложив журналы службы RabbitMQ.

[12] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.10 Предупреждение "Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога"

Возможные причины

Производительность и объем жестких дисков не соответствуют входящему потоку событий. Также производительность может снижаться при обработке сложных запросов или событий с нетиповой структурой.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики сервера Ankey SIEM NG ES соответствуют минимальным требованиям к конфигурации.
2. Убедитесь, что объем раздела подкачки (см. пункт 24.24.1) на сервере Ankey SIEM NG ES равен нулю.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[13], приложив следующую информацию:

- нагрузке на файловую систему и запущенных процессах (см. пункт 24.24.2); файлы журналов служб Core Health Monitoring и Elasticsearch;
- файлы журналов (см. пункт 24.24.2) служб SIEM Server storage и SIEM Server frontend, собранные в режиме расширенного журналирования;
- снимок экрана страницы Система → Мониторинг обработки событий;
- аппаратные характеристики сервера Ankey SIEM NG ES, включая информацию об уровне RAID-массива и параметрах жестких дисков.

24.11 Индексы Elasticsearch находятся в состоянии red

Индексы Elasticsearch предназначены для хранения данных о событиях информационной безопасности и их последующего поиска. Если не удается прочитать данные из индекса, его состояние сменится на red. В такой индекс нельзя ни записать данные, ни считать их из него.

Возможные причины

Возможной причиной проблемы является незапланированное завершение записи данных на диск (например, в случае аварийного выключения питания сервера, сбоя в работе файловой системы или сбора данных о событиях во время обновления Ankey SIEM NG). Также индексы находятся в состоянии red во время инициализации Elasticsearch (например, после перезагрузки сервера), что является корректным поведением системы (после инициализации все

[13] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

индексы должны находиться в состоянии green или yellow).

Решение

Перед выполнением инструкции необходимо убедиться, что службы Elasticsearch запущены (см. пункт 24.24.3) и не менее 15 минут находятся в статусе active (running).

❖ Чтобы решить проблему:

1. На сервере Ankey SIEM NG ES выполните команду:
   curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true
2. Если индексы все еще находятся в состоянии (см. пункт 24.24.5) red, повторно выполните команду: curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true

   Примечание. Рекомендуется выполнять команду повторно не более двух раз.

3. Если требуется оперативно восстановить работоспособность системы, удалите индексы (см. подраздел 12.6), которые находятся в состоянии red.

   Внимание! При удалении индексов будут потеряны сохраненные в них данные.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[14], приложив следующую информацию:

- данные о состоянии (см. пункт 24.24.5) индексов и шардов (фрагментов индексов);
- время запуска каждой команды curl -XPOST localhost:9200/_cluster/reroute? retry_failed=true;
- файлы журналов Elasticsearch, SIEM Health Monitor.

[14] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.12 Служба Elasticsearch останавливается через некоторое время после запуска

Возможные причины

Возможными причинами незапланированной остановки службы являются внезапный сбой в ее работе или недостаточный объем памяти ОЗУ сервера Ankey SIEM NG ES.

Решение

❖ Чтобы решить проблему:

1. Запустите службу вручную.

> **Примечание.** После запуска службы начнется процесс инициализации Elasticsearch, которая может занять до 15 минут. По завершении инициализации все индексы должны находится в состоянии (см. пункт 24.24.5) green или yellow.

2. Зафиксируйте время повторной остановки службы.
3. Если Ankey SIEM NG ES установлен на Linux, убедитесь, что суммарный объем памяти ОЗУ, выделяемый для всех узлов кластера (параметры DataNodeHeapSize, ClientNodeHeapSize и MasterNodeHeapSize (см. приложение А)), не превышает 58% от объема памяти ОЗУ сервера.
4. Убедитесь, что объем раздела подкачки (см. пункт 24.24.1) на сервере Ankey SIEM NG ES равен нулю.
5. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. пункт 24.24.5). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 12).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[15], приложив следующую информацию:

- период остановки службы, точное время каждой остановки;
- скорость потока событий;
- файл /tmp/hs_err_pid.log (на Linux);
- аппаратные характеристики сервера Ankey SIEM NG ES, включая информацию об уровне RAID-массива и параметрах жестких дисков.

24.13 Система не получает данные от задачи

Возможные причины

Возможными причинами проблемы являются ошибки в работе компонентов системы, неправильная настройка профиля для сбора данных, сбои в работе источника событий, а также сбор событий с неподдерживаемых источников.

[15] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что задача запущена.
2. Проверьте наличие ошибок (см. подраздел 24.1) системы автоматического мониторинга. Если ошибки присутствуют, устраните их.
3. Проверьте, что источник событий поддерживается системой. Если источник не поддерживается, система не сможет получать от него данные.

> **Примечание.** Список поддерживаемых источников приведен в Руководстве по интеграции с источниками Ankey SIEM NG 5.2.3.

4. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 5.2.3) и проверьте наличие в нем строк с параметром PackCount. Если такие строки отсутствуют, проверьте наличие сетевого соединения между коллектором и источником.
5. Проверьте журнал задачи на наличие ошибок. Если ошибки присутствуют, убедитесь, что профиль задачи и параметры источника настроены правильно (см. Руководство по интеграции с источниками Ankey SIEM NG 5.2.3).
6. На странице **Система** → **Управление системой** → **Коллекторы** проверьте статус коллектора. Если коллектор имеет статус "Недоступен", сохраните файлы его журналов для последующей отправки в службу технической поддержки.
7. Проверьте очереди в RabbitMQ (см. пункт 24.2.1). Если количество сообщений в очередях не уменьшается, сделайте снимок экрана со списком очередей для последующей отправки в службу технической поддержки.
8. Проверьте состояние Elasticsearch. Если Elasticsearch имеет статус red, перейдите к решению проблемы "Индексы Elasticsearch находятся в состоянии red (см. подраздел 24.11)".
9. Проверьте состояние служб (см. пункт 19.20.3) Ankey SIEM NG Server. Если служба остановлена, запустите ее вручную.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[16], приложив следующую информацию:

- файлы журналов задачи и коллектора;
- название и версию источника;
- снимок экрана с очередями RabbitMQ;
- файлы журналов служб Ankey SIEM NG Server, которые были запущены вручную;
- сведения о том, поступали ли ранее данные от этого источника.

[16] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.14 Отсутствуют события от источников

Возможные причины

Возможными причинами проблемы являются неправильная настройка источника событий или задачи по сбору данных, а также сбои в работе системы, возникающие при выполнении сбора, обработки или хранении событий.

Решение

❖ Чтобы решить проблему:

1. На странице **События** в панели **Фильтры** выберите фильтр **Все события**. Если на странице отобразились ожидаемые события, рекомендуется проверить условия, используемые для фильтрации (см. документ Синтаксис языка запроса PDQL Ankey SIEM NG 5.2.3).
2. Убедитесь, что источники событий поддерживаются системой и правильно настроены (см. Руководство по интеграции с источниками Ankey SIEM NG 5.2.3).
3. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 5.2.3) и проверьте наличие в нем строк с параметрами PackCount и RawCount. Если такие строки отсутствуют, обратитесь в службу технической поддержки ООО «Газинформсервис».
4. На странице **Система** → **Мониторинг обработки событий** проверьте наличие входящего потока событий от источников. Если события отсутствуют, обратитесь в службу технической поддержки ООО «Газинформсервис».

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[17], приложив следующую информацию:

- предупреждения и ошибки (см. подраздел 24.1) системы автоматического мониторинга;
- файлы журналов задачи, от которой ожидается поступление данных;
- снимок экрана, содержащий страницу **Задачи** с запущенными задачами;
- информацию о статусе служб (см. пункт 24.24.3) Ankey SIEM NG Server;
- файлы журналов Ankey SIEM NG Server, Ankey SIEM NG ES и RabbitMQ;
- снимок экрана, содержащий страницу **Queues** веб-интерфейса RabbitMQ;
- HAR-файл с данными об открытии страницы **События**.

[17] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.15 Задача аудита не собирает сведения об активах

Возможные причины

Возможными причинами проблемы являются сбор сведений от неподдерживаемых источников, отсутствие необходимых для сканирования инфраструктуры прав, а также ошибки в работе модуля аудита.

Решение

❖ Чтобы решить проблему:

1. Проверьте, что версия сканируемого источника данных поддерживается системой (см. Руководство по интеграции с источниками Ankey SIEM NG 5.2.3). Если источник не поддерживается, система не сможет получать от него данные.
2. Убедитесь, что учетная запись для аудита имеет необходимые права доступа к источнику (см. Руководство по интеграции с источниками Ankey SIEM NG 5.2.3).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[17], приложив следующую информацию:

- файлы журналов задачи аудита, собранные с уровнем журналирования debug;
- название и версию источника;
- снимки экрана с данными о правах доступа и привилегиях учетной записи, используемой для аудита.

24.16 Не приходят уведомления, отправляемые по электронной почте

❖ Чтобы решить проблему:

1. Откройте файлы журналов Notifications.log и Triggers.log, расположенные на серверах Ankey SIEM NG MC Ankey SIEM NG Core соответственно.
   Если журналы содержат сообщения об ошибках (например, Can't send email to <Адрес электронной почты>. Reason: Failure sending mail.; Unable to connect to the remote server; No connection could be made because the target machine actively refused it), убедитесь, что значения параметров SmtpHost, SmtpPort, SmtpUser и SmtpPassword роли Core соответствуют значениям параметров для подключения к серверу электронной почты.
2. Если журналы содержат сообщения об отправке (например, Email ["Название задачи"] "Название события" was sent to "Адрес электронной почты"), обратитесь к системному администратору предприятия для проверки параметров сервера электронной почты и просмотра его журналов на наличие ошибок.

24.17 Ошибка "Sdk пакет <Номер версии> поврежден. Необходимо восстановление"

Ошибка может возникнуть во время обновления компонента Ankey SIEM NG Core.

Решение

❖ Чтобы решить проблему:

1. Перейдите в папку с дистрибутивом:
2. cd "/<Путь к файлам дистрибутива>/Ankey_SIEM_NG_<Номер версии>/03.App_Knowledge_Base/Roles/ kb_<Номер версии>.tar.gz"
3. Распакуйте архив:
   tar -xf kb_<Номер версии>.tar.gz
4. Скопируйте папку kb_<Номер версии>/data/resources/siemsdk/<Номер версии пакета> в папку /var/lib/deployed-roles/<Название приложения Knowledge Base>/<название экземпляра роли приложения Knowledge Base/data/resources/siemsdk/<Номер версии пакета>.
   Например:
   cp -r ./kb_<Номер версии>/data/resources/siemsdk/<Номер версии пакета> /var/lib/deployed-roles/kb-application-ankey/kb/data/resources
5. Распакуйте архив siemsdk-windows_<Номер версии>.tar.gz в папку <Номер версии пакета>.
6. Войдите в Knowledge Base.
7. В меню **SIEM** выберите пункт **Выбор версии SDK**.
8. На отрывшейся странице в центральной панели выберите последнюю версию SDK и нажмите кнопку **Восстановить**.

24.18 Не удается импортировать отчет из MaxPatrol 8

Возможные причины

Возможными причинами проблемы являются сбои при создании отчета в MaxPatrol 8 или при его обработке в Ankey SIEM NG.

Решение

❖ Чтобы решить проблему:

1. Убедитесь, что MaxPatrol 8 как источник событий правильно настроен (см. Руководство по интеграции с источниками Ankey SIEM NG 5.2.3).
2. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 5.2.3). Если в журнале есть строки с ошибками Failed to convert report scan.xml или mp_scan_converter.conversion_error.ConversionError: Errors in the hosts, произошел сбой при обработке данных отчета. Необходимо

обратиться в службу технической поддержки ООО «Газинформсервис»[18].

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[18], приложив следующую информацию:

- снимки экрана, содержащие параметры создания отчета в MaxPatrol 8;
- файлы журнала задачи по импорту данных отчета из MaxPatrol 8;
- файлы из папки not processed (находится в одной папке с файлом отчета);
- файл с консолидированными результатами сканирования, выполненного в MaxPatrol 8.

24.19 Настройка компонентов после изменения IP-адресов или FQDN их серверов

Для взаимодействия между собой компоненты системы используют IP-адреса или FQDN серверов, на которых они установлены. Эти сетевые параметры указываются администратором при установке компонента и сохраняются в его конфигурации. Если во время работы системы IP-адрес или FQDN сервера изменился, взаимодействие между компонентами нарушится, поскольку в конфигурации компонента будет храниться прежнее значение параметра. Для восстановления взаимодействия необходимо в качестве значений параметров компонентов указать актуальные IP-адреса или FQDN серверов.

Если был изменен IP-адрес или FQDN сервера компонентов Ankey SIEM NG Core, Ankey SIEM NG Management and Configuration и Knowledge Base, необходимо указать актуальные значения следующих параметров:

- HostAddress, KBAddress и MCAddress компонента Ankey SIEM NG Core;
- HostAddress, MCAddress и CoreAddress компонента Knowledge Base;
- HostAddress компонента Ankey SIEM NG Management and Configuration;
- CoreAddress и RMQHost компонента Ankey SIEM NG Server на Linux;
- RMQHost компонента Ankey SIEM NG Collector, установленного для отдельного сегмента сети.

Если был изменен IP-адрес или FQDN сервера Ankey SIEM NG ES, необходимо указать актуальные значения параметров SiemElasticsearchHost компонента Ankey SIEM NG Core и ElasticsearchHost компонента Ankey SIEM NG Server на Linux, а также выполнить команду dpkg-reconfigure siem-storage на сервере Ankey SIEM NG ES.

[18] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

Внимание! Если компоненты Ankey SIEM NG развернуты на нескольких площадках, перед сменой IP-адресов необходимо разорвать связи между площадками. После смены IP-адресов связи можно восстановить.

24.20 Подсеть Docker-контейнера Ankey SIEM NG совпадает с одной из подсетей предприятия

Решение

Необходимо изменить подсеть Docker-контейнера Ankey SIEM NG. Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

❖ Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленными ролями Ankey SIEM NG остановите Docker-контейнеры:
   docker stop $(docker ps -qa)
2. На всех серверах с установленными ролями Ankey SIEM NG удалите Docker-контейнеры:
   docker rm $(docker ps -qa)
3. На всех серверах с установленными ролями Ankey SIEM NG удалите действующие параметры сети Docker:
   docker network prune
4. На сервере с установленной ролью Deployer распакуйте архив <Название роли>_<Номер версии>.tar.gz из комплекта поставки.
5. На сервере с установленной ролью Deployer запустите сценарий:
   deployer_<Номер версии>/install.sh
6. В открывшемся окне нажмите кнопку **Yes**.
7. В открывшемся окне выберите вариант с идентификатором приложения роли.
8. В открывшемся окне выберите вариант с названием экземпляра роли.
   Откроется окно для выбора набора параметров.
9. Выберите вариант **Advanced configuration**.
   Откроется страница со списком параметров (см. приложение А).
10. В качестве значения параметра CustomDockerAddressPool укажите подсеть для Docker-контейнеров Ankey SIEM NG, отличную от подсетей, используемых в вашей организации.
11. В качестве значения параметра CustomDockerNetworkSize введите размер подсети, указанной в параметре CustomDockerAddressPool.
12. Нажмите кнопку **OK**.
13. В открывшемся окне нажмите кнопку **Submit**.
    Начнется изменение конфигурации роли. По его завершении появится сообщение Deployment configuration successfully applied.
14. Нажмите кнопку **OK**.
15. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

16. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов Ankey SIEM NG:
    /opt/deployer/bin/Restart-Configuration.ps1 '*' -Verbose
17. Подсеть Docker-контейнера изменена.
18. Вы можете проверить изменение подсети Docker-контейнера, выполнив команды вывода информации о сетевых интерфейсах:
    ip r
    ip a | grep docker
    iptables -L

24.20.1 Изменение подсети Docker-контейнера при обновлении компонентов

Возможна ситуация, когда изменить подсеть Docker-контейнера Ankey SIEM NG необходимо во время обновления компонентов Ankey SIEM NG. В этом случае необходимо воспользоваться инструкцией, приведенной ниже.

❖ Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленными ролями Ankey SIEM NG остановите Docker-контейнеры:
   docker stop $(docker ps -qa)
2. На всех серверах с установленными ролями Ankey SIEM NG удалите Docker-контейнеры:
   docker rm $(docker ps -qa)
3. На всех серверах с установленными ролями Ankey SIEM NG удалите действующие параметры сети Docker:
   docker network prune
4. На сервере с установленной ролью Deployer распакуйте архив deployer_<Номер версии>.tar.gz с новой версией роли:
   tar -xf deployer_<Номер версии>.tar.gz
5. Запустите сценарий:
   deployer_<Номер версии>/install.sh
6. В открывшемся окне нажмите кнопку **Yes.**
7. Начнется распаковка и подготовка пакетов. По завершении подготовки откроется окно для проверки и изменения параметров обновления.
8. Выберите вариант **Advanced configuration**.
9. Откроется страница со списком параметров (см. приложение А).
10. Убедитесь, что в качестве значения параметра HostAddress указан IP-адрес или FQDN сервера, на который установлена роль Deployer.
11. В качестве значения параметра CustomDockerAddressPool укажите подсеть для Docker-контейнеров Ankey SIEM NG, отличную от подсетей, используемых в вашей организации.
12. В качестве значения параметра CustomDockerNetworkSize введите размер подсети, указанной в параметре CustomDockerAddressPool.
13. Нажмите кнопку **ОК**.
14. Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
15. Нажмите кнопку **ОК**.

16. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
17. Обновите остальные роли согласно инструкциям в документе «Руководство по инсталляции Ankey SIEM NG (с компонентом VM)».
18. Подсеть Docker-контейнера изменена.
19. Вы можете проверить изменение подсети Docker-контейнера, выполнив команды вывода информации о сетевых интерфейсах:

```
ip r
ip a | grep docker
iptables -L
```

24.21 Диагностика коннекторов по сбору данных с источников событий

В этом подразделе приведены инструкции по диагностике и решению проблем, возникающих при получении поддерживаемого набора данных от источников событий в ПК Ankey SIEM NG. Шаги инструкции приведены в виде чек-листа, шаги необходимо выполнять в порядке их перечисления.

Общие условия применения коннекторов:

- пользователь ознакомлен с сопроводительной (эксплуатационной) документацией в части применения функциональных возможностей, а также приняты условия лицензионного соглашения;
- аппаратные характеристики оборудования соответствуют минимальным требованиям для эксплуатации;
- версия источника событий присутствует в списке поддерживаемых версий в документации на коннектор Ankey SIEM NG;
- окружение источника (версия ОС, версия СУБД) соответствует указанным в проектной документации;
- механизм сбора данных соответствует документации на коннектор Ankey SIEM NG;
- коннектор совместим с данной версией платформы ПК Ankey SIEM NG;
- в платформу ПК Ankey SIEM NG установлена актуальная версия[19] коннектора, совместимая с контентом;
- компонент Ankey SIEM NG Collector установлен и настроен для приема событий;
- настроено сетевое взаимодействие источника событий и ПК Ankey SIEM NG;
- журналирование событий источника корректно настроено (в соответствии с эксплуатационной документацией на

[19] Для определения версии установленного коннектора см. пункт 24.21.5, для определения версии пакета контента см. пункт 24.22.7.

источник), учтены требования, представленные в документации на коннектор и проектной документации;
– коннектор установлен в активную установочную базу, формулы нормализации, формулы обогащения и табличные списки (при наличии) включены.

24.21.1 Диагностика источника событий (журналирование данных)

В этом пункте приведены инструкции по диагностике и решению проблем, возникающих на стороне источников событий.

Для диагностики работы источника событий:

1. Убедиться, что источник событий функционирует корректно, в полном соответствии с эксплуатационной документацией на источник.

> **Примечание.** Описание проблемы отсутствия событий от источников представлено в подразделе 24.14.

2. Убедиться в корректности работы сетевого взаимодействия источника событий и сервера сбора событий Ankey SIEM NG Collector:
   – корректность маршрутизации сетевых пакетов;
   – доступность сетевых портов.
3. Убедиться, что источник событий регистрирует события в соответствии с эксплуатационной документацией, в журналах регистрации событий присутствуют новые события в поддерживаемом формате журналов для интеграции с ПК Ankey SIEM NG с учетом поддерживаемого состава обрабатываемых событий.

> **Примечание.** Если на стороне источника используются методы выгрузки и передачи журналируемых событий посредством Syslog/SNMP в адрес компонента Ankey SIEM NG Collector, то рекомендуется проверить, что такие события отправляются со стороны источника и поступают в программный комплекс[20].

4. Убедиться, что выполнены рекомендации[21] по настройке источника, включая настройки аудита источника (регистрации сведений в журнале событий):
   – для аудита источника на соответствие параметрам, указанным в документе «Руководство по настройке аудита активов Ankey SIEM NG (AM+VM+HCC) 5.2.3»;
   – для сбора событий стандартными коннекторами на соответствие параметрам, указанным в документе

[20] Например, через tcpdump и т.п.
[21] Указанные в документации на коннектор настройки носят рекомендательный характер. Итоговые настройки определяются особенностями проекта и представлены в проектной документации.

«Руководство по интеграции с источниками Ankey SIEM NG 5.2.3»;

– для сбора событий дополнительными коннекторами на соответствие параметрам, указанным в разделе 4 «Особенности сбора событий с источника» документации, поставляемой вместе с дополнительным коннектором.

5. Проверить версию источника, среду функционирования (окружение работы), формат событий и метод взаимодействия. Для корректного сбора событий версия источника, среда функционирования, формат событий и метод взаимодействия должны соответствовать сопроводительной документации на коннектор.

Внимание! Если данные параметры соответствуют параметрам, указанным в сопроводительной документации на коннектор[22], и при этом сбор событий не выполняется с заявленными функциональными возможностями, то необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[23].

Примечание. Результаты обработки событий должны соответствовать заявленным в сопроводительной документации, в противном случае корреляционные механизмы не могут гарантированно работать в штатном режиме.

6. В случае если настройки источника событий не соответствуют рекомендуемым, необходимо скорректировать конфигурацию источника событий, при необходимости с привлечением специалистов, осуществляющих техническую поддержку источника событий.

Внимание! Если настройки источника в отношении формата и состава регистрируемых данных источника (для поддерживаемых версии, окружения, типа сбора и протокола взаимодействия) соответствуют настройкам, указанным в сопроводительной документации на коннектор[22], и при этом сбор событий не выполняется с заявленными функциональными возможностями, то необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[23].

После выполнения диагностики источника событий перейти к диагностике работы ПК Ankey SIEM NG, представленной в пункте 24.21.2.

[22] Если данные параметры отличаются от рекомендуемых и поддерживаемых производителем, то необходимо оформить заявку на доработку, так как данный функционал отсутствует (не поддерживается) в используемой версии изделия. Подробнее см. раздел 25.

[23] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.21.2 Проверка функционирования ПК Ankey SIEM NG

Убедиться в корректности функционирования ПК Ankey SIEM NG.

❖ Для этого необходимо воспользоваться функцией контроля **Состояния системы**. Чтобы просмотреть параметры жизнеспособности и целостности системы и ее компонентов:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Ankey SIEM NG**.
   Откроется главная страница.
2. Нажмите на цветовой индикатор состояния Ankey SIEM NG в верхнем правом углу рабочей области. Подробнее см. подраздел 24.1.
   По нажатию на индикатор откроется список уведомлений о состоянии системы (подробнее см. документ «Руководство оператора Ankey SIEM NG»).

При наличии в окне с результатами мониторинга сообщений об ошибках, связанных с компонентами платформы, необходимо провести диагностику системы. Методика проведения диагностики функционирования ПК Ankey SIEM NG, типовые проблемы, а также возможные решения типовых проблем приведены в текущем разделе.

В случае если ПК Ankey SIEM NG функционирует корректно, переходите к пункту 24.21.3.

24.21.3 Диагностика работы коннектора

Для диагностики работы коннектора в ПК Ankey SIEM NG необходимо:

1. Убедитесь, что все зависимые ресурсы импортированы в систему и/или добавлены в набор установок. Для этого необходимо выполнить инструкции из подраздела 24.23.
2. Проверить наличие событий от источника в ПК Ankey SIEM NG в соответствии с подразделом 24.14.
3. Если в результате выполнения пункта 1 события от источника отсутствуют, необходимо проверить работу задачи на сбор событий. Для этого:
   - в главном меню нажмите и в раскрывшемся меню выберите пункт **Ankey SIEM NG**.
     Откроется главная страница;
   - выберите пункт меню **Сбор данных** → **Задачи**.
     Откроется окно с перечнем всех задач на сбор событий;
   - в списке задач выберите необходимую задачу по сбору событий с интересующего источника;
   - проверьте статус выполнения задачи, для корректной работы сбора событий задача должна иметь статус **Выполняется**, как показано на рисунке 24.1.



Рисунок 24.1 – Статус задачи

Примечание. Если задача имеет статус **Завершена**, значит в ходе выполнения задачи сбора событий возникла ошибка, необходимо проверить параметры задачи, параметры профиля и журнал выполнения задачи.

- проверьте параметры задачи на соответствие параметрам, указанным в документации:
- для стандартных коннекторов на соответствие параметрам, указанным в документе «Руководство по интеграции с источниками Ankey SIEM NG 5.2.3»;
- для дополнительных коннекторов на соответствие параметрам, указанным в документации, поставляемой вместе с дополнительным коннектором.
- выполните инструкции из подраздела 24.13.

4. Проверить корректность настроек профиля сбора событий с источника, для этого:
   - в главном меню нажмите и в раскрывшемся меню выберите пункт **Ankey SIEM NG**.
     Откроется главная страница;
   - выберите пункт меню **Сбор данных** → **Профили**. Откроется окно с перечнем созданных профилей сбора;
   - в списке профилей выберите профиль сбора для интересующего источника;
   - проверьте параметры профиля сбора на соответствие параметрам, указанным в документации[24]:
   - для стандартных коннекторов на соответствие параметрам, указанным в документе «Руководство по интеграции с источниками Ankey SIEM NG 5.2.3»;
   - для дополнительных коннекторов на соответствие параметрам, указанным в документации, поставляемой вместе с дополнительным коннектором.
   - в том числе проверьте параметры учетной записи (при активном сборе), сетевые настройки: порт, транспорт (см. рисунок 24.2), указанный справочник на языке python для профилей на базе Custom Event Collector (см. рисунок 24.3);

[24] Указанные в документации на коннектор настройки носят рекомендательный характер. Итоговые настройки определяются особенностями проекта и приведены в проектной документации.

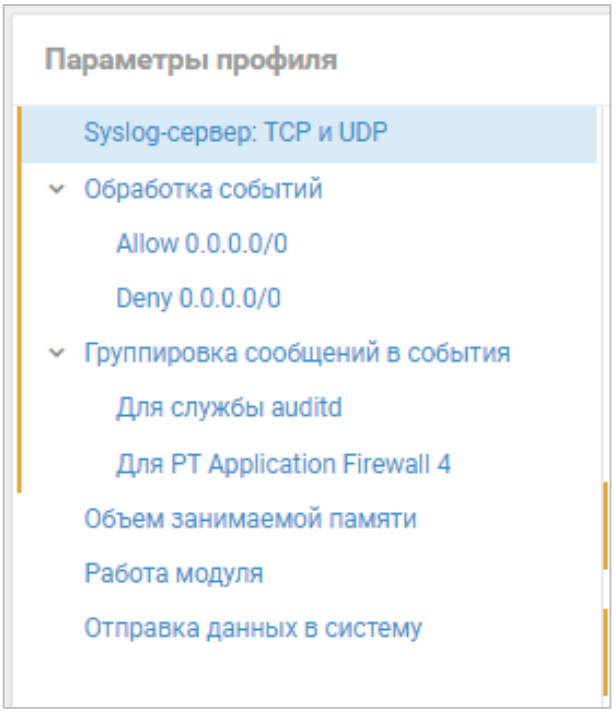


Рисунок 24.2 – Сетевые настройки

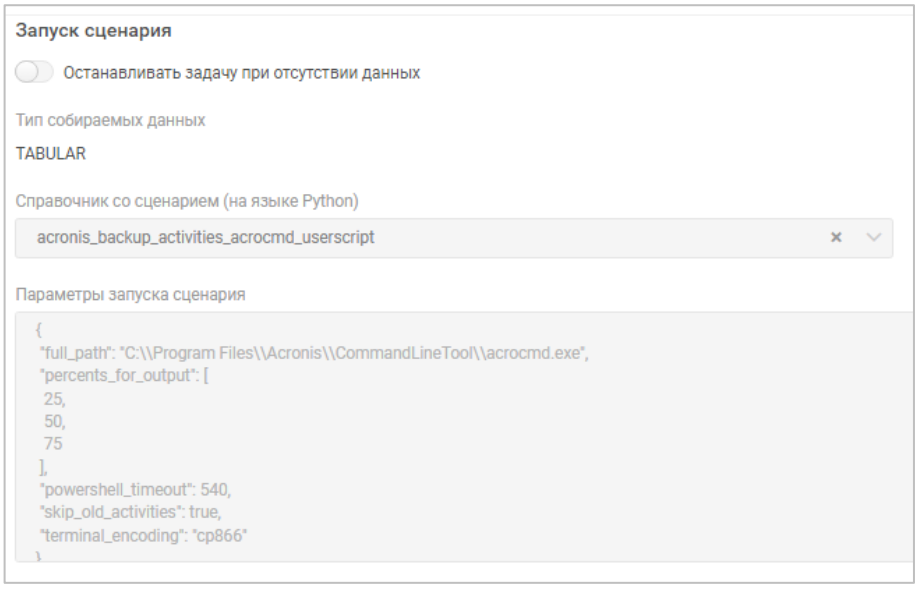


Рисунок 24.3 − Справочник со сценарием

5. Проверить журнал выполнения задачи на сбор событий, выполнив экспорт журнал.
   Экспортировать журнал работы задачи. Для этого:
   - в главном меню нажмите ⋮⋮⋮ и в раскрывшемся меню выберите пункт **Ankey SIEM NG**.
     Откроется главная страница;
   - в главном меню в разделе **Сбор данных** выберите пункт **Задачи**;
   - выберите задачу и нажмите **История запусков**;

– нажмите **Скачать журнал**, как показано на рисунке 24.4;

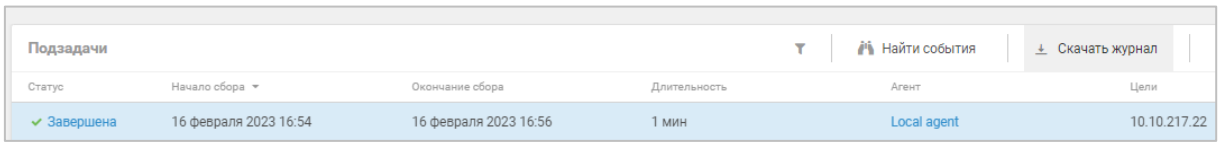


Рисунок 24.4 − Журнал событий

– откройте экспортированный zip-архив;
– откройте текстовый файл с журналом выполнения задачи;
– проанализируйте содержание журнала на предмет наличия ошибок в ходе выполнения задачи сбора событий, подробнее см. подраздел 24.13;
– при наличии ошибок в работе задачи, применить корректирующие мероприятия. Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»[25].

Дополнительные рекомендации:

Если события поступают в ПК Ankey SIEM NG, а также формат события, протокол взаимодействия, версия источника и среда функционирования (рабочее окружение) поддерживаются коннектором, но нормализация событий не осуществляется, необходимо свериться с таблицей «Перечень регистрируемых событий» документации, поставляемой вместе с коннектором:

– если событие присутствует в таблице «Перечень регистрируемых событий» документации, поставляемой вместе с коннектором, то необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»;
– если событие отсутствует в таблице «Перечень регистрируемых событий» и необходимо добавить событие в обработку ПК Ankey SIEM NG, то необходимо оформить заявку на доработку, так как данный функционал отсутствует (не поддерживается) в используемой версии изделия. Подробнее см. раздел 25.

24.21.4 Включение расширенного режима логирования (debug-режим)

Для дополнительных и стандартных коннекторов, поставляемых с ПК Ankey SIEM NG, возможно активировать расширенный режим логирования (debug-режим). Данный функционал позволяет отследить ошибки при подключении к источнику.

❖ Для активации debug-режима (кроме модуля CEC):

1. В главном меню нажмите и в раскрывшемся меню выберите приложение Ankey SIEM NG.
2. Перейдите на вкладку **Справочники** раздела **Сбор данных**.

[25] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

3. В списке **Все справочники** выберите справочник **logging_settings**.
4. Сделайте копию справочника, нажав кнопку **Копировать**.
5. В редактируемом поле найдите требуемый модуль сбора <<название модуля> level="INFO"/> и замените для него значение INFO на DEBUG.
   Например, <FileMonitor level="DEBUG">.
6. Нажмите кнопку **Сохранить**.
7. Перейдите на вкладку **Профили** раздела **Сбор данных**.
8. Выберите профиль, для которого необходимо активировать расширенный режим логирования, и нажмите **Создать → На базе выбранного профиля**.
9. Активируйте параметр **Показывать дополнительные параметры**.
10. Перейти на вкладку **Работа модуля**.
11. В выпадающем списке **Справочник с параметрами журналирования** выберите созданный ранее справочник.
12. Нажмите кнопку **Сохранить**.

Для коннекторов на базе модуля Custom Event Collector (CEC) реализована возможность активировать расширенный режим логирования при создании профиля сбора.

❖ Для включения debug-режима на базе модуля CEC при создании профиля сбора:

1. В меню приложения Ankey SIEM NG перейдите на вкладку **Профили** раздела **Сбор данных**.
2. В списке **Все профили → По типу профиля** выберите **CustomEventCollector**.
3. В списке **Список профилей** выберите требуемый профиль.
4. Нажмите **Создать → На базе выбранного профиля**.
5. Перейдите на вкладку **Запуск сценария**.
6. В поле **Параметры запуска сценария** добавьте параметр "debug":"true". Пример включения debug-режима представлен на рисунке 24.5.

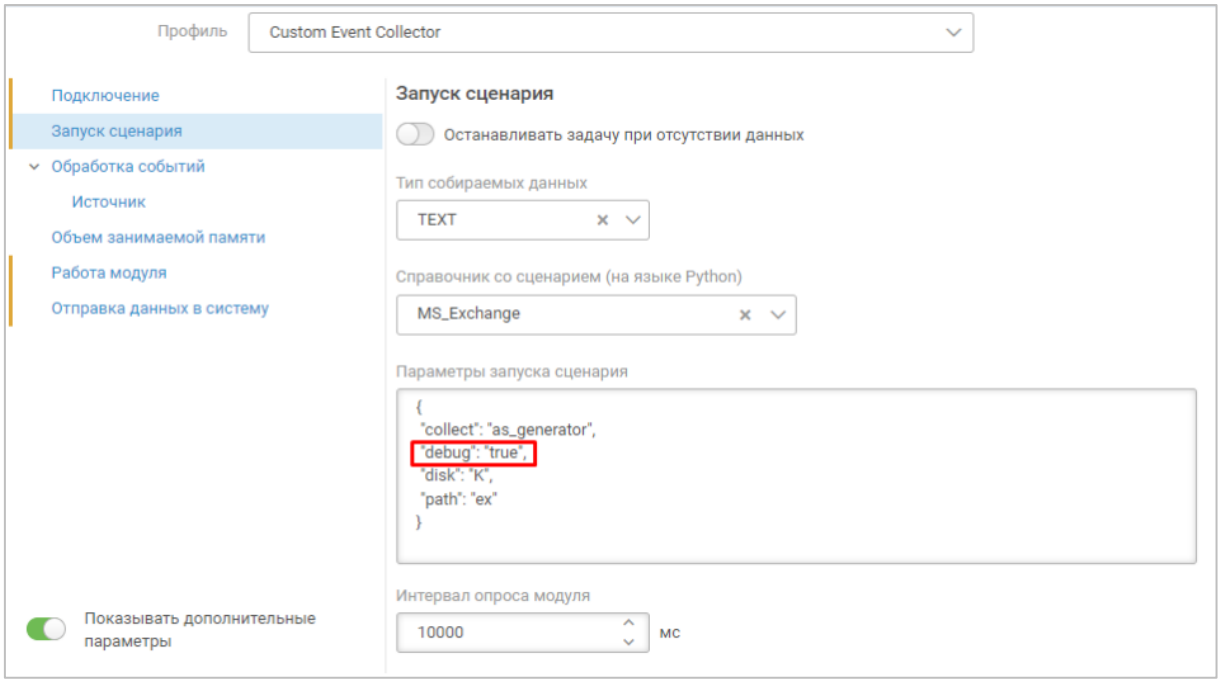


Рисунок 24.5 – Параметр включения Debug-режима

24.21.5 Версия дополнительного коннектора

Перед обращением в службу технической поддержки ООО «Газинформсервис» необходимо найти версию коннектора.

❖ Чтобы посмотреть версию дополнительного коннектора:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт Knowledge Base.
   Откроется веб-интерфейс Ankey SIEM NG Knowledge Base на странице **Статистика**.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите **Пакет дополнительных коннекторов** → **<Тип источника>** → **<Вендор источника>** → **<Наименование источника>** и откройте правило нормализации **INFO_Gazinformservice_<Наименование источника>**, как показано на рисунке 24.6.

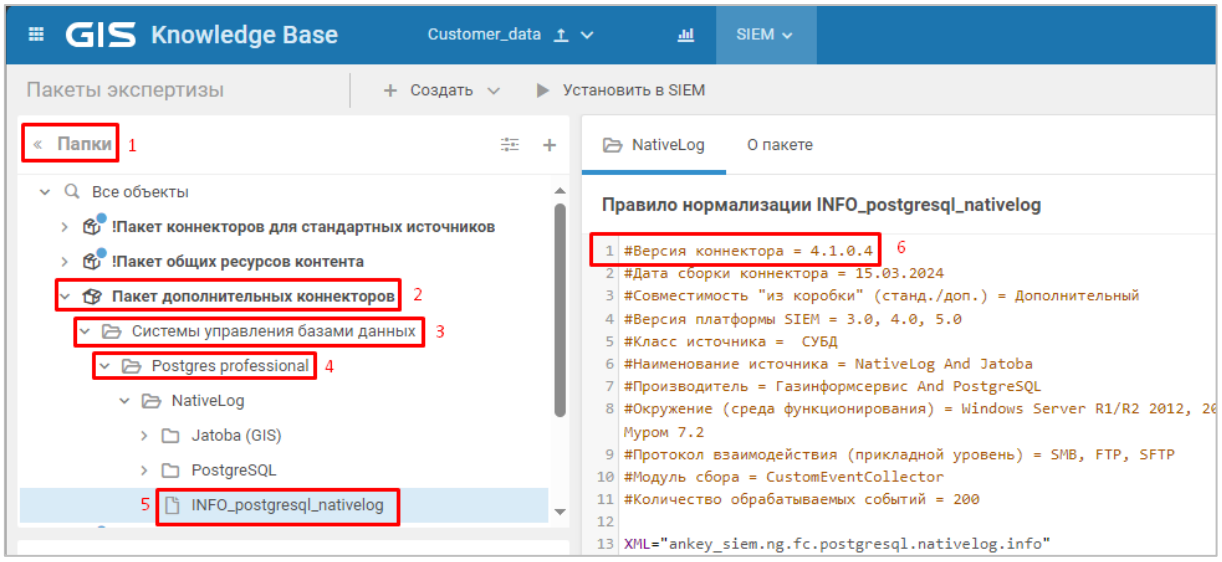


Рисунок 24.6 – Просмотр версии дополнительного коннектора в веб-интерфейсе

Номер версии коннектора будет указан в коде правила нормализации в комментарии #Версия коннектора =V<A.B.C>.

24.22 Диагностика пакетов контента

В этом подразделе приведены инструкции по диагностике и решению проблем, возникающих при работе ресурсов пакетов контента[26] в ПК Ankey SIEM NG.

Внимание! Механизмы корреляции взаимосвязаны с результатами нормализации событий от источников, поэтому рекомендуется использовать наиболее актуальные поддерживаемые версии коннекторов.

С целью штатной работы механизмов корреляции необходимо установить правила в составе пакетов контента в ПК Ankey SIEM NG. После инсталляции требуется провести настройку настраиваемых параметров, после чего перевести правила в активный режим (включить для работы в режиме «реального» времени).

Подробная схема этапов диагностики правил корреляции представлена в Приложении Д.

Общие условия применения пакетов контента:

- пользователь ознакомлен с сопроводительной (эксплуатационной) документацией в части применения функциональных возможностей, а также приняты условия лицензионного соглашения;
- аппаратные характеристики оборудования соответствуют минимальным требованиям для эксплуатации;
- пакет контента совместим с данной версией платформы ПК Ankey SIEM NG;

[26] Ключевой ресурс пакета контента – сигнатуры нарушений ИБ (корреляционные правила).

- журналирование событий источника корректно настроено (в соответствии с эксплуатационной документацией на источник), учтены требования, представленные в документации на коннектор и проектной документации;
- установленные версии коннекторов поддерживаются используемыми версиями пакетов контента (рекомендуется использовать самые актуальные версии коннекторов и контента);
- выполнены настройки пакетов контента в соответствии с сопроводительной документацией (заполнены табличные списки конфигурации и табличный список исключений, исходя из особенностей эксплуатации);
- ресурсы провалидированы и установлены в SIEM.

24.22.1 Начальная проверка правила корреляции

В данном пункте описывается проверка статуса правил корреляции и установка, а также наличие событий в системе.

24.22.1.1 *Проверка статуса правила*

❖ Для того чтобы проверить, что правило корреляции установлено в системе необходимо:

1. Перейти на вкладку **Knowledge Base** → **SIEM** → **Пакет экспертизы**.
4. Выбрать необходимую папку (рисунок 24.7) или правило (рисунок 24.8) и посмотреть на **Статус установки** :
   - если **Установлен**, то правило установлено в систему;
   - если **Установлен, не актуален**, то в системе установлена не последняя версия правила и рекомендуется переустановить правило в системе;
   - если **Не установлен**, то правило не установлено в систему.

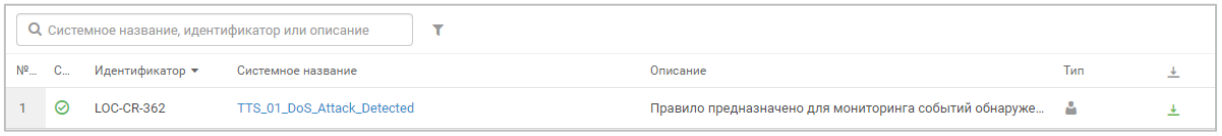


Рисунок 24.7 – Статус установки в перечне правил

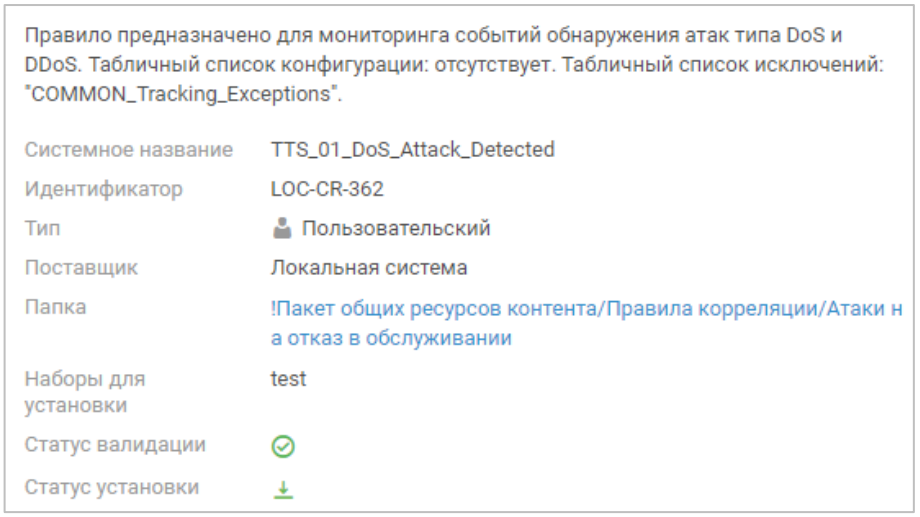


Рисунок 24.8 – Статус установки в описании правила

Возможные проблемы и их решение:

- не выбран набор для установки, либо не добавлено правило в набор для установки (см. пункт 1);
- выбранная база данных не является установочной (см. пункт 2);
- статус установки **Не установлен** (см. пункт 3).

❖ Если иконки **Статуса установки** нет (рисунки 24.9 и 24.10), то возможны варианты:

1. Не выбран нужный набор для установки, либо не добавлено правило в набор для установки.

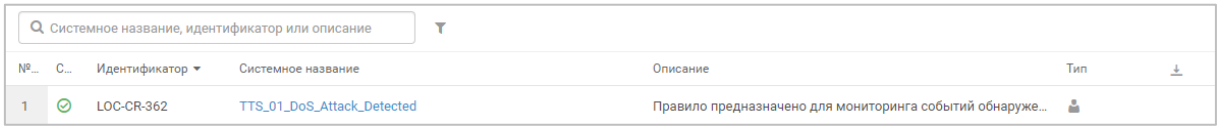


Рисунок 24.9 – Отсутствие значка статуса установки в папке с ресурсами

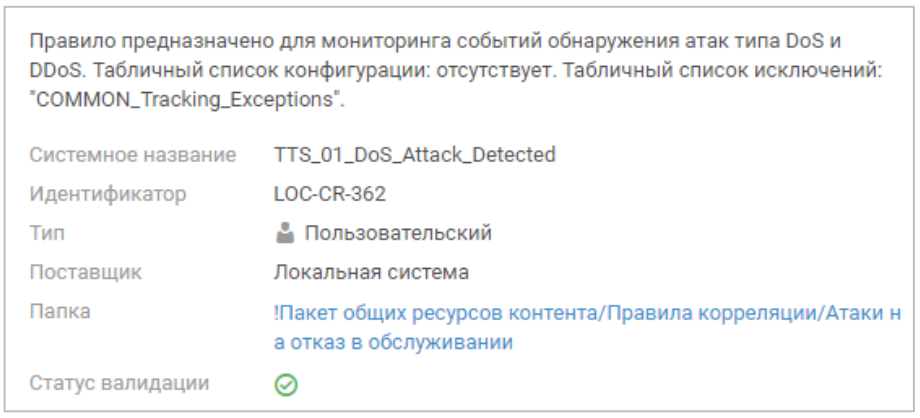


Рисунок 24.10 – Отсутствие значка статуса установки в описании правила

Для того чтобы проверить наличие правила в наборе для установки, можно либо выбрать правило и нажать на

кнопку **Наборы для установки** (на рисунке 24.11 представлено, как будет выглядеть правило без набора для установки), либо открыть само правило и посмотреть справа на сводную информацию о правиле (в случае, если правило вне установочного набора, поле будет отсутствовать), представлено на рисунке 24.12.

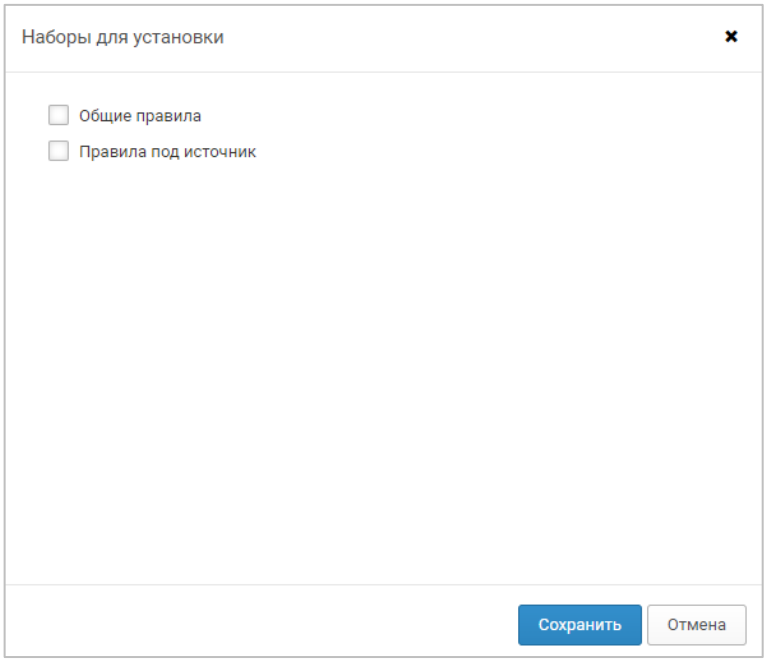


Рисунок 24.11 – Выбор набора для установки

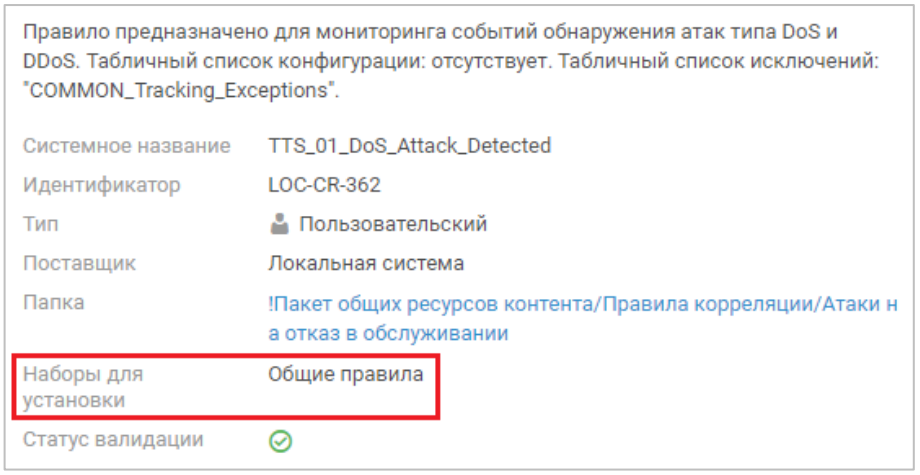


Рисунок 24.12 – Набор для установки в описании правила

Внимание! При создании набора для установки необходимо выбрать требуемый конвейер (рисунок 24.13), иначе при установке появится ошибка, как показано на рисунке 24.14. Создание и редактирование наборов для установки описано в разделе «Работа с наборами для установки» документа «Руководство оператора Ankey SIEM NG».

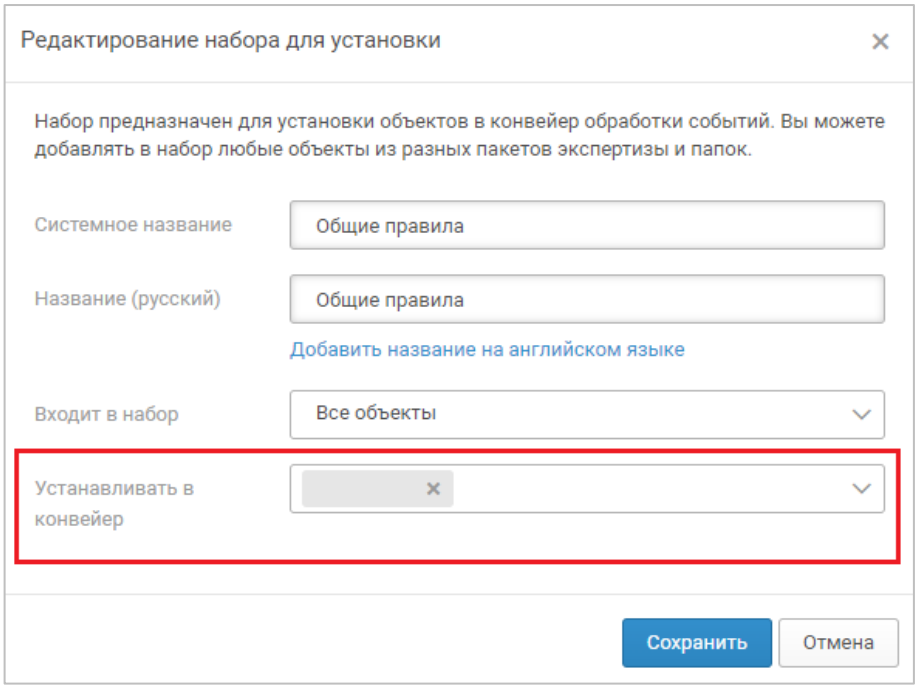


Рисунок 24.13 – Выбор конвейера для установки ресурсов

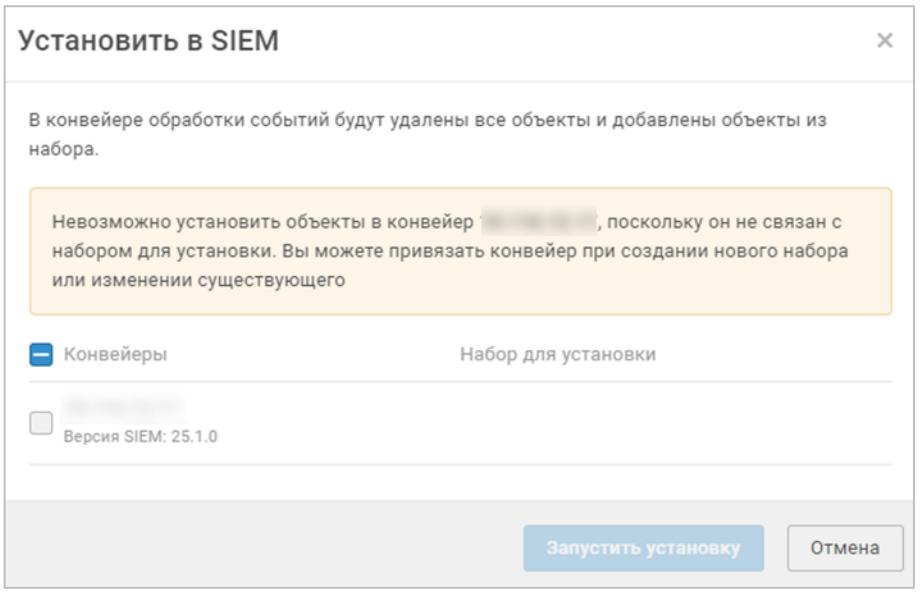


Рисунок 24.14 – Ошибка при отсутствии привязки конвейера к набору для установки

Если у набора для установки выбран конвейер, то рядом с ним будет иконка (аналогичная иконка будет и у правила), как показано на рисунке 24.15.

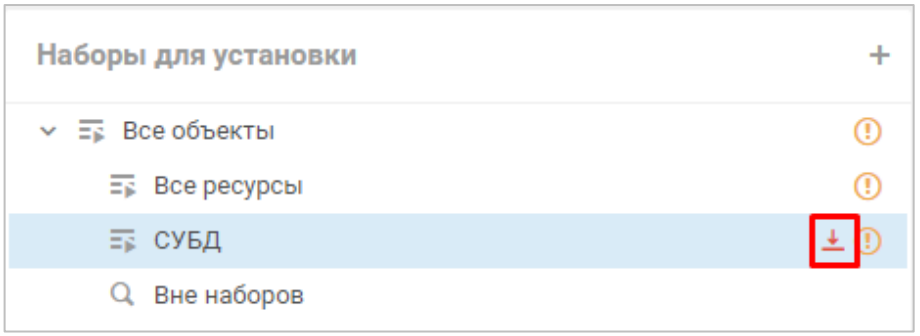


Рисунок 24.15 – Иконка установки у набора

Внимание! Необходимо в набор для установки добавлять все зависимые ресурсы, иначе установка выполнится с ошибкой (рисунок 24.16), пример представлен на рисунке 24.17.

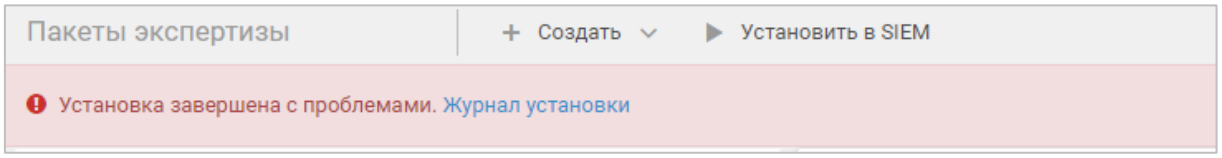


Рисунок 24.16 – Сообщение об ошибке установки

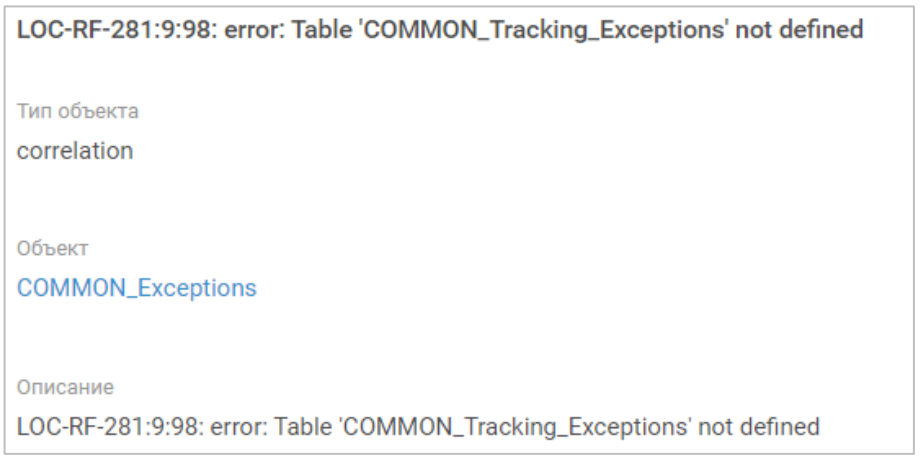


Рисунок 24.17 – Описание ошибки установки при отсутствии ресурсов

2. Выбранная база данных не является установочной, нет иконки у названия БД, нет кнопки **Установить в SIEM**.
   Для решения данной проблемы необходимо:
   - в главном меню нажать и в раскрывшемся меню выбрать пункт **Knowledge Base**.
   - в главном меню в разделе **<Название БД>** выбрать пункт **Базы данных**.
   - в панели **Базы данных** выбрать необходимую базу данных и нажать на **Сделать установочной**, согласиться с предупреждением.

3. Если имеется иконка **Статуса установки** (не установлен в систему), то необходимо установить правило в систему.
Для этого выберите необходимый набор для установки, нажмите **Установить в SIEM**.

Возможные проблемы и их решение:

- не выбран набор для установки или правило не добавлено в набор для установки (см. пункт 1);
- у набора для установок не выбран конвейер (см. пункт 2);
- не все зависимые ресурсы импортированы в систему и/или добавлены в набор установок (см. пункт 3).

❖ Если при нажатии на кнопку **Установить в SIEM** возникает ошибка, которая указана на рисунке 24.18, то:

1. Либо не выбран нужный набор для установки, либо не добавлено правило в набор для установки. Для решения этой проблемы обратитесь к пункту 1 «Не выбран нужный набор для установки».

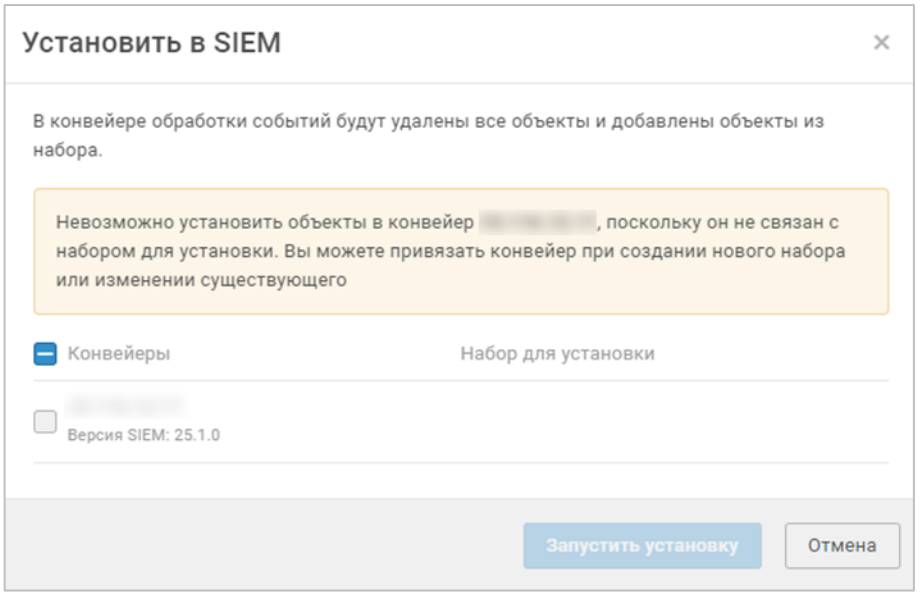


Рисунок 24.18 – Ошибка установки

2. В случае, если правило добавлено в набор для установки, а ошибка сохраняется, убедитесь, что у набора для установок выбран конвейер (см. предыдущий пункт).
3. При установке появляется ошибка зависимостей ресурсов (рисунок 24.19).

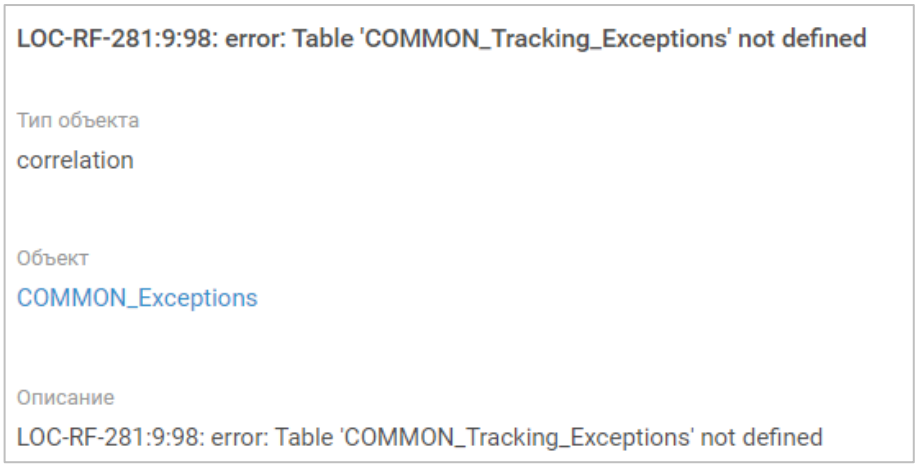


Рисунок 24.19 – Ошибка зависимостей

Убедитесь, что все зависимые ресурсы импортированы в систему и/или добавлены в набор установок. Для этого необходимо выполнить инструкции из подраздела 24.23.

24.22.1.2 *Проверка состояния правила*

Для того чтобы проверить, что правило корреляции включено в системе, необходимо перейти на вкладку **Ankey SIEM NG** → **Сбор данных** → **Правила корреляции** и либо посмотреть на значок в таблице (рисунок 24.20), либо выбрав конкретное правило (рисунок 24.21).

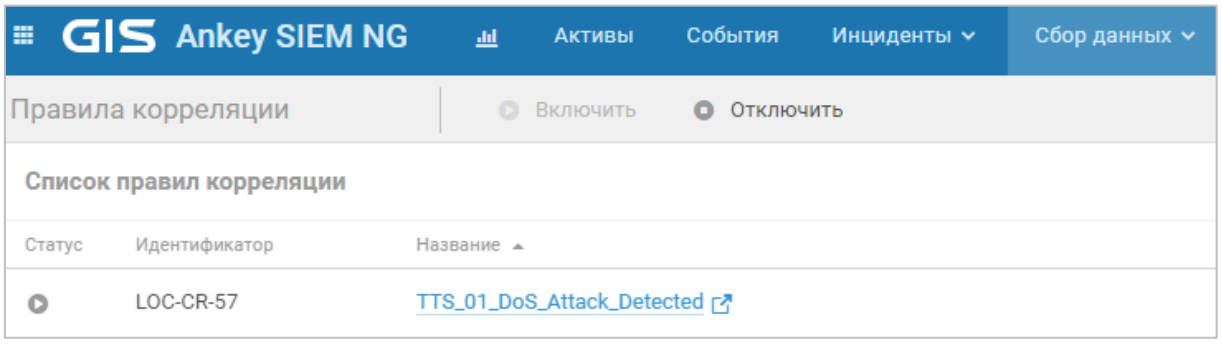


Рисунок 24.20 – Статус правила в списке правил

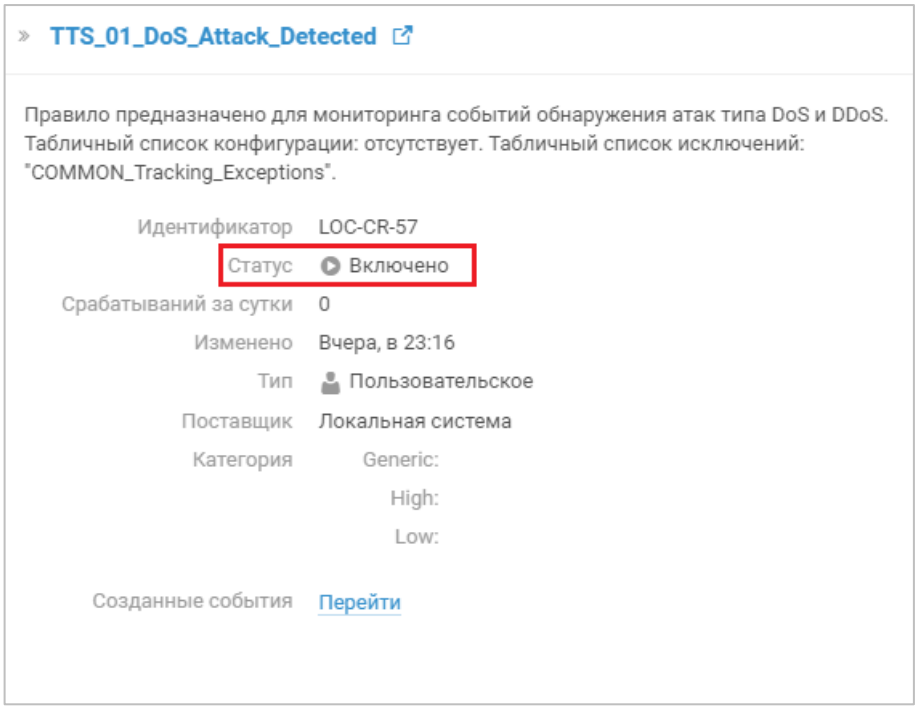


Рисунок 24.21 – Статус правила в описании

Основные статусы правил представлены в таблице 24.2.

Таблица 24.2 – Основные статусы правил

Статус	Описание
	Включено
	Отключается, Включается
	Отключено
	Правило автоматически остановлено на основании результатов мониторинга работы правил корреляции. Подробнее см. пункт 2
	Ошибка валидации

Возможные проблемы и их решение:

– правило выключено вручную (см. пункт 1);
– правило выключено автоматически (см. пункт 2).

❖ Правило может быть выключено как вручную, так и автоматически:

1. Если правило выключено вручную, то необходимо его просто включить, нажав на кнопку **Включить**, как показано на рисунке 24.22.

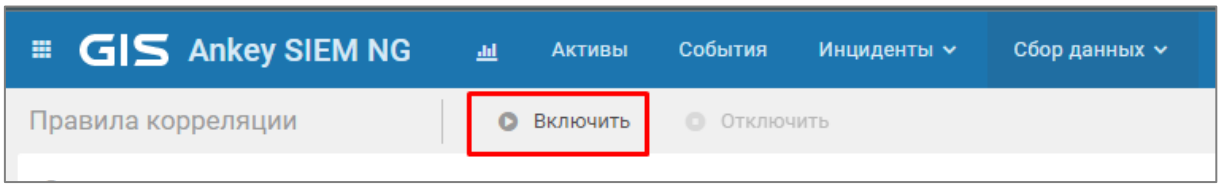


Рисунок 24.22 – Включение правила

2. Если же правило выключено автоматически, то прежде чем его включать необходимо разобраться с причинами его выключения. Правило может выключаться автоматически при большом количестве срабатываний или же при превышении объема оперативной памяти (более 95%), выделенной для работ правил корреляции (настройка данных параметров описана ниже).
   Если же правило выключено автоматически, но Администратор считает, что механизм автоматического выключения работает некорректно. То имеется возможность изменить значения по умолчанию по количеству срабатываний правил корреляции и объему оперативной памяти, занимаемой правилами корреляции.

❖ Для изменения параметров настроек вручную нужно использовать утилиту install.sh (*Ankey SIEM NG Server установлен на Linux*):

1. Запустить утилиту конфигурирования:
   cd <путь в каталог, где находится скрипт install.sh>
   ./install.sh
2. На открывшейся странице выбрать приложение с помощью стрелок, текущий Ankey SIEM NG, и нажать **Enter**, как показано на рисунке 24.23.

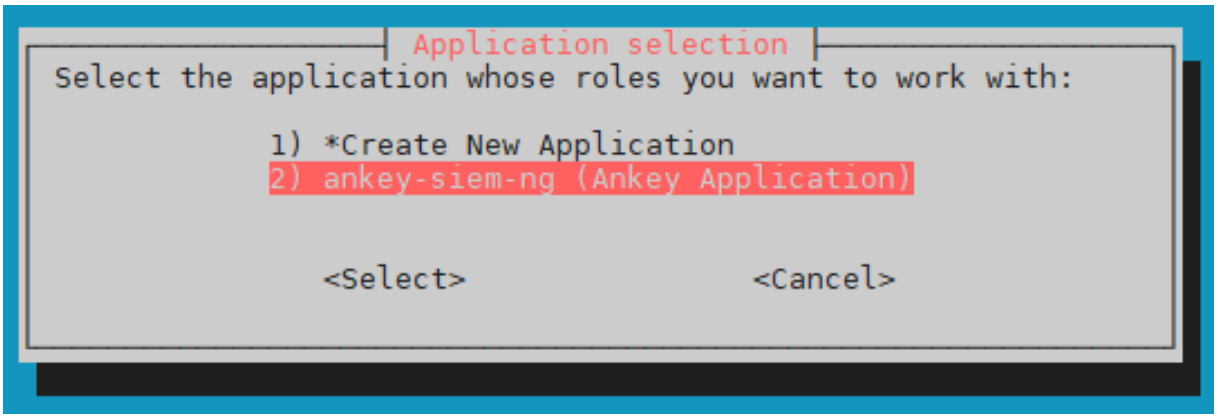


Рисунок 24.23 – Выбор приложения

3. В открывшемся окне выбрать с помощью стрелок необходимый экземпляр (Instance) и нажать **Enter**, как показано на рисунке 24.24.

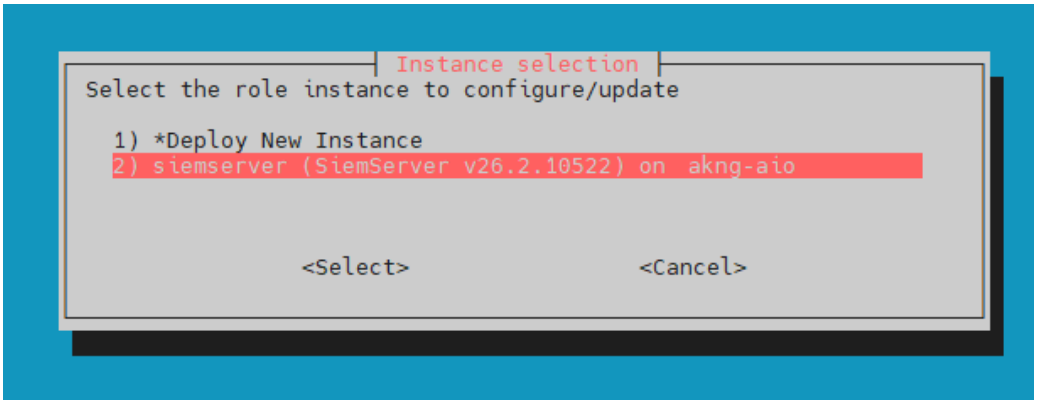


Рисунок 24.24 – Выбор экземпляра (Instance)

4. На открывшейся странице выбрать параметр **Advanced configuration** и нажать **Enter**, как показано на рисунке 24.25.

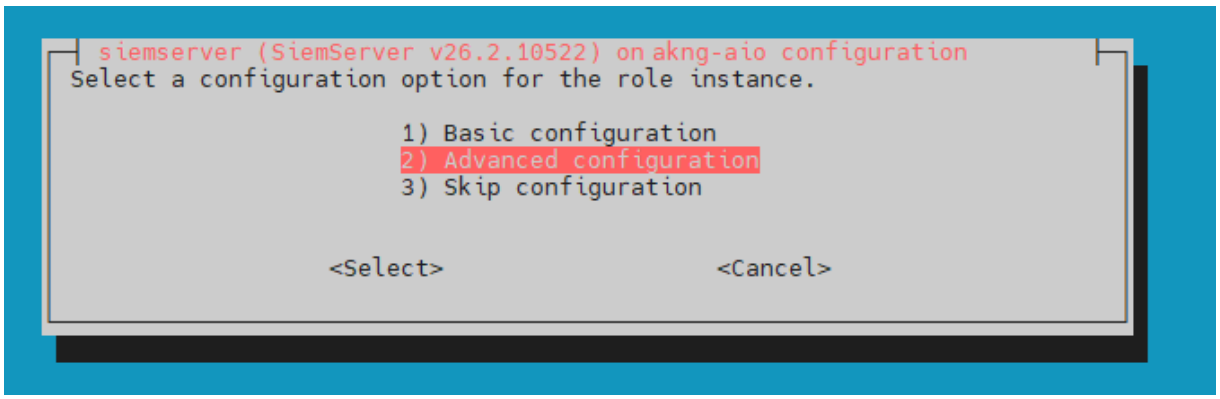


Рисунок 24.25 – Выбор типа настроек

5. В открывшемся перечне настроек внести требуемые изменения в параметры, указанные в таблице 24.3, как показано на рисунке 24.26.

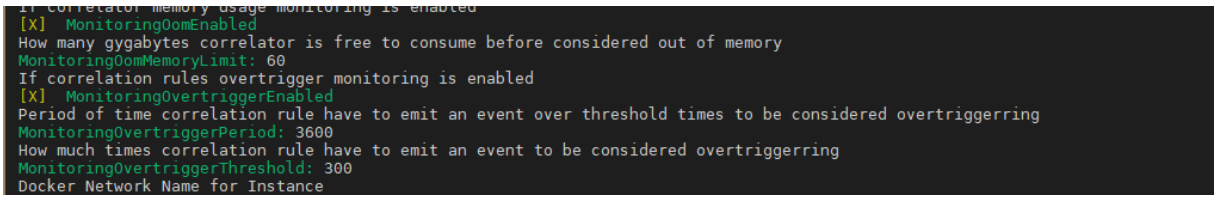


Рисунок 24.26 – Перечень настроек

Примечание. Для проставления или убирания флажка нажмите пробел у соответствующего параметра.

6. После изменения всех необходимых параметров прокрутите список настроек вниз, выберите **OK** и нажмите **Enter**, как показано на рисунке 24.27.



Рисунок 24.27 – Выход из настроек

7. Будет выполнена реконфигурация настроек (рисунок 24.28).

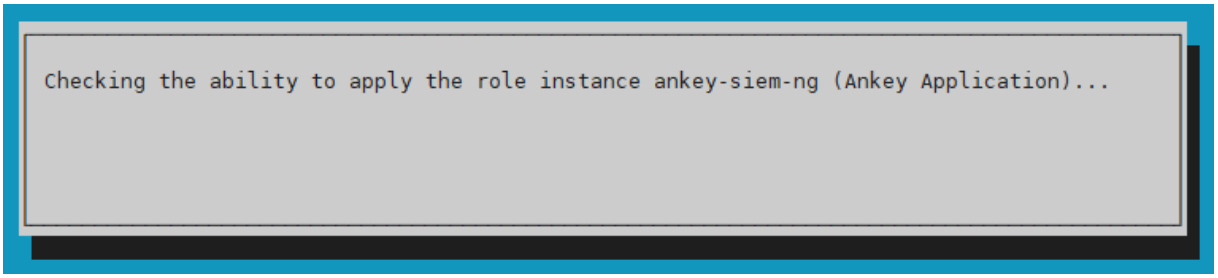


Рисунок 24.28 – Применение настроек

8. После успешного выполнения операции появится информационное окно, в котором необходимо нажать **ОК**, как показано на рисунке 24.29.



Рисунок 24.29 – Сообщение об успешной перенастройке

Таблица 24.3 – Параметры конфигурации

Параметр	Описание	По умолчанию
ProtectedRulesPath	Для включения правил в список исключений необходимо добавить их системные названия в текстовый файл (каждое название в отдельной строке) и указать путь к файлу в качестве значения параметра ProtectedRulesPath. Система не приостанавливает работу этих правил, если они срабатывают слишком часто, и приостанавливает их работу в последнюю очередь, когда освобождает выделенную для работы правил оперативную память	-
MonitoringOomMemoryLimit	Изменяет объем оперативной памяти, выделенной для работы правил корреляции (в ГБ)	60

Параметр	Описание	По умолчанию
MonitoringOomEnabled	Отключение отслеживания объема оперативной памяти, занимаемой правилами (по умолчанию флажок установлен)	Флажок установлен
MonitoringOvertriggerPeriod	Изменение периода для подсчета количества срабатываний правил корреляции (в секундах)	3600
MonitoringOvertriggerThreshold	Максимальное количество срабатываний за установленный период, которое не приведет к остановке правила	300
MonitoringOvertriggerEnabled	Полностью отключить отслеживание количества срабатываний для всех правил	Флажок установлен

Примечание. Настоятельно не рекомендуется отключать отслеживание объема оперативной памяти, занимаемой правилами, а также количества срабатываний для всех правил, так как тем самым выключаются механизмы самозащиты системы, что может привести к полной неработоспособности программного комплекса при высоких нагрузках.

24.22.1.3 *Проверка наличия событий*

Для того, чтобы правило срабатывало в режиме «реального времени», должен быть поток событий от источника[27]. Для проверки наличия событий необходимо перейти на вкладку **Ankey SIEM NG → События**.

Проверка наличия событий от источника описана в подразделе 24.14.

Внимание! Подробное описание диагностики коннекторов и источников событий представлено в подразделе 24.20.

Возможные проблемы и их решение:

❖ Вы открыли таблицу событий и обнаружили, что в нем есть только необработанные события (рисунок 24.30):

[27] Рекомендуется использовать наиболее актуальную версию коннектора для работы с правилами и убедиться в совместимости пакета контента с коннектором.

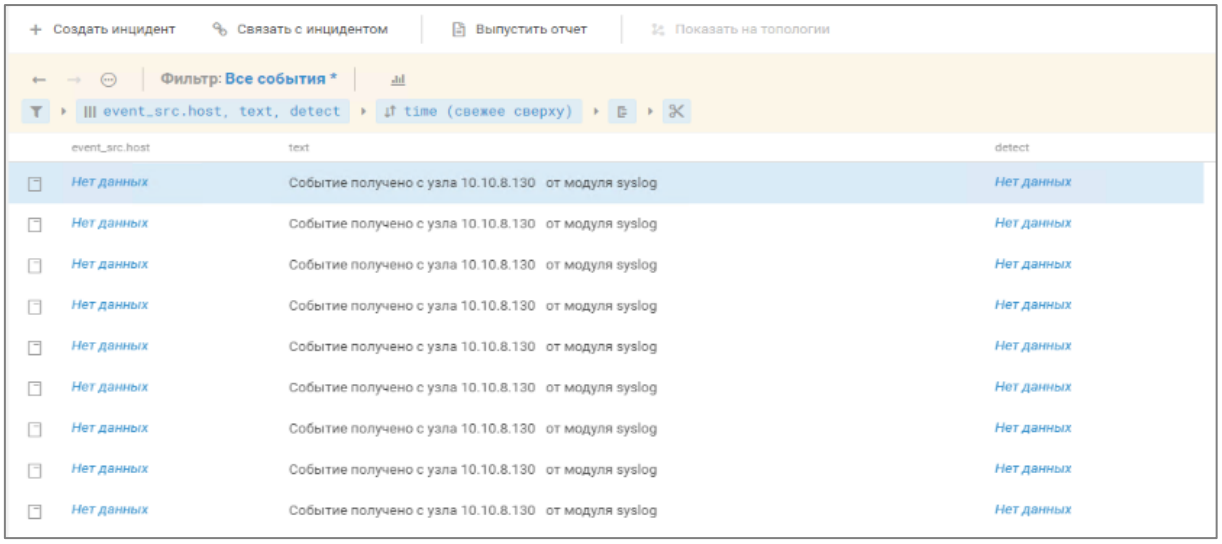


Рисунок 24.30 – Необработанные события

1. Проверьте, установлен ли коннектор в системе, если установлен, то убедитесь, что настроили источник по инструкции, если все верно, но события все равно не обрабатываются, обратитесь в службу технической поддержки ООО «Газинформсервис»[28].

❖ Вы открыли таблицу событий, а она пуста (рисунок 24.31):

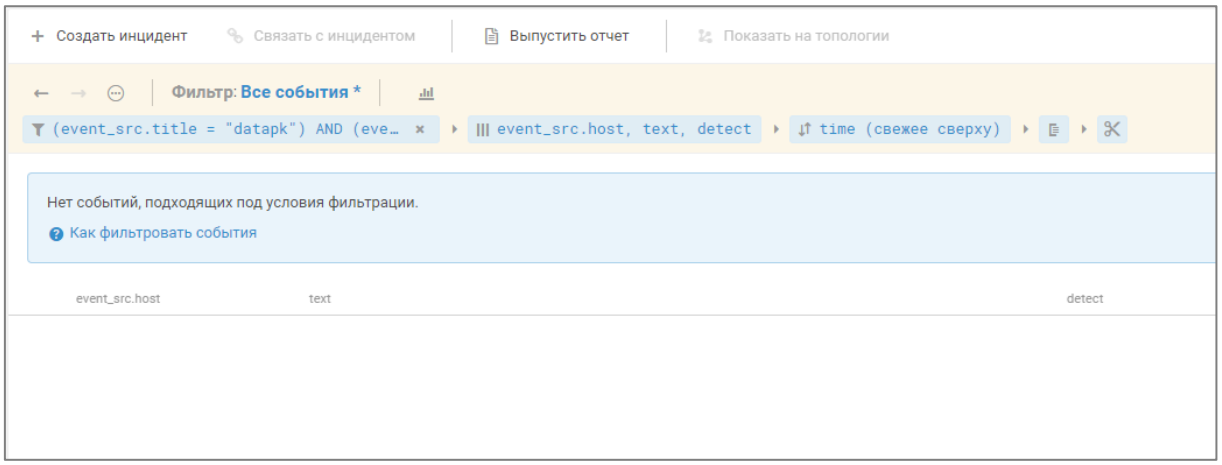


Рисунок 24.31 – Отсутствие событий от источника

1. Убедитесь, что правильно написали условие в фильтре для источника.
2. Проверить работу задачи на сбор событий в соответствии с пунктом 24.21.3.

Примечание. Если Вы убедились, что все настроено корректно, а событий все еще нет, то обратитесь в службу технической поддержки ООО «Газинформсервис»[28].

[28] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.22.2 Проверка корректности обработки события

В данном пункте описывается проверка корректности обработки событий.

24.22.2.1 *Проверка фильтра правила*

Для проверки того, что событие попадает под условие правила можно воспользоваться таблицей с событиями, при этом уточнив запрос условием из правила. Для получения информации об условии срабатывания правила необходимо перейти на вкладку **Knowledge Base → SIEM → Пакет экспертизы**, выбрать интересующее правило, нажав на него, и посмотреть затем на инструкцию filter директивы event (рисунок 24.32). Если после уточнения запроса в таблице событий есть интересующее событие, то перейти к подпункту 24.22.2.3, если нет, то перейти к подпункту 24.22.2.2.



Рисунок 24.32 – Правило. Директива event, инструкция filter

Примечание. В коде правил могут встречаться вложенные условия в виде макросов. Для просмотра информации по макросам перейдите на вкладку **Knowledge Base → SIEM → Макросы** и с помощью поиска найдите требуемый ресурс. Информация о макросе и его коде будет отображаться с правой стороны.

24.22.2.2 *Проверка маппинга событий*

Если в таблице событий после уточнения запроса (фильтр по условию правила) требуемое событие не появилось, то необходимо дополнительно к открытому условию правила открыть таблицу с нужным событием от источника (подходящим под правило корреляции по смыслу) и посмотреть на его маппинг (рисунок 24.33). При этом необходимо сравнить каждое поле из условия правила с каждым полем в событии.

В связи с тем, что на предыдущем шаге событие не было обнаружено, то полного соответствия по условию быть не может, необходимо найти поле, в которое записана другая информация и/или не хватает данных. Если же маппинг полностью совпадает с правилом, то посмотрите на правильность запроса в таблице событий (фильтр, время).

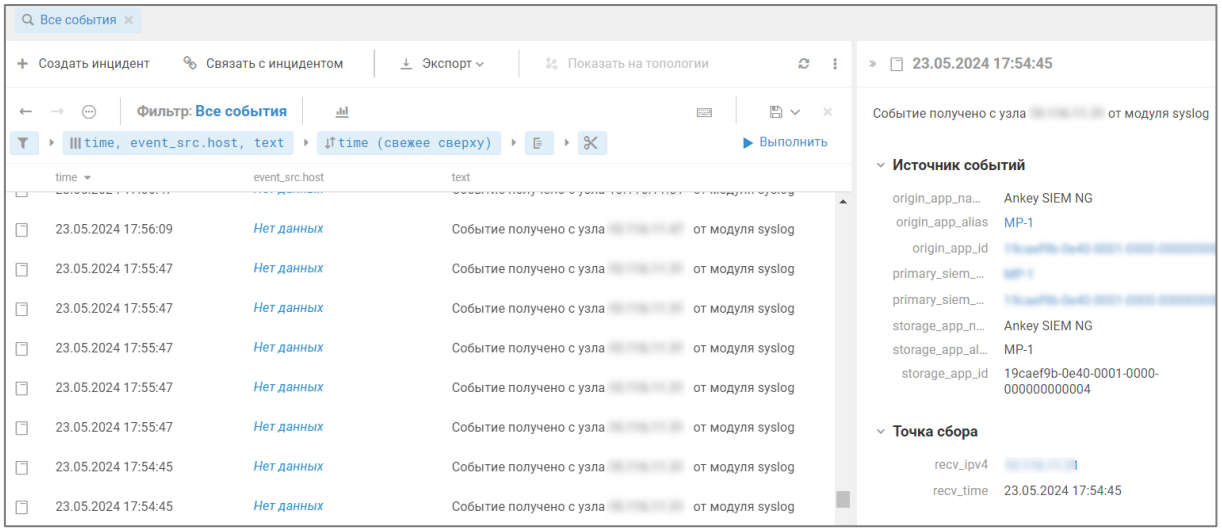


Рисунок 24.33 – Поля события источника

Возможные проблемы и их решение:

❖ В одном из полей обнаружено несоответствие. При нахождении данной проблемы обратитесь в службу технической поддержки ООО «Газинформсервис»[29].

❖ В требуемых полях отсутствует информация. В таком случае необходимо обратиться в службу технической поддержки ООО «Газинформсервис»[29].

❖ Маппинг в событии неправильный, неподходящий под правило корреляции:

1. Возможно при обработке более общее правило нормализации или обогащения перехватывает нужное событие от источника.

Примечание. Если Вы обнаружили данную ошибку обратитесь в службу технической поддержки ООО «Газинформсервис»[29].

2. Возможно данное событие не подходит под это правило.

Примечание. Если данное правило должно подходить под правило, то необходимо обратиться в службу технической поддержки ООО «Газинформсервис»[29], приложив исходное событие и обоснование.

❖ Исходное событие дополнительно обрабатывается правилом обогащения для последующей корреляции:

1. В данном случае нужно удостовериться в работе правила обогащения аналогично проверке работоспособности правила корреляции.

[29] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.22.2.3 *Проверка использования табличного списка*

Если правило использует табличный список, то в таком случае правило может не отрабатывать, если табличный список неправильно настроен/не установлен и т.п.

❖ Для проверки того, что правило используют табличные списки необходимо:

1. Изучить информацию об использовании правилом табличных списков, представленную в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание».
2. Для проверки, что данный табличный список в действительности используется, необходимо перейти на вкладку **Ankey SIEM NG** → **Сбор данных** → **Табличные списки**, где выбрать нужный список, а затем перейти на вкладку **Правила корреляции**, как показано на рисунке 24.34.

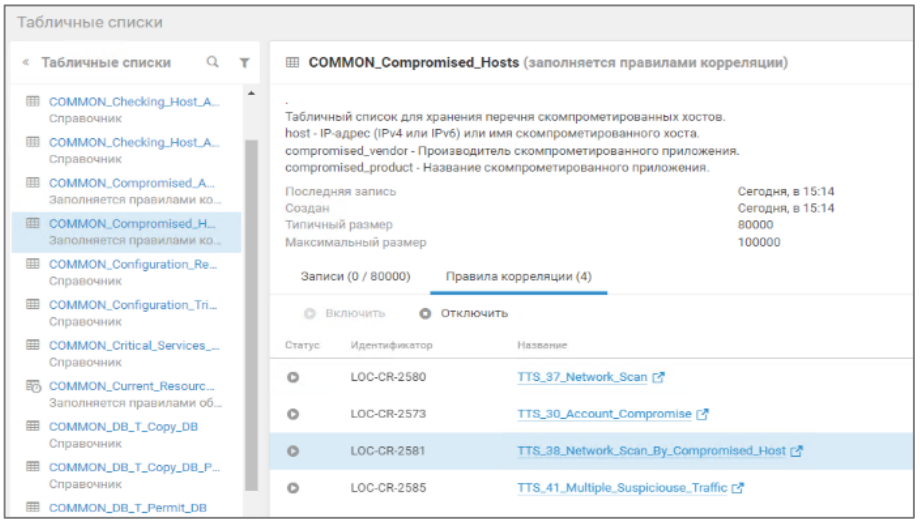


Рисунок 24.34 – Список правил корреляций, использующих табличный список

Примечание. Табличные списки могут быть использованы по-разному. Это могут быть справочники, которые требуют заполнения вручную согласно настройкам на инсталляции ПК Ankey SIEM NG в разрезе подключаемой инфраструктуры. Примеры заполнения представлены в документации на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание». Или же это могут быть табличные списки, заполняемые правилами корреляции или обогащения. И если эти табличные списки не заполнены, то могут быть ложные срабатывания или вовсе отсутствие любых срабатываний правил корреляций.

24.22.3 Проверка корректности использования табличного списка

В данном пункте описывается проверка корректности работы и заполнения табличного списка.

24.22.3.1 *Проверка установки табличного списка в систему*

Проверка установки табличного списка в систему проводится аналогично проверке установки правила корреляции, описание представлено в пункте 24.22.1.1.

Статус установки табличного списка также можно посмотреть двумя способами:

– в папке, в общем перечне (рисунок 24.35);
– в описании к ресурсу (рисунок 24.36).

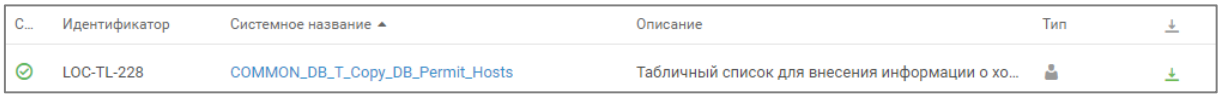


Рисунок 24.35 – Статус установки табличного списка в дереве ресурсов

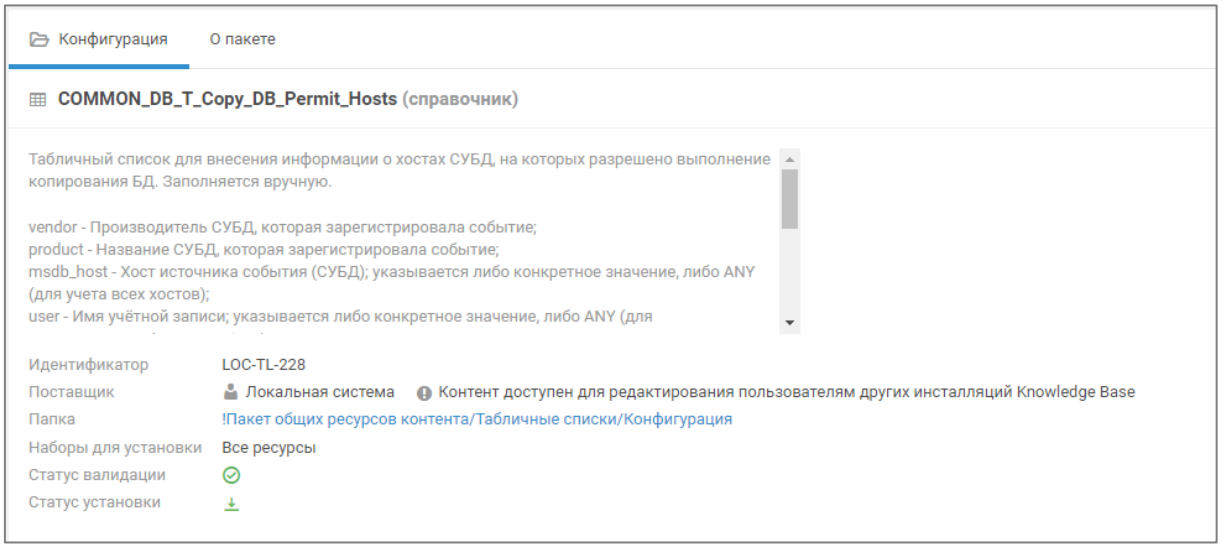


Рисунок 24.36 – Статус установки табличного списка в описании

24.22.3.2 *Проверка корректности заполнения табличного списка*

Для работы правила табличный список должен быть корректно заполнен.

❖ Для проверки корректности заполнения табличного списка необходимо:

1. Для табличного списка – тип Справочник:
   Перейти на вкладку **Knowledge Base** → **SIEM** → **Пакет экспертизы** и выбрать необходимый табличный список. В результате в окне отобразится вся информация по табличному списку, как показано на рисунке 24.37.

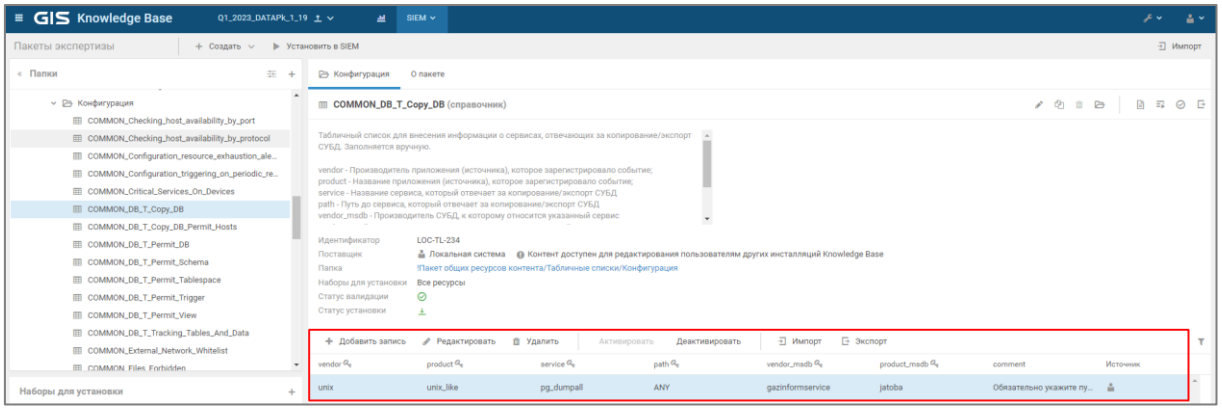


Рисунок 24.37 – Информация по табличному списку

Примечание. Здесь не будет отображаться информация о наполненности табличных списков, заполняемых правилами корреляции и обогащения.

3. Для табличного списка – любой тип:
Перейти на вкладку **Ankey SIEM NG** → **Сбор данных** → **Табличные списки** и выбрать необходимый табличный список. В результате в окне отобразится вся информация по табличному списку, как показано на рисунке 24.38.

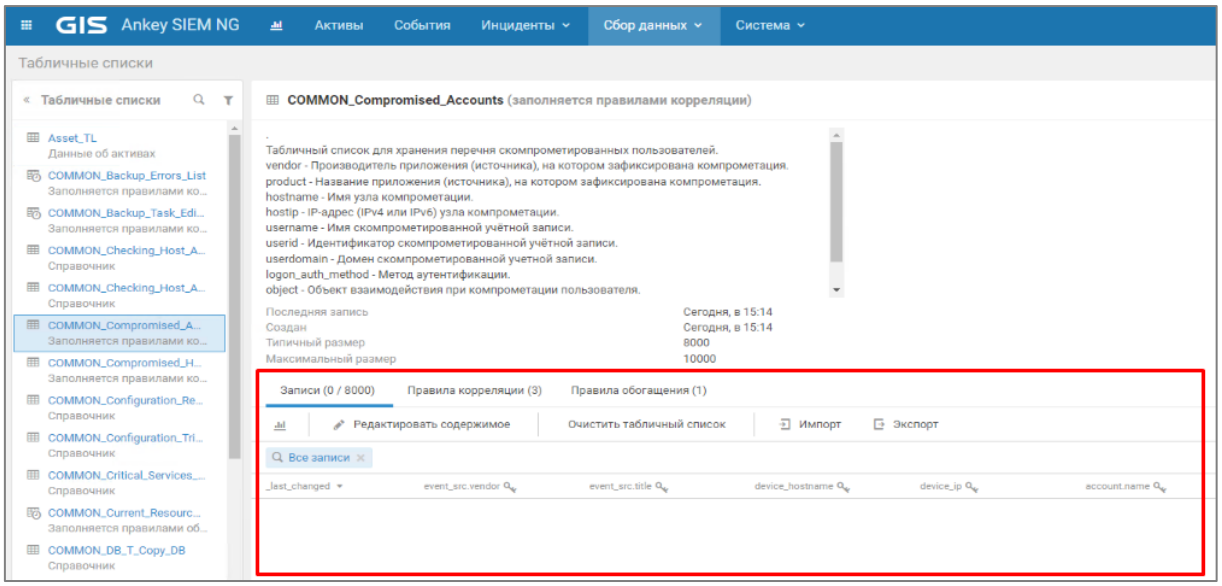


Рисунок 24.38 – Информация о наполненности табличного списка

Возможные проблемы и их решение:

❖ Табличный список не заполнен:

1. Если это табличный список типа Справочник, то его необходимо заполнить вручную необходимыми данными с учетом

поддерживаемых параметров согласно сопроводительной документации на пакет контента[30].

4. Если это табличный список, заполняемый правилами корреляции/обогащения, то убедитесь, что требуемые правила включены и корректно работают, согласно описанию, представленному в подразделе 24.22.

❖ Запись в табличном списке не активирована:

1. Для того чтобы система работала с записями, они должны быть активированы, деактивированные записи подсвечены светло-серым цветом (рисунок 24.39).

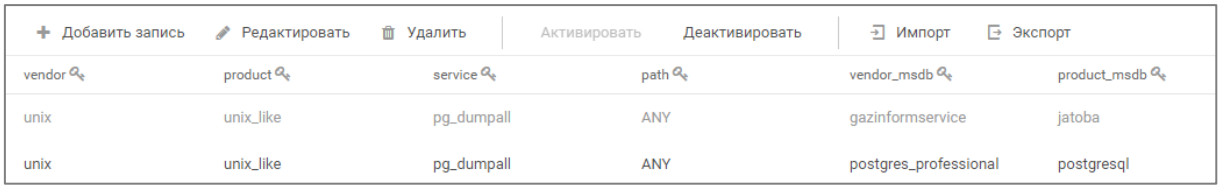


Рисунок 24.39 – Деактивированная запись

5. Для того чтобы активировать запись, выделите ее и нажмите на кнопку **Активировать**, как показано на рисунке 24.40.

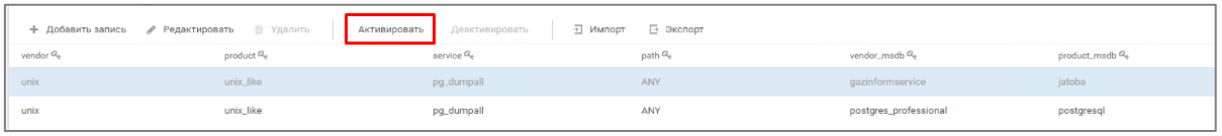


Рисунок 24.40 – Кнопка активации записей

❖ Записи есть в табличном списке, но правило все равно не работает:

1. Если записи были добавлены и активированы, но правило не работает, рекомендуется еще раз установить список в систему (подробно описано в пункте 24.22.3.1).

Примечание. Рекомендуется каждый раз, когда табличный список изменяется, заново устанавливать его в систему.

❖ Список заполнен некорректными значениями:

1. При заполнении списка необходимо всегда следовать описанию по его заполнению. Каждый табличный список имеет свои особенности: для табличного списка может быть важен регистр полей и не все поля могут поддерживать значение **any**, а также табличный список может обладать любыми другими особенностями заполнения, которые указаны в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание» или в описании табличного списка.

[30] Конечные настройки на инсталляции ПК Ankey SIEM NG определяются в проектной документации.

Примечание. При использовании табличного списка всегда стоит понимать его назначение (конфигурация, список исключений и т.п.) с целью его корректного применения согласно представленным функциональным возможностям.

24.22.4 Корректность проверки правила

В данном пункте описывается проверка корректности выполнения условия правила при тестировании на событиях, а также контроль частоты срабатываний правил корреляций.

24.22.4.1 *Проверка условия выполнения правила*

Для каждого правила есть свое условие, при котором оно срабатывает. Это может быть множественные поступление одного события в течение минуты, а может закономерность в виде последовательности событий. Если не работает правило, убедитесь, что условия для правила соблюдены.

❖ Информацию об условии срабатываний правил корреляций можно посмотреть:

1. В документах на пакеты контента «Наименование пакета Ankey SIEM NG>. Описание».
2. В условии самого правила в ПК Ankey SIEM NG.
   Для этого необходимо перейти на вкладку **Knowledge Base** → **SIEM** → **Пакет экспертизы** и выбрать нужное правило, открыв его, в директиве rule будут прописаны необходимые условия, как показано на рисунке 24.41.

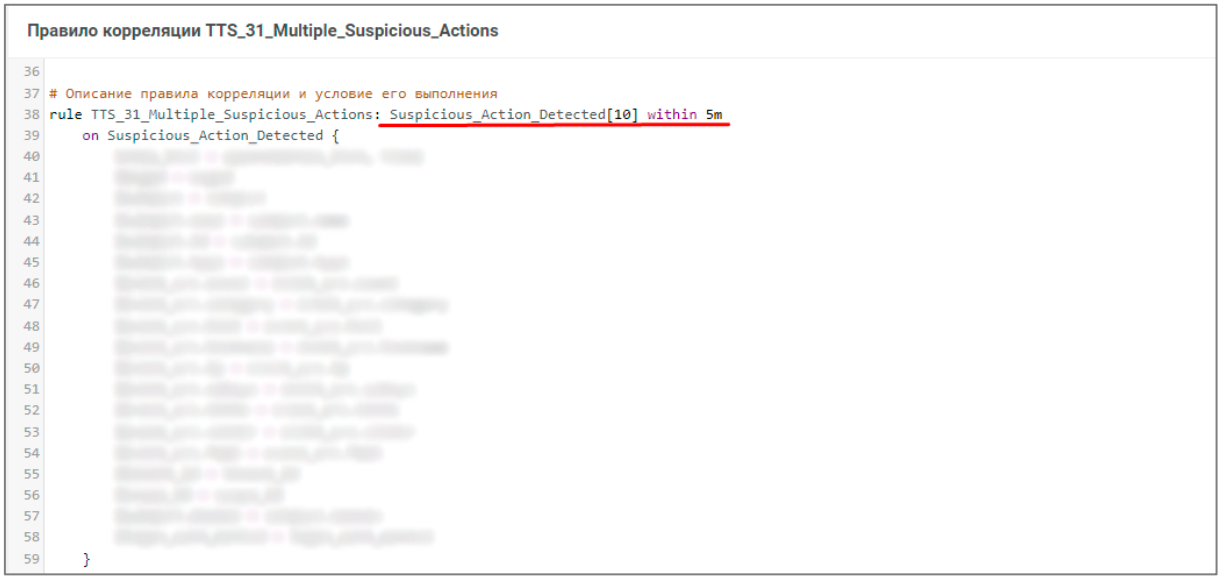


Рисунок 24.41 – Условие для срабатывания правила корреляции

24.22.4.2 *Проверка частоты срабатывания правила*

❖ Частоту срабатывания правила можно посмотреть несколькими способами:

1. Системный дашборд.
   Для этого необходимо перейти на вкладку **Ankey SIEM NG** → **Система** → **Мониторинг обработки событий** и выбрать вкладку **Корреляция**, как показано на рисунке 24.42.
   Подробное описание системного дашборда Мониторинг обработки событий представлено в документе «Руководство оператора Ankey SIEM NG».

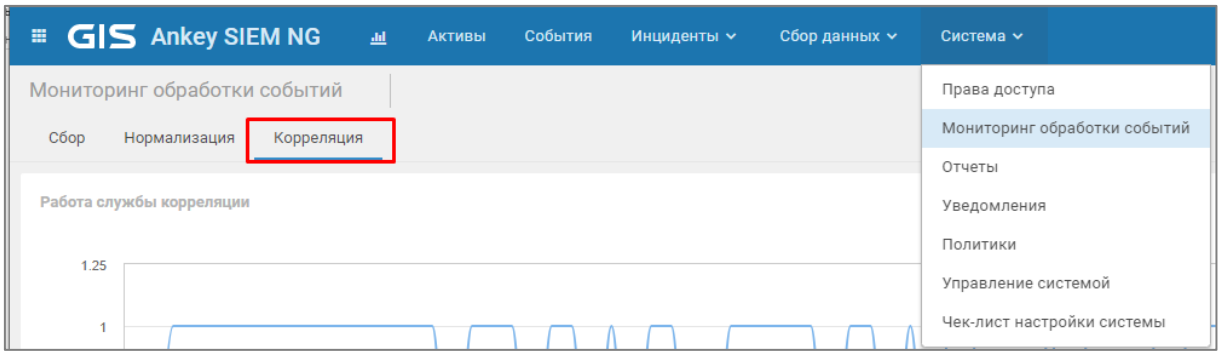


Рисунок 24.42 – Вкладка Корреляция

6. В результате на данном дашборде (рисунок 24.43) отобразится следующая информация:
   – работа службы корреляции;
   – срабатывание правил;
   – наиболее частые корреляции за 24 часа.
   С помощью данной информационной панели имеется возможность оценить работу коррелятора за сутки.

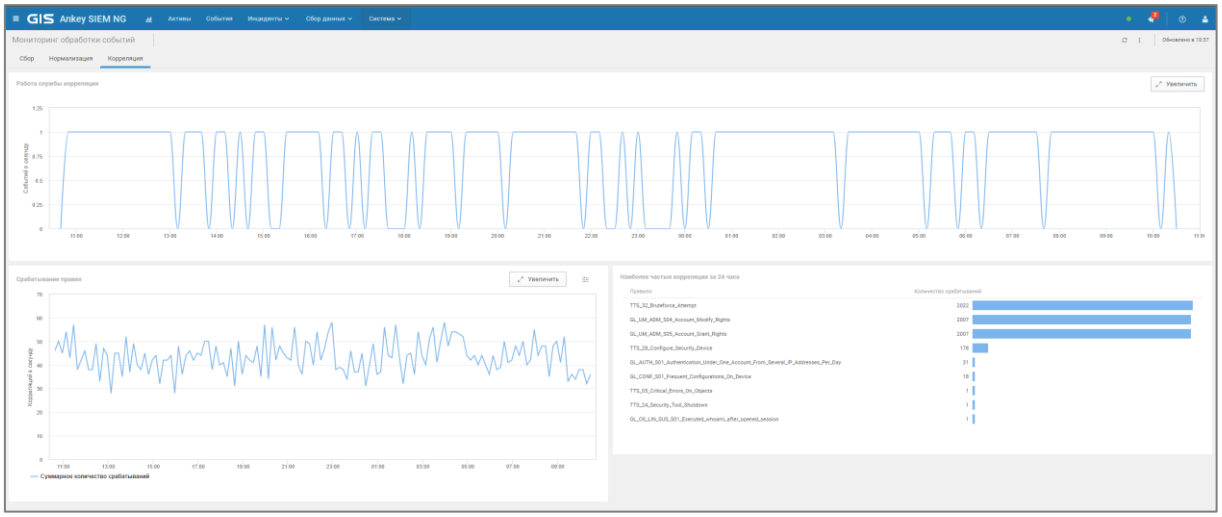


Рисунок 24.43 – Информация в виде дашборда по правилам корреляции

7. Список правил корреляций.

Для отображения списка правил корреляций необходимо перейти на вкладку **Ankey SIEM NG → Сбор данных → Правила корреляции**, как показано на рисунке 24.44.

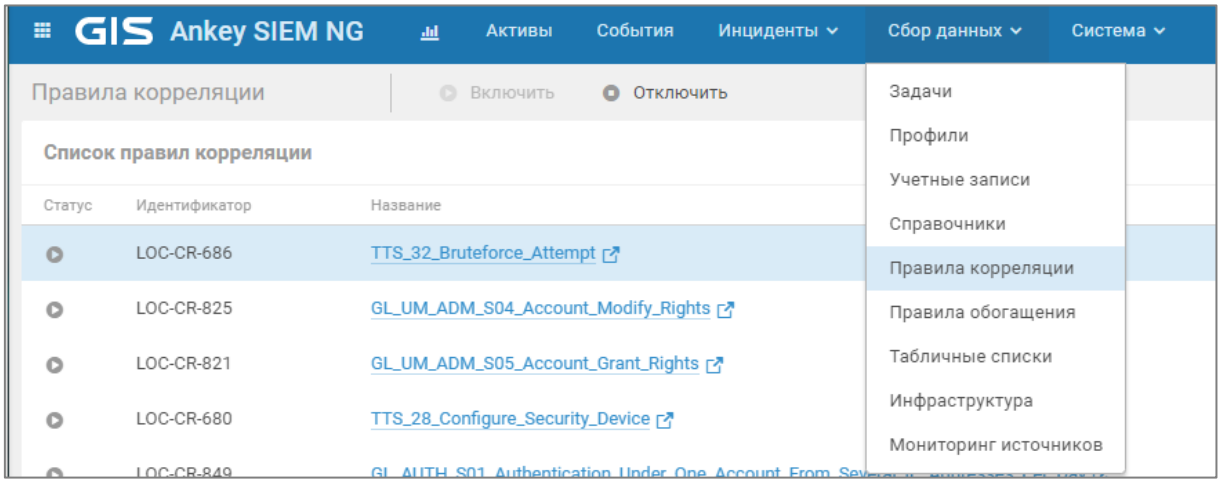


Рисунок 24.44 – Вкладка «Правила корреляции»

После этого необходимо выполнить сортировку по столбцу **Срабатывания за сутки**, в результате будет отображена информация о количестве срабатываний правил корреляций за сутки (от большего к меньшему), как показано на рисунке 24.45.

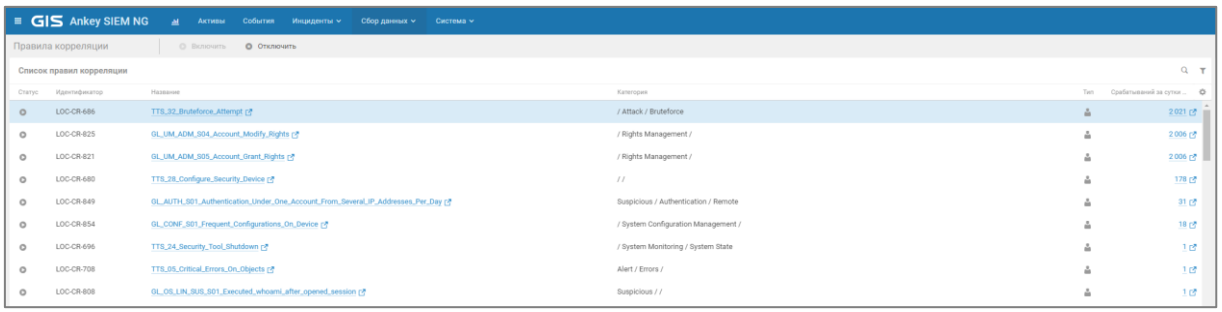


Рисунок 24.45 – Статистика срабатываний правил корреляций на вкладке Правила корреляции

8. Таблица событий.
Для отображения в таблице событий статистики по срабатываниям правил корреляций необходимо перейти на вкладку **Ankey SIEM NG → События**, указать в фильтре correlation_name != null, а также выполнить группировку по correlation_name, в результате чего отобразится количество срабатываний правил корреляции за любой произвольный период времени, как показано на рисунке 24.46.

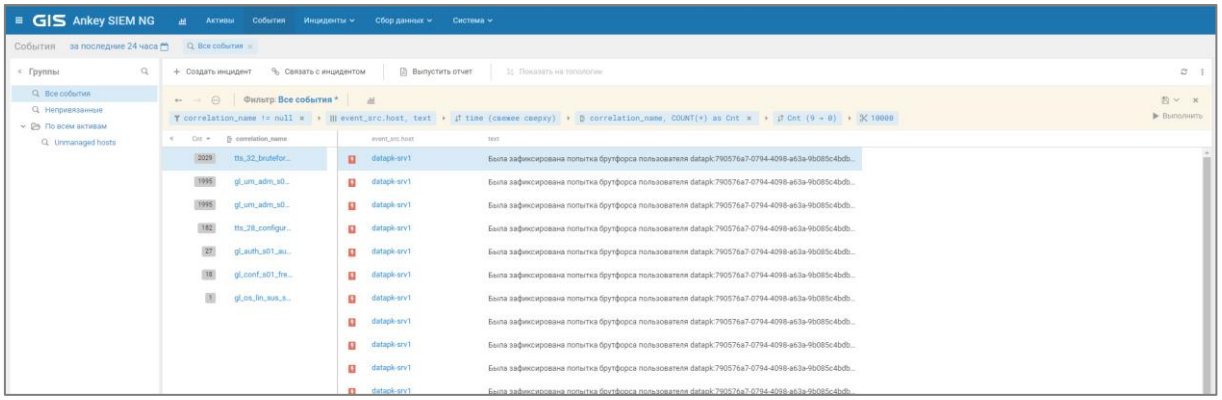


Рисунок 24.46 – Статистика в таблице событий по правилам корреляции

Примечание. На данной вкладке возможно проводить анализ срабатываний правил корреляций с разных сторон: можно уточнить запрос по хосту/источнику и т.д., а также имеется возможность сгруппировать события не только по названию правил корреляций, но и по любым другим полям, например, по наименованию источника (рисунок 24.47).

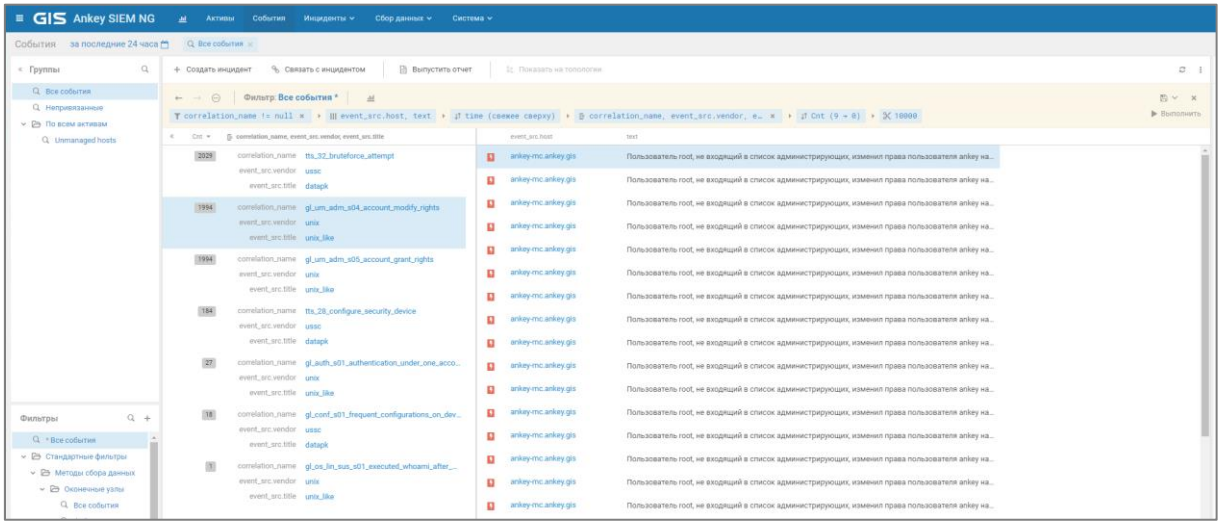


Рисунок 24.47 – Статистика по правилам корреляции с учетом источников

Возможные проблемы и их решение:

- Если правило отрабатывает слишком часто, то проверьте:
  1. Правильность заполнение табличного списка конфигурации, если он используется:
     - данный список может иметь слишком общую настройку (используется значение **any**, выбрана широкая подсеть, обобщенный regex).
       В таком случае можно попытаться, если есть возможность, сократить значения конфигурационного списка;
     - некорректно заполнен список. Не соблюдены требования по заполнению табличного списка.
  2. Возможность использования списка исключений (подробнее см. в пункте 24.22.5) и правильность его заполнения.

3. События от источника.
Если под правило корреляции попадает одно и тоже событие от источника, при этом данное событие имеет неправильный маппинг, то необходимо обратиться в службу технической поддержки ООО «Газинформсервис»[31].

Примечание. [Не рекомендуется, но возможно]. Если проблему нужно решить срочно, то можно отключить правило нормализации или обогащения, связанное с этим событием. При невозможности отключить данное правило – в него входят другие значимые события, то закомментировать строки, связанные с часто появляющимся событием.

4. Возможно большое количество срабатываний правил во время проведения работ с источниками на объекте.

24.22.5 Возможность уменьшения срабатываний правил корреляции

В данном пункте описывается возможность использования списков исключений для уменьшения количества срабатываний или для возможности точечного контроля за объектами за счет исключения по определенным значениям.

24.22.5.1 *Проверить наличие исключения в правиле*

Информацию по табличным спискам исключений представлена в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание».

Для того чтобы проверить, что правило использует общий список исключений необходимо перейти на вкладку **Ankey SIEM NG → Сбор данных → Табличные списки**, выбрать общий табличный список исключений и посмотреть в перечне интересующее правило, как показано на рисунке 24.48.

[31] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

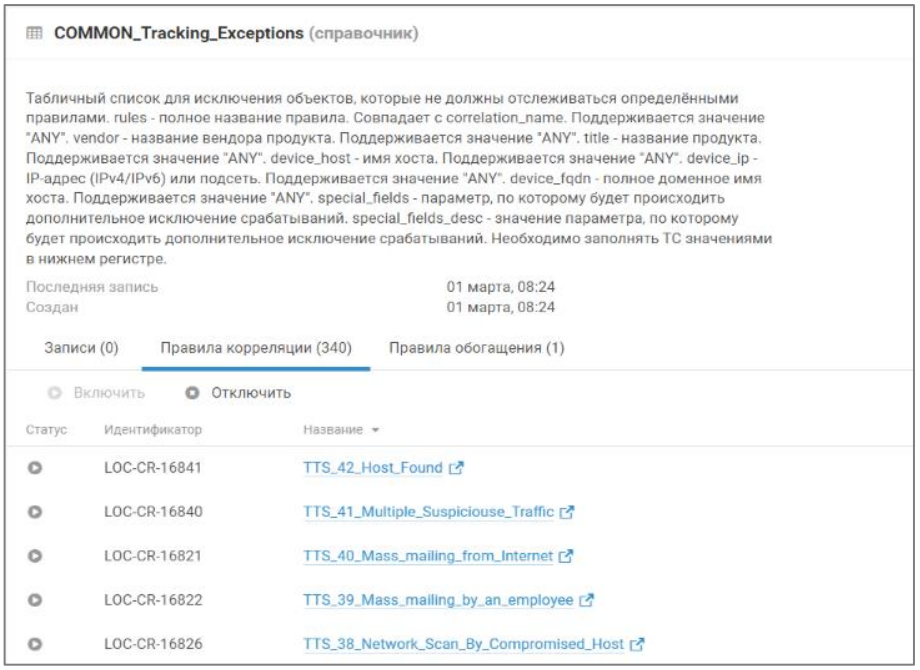


Рисунок 24.48 – Табличный список COMMON_Tracking_Exceptions

Данный табличный список, кроме основных полей, также имеет несколько специальных полей, с помощью которых для определенных правил можно настроить дополнительное исключение для срабатываний.

Информацию для каждого правила можно найти в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание».

Примечание. Для любого правила возможен собственный список исключений, подробнее указано в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание».

24.22.5.2 *Проверить корректность исключения*

Заполнение списка исключений возможно двумя способами:

- вручную;
- с помощью шаблона исключений (подробно описано в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание»).

Примечание. Всегда, когда заполняете шаблон исключений вручную, необходимо следовать правилам заполнения, описанным в документации.

Возможные проблемы и их решение:

1. Заполнили или изменили содержимое списка исключений, но правило все равно отрабатывает:
   - необходимо заново установить табличный список исключений в систему;

Примечание. Каждый раз, когда изменяется список исключений, рекомендуется его заново устанавливать в систему.

– некорректно заполнен список исключений.

2. Если список исключений был заполнен с помощью шаблона исключений, т.е. автоматически, но правило все равно отрабатывает:
   – проверьте заполнение специальных полей, которые позволяют более тонко настроить исключения;
   – если все правильно заполнено, то сообщите в службу технической поддержки ООО «Газинформсервис»[32].

24.22.6 Дополнительная информация

Дополнительные рекомендации по источникам и правилам:

1. Если нужное правило все еще не работает на источнике, проверьте по документации, что данный источник совместим с данным правилом и у него есть требуемые события.
2. Если правило можно улучшить или обеспечить совместимость функциональных возможностей по определенным источникам, то обратитесь в службу технической поддержки ООО «Газинформсервис».
3. В случае необрабатываемых событий со стороны источника необходимо сформировать запрос в службу технической поддержки ООО «Газинформсервис» и передать исходные события со стороны источника.

Внимание! Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

24.22.7 Версия пакета контента

Перед обращением в службу технической поддержки ООО «Газинформсервис» необходимо найти версию пакета контента.

❖ Чтобы посмотреть версию пакета контента:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт Knowledge Base.
   Откроется веб-интерфейс Ankey SIEM NG Knowledge Base на странице **Статистика**.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите **<Наименование пакета контента>** и откройте вкладку **О пакете**, как показано на рисунке 24.49.

[32] Обращение в техническую поддержку осуществляется в соответствии с разделом 25.

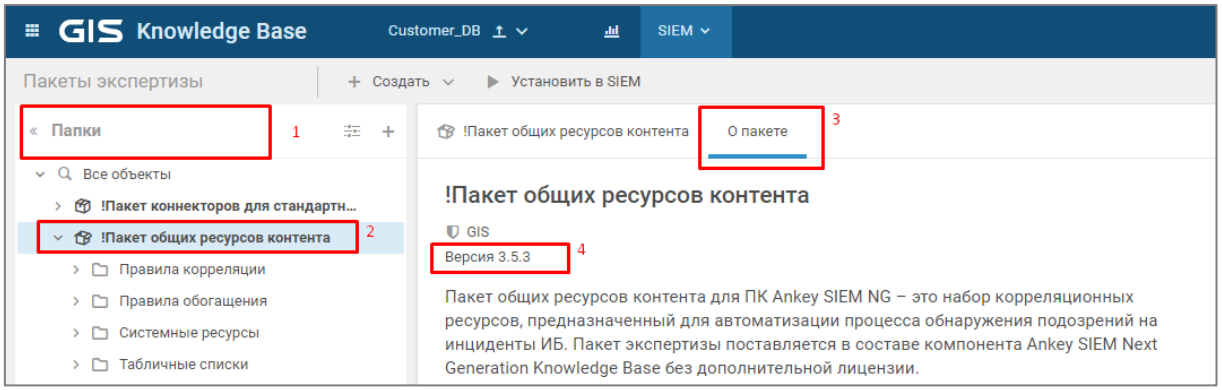


Рисунок 24.49 – Просмотр версии пакета контента в веб-интерфейсе

Номер версии пакета контента будет указан на вкладке **О пакете** в строке **Версия:<A.B.C>**.

24.23 Не все зависимые ресурсы импортированы в систему и/или добавлены в набор установок

Решение

❖ Чтобы решить проблему:

1. Если не установлена (импортирована) таксономия полей в систему, то появится ошибка (рисунок 24.50).

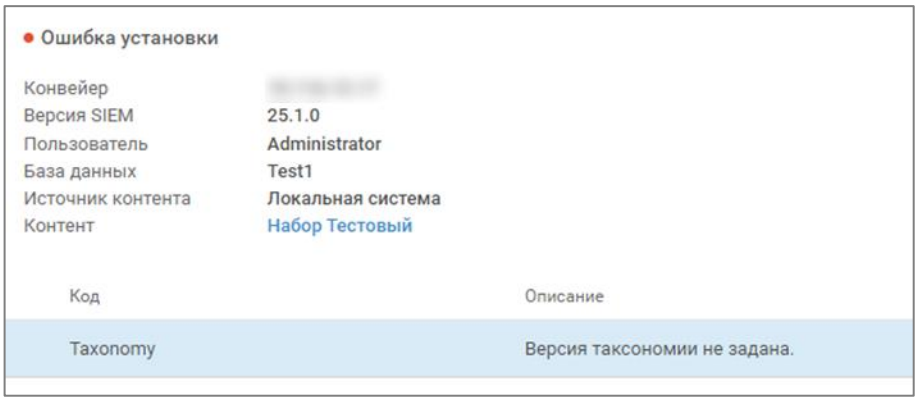


Рисунок 24.50 – Ошибка таксономии

В таком случае установите в систему недостающую таксономию полей (возможно при импорте пакета Вы забыли добавить ключ для импорта таксономии --ImportTaxonomy).
Подробнее см. документ «Руководство по инсталляции Ankey SIEM NG 5.2.3 (с компонентом VM)».

2. Если версия схемы полей событий не совпадает с версией SDK (рисунок 24.51), то возникает ошибка, показанная на рисунке 24.52.

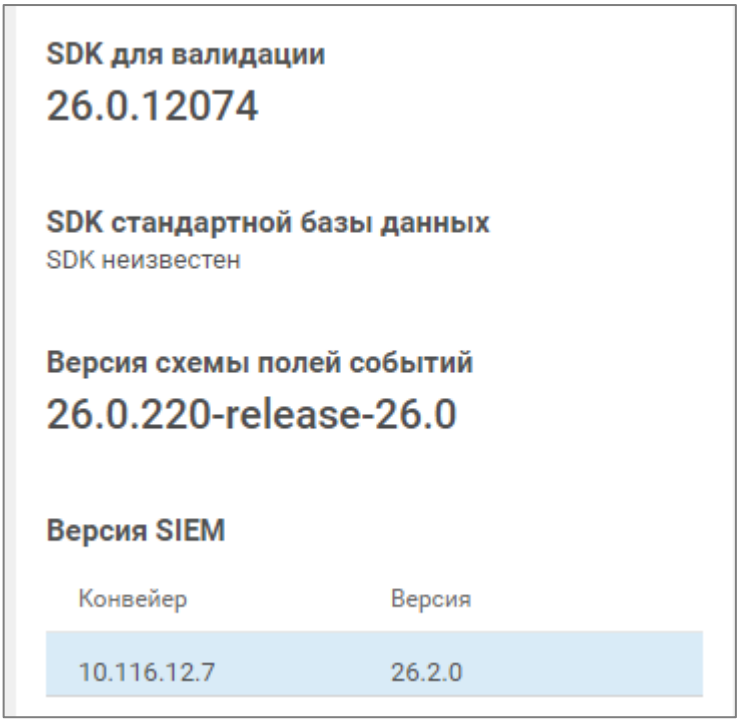


Рисунок 24.51 – Различия в версиях SDK и схемы полей

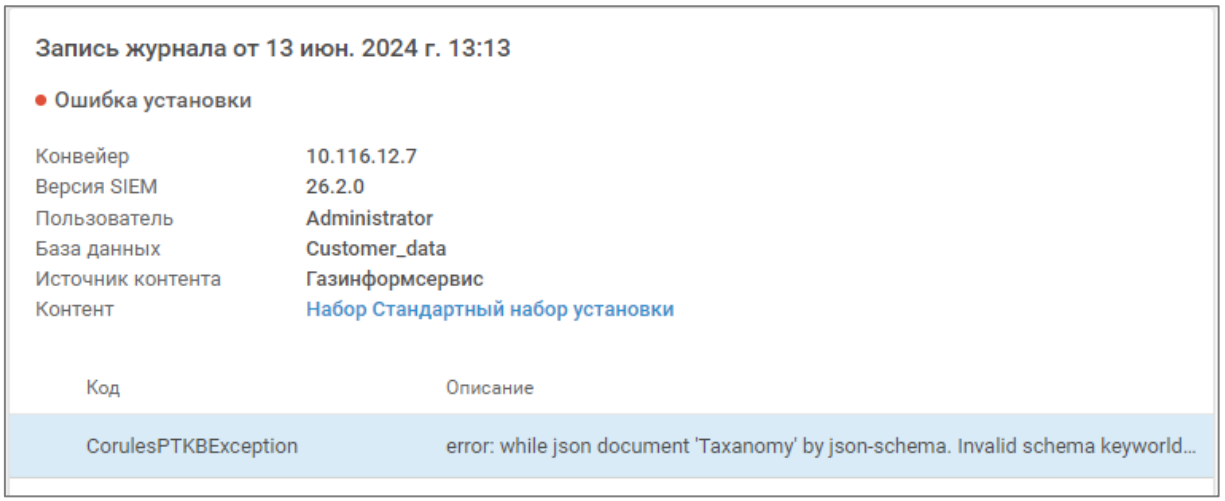


Рисунок 24.52 – Ошибка, возникающая при различных версиях SDK и таксономии

3. Необходимо в систему импортировать нужную версию таксономии полей с помощью команды из командной строки:
importPackage --db <Имя БД, например:TestDB> --kbhost <Обязательно полное доменное имя хоста с приложением КВ (например core.test.dom)> --login <логин> --password <пароль> --source "<Полный путь до файла таксономии (например, /home/administrator/knowledgebase_tax.kb)>" --mode Upsert –ImportTaxonomy

Примечание. На установку ресурсов в систему не повлияет, но будет недоступна валидации ресурсов, если в системе SDK не будет установлена.

4. Для установки SDK в систему необходимо перейти на вкладку **Knowledge Base → SIEM → Выбор версии SDK**, выбрать необходимую версию SDK и установить в систему, как показано на рисунке 24.53.

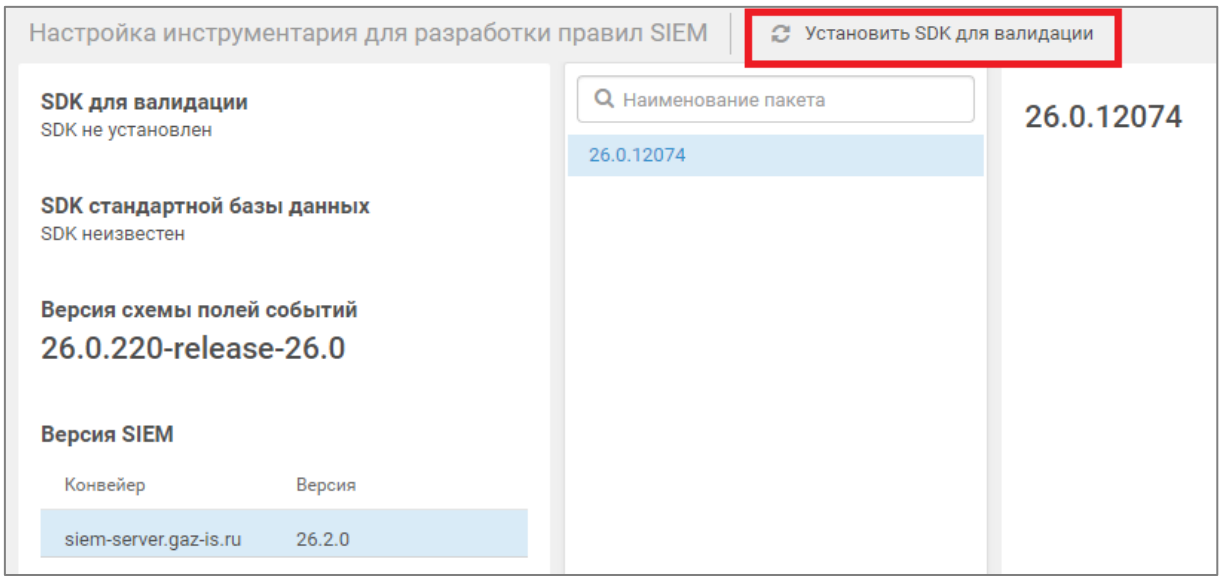


Рисунок 24.53 – Установка SDK для валидации

24.24 Справочная информация

В подразделе приведены рекомендации по выполнению шагов инструкций.

24.24.1 Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки

❖ Чтобы просмотреть данные о распределении памяти ОЗУ, выполните команду: free -h

Интерфейс терминала отобразит информацию об объеме используемой и неиспользуемой памяти ОЗУ, а также информацию об объеме раздела подкачки.

Если объем раздела подкачки не равен нулю, необходимо его отключить.

❖ Чтобы отключить раздел подкачки, выполните команду: swapoff -a

24.24.2 Сбор информации о нагрузке на файловую систему и запущенных процессах

❖ Чтобы собрать информацию о нагрузке на файловую систему, выполните команду: iostat -xt 10 10 > iostat.txt

Информация о нагрузке на файловую систему сохранится в файле /root/iostat.txt.

Примечание. Если утилита iostat отсутствует в ОС, необходимо установить ее, выполнив команду apt-get install -f sysstat.

❖ Чтобы собрать информацию о запущенных в системе процессах, выполните команду: top -b -d 10 -n 10 -o %MEM > top.txt

Информация о запущенных в системе процессах сохранится в файле /root/top.txt.

24.24.3 Просмотр статуса службы

❖ Чтобы просмотреть статус служб (Docker-контейнеров ролей) компонентов Ankey SIEM NG Core, Ankey SIEM NG MC и Knowledge Base, выполните команду:

docker ps --format "table {{.Names}}\t{{.State}}\t{{.Status}}"

❖ Чтобы просмотреть статус служб Ankey SIEM NG Server на Linux, выполните команду: systemctl --all status siemserver*service

❖ Чтобы просмотреть статус служб Ankey SIEM NG ES на Linux, выполните команду: systemctl --all status elastic*service

❖ Чтобы просмотреть статус службы (Docker-контейнера роли) RabbitMQ на Linux, выполните команду: docker ps --filter "name=rabbitmq" --format "table {{.Names}}\t{{.State}}\t{{.Status}}"

24.24.4 Проверка доступности сетевого порта сервера

❖ Чтобы проверить доступность сетевого порта сервера, выполните команду:

telnet <IP-адрес или FQDN сервера> <Номер порта>

Если порт доступен, интерфейс терминала отобразит Connected to <IP-адрес или FQDN сервера>.

24.24.5 Просмотр состояния индексов Elasticsearch

Во время инициализации Elasticsearch (например, после перезагрузки сервера) индексы находятся в состоянии red, что является корректным поведением системы (после инициализации все индексы должны сменить состояние на green или yellow). Поэтому рекомендуется просматривать состояние индексов через 15 минут после запуска всех служб Elasticsearch.

❖ Чтобы просмотреть состояние индексов, выполните команду:

curl localhost:9200/_cat/indices?v

Примечание. Вы можете сохранить данные о состоянии индексов в файл с помощью команды curl localhost:9200/_cat/indices &> /usr/ all_indices_and_errors.txt.

❖ Чтобы просмотреть состояние шардов (фрагментов индексов), выполните команду:

curl localhost:9200/_cat/shards?v

Примечание. Вы можете сохранить данные о состоянии шардов в файл с помощью команды curl localhost:9200/_cat/shards &> /usr/ all_indices_and_errors.txt.

24.24.6 Просмотр состояния Elasticsearch

❖ Чтобы просмотреть состояние Elasticsearch, выполните команду:
curl localhost:9200/_cluster/health?pretty

24.24.7 Создание дампа памяти процесса

❖ Чтобы создать дамп памяти процесса на Linux:

1. Определите идентификатор процесса:
   pgrep <Название процесса>
   Интерфейс терминала отобразит идентификатор процесса.
2. Создайте файл дампа:
   kill -12 <Идентификатор процесса>
   DMP-файл дампа сохранится в том же каталоге, где расположен исполняемый файл процесса.

Дамп памяти процесса создан.

24.24.8 Расположение индексов Elasticsearch

Путь к индексам Elasticsearch указан в качестве значения параметра path.data в файле /etc/elasticsearch/<Название узла>/ elasticsearch_<Название узла>.yml.

Путь к архивным индексам указан в качестве значения параметра path.repo в файле /etc/opt/siem/siem-storage/params.yaml.

24.24.9 Расположение файлов журналов

Для анализа проблемы и выработки путей ее решения службе технической поддержки могут потребоваться файлы журналов. Система может использовать эти файлы во время их сбора, поэтому для сбора файлов необходимо их скопировать, создать из скопированных файлов архив (со сжатием) и отправить его в службу технической поддержки.

Таблица 24.4 – Расположение файлов журналов компонентов на Linux

Компонент	Путь к файлам
Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Collector	Файлы журналов находятся в каталоге /var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log, журнал установки – в файле <Каталог со сценарием установки install.sh>/ install_<Название роли>_<Номер версии>.log
Ankey SIEM NG Server	Файлы журналов находятся в каталогах /opt/siem/log и /opt/siem/log/<Название службы>/logs, журнал установки – в файле <Каталог со сценарием установки install.sh>/install_SiemServer_<Номер версии>.log
Ankey SIEM NG ES	Файлы журналов находятся в каталогах /var/log/elasticsearch/ и /es_logs/, журнал установки – в файле <Каталог со сценарием установки install.sh>/install_SiemStorage_<Номер версии>.log

Компонент	Путь к файлам
RabbitMQ	Файлы журналов находятся в каталоге /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли RMQ Message Bus>/log, журнал установки – в файле <Каталог со сценарием установки install.sh>/install_RmqMessagebus_<Номер версии>.log
СУБД PostgreSQL	Файлы журналов находятся в каталоге /var/lib/deployed-roles/<Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли SqlStorage>/log, журнал установки – в файле <Каталог со сценарием установки install.sh>/install_<Название роли>_<Номер версии>.log

По умолчанию журналы компонента Ankey SIEM NG Server содержат информацию уровня debug и info. Если требуется журналировать всю информацию о работе службы, необходимо в файле siem.conf в секции <Название службы> → logger изменить значение параметра level на trace и перезапустить службу. Расширенное журналирование рекомендуется включать только при диагностике проблем или по запросу службы технической поддержки.

Примечание. Файл siem.conf находится в каталоге /opt/siem/etc.

24.24.10 Параметры мониторинга обработки активов

Основными показателями обработки активов являются длина очереди, время ожидания в очереди и средняя скорость обработки активов. Для тонкой настройки мониторинга обработки вы можете изменять пороговые значения длины очереди и времени ожидания, а также период вычисления средней скорости обработки активов для каждой стадии обработки. Эти параметры находятся в каталоге /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>-<уникальный идентификатор>/images/<название службы>/config/default.env и приведены в таблице.

Пример:
/var/lib/deployed-roles/ankey-application/core/images/core.assets.scans.extended

Таблица 24.5 – Параметры мониторинга обработки активов

Ста-дия обработки	Служба	Длина очереди	Время ожидания	Период вычисления средней скорости обработки	Стадия обработки	Служба
		Допустимое значение	Критическое значение	Допустимое значение	Критическое значение	
Обога-щение собран-ных данных	Assets Scans	QueueLengthAllowedThreshold	QueueLengthCriticalThreshold	WaitingTimeAllowedThreshold	WaitingTimeCriticalThreshold	ProcessingSpeedCalculationPeriod
Иденти-фикация актива	Assets Identification					
Буферизация	Assets Processing	IdentityCommandsBufferingQueueLengthAllowedThreshold	IdentityCommandsBufferingQueueLengthCriticalThreshold	IdentityCommandsBufferingWaitingTimeAllowedThreshold	IdentityCommandsBufferingWaitingTimeCriticalThreshold	IdentityCommandsBufferingProcessingSpeedCalculationPeriod
Слияние данных об активах	Assets Processing	AssetsMergingQueueLengthAllowedThreshold	AssetsMergingQueueLengthCriticalThreshold	AssetsMergingWaitingTimeAllowedThreshold	AssetsMergingWaitingTimeCriticalThreshold	AssetsMergingProcessingSpeedCalculationPeriod

Расчет содер-жимого динами-ческих групп	Assets Processing	DynamicGroupsCalculationQueueLengthAllowedThreshold	DynamicGroupsCalculationQueueLengthCriticalThreshold	DynamicGroupsCalculationWaitingTimeAllowedThreshold	DynamicGroupsCalculationWaitingTimeCriticalThreshold	DynamicGroupsCalculationProcessingSpeedCalculationPeriod
Расчет данных об уязви-мостях	Assets Processing	VulnerabilityCalculationQueueLengthAllowedThreshold	VulnerabilityCalculationQueueLengthCriticalThreshold	VulnerabilityCalculationWaitingTimeAllowedThreshold	VulnerabilityCalculationWaitingTimeCriticalThreshold	VulnerabilityCalculationProcessingSpeedCalculationPeriod
Обнов-ление отобра-жаемых данных об активе	Assets Temporal Read Model	QueueLengthAllowedThreshold	QueueLengthCriticalThreshold	WaitingTimeAllowedThreshold	WaitingTimeCriticalThreshold	ProcessingSpeedCalculationPeriod
Обнов-ление таблич-ных списков	Tables					

24.24.11 Просмотр данных о политиках ILM

❖ Чтобы просмотреть текущее состояние индекса Elasticsearch и список политик ILM, которые к нему применены,
выполните команду:
curl 127.0.0.1:9200/siem_events_<Дата создания индекса>-000001/_ilm/explain?pretty

❖ Чтобы просмотреть статус политики ILM,
выполните команду:
curl 127.0.0.1:9200/_ilm/status

❖ Чтобы просмотреть текущую политику ILM без указания индекса,
выполните команду:
curl 127.0.0.1:9200/_ilm/policy/siem_events_policy

24.24.12 Экспорт конфигурационных параметров ролей в файл

Вы можете экспортировать конфигурационные параметры ролей Ankey SIEM NG в файл манифеста с помощью утилиты Export-Configuration, поставляемой с ролью Deployer. Полученный в результате экспорта манифест вы можете использовать при развертывании Ankey SIEM NG на другом сервере.

❖ Чтобы экспортировать конфигурационные параметры ролей в файл:

1. Запустите утилиту Export-Configuration:
   /opt/deployer/bin/Export-Configuration.ps1
2. В открывшемся окне выберите варианты с идентификаторами приложений.
3. В открывшемся окне выберите экземпляры ролей, для которых необходимо экспортировать конфигурационные параметры.
   Начнется экспорт параметров выбранных экземпляров ролей. В каталоге с утилитой появится файл export_manifest.yaml.

> **Примечание.** Если в каталоге уже существует файл с именем export_manifest.yaml, в конец его имени будут добавлены дата и время создания нового файла: export_manifest.yaml.<yyyyMMddHHmmss>. Новый файл будет сохранен с именем export_manifest.yaml.

4. Параметры роли экспортированы.
5. При запуске утилиты вы можете также использовать специальные ключи:
   – для указания приложения – ключ AppInstanceId <Идентификатор приложения>. Например: /opt/deployer/bin/Export-Configuration.ps1 -AppInstanceId mc-application

> **Примечание.** После запуска утилиты с этим ключом в файл манифеста будут экспортированы конфигурационные параметры всех ролей приложения, указанного в ключе.

- для указания роли – ключ RoleInstanceId <Идентификатор экземпляра роли>. Например: /opt/deployer/bin/Export-Configuration.ps1 -RoleInstanceId managementandconfiguration

6. Для каждого ключа можно указать только один идентификатор.

25 Обращение в службу технической поддержки

Уполномоченные представители эксплуатационной службы заказчика могут обращаться в диспетчерскую службу ООО «Газинформсервис», формируя для этого заявки любым из способов:

- по телефонам (в рабочие дни с 9:00 до 18:00 по московскому времени):
  - **+7 812 385 11 03** (для звонков из Санкт-Петербурга и Ленинградской области);
  - **+7 800 700 09 87** (для звонков из любой точки России).
- по электронной почте: support@gaz-is.ru;
- на сайте gaz-is.ru в разделе **Поддержка**.

25.1 Требования к содержанию заявки

Заявки принимаются по неисправностям в работе программного обеспечения.

Внимание! Пример формы обращения в службу технической поддержки представлен в приложении Е.

В заявке необходимо указать:

- полное наименование организации;
- номер договора либо наименование объекта эксплуатации;
- контактные данные для обратной связи (фамилия и имя, телефон, адрес электронной почты).

Кроме того, необходимо предоставить:

- номер лицензии, сертификат технической поддержки − при наличии;
- подробное описание неисправности, сопутствующих обстоятельств, при которых она возникла (какие операции проводились, при каких условиях выполнялась работа и т. п.);

  Внимание! Описание проблемы необходимо предоставить с учетом выполненных действий по диагностике работы используемой продукции в составе ПК Ankey SIEM NG (подробнее см. раздел 24)[33].

- журналы событий технических средств, копии экранов, которые наглядно отображают проявление неисправности, и иные дополнительные сведения, которые могут помочь при устранении неисправности;

[33] Описание инструкций по диагностике коннекторов представлено в подразделе 24.20, контента в подразделе 24.22.

- наименования и версии[34] используемых программных модулей, включая дополнительные (компоненты платформы, пакеты контента и коннекторы, в отношении которых были выявлены проблемы относительно выполнения поддерживаемых функций);
- настройки этих программных модулей, профили сбора, настроенные параметры контента (редактируемые параметры, табличные списки, подробнее о редактируемых параметрах см. в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание»;
- наименования и конкретные версии/модели (серии) затрагиваемых источников событий с указанием наименования и версии среды функционирования (ОС) и прошивок, тип сбора с источника и протокол взаимодействия с источником, по которому выполняется сбор событий, а также аппаратные характеристики источника;
- аппаратные характеристики используемого оборудования, на котором эксплуатируются программные компоненты ПК Ankey SIEM NG.

25.2 Порядок регистрации и учета заявок

Все поступающие заявки регистрируются в автоматизированной системе учета заявок и получают уникальный идентификационный номер:

- при обращении по телефону диспетчер на основании полученных данных регистрирует заявку, сообщает идентификационный номер и предварительный порядок ее отработки;
- при обращении по электронной почте заявка регистрируется автоматически и в ответ высылается уведомление с указанием ее идентификационного номера;
- при обращении через сайт «Газинформсервис» заявка регистрируется автоматически и уведомление с указанием ее идентификационного номера высылается на адрес, указанный при заполнении формы заявки.

Внимание! Для дальнейшего взаимодействия при обработке заявки необходимо знать ее регистрационный номер.

Необходимо предоставить согласно выполненным действиям по диагностике работы используемой продукции в составе ПК Ankey SIEM NG (подробнее см. раздел 24)[35] диагностическую информацию максимально подробно (файлы журналов, снимки экрана, результаты выполнения рекомендаций исполнителя, каналы для удаленного доступа, условия и шаги для

[34] Для определения версии установленного коннектора см. пункт 24.21.5, для определения версии пакета контента см. пункт 24.22.7.

[35] Описание инструкций по диагностике коннекторов представлено в подразделе 24.20, контента в подразделе 24.22.

воспроизведения проблемы, а также перечень данных из подраздела 25.1) для своевременного разрешения обращения.

Инженер технической поддержки ООО «Газинформсервис» по мере проведения основных этапов работ информирует заявителя:

- о процессе и результатах диагностики проблемы;
- поиске решения или возможности обойти причины возникновения проблемы;
- планировании и выпуске обновления продукта (если это требуется для устранения проблемы).

Работы по заявке считаются выполненными, если предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функциональность ПК Ankey SIEM NG.

Если в рамках устранения проблемы необходимо внести изменения в изделие (провести его доработку)[36], то работы по исправлению включаются в ближайшее возможное плановое обновление изделия (в зависимости от сложности изменений).

Время реакции и время обработки

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа инженера технической поддержки ООО «Газинформсервис» с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного уровня значимости запроса[37].

В случае неактивности заявителя в течение значительного периода времени, установленного регламентом производителя в рамках приобретенного уровня технической поддержки, производитель оставляет за собой право считать обращение неактуальным и, уведомив, закрыть запрос.

[36] Улучшения изделий в отношении потребностей в новых функциональных возможностях регистрируются от различных заявителей и на основании наибольшего количества запросов. Формируется приоритизация их реализации в отношении используемой продукции. При этом в связи с тем, что изделие поставляется в виде «как есть», такие обращения не рассматриваются как некорректная работа действующего функционала для оперативного выпуска исправлений. В связи с этим улучшения функциональных возможностей реализуются на усмотрение производителя в зависимости от количества обращений в последующих релизах продукции ПК Ankey SIEM NG.

[37] Инженер технической поддержки ООО «Газинформсервис» оставляет за собой право переопределять уровень значимости запроса. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

25.3 В техническую поддержку входит

В состав услуг технической поддержки ПК Ankey SIEM NG входят следующие виды услуг:

1. Дистанционные консультации по вопросам:
   - лицензирования ПК Ankey SIEM NG;
   - приобретения ПК Ankey SIEM NG;
   - установки, настройки, обновления и особенностям действующих функциональных возможностей в отношении продукции ПК Ankey SIEM NG (платформа, коннекторы, контент);
   - диагностики и устранения проблем действующих функциональных возможностей ПК Ankey SIEM NG[38].
2. Предоставление актуальной технической документации, обновлений и исправлений ПК в соответствии с лицензионными соглашениями.
3. Предоставление актуальной информации по продукту.

Примечание. Выезды сотрудников ООО «Газинформсервис» для выполнения обязательств по технической поддержке заказчиков осуществляются только в рамках действующего договора на техническое сопровождение.

Техническая поддержка может быть оказана, если параметры/функциональные возможности, указанные в таблице 25.1, присутствуют в поддерживаемой релизной версии[39].

Таблица 25.1 – Поддерживаемые параметры и функциональные возможности

Направление/ Модуль SIEM	Параметры и функциональные возможности*
Платформа**	Поддерживаемые функциональные возможности компонентов платформы ПК Ankey SIEM NG
Коннекторы***	Поддерживаемый механизм сбора данных (Syslog/SNMP/ODBC/HTTPS/OPSECLEA/SSH/SMB и пр.)
	Поддерживаемое окружение (среда функционирования) источника
	Поддерживаемая версия источника
	Состав поддерживаемых событий
	Поддерживаемый формат журналов событий (в отношении поддерживаемой версии и окружения источника) Внимание! Поддерживается формат только по настройкам на изделие для совместимости с источником

[38] Для полноценной диагностики необходимо выполнить инструкции и предоставить информацию о проблеме согласно разделу 20 для платформы, подразделы 20.18 и 20.19 для диагностики коннекторов и контента.

[39] В документации представлены сведения по основным существующим функциональным возможностям под соответствующий релиз.

Направление/ Модуль SIEM	Параметры и функциональные возможности*
	Версия платформы ПК Ankey SIEM NG для коннекторов (коннекторы совместимы с определенными версиями платформы)
	Поддерживаемая версия пакета контента для коннекторов (коннекторы совместимы с определенными версиями пакетов контента)
Контент****	Сформированный состав поддерживаемых сигнатур ИБ (корреляционные правила в пакете контента)
	Поддерживаемые функции корреляционных механизмов и взаимосвязанных ресурсов в пакете контента
	Версия платформы ПК Ankey SIEM NG для контента (контент совместим с определенными версиями платформы)
	Поддерживаемый коннектор (коннекторы совместимы с определенными версиями пакетов контента)
* В составе последних поддерживаемых версий коннекторов и пакетов контента. ** В документации представлены сведения по основным существующим функциональным возможностям под соответствующий релиз. *** Информация по поддерживаемым параметрам представлена в документации, поставляемой вместе с коннектором. **** Информация по поддерживаемым параметрам представлена в документации, поставляемой вместе с пакетами контента.	

25.4 Ограничения в предоставлении услуг технической поддержки

Техническая поддержка предоставляется только по продукции ПК Ankey SIEM NG[40], который используется (применяется) в строгом соответствии с требованиями эксплуатационной и сопроводительной документации от производителя (с учетом соблюдения всех указанных рекомендаций и требований в отношении аппаратного и программного обеспечения).

Техническая поддержка оказывается только по действующему функционалу в релизной версии[41].

Техническая поддержка не может быть оказана, если:

- диагностирован дефект действующих функциональных возможностей (собрана техническая информация о дефекте и условиях его воспроизведения), что требует внесения исправлений в части функциональных возможностей[42];

[40] 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)).

[41] Техническая поддержка распространяется только на:

основные функции программы (функциональные возможности), предусмотренные действующей релизной версией;

на комплектность, предусмотренную действующей релизной версией изделия;

на документацию, предусмотренную действующей релизной версией изделия.

[42] Исправления дефектов по функциональным возможностям могут быть представлены несколькими вариантами: патч, фикс либо новая релизная версия изделия.

- зафиксирован запрос на улучшение существующих функциональных возможностей, что требует рассмотрения заявки и выпуска новой релизной версии со стороны производителя;
- проблема вызвана программными продуктами или оборудованием сторонних производителей и не попадает под услуги технической поддержки ПК Ankey SIEM NG;
- проблема классифицирована как неподдерживаемая.

Если указанные в таблице 25.2 параметры/функциональные возможности отличаются от поддерживаемых, то техническая поддержка не может быть оказана, так как данный функционал отсутствует в релизной версии.

Таблица 25.2 – Ограничение параметров и функциональных возможностей

Направление/ Модуль SIEM	**Ограничения***
Платформа**	Отсутствуют функциональные возможности в компонентах платформы ПК Ankey SIEM NG
Коннекторы***	Отличается механизм сбора данных (Syslog/SNMP/ODBC/HTTPS/OPSECLEA/SSH/SMB и пр.)
	Отличается окружение (среда функционирования) источника (например, другая ОС/СУБД или другая версия прошивки АСО)
	Отличается версия источника
	Отличаются типы поддерживаемых событий источника для коннектора (состав событий не соответствует поддерживаемому перечню)
	Отличается формат регистрируемых данных источника (в отношении поддерживаемой версии и окружения источника) Внимание! Поддерживается формат только по настройкам на изделие для совместимости с источником
	Неподдерживаемая версия платформы ПК Ankey SIEM NG для коннекторов (коннекторы совместимы с определенными версиями платформы)
	Неподдерживаемая версия пакета контента для коннекторов (коннекторы совместимы с определенными версиями пакетов контента)
Контент****	Требуются новые сигнатуры нарушений ИБ (отсутствуют соответствующие правила корреляции в пакете контента)
	Не достаточно поддерживаемых функций корреляционных возможностей в действующих правилах/списках и пр. взаимосвязанных ресурсах
	Неподдерживаемая версия платформы ПК Ankey SIEM NG для контента (контент совместим с определенными версиями платформы)
	Неподдерживаемый коннектор (коннекторы совместимы с определенными версиями пакетов контента)
* В составе последних поддерживаемых версией коннекторов и пакетов контента. ** В документации представлены сведения по основным существующим функциональным возможностям под соответствующий релиз.	

Направление/ Модуль SIEM	Ограничения*
*** Информация по поддерживаемым параметрам представлена в документации, поставляемой вместе с коннектором. **** Информация по поддерживаемым параметрам представлена в документации, поставляемой вместе с пакетами контента.	

В случае отсутствия действующего функционала возможны два варианта:

1. Сформировать запрос на доработку («feature request») с предоставлением всей информации для оценки реализации функционала (подробнее см. подраздел 25.2).

> Внимание! Для корректной работы ПК Ankey SIEM NG и сохранения возможности получения технической поддержки рекомендуется использовать запрос на доработку.

2. [*Не рекомендуется, но возможно при острой необходимости и с учетом принятия ограничений в технической поддержке, см. ниже*]. Провести изменения прикладного набора изделий в виде коннекторов и пакетов контента (функции нормализация и функции корреляция) самостоятельно. При этом все изменения выполняются в пользовательской ветке (подробнее см. документ Руководство оператора Ankey SIEM NG).

> Внимание! Если пользователь вносит изменения в действующие функциональные возможности продукции Ankey SIEM NG, то производитель не несет ответственности[43] за этот набор функционала пользователя, только за эталонный набор от производителя без изменений.

В том числе в состав услуг технической поддержки ПК Ankey SIEM NG не входят следующие услуги:

- техническая поддержка самописных прикладных изделий в виде коннекторов (нормализация и пр. взаимозависимые ресурсы) и пакетов контента (корреляция и пр. взаимозависимые ресурсы);

> Внимание! Технической поддержке подлежат только действующие релизные изделия производства ООО «Газинформсервис».

- обучение пользователей работе с ПК Ankey SIEM NG;
- обучение разработке ресурсов для ПК Ankey SIEM NG;

[43] Не распространяется на внесение записей в табличные списки в отношении последних действующих версий пакетов контента от производителя.

Примечание. Для эксплуатации ПК Ankey SIEM NG необходимо ознакомиться лицензионным соглашением, ознакомиться с предоставляемым комплектом документации на продукцию, а также рекомендуется пройти соответствующий обучающий курс. Вопрос обучения по продукции ПК Ankey SIEM NG необходимо обсуждать с производителем в рамках отдельного запроса с целью проведения соответствующего обучающего курса в рамках действующей программы.

- написание отдельных инструкций по настройке функционала ПК Ankey SIEM NG, для которого уже есть описание в документации[44];
- подготовка нетипового облика комплектности поставляемых изделий[45];
- техническая поддержка в случае использования ПК Ankey SIEM NG с несоблюдением правил и требований эксплуатации, которые заявляет производитель ПК в документации и официальных уведомлениях, справочных материалах.

[44] Документация предоставляется на условиях «как есть». При необходимости дополнительных инструкций нужно сформировать запрос на доработку.

[45] Изделия предоставляются на условиях «как есть». При необходимости подготовки нестандартного облика поставляемых изделий нужно сформировать запрос на доработку.

Перечень сокращений

AIO	–	All in One, конфигурация ПК Ankey SIEM NG для небольших территориально-нераспределенных предприятий (одна площадка) с IT-инфраструктурой не более 1000 активов
API	–	Application Programming Interface – протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого
ARP	–	Таблица Address Resolution Protocol – хранится в памяти операционной системы и содержит записи для каждого известного ей узла сети
CEC	–	Custom Event Collector, модуль Ankey SIEM NG
CSV	–	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
DHCP	–	Dynamic Host Configuration Protocol – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DLP	–	Data Leak Prevention – специализированное ПО, которое защищает организацию от утечек данных
DMP-файл	–	Дамп памяти Microsoft Windows, содержащий отладочную информацию и основные данные о системе на момент его создания
DNS	–	Domain Name System – компьютерная распределённая система для получения информации о доменах
DPI	–	Deep Packet Inspection − технология проверки сетевых пакетов по их содержимому с целью регулирования и фильтрации трафика
EB	–	Модуль Ankey SIEM Next Generation Event Broker
ES	–	Компонент Ankey SIEM Next Generation Events Storage
FQDN	–	Fully Qualified Domain Name − имя домена, не имеющее неоднозначностей в определении
HAR-файл	–	HTTP Archive, формат, используемый инструментами записи HTTP-сеансов для экспорта данных

HCC	–	Модуль Ankey SIEM NG Host Compliance Control
HDD	–	Hard Disc Drive – накопитель на жёстких магнитных дисках
HTML	–	HyperText Markup Language – стандартизированный язык гипертекстовой разметки
HTTP	–	HyperText Transfer Protocol – протокол передачи гипертекста
HTTPS	–	HyperText Transfer Protocol Secure – расширение протокола HTTP в целях повышения уровня безопасности
IDS	–	Intrusion Detection System − система обнаружения вторжений
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
IP	–	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
IPS	–	Intrusion Prevention System − система предотвращения вторжений
JSON	–	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
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 облегчённый вариант разработанного ITU-T протокола DAP
LUS	–	Local Update Server, Локальный сервер обновлений Ankey SIEM NG
MAC	–	Media Access Control – уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet
MC	–	Компонент Ankey SIEM NG Management and Configuration

ODBC	–	Open Database Connectivity – программный интерфейс (API) доступа к базам данных
OPSECLEA	–	Log Export API – интерфейс, позволяющий получать логи с сервера управления (Checkpoint)
PEM	–	Privacy-Enhanced Mail, файл сертификата безопасности, который используется для установления безопасного канала связи между веб-сервером и браузером
PDQL	–	Язык, разработанный для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в ПК Ankey SIEM NG
RAID	–	Redundant Array of Independent Disks – технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности
RC	–	Компонент Ankey SIEM NG Retro Correlator
RDP	–	Remote Desktop Protocol − протокол удалённого рабочего стола
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
SDK	–	Software Development Kit, утилиты Ankey SIEM NG, используемые для отладки правил нормализации, обогащения, корреляции и агрегации
SIEM	–	Security information and event management – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности
SMB	–	Server Message Block – сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам
SMTP	–	Simple Mail Transfer Protocol – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SNMP	–	Simple Network Management Protocol – протокол сетевого управления

SOC	–	Security operations center – центр управления безопасностью отвечает за защиту организации от киберугроз
SSH	–	Secure Shell − сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	–	Secure Sockets Layer – ,безопасный криптографический протокол.
SYSLOG	–	Стандарт отправки сообщений о происходящих в системе событиях
TCP	–	Transmission Control Protocol − протоколов передачи данных интернета
TLS	–	Transport Layer Security – криптографический протокол, основанный на портоколе SSL
TXT	–	Компьютерный файл, содержащий текстовые данные
UDP	–	User Datagram Protocol, протокол пользовательских датаграмм – сетевой протокол транспортного уровня
USB	–	Universal Serial Bus – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
VM	–	Vulnerability Management, дополнительный компонент Ankey SIEM NG
VPN	–	Virtual private network − технология, позволяющая обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети
XML	–	Xtensible Markup Language – расширяемый язык разметки
АРМ	–	Автоматизированное рабочее место
АСО	−	Активное сетевое оборудование
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
СКУД	–	Система контроля и управления доступом
СрЗИ	–	Средство защиты информации
СУБД	–	Система управления базами данных

Приложение А
Параметры конфигурации компонентов Ankey SIEM NG на Linux

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

Таблица А.1 − Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
CustomDockerAddressPool	Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию	–
CustomDockerNetworkSize	Размер подсети, указанной пользователем в параметре CustomDockerAddressPool	–
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	–
RegistryBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	–
RegistryPort	Номер порта для доступа к локальному реестру Docker-образов	5000

Таблица А.2 – Параметры конфигурации роли SqlStorage и JatobaStorage

Параметр	Описание	Значение по умолчанию
Параметры конфигурации роли SqlStorage		
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorAgentHttpPort	Порт для доступа к коллектору OpenTelemetry в роли SqlStorage/JatobaStorage по протоколу HTTP	4319
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента Ankey SIEM NG Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage	–
Network	Сетевое имя реестра Docker-образов	storage-network.sqlstorage

Параметр	Описание	Значение по умолчанию
NetworkDriver	Драйвер Docker-образов	bridge
PgAdminPort	Порт для доступа к PgAdmin	9001
PgAnalyzeScaleFactor	Доля от числа кортежей в таблице, которая прибавляется к значению параметра PgAnalyzeThreshold при расчете порога срабатывания команды ANALYZE. Например, если значение PgAnalyzeThreshold равно 200 000, а значение параметра PgAnalyzeScaleFactor равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет 200 000 + 100 000 = 300 000 кортежей	0.0
PgAnalyzeThreshold	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	200000
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB

Параметр	Описание	Значение по умолчанию
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
Параметры конфигурации роли JatobaStorage		
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorAgentHttpPort	Порт для доступа к коллектору OpenTelemetry в роли SqlStorage/JatobaStorage по протоколу HTTP	4319
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента Ankey SIEM NG Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage	–
Network	Сетевое имя реестра Docker-образов	storage-network.jatobastorage
NetworkDriver	Драйвер Docker-образов	bridge
PgAdminPort	Порт для доступа к PgAdmin	9001
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Параметр	Описание	Значение по умолчанию
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key

Таблица А.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 единовременно 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
ExpertDataUpdateMethod	Метод получения обновлений экспертных данных. Возможные значения: Online или Offline	–
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG MC	–
IamCookieLifetime	Время 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
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
PackageManagementPort	Номер порта сервиса управления пакетами Package Management	8585
PackagesSourceCredentialToken	Токен для авторизации на сервере обновлений. Хранится в файле instance-access-token.key и представляет собой набор символов, закодированных с использованием стандарта Base64	–

Параметр	Описание	Значение по умолчанию
PackagesSourceUri	Адрес сервера обновлений	–
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/Jatoba	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от ANKEY SIEM NG MC	5432
PostgreUserName	Логин служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL/Jatoba	pt_system
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	–
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	–

Таблица А.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 SIEM NG Server	Флажок установлен
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

Параметр	Описание	Значение по умолчанию
MCAddress	IP-адрес или FQDN сервера Ankey SIEM NG Management and Configuration	–
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/Jatoba	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL/Jatoba	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL/Jatoba для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL/Jatoba	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
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	Флажок установлен

Параметр	Описание	Значение по умолчанию
	параметров SmtpUser и SmtpPassword); флажок снят – для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword	
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	–
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Таблица А.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
ContentDeployerPort	Номер порта сервиса установки обновлений экспертизы Content Deployer	8586
DefaultAssetTtl	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	90.00:00:00
DefaultLocale	Интерфейс Ankey SIEM NG отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на SMTPсервер	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
KBAddress	IP-адрес или FQDN сервера Knowledge Base	–

Параметр	Описание	Значение по умолчанию
MCAddress	IP-адрес или FQDN сервера Ankey SIEM NG Management and Configuration	–
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL/Jatoba	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL/Jatoba	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Ankey SIEM NG Core	–
PostgreUserName	Логин служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL/Jatoba	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
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	mpx_core
SiemFrontendAddress	IP-адрес или FQDN сервера Ankey SIEM NG Server	–
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpIgnoreCertificateValidation	Ankey SIEM NG Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу	True
SmtpPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу	–

Параметр	Описание	Значение по умолчанию
SmtpPort	Порт SMTP-сервера для входящих подключений от Ankey SIEM NG Core	25
SmtpSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: None – шифрование не используется; Auto – почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; SslOnConnect – протоколы SSL или TLS используются при соединении; StartTls – протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; StartTlsWhenAvailable – протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	Auto
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpUser	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
UsePtbkServer	Ankey SIEM NG Core проверяет (флажок установлен) или не проверяет (флажок снят) наличие обновления базы знаний об уязвимостях в Knowledge Base	Флажок установлен
VulnerStateCheckInterval	Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)	01.00:00:00
VulnerStateCheckPeriodEnabled	Ankey SIEM NG Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей	Флажок установлен

Параметр	Описание	Значение по умолчанию
VulnerStateCheckPeriodEnd	Время окончания суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	01:00:00
VulnerStateCheckPeriodOfRetry	Продолжительность паузы (<Часы>:<Минуты>:<Секунды>) перед повторным запуском проверки, если предыдущий запуск завершился с ошибкой	00:01:00
VulnerStateCheckPeriodStart	Время начала суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	00:00:00

Таблица А.6 – Параметры конфигурации роли Collector

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

Параметр	Описание	Значение по умолчанию
	AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentName	Имя коллектора в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Collector
AgentRMQHost	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
AgentRMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector	5671
AgentRMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt

Параметр	Описание	Значение по умолчанию
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Collector 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

Таблица А.7 – Параметры конфигурации роли Events Storage

Параметр	Описание	Значение по умолчанию
BindHost	IP-адреса или FQDN сетевых интерфейсов сервера Ankey SIEM NG ES. **Примечание.** Elasticsearch обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы	0.0.0.0
ClientNodeHeapSize	Объем оперативной памяти, выделяемый для клиентского узла (в гигабайтах). **Примечание.** Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile	16g

Параметр	Описание	Значение по умолчанию
ClusterConfigurationProfile	Объем оперативной памяти, выделяемый каждому типу узлов кластера Elasticsearch. Для выбора доступны следующие варианты: – AIO – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для низконагруженных систем; – SIEMandStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для средненагруженных систем; – Standalone – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для высоконагруженных систем с потоком событий до 20000 в секунду; – ManagedStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для высоконагруженных систем с потоком событий выше 20000 в секунду; – Manual – ввод значений вручную (параметры DataNodeHeapSize, ClientNodeHeapSize, MasterNodeHeapSize)	Standalone
DataNodeHeapSize	Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах). **Примечание.** Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile	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	Объем оперативной памяти, выделяемый для главного узла (в гигабайтах).	16g

Параметр	Описание	Значение по умолчанию
	Примечание. Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile	
PathData	Путь к индексам Elasticsearch. Если Ankey SIEM NG развернут для высоконагруженных 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
PathRepo	Путь к резервным копиям индексов	/es_backup
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
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 А.8 – Параметры конфигурации роли Event Storage

Параметр	Описание	Значение по умолчанию
BindHost	IP-адреса или FQDN сетевых интерфейсов сервера Ankey SIEM NG ES. **Примечание.** LogSpace обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы	0.0.0.0
Database	Название базы данных хранилища LogSpace	siem
PathData	Корневой каталог хранилища LogSpace	/db_data
RotateCount	Максимальное количество сохраняемых файлов журналов	10
RotateSize	Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)	200M
SetRecomendedDiskScheduler	Для операций ввода-вывода ядро Linux использует планировщик по умолчанию (флажок снят) или планировщик deadline (флажок установлен)	Флажок установлен
TailcutterDbspace	Максимальный объем дискового пространства, выделяемый для разделов хранилища, 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 разделов для событий (в днях)	365
TailcutterTtlc	Срок хранения разделов для счетчиков событий (в днях)	7

Таблица А.9 – Параметры конфигурации роли SIEM Server

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ для подключения Ankey SIEM NG Server	mpx
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

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). **Примечание.** 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
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

Параметр	Описание	Значение по умолчанию
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
EventsCaseSensitiveSearch	Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False). **Примечание.** Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения	EventsCaseSensitiveSearch
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	0.0.0.0
GlobalRabbitHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** 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

Параметр	Описание	Значение по умолчанию
HighLoad	Для службы SIEM server storage выделено шесть (флажок установлен) или четыре (флажок снят) потока операционной системы	Флажок снят
HostAddress	IP-адрес или FQDN Ankey SIEM NG Server	–
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
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)	–

Параметр	Описание	Значение по умолчанию
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, сохранятся (флажок установлен) или не сохранятся (флажок снят) после перезагрузки брокера	Флажок установлен
RMQHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** 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

Параметр	Описание	Значение по умолчанию
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
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 стандарная (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 хралища событий используется Elasticsearch или LogSpace	elasticsearch
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (флажок установлен) или без него (флажок снят)	Флажок установлен
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 fptarestorer. Для выбора доступны следующие варианты: – 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
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица А.10 – Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
CACertFile	Имя файла корневого сертификата	rootCA.crt
CertFile	Имя файла публичного сертификата	RMQ_Server.crt
HostAddress	IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus	–
KeyFile	Имя файла закрытого ключа сертификата	RMQ_Server.pem
MEMORY_HIGH_WATERMARK_GB	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10
RMQAdminPassword	Пароль служебной учетной записи администратора RabbitMQ	P@ssword
RMQAdminUser	Логин служебной учетной записи администратора RabbitMQ	Administrator
RMQAgentPassword	Пароль служебной учетной записи для доступа коллекторов к RabbitMQ	P@ssword
RMQAgentUser	Логин служебной учетной записи для доступа коллекторов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671
RMQLogRotateSize	Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)	50M
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

Параметр	Описание	Значение по умолчанию
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). **Примечание.** Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица А.11 – Параметры конфигурации роли Retro Correlator

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

Параметр	Описание	Значение по умолчанию
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 коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentName	Имя коллектора 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 Collector	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
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Collector 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
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
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 коллектора на Debian	0.0.0.0
SiemServerAddress	IP-адрес или FQDN сервера Ankey SIEM NG Server	localhost

Приложение Б
Параметры конфигурации компонентов Ankey SIEM NG на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов Ankey SIEM NG на Microsoft Windows.

Таблица Б.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\Pki\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

Параметр	Описание	Значение по умолчанию
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
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

Параметр	Описание	Значение по умолчанию
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60
EventsCaseSensitiveSearch	Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False). **Примечание.** Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения	False
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	127.0.0.1
GlobalRabbitHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** 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	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

Параметр	Описание	Значение по умолчанию
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey SIEM NG Server\.install\scripts\Certificates\RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохранятся (True) или не сохранятся (False) после перезагрузки брокера	True
RMQHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** 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	5000

Параметр	Описание	Значение по умолчанию
	Server frontend из службы (в службу) SIEM Server commander	
SiemOnAgent	Установлена облегченная (True) или стандарная (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

Параметр	Описание	Значение по умолчанию
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
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица Б.2 – Параметры конфигурации компонента Ankey SIEM NG Collector

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	20480M free

Параметр	Описание	Значение по умолчанию
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 коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentName	Имя коллектора в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Collector
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 Collector\.install\scripts \Certificates\RMQ_Agent_Client.key

Параметр	Описание	Значение по умолчанию
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 Collector к RabbitMQ	P@ssword
RMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector	5671
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ	mpx_agent
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SSLEnabled	Ankey SIEM NG Collector подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение	True

Приложение В
Параметры проверок по чек-листу

В разделе приведены описания параметров и их значения по умолчанию.
Инструкция по изменению проверок приведена в разделе «Изменение проверок по чек-листу» (см. раздел 23).

Таблица В.1 − Параметры проверок по чек-листу

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
Значимость активов присваивается политикой	AM3-CriticalAssetsDEfined	valued_assets_absolute_amount	Минимальное количество выделенных активов	10
		valued_assets_definition	В качестве значимых учитываются активы: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	high
		valued_assets_minscope	Проверка учитывает (true) или не учитывает (false) минимальное количество выделенных активов	true
		asset_importance_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для присвоения значимости активов	true
Данные о значимых активах актуальны (аудит)	AM8-CriticalAssetsActualAudit	valued_assets_refresh_period	Максимальный период запуска задачи на сбор данных (в днях)	7
		valued_assets_definition	Задача собирает данные с активов: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	high

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		actual_valued_assets_amount	Максимальное количество неактуальных активов	3
		manual_asset_actuality_check	Проверка учитывает (true) или не учитывает (false) ручной контроль выполнения периодических задач сбора данных для обеспечения актуальных данных об активах, а также успешности их выполнения	true
		asset_actuality_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для сроков актуальности данных (аудит)	false
Данные о значимых активах актуальны (пентест)	AM9-CriticalAssetsActualPentest	valued_assets_refresh_period	Максимальный период запуска задачи на сбор данных (в днях)	7
		valued_assets_definition	Задача собирает данные с активов: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	high
		actual_valued_assets_amount	Максимальное количество неактуальных активов	3
		manual_asset_actuality_check	Проверка учитывает (true) или не учитывает (false) ручной контроль выполнения периодических задач сбора данных для обеспечения актуальных данных об активах, а также успешности их выполнения	true

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		asset_actuality_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для сроков актуальности данных (пентест)	false
Проводится расширенный аудит активов (Windows)	SM1-ExtAuditCriticalWindowsAssets	share_objects	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификаторами 5140 и 5145	true
		process_monitoring_powershell_operations	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификаторами 4103 и 4104	true
		process_monitoring_winevents	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификатором 4688 и события службы Microsoft Sysmon с идентификатором 1	true
		events_receive_interval	Максимальный период (в часах) между событиями, поступающими от одного и того же актива	120
		valued_assets_definition	Задача собирает данные с активов: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	any
		valued_assets_relative_amount	Минимальная доля (в процентах) от общего количества участвующих в проверке активов, с которых ожидается получение данных	95

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
Проводится расширенный аудит активов (Linux)	SM3-AuditDCriticalLinuxAssets	events_receive_interval	Максимальный период (в часах) между событиями, поступающими от одного и того же актива	120
		valued_assets_definition	Задача собирает данные с активов: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	any
Настроен мониторинг значимых источников событий	SM4-EventSourcesMonitoring	event_sources_monitoring	Задача собирает данные с активов: – любого уровня значимости – all; – только среднего и высокого уровня – any; – только среднего – medium; – только высокого – high	any
Общий параметр для всех проверок	–	check_period	Период (в минутах) запуска проверок и обновления их результатов в веб-интерфейсе	15

Приложение Г
Управление нормализацией событий с помощью команды drop

Примечание. Использование команды drop позволяет снизить общую утилизацию лицензии на сбор и обработку событий Ankey SIEM NG путем запрета нормализации событий, которые соответствуют условиям этой команды.

Команда drop используется для прекращения нормализации события. В результате срабатывания команды нормализованное событие не создается.

Использование команды drop актуально в тех случаях, когда поступает большое количество неинформативных с точки зрения информационной безопасности нормализованных событий, а настроить фильтрацию сырых событий не позволяет отсутствие данного функционала.

❖ Чтобы прекратить нормализацию конкретных событий, необходимо:

1. В главном меню приложения Ankey SIEM NG выберите раздел **События**.
   Откроется страница **События**.
2. В таблице событий выберите событие, нормализацию которого необходимо прекратить.
3. В панели **Сводка** перейдите в подраздел **Служебные данные**. Скопируйте id события.
4. Перейдите в приложение Knowledge Base.
5. Выберите пункт **Пакеты экспертизы** в разделе **SIEM**.
6. Нажмите кнопку , выберите фильтр **Текст правила**, введите ранее скопированный id и нажмите **Применить**.
7. Выберите полученное правило нормализации и нажмите кнопку **Создать копию**, как показано на рисунке Г.1
   Откроется код правила нормализации.

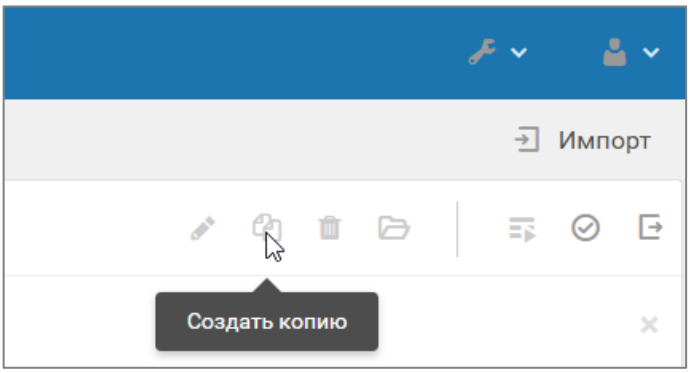


Рисунок Г.1 – Создание копии правила нормализации

8. Выполните одно из следующих действий:
   – если в правиле нормализации используется один идентификатор **detect**, то добавьте команду drop в конец строки, как показано на рисунке Г.2;

```
55
56 id = "GIS_kaspersky_lab_SM_auth_remote"
57
58 drop
59
```

Рисунок Г.2 - Добавление команды drop в конец строки

– если в правиле нормализации используется два и более идентификатора **detect**, а отбрасывать нужно определенный идентификатор, то команду необходимо добавить в блок кода, где выполняется присваивание идентификатора переменной **detect**, как показано на рисунке Г.3 и Г.4.

```
31 if $auth_type == "ntlm" then
32     msgid          = "SEC-LOGIN-002"
33     detect         = msgid
34     logon_service = "ntlm"
35 elif $auth_type == "krb" then
36     msgid          = "SEC-LOGIN-003"
37     detect         = msgid
38     logon_service = "kerberos"
39     drop
40 endif
```

Рисунок Г.3 – Добавление команды drop в блок кода if

```
291 subformula "json"
292     JSON = ''
293     COND = (
294     (lower($action) == "delete" or number($action) == 2) and
295     (in_list(["user", "users"], lower($resource)) == true or number($resource) == 0)
296     )
297
298     # Поля корреляционного события
299     $detect__msgid = "SEC-DELETE-001"
300
301     # Поля категоризации событий
302     $category__high = "User Management"
303     $category__low = "Deletion"
304
305     # Параметры взаимодействия
306     $action = "remove"
307     $status = "success" # Обязательное поле
308
309     # Поля, описывающие объект при взаимодействии
310     $object = "account" # Обязательное поле
311     $object__id = $item_id
312     $object__name = $item_name
313     if maybe_number($resource) == null then
314         $object__type = $resource
315     else
316         $object__type = number($resource)
317     endif
318
319     drop
320 endsubformula
```

Рисунок Г.4 – Добавление команды drop в блок кода subformula

9. Удалите из набора для установки стандартное правило нормализации, на основе которого была создана копия.
10. Добавьте в набор для установки созданную копию правила нормализации.
11. Нажмите кнопку **Установить в SIEM**.
    Нормализация события остановлена.

Приложение Д
Структурная схема проверки работоспособности правила корреляции

На рисунке Д.1 представлена структурная схема проверки работоспособности правила корреляции, которая подробно описана в подразделе 24.22.

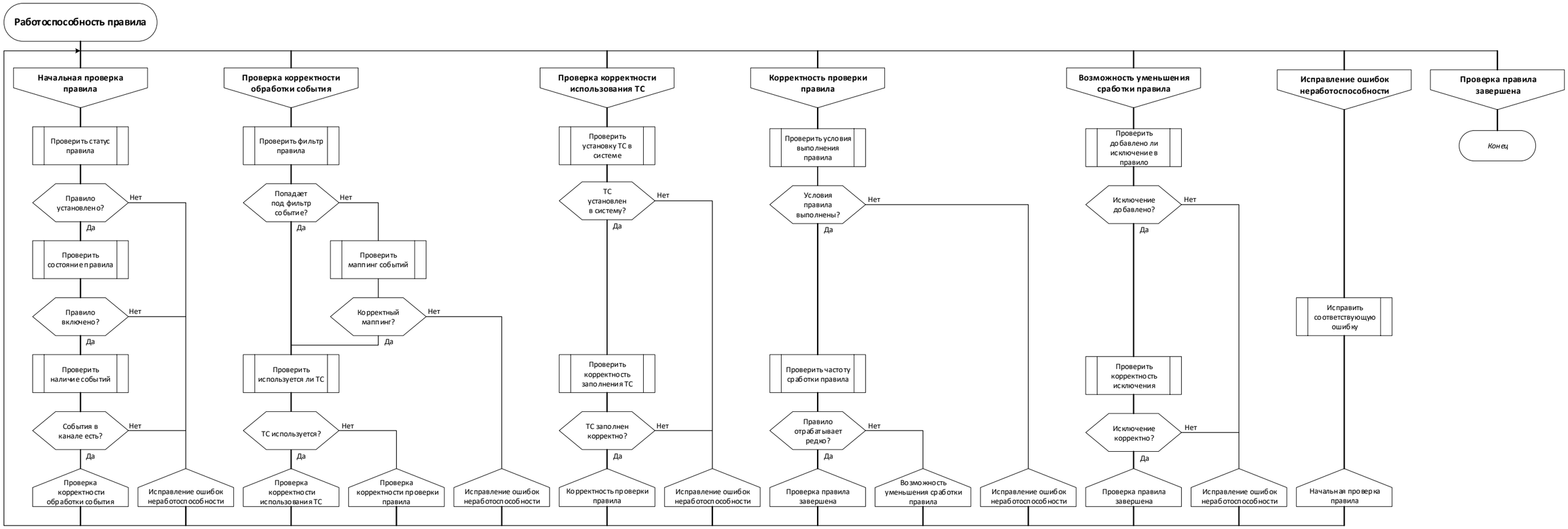
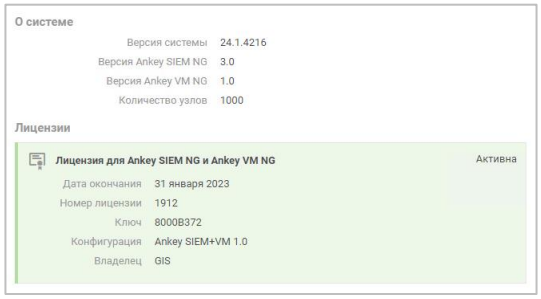
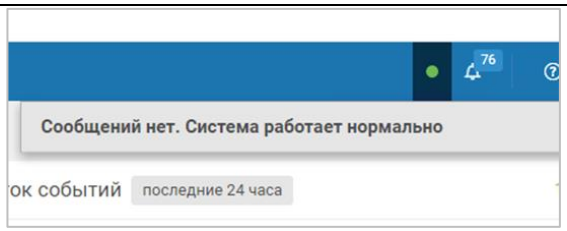


Рисунок Д.1 – Схема проверки работоспособности правила корреляции

Приложение Е
Формы обращения в техническую поддержку

В таблице Е.1 представлен пример формы обращения в техническую поддержку с общими параметрами. Данные параметры необходимо указать для всех трех направлений: платформа, коннекторы и контент.

Таблица Е.1 − Пример формы обращения в техническую поддержку с общими параметрами

Параметры	Описание	Пример
Наименование организации	Полное наименование организации	ООО "Аэрофлот"
Номер договора либо наименование объекта эксплуатации	Номер договора либо наименование объекта эксплуатации	Объект в г. Москва
Номер лицензии	Указать номер лицензии и сертификат технической поддержки − при наличии	12345678
Версия ПК Ankey SIEM NG	Версия платформы	5.2
Направление (принадлежность функционала)	Платформа, коннектор или контент	Коннектор
Состояние лицензии и версии компонента Ankey SIEM NG Core	Состояние (подтверждение) действующей лицензии для соответствующей версии компонента Ankey SIEM NG Core	
Состояние системы	Состояние системы с развернутой вкладкой уведомлений	 В случае нештатного состояния необходимо предоставление полной информации обо всех предупреждениях и ошибках

В таблице Е.2 представлен пример формы обращения в техническую поддержку с параметрами для направления платформа.

Таблица Е.2 − Пример формы обращения в техническую поддержку с параметрами для направления платформа

Параметры	Описание	Пример
Компонента платформы	Наименование компонента платформы. Заполняется всегда при обращении по платформе ПК Ankey SIEM NG	Ankey SIEM NG Server
Схема развертывания ПК	Низконагруженная или AIO (All in One) Средненагруженная Высоконагруженная	Низконагруженная
Описание неисправности	Подробное описание неисправности, сопутствующих обстоятельств, при которых она возникла (какие операции проводились, при каких условиях выполнялась работа и т. п.)	Описанная конфигурация поддерживается производителем. Настройки выполнены согласно документации. При этом не сервис «Normalizer» переходит в неактивное состояние с определенной периодичностью
Результаты диагностики	Выполненные действия по диагностике платформы с учетом раздела 24 данного руководства	Выполнены все действия по диагностике платформы. Результат: ….
Дополнительные сведения	Дополнительная информация, которая полезна производителю для анализа возникшей проблемы	Журналы работы платформы и другие материалы

В таблице Е.3 представлен пример формы обращения в техническую поддержку с параметрами для направления коннекторы.

Таблица Е.3 − Пример формы обращения в техническую поддержку с параметрами для направления коннекторы

Параметры	Описание	Пример
Наименования коннектора	Наименование коннектора (источника)	СрЗИ VipNet Policy Manager
Версия изделия[46]	Версия изделия – коннектора	3.1.45
Тип сбора	Тип сбора с источника	Syslog
Протокол взаимодействия	Протокол взаимодействия с источником, по которому выполняется сбор событий	tcp (514)
Среда функционирования источника данных	Наименование среды функционирования (ОС) источника	RedOS 7.2

[46] Для определения версии установленного коннектора см. пункт 24.21.5.

Параметры	Описание	Пример
Версия источника данных	Версия источника	4.2
Описание неисправности	Подробное описание неисправности, сопутствующих обстоятельств, при которых она возникла (какие операции проводились, при каких условиях выполнялась работа и т. п.)	Описанная конфигурация поддерживается производителем, при этом не выполняется обработка событий. Формат событий также поддерживается
Результаты диагностики	Выполненные действия по диагностике коннектора с учетом подраздела 24.20 данного руководства .	Выполнены все действия по диагностике коннектора. Результат: ….
Дополнительные сведения	Дополнительная информация, которая полезна производителю для анализа возникшей проблемы	Журнал работы задачи сбора данных, образцы событий источника (в исходном необработанном виде) и другие материалы

В таблице Е.4 представлен пример формы обращения в техническую поддержку с параметрами для направления контент.

Таблица Е.4 − Пример формы обращения в техническую поддержку с параметрами для направления контент

Параметры	Описание	Пример
Наименования коннектора	Наименование коннектора (источника)	СрЗИ VipNet Policy Manager
Пакет контента	Наименование пакета контента	Пакет общих ресурсов контента
Версия изделия [47]	Версия изделия − пакета контента	3.4.1
Используемая версия коннектора к источнику	Версия коннектора[48]	3.1.45
Тип сбора	Тип сбора с источника	Syslog
Протокол взаимодействия	Протокол взаимодействия с источником, по которому выполняется сбор событий	tcp (514)
Среда функционирования источника данных	Наименование среды функционирования (ОС) источника	RedOS 7.2
Версия источника данных	Версия источника	4.2

[47] Для определения версии пакета контента см. пункт 24.22.7.
[48] Коннекторы совместимы с определенными версиями пакетов контента.

Параметры	Описание	Пример
Описание неисправности	Подробное описание неисправности, сопутствующих обстоятельств, при которых она возникла (какие операции проводились, при каких условиях выполнялась работа и т. п.)	Описанная конфигурация поддерживается производителем, при этом не выполняется корреляция событий. Настройки контента выполнены в соответствии с документацией (настроены соответствующие зависимые ресурсы, - справочники данных (табличные списки), установлены параметры работы правил). Необходимые события для корреляции данных поступают в ПК Ankey SIEM NG с источников
Результаты диагностики	Выполненные действия по диагностике контента с учетом подраздела 24.22 данного руководства	Выполнены все действия по диагностике контента. Результат: ….
Дополнительные сведения	Дополнительная информация, которая полезна производителю для анализа возникшей проблемы	Выгрузка нормализованных событий источника, на которых не проводится корреляция, и другие материалы