

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

© ООО «Газинформсервис» с 2004 года

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

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

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

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

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

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

Дата редакции документа: 3 квартал 2023 года.

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

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

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

Содержание

1	Об этом документе	8
2	О ПК Ankey SIEM NG	11
2.1	Архитектура ПК Ankey SIEM NG	11
2.1.1	Компонент Ankey SIEM Next Generation Core	12
2.1.2	Компонент Ankey SIEM Next Generation Server	12
2.1.3	Компонент Ankey SIEM Next Generation Events Storage	12
2.1.4	Компонент Ankey SIEM Next Generation Agent	12
2.1.5	Компонент Ankey SIEM Next Generation Management and Configuration	13
2.1.6	Компонент Ankey SIEM Next Generation Knowledge Base	13
2.1.7	Компонент Ankey SIEM Next Generation Retro Correlator	13
2.2	Схема взаимодействия компонентов	13
3	Предоставление прав доступа	17
3.1	О приложениях Ankey SIEM NG Management and Configuration	17
3.2	Предоставление доступа к событиям	18
3.3	Предоставление доступа к активам, инцидентам и источникам	18
4	Распределенный поиск и репликация событий	20
4.1	Добавление связей для распределенного поиска	21
4.2	Удаление связи для распределенного поиска	22
4.3	Добавление правила репликации событий	22
4.4	Изменение правила репликации событий	23
4.5	Удаление правила репликации событий	23
5	Управление политиками	25
5.1	Страница Политики	25
5.2	Создание правила для значимости активов	26
5.3	Создание правила для сроков актуальности данных	27
5.4	Изменение правила	27
5.5	Копирование правила	27
5.6	Включение и отключение правила	28
5.7	Удаление правила	28
5.8	Применение изменений в политиках	28
5.9	Отмена изменений в черновике политики	29
6	Мониторинг источников событий	30
6.1	Просмотр списка источников и списка потоков событий от источника	31
6.2	Просмотр списка форвардеров и списка источников форвардера	32
6.3	Создание предупреждения для отслеживания наличия событий	32
6.4	Создание предупреждения для отслеживания средней скорости потока событий	33
6.5	Создание предупреждения для отслеживания задержки в получении события агентом	34
6.6	Остановка и повторный запуск отслеживания потока событий	34
6.7	Удаление источника (форвардера) из списка	35

6.8 Экспорт списка источников (форвардеров) в текстовый файл	36
6.9 Обновление списка источников (форвардеров).....	36
7 Мониторинг состояния ПК Ankey SIEM NG	37
7.1 Страница Управление системой	37
7.2 Удаление агента сбора событий из списка	39
7.3 Мониторинг работы правил корреляции.....	39
8 Резервное копирование данных.....	41
8.1 Создание резервной копии данных роли на Linux	41
8.2 Создание резервной копии индексов Elasticsearch на Linux	41
8.3 О резервном копировании данных о площадках и их связях.....	43
9 Восстановление данных из резервной копии	44
9.1 Восстановление данных компонентов Ankey SIEM NG на Linux из резервной копии	44
9.2 Восстановление индексов Elasticsearch из резервной копии на Linux	46
9.3 О восстановлении резервной копии данных о площадках и их связях	47
10 Индексы Elasticsearch: ротация, архивация, перемещение и удаление	48
10.1 Просмотр списка индексов	49
10.2 Настройка ротации индексов.....	49
10.3 Архивация индексов.....	49
10.3.1 Создание хранилища для архивных индексов.....	49
10.3.2 Архивация индексов на Linux	49
10.3.3 Настройка архивации индексов по расписанию	50
10.4 Восстановление индекса из архива	50
10.5 Удаление архивных индексов.....	51
10.5.1 Удаление архивных индексов на Linux.....	51
10.5.2 Удаление архивных индексов по расписанию	51
10.6 Удаление индекса без архивации	51
10.7 Перемещение индексов на Linux.....	52
11 Смена паролей служебных учетных записей	53
11.1 Смена пароля служебной учетной записи в PostgreSQL	53
11.2 Смена паролей служебных учетных записей в RabbitMQ	53
11.2.1 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Core на Linux.....	54
11.2.2 RabbitMQ: смена паролей служебных учетных записей компонента Ankey SIEM NG Server на Linux.....	54
11.2.3 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Agent на Linux	55
12 Настройка журналирования работы ПК Ankey SIEM NG	57
12.1 Настройка журналирования работы компонента Ankey SIEM NG Core	57
12.2 Настройка журналирования работы компонента Ankey SIEM NG Core на Linux	57
12.3 Настройка журналирования работы компонента Ankey SIEM NG Server.....	58
12.4 Настройка журналирования работы компонента Ankey SIEM NG Events Storage с Elasticsearch версии 7	58

12.5	Настройка журналирования работы компонента Ankey SIEM NG Agent на Microsoft Windows	59
13	Просмотр и изменение параметров конфигурации Ankey SIEM NG.....	61
13.1	Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux	61
13.1.1	Просмотр конфигурации роли.....	61
13.1.2	Изменение конфигурации роли.....	61
13.1.3	Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch.....	62
13.1.4	Изменение степени сжатия данных в Elasticsearch	62
13.2	Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Microsoft Windows	63
13.2.1	Просмотр конфигурации	64
13.2.2	Изменение конфигурации вручную.....	64
13.2.3	Изменение конфигурации с помощью XML-файла.....	64
14	Отключение отправки ненормализованных событий облегченной версией компонента Ankey SIEM NG Server («SIEM на агенте»)	65
15	Пользовательские поля в модели актива	66
15.1	Добавление пользовательских полей в модель актива	66
15.2	Добавление описания пользовательских полей	68
15.3	Изменение имен пользовательских полей	69
15.4	Удаление пользовательских полей из модели актива	70
16	Настройка категоризации.....	72
17	Управление модулями сбора и обработки данных, модулями выявления нарушений ИБ (корреляционной обработки данных)	74
17.1	Рекомендации по обновлению ресурсов	76
17.2	Алгоритм обновления ресурсов в эталонной базе данных до новой версии	77
17.3	Алгоритм обновления ресурсов в ветке Customer_Data	79
17.4	Алгоритм обновления отдельных ресурсов, полученных в рамках технической поддержки (hotfix).....	80
18	Работа с инфраструктурами	83
18.1	Создание инфраструктуры	83
18.2	Изменение названия инфраструктуры.....	83
18.3	Удаление инфраструктуры	83
19	Изменение проверок по чек-листу.....	85
20	Диагностика и решение проблем	86
20.1	Уведомления о состоянии системы	86
20.2	Обмен данными между компонентами системы	86
20.2.1	Вход в RabbitMQ.....	88
20.2.2	Мониторинг потока событий в RabbitMQ	88
20.2.3	Очередь storageq не уменьшается	88
20.2.4	Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается ..	89

20.2.5	Очередь storageq растёт и начинает уменьшаться только после появления ошибки.....	90
20.2.6	Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растёт и начинает уменьшаться только после появления ошибки.....	91
20.3	Мониторинг состояния RabbitMQ и Elasticsearch	92
20.3.1	Параметры конфигурации службы Core Watchdog.....	92
20.3.2	Параметры конфигурации службы SIEM Server health monitor	94
20.4	Ошибка "Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога"	97
20.5	Ошибка "Объем свободного места на диске, выделенном для SIEM Messaging Service, достиг критического порога	97
20.6	Ошибка "Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога".....	98
20.7	Ошибка "Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем"	99
20.8	Предупреждение "Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога".....	99
20.9	Индексы Elasticsearch находятся в состоянии red	100
20.10	Служба Elasticsearch останавливается через некоторое время после запуска	101
20.11	Система не получает данные от задачи.....	102
20.12	Отсутствуют события от источников.....	103
20.13	Задача аудита не собирает сведения об активах.....	104
20.14	Не приходят уведомления, отправляемые по электронной почте	105
20.15	Ошибка "Sdk пакет <Номер версии> поврежден. Необходимо восстановление".....	105
20.16	Не удается импортировать отчет из MaxPatrol 8	105
20.17	Настройка компонентов после изменения IP-адресов или FQDN их серверов.....	106
20.18	Диагностика коннекторов по сбору данных с источников событий.....	107
20.18.1	Диагностика источника событий (журналирование данных).....	108
20.18.2	Проверка функционирования ПК Ankey SIEM NG	110
20.18.3	Диагностика работы коннектора	110
20.18.4	Версия дополнительного коннектора	113
20.19	Диагностика пакетов контента.....	114
20.19.1	Начальная проверка правила корреляции.....	115
20.19.2	Проверка корректности обработки события.....	127
20.19.3	Проверка корректности использования табличного списка	130
20.19.4	Корректность проверки правила	133
20.19.5	Возможность уменьшения срабатываний правил корреляции.....	138
20.19.6	Дополнительная информация.....	140
20.19.7	Версия пакета контента.....	140
20.20	Не все зависимые ресурсы загружены в систему и/или добавлены в	

набор установок	141
20.21 Справочная информация.....	142
20.21.1 Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки	143
20.21.2 Сбор информации о нагрузке на файловую систему и запущенных процессах.....	143
20.21.3 Просмотр статуса службы	143
20.21.4 Проверка доступности сетевого порта сервера.....	143
20.21.5 Просмотр состояния индексов Elasticsearch	143
20.21.6 Просмотр состояния Elasticsearch	144
20.21.7 Создание дампа памяти процесса	144
20.21.8 Создание аварийного дампа памяти на Microsoft Windows	144
20.21.9 Расположение индексов Elasticsearch	145
20.21.10 Расположение файлов журналов.....	145
21 Обращение в службу технической поддержки	148
21.1 Требования к содержанию заявки.....	148
21.2 Порядок регистрации и учета заявок	149
21.3 В техническую поддержку входит.....	151
21.4 Ограничения в предоставлении услуг технической поддержки	152
Перечень сокращений.....	156
Приложение А Параметры конфигурации компонентов Ankey SIEM NG на Linux	160
Приложение Б Параметры конфигурации компонентов Ankey SIEM NG на Microsoft Windows	182
Приложение В Параметры проверок по чек-листу.....	191
Приложение Г Справочник категорий	195
Г.1 Значения полей с типом данных Enum	195
Г.2 Правила заполнения полей category.high, category.low	200
Г.3 Правила заполнения полей category.generic	205
Приложение Д Структурная схема проверки работоспособности правила корреляции.....	207
Приложение Е Формы обращения в техническую поддержку.....	208

1 Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию 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
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию и инструкции по настройке и администрированию продукта
	Руководство оператора Ankey SIEM NG	Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности
	Руководство по инсталляции Ankey SIEM NG	Содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
	Руководство администрирования Ankey SIEM NG Management and Configuration	Содержит справочную информацию и инструкции по настройке и администрированию компонента Ankey SIEM NG Management and Configuration
	Руководство по настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker
Подключение источников	Руководство по интеграции с источниками Ankey SIEM NG	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников и аудита активов
	Руководство по интеграции с источниками Ankey SIEM NG. Приложение А	Содержит перечни регистрируемых событий, маппинг событий и результаты обработки для поддерживаемых источников пакета стандартных коннекторов ПК Ankey SIEM NG

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

В документе приняты условные обозначения.

Таблица 1.2 – Условные обозначения

Пример	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

Пример	Описание
Нажмите кнопку OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <code>Stop-Service</code>	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
<code>Ctrl+Alt+Delete</code>	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.

ПК Ankey SIEM NG предоставляет следующие основные возможности:

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

ПК Ankey SIEM NG предоставляет также дополнительные возможности:

- **пакеты экспертизы.** Использование базы знаний, разработанной экспертами ООО «Газинформсервис». База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки;
- **автоматизация работы с активами.** Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования 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.

2.1 Архитектура ПК Ankey SIEM NG

Ankey SIEM NG состоит из программных компонентов, которые возможно размещать как на одном сервере, так и на нескольких. Гибкая архитектура позволяет масштабировать и внедрять Ankey SIEM NG в организации с ИТ-

инфраструктурами разных масштабов. Если поток событий в Ankey SIEM NG превышает 3000 событий в секунду, то требуется распределенная установка компонентов ПК Ankey SIEM NG.

2.1.1 Компонент Ankey SIEM Next Generation Core

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

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

2.1.2 Компонент Ankey SIEM Next Generation Server

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

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

2.1.3 Компонент Ankey SIEM Next Generation Events Storage

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

2.1.4 Компонент Ankey SIEM Next Generation Agent

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

Ankey SIEM NG Agent собирает следующую информацию об активах:

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

- параметрах сети и средств защиты.

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

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

2.1.5 Компонент Ankey SIEM Next Generation Management and Configuration

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

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

2.1.6 Компонент Ankey SIEM Next Generation Knowledge Base

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

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

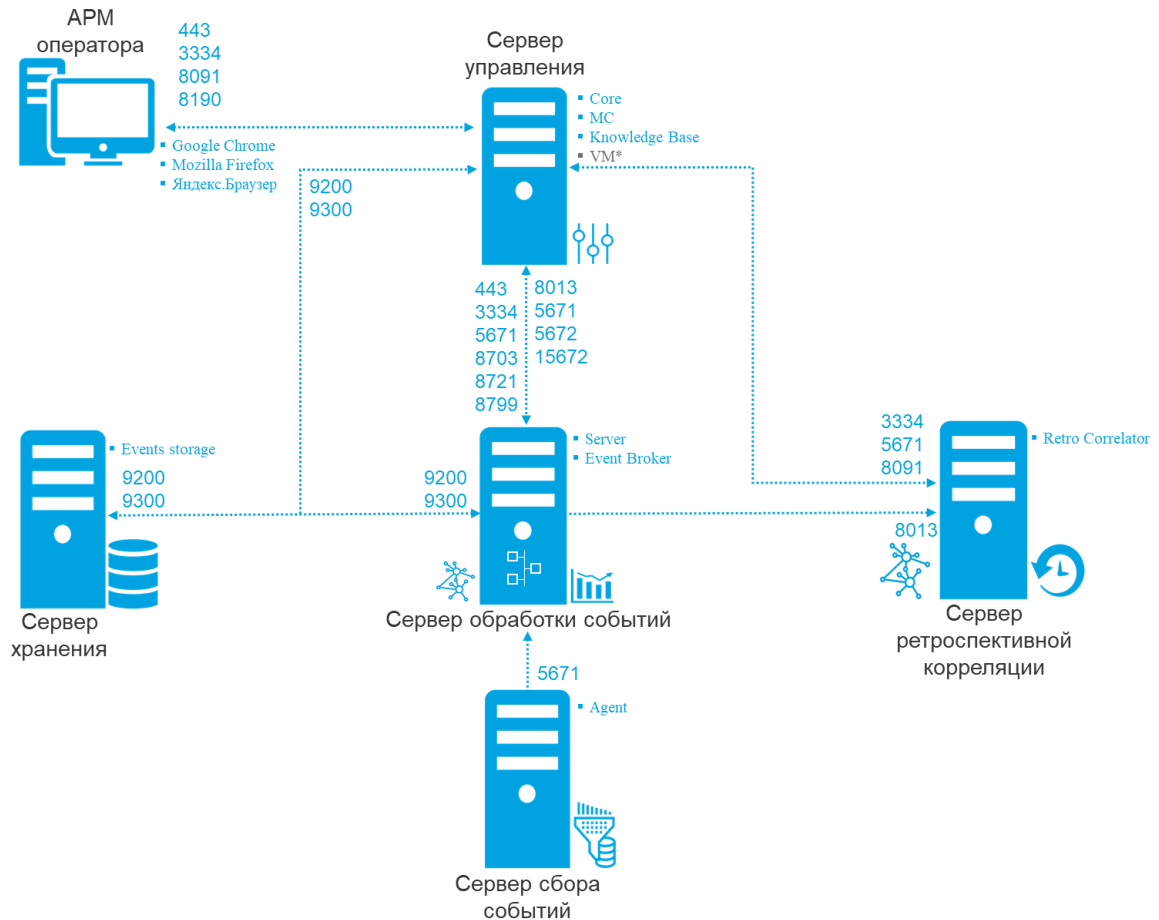
Примечание. Описание модулей сбора и обработки данных и модули выявления нарушений ИБ (корреляционной обработки данных) представлено в разделе 17.

2.1.7 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.

2.2 Схема взаимодействия компонентов

Взаимодействие компонентов ПК Ankey SIEM NG отражено на рисунке 2.1.



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

Рисунок 2.1 – Схема взаимодействия компонентов ПК Ankey SIEM NG¹

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Agent сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и события с источников. Собранные данные агенты передают в Ankey SIEM NG Server и 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. Собранные события передаются на Ankey SIEM NG Server для нормализации, агрегации, обогащения и корреляции.

¹ При наличии дополнительного модуля Ankey SIEM NG VM для обновления базы данных уязвимостей может использоваться дополнительный компонент Ankey SIEM NG UCS. Для обновления баз данных модули Salt Minion инициируют подключение к модулю Salt Master на сервере Ankey SIEM NG UCS, используя TCP-порты 4505 и 4506.

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

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

4. Компонент Knowledge Base содержит базу знаний, необходимых Ankey SIEM NG для структурирования сведений, собранных от источников событий и объектов инфраструктуры.
5. Компонент Ankey SIEM NG 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 2.1.

Таблица 2.1 – Компоненты и порты взаимодействия

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

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

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

- через порт 3389/TCP (протокол RDP) – к серверу под управлением ОС Windows Server 201x с установленным компонентом Ankey SIEM NG Agent;
- через порт 22/TCP – к серверам под управлением ОС Linux-like с установленными компонентами ПК Ankey SIEM NG.

3 Предоставление прав 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 получают 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.

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. Подробная информация об учетных записях пользователей, их ролях и привилегиях, а также инструкции по работе с ними приведены в руководстве администрирования Ankey SIEM NG Management and Configuration 4.1.2.

3.1 О приложениях Ankey SIEM NG Management and Configuration

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**.

3.2 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.

3.3 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 Распределенный поиск и репликация событий

После создания связей между площадками (подробное описание см. в Руководстве администрирования Ankey SIEM NG Management and Configuration 4.1.2) вы сможете настроить связи между приложениями Ankey SIEM NG, предназначенные для выполнения следующих задач.

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. Указать IP-адрес или FQDN сервера Ankey SIEM NG Events Storage в качестве значения параметра ClusterSeedHost компонента Ankey SIEM NG Server.

3. Если компонент Ankey SIEM NG Core установлен на Linux – повторно запустить его настройку:

`/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId Core.`

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

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.

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

5 Управление политиками

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 ПК Ankey SIEM NG предусмотрен механизм для автоматизации контроля за регулярностью сканирования активов – политики. Политика состоит из совокупности правил, которые автоматически устанавливают значимость или 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.

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), применяются 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 применяются изменения, внесенные тем пользователем, который последним работал с черновиком.

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

5.1 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 5.4);
- **Копировать** – для создания правила на основе имеющегося правила (см. подраздел 5.5);
- **Удалить** – для удаления правила (см. подраздел 5.7);
- **Включить** – для включения правила в работу (см. подраздел 5.6);
- **Отключить** – для приостановки работы правила (см. подраздел 5.5).

В рабочей области страницы расположены:

- панель **Список политик**. Содержит список политик и предназначена для выбора политики, применения изменений (см. подраздел 5.8, а также отмены не примененных изменений (см. подраздел 5.9). 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.

5.2 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 5.8).

5.3 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 5.8).

5.4 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 5.8).

5.5 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 5.7).

5.6 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 5.7).

❖ 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 5.7).

5.7 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 5.7).

5.8 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.

5.9 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.

6 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 форвадера).

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

6.1 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 агентом. 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.

6.2 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 агентом. 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.

6.3 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.

6.4 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.

6.5 Создание предупреждения для отслеживания задержки в получении события агентом

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

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 агентом.
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 агентом запущено.


6.6 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.


2. В панели инструментов нажмите кнопку **Отключение предупреждения**.
3. 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.

6.7 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 агентом.
4. Нажмите кнопку **Сохранить**.
5. Нажмите кнопку **Удалить источник** или кнопку **Удалить форвардер** и подтвердите удаление.

Источник (форвардер) удален из списка.

6.8 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.

6.9 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.

7 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 цветové индикаторы уровня опасности события:

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

7.1 Страница Управление системой

Страница **Управление системой** предназначена для просмотра состояния лицензии, управления агентами 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 агентов.

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).

Слева от доменного имени сервера Ankey SIEM NG Server главного конвейера отображается значок . 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 агенты, а также единственный конвейер в списке.

Агенты

Раздел предназначен для просмотра подробной информации об агентах, для обновления их версий и удаления недоступных агентов. При выборе раздела в центральной панели отобразится таблица с агентами. Для каждого агента 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 агента в списке вы можете нажать  и ввести в поле поиска параметр агента.

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

В таблице отображаются следующие статусы агента:

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

В панели инструментов находятся следующие кнопки:

- **удалить** – для удаления недоступного агента (см. подраздел 7.2). Если после удаления агент начнет присылать данные, он снова будет отображаться в списке;
- **обновить версию** – для обновления версии агента.

База знаний

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

7.2 Удаление агента сбора событий из списка

Агент, который был установлен в системе, а затем выведен из ее состава (например, по причине неисправности сервера агента), автоматически не удаляется из списка агентов и продолжает отображаться в интерфейсе со статусом **Недоступен**. Такой агент необходимо удалить из списка вручную. После удаления агента будут автоматически остановлены:

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

❖ Чтобы удалить агент 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 **Агенты**.
В рабочей области страницы отобразится таблица со списком агентов.
3. Выберите агент 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 агент используется запущенными задачами сбора событий.

Статус удаляемого агента изменится на **Удаляется**. По завершении удаления агент не будет отображаться в списке. Агент сбора событий удален из списка.

7.3 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`).

8 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. 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 агентами во время создания копии, не отправляются другим компонентам системы и накапливаются на серверах агентов. По завершении создания копии эти данные будут отправлены одновременно всеми агентами, 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.

8.1 Создание резервной копии данных роли на Linux

❖ 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`.

8.2 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` регистрирует 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.

8.3 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.

9 Восстановление данных из резервной копии

Вы можете восстанавливать данные 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. 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 экземпляра 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.

9.1 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 Agent и повторная активация лицензии, подробнее см. документ Руководство по инсталляции Ankey SIEM NG 4.1.2.

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** → **Management and Configuration** → **Knowledge Base** → **RMQ Message Bus** → **Core** → **SIEM Storage** → **SIEM Server** → **Agent** выполните сценарий:

```
cd /opt/deployer/bin ./Install-RolePackage.ps1 -ManifestPath <Путь к  
файлам дистрибутива роли>/package.yaml
```

Например:

```
./Install-RolePackage.ps1 -ManifestPath  
/home/Roles/SqlStorage_1.0.3218/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/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
```

Данные компонентов восстановлены.

9.2 Восстановление индексов Elasticsearch из резервной копии на Linux

Если в системе запущена задача архивации индексов по расписанию, перед восстановлением индексов из 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 восстановить индексы Elasticsearch из резервной копии на Linux:

1. Укажите путь к каталогу с резервной копией индексов:

```
/opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу с резервной копией индексов>"
```

Утилита `es_initrepo` регистрирует в Elasticsearch хранилище резервной копии индексов и свяжет его с указанным каталогом. После регистрации хранилища интерфейс терминала 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. Восстановите индексы из файла резервной копии:
 - если требуется восстановить индексы, созданные в определенную дату, выполните команду:
`/opt/estools/bin/es_backup_tool -cmd restore -host 127.0.0.1 -port 9200 -arc snapshot_<Дата создания индексов>`
 - если требуется восстановить все индексы из резервной копии, выполните команду:
`/opt/estools/bin/es_backup_tool -cmd full_restore -host 127.0.0.1 -port 9200`

После восстановления данных из файла интерфейс терминала Linux 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 Debian.

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

9.3 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.

10 Индексы Elasticsearch: ротация, архивация, перемещение и удаление

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.

10.1 Просмотр списка индексов

❖ Чтобы просмотреть список индексов, используемых системой, выполните команды:

- в интерфейсе терминала Linux:
`/opt/estools/bin/es_backup_tool -cmd listindex`

❖ Чтобы просмотреть список архивных индексов, выполните команды:

- в интерфейсе терминала Linux:
`/opt/estools/bin/es_backup_tool -cmd listarchive`

10.2 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 `TailcutterDbospace`).

10.3 Архивация индексов

Вы можете запускать архивацию индексов вручную или настроить архивацию по расписанию. Перед архивацией индексов необходимо создать для них хранилище (см. пункт 10.3.1).

10.3.1 Создание хранилища для архивных индексов

❖ Чтобы создать хранилище для архивных индексов, выполните команды:

- в интерфейсе терминала Linux:
`/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 ptsiem_backup created successfully.`

10.3.2 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>
```

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>
```

10.3.3 Настройка архивации индексов по расписанию

❖ Чтобы настроить архивацию индексов по расписанию, создайте задачу:

– в планировщике заданий cron на Linux:

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

```
<Логин служебной учетной записи ОС> – NT  
AUTHORITY\LOCALSERVICE или  
NT AUTHORITY\NETWORKSERVICE;
```

```
<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) – 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 создать задачу:

– в планировщике заданий cron на Linux:

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

10.4 Восстановление индекса из архива

❖ Чтобы восстановить индекс из архива, выполните команды:

– интерфейсе терминала Debian:

```
/opt/estools/bin/es_backup_tool -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.

10.5 Удаление архивных индексов

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

10.5.1 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>
```

10.5.2 Удаление архивных индексов по расписанию

❖ Чтобы настроить удаление архивных индексов по расписанию, создайте задачу:

- в планировщике заданий cron на Linux:
<Расписание> /opt/estools/bin/es_backup_tool -cmd cleanarchive -
t <Дней до удаления> >> /opt/estools/log/es_backup.log где:
<Логин служебной учетной записи ОС> – NT
AUTHORITY\LOCALSERVICE или
NT AUTHORITY\NETWORKSERVICE;
- <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) – 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 создать задачу:

- в планировщике заданий cron на Linux:
30 2 * * 7 /opt/estools/bin/es_backup_tool -cmd cleanarchive -t 100
>> /opt/estools/log/es_backup.log

10.6 Удаление индекса без архивации

❖ Чтобы удалить индекс, выполните команды:

- если для средненагруженных или высоконагруженных систем – в интерфейсе терминала Linux:

```
/opt/estools/bin/es_backup_tool -cmd deleteindex --index <Тип  
индекса>_<Дата создания>
```

- если для сверхнагруженных – в интерфейсе терминала Linux:

```
/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.

10.7 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:
/var/lib/deployer/role_packages/ankey_SiemStorage_<Номер версии>/install.sh
 6. В открывшемся окне нажмите кнопку **Yes**.
 7. В открывшемся окне выберите вариант с идентификатором приложения Ankey SIEM NG.
 8. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Storage.
Откроется окно для проверки и изменения параметров.
 9. Выберите вариант **Basic configuration**.
Откроется страница со списком параметров.
 10. Измените значение параметра PathData:
PathData: <Путь к каталогу нового хранилища>
 11. Нажмите кнопку **OK**.
По завершении изменения конфигурации появится сообщение Deployment configuration successfully applied.
 12. Нажмите кнопку **OK**.
 13. На сервере Ankey SIEM NG Server запустите службу SIEM Server storage:
systemctl start siemserver-storage
 14. На сервере Ankey SIEM NG ES запустите все службы Elasticsearch:
systemctl --all start elasticsearch_*
 15. Запустите остановленные задачи.Индексы перемещены.

11 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).

11.1 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 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.

11.2 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 Agent, установленных на одном сервере ("SIEM на агенте").

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, высоконагруженных и сверхнагруженных 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.

11.2.1 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 экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
docker-compose down
docker-compose up -d

Пароль изменен.

11.2.2 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.

11.2.2.1 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 экземпляра 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.

11.2.2.2 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 экземпляра 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 экземпляра 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.

11.2.3 RabbitMQ: смена пароля служебной учетной записи компонента Ankey SIEM NG Agent на Linux

По умолчанию логин служебной учетной записи компонента Ankey SIEM NG Agent 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 Core:
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 Agent измените конфигурацию роли Agent:**
AgentRMQPassword: <Новый пароль>

Пароль изменен.

12 Настройка журналирования работы ПК Ankey SIEM NG

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

12.1 Настройка журналирования работы компонента Ankey SIEM NG Core

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. Настройка выполняется отдельно для каждой службы компонента Ankey SIEM NG Core.

❖ Чтобы настроить журналирование работы компонента Ankey SIEM NG Core, в файле конфигурации для параметров `log4net → root → level`, `log4net → appender name="FileAppender" → maxSizeRollBackups` и `log4net → appender name="FileAppender" → maximumFileSize` измените значение атрибута `value`:

```
<level value="<Уровень журналирования>" />
```

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

```
<maxSizeRollBackups value="<Максимальное количество сохраняемых файлов журналов>" />  
<maximumFileSize value="<Максимальный размер файла журнала (в мегабайтах)>MB" />
```

При обновлении системы значения всех параметров журналирования будут автоматически изменены на значения по умолчанию.

12.2 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. Возможны 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.

12.3 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:

- если компонент установлен на Linux – 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. Возможны 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. Перезапустите службу, параметры журналирования которой были изменены:
 - если Ankey SIEM NG Server установлен на Linux, в интерфейсе терминала от имени суперпользователя (`root`) выполните команду:
`systemctl siemserver-<Название службы>.service restart`

Журналирование настроено.

12.4 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:

- если на Linux – 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. Перезапустите службы Elasticsearch:
 - если Ankey SIEM NG Events Storage установлен на Linux, в интерфейсе терминала от имени суперпользователя (`root`) выполните команду:
`systemctl --all restart elastic*service`

Журналирование настроено.

12.5 Настройка журналирования работы компонента Ankey SIEM NG Agent 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 Agent\agent.log.xml`, который находится на сервере Ankey SIEM NG Agent.

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 агента> 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 Agent и их компонентов. Оно настраивается с помощью справочников ПК Ankey SIEM NG (подробное описание см. в Руководстве по интеграции с источниками Ankey SIEM NG 4.1.2).

13 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.

13.1 Просмотр и изменение конфигурации компонентов Ankey SIEM NG на Linux

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

13.1.1 Просмотр конфигурации роли

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

13.1.2 Изменение конфигурации роли

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

13.1.3 Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch

- ❖ Чтобы изменить объем оперативной памяти:
 1. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/<Название роли SIEM Storage>/install.sh`
 2. В открывшемся окне нажмите кнопку **Yes**.
 3. В открывшемся окне выберите вариант с идентификатором приложения роли.
 4. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
 5. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение 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. Суммарный объем оперативной памяти всех узлов кластера, умноженный на коэффициент 1,7, не должен превышать объем оперативной памяти сервера Ankey SIEM NG ES.

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

13.1.4 Изменение степени сжатия данных в Elasticsearch

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

- ❖ Чтобы выбрать алгоритм сжатия данных:
 1. На сервере с установленной ролью Deployer запустите сценарий:
`/var/lib/deployer/role_packages/<Название роли SIEM Storage>/install.sh`
 2. В открывшемся окне нажмите кнопку **Yes**.
 3. В открывшемся окне выберите вариант с идентификатором приложения роли.
 4. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
 5. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение 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 **ОК**.
Начнется изменение конфигурации роли.
По его завершении появится сообщение `Deployment configuration successfully applied`.
 - 8. Нажмите кнопку **ОК**.
- Алгоритм сжатия данных выбран и будет применен к новым индексам.

13.2 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 13.1 – Список компонентов и поставляемых с ними утилит

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

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

Таблица 13.2 – 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

13.2.1 Просмотр конфигурации

❖ Чтобы просмотреть конфигурацию, выполните команду:

```
<Название утилиты> get -p <Название параметра 1> <Название параметра 2> ...  
<Название параметра N>
```

Например:

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

13.2.2 Изменение конфигурации вручную

❖ Чтобы изменить конфигурацию вручную, выполните команду:

```
<Название утилиты> set -p <Название параметра 1> <Значение параметра 1>  
<Название параметра 2> <Значение параметра 2> ... <Название параметра N>  
<Значение параметра N>
```

Например:

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

13.2.3 Изменение конфигурации с помощью XML-файла

❖ Чтобы изменить конфигурацию с помощью XML-файла:

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

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

2. Выполните команду:

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

Конфигурация изменена.

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

По умолчанию компонент Ankey SIEM NG Server, установленный на сервере Ankey SIEM NG Agent, 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 Windows, 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 Linux, используйте для перезапуска команду `systemctl restart siemserver-normalizer.service`

Отправка ненормализованных событий отключена.

15 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:

- если Ankey SIEM NG Core установлен на Linux – в каталоге `/var/lib/deployed-roles/ <Идентификатор приложения Ankey SIEM NG>/<Название экземпляра роли Core>/config/user_model/`.

15.1 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:

- если Ankey SIEM NG Core установлен на Linux – 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 15.2).
6. Перезапустите следующие службы.
Если `Ankey SIEM NG Core` установлен на `Linux`, выполните команду:

```
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.

15.2 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. Если Ankey SIEM NG Core установлен на Linux – 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.

15.3 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_AssetNumber"
NewName="UF_AssetNumber"/>
    <RenameProperty Property="UF_AssetOwner"
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.

15.4 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.

16 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 16.1) 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 16.1 – Схема полей событий

Название поля	Обязательное заполнение	Тип данных	Описание поля
Поля категоризации событий			
category.generic	Нет	String	Уровень категоризации generic (см. Приложение Г таблицу Г.7)
category.high	Нет	String	Уровень категоризации high (см. таблицу Г.6)
category.low	Нет	String	Уровень категоризации low (см. Приложение Г таблицу Г.6)
Поле, описывающие источник события			
event_src.category	При нормализации	Enum ¹	Категория источника события (см. Приложение Г таблицу Г.5), например IDS/IPS, Firewall, Mail server
Параметры взаимодействия			
action	Обязательно	Enum ¹	Характер воздействия на объект (см. Приложение Г таблицу Г.1)
status	Обязательно	Enum ¹	Конечный результат воздействия (см. Приложение Г таблицу Г.3)

Название поля	Обязательное заполнение	Тип данных	Описание поля
Поле, описывающие субъект при взаимодействии			
subject	Нет	Enum ¹	Субъект воздействия (см. Приложение Г таблицу Г.4)
Поле, описывающие объект при взаимодействии			
object	Обязательно	Enum ¹	Объект воздействия (см. Приложение Г таблицу Г.2)
¹ Enum – это тип данных, чье множество значений представляет собой ограниченный список идентификаторов.			

Справочник значений категорий представлен в приложении Г.

Пример категоризации события Kaspersky Security Center об обнаруженном бэкдоре представлен в таблице 16.2.

Таблица 16.2 – Классификация события

Категория	Значение
Category.generic	Warning
Subject	Application
Action	Found
Object	Malware
Event_src.category	Antivirus
Status	Success
Category.high	Backdoor
Category.low	Detection

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

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

Примечание. Номер версии² дополнительных коннекторов Ankey SIEM NG и пакетов контента Ankey SIEM NG имеет формат A.B.C, где A – минимально поддерживаемая версия платформы Ankey SIEM NG, B – мажорная версия изделия, C – минорная версия изделия. Например: 4.2.1.

Примечание. Дополнительные контент и коннекторы версии 3.x совместимы с платформой ПК Ankey SIEM NG 4.x.

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 событий³;

Внимание! Установка стандартных коннекторов Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 4.1.2». Настройка сбора событий от стандартных источников в Ankey SIEM NG описана в «Руководстве по интеграции с источниками Ankey SIEM NG 4.1.2».

- дополнительные коннекторы, предназначенные для интеграции ПК Ankey SIEM NG с нестандартными источниками событий⁴, которые не поддерживаются платформой Ankey SIEM NG (не являются «коробочным» решением).

² Для определения версии установленного коннектора см. пункт 20.18.4, для определения версии пакета контента см. пункт 20.19.7.

³ Список поддерживаемых стандартных источников приведен в документе «Обзор новых возможностей Ankey SIEM NG 4.1.2».

⁴ Список поддерживаемых нестандартных источников приведен в документе «Руководство по интеграции с источниками Ankey SIEM NG 4.1.2».

Внимание! Установка дополнительных коннекторов Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 4.1.2». 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 4.1.2». 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.

Внимание! Установка дополнительных пакетов контента Ankey SIEM NG описана в «Руководстве по инсталляции Ankey SIEM NG 4.1.2». Настройка дополнительных пакетов контента в Ankey SIEM NG описана в документации на использование дополнительного пакета контента, которая поставляется в рамках приобретения такого изделия.

17.1 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 17.1.
3. Выбрать инструмент  **Экспорт**.



Рисунок 17.1 – 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 17.2. 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.

Ошибка Табличный список с названием:
'COMMON_Tracking_Exceptions_copy' не содержит
поле с названием 'some_field'

Рисунок 17.2 – 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>"
```

17.2 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 17.3.

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.

Импорт объектов [X]

< Выбрать другой файл

Файл GIS_KB.kb готов к импорту

Параметры импорта

Добавить и обновить объекты из файла
Все объекты из файла добавятся как пользовательские. Существующие в системе объекты будут заменены, в том числе записи табличных списков.

Добавить объекты Газинформсервис как стандартные
Будут импортированы только объекты Газинформсервис. Новые объекты добавятся, существующие будут заменены.

Синхронизировать объекты Газинформсервис с содержимым файла
Будут импортированы только объекты Газинформсервис. Существующие объекты будут заменены на объекты из файла, а объекты, которых нет в файле, будут удалены из системы.

Импортировать макросы Газинформсервис

Импортировать Отмена

Рисунок 17.3 – Параметры импорта ресурсов для базы данных GIS_DB

- 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.

- Далее необходимо выполнить импорт остальных пакетов экспертизы. Очередность в данном случае не имеет значения.
- Последующий импорт выполняется аналогично пункту 4 с параметрами, указанными на рисунке 17.4.

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.

Импорт объектов

< [Выбрать другой файл](#)

Файл **GIS_KB.kb** готов к импорту

Параметры импорта

Добавить и обновить объекты из файла
Все объекты из файла добавятся как пользовательские. Существующие в системе объекты будут заменены, в том числе записи табличных списков.

Добавить объекты Газинформсервис как стандартные
Будут импортированы только объекты Газинформсервис. Новые объекты добавятся, существующие будут заменены.

Синхронизировать объекты Газинформсервис с содержимым файла
Будут импортированы только объекты Газинформсервис. Существующие объекты будут заменены на объекты из файла, а объекты, которых нет в файле, будут удалены из системы.

Импортировать макросы Газинформсервис

Импортировать

Рисунок 17.4 – 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**.

17.3 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 4.1.2».

17.4 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 17.2 пункту 4 с параметрами приведенными на рисунке 17.5.

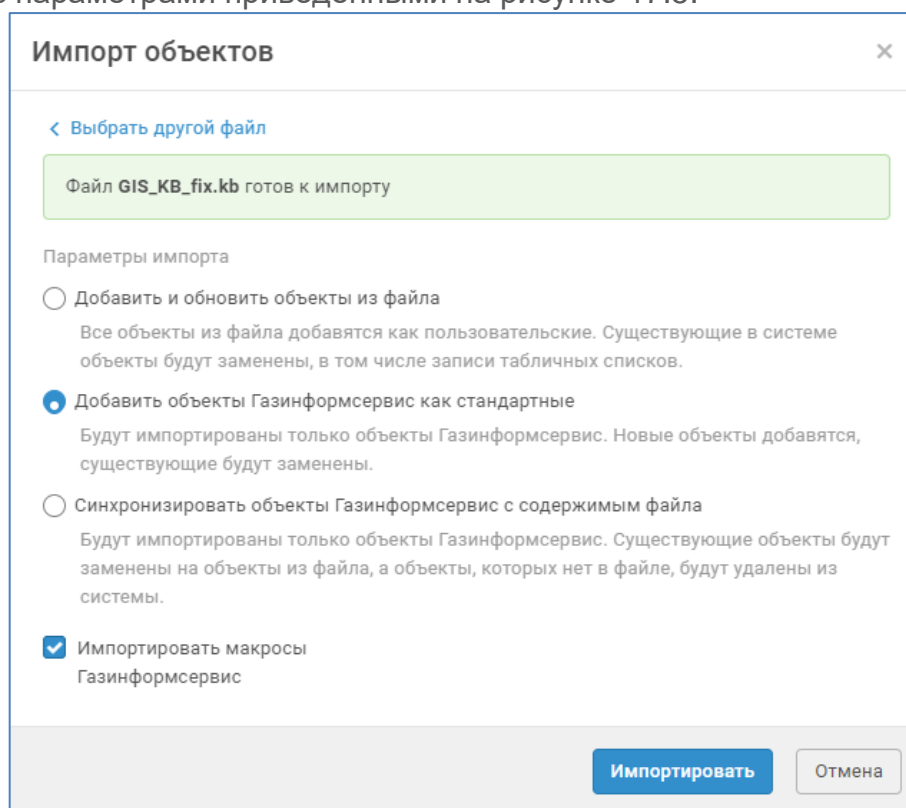


Рисунок 17.5 – Окно импорта hotfix

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 17.3.

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 21.

18 Работа с инфраструктурами

При сканировании ИТ-инфраструктуры предприятия важно правильно идентифицировать активы. Сканирование одним агентом 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 агентом 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**.

18.1 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.

18.2 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.

18.3 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.

19 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`.
 2. В файле `check_settings.yaml` измените необходимые параметры (см. приложение В).
 3. Перезапустите контейнер `core-usage-monitoring`:
`docker restart $(docker ps | awk '/core-usage-monitoring/ {print $NF}')`

Проверки изменены.




20 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.

20.1 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:

-  – информирует о каком-либо событии, не связанном с ошибками в работе системы (например, сообщает об инициализации компонента);
-  – предупреждает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра);
-  – сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен).

20.2 Обмен данными между компонентами системы

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:

1. 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.
2. 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.
3. Как только сообщение становится первым в очереди, брокер отправляет его службе-получателю. Обработав сообщение, служба-получатель уведомляет об этом брокер.
4. 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 4.1.2.

Таблица 20.1 – 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
storageq	SIEM Server normalizer, SIEM Server resolver, SIEM Server router	SIEM Server storage

Приведенные в таблице очереди принадлежат брокеру Ankey SIEM NG Server.

20.2.1 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.

20.2.2 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.

20.2.3 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 20.21.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. подраздел 20.10).
2. Убедитесь, что параметр ElasticsearchHost компонента Ankey SIEM NG Server равен IP-адресу или FQDN сервера Ankey SIEM NG ES.
3. Убедитесь, что порт 9200/TCP сервера Ankey SIEM NG ES доступен для входящих соединений от сервера Ankey SIEM NG Server.
4. Создайте файл дампа памяти (см. пункт 20.21.7) службы SIEM Server storage.
5. Перезапустите службу SIEM Server storage.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»⁵, 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 20.21.7) службы SIEM Server storage;
- файлы журналов Elasticsearch, RabbitMQ, служб SIEM Server storage и SIEM Server frontend.

20.2.4 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.

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 20.21.3) 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»⁶, приложив следующую информацию:

- снимок экрана, содержащий страницу **Queues** веб-интерфейса RabbitMQ;

⁵ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

⁶ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

- снимок экрана, содержащий параметры очереди и таблицу с получателями сообщений (в раскрывающемся блоке **Consumers**);
- результат запроса о статусе служб (см. пункт 20.21.3) 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**.

20.2.5 Очередь storageq растёт 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 20.21.1) на сервере Ankey SIEM NG ES равен нулю.
 3. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. пункт 20.21.5). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 10).
 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 20.21.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки ООО «Газинформсервис»⁷, приложив снимки экрана.
 5. Убедитесь, что скорость потока событий от источников соответствует развернутой конфигурации системы.

Если выполнение указанных выше шагов не решило проблему,

⁷ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»⁸, 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 20.21.2) сервера Ankey SIEM NG ES;
- результат запроса о состоянии индексов (см. пункт 20.21.5);
- снимок экрана страницы **Система** → **Мониторинг обработки событий**.

20.2.6 Очередь `pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq` или `notifierq` растёт 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 испытывают высокой нагрузки от запущенных процессов (см. пункт 20.21.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки ООО «Газинформсервис»⁹, 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, RabbitMQ, служб SIEM Server Watchdog (только в конфигурации для низконагруженных систем) и Core Watchdog;

⁸ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

⁹ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

¹⁰ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

- файл конфигурации `siem.conf`;
- снимок экрана страницы **Система** → **Мониторинг обработки событий**;
- данные о нагрузке (см. пункт 20.21.2) на центральный процессор, ОЗУ и жесткие диски сервера Ankey SIEM NG Server.

20.3 Мониторинг состояния RabbitMQ и Elasticsearch

Ankey SIEM NG с помощью служб Core Watchdog и SIEM Server health monitor автоматически отслеживает состояние брокера сообщений RabbitMQ и хранилища событий Elasticsearch. Служба Core Watchdog отслеживает состояние брокера RabbitMQ, установленного на сервере Ankey SIEM NG Core. Служба SIEM Server health monitor отслеживает состояние брокера RabbitMQ, установленного на сервере Ankey SIEM NG Server, а также хранилища Elasticsearch. Если Ankey SIEM NG Core и Ankey SIEM NG Server используют один и тот же брокер RabbitMQ (компоненты установлены на один сервер), его состояние отслеживается обеими службами. На основании результатов мониторинга поток данных, поступающих в систему, может быть временно ограничен.

Службы содержат 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 служб Core Watchdog и 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 службы. После обновления системы значения параметров возвращаются в используемые по умолчанию.

20.3.1 Параметры конфигурации службы Core Watchdog

Если Ankey SIEM NG Core установлен на Linux, параметры конфигурации находятся в файле `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/config/healthmonitoring.watchdog/watchdogSettings.json`.

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

rmqAvailability

Объект содержит параметры для настройки мониторинга статуса RabbitMQ. По умолчанию модуль проверки запрашивает статус RabbitMQ каждые 30 секунд (параметр `checkPeriod`).

Примечание. Если модуль не получил ответ от RabbitMQ в течение 20 секунд (параметр `timeout`), он повторяет запрос (количество повторений – параметр `retries`, интервал между повторениями – параметр `retryDelay`).

В случае обнаружения статуса «failed» модуль сообщает об ошибке службе Core Health Monitoring.

rmqQueueSize

Объект содержит параметры для настройки мониторинга очереди `pt.mpx.siem.receiver.incoming.<Идентификатор Ankey SIEM NG Server>`. По умолчанию модуль проверки запрашивает количество сообщений в очереди каждые 30 секунд (параметр `checkPeriod`).

Примечание. Если модуль не получил ответ от RabbitMQ в течение 20 секунд (параметр `timeout`), он повторяет запрос (количество повторений – параметр `retries`, интервал между повторениями – параметр `retryDelay`).

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 Core Health Monitoring;
- если в очереди находится больше 2000 сообщений (параметр `limits` → `max`) – сообщает об ошибке службе Core Health Monitoring и запрашивает остановку отправки данных от агентов.

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.

rmqQueueSpace

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 `checkPeriod`).

Примечание. Если модуль не получил ответ от RabbitMQ в течение 20 секунд (параметр `timeout`), он повторяет запрос (количество повторений – параметр `retries`, интервал между повторениями – параметр `retryDelay`).

По результатам запроса модуль:

- если используемый объем больше 1 ГБ (параметр `limits` → `warn`), но меньше 2 ГБ (параметр `limits` → `max`) – предупреждает об этом службу Core Health Monitoring;
- если используемый объем больше 2 ГБ (параметр `limits` → `max`) – сообщает об ошибке службе Core Health Monitoring и запрашивает остановку отправки данных от агентов.

Объем используемой памяти будет уменьшаться после остановки

отправки данных. Если он становится меньше 1 ГБ (параметр `limits` → `min`), модуль проверки отзывает запросы на остановку.

rmqDisk

Объект содержит параметры для настройки мониторинга свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ. По умолчанию модуль проверки запрашивает объем свободного места каждые 60 секунд (параметр `checkPeriod`).

Примечание. Если модуль не получил ответ от RabbitMQ в течение 30 секунд (параметр `timeout`), он повторяет запрос (количество повторений – параметр `retries`, интервал между повторениями – параметр `retryDelay`).

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 Core Health Monitoring;
- если диск содержит меньше 30 ГБ (параметр `limits` → `min`) свободного места – сообщает об ошибке службе Core Health Monitoring и запрашивает остановку отправки данных от агентов.

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

flowAgent

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

20.3.2 Параметры конфигурации службы SIEM Server health monitor

Параметры конфигурации находятся в файле `siem.conf` в секции `monitoring` → `flowcontrol`. Если Ankey SIEM NG Server установлен на Linux, файл `siem.conf` находится в каталоге `/opt/siem/etc`.

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 агентами 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 агентами 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 агентами 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 агентов 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 агентами 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 агентом. По умолчанию модуль действия каждые 30 секунд (параметр `check_period`) проверяет наличие запроса на остановку отправки данных. При наличии запроса модуль запрещает агенту отправлять данные в течение 40 секунд (параметр `timeout`). Если при следующих проверках модуль не обнаруживает ранее существовавший запрос, он снова отправляет агенту 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.

20.4 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.
 2. Войдите в RabbitMQ (см. пункт 20.2.1) и проверьте состояние очередей (см. пункт 20.2.2):
 - 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".

20.5 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.

1. 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.
2. 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 Watchdog;
- снимок экрана, отображающий свободное место на логическом диске.

20.6 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.

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 20.21.9) 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 20.21.9). Если на диске менее 40 ГБ свободного места, настройте архивацию индексов по расписанию (см. подраздел 10.3).
4. Проверьте свободное место на логическом диске с архивными индексами (см. пункт 20.21.9). Если на диске отсутствует

¹¹ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

свободное место, настройте удаление архивных индексов по расписанию (см. пункт 10.5.2).

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 журналов служб Core Health Monitoring, Core Watchdog;
- снимок экрана, отображающий свободное место на логическом диске.

20.7 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 20.21.3). Если служба остановлена, запустите ее вручную.
 2. Проверьте доступность страницы входа в RabbitMQ (см. пункт 20.21.1). Если страница недоступна, сообщите об этом в службу технической поддержки ООО «Газинформсервис»¹³, приложив журналы службы RabbitMQ.

20.8 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.

¹² Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

¹³ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

2. Убедитесь, что объем раздела подкачки (см. пункт 20.21.1) 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»¹⁴, приложив следующую информацию:

- нагрузке на файловую систему и запущенных процессах (см. пункт 20.21.2); файлы журналов служб Core Health Monitoring, Core Watchdog и Elasticsearch;
- файлы журналов (см. пункт 20.21.2) 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.

20.9 Индексы Elasticsearch находятся в состоянии red

Индексы Elasticsearch предназначены для хранения данных о событиях информационной безопасности и их последующего поиска. Если не удастся 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 индексы должны находиться в состоянии green или yellow).

Решение

Перед выполнением инструкции необходимо убедиться, что службы Elasticsearch запущены (см. пункт 20.21.3) 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 20.21.5) red, повторно выполните команду: `curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true`

Примечание. Рекомендуется выполнять команду повторно не более двух раз.

¹⁴ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

3. Если требуется оперативно восстановить работоспособность системы, удалите индексы (см. подраздел 10.6), 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»¹⁵, приложив следующую информацию:

- данные о состоянии (см. пункт 20.21.5) индексов и шардов (фрагментов индексов);
- время запуска каждой команды `curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true;`
- файлы журналов Elasticsearch, SIEM Server Watchdog (в конфигурации для низконагруженных систем) и Core Watchdog (в конфигурациях для средненагруженных и высоконагруженных систем).

20.10 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 находиться в состоянии (см. пункт 20.21.5) 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 20.21.1) на сервере Ankey SIEM NG ES равен нулю.
5. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. пункт 20.21.5). Если таких индексов более 900,

¹⁵ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 10).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»¹⁶, приложив следующую информацию:

- период остановки службы, точное время каждой остановки;
- скорость потока событий;
- файлы журналов служб Core Watchdog и Elasticsearch;
- 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.

20.11 Система не получает данные от задачи

Возможные причины

Возможными причинами проблемы являются ошибки в работе компонентов системы, неправильная настройка профиля для сбора данных, сбой в работе источника событий, а также сбор событий с неподдерживаемых источников.

Решение

- ❖ Чтобы решить проблему:
 1. Убедитесь, что задача запущена.
 2. Проверьте наличие ошибок (см. подраздел 20.1) 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 4.1.2.

4. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 4.1.2) и проверьте наличие в нем строк с параметром PackCount. Если такие строки отсутствуют, проверьте наличие сетевого соединения между агентом 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 4.1.2).
6. На странице **Система** → **Управление системой** → **Агенты** проверьте статус агента. Если агент имеет статус "Недоступен", сохраните файлы его журналов для последующей отправки в службу технической поддержки.

¹⁶ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

7. Проверьте очереди в RabbitMQ (см. пункт 20.2.1). 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 20.9)".
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»¹⁷, приложив следующую информацию:

- файлы журналов задачи и агента;
- 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.

20.12 Отсутствуют события от источников

Возможные причины

Возможными причинами проблемы являются неправильная настройка источника событий или задачи по сбору данных, а также сбой 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 4.1.2).
 2. Убедитесь, что источники событий поддерживаются системой и правильно настроены (см. Руководство по интеграции с источниками Ankey SIEM NG 4.1.2).
 3. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 4.1.2) 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.

¹⁷ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

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»¹⁸, приложив следующую информацию:

- предупреждения и ошибки (см. подраздел 20.1) 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 20.21.3) 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**.

20.13 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 4.1.2). 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 4.1.2).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»¹⁹, 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.

¹⁸ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

¹⁹ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

20.14 Не приходят уведомления, отправляемые по электронной почте

- ❖ Чтобы решить проблему:
 1. Откройте файлы журналов `NotificationsManagement.log` и `Triggers.log`, расположенные на сервере Ankey SIEM NG Core. 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`, `Smtphost` и `Smtppassword` утилиты `corecfg.exe` 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.

20.15 Ошибка "Sdk пакет <Номер версии> поврежден. Необходимо восстановление"

Ошибка может возникнуть во время обновления компонента Ankey SIEM NG Core.

Решение

Для решения проблемы вам потребуется архив `packages\siem-sdk.<Номер версии>.tar.gz` из комплекта поставки.

- ❖ Чтобы решить проблему:
 1. После обновления Ankey SIEM NG Core в папке `C:\ProgramData\Gazinformservice\Knowledge Base\SiemSdks` создайте папку `<Номер версии пакета>`.
 2. Распакуйте архив `siem-sdk.<Номер версии>.tar.gz` в папку `<Номер версии пакета>`.
 3. Войдите в Knowledge Base.
 4. В меню **SIEM** выберите пункт **Выбор версии SDK**.
 5. На отрывшейся странице в центральной панели выберите последнюю версию SDK и нажмите кнопку **Восстановить**.

20.16 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 4.1.2).
 2. Скачайте журнал задачи (см. Руководство оператора Ankey SIEM NG 4.1.2). 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»²⁰.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»²¹, 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.

20.17 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 MC и Knowledge Base, необходимо указать актуальные значения следующих параметров:

- HostAddress, PtkbFeatureHost и PtmcHostAddress компонента Ankey SIEM NG Core;
- HostAddress, IdentityServerAddress и CoreAddress компонента Knowledge Base;
- HostAddress компонента Ankey SIEM NG MC;
- CoreAddress и RMQHost компонента Ankey SIEM NG Server на Linux;

²⁰ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

²¹ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

- RMQHost компонента Ankey SIEM NG Agent, установленного для отдельного сегмента сети.

Если был изменен IP-адрес или FQDN сервера Ankey SIEM NG Server, необходимо указать актуальное значение параметра `SiemAddress` компонентов Ankey SIEM NG Core и Knowledge Base.

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.

20.18 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 версия²² коннектора, совместимая с контентом;
- компонент Ankey SIEM NG Agent 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 источник), учтены требования, представленные в документации на коннектор и проектной документации;

²² Для определения версии установленного коннектора см. пункт 20.18.4, для определения версии пакета контента см. пункт 20.19.7.

- коннектор установлен в активную установочную базу, формулы нормализации, формулы обогащения и табличные списки (при наличии) включены.

20.18.1 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 20.12.

2. Убедиться в корректности работы сетевого взаимодействия источника событий и сервера сбора событий Ankey SIEM NG Agent:
 - 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 Agent, то рекомендуется проверить, что такие события отправляются со стороны источника и поступают в программный комплекс²³.

4. Убедиться, что выполнены рекомендации²⁴ по настройке источника, включая настройки аудита источника (регистрации сведений в журнале событий):
 - для стандартных коннекторов на соответствие параметрам, указанным в документе «Руководство по интеграции с источниками Ankey SIEM NG 4.1.2»;
 - для дополнительных коннекторов на соответствие параметрам, указанным в разделе 4 «Особенности сбора событий с источника» документации, поставляемой вместе с дополнительным коннектором.

²³ Например, через tcpdump и т.п.

²⁴ Указанные в документации на коннектор настройки носят рекомендательный характер. Итоговые настройки определяются особенностями проекта и представлены в проектной документации.

Примечание. Убедиться, что настройки аудита событий соответствуют рекомендациям вендора/интегратора, приведенным в эксплуатационной/проектной документации на источник.

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 коннектор²⁵, и при этом сбор событий не выполняется с заявленными функциональными возможностями, то необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»²⁶.

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 коннектор²⁷, и при этом сбор событий не выполняется с заявленными функциональными возможностями, то необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис»²⁸.

После выполнения диагностики источника событий перейти к диагностике работы ПК Ankey SIEM NG, представленной в пункте 20.18.2.

²⁵ 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 21.

²⁶ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.


²⁷ 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 21.

²⁸ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

20.18.2 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 **ПК Ankey SIEM NG**.
Откроется главная страница.
2. Нажмите на цветовой индикатор состояния Ankey SIEM NG в верхнем правом углу рабочей области. Подробнее см. подраздел 20.1.
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 20.18.3.

20.18.3 Диагностика работы коннектора

Для диагностики работы коннектора в ПК Ankey SIEM NG необходимо:

1. Убедитесь, что все зависимые ресурсы загружены в систему и/или добавлены в набор установок. Для этого необходимо выполнить инструкции из подраздела 20.20.
2. Проверить наличие событий от источника в ПК Ankey SIEM NG в соответствии с подразделом 20.12.
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 **ПК 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 20.1.

 Завершена Ankey IDM incident

 Выполняется ankey_siem_correlator_679_u...




 Завершена ASAP

Рисунок 20.1 – 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 4.1.2»;
 - для дополнительных коннекторов на соответствие параметрам, указанным в документации, поставляемой вместе с дополнительным коннектором.
 - выполните инструкции из подраздела 20.11.
4. Проверить корректность настроек профиля сбора событий с источника, для этого:
- в главном меню нажмите  и в раскрывшемся меню выберите пункт **ПК Ankey SIEM NG**.
Откроется главная страница;
 - выберете 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 документации²⁹:
 - для стандартных коннекторов на соответствие параметрам, указанным в документе «Руководство по интеграции с источниками Ankey SIEM NG 4.1.2»;
 - 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 20.2), указанный справочник на языке python для профилей на базе Custom Event Collector (см. рисунок 20.3);

Примечание. Для коннекторов на базе механизма сбора Custom Event Collector реализована возможность активировать расширенный режим логирования (Debug-режим). Данный функционал позволяет отследить ошибки при подключении к источнику. Описание работы Debug-режима представлено в пункте «Модуль CustomEventCollector» в документе «Руководство по интеграции с источниками Ankey SIEM NG 4.1.2».

²⁹ Указанные в документации на коннектор настройки носят рекомендательный характер. Итоговые настройки определяются особенностями проекта и приведены в проектной документации.

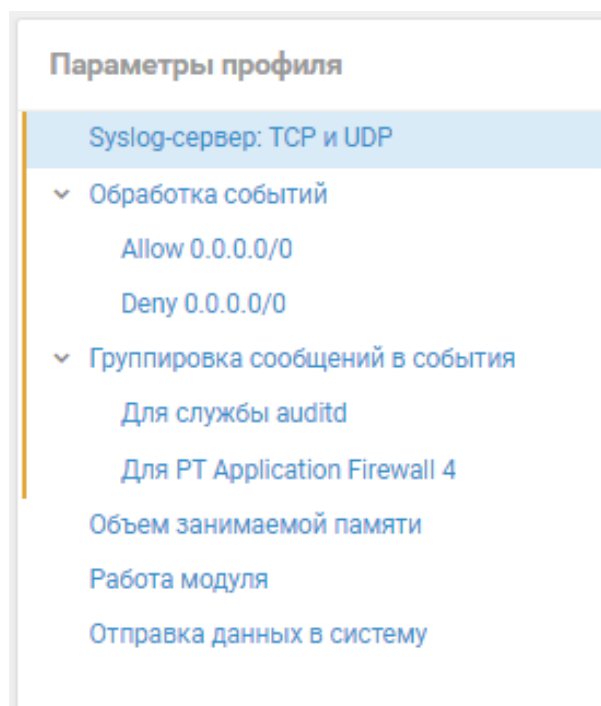


Рисунок 20.2 – Сетевые настройки

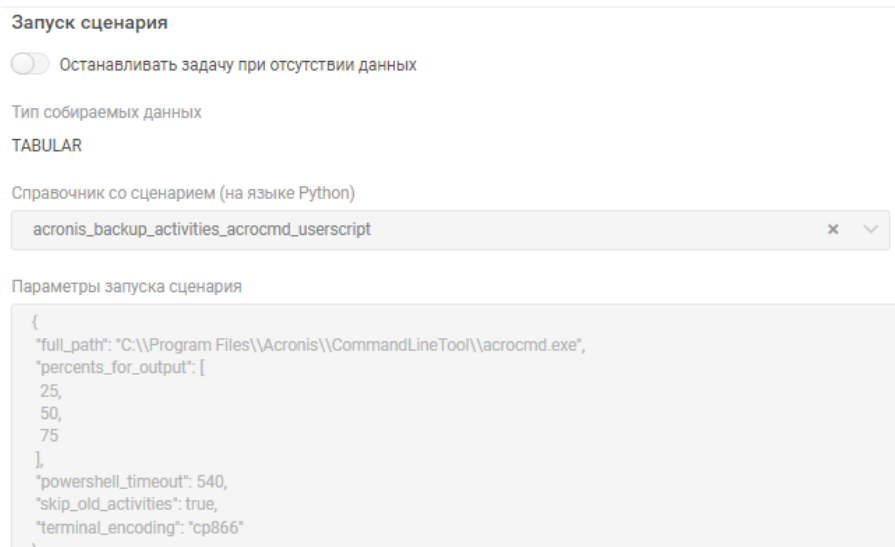




Рисунок 20.3 – Справочник со сценарием

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 **ПК 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 20.4;

Подзадачи					
Статус	Начало сбора	Окончание сбора	Длительность	Агент	Цели
✓ Завершена	16 февраля 2023 16:54	16 февраля 2023 16:56	1 мин	Local agent	10.10.217.22

Рисунок 20.4 – 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 20.11;
- 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»³⁰.

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 21.

20.18.4 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**

³⁰ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

источника> и откройте правило нормализации **INFO_Gazinformservice_<Наименование источника>**, как показано на рисунке 20.5.

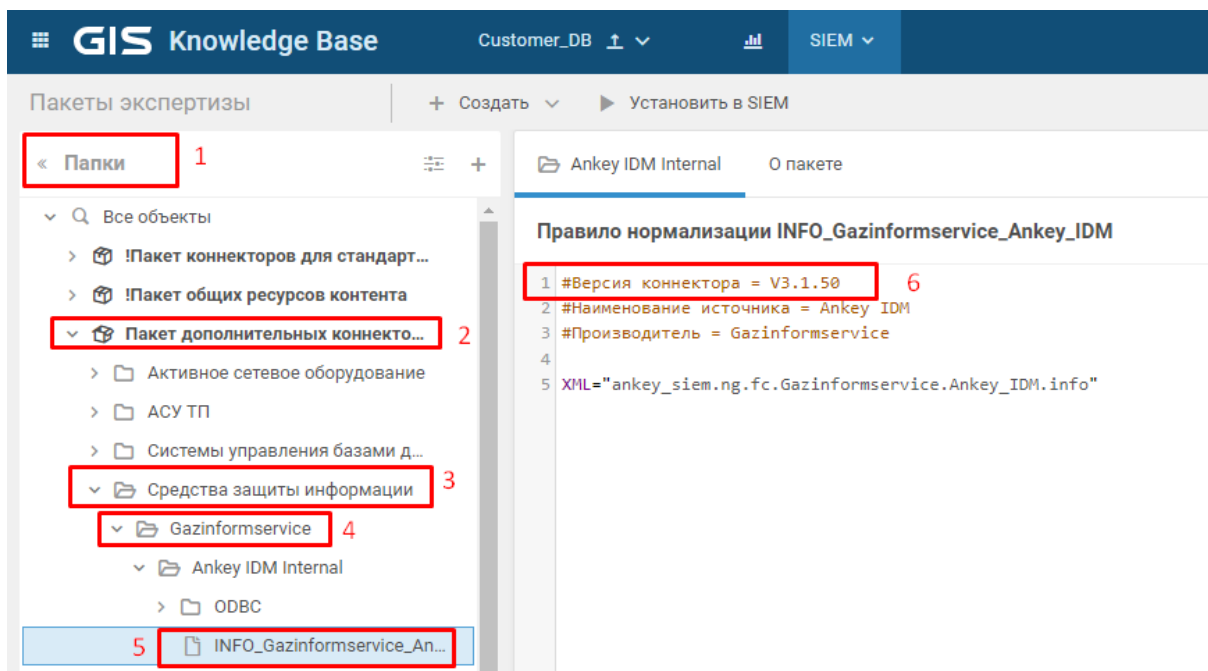


Рисунок 20.5 – Просмотр версии дополнительного коннектора в веб-интерфейсе

Номер версии коннектора будет указан в коде правила нормализации в комментарии `#Версия коннектора =V<A.B.C>`.

20.19 Диагностика пакетов контента

В этом подразделе приведены инструкции по диагностике и решению проблем, возникающих при работе ресурсов пакетов контента³¹ 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

³¹ Ключевой ресурс пакета контента – сигнатуры нарушений ИБ (корреляционные правила).





- 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;
 - 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.

20.19.1 Начальная проверка правила корреляции

В данном пункте описывается проверка статуса правил корреляции и установка, а также наличие событий в системе.

20.19.1.1 Проверка статуса правила

❖ Для того чтобы проверить, что правило корреляции установлено в системе необходимо:

1. Перейти на вкладку **Knowledge Base** → **SIEM** → **Пакет экспертизы**.
2. Выбрать необходимую папку (рисунок 20.6) или правило (рисунок 20.7) 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.



<input type="text" value="Системное название, идентификатор или описание"/>					
№	С...	Идентификатор	Системное название	Описание	Тип
1		LOC-CR-362	TTS_01_DoS_Attack_Detected	Правило предназначено для мониторинга событий обнаруже...	

Рисунок 20.6 – Статус установки в перечне правил

Правило предназначено для мониторинга событий обнаружения атак типа DoS и DDoS. Табличный список конфигурации: отсутствует. Табличный список исключений: "COMMON_Tracking_Exceptions".

Системное название	TTS_01_DoS_Attack_Detected
Идентификатор	LOC-CR-362
Тип	Пользовательский
Поставщик	Локальная система
Папка	!Пакет общих ресурсов контента/Правила корреляции/Атаки н а отказ в обслуживании
Наборы для установки	test
Статус валидации	
Статус установки	

Рисунок 20.7 – 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 20.8 и 20.9), то возможны варианты:

1. Не выбран нужный набор для установки, либо не добавлено правило в набор для установки.

<input type="text" value="Системное название, идентификатор или описание"/>						
№...	С...	Идентификатор	Системное название	Описание	Тип	↓
1		LOC-CR-362	TTS_01_DoS_Attack_Detected	Правило предназначено для мониторинга событий обнаруже...		

Рисунок 20.8 – Отсутствие значка статуса установки в папке с ресурсами

Правило предназначено для мониторинга событий обнаружения атак типа DoS и DDoS. Табличный список конфигурации: отсутствует. Табличный список исключений: "COMMON_Tracking_Exceptions".

Системное название	TTS_01_DoS_Attack_Detected
Идентификатор	LOC-CR-362
Тип	Пользовательский
Поставщик	Локальная система
Папка	!Пакет общих ресурсов контента/Правила корреляции/Атаки н а отказ в обслуживании
Статус валидации	

Рисунок 20.9 – Отсутствие значка статуса установки в описании правила

Для того чтобы проверить, что правило в наборе для установки, можно либо выбрать правило и нажать на кнопку **Наборы для установки** (на рисунке 20.10

представлено, как будет выглядеть правило без набора для установки) или же открыть само правило и посмотреть справа на сводную информацию о правиле (в случае, если правило будет вне установочного набора, поле будет отсутствовать), представлено на рисунке 20.11.

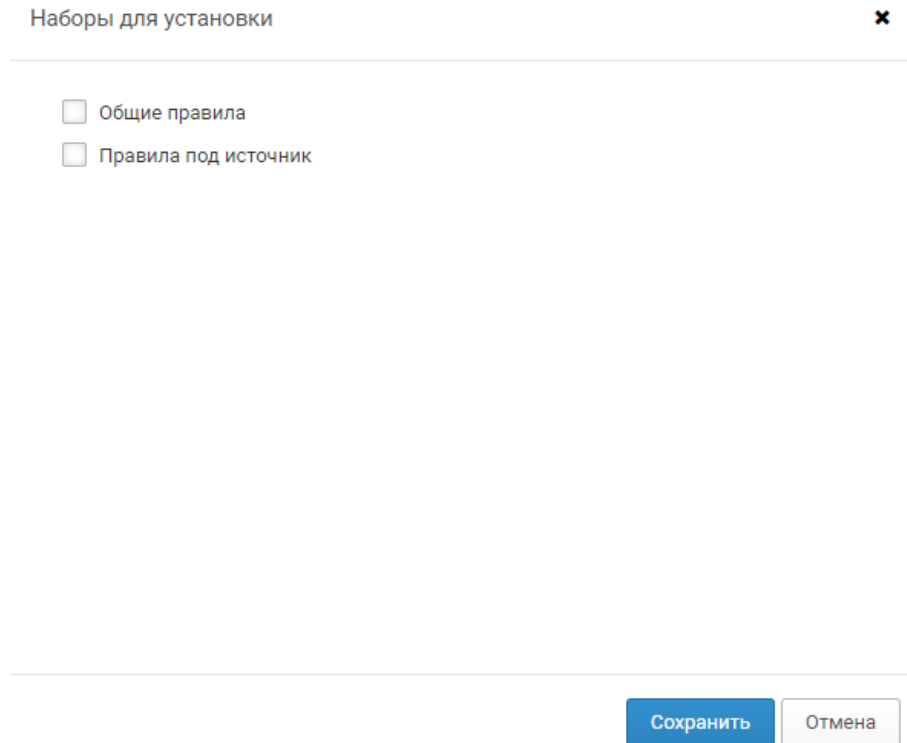


Рисунок 20.10 – Выбор набора для установки

Правило предназначено для мониторинга событий обнаружения атак типа DoS и DDoS. Табличный список конфигурации: отсутствует. Табличный список исключений: "COMMON_Tracking_Exceptions".

Системное название	TTS_01_DoS_Attack_Detected
Идентификатор	LOC-CR-362
Тип	Пользовательский
Поставщик	Локальная система
Папка	!Пакет общих ресурсов контента/Правила корреляции/Атаки на отказ в обслуживании
Наборы для установки	Общие правила
Статус валидации	

Рисунок 20.11 – Набор для установки в описании правила

Также стоит отметить, что при создании набора для установки необходимо выбрать требуемый конвейер (рисунок 20.12), иначе при установке появится ошибка, как показано на рисунке 20.13.

Редактирование набора для установки ✕

Набор предназначен для установки объектов в конвейер обработки событий. Вы можете добавлять в набор любые объекты из разных пакетов экспертизы и папок.

Системное название:

Название (русский):
[Добавить название на английском языке](#)

Входит в набор:

Устанавливать в конвейер:

Рисунок 20.12 – Выбор конвейера для установки ресурсов

Установить в SIEM ✕

В конвейере обработки событий будут удалены все объекты и добавлены объекты из набора.

Невозможно установить объекты в конвейер , поскольку он не связан с набором для установки. Вы можете привязать конвейер при создании нового набора или изменении существующего

Конвейеры Набор для установки

Версия SIEM: 25.1.0

Рисунок 20.13 – 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 20.14.

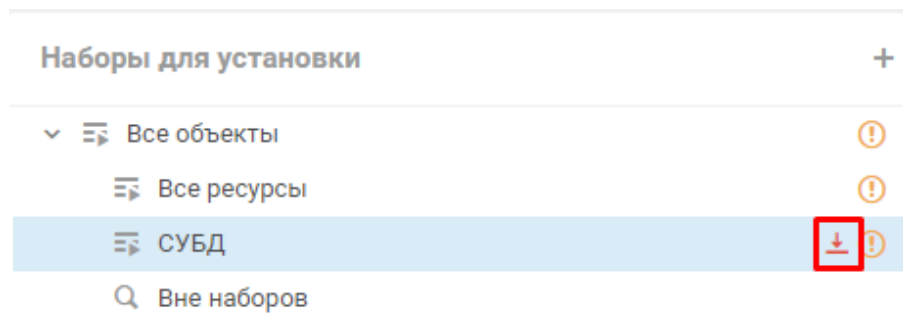


Рисунок 20.14 – Иконка установки у набора

Внимание! Необходимо в набор для установки добавлять все зависимые ресурсы, иначе установка выполнится с ошибкой (рисунок 20.15), пример представлен на рисунке 20.16.

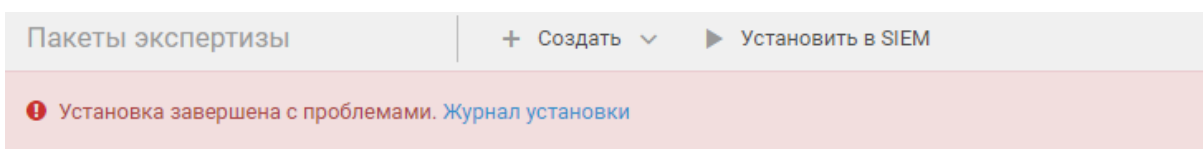


Рисунок 20.15 – Сообщение об ошибке установки

LOC-RF-281:9:98: error: Table 'COMMON_Tracking_Exceptions' not defined

Тип объекта

correlation

Объект

COMMON_Exceptions

Описание

LOC-RF-281:9:98: error: Table 'COMMON_Tracking_Exceptions' not defined

Рисунок 20.16 – 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:
 - открыть выпадающий список с названием баз данных в **Knowledge Base** → **SIEM** и выбрать **Базы данных**;
 - в открывшейся вкладке 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 загружены 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 20.17, то:
1. Либо не выбран нужный набор для установки, либо не добавлено правило в набор для установки (см. предыдущий пункт).

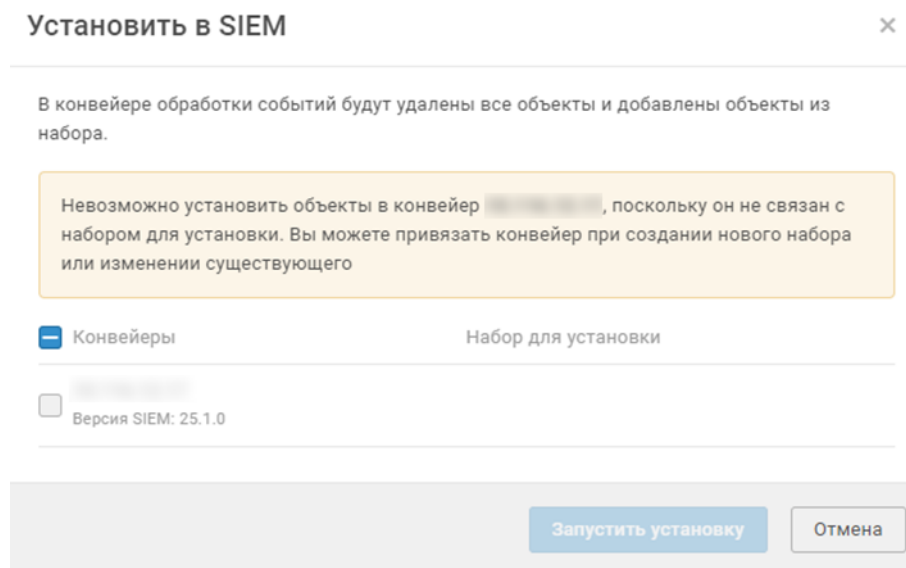


Рисунок 20.17 – Ошибка установки

2. В случае, если правило добавлено в набор для установки, а ошибка сохраняется, убедитесь, что у набора для установок выбран конвейер (см. предыдущий пункт). При установке появляется ошибка зависимостей ресурсов (рисунок 20.18).

LOC-RF-281:9:98: error: Table 'COMMON_Tracking_Exceptions' not defined

Тип объекта
correlation

Объект
COMMON_Exceptions

Описание
LOC-RF-281:9:98: error: Table 'COMMON_Tracking_Exceptions' not defined

Рисунок 20.18 – Ошибка зависимостей

- Убедитесь, что все зависимые ресурсы загружены в систему и/или добавлены в набор установок. Для этого необходимо выполнить инструкции из подраздела 20.20.

20.19.1.2 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 посмотреть либо на значок в таблице (рисунок 20.19), либо выбрав конкретное правило (рисунок 20.20).

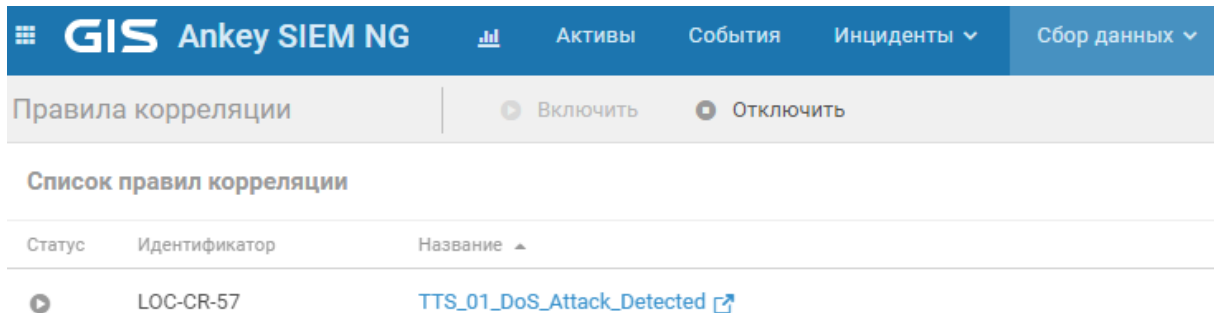


Рисунок 20.19 – Статус правила в списке правил

» [TTS_01_DoS_Attack_Detected](#)

Правило предназначено для мониторинга событий обнаружения атак типа DoS и DDoS. Табличный список конфигурации: отсутствует. Табличный список исключений: "COMMON_Tracking_Exceptions".

Идентификатор	LOC-CR-57
Статус	<input checked="" type="radio"/> Включено
Срабатываний за сутки	0
Изменено	Вчера, в 23:16
Тип	Пользовательское
Поставщик	Локальная система
Категория	Generic: High: Low:

Созданные события [Перейти](#)

Рисунок 20.20 – Статус правила в описании

Основные статусы правил представлены в таблице 20.2.

Таблица 20.2 – Основные статусы правил

Статус	Описание
<input checked="" type="radio"/>	Включено
<input type="radio"/>	Отключено
<input type="checkbox"/>	Правило автоматически остановлено на основании результатов мониторинга работы правил корреляции. Подробнее см. пункте 2

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 20.21.

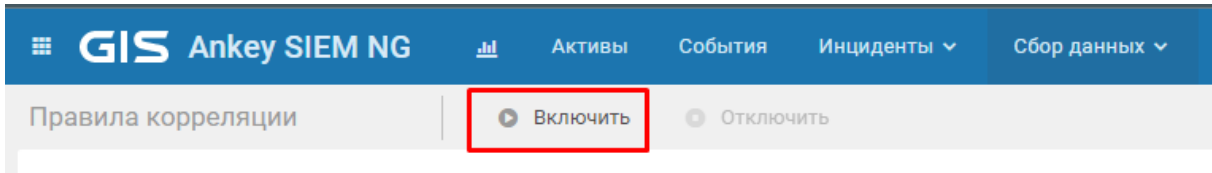


Рисунок 20.21 – Включение правила

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 20.22.

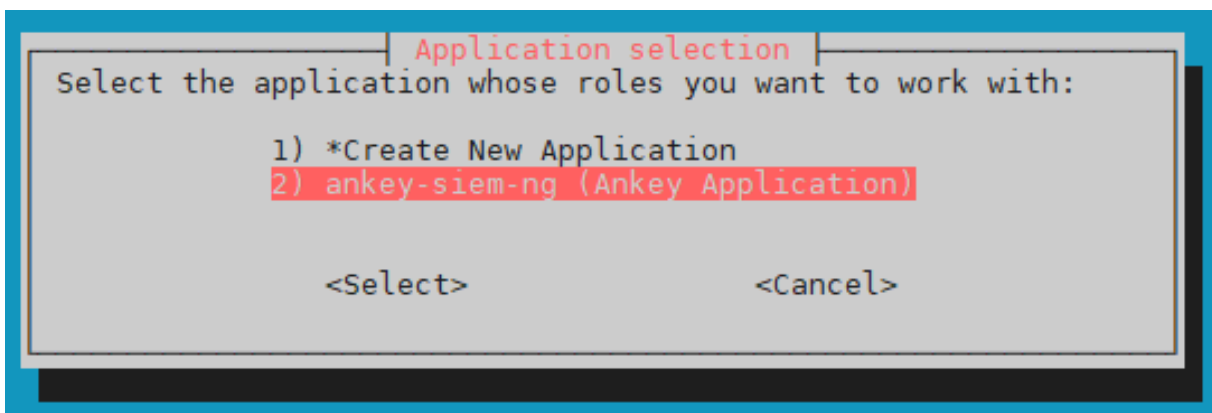


Рисунок 20.22 – Выбор приложения

3. В открывшемся окне выбрать с помощью стрелок необходимый экземпляр (Instance) и нажать **Enter**, как показано на рисунке 20.23.

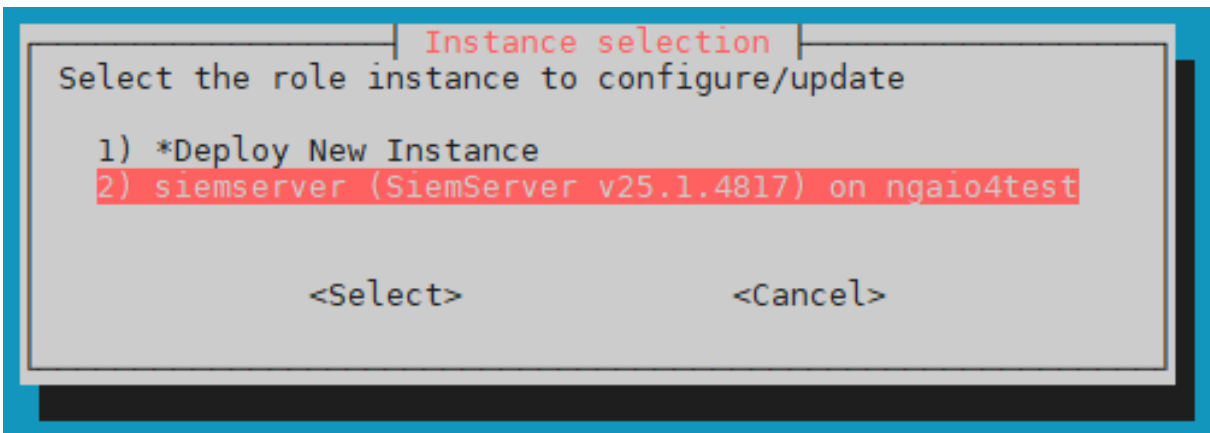


Рисунок 20.23 – Выбор экземпляра (Instance)

4. На открывшейся странице выбрать параметр **Advanced configuration** и нажать **Enter**, как показано на рисунке 20.24.

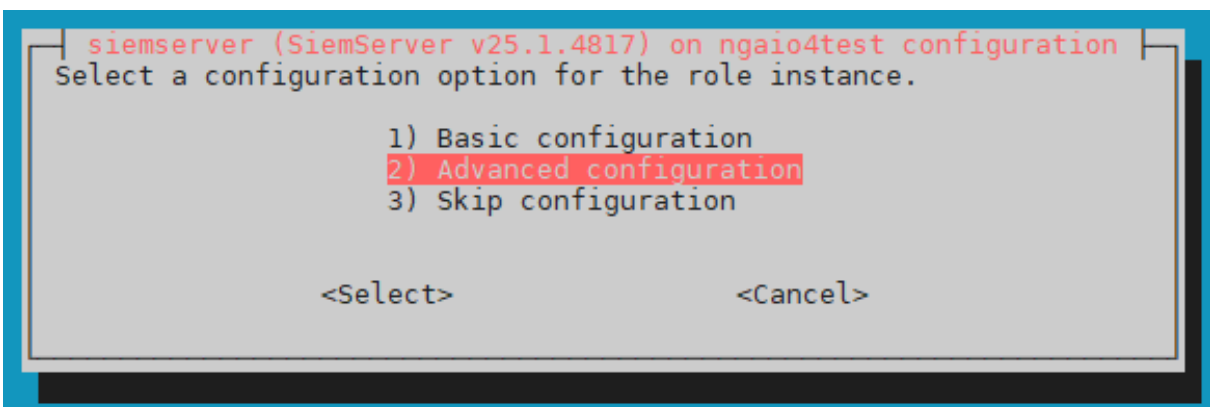


Рисунок 20.24 – Выбор типа настроек

5. В открывшемся перечне настроек внести требуемые изменения в параметры, указанные в таблице 20.3, как показано на рисунке 20.25.

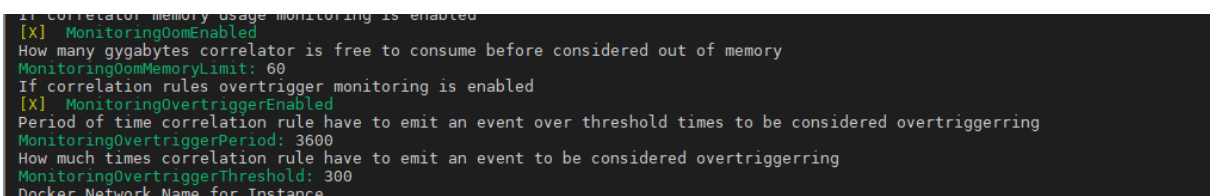


Рисунок 20.25 – Перечень настроек

Примечание. Для проставления или убирания флажка нажмите пробел у соответствующего параметра.

- После изменения всех необходимых параметров прокрутите список настроек вниз, выберите **OK** и нажмите **Enter**, как показано на рисунке 20.26.

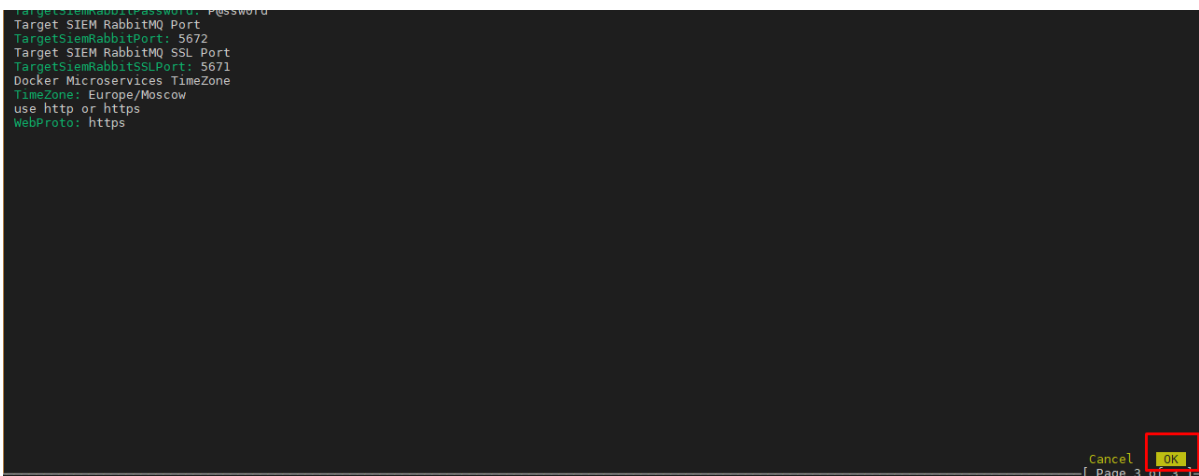


Рисунок 20.26 – Выход из настроек

- Будет выполнена реконфигурация настроек (рисунок 20.27).

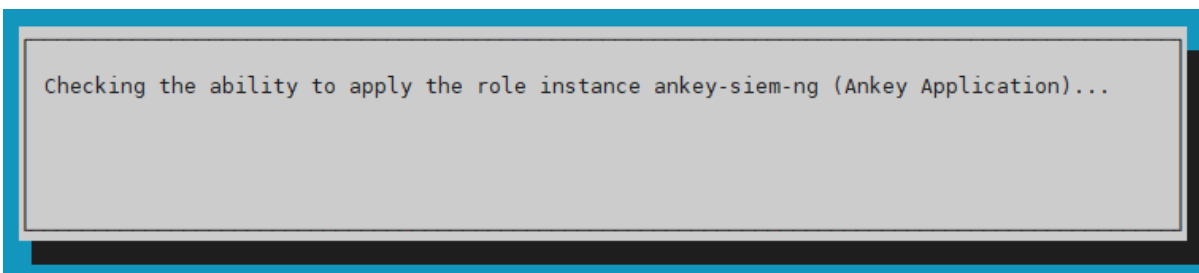


Рисунок 20.27 – Применение настроек

- После успешного выполнения операции появится информационное окно, в котором необходимо нажать **OK**, как показано на рисунке 20.28.

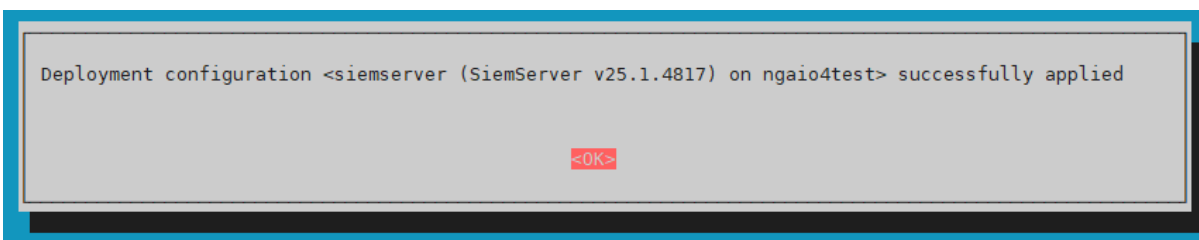


Рисунок 20.28 – Сообщение об успешной перенастройке

Таблица 20.3 – Параметры конфигурации

Параметр	Описание	По умолчанию
ProtectedRulesPath	Для включения правил в список исключений необходимо добавить их системные названия в текстовый файл (каждое	-

Параметр	Описание	По умолчанию
	<p>название в отдельной строке) и указать путь к файлу в качестве значения параметра ProtectedRulesPath.</p> <p>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</p>	
MonitoringOomMemoryLimit	Изменяет объем оперативной памяти, выделенной для работы правил корреляции (в ГБ)	60
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.

20.19.1.3 Проверка наличия событий

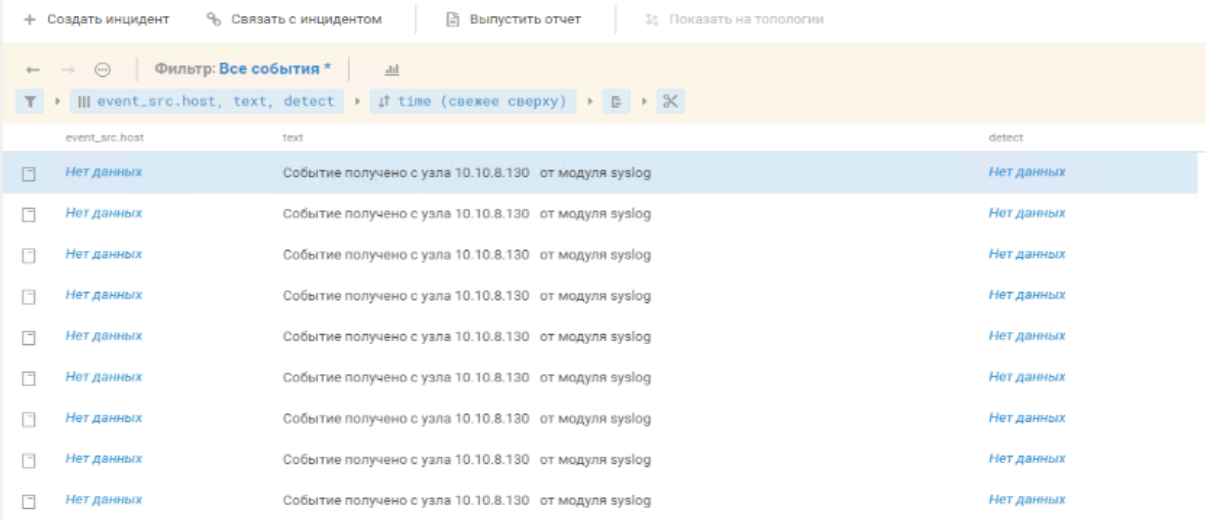
Для того чтобы правило срабатывало в режиме «реального времени», должен быть поток событий от источника³². Для проверки наличия событий необходимо перейти на вкладку **Ankey SIEM NG** → **События**.

Проверить наличие событий от источника в соответствии с подразделом 20.12.

Внимание! Подробнее о диагностике коннекторов и источников событий описано в подразделе 20.18.

Возможные проблемы и их решение:

❖ Вы открыли таблицу событий и обнаружили, что в нем есть только необработанные события (рисунок 20.29):



event_src.host	text	detect
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных
Нет данных	Событие получено с узла 10.10.8.130 от модуля syslog	Нет данных

Рисунок 20.29 – 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»³³.

³² Рекомендуется использовать наиболее актуальную версию коннектора для работы с правилами и убедиться в совместимости пакета контента с коннектором.

³³ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

❖ Вы открыли таблицу событий, а он пустой (рисунок 20.30):

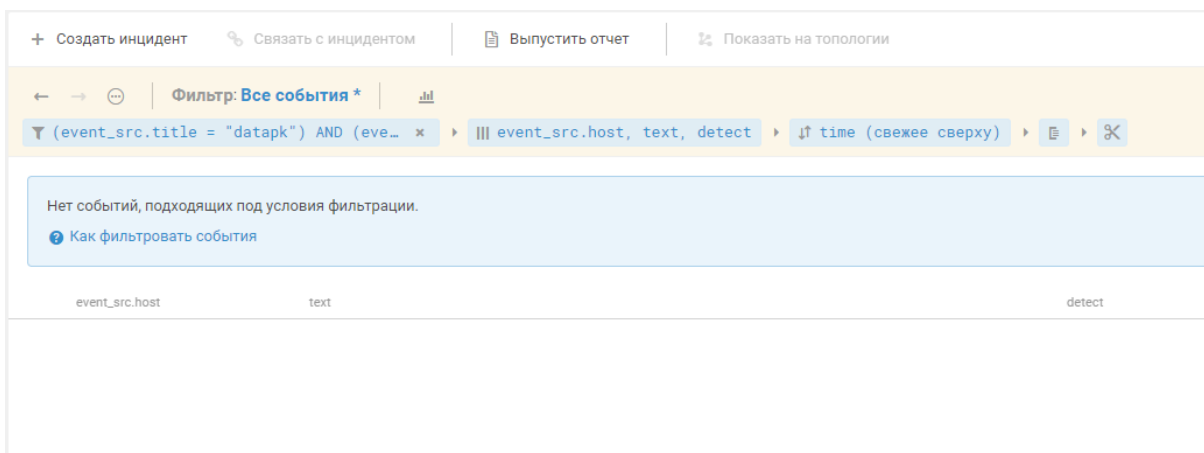


Рисунок 20.30 – Отсутствие событий от источника

1. Убедитесь, что правильно написали условие в фильтре для источника.
2. Проверить работу задачи на сбор событий в соответствии с пунктом 20.18.3.

Примечание. Если Вы убедились, что все настроено корректно, а событий все еще нет, то обратитесь в службу технической поддержки ООО «Газинформсервис»³⁴.

20.19.2 Проверка корректности обработки события

В данном пункте описывается проверка корректности обработки событий.

20.19.2.1 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 20.31). Если после уточнения запроса в таблице событий есть интересующее событие, то перейти к подпункту 20.19.2.3, если нет, то перейти к подпункту 20.19.2.2.

³⁴ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

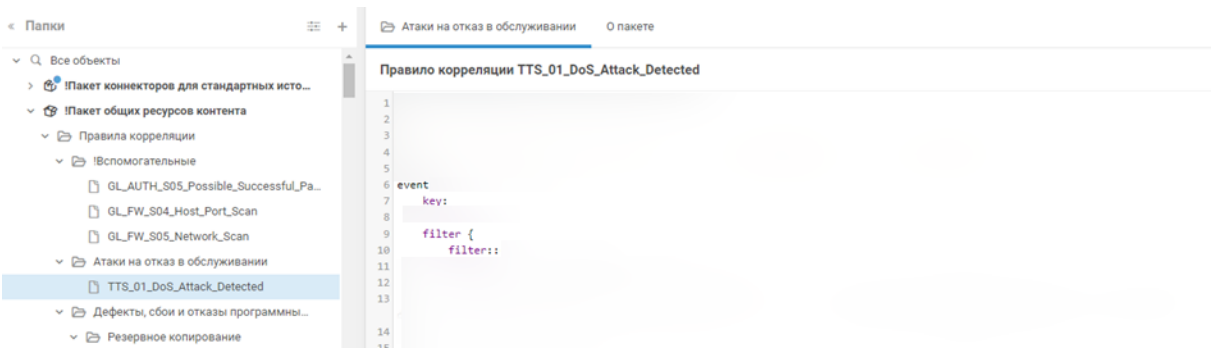


Рисунок 20.31 – Правило. Директива event, инструкция filter

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.

20.19.2.2 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 20.32). 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).

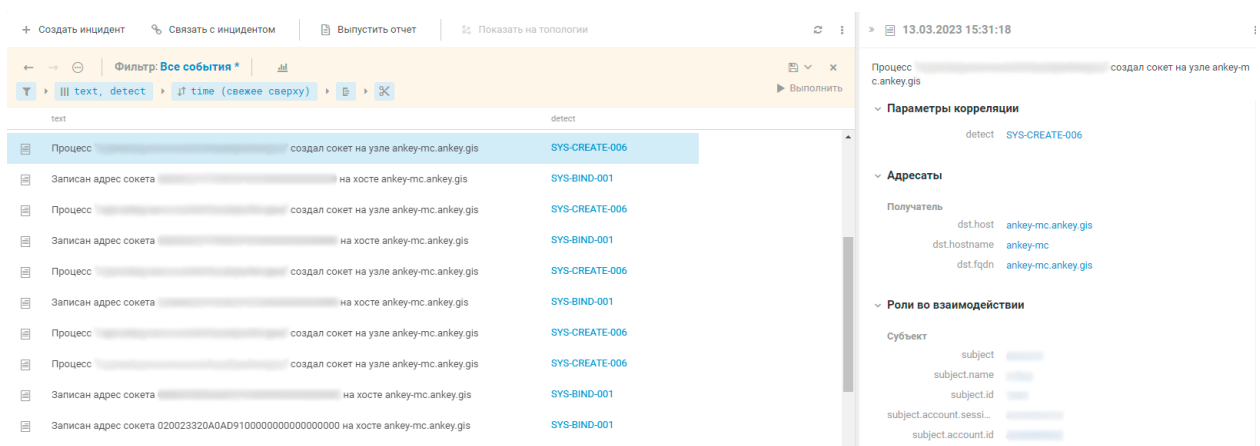


Рисунок 20.32 – Поля события источника

Возможные проблемы и их решение:

❖ В одном из полей обнаружено несоответствие. При нахождении данной проблемы обратитесь в службу технической поддержки ООО «Газинформсервис»³⁵.

❖ В требуемых полях отсутствует информация. В таком случае необходимо обратиться в службу технической поддержки ООО «Газинформсервис»³⁶.

❖ 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»³⁷.

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»³⁸, 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.

20.19.2.3 Проверка использования табличного списка

Если правило использует табличный список, то в таком случае правило может не обрабатывать, 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 20.33.

³⁵ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

³⁶ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

³⁷ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

³⁸ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

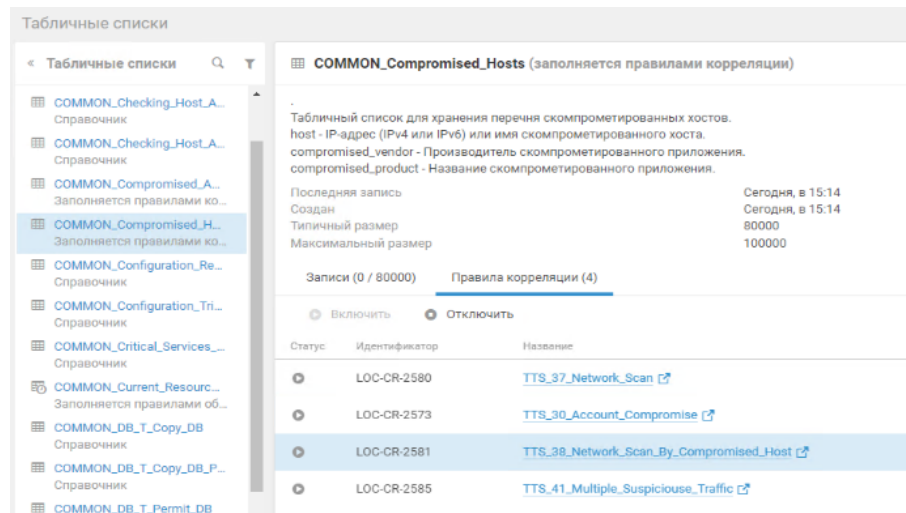


Рисунок 20.33 – Список правил корреляций, использующих табличный список

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.

20.19.3 Проверка корректности использования табличного списка

В данном пункте описывается проверка корректности работы и заполнения табличного списка.

20.19.3.1 Проверка установки табличного списка в систему

Проверка установки табличного списка в систему проводится аналогично проверке установки правила корреляции, описание представлено в пункте 20.19.1.1.

Статус установки табличного списка также можно посмотреть двумя способами:

- в папке, в общем перечне (рисунок 20.34);
- в описании к ресурсу (рисунок 20.35).

С...	Идентификатор	Системное название	Описание	Тип	↓
✓	LOC-TL-228	COMMON_DB_T_Copy_DB_Permit_Hosts	Табличный список для внесения информации о хо...		↓

Рисунок 20.34 – Статус установки табличного списка в дереве ресурсов

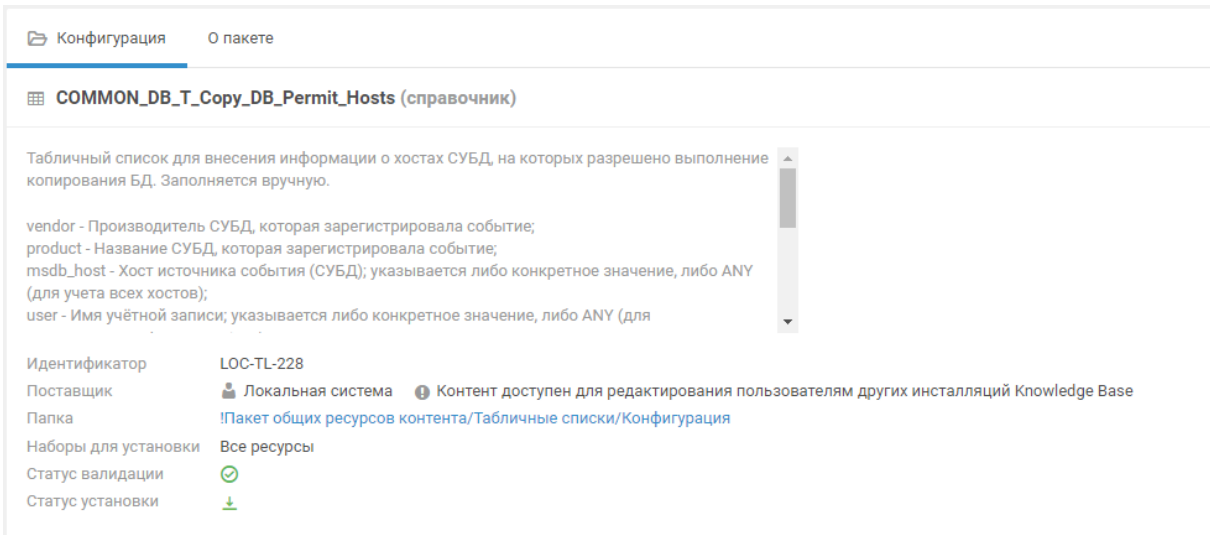


Рисунок 20.35 – Статус установки табличного списка в описании

20.19.3.2 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 20.36.

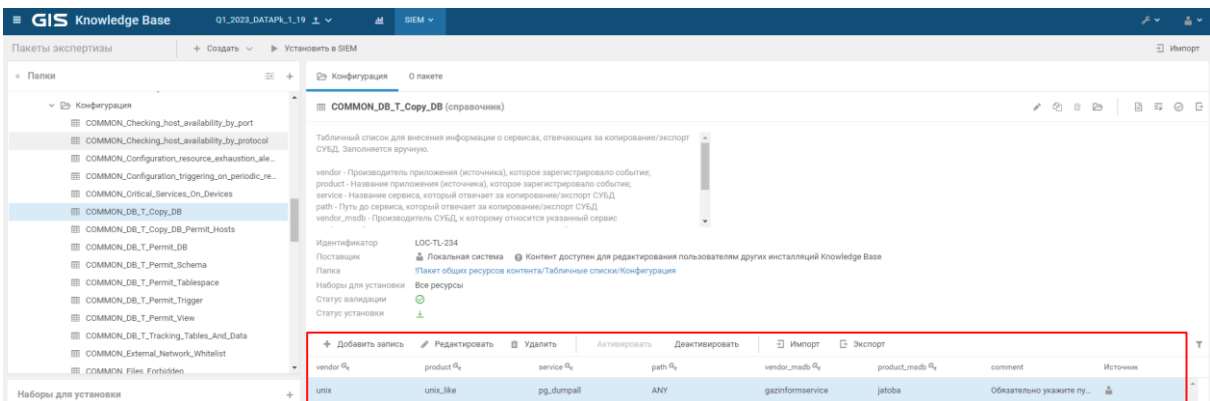


Рисунок 20.36 – Информация по табличному списку

Примечание. Здесь не будет отображаться информация о наполненности табличных списков, заполняемых правилами корреляции и обогащения.

2. 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 20.37.

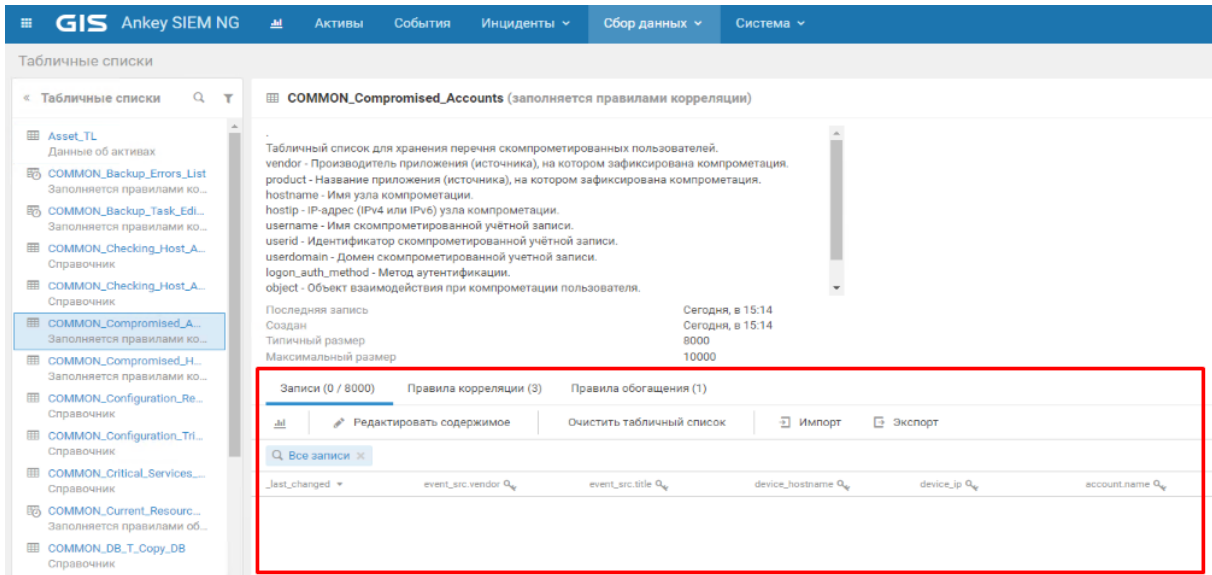


Рисунок 20.37 – Информация о наполненности табличного списка

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 контента³⁹.
 2. Если это табличный список, заполняемый правилами корреляции/обогащения, то убедитесь, что требуемые правила включены и корректно работают, согласно описанию, представленному в подразделе 20.19.
- ❖ 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 20.38).

vendor	product	service	path	vendor_msdb	product_msdb
unix	unix_like	pg_dumpall	ANY	gazinformservice	jatoba
unix	unix_like	pg_dumpall	ANY	postgres_professional	postgresql

Рисунок 20.38 – Деактивированная запись

2. Для того чтобы активировать запись, выделите ее и нажмите на кнопку **Активировать**, как показано на рисунке 20.39.

³⁹ Конечные настройки на инсталляции ПК Ankey SIEM NG определяются в проектной документации.

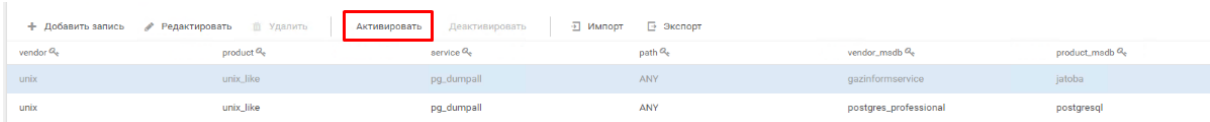


Рисунок 20.39 – Кнопка активации записей

- ❖ Записи есть в табличном списке, но правило все равно не работает:
 1. Если записи были добавили и активированы, но правило не работает, рекомендуется еще раз установить список в систему (подробно описано в подпункте 20.19.3.1).

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.

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.

20.19.4 Корректность проверки правила

В данном пункте описывается проверка корректности выполнения условия правила при тестировании на событиях, а также контроль частоты срабатываний правил корреляций.

20.19.4.1 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 20.40.

```

Правило корреляции TTS_31_Multiple_Suspicious_Actions
36
37 # Описание правила корреляции и условие его выполнения
38 rule TTS_31_Multiple_Suspicious_Actions: Suspicious_Action_Detected[10] within 5m
39   on Suspicious_Action_Detected {
40     ...
41     ...
42     ...
43     ...
44     ...
45     ...
46     ...
47     ...
48     ...
49     ...
50     ...
51     ...
52     ...
53     ...
54     ...
55     ...
56     ...
57     ...
58   }
59

```

Рисунок 20.40 – Условие для срабатывания правила корреляции

20.19.4.2 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 20.41.
Подробное описание системного дашборда Мониторинг обработки событий представлено в документе «Руководство оператора Ankey SIEM NG».

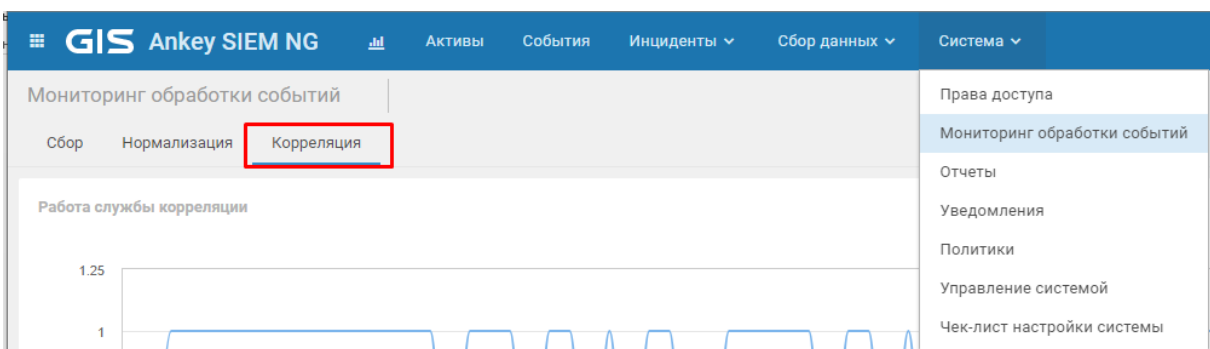


Рисунок 20.41 – Вкладка Корреляция

2. В результате на данном дашборде (рисунок 20.42) 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.

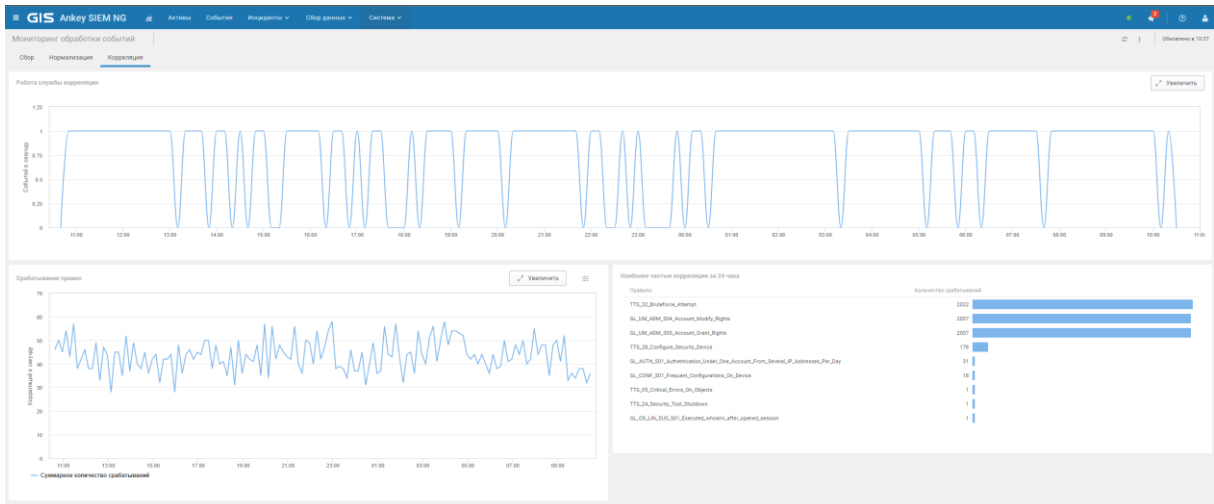


Рисунок 20.42 – Информация в виде дашборда по правилам корреляции

3. Список правил корреляций.
Для отображения списка правил корреляций необходимо перейти на вкладку **Ankey SIEM NG** → **Сбор данных** → **Правила корреляции**, как показано на рисунке 20.43.

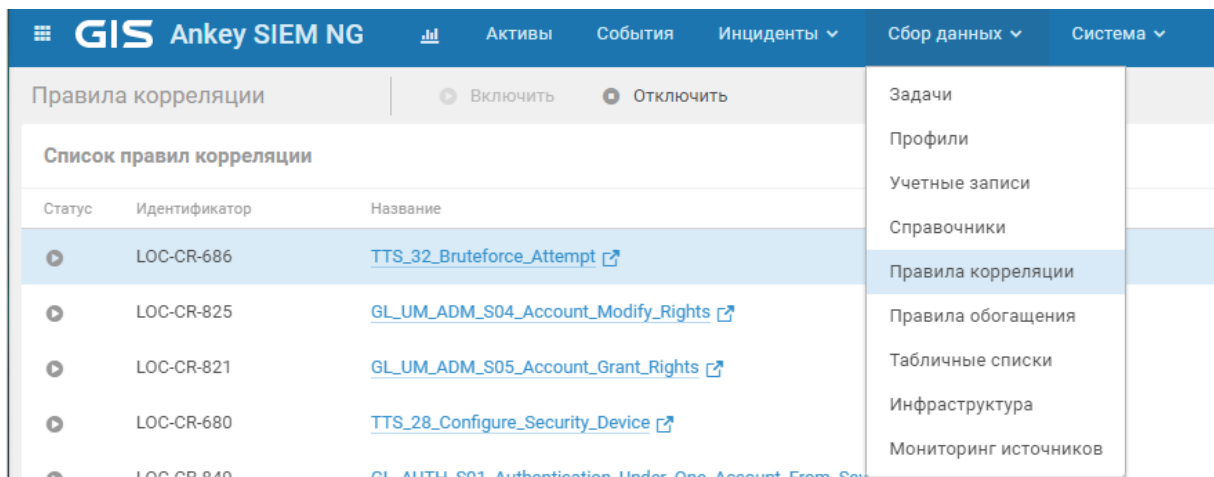


Рисунок 20.43 – Вкладка Правила корреляции

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 20.44.

Статус	Идентификатор	Название	Категория	Тип	Срабатываний за сутки
○	LOC-CR-686	TTS_32_BruteForce_Attempt [?] [?]	/ Attack / Bruteforce	▲	2 021 [?]
○	LOC-CR-823	GL_UM_ADM_S04_Account_Modify_Rights [?]	/ Rights Management /	▲	2 009 [?]
○	LOC-CR-821	GL_UM_ADM_S03_Account_Grant_Rights [?]	/ Rights Management /	▲	2 009 [?]
○	LOC-CR-680	TTS_28_Configure_Security_Device [?]	/ /	▲	178 [?]
○	LOC-CR-849	GL_AUTH_S01_Authentication_Under_One_Account_From_Several_IP_Addresses_Per_Day [?]	Suspicious / Authentication / Remote	▲	31 [?]
○	LOC-CR-854	GL_CONF_S01_Frequent_Configurations_On_Device [?]	/ System Configuration Management /	▲	18 [?]
○	LOC-CR-696	TTS_24_Security_Tool_Shutdown [?]	/ System Monitoring / System State	▲	1 [?]
○	LOC-CR-708	TTS_05_Critical_Errors_On_Objects [?]	Alert / Errors /	▲	1 [?]
○	LOC-CR-808	GL_OS_LIN_BUR_S01_Executed_whoami_after_opened_session [?]	Suspicious / /	▲	1 [?]

Рисунок 20.44 – Статистика срабатываний правил корреляций на вкладке Правила корреляции

4. 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 отобразится за любой произвольный период времени количество срабатываний правил корреляции, как показано на рисунке 20.45.

Идентификатор	Имя корреляции	event_src.host	event_time	event_text
2029	tts_32_brutefor...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
1998	gl_um_admin_s0...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
1995	gl_um_admin_s0...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
1982	tts_28_configur...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
201	gl_auth_s01_au...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
181	gl_conf_s01_fre...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...
181	gl_os_lin_sus_s...	dataark-0v1	...	Была зафиксирована попытка брутфорса пользователем dataark.790576a7-0794-4098-a63a-9b085c4bd...

Рисунок 20.45 – 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 20.46).

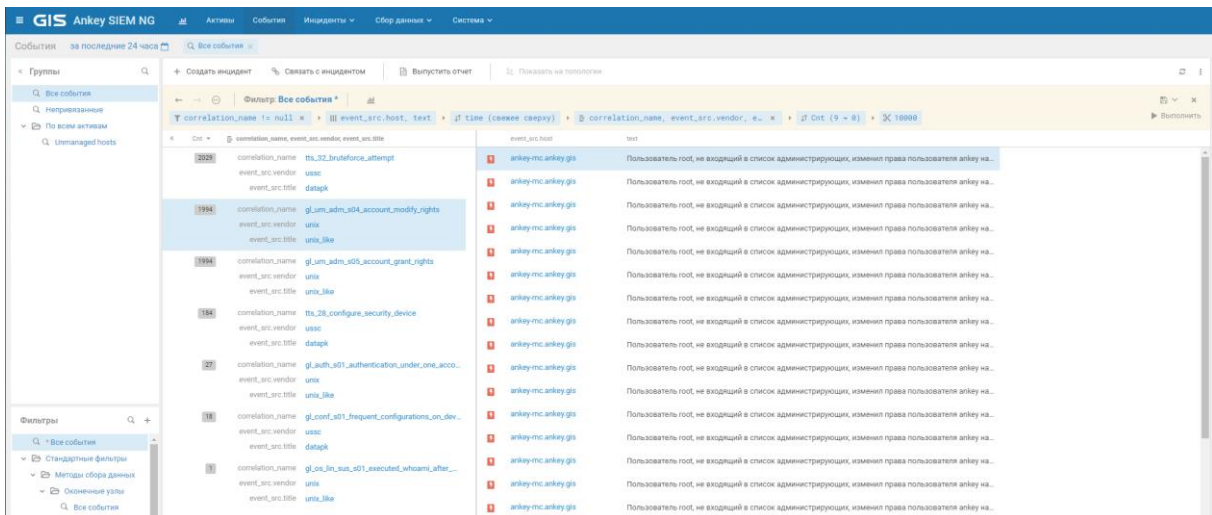


Рисунок 20.46 – Статистика по правилам корреляции с учетом источников

Возможные проблемы и их решение:

- ❖ Если правило обрабатывает слишком часто, то проверьте:
 1. Правильность заполнения 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 20.19.5) 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»⁴⁰.

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.

⁴⁰ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

20.19.5 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.

20.19.5.1 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 20.47.

COMMON_Tracking_Exceptions (справочник)

Табличный список для исключения объектов, которые не должны отслеживаться определенными правилами. rules - полное название правила. Совпадает с correlation_name. Поддерживается значение "ANY". vendor - название вендора продукта. Поддерживается значение "ANY". title - название продукта. Поддерживается значение "ANY". device_host - имя хоста. Поддерживается значение "ANY". device_ip - IP-адрес (IPv4/IPv6) или подсеть. Поддерживается значение "ANY". device_fqdn - полное доменное имя хоста. Поддерживается значение "ANY". special_fields - параметр, по которому будет происходить дополнительное исключение срабатываний. special_fields_desc - значение параметра, по которому будет происходить дополнительное исключение срабатываний. Необходимо заполнять TC значениями в нижнем регистре.

Последняя запись: 01 марта, 08:24
Создан: 01 марта, 08:24

Записи (0) Правила корреляции (340) Правила обогащения (1)

Включить Отключить

Статус	Идентификатор	Название
<input checked="" type="radio"/>	LOC-CR-16841	TTS_42_Host_Found
<input checked="" type="radio"/>	LOC-CR-16840	TTS_41_Multiple_Suspiciouse_Traffic
<input checked="" type="radio"/>	LOC-CR-16821	TTS_40_Mass_mailing_from_Internet
<input checked="" type="radio"/>	LOC-CR-16822	TTS_39_Mass_mailing_by_an_employee
<input checked="" type="radio"/>	LOC-CR-16826	TTS_38_Network_Scan_By_Compromised_Host

Рисунок 20.47 – 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».

А также можно определить из кода правила по каким полям в данном правиле можно настроить исключения. Для этого необходимо перейти на вкладку **Knowledge Base** → **SIEM** → **Пакет экспертизы** и выбрать нужное правило, открыв его, в директиве query, tracking_exceptions_query_host, будут прописаны поля, по которым можно делать исключения для срабатываний для данного правила (рисунок 20.48).

Правило корреляции TTS_14_Attempt_Authentication_With_Standard_User

```
1  
2  
3  
4 # Запрос к табличному списку конфигураций  
5 query Standart User Query ($vendor, ) from COMMON Standard_Accounts_And_Exceptions {  
6 (column::event_src.vendor == $vendor or column::event_src.vendor == "ANY")  
7  
8  
9  
10  
11 }
```

Рисунок 20.48 – Запрос к табличному списку исключений

Примечание. Для любого правила возможен собственный список исключений, подробнее указано в документах на пакеты контента «<Наименование пакета Ankey SIEM NG>. Описание».

20.19.5.2 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 обрабатывает:
 - 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 обрабатывает:
 - проверьте заполнение специальных полей, которые позволяют более тонко настроить исключения;
 - если все правильно заполнено, то сообщите в службу технической поддержки ООО «Газинформсервис»⁴¹.

⁴¹ Обращение в техническую поддержку осуществляется в соответствии с разделом 21.

20.19.6 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 21.

20.19.7 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 20.49.

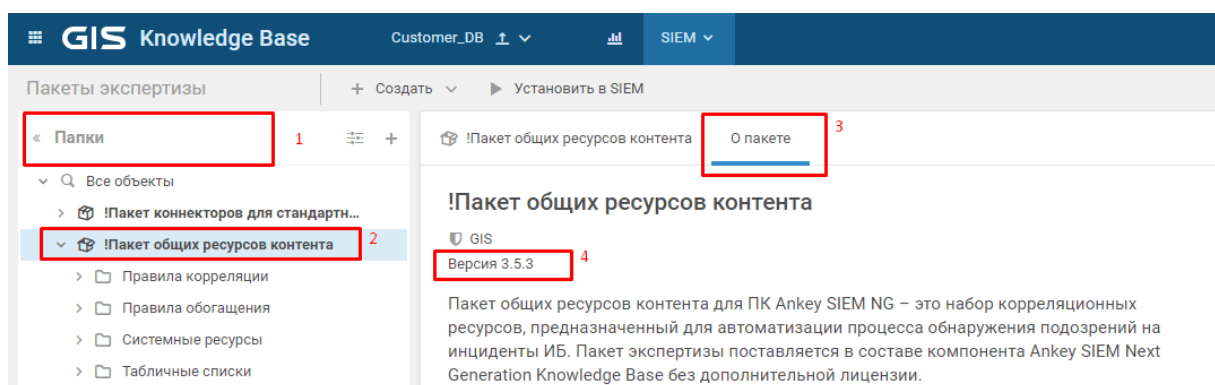


Рисунок 20.49 – Просмотр версии пакета контента в веб-интерфейсе

Номер версии пакета контента будет указан на вкладке **О пакете** в строке **Версия:<А.В.С>**.

20.20 Не все зависимые ресурсы загружены 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 20.50).

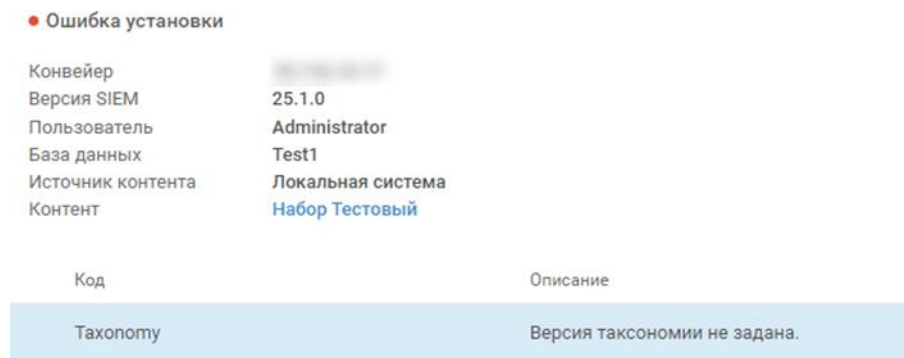


Рисунок 20.50 – Ошибка таксономии

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 4.1.2».

2. Если версия схемы полей событий не совпадает с версией SDK (рисунок 20.51), то возникает ошибка, показанная на рисунке 20.52.

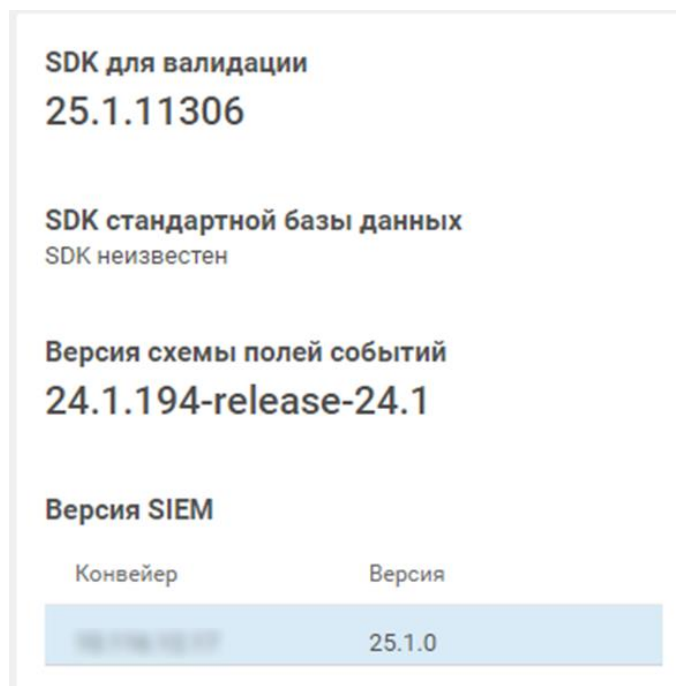


Рисунок 20.51 – Различия в версиях SDK и схемы полей

• Ошибка установки	
Конвейер	██████████
Версия SIEM	25.1.0
Пользователь	Administrator
База данных	Test1
Источник контента	Локальная система
Контент	Набор Тестовый

Код	Описание
CorulesPTKBEException	error: while validating json document 'Taxonomy' by json-schema. Invalid schema keyword 'allOf' (#/components/sch...

Рисунок 20.52 – Ошибка, возникающая при различных версиях SDK и таксономии

- 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.

- 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 20.53.

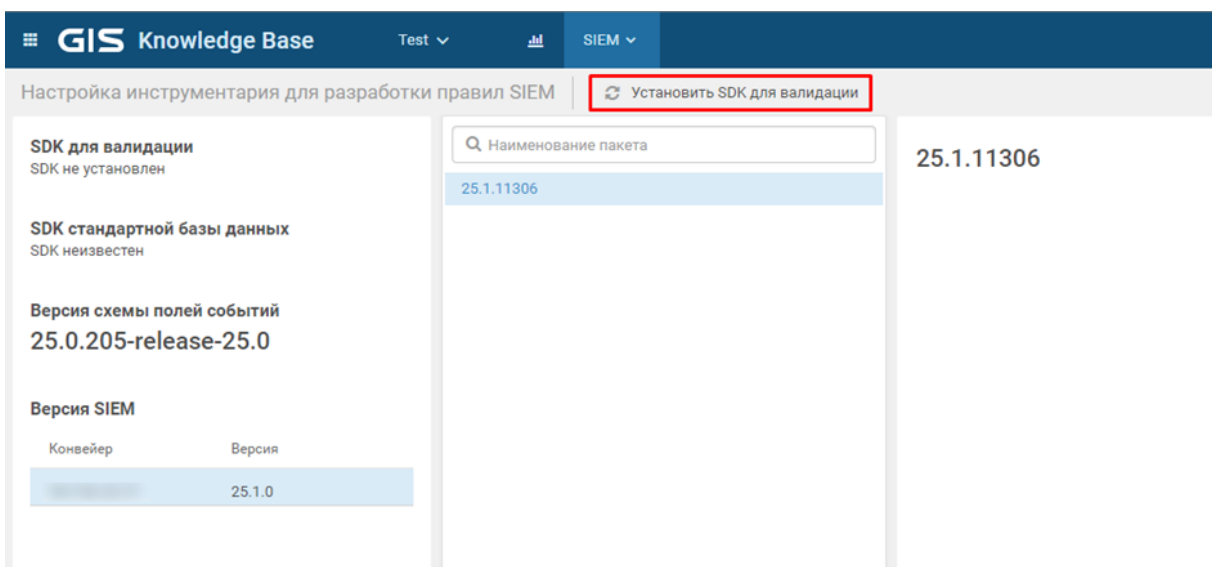


Рисунок 20.53 – Установка SDK для валидации

20.21 Справочная информация

В подразделе приведены рекомендации по выполнению шагов

инструкций.

20.21.1 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: `swapon -a`

20.21.2 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`.

20.21.3 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}}"`

20.21.4 Проверка доступности сетевого порта сервера

❖ Чтобы проверить доступность сетевого порта сервера, выполните команду:

– в терминале Linux: `telnet <IP-адрес или FQDN сервера>
<Номер порта>`

Если порт доступен, интерфейс терминала отобразит `Connected to <IP-адрес или FQDN сервера>`.

20.21.5 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:
 - если Ankey SIEM NG ES установлен на Linux – в интерфейсе терминала: `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:
 - если Ankey SIEM NG ES установлен на Linux – в интерфейсе терминала: `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`.

20.21.6 Просмотр состояния Elasticsearch

- ❖ Чтобы просмотреть состояние Elasticsearch, выполните команду:
 - если Ankey SIEM NG ES установлен на Linux – в интерфейсе терминала:
`curl localhost:9200/_cluster/health?pretty`

20.21.7 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.

20.21.8 Создание аварийного дампа памяти на Microsoft Windows

Если при попытке запуска службы она сразу останавливается, для определения причины остановки могут потребоваться аварийные дампы памяти. В них сохраняется состояние оперативной памяти на момент сбоя.

Для создания аварийного дампа вам потребуется утилита ProcDump. Вы можете скачать архив с утилитой `Procdump.zip` на сайте `docs.microsoft.com`. Перед созданием дампа необходимо распаковать архив в папку на сервере компонента Ankey SIEM NG. Команду для создания аварийного дампа необходимо выполнять в командной строке Windows PowerShell от имени администратора.

❖ Чтобы создать аварийный дамп памяти:

1. Выполните команду:

```
<Путь к папке с утилитой ProcDump>> .\procdump64.exe -w -ma -e 1 -n 5  
"<Исполняемый файл службы, для которой необходимо создать  
аварийный дамп>"
```

Например:

```
C:\Procdump> .\procdump64.exe -w -ma -e 1 -n 5  
"HealthMonitoring.Watchdog.Host.exe"
```

Примечание. Утилита выполнит пять попыток запуска службы и создаст аварийный дамп при каждой попытке.

2. Воспроизведите ситуацию, которая приводит к аварийной остановке службы.
После остановки службы DMP-файл аварийного дампа сохранится в папке с утилитой.

Аварийный дамп памяти создан.

20.21.9 Расположение индексов Elasticsearch

Путь к индексам Elasticsearch указан в качестве значения параметра path.data в файле:

- если Ankey SIEM NG ES установлен на Linux –
/etc/elasticsearch/<Название узла>/ elasticsearch_<Название узла>.yml.

Путь к архивным индексам указан в качестве значения параметра path.repo в файле:

- если Ankey SIEM NG ES установлен на Linux –
/etc/opt/siem/siem-storage/params.yaml.

20.21.10 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 20.4 – Расположение файлов журналов компонентов на Microsoft Windows

Компонент	Путь к файлам
Ankey SIEM NG Server	Файлы журналов находятся в папках C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\<Название службы>\logs и C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\log, журнал установки – в архиве C:\Users\<Логин пользователя, от имени которого выполнялась установка>\AppData\Local\Temp\Ankey_SIEM_NG_Server<Дата установки>.zip

Компонент	Путь к файлам
Ankey SIEM NG Agent	Файлы журналов находятся в папках C:\ProgramData\Gazinformservice\Ankey SIEM NG Agent\log и C:\ProgramData\Gazinformservice\Ankey SIEM NG Agent\log\modules\<Название модуля для сбора событий>, журнал установки – в файле C:\Users\<Логин пользователя, от имени которого выполнялась установка>\AppData\Local\Temp\Ankey_SIEM_NG_Agent<Дата установки>.zip
RabbitMQ	Файлы журналов находятся в папке C:\ProgramData\RabbitMQ\log

Таблица 20.5 – Расположение файлов журналов компонентов на Linux

Компонент	Путь к файлам
Ankey SIEM NG Core, Ankey SIEM NG MC, Knowledge Base, Ankey SIEM NG Agent	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
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_SqlStorage_<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. Если Ankey SIEM NG Server развернут на Linux, файл `siem.conf` находится в каталоге `/opt/siem/etc`.

21 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**.

21.1 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 20)⁴².

- журналы событий технических средств, копии экранов, которые наглядно отображают проявление неисправности,

⁴² Описание инструкций по диагностике коннекторов представлено в подразделе 20.18, контента в подразделе 20.19.

- и иные дополнительные сведения, которые могут помочь при устранении неисправности;
- наименования и версии⁴³ 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.

21.2 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 обработки;
- 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

⁴³ Для определения версии установленного коннектора см. пункт 20.18.4, для определения версии пакета контента см. пункт 20.19.7.

(подробнее см. раздел 20)⁴⁴ диагностическую информацию максимально подробно (файлы журналов, снимки экрана, результаты выполнения рекомендаций исполнителя, каналы для удаленного доступа, условия и шаги для воспроизведения проблемы, а также перечень данных из подраздела 21.1) 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)⁴⁵, 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 запроса⁴⁶.

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.

⁴⁴ Описание инструкций по диагностике коннекторов представлено в подразделе 20.18, контента в подразделе 20.19.

⁴⁵ 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.

⁴⁶ 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.

21.3 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 NG⁴⁷.
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 21.1, присутствуют в поддерживаемой релизной версии⁴⁸.

Таблица 21.1 – 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

⁴⁷ 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.

⁴⁸ 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)
<p>* 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.</p>	

21.4 Ограничения в предоставлении услуг технической поддержки

Техническая поддержка предоставляется только по продукции ПК Ankey SIEM NG⁴⁹, 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 версии⁵⁰.

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 возможностей⁵¹;

⁴⁹ 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)).

⁵⁰ 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.

⁵¹ 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 21.2 параметры/функциональные возможности отличаются от поддерживаемых, то техническая поддержка не может быть оказана, так как данный функционал отсутствует в релизной версии.

Таблица 21.2 – 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
	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
	Версия платформы ПК Ankey SIEM NG для контента (контент совместим с определенными версиями платформы)
	Неподдерживаемый коннектор (коннекторы совместимы с определенными версиями пакетов контента)
<p>* В составе последних поддерживаемых версией 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.</p>	

Направление/ Модуль SIEM	Ограничения*
**** 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 21.2).

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 набор 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 ответственности⁵² 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;

⁵² 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 документации⁵³;
- подготовка нетипового облика комплектности поставляемых изделий⁵⁴;
- 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.

⁵³ Документация предоставляется на условиях «как есть». При необходимости дополнительных инструкций нужно сформировать запрос на доработку.

⁵⁴ Изделия предоставляются на условиях «как есть». При необходимости подготовки нестандартного облика поставляемых изделий нужно сформировать запрос на доработку.

Перечень сокращений

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
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
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 облегченный вариант разработанного ITU-T протокола DAP
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)
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 удаленного 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
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
SYSLOG	–	Стандарт отправки сообщений о происходящих в системе событиях
TCP	–	Transmission Control Protocol – протоколов передачи данных интернета
TXT	–	Компьютерный файл, содержащий текстовые данные
USB	–	Universal Serial Bus – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
VPN	–	Virtual private network – технология, позволяющая обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети
XML	–	Xtensible Markup Language – расширяемый язык разметки
APM	–	Автоматизированное рабочее место
ASO	–	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
СКУД	–	Система контроля и управления доступом
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
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	–
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		
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
PgAdminPort	Порт для доступа к PgAdmin	9001
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
Параметры конфигурации роли JatobaStorage		
HostAddress	IP-адрес или FQDN сервера с установленной ролью JatobaStorage	—
JatobaLicenseActivationType	Тип активации лицензии	online
LicenseEmail	Адрес электронной почты, указанный при получении лицензии	email@email.com

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

Таблица 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 одновременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DefaultLocale	Интерфейс Ankey SIEM NG MC отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG MC	–
IamCookieLifetime	Продолжительность жизни неактивной сессии в Ankey SIEM NG (в часах)	168
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят

Параметр	Описание	Значение по умолчанию
PostgreHost	IP-адрес или FQDN сервера с установленной ролью SqlStorage или JatobaStorage	–
PostgrePassword	Пароль служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	P@sswordP@ssword
PostgreUserName	Логин служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	pt_system
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	–
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	–

Таблица 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

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
ShowDiffObjectId	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
SiemAddress	IP-адрес или FQDN сервера Ankey SIEM NG Server	localhost
SiemPort	Порт сервера Ankey SIEM NG Server для входящих подключений от Knowledge Base	8013
Smtphost	IP-адрес или FQDN SMTP-сервера	localhost
Smtppassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	–

Параметр	Описание	Значение по умолчанию
SmtпPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25
SmtпSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtпUseDefaultCredentials	Режим аутентификации SMTP-сервера: флажок установлен – для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtпUser и SmtпPassword); флажок снят – для аутентификации используются логин и пароль, указанные в параметрах SmtпUser и SmtпPassword	Флажок установлен
SmtпUser	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
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 SMTP-сервер	10

Параметр	Описание	Значение по умолчанию
EmailNotificationRetryPeriod Seconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
IncidentAggregationTimeout	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	00:01:00
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	P@sswordP@ssword
PostgreUserName	Логин служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	–
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в Ankey SIEM NG Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie20
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost

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

Таблица А.6 – Параметры конфигурации роли Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	–

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

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Agent
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ. 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 Agent к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
AgentRMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt
Agent_RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key

Таблица А.7 – Параметры конфигурации роли SIEM 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
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
	– Standalone – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для высоконагруженных систем; – ManagedStorage – значения установлены производителем и соответствуют требованиям конфигурации Ankey SIEM NG для сверхнагруженных систем; – Manual – ввод значений вручную (параметры DataNodeHeapSize, ClientNodeHeapSize, MasterNodeHeapSize)	

Параметр	Описание	Значение по умолчанию
DataNodeHeapSize	Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах). Примечание. Перед изменением параметра необходимо выбрать вариант <i>Manual</i> в качестве значения параметра <i>ClusterConfigurationProfile</i>	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). Примечание. Перед изменением параметра необходимо выбрать вариант <i>Manual</i> в качестве значения параметра <i>ClusterConfigurationProfile</i>	16g
PathData	Путь к индексам Elasticsearch. Если Ankey SIEM NG развернут для сверхнагруженных систем – путь к индексам, находящимся в «теплой» стадии	/data
PathDataHot	Путь к индексам, находящимся в «горячей» стадии	/datahot
PathLog	Путь к файлам журналов	/es_logs
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

Параметр	Описание	Значение по умолчанию
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 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 SIEM Server

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

Параметр	Описание	Значение по умолчанию
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
ElasticsearchAggregationSize	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	1000
ElasticsearchAPIVersion	Версия API, используемая для взаимодействия с Elasticsearch	7.4

Параметр	Описание	Значение по умолчанию
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
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
HighLoad	Для службы SIEM server storage выделено шесть (флажок установлен) или четыре (флажок снят) потока операционной системы	Флажок снят
LogCount	Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)	10

Параметр	Описание	Значение по умолчанию
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)	–
RemoteEventsSkipAggregator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) агрегацию реплицированных событий	Флажок установлен

Параметр	Описание	Значение по умолчанию
RemoteEventsSkipCorrelator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) корреляцию реплицированных событий	Флажок установлен
RemoteEventsSkipEnricher	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) обогащение реплицированных событий	Флажок установлен
RemoteEventsSkipResolver	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) привязку реплицированных событий к активам	Флажок установлен
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	/opt/siem/etc/rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	/opt/siem/etc/ RMQ_SIEM_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	/opt/siem/etc/ RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохраняются (флажок установлен) или не сохраняются (флажок снят) после перезагрузки брокера	Флажок установлен
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
RMQVirtualHost	Имя виртуального узла RabbitMQ для подключения Ankey SIEM NG Server	mpx
RowBatchSize	Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM Server frontend из службы (в службу) SIEM Server commander	5000
SiemOnAgent	Установлена облегченная (флажок установлен) или стандартная (флажок снят) версия Ankey SIEM NG Server	Флажок снят
StatsPublishPeriod	Период обновления данных, отображаемых в рабочей области главной страницы Ankey SIEM NG (в секундах)	30
StorageBackendType	В качестве хранилища событий используется Elasticsearch или LogSpace	elasticsearch
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (флажок установлен) или без него (флажок снят)	Флажок установлен
StoreUnnormalizedRaw	Ненормализованные события хранятся (флажок установлен) или не хранятся (флажок снят) в системе	Флажок установлен
TableListsRestorePolicy	Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestorер. Для выбора доступны следующие варианты: – disabled – автоматическое восстановление выключено; – fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери;	best_effort

Параметр	Описание	Значение по умолчанию
	<ul style="list-style-type: none"> – 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) 	
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица А.9 – Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
CACertFile	Путь к файлу корневого сертификата	rootCA.crt
CertFile	Путь к файлу публичного сертификата	RMQ_Server.crt
HostAddress	IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus	–
KeyFile	Путь к файлу закрытого ключа сертификата	RMQ_Server.pem
MEMORY_HIGH_WATERMARK	<p>Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах).</p> <p>Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений</p>	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 агентов к RabbitMQ	P@ssword
RMQAgentUser	Логин служебной учетной записи для доступа агентов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671

Параметр	Описание	Значение по умолчанию
RMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSiemPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ	P@ssword
RMQSiemUser	Логин служебной учетной записи для доступа Ankey SIEM NG Server к RabbitMQ	siem
RMQsslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
RMQ_DISK_FREE_LIMIT	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.10 – Параметры конфигурации роли Retro Correlator

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	–

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

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG RC
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
AgentRMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
AgentRMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	rootCA.crt
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG RC (возможные значения – fatal, error, warn, info, debug или trace)	info

Параметр	Описание	Значение по умолчанию
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 агента 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\Pk\authKey.pem
ClusterSeedHost	IP-адрес или FQDN сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	–
ClusterSeedPort	Порт сервера Ankey SIEM NG ES для входящих подключений от связанных приложений при выполнении распределенного поиска событий	9300
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CorePort	Порт сервера Ankey SIEM NG Core для входящих подключений от Ankey SIEM NG Server	8799
CoreRabbitAuthMethod	Аутентификация Ankey SIEM NG Server в RabbitMQ выполняется с помощью логина и пароля (plain) или с помощью сертификатов безопасности (ssl)	ssl
CoreTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)	16384
CorrRegister	Служба SIEM Server correlator запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)	True
CorrTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых данными об активах, справочной информацией и данными от репутационных сервисов (в мегабайтах)	4096
CounterRefreshInterval	Период обновления данных о счетчиках производительности (в секундах)	60

Параметр	Описание	Значение по умолчанию
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG Server (возможные значения – fatal, error, warn, info, debug или trace)	info
ElasticsearchAggregationQueryTimeout	Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)	600
ElasticsearchAggregationResponseTimeout	Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)	600
ElasticsearchAggregationSize	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	1000
ElasticsearchAPIVersion	Версия API, используемая для взаимодействия с Elasticsearch	7.4
ElasticsearchCompression	Алгоритм сжатия данных, используемый в Elasticsearch	default
ElasticsearchCountersLimit	Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (0 – количество получаемых записей не ограничено)	0
ElasticsearchDefaultQueryTimeout	Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)	600
ElasticsearchDefaultResponseTimeout	Тайм-аут выполнения запроса фильтрации событий (в секундах)	600
ElasticsearchHost	IP-адрес или FQDN сервера Ankey SIEM NG ES	localhost
ElasticsearchMaxReplySize	Максимальный размер ответа от Elasticsearch (в байтах)	524288000
EnriTableListsSize	Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)	8192
EnrRegister	Служба SIEM Server enricher запускается только после запуска службы SIEM Server commander (True) или независимо от ее запуска (False)	True
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60

Параметр	Описание	Значение по умолчанию
EventsCaseSensitiveSearch	<p>Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False).</p> <p>Примечание. Тип поиска изменится в течение суток после изменения параметра и применится только для тех событий, которые поступят после его изменения</p>	False
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	127.0.0.1
GlobalRabbitHost	<p>IP-адрес или FQDN сервера RabbitMQ.</p> <p>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</p>	127.0.0.1
GlobalRabbitPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Core	5672
LogCount	Максимальное количество файлов журналов Ankey SIEM NG Server (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов Ankey SIEM NG Server	2
LogSize	Максимальный размер файла журнала Ankey SIEM NG Server (в байтах)	104857600
MonitoringOomEnabled	Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (True) или не выполняется (False)	True
MonitoringOomMemoryLimit	Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)	60

Параметр	Описание	Значение по умолчанию
MonitoringOvertriggerEnabled	Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (True) или не выполняется (False)	True
MonitoringOvertriggerPeriod	Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)	3600
MonitoringOvertriggerThreshold	Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила	300
ProtectedRulesPath	Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)	-
RemoteEventsSkipAggregator	Площадка-получатель выполняет (False) или не выполняет (True) агрегацию реплицированных событий	True
RemoteEventsSkipCorrelator	Площадка-получатель выполняет (False) или не выполняет (True) корреляцию реплицированных событий	True
RemoteEventsSkipEnricher	Площадка-получатель выполняет (False) или не выполняет (True) обогащение реплицированных событий	True
RemoteEventsSkipResolver	Площадка-получатель выполняет (False) или не выполняет (True) привязку реплицированных событий к активам	True
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey SIEMNGServer\install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey SIEM NGServer\install\scripts\Certificates\RMQ_SIEM_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\ProgramFiles\Gazinformservice\Ankey

Параметр	Описание	Значение по умолчанию
		SIEM NG Server\install\scripts\Certificates\RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохраняются (True) или не сохраняются (False) после перезагрузки брокера	True
RMQHost	IP-адрес или FQDN сервера RabbitMQ. 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 Server frontend из службы (в службу) SIEM Server commander	5000

Параметр	Описание	Значение по умолчанию
SiemOnAgent	Установлена облегченная (True) или стандартная (False) версия Ankey SIEM NG Server	False
StatsPublishPeriod	Период обновления данных, отображаемых в рабочей области главной страницы Ankey SIEM NG	30
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (True) или без него (False)	True
StoreUnnormalizedRaw	Ненормализованные события хранятся (True) или не хранятся (False) в системе	True
TableListsRestorePolicy	Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestorer. Вы можете указать следующие значения: – disabled – автоматическое восстановление выключено; – fragile – данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери; – best_effort – в процессе восстановления допустима потеря одной-двух последних записей; – robust – в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы)	best_effort
TailcutterDbSPACE	Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)	92%
TailcutterLog	Путь к файлу журнала утилиты tailcutter	C:\ProgramData\Gazinformservice\Ankey SIEM NG Server\log\tailcutter.log
TailcutterLogLevel	Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)	WARNING
TailcutterTtl	Срок хранения индексов для событий (в днях)	365

Параметр	Описание	Значение по умолчанию
TailcutterTtlc	Срок хранения индексов для счетчиков событий (в днях)	7
WebProto	HTTP-запросы к Ankey SIEM NG Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица Б.2 – Параметры конфигурации компонента Ankey SIEM NG Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	–
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	–
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	20480M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	–

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	-
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	-
AgentName	Имя агента в веб-интерфейсе Ankey SIEM NG	FQDN сервера Ankey SIEM NG Agent
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\Program Files (x86)\Gazinformservice\Ankey SIEM NGAgent\install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\Program Files (x86)\Gazinformservice\Ankey SIEM NGAgent\install\scripts\Certificates\RMQ_Agent_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\Program Files(x86)\Gazinformservice\Ankey SIEM NG Agent\install\scripts\Certificates\RMQ_Agent_Client.key
RMQHost	IP-адрес или FQDN сервера RabbitMQ. Примечание. Брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами Ankey SIEM NG	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	P@ssword

Параметр	Описание	Значение по умолчанию
RMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Agent	5671
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Agent к RabbitMQ	mpx_agent
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SSLEnabled	Ankey SIEM NG Agent подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение	True

Приложение 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 19).

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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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- ExtAuditCritical WindowsAssets	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
Проводится расширенный аудит активов	SM3-	events_receive_interval	Максимальный период (в часах) между событиями, поступающими от одного и того же актива	120

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
(Linux)	AuditDCriticalLinuxAssets	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 Справочник категорий

Г.1 Значения полей с типом данных Enum

Поля событий `action`, `object`, `status`, `event_src.category` и `subject` могут принимать значения, указанные в таблицах ниже.

Таблица Г.1 – Значения поля `action`

Значение	Действие
access	Получение доступа
alert	Получение предупреждения
allow	Разрешение
apply	Применение
backup	Резервное копирование
bind	Присвоение IP-адреса, добавление политики в группу
call	Звонок
check	Проверка
clean	Очистка
close	Закрытие
configure	Настройка
connect	Соединение
copy	Копирование
create	Создание
decrypt	Расшифровка
deescalate	Завершение сессии с повышенными привилегиями
deliver	Доставка
deny	Запрет
detect	Обнаружение
disable	Выключение
disconnect	Разъединение
down	Изменение состояния интерфейса на down (выключение)
download	Скачивание
enable	Включение
encrypt	Зашифровка
escalate	Начало сессии с повышенными привилегиями

Значение	Действие
exclude	Исключение
execute	Выполнение
extract	Извлечение
grant	Предоставление права, привилегии
info	События, носящие информационный характер, без возможности выделить действия
initiate	Инициирование
install	Установка
leak	Утечка данных
lock	Блокирование
login	Вход в систему
logout	Выход из системы
modify	Изменение
move	Перемещение
open	Открывание
print	Распечатывание
protect	Защита
quarantine	Изолирование
receive	Принятие
reject	Отмена
remove	Удаление
rename	Переименование
reset	Сброс к состоянию по умолчанию
restart	Перезапуск
restore	Восстановление
revoke	Отзыв права, привилегии
rollback	Откат к предыдущему состоянию
scan	Сканирование
search	Поиск
send	Отправка
start	Запуск
stop	Остановка
sync	Синхронизация
terminate	Завершение

Значение	Действие
unbind	Удаление политики из группы, освобождение IP-адреса
uninstall	Удаление продукта
unlock	Разблокирование
up	Изменение состояния интерфейса на up (включение)
update	Обновление (минорное)
upgrade	Обновление (мажорное)
upload	Загрузка
view	Просмотр

Таблица Г.2 – Значения поля object

Значение	Описание
account	Учетная запись
alert	Оповещение
application	Приложение
arp_table	Таблица ARP
attack	Атака
certificate	Сертификат
check	Проверка
client	Клиент
cmdlet	Командлет
command	Команда
compliance	Соответствие требованиям безопасности
computer	Компьютер
configuration	Конфигурация
connection	Соединение
database	База данных
db_object	Объект базы данных
device	Устройство
ds_object	Объект службы каталогов
file	Файл
flow	Поток
host	Узел, для которого известен только IP-адрес или MAC-адрес
infected_object	Инфицированный объект
interface	Интерфейс

Значение	Описание
ip_address	IP-адрес
link	Ссылка
log	Файл журнала записи событий
logging	Журналирование
mailbox	Почтовый ящик
malware	Вредоносный объект
message	Сообщение
mode	Режим
module	Модуль
network	Сеть
node	Сетевой узел
package	Дистрибутив приложения
packet	Пакет
policy	Политика
port	Порт
process	Процесс
profile	Профиль
report	Отчет
request	Запрос
resource	Ресурс
rule	Правило
scan	Результат сканирования
service	Сервис
session	Сессия
socket	Программный интерфейс для передачи данных
system	Система
table	Таблица
task	Задача
transaction	Транзакция
translation	Трансляция сетевого адреса (запись в таблице NAT)
trust	Доверительное отношение (например, между доменами)
update	Обновление
user_group	Группа пользователей
virtual_machine	Виртуальная машина

Значение	Описание
volume	Том
vulnerability	Уязвимость

Таблица Г.3 – Значения поля status

Значение	Описание
failure	Неуспешная попытка
success	Успешная попытка
Ongoing	Действие происходит в данный момент. Результат выполнения еще неизвестен

Таблица Г.4 –Значения поля subject

Значение	Описание
account	Пользователь (действия выполняются от имени учетной записи)
application	Приложение
host	Узел
process	Процесс
rule	Правило
System	Система

Таблица Г.5 – Значения поля event_src.category

Значение	Описание
AAA	Аутентификация, авторизация, учетные записи
Anti-virus	Антивирусное программное обеспечение
Application security	Защита приложений
Application server	Сервер приложений (например, SAP)
Backup server	Система резервного копирования и восстановления
Certification authority	Служба сертификации (например, Microsoft Windows CA, OpenSSL)
Database server	Сервер баз данных
DHCP server	Сервер DHCP
Directory service	Служба каталогов (например, Microsoft AD, Novell eDirectory, OpenLDAP)
DLP	DLP
DNS server	Сервер DNS
DPI	Система DPI
File service	Файловая служба (например, Samba)
Firewall	Межсетевой экран
Honeypot	Honeypot
Host security	Защита узлов
IDS/IPS	IDS/IPS
Mail server	Почтовый сервер

Значение	Описание
Mobile	Мобильное устройство
Network device	Сетевое оборудование
Network monitoring system	Система мониторинга сети
Network security	Защита сети
Operating system	Операционная система
Other	Другое
Physical security	Система физической защиты (например, СКУД, видеонаблюдение)
Proxy server	Прокси-сервер
SCADA	Система SCADA
SIEM	Система SIEM
Storage device	Система хранения данных
Telecom	Система связи
Terminal services	Служба каталогов (например, Microsoft AD, Novell eDirectory, OpenLDAP)
Virtualization	Система виртуализации
Voice over IP	IP-телефония
VPN	VPN
Web security	Сетевая защита
Web server	Веб-сервер
Wireless	Беспроводная сеть

Г.2 Правила заполнения полей category.high, category.low

Правила заполнения полей корреляционных событий для категоризации событий представлены в таблице ниже.

Таблица Г.6 – Правила заполнения полей category.high, category.low

High	Low
Authentication	Default Credentials
	Host
	Local
	Remote
	Service
	Unknown Type
Authorization	Host
	Network
	Object
	User
Network Accounting	Address Translation

High	Low
	Connections & Sessions
	Firewall Rules Usage
	Traffic
User Accounting	Administrative Privilege Use
	Application & Component Launching
	Command Execution
	Data Usage
	System Accounts Use
	System Application Launching
Network Anomaly	Detection
System Anomaly	
User Behavior Anomaly	
Asset Group Management	Activation
	Creation
	Deactivation
	Deletion
	Modification
Asset Management	Domain Activation
	Domain Creation
	Domain Data Collection
	Domain Deactivation
	Domain Deletion
	Host Activation
	Host Creation
	Host Data Collection
	Host Deactivation
	Host Deletion
	Hypervisor Activation
	Hypervisor Creation
	Hypervisor Data Collection
	Hypervisor Deactivation
	Hypervisor Deletion
	Link Activation
	Link Creation
	Link Data Collection
	Link Deactivation
	Link Deletion
	Network Activation
	Network Creation
	Network Data Collection
	Network Deactivation
Network Deletion	
Virtual Host Activation	
Virtual Host Creation	
Virtual Host Data Collection	
Virtual Host Deactivation	
Virtual Host Deletion	
Attack	Bruteforce
	Complex Attack

High	Low
	DDoS
	DoS
	HIPS Alert
	Identity Theft
	IDS/IPS Alert
	Miscellaneous
	Network Attack
	Post Compromise
	Potential Attack
	Privilege Escalation
	Spam Attack
	Vulnerability Exploitation
Recon	Crawling/Dictionary Bruteforce
	Enumeration
	Fingerprinting
	Network Scan
	OS Discovery
	Port Discovery
	Service Discovery
Backup/Restore	Backup Jobs
	Backup Schedule
	Restore Jobs
Cluster Nodes	Connection
	Creation
	Deletion
	Replication
Replication	Data
	Heartbeat
	Settings
Policy Violation	Application Policy Violation
	AV Policy Violation
	Confidentiality Policy Violation
	Database Policy Violation
	IM Policy Violation
	IP Access Policy Violation
	Mail Policy Violation
	P2P Policy Violation
	Remote Access Policy Violation
	System Update Policy Violation
	Web Policy Violation
Network Configuration	Access Rule Modification
	Interface Modification
	Link Modification
	Port Detection
	Port State Change
	Routing Changes
Rights Management	Critical Privileges
	Group Assignment
	Group Creation

High	Low
	Group Deletion
	Group Modification
	Object Rights Modification
	Rights Assignment
	Rights Revocation
	Role Assignment
	Role Creation
	Role Deletion
	Role Modification
	Role Revocation
	User Membership Modification
System Configuration Management	Application Object Modification
	Application Settings Modification
	Network Service Detection
	Network Service Modification
	Network Service Resumption
	Network Service Stoppage
	OS Service Detection
	OS Service Modification
	OS Service Resumption
	OS Service Stoppage
	OS Settings Modification
	Security Settings Modification
User Management	Creation
	Deletion
	Detection
	External User Connection
	Locking
	Modification
	Unlocking
Bruteforcer	Deletion
DoS	Detection
Encryption	Exploitation
Enumeration	Installation
Exploit Kit	
Fingerprint	
Miscellaneous	
MITM	
Remote Shell	
Scanner	
Shellcode	
Sniffer	
Spoofing	
Tunnel	
Web Scanner	
CPU Management	CPU Detection
	CPU Resources Change
External Device Management	Bluetooth pairing
	Mobile device

High	Low
	Printer
	Scanner
	USB Device
External Storage Management	External Disk Detection
	External Disk Mounting
	External Disk Unmounting
	SAN/NAS Detection
	SAN/NAS Mounting
	SAN/NAS Unmounting
Hardware inventory	Hardware Configuration Errors
	Hardware Detection
	Hardware Installation
	Hardware Removal
Memory Management	Memory Resizing
Storage Management	Local Storage
	Network Storage
Incident	Creation
	Deletion
	Detection
	Modification
	Remediation
Data Loss	Accidental
	Deliberate
Data Modification	By System
	By User
Information Access Control	Assignment
	Object Access
	Settings
Information Labeling	Label Assignment
	Label Management
Information Leak	Confidential Information
	Critical Information
Leakage Channel	External Drive
	Mail
	Mobile Device
	Printer
	Web
Backdoor	Curing
Bootkit	Detection
Botnet	Epidemic
Miscellaneous	Mitigation
Rootkit	
Trojan	
Virus	
Worm	
Errors	Application
	Hardware
	Network

High	Low
	System
Network Monitoring	Interface State
	Performance
System Monitoring	Notification
	Performance
	Processes
	System State
Network Interaction	Application
	Database
	File transfer
	Mail transfer
	Remote Management
	Suspicious
	Unknown
	VPN
	Web
Operating System Management	Deletion
	Detection
	Installation
	Update
Patch Management	Deletion
	Installation
Security Software Management	Deletion
	Detection
	Installation
	Update
Software Inventory	Deletion
	Detection
	Installation
	Update
Vulnerability	Knowledge Base Updates
	Potential Exploit Detection
	Vulnerability Detection
	Vulnerability Exception
	Vulnerability Remediation

Г.3 Правила заполнения полей category.generic

Таблица Г.7 – Правила заполнения полей category.generic

Значение	Описание
Compromise	Система взломана и принадлежит атакующей стороне
Hostile	Эта категория указывает на открытую попытку компрометации систем, участвующих в этом событии

Значение	Описание
Suspicious	Эта категория указывает на необходимость дальнейшего изучения обнаруженного трафика
Recon	Эта категория указывает, что источник пытается собрать информацию об объекте
Normal	Эта категория указывает на то, что событие не является угрозой
Informational	Эта категория указывает на то, что событие не представляет угрозы и никаких действий не требуется
Warning	Эта категория указывает на возможную проблему, которая может потребовать вашего внимания в какой-то момент
Error	Сообщается об ошибке при выполнении задачи. Это не означает, что задача не была выполнена успешно
Alert	Требуется ваше немедленное внимание

Приложение Д

Структурная схема проверки работоспособности правила корреляции

На рисунке Д.1 представлена структурная схема проверки работоспособности правила корреляции, которая подробно описана в подразделе 20.19.

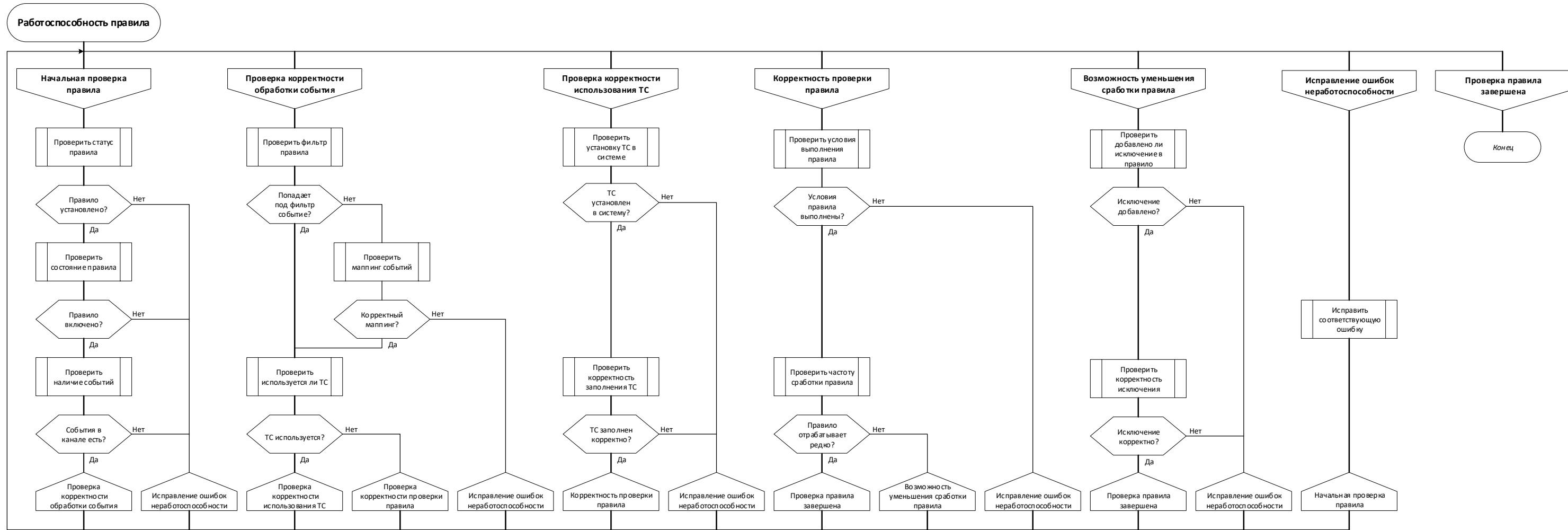


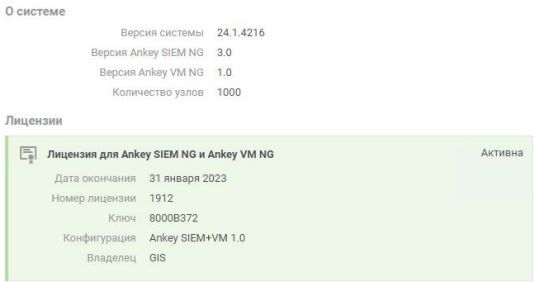
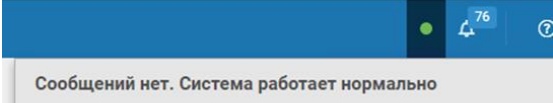
Рисунок Д.1 – Схема проверки работоспособности правила корреляции

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	4.1
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	 <p>В случае нештатного состояния необходимо предоставление полной информации обо всех предупреждениях и ошибках</p>

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 Сверхнагруженная	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 20 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 ⁵⁵	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)

⁵⁵ Для определения версии установленного коннектора см. пункт 20.18.4.

Параметры	Описание	Пример
Среда функционирования источника данных	Наименование среды функционирования (ОС) источника	RedOS 7.2
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 20.18 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 ⁵⁶	Версия изделия – пакета контента	3.4.1
Используемая версия коннектора к источнику	Версия коннектора ⁵⁷	3.1.45
Тип сбора	Тип сбора с источника	Syslog
Протокол взаимодействия	Протокол взаимодействия с источником, по которому выполняется сбор событий	tcp (514)

⁵⁶ Для определения версии пакета контента см. пункт 20.19.7.

⁵⁷ Коннекторы совместимы с определенными версиями пакетов контента.

Параметры	Описание	Пример
Среда функционирования источника данных	Наименование среды функционирования (ОС) источника	RedOS 7.2
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 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 20.19 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