GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс «Система мониторинга и управления событиями безопасности Ankey SIEM Next Generation» v.5.2.6

Обзор новых возможностей

Ankey SIEM NG®

© ООО «Газинформсервис» с 2004 года

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

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

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

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

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

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

Дата редакции документа: 3 квартал 2025 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 Общие сведения 4
1.1 О ПК Ankey SIEM NG 4
1.2 Технические ограничения 7
2 Улучшения 8
2.1 Платформа 8
2.1.1 Исправления 8
2.2 Коннекторы 8
2.2.1 Перечень новых нестандартных источников событий 10
2.2.2 Перечень нестандартных источников с новой конфигурацией 11
2.3 Контент 12
2.3.1 Основные изменения пакетов контента 13
2.3.2 Количество сигнатур мониторинга нарушений ИБ в пакетах контента 15
3 Изменения документации 18
4 Планируемые изменения 19
Перечень сокращений 20
Приложение А Доработки по улучшениям и исправлениям ошибок в направлении коннекторов 22
Приложение Б Доработки по улучшениям и исправлениям ошибок в направлении контента 33
Приложение В Перечень стандартных источников 42
Приложение Г Перечень нестандартных источников 49

1 Общие сведения

1.1 О ПК Ankey SIEM NG

ПК Ankey SIEM Next Generation (далее — Ankey SIEM NG) представляет собой программный комплекс, который предназначен для мониторинга и управления событиями безопасности в составе информационной системы.

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

Существуют следующие варианты исполнения ПК Ankey SIEM NG:

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

Примечание. Подробное описание вариантов исполнения ПК Ankey SIEM NG и их функций приведено в документе «Руководство администратора Ankey SIEM NG 5.2.6».

ПК Ankey SIEM NG предоставляет следующие возможности в зависимости от варианта исполнения, который определяется приобретенной лицензией.

Таблица 1.1 – Функции ПК Ankey SIEM NG

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

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

Возможности ПК Ankey SIEM NG	Ankey SIEM NG	Ankey SIEM NG VM[1]	Ankey SIEM NG с дополнительным компонентом VM
Визуализация данных	+	+	+
Оценка соответствия стандартам безопасности[2]	-	+	+
Пакеты экспертизы	+	-	+
Автоматизация работы с активами	+	+	+
Повторная проверка событий	+	-	+
Отправка уведомлений	+	+	+

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

ПК Ankey SIEM NG состоит из программных компонентов, которые размещаются на нескольких серверах. Такая структура обеспечивает масштабирование и позволяет внедрять ПК Ankey SIEM NG в организациях с крупными и географически распределенными ИТ-инфраструктурами. Состав компонентов определяется вариантом исполнения в зависимости от приобретенной лицензии.

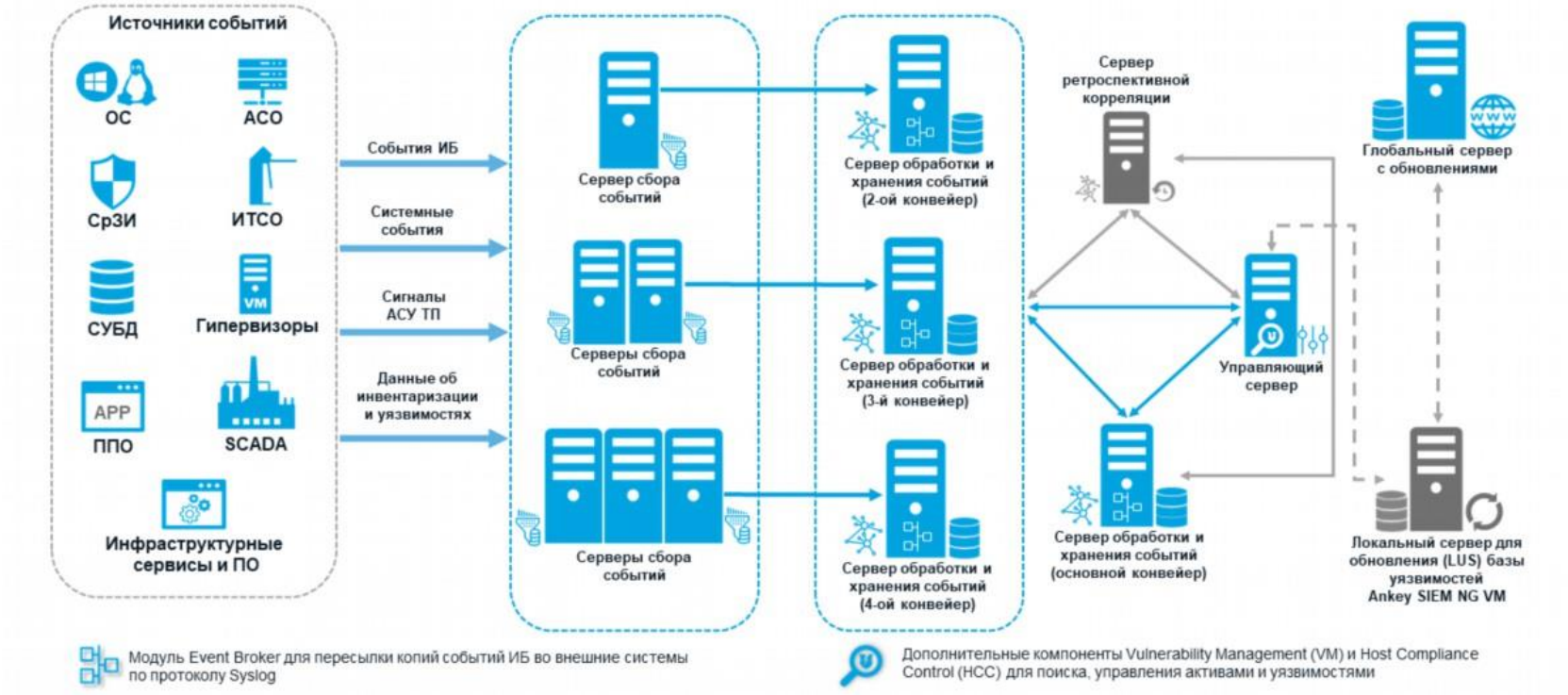


Рисунок 1.1 − Структура ПК Ankey SIEM NG

1.2 Технические ограничения

В данном подразделе представлена информация о технических особенностях ПК Ankey SIEM NG, которые необходимо учитывать для реализации корректной инсталляции и исключения ошибок при дальнейшей работе с системой.

Внимание! Начиная с 1 квартала 2026 года поддержка ПК Ankey SIEM NG версий 4.x.x прекращается. Для получения последних обновлений системы, а также для корректной работы ПК Ankey SIEM NG с новыми модулями сбора и обработки данных и модулями выявления нарушений ИБ запланируйте переход на версию 5.2. заблаговременно.

1. Если в организации установлена версия ПК Ankey SIEM NG 4.x и требуется обновить систему до последней версии 5.2.6, необходимо учитывать особенности версионного перехода. Для успешного обновления до последней версии следуйте пошаговой инструкции, описанной в документе «Инструкция по обновлению Ankey SIEM NG с версии 4.x на версию 5.x».
2. В релизах версий 5.2.x не поддерживается схема полей событий ниже 26.x.xxx-release-26.x, а также пакеты ресурсов, не соответствующие актуальной схеме полей событий. Для корректной работы с ресурсами ПК Ankey SIEM NG требуется установить схему полей событий и пакеты коннекторов и контента актуальной версии. Для успешного обновления схемы полей следуйте пошаговым инструкциям, описанным в документе «Инструкция по обновлению пакетов ресурсов с версии 3.x.x на версию 4.x.x/5.x.x».
   Если не выполнить обновление схемы полей событий и SDK до актуальной версии, то при выполнении валидации или установки ресурсов возможны ошибки.
3. Прежде чем приступать к обновлению компонентов платформы Ankey SIEM NG, рекомендуется остановить все задачи на сбор данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.
4. Начиная с 1 квартала 2024 года поддержка совместимости коннекторов и контента с версиями платформы Ankey SIEM NG 3.x прекращена.

2 Улучшения

В данном разделе описаны функции и улучшения, реализованные в релизе ПК Ankey SIEM NG v.5.2.6.

2.1 Платформа

В платформе ПК Ankey SIEM NG сформированы следующие пакеты для библиотеки системных ресурсов, которые входят в базу данных GIS_DB[3]:

- пакет коннекторов для стандартных источников — **GIS_KB_Connectors_Std_R_5.1.10**;

> **Примечание.** Информация об изменениях пакета стандартных коннекторов представлена в таблице А.1 в приложении А.

- пакет общих ресурсов контента — **GIS_KB_Content_Std_5.2.0**;
- пакет мониторинга SIEM — **GIS_KB_Content_SIEM_Monitoring_5.1.3**.

> **Примечание.** Подробная информация об изменениях данных пакетов контента представлена в подразделе 2.3, а также в таблице Б.1 в приложении Б.

Этот набор ресурсов является «коробочным» решением и поставляется совместно с ПК Ankey SIEM NG v.5.2.6.

2.1.1 Исправления

Добавлено следующие исправление для компонентов платформы Ankey SIEM NG: **Патч для исправления ошибки «В запросе указаны недоступные конвейеры»**.

Данный патч устраняет ошибку «В запросе указаны недоступные конвейеры», которая появляется при просмотре событий в веб-интерфейсе приложения Ankey SIEM NG во вкладке «События».

2.2 Коннекторы

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 и вспомогательных ресурсов. 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.

[3] Либо GIS_DB_NT, если база данных была создана для актуальных ресурсов версии 4.x.x/5.x.x на Ankey SIEM NG версии 4.1.x.

В ПК Ankey SIEM NG предусмотрены следующие типы коннекторов:

- коннекторы, предназначенные для интеграции ПК Ankey SIEM NG со **стандартными** источниками событий[4];
- коннекторы, предназначенные для интеграции ПК Ankey SIEM NG с **нестандартными** источниками событий[5].

В данном релизе расширены возможности сбора событий средствами коннекторов ПК Ankey SIEM NG. Возможности нового релиза позволяют обрабатывать события более 200 различных типов источников событий.

Теперь поддерживается совместимость с источниками, перечисленными в таблице 2.1. Были улучшены возможности сбора и обработки событий для источников событий, перечисленных в таблице 2.2.

Также в ПК Ankey SIEM NG v.5.2.6 были реализованы изменения в коннекторах, связанные с поступающими обращениями от внешних пользователей. Информация о доработках по улучшениям и исправлении ошибок приведена в приложении А.

[4] Перечень стандартных источников событий представлен в приложении В.
[5] Перечень нестандартных источников событий представлен в приложении Г.

2.2.1 Перечень новых нестандартных источников событий

Таблица 2.1 – Перечень новых нестандартных источников событий

№	Тип источника	Производитель	Наименование	Поддерживаемая версия/модель	Окружение (среда функционирования)
1	АСУ ТП	ЭЛНА	Комета	01.08.2024	Astra Linux SE 1.7
2	Инфраструктурное ПО	Eltex	ECCM	2.0	Ubuntu 20.04 & PostgreSQL 12.22
3		ИНИТИ	СОЛО	3.05	РЕД ОС
4		Протей	ВКС	15.1	Astra Linux 1.7
5		Протей	imSwitch	4 (odbclog), 5 (odbclog), 5 (filemonitor)	Astra Linux 1.7.4
6	ППО	1С-Битрикс	Битрикс24	23.300.100	Centos 7 & MySQL 5.7
7		OpenText	Archive Server	16.0.0	SLES11 & SAP HANA / Oracle / MS SQL
8		OpenText	Content Server	16.0.5	Linux & SAP HANA Windows & SAP HANA
9		OpenText	Directory Server	1.18	Linux Windows
10		Sarex	SRX	1.1.12	CentOS 8 & PostgreSQL 10.23
11		Газпром ЦПС	ИС ПНР	2.7	Linux
12		РЕД СОФТ	РЕД DC	2.0.0	РЕД ОС 7.3
13		СИНТЕЛЛЕКТ	TESSA	3.5	Astra Linux CE & PostgreSQL 14.4
14	СрЗИ	R-Vision	SOAR	5.4	Astra Linux 1.7
15		Газинформсервис	SafeERP CS EM	4.9.5	РЕД ОС & PostgreSQL 9.6.4 & Container
16	СУБД	Opensource	ClickHouse	22.1.3.7	Debian 11

2.2.2 Перечень нестандартных источников с новой конфигурацией

Новая конфигурация источника — это переработка функционала, которая включает одно или более крупное изменение, например:

- изменение метода/методов сбора с источника событий;
- изменение окружения источника событий;
- добавление новой версии/версий источника событий.

Примечание. Подробная информация о дополнительных коннекторах и указанных изменениях приведена в документации на использование дополнительного коннектора, которая поставляется в рамках приобретения такого изделия.

Таблица 2.2 – Перечень нестандартных коннекторов с обновленной конфигурацией

№	Тип источника	Производитель	Наименование	Поддерживаемая версия/модель	Окружение (среда функционирования)	Описание изменений
1	ППО	SAP	BO	3.1, 4.2	3.1: SUSE Linux Enterprise Server 11 & Oracle Database 11.2 4.2: SUSE Linux Enterprise Server 12 & SQL Anywhere 17	Добавлена поддержка версии 3.1
2	Системы виртуализации (гипервизоры)	OrionSoft	zVirt	3.0, 4.2	Собственная ОС	Добавлена поддержка версии 4.2
3	СрЗИ	Аладдин РД	Enterprise Certification Authority	2.0.1.367, 2.2.1.286	RedOs 7.3, Astra Linux 1.7.5 / PostgreSQL 11.21, Jatoba	Добавлена поддержка версий 2.2.0, 2.2.1

2.3 Контент

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), разработанный экспертами и аналитиками ИБ ООО «Газинформсервис», предназначенный для автоматизации процесса предупреждения, обнаружения и реагирования на инциденты ИБ.

В ПК Ankey SIEM NG предусмотрены следующие пакеты контента:

- **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;
- **пакет мониторинга SIEM** — коробочный набор инструментов мониторинга и выявления инцидентов, которые предназначены для автоматизации процесса обнаружения подозрений на инциденты ИБ. Пакет функционирует на событиях внутреннего аудита ПК Ankey SIEM NG и позволяет выполнять контроль за ресурсами системы и действиями пользователей в системе;
- **пакет инфраструктурного контента** — наборы инструментов мониторинга и выявления инцидентов для различных типов источников (не является «коробочным» решением);
- **пакет мониторинга ПО SCADA** — наборы инструментов мониторинга и выявления инцидентов для источников событий типа АСУ ТП (не является «коробочным» решением);
- **пакет мониторинга SOC** — наборы инструментов мониторинга и выявления инцидентов, которые предназначены для выявления распределенных атак на различные дочерние общества. Верхнеуровневая корреляция, включающая кросскорреляцию между различными подчиненными площадками, применяемая в SOC для выявления зависимостей между инцидентами в своей зоне ответственности (не является «коробочным» решением);
- **пакет обнаружения компьютерных атак (корпоративный сегмент)** — наборы инструментов мониторинга и выявления инцидентов, которые предназначены для выявления вредоносной активности в инфраструктуре на основе матрицы MITRE ATT&CK, а также для последующего построения цепочек атак и их обогащения в случае распределенного во времени развития атаки (не является «коробочным» решением);
- **пакет мониторинга ППО** — это наборы инструментов для автоматизации процесса обнаружения подозрений на инциденты ИБ (не является «коробочным» решением).

2.3.1 Основные изменения пакетов контента

Для всех пакетов контента реализованы следующие общие изменения:

- реализована совместимость с источниками, представленными в таблицах 2.1 и 2.2;
- реализован функционал выбора сущности, регистрируемой по результатам работы правила корреляции (**event/incident**) с возможностью конфигурации различных параметров (агрегация инцидентов, важность и пр.);
- реализованы улучшения и устранены ошибки, связанные с поступающими обращениями от внешних пользователей.

Примечание. Детальная информация о доработках по улучшениям и исправлении ошибок приведена приложении Б.

Для **пакета общих ресурсов контента** реализованы следующие ключевые изменения:

- переработана логика работы правил на выключение устройств и средств защиты информации. Предусмотрено каскадное срабатывание правил корреляции (из состава пакета инфраструктурного контента) на основе влияния выключения конкретного хоста на состав запущенных сервисов и различного ПО;
- проработан механизм исключений по пустому значению поля (внедрено в рамках правила «TTS_28_Configure_Security_Tool» для регигистрации изменений конфигурации средства защиты информации).

Для **пакета инфраструктурного контента** реализованы следующие ключевые изменения:

- проведен рефакторинг группы правил на управление пользователями. Правила вынесены в отдельный дочерний пакет «ПИК. Управление пользователями, группами и ролями». Правила корреляции разделены по сущностям. Добавлена сущность «роль» для контроля на источниках событий. Для каждой сущности реализованы кейсы создания, изменения, удаления, отзыва прав и прочие действия;
- реализованы правила корреляции для детектирования следующий кейсов:
  - множественное изменение политик безопасности;
  - множественное удаление политик безопасности;
  - множественное изменение паролей УЗ;
  - попытка повышения привилегий до суперпользователя под не привилегированным пользователем;
  - неразрешенная аутентификация пользователя (под любым пользователем с ограничениями на аккаунт).
- в рамках переработки правил на выключение устройств и средств защиты информации добавлены новый кейсы:
  - остановка базы данных;
  - выключение критичных сервисов или ПО.

Для **пакета обнаружения компьютерных атак (корпоративный сегмент)** реализованы следующие ключевые изменения:

- проведена оптимизация работы отдельных правил для уменьшения ложноположительных срабатываний, а также дублирования срабатываний между правилами пакета;
- выполнена доработка исключений для правил на контроль реестра Windows с возможностью исключения по полному пути исполняемого файла (на основе регулярных выражений).
- теперь поддерживаются[6] новые векторы кибератак:
  - Восстановление паролей из NTDS.dit;
  - NTLM relay. To MsSQL;
  - NTLM relay. To LDAP(S);
  - NTLM relay. HTTP -> LDAP(S);
  - NTLM relay. SMB -> LDAP(S) (remove-mic);
  - SMBleed (CVE-2020-1206);
  - NTLM relay. MS08-068 (SMB relay);
  - Blind kerberoasting;
  - Sudo heap-based buffer overflow (CVE-2021-3156);
  - Возможность получения учетных данных DPAPI и CredHist;
  - NTLM relay. To SMB;
  - DCsync (Mimicatz);
  - MTE_EXP_CVE_2022_26923;
  - Zone Transfer. AXFR-атака;
  - DNS Spoofing;
  - DNS cache poisoning;
  - Skeleton Key;
  - GoldenTicket;
  - Возможность редактирования PATH;
  - Анонимный доступ по LDAP;
  - Сканирование PingCastle;
  - SMB Spoofing;
  - Перечисление пользователей (Enumeration);
  - Перечисление LDAP (LDAP enumerate);
  - Перечисление пользователей (Users enumerate);
  - Анонимный доступ по SMB (NULL-сессии);
  - WebDAV-coerce;
  - PSPKIAudit;
  - Сканирование PingCastle (RedADM);
  - Использование инструмента adPeas;
  - NTLM relay. To WSUS HTTP;
  - DC-Sync (RedDC);
  - Pass_The_Hash (RedADM);
  - Forest Trust (новая реализация);

[6] Дополнительные функции поставляются в виде расширения к пакету обнаружения компьютерных атак (корпоративный сегмент).

- Возможность получения учетных данных DPAPI и CredHist (новая реализация);
- PSPKIAudit;
- adPeas;
- Получение пароля LAPS;
- Получение пароля GMSA.

Сформированы новые релизы пакетов контента ПК Ankey SIEM NG. В таблице 2.3 представлены версии, описание пакетов и количество сигнатур мониторинга нарушений ИБ, входящих в данные пакеты. Подробная информация об изменениях функционала пакетов контента приведена в списке изменений к каждому пакету.

2.3.2 Количество сигнатур мониторинга нарушений ИБ в пакетах контента

Таблица 2.3 − Количество сигнатур мониторинга нарушений ИБ

Наименование пакета	Версия пакета	Количество сигнатур мониторинга нарушений ИБ	Описание пакета
Пакет общих ресурсов контента	5.2.0	Всего: 46 Новые: 0 Обновлено: 46	Пакет является основой для всех остальных пакетов контента и содержит: – общие макросы; – общие табличные списки; – общие правила обогащения; – набор правил корреляции для выявления инцидентов информационной безопасности (правила TTS) Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет общих ресурсов контента. Список изменений»
Пакет инфраструктурного контента	5.2.0	Всего: 376 Новые: 73 Обновлено: 303	Контент для выявления инцидентов ИБ в инфраструктуре. В состав пакета экспертизы входят наборы правил корреляции (GL_) для следующих типов источников: – операционные системы (ОС); – активное сетевое оборудование (АСО); – системы управления базами данных (СУБД); – системы резервного копирования и восстановления информации (СРКВИ); – электронная почта; – DNS; – DHCP;

Наименование пакета	Версия пакета	Количество сигнатур мониторинга нарушений ИБ	Описание пакета
			– веб-серверы; – гипервизоры; – межсетевые экраны (МЭ); – средства контроля конфигураций; – IDS; – антивирусы; – DLP; – PKI; – VPN. А также в состав пакета входят общие правила для всех типов источников (аутентификация, службы, файлы, лицензии, управление пользователями и пр.) Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет инфраструктурного контента.Список изменений»
Пакет мониторинга ПО SCADA	5.1.1	Всего: 22 Новые: 0 Обновлено:22	Контент для выявления инцидентов ИБ в сегменте АСУ ТП для источников типа SCADA Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет мониторинга ПО SCADA.Список изменений»
Пакет мониторинга SOC	5.2.0	Всего: 12 Новые: 0 Обновлено: 12	Контент для выявления распределенных атак на различные дочерние общества, функционирует на верхнем уровне иерархии ПК Ankey SIEM NG Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет мониторинга SOC.Список изменений»
Пакет мониторинга SIEM	5.1.3	Всего: 0 Новые: 0 Обновлено: 8	Контент для выявления воздействия на ключевые ресурсы (задачи сбора, правила корреляции, табличные списки) платформы Ankey SIEM NG со стороны пользователей и системы. Функционирует на событиях

Наименование пакета	Версия пакета	Количество сигнатур мониторинга нарушений ИБ	Описание пакета
			внутреннего аудита ПК Ankey SIEM NG Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет мониторинга SIEM.Список изменений»
Пакет обнаружения компьютерных атак (корпоративный сегмент)	5.2.2	Всего: 237 Новые: 1 Обновлено: 236 **Расширение[7]:** Всего: 189 Новые: 45 Обновлено: 26	Контент для выявления вредоносной активности в инфраструктуре на основе матрицы MITRE ATT&CK. Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет обнаружения компьютерных атак (КС).Список изменений»
Пакет мониторинга ППО	5.1.1	Всего: 14 Новые: 0 Обновлено: 14	Контент для автоматизации процесса обнаружения подозрений на инциденты ИБ. Информация об изменениях и состав изменений по поддерживаемым источникам представлены в документе «Пакет мониторинга ППО.Список изменений»

[7] Подробнее о расширении пакета ПОКА (КС) – в списке изменений пакета ПОКА (КС) на странице *14*.

3 Изменения документации

Проведена актуализация эксплуатационной документации в соответствии с особенностями нового релиза.

4 Планируемые изменения

Планируется выход новых релизов в следующем порядке:

- ПК Ankey SIEM NG 5.2.7 (4 квартал 2025 года).

Начиная с 1 квартала 2026 года поддержка ПК Ankey SIEM NG версий 4.x.x прекращается. Для получения последних обновлений системы, а также для корректной работы ПК Ankey SIEM NG с новыми модулями сбора и обработки данных и модулями выявления нарушений ИБ требуется переход на версию 5.2.

Перечень сокращений

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
DNS	–	Domain Name System — компьютерная распределенная система для получения информации о доменах
EB	–	Модуль Ankey SIEM Next Generation Event Broker
IP	–	Internet Protocol — маршрутизируемый протокол сетевого уровня стека TCP/IP
PKI	–	Public Key Infrastructure — набор средств, используемых для поддержки криптозадач на основе закрытого и открытого ключей
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
SOC	–	Security Operations Center — центр управления безопасностью отвечает за защиту организации от киберугроз
VPN	–	Virtual private network — технология, позволяющая обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети
АСО	–	Активное сетевое оборудование
АСУ ТП	–	Автоматизированная система управления технологическим процессом
ЗПС	–	Замкнутая программная среда
ИБ	–	Информационная безопасность
ИТ	–	Информационные технологии

ОС	–	Операционная система
ПАК	–	Программно-аппаратный комплекс
ППО	–	Прикладное программное обеспечение
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных
УЗ	–	Учетная запись
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю Российской федерации

Приложение А
Доработки по улучшениям и исправлениям ошибок в направлении коннекторов

Доработки по улучшениям и исправлениям ошибок стандартных коннекторов приведены в таблице А.1.

Примечание. Подробная информация о указанных изменениях приведена в документе «Руководство по интеграции с источниками Ankey SIEM NG 5.2.5. Список изменений».

Таблица А.1 – Описание доработок по улучшениям и исправлениям ошибок стандартных коннекторов

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-13736	Улучшение	Cisco IOS	5.1.2	В формуле нормализации GIS_Cisco_IOS_syslog_PORT_SECURITY_PSECURE_VIOLATION (SEC-ALERT-042) доработан парсер. Обновление позволило обрабатывать новый тип события, содержащего в себе дополнительную информацию: (sw-n-11-1-1)
SIEMINT-6025	Улучшение			Добавлено 11 событий источника (APP-CONNECT-001, APP-DISCONNECT-001, SYS-ALERT-001, SYS-INFO-006, APP-CONNECT-002, APP-DISCONNECT-002, APP-DETECT-001, SYS-ALERT-002, SEC-MODIFY-017, SYS-ALERT-003, SYS-ENCRYPT-001)
SIEMINT-7462	Исправление	Газинформсервис Ankey SIEM NG Internal	4.1.6	Добавлено заполнение полей external_src.host/external_dst.host в файле appendix.xp
SIEMINT-8241	Исправление			Добавлено заполнение поля recv_host в файле appendix.xp
SIEMINT-12279	Улучшение	Лаборатория Касперского Security Center & Security Center Network Agent &	4.1.13	Изменен маппинг событий для того, чтобы получить возможность отключать ложную сработку правила корреляции

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-13870	Исправление	Endpoint Security & Security For Virtualization & Security For Virtualization Light Agent & Security For Windows Servers & Industrial Cybersecurity For Nodes & Endpoint Security For Linux		В формуле нормализации GIS_Kaspersky_Security_Center_syslog_KLAUD_EV_OBJECTMODIFY исправлен маппинг поля event_src_fqdn, event_src_hostname, event_src_ip
SIEMINT-14304	Исправление			В формуле нормализации GIS_Kaspersky_Security_Center_syslog_GNRL_EV_DEVCTRL_DEV_UNPLUGGED (SEC-DISCONNECT-001) изменен маппинг поля object.type
SIEMINT-14863	Улучшение	Microsoft Active Directory Federation Services	4.1.6	Разработана формула нормализации GIS_Microsoft_ADFS_wineventlog_2889_LDAP_bind_connection (APP-INFO-001) для обработки нового события с msgid = 2889
SIEMINT-13821	Улучшение			
SIEMINT-15014	Исправление	Microsoft Sysmon	5.1.5	Из формулы нормализации GIS_Microsoft_Windows_eventlog_Sysmon_13_Registry_value_changed удалено поле object.new_value
SIEMINT-16177	Исправление	Microsoft Windows	5.1.1	В формуле нормализации GIS_Microsoft_Windows_eventlog_4769_Kerberos_service_ticket_requested доработан маппинг (4769). Информация про протокол маппится в поле datafield3, datafield8
SIEMINT-5967	Улучшение			Разработаны формулы нормализации под 65 новых событий: – GIS_Microsoft_Windows_eventlog_1000_Application_Error – GIS_Microsoft_Windows_eventlog_10000_Starting_Session – GIS_Microsoft_Windows_eventlog_10001_Ending_Session – GIS_Microsoft_Windows_eventlog_10005_Machine_Restart_Is_Required – GIS_Microsoft_Windows_eventlog_10020_Incorrect_Security_Descriptor – GIS_Microsoft_Windows_eventlog_10028_Dcom_Connection_Computer_Could_Not_Established – GIS_Microsoft_Windows_eventlog_1003_Software_Protection_Platform_Completed_Licensing_Status_Check

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				– GIS_Microsoft_Windows_eventlog_10036_Server_Authentication_Level_Policy_Does_Not_Allow – GIS_Microsoft_Windows_eventlog_1023_Windows_Cannot_Load_Extensible_Counter – GIS_Microsoft_Windows_eventlog_1033_Software_Protection_Platform_Policies_Excluded – GIS_Microsoft_Windows_eventlog_1034_Duplicate_Policy_Definition_Detected – GIS_Microsoft_Windows_eventlog_1040_Windows_Installer_Beginning_Transaction – GIS_Microsoft_Windows_eventlog_105_Timer_Starvation_Has_Been_Detected – GIS_Microsoft_Windows_eventlog_106_Timer_Starvation_Has_Subsided – GIS_Microsoft_Windows_eventlog_1066_Software_Protection_Platform_Object_State – GIS_Microsoft_Windows_eventlog_1085_Windows_Failed_To_Apply_Settings – GIS_Microsoft_Windows_eventlog_1130_Error – GIS_Microsoft_Windows_eventlog_11705_Windows_Installer_Application_Install_Failure – GIS_Microsoft_Windows_eventlog_11728_Windows_Installer_Configuration_Completed_Successfully – GIS_Microsoft_Windows_eventlog_12288_The_Client_Sent_An_Activation_Request – GIS_Microsoft_Windows_eventlog_12289_The_Client_Receive_Answer – GIS_Microsoft_Windows_eventlog_12325_User_Has_Reached_The_Quota_Limit_For_Quota – GIS_Microsoft_Windows_eventlog_14554_Dfs_Share_Acquire_Success

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				– GIS_Microsoft_Windows_eventlog_1502_The_Group_Policy_Settings_Processed_Successfully – GIS_Microsoft_Windows_eventlog_1503_The_Group_Policy_Settings_For_User_Processed_Successfully – GIS_Microsoft_Windows_eventlog_1530_User_Registry_Handles_Leaked – GIS_Microsoft_Windows_eventlog_154_The_Io_Operation_Failed – GIS_Microsoft_Windows_eventlog_16_Access_Log_In_Bush – GIS_Microsoft_Windows_eventlog_16384_Software_Protection_Platform_Restart_Successfully_Scheduled – GIS_Microsoft_Windows_eventlog_2003_The_Configuration_Information_Does_Not_Match – GIS_Microsoft_Windows_eventlog_2006_Unable_Read_Server_Queue_Performance_Data – GIS_Microsoft_Windows_eventlog_3036_Could_Not_Complete_The_Craw – GIS_Microsoft_Windows_eventlog_4098_Group_Policy_Did_Not_Apply – GIS_Microsoft_Windows_eventlog_4102_Threshold_Value_Has_Been_Reached – GIS_Microsoft_Windows_eventlog_4107_Error_Extracting_Root_List – GIS_Microsoft_Windows_eventlog_4227_A_Tcp_Ip_Error_Has_Occurred – GIS_Microsoft_Windows_eventlog_45057_Login_Cache_Entry_Has_Been_Deleted – GIS_Microsoft_Windows_eventlog_45058_Login_Cache_Entry_Has_Been_Deleted – GIS_Microsoft_Windows_eventlog_4797_An_Attempt_Check_Blank_Password

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				– GIS_Microsoft_Windows_eventlog_4825_A_User_Was_Denied_The_Access_To_Remote_Desktop – GIS_Microsoft_Windows_eventlog_501_Policy_Has_Been_Successfully_Applied – GIS_Microsoft_Windows_eventlog_5031_The_Windows_Firewall_Blocked_Application_From_Incoming_Connections – GIS_Microsoft_Windows_eventlog_5379_Credential_Manager_Credentials_Were_Read – GIS_Microsoft_Windows_eventlog_5380_Vault_Find_Credential – GIS_Microsoft_Windows_eventlog_5381_Vault_Credentials_Were_Read – GIS_Microsoft_Windows_eventlog_5382_Vault_Credentials_Were_Read – GIS_Microsoft_Windows_eventlog_5723_The_Session_Setup_From_Computer_Failed – GIS_Microsoft_Windows_eventlog_5807_IP_Addresses_Do_Not_Map_Any_Existing_Sites – GIS_Microsoft_Windows_eventlog_6038_Detect_Connection_Nt ml – GIS_Microsoft_Windows_eventlog_6281_Code_Integrity_Detect_Not_Valid_Hashes_For_Image – GIS_Microsoft_Windows_eventlog_7001_Unable_Create_Shadow_Copy – GIS_Microsoft_Windows_eventlog_7002_User_Logout_Notification – GIS_Microsoft_Windows_eventlog_7006_The_ScRegSetValueExW_Call_Failed – GIS_Microsoft_Windows_eventlog_8192_Group_Policy_Did_Not_Apply – GIS_Microsoft_Windows_eventlog_8197_The_Activation_Program_Has_Been_Launched

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				– GIS_Microsoft_Windows_eventlog_8198_License_Activation_Failure – GIS_Microsoft_Windows_eventlog_8200_Information_About_License_Purchase_Failure – GIS_Microsoft_Windows_eventlog_8208_Failure_Purchase_Genuine_Ticket – GIS_Microsoft_Windows_eventlog_8224_The_VSS_Service_Is_Shutting_Down_Timeout – GIS_Microsoft_Windows_eventlog_8230_The_Rule_Handler_Successfully_Re_Processed_Schedule – GIS_Microsoft_Windows_eventlog_900_Software_Protection_Platform_Starting – GIS_Microsoft_Windows_eventlog_9009_Desktop_Window_Manager_Stop – GIS_Microsoft_Windows_eventlog_902_Software_Protection_Platform_Start – GIS_Microsoft_Windows_eventlog_903_Software_Protection_Platform_Stop
SIEMINT-6119	Улучшение			Для события 4656 добавлен маппинг AccessMask в поле datafield7
SIEMINT-11928	Исправление	Positive Technologies Application Firewall	4.1.5	Исправлена ошибка скрипта CustomEventCollector Исправлена нормализация событий, получаемых через CustomEventCollector
SIEMINT-13275	Улучшение			Доработана обработка события для GIS_pt_application_firewall_syslog_structured_attack_detected
SIEMINT-11970	Исправление	Positive Technologies Multiscanner	4.1.9	Доработан скрипт CustomEventCollector при объединении коннекторов PT Multiscanner и PT Sandbox. Исправлены ошибки
SIEMINT-11807	Улучшение	Positive Technologies Network Attack Discovery	4.1.6	Добавлено 8 новых событий для сообщений типа syslog_notifier.detection

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-15887	Исправление	Русбитех & Red Hat & РЕД СОФТ & Базальт СПО & FreeBSD Team & AlmaLinux Astra Linux Special Edition 1.6, 1.7 CentOS 6, 7 Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x РЕД СОФТ РЕД ОС 7.1, 7.2, 7.3 Альт Сервер 8 СП, 10.1 Альт Виртуализация 10.1 FreeBSD 11.0 AlmaLinux 8.9	5.1.1	Исправлена формула нормализации для корректной нормализации события монтирования папки
SIEMINT-15899	Исправление			Исправлен маппинг полей: – subject.account.name – object.account.name
SIEMINT-15064	Исправление			Исправлена локализация для правила нормализации GIS_UNIX_like_auditd_syslog_syscall_o. Добавлено заполнение поля subject.account.name
SIEMINT-15063	Исправление			Доработана формула нормализации GIS_UNIX_like_auditd_syslog_syscall_o
SIEMINT-6440	Исправление			Изменен маппинг событий для работы правил корреляции (SYS-SHUTDOWN-001)
SIEMINT-6172	Улучшение			Добавлено 25 событий источника (SEC-ALERT-010, SEC-CONNECT-001, SEC-DELETE-001, SEC-DISCONNECT-002, SEC-GRANT-002, SEC-MODIFY-014, SEC-MODIFY-015, SEC-REQUEST-001, SEC-VIEW-101, SYS-ALERT-002, SYS-ERROR-002, SYS-INFO-0{26-33}, SYS-MODIFY-115, SYS-MODIFY-116, SYS-START-020, SYS-START-021, SYS-STOP-004, SYS-STOP-006)
SIEMINT-13371	Исправление			Добавлены новые условия в блок filter (уровень журналирования) для конфигурационного файла syslog-ng. Добавлен блок об отключении службы systemd-journald-audit
SIEMINT-11260	Исправление			Добавлены новые условия в блок filter для конфигурационного файла syslog-ng
SIEMINT-15062	Исправление			Исправлена формула нормализации GIS_UNIX_like_common_syslog_ssh_login_fail
SIEMINT-14500	Улучшение			Добавлено 10 событий источника (SYS-RESTART-005, SYS-STOP-020, SYS-INFO-039, SYS-MODIFY-017, SYS-START-022, SYS-READ-001, SEC-MODIFY-012, SYS-INFO-041, SYS-READ-002, SYS-INFO-040), изменен маппинг 50 событий для соответствия схеме полей

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-14891	Исправление			Исправлена формула нормализации GIS_UNIX_like_auditd_syslog_structured_user_start
SIEMINT-15010	Исправление			Исправлена формула нормализации GIS_UNIX_like_auditd_syslog_structured_syscall_link_remove
SIEMINT-14920	Улучшение	VMware ESXi	4.1.7	Добавлена формула нормализации GIS_VMware_ESXi_syslog_Vmkernel_Requested_Promiscuous_Mode (SYS-MODIFY-001) для одного нового события

Доработки по улучшениям и исправлениям ошибок дополнительных коннекторов приведены в таблице А.2.

Примечание. Подробная информация о дополнительных коннекторах и указанных изменениях приведена в документации на использование дополнительного коннектора, которая поставляется в рамках приобретения такого изделия.

Таблица А.2 – Описание доработок по улучшениям и исправлениям ошибок дополнительных коннекторов

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-10736	Улучшение	RedCheck. Module Data RedCheck. Internal	4.1.2	– объединены тесты покрытия правилами корреляции для источников RedCheck.Module Data и RedCheck.Internal; – объединена документация для источников RedCheck.Module Data и RedCheck.Internal
SIEMINT-15162	Исправление	УЦСБ DATAPK	5.1.2	Доработано 1 правило агрегации GIS_USSC_DATAPK_SYSLOG_several_start_suricata_fail (SYS-START-203). Удалено поле datafield4 для корректной сработки
SIEMINT-11441	Улучшение	Киберпротект Кибер Бэкап	4.1.10	Исправлен маппинг object.account.privileges в правиле обогащения GIS_Cyberprotect_Cyber_Backup_enrich_role_modify_acronis_v16_events
SIEMINT-14831	Улучшение			Изменен маппинг поля subject.account.name, в зависимости от заполнения полей в исходном (сыром) событии

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
SIEMINT-13659	Улучшение	Eltex Routing OS	4.1.8	Добавлено 1 событие источника (SYS-ALERT-017)
SIEMINT-8859	Улучшение	Газинформсервис Ankey ASAP	4.1.5	Изменены формулы нормализации для типов событий: – SEC-LOGIN-001 – SEC-LOGIN-101
SIEMINT-11564	Исправление			Проверена и актуализирована нормализация для работы правил: – GL_UM_ADM_S03 – GL_UM_ACC_S03 – GL_UM_S02 – GL_AUTH_S1
SIEMINT-16053	Исправление	Газинформсервис Efros CI	4.1.4	Исправлен маппинг полей: – subject.account.name; – subject.account.domain
SIEMINT-15088	Исправление	Infotecs VipNet xFirewall & VipNet Coordinator	4.1.7	Исправлена логика заполнения полей: – src.host; – dst.host
SIEMINT-5970	Улучшение			Добавлено 27 событий источника (APP-CHANGE-01{6-9}, APP-CHECK-0{17-25}, APP-CHECK-123, APP-DETECT-001, SEC-LOGIN-022, SEC-LOGOUT-009, APP-ERROR-005, APP-MOUNT-001, APP-SAVE-003, APP-SET-01{5-7}, APP-START-028, APP-UPDATE-0{09-10}, APP-CHANGE-021)
SIEMINT-11046	Улучшение	Лаборатория Касперского Secure Mail Gateway & Security For Linux Mail Server	4.1.6	Доработано правило GIS_kaspersky_lab_SM_send_message. Добавлена передача хеша сырого события в правило
SIEMINT-14306	Исправление			Исправлена ошибка неверной кодировки в CEC
SIEMINT-15874	Улучшение	MPS Soft MasterSCADA	4.1.8	Добавлена обработка новых типов событий для MasterSCADA 3.10, получаемых по протоколу Syslog. Формулы нормализации доработаны для обработки событий, содержащих структуру: "EVENTS":[] (APP-ADD-001, APP-CHANGE-002, APP-CHANGE-004, APP-CLOSE-001, APP-COMMAND-001, APP-DELETE-003, APP-EXPORT-006, APP-

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				EXPORT-007, APP-PRINTING-008, APP-SHUTDOWN-005, APP-SHUTDOWN-015, APP-START-001, APP-START-011, APP-VIEW-001, SEC-ACCESS-023, SEC-ACCESS-024, SEC-ACCESS-025, SEC-ACCESS-026, SEC-ACCESS-027, SEC-ACCESS-028, SEC-ACCESS-029, SEC-ACCESS-030, SEC-ACCESS-031, SEC-ACCESS-130, SEC-CHANGE-004, SEC-CHANGE-005, SEC-CHANGE-006, SEC-CHANGE-008, SEC-CHANGE-009, SEC-CHANGE-010, SEC-CHANGE-011, SEC-CHANGE-012, SEC-CHANGE-013, SEC-CHANGE-014, SEC-CHANGE-015, SEC-CHANGE-016, SEC-CHANGE-034, SEC-CHANGE-035, SEC-CHANGE-036, SEC-CHANGE-037, SEC-CHANGE-038, SEC-CHANGE-039, SEC-CHANGE-040, SEC-CHANGE-041, SEC-CHANGE-042, SEC-CHANGE-043, SEC-CHANGE-046, SEC-CHANGE-047, SEC-CHANGE-048, SEC-CHANGE-049, SEC-CHANGE-050, SEC-CHANGE-051, SEC-CREATE-032, SEC-CREATE-044, SEC-CREATE-045, SEC-CREATE-046, SEC-CREATE-047, SEC-DELETE-031, SEC-DELETE-033, SEC-LOGIN-019, SEC-LOGIN-020, SEC-LOGIN-021, SEC-LOGIN-115, SEC-LOGIN-116, SEC-LOGIN-117, SEC-LOGIN-118, SEC-LOGOUT-022, SEC-LOGOUT-023, SEC-OVERFLOW-007, SEC-SYNC-001, SEC-VIEW-001, SEC-VIEW-002, SEC-VIEW-003, SEC-VIEW-004, SYS-CHECK-001, SYS-CHECK-002, SYS-CHECK-003, SYS-CHECK-004, SYS-CHECK-005, SYS-CHECK-006, SYS-CHECK-007, SYS-CHECK-008, SYS-CHECK-009, SYS-INFO-001)
SIEMINT-1830	Исправление	Газинформсервис & PostgreSQL Jatoba & NativeLog	5.1.3	Доработана формула нормализации SEC-CREATE-002 (создание таблицы). Изменен маппинг поля object.name
SIEMINT-13666	Улучшение			Добавлено новое условие отбора в COND, чтобы разграничить поток событий в следующих формулах нормализации: – GIS_gazinformservice_jatoba_syslog_select (SEC-SELECT-001, SEC-DETECT-001, SEC-DETECT-002, SEC-DETECT-003, SEC-DETECT-004, SEC-DETECT-005, SEC-DETECT-

ID запроса	Тип запроса	Наименование источника	Номер сборки	Описание изменения
				006, SEC-DETECT-007, SEC-DETECT-008, SEC-DETECT-009, SEC-DETECT-010, SEC-DETECT-011, SEC-DETECT-012, SEC-DETECT-013, SEC-DETECT-014, SEC-DETECT-015, SEC-DETECT-016, SEC-DETECT-017, SEC-DETECT-018, SEC-MODIFY-001, SEC-CHECK-001, SEC-SELECT-004, SEC-SELECT-005, SEC-DETECT-022, SEC-DETECT-021, SEC-SELECT-006, SYS-INFO-005, SYS-INFO-006, SEC-INFO-006, SYS-INFO-001, APP-REFRESH-001, APP-CALL-001, APP-EXECUTE-001, SEC-SELECT-002, SEC-SELECT-003); – GIS_postgres_professional_postgresql_cec_select_as (SEC-SELECT-002, SEC-SELECT-003, SEC-SELECT-004, SEC-SELECT-005, SEC-SELECT-007, SEC-SELECT-006, SEC-SELECT-001). Разработаны формулы нормализации для событий копирования БД GIS_gazinformservice_jatoba_syslog_DB_copy (APP-COPY-002), GIS_postgres_professional_postgresql_cec_DB_copy (APP-COPY-002). Добавлены правила агрегации для событий копирования БД GIS_gazinformservice_jatoba_syslog_Numerous_DB_copy (APP-COPY-002), GIS_postgres_professional_postgresql_cec_Numerous_DB_copy (APP-COPY-002). Добавлена сработка правила корреляции GL_DB_ACT_S04_Copy_DBMS
SIEMINT-14305	Улучшение			Обновлен скрипт CustomEventCollector для корректного заполнения поля event_src.host
SIEMINT-13096	Улучшение			Доработана документация. В разделе 4.1.1 указано, что пакет расширения поставляется вместе с дистрибутивом Jatoba
SIEMINT-13273	Улучшение	Xello Deception	4.1.3	Доработана документация. Из протокола проверок удалены правила: GL_UM_ACC_S12, GL_UM_ACC_S12

Приложение Б
Доработки по улучшениям и исправлениям ошибок в направлении контента

Доработки по улучшениям и исправлениям ошибок по каждому пакету контента приведены в таблице Б.1. Подробные изменения представлены в документации на следующие новые сборки пакетов контента:

- Пакет инфраструктурного контента, сборка_5.2.0;
- Пакет обнаружения компьютерных атак (корпоративный сегмент), сборка_5.2.2;
- Пакет общих ресурсов контента, сборка_5.2.0.

Примечание. Подробная информация об указанных изменениях приведена в списке изменений к каждому пакету.

Таблица Б.1 – Описание доработок по улучшениям и исправлениям ошибок в направлении контента

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
Пакет инфраструктурного контента, сборка_5.2.0			
SIEMCONT-2249	GL_UM_ACC_S08_Tracking_Creation	Улучшение	Доработано правило корреляции: – добавлена отдельная локализация для пользователя subject.account.name, если он обладает правами администратора (проверка на категорию admin в TC COMMON_Users_Configurating); – добавлена директива event
SIEMCONT-2243	GL_UM_ACC_S07_Removing	Улучшение	В правиле корреляции переработан запрос к табличному списку COMMON_Users_Configurating для поддержки значения any в колонках account_or_group.name, account_or_group.domain, account_or_group.id
SIEMCONT-2211	GL_OS_LIN_SUS_S02_Su_Root_Execution	Улучшение	Разработано общее правило корреляции для детектирования выполнения команды su root (повышение привилегий) в системах Unix-like
SIEMCONT-2185	– GL_UM_ADM_S02_Modify – GL_UM_ACC_S02_Changing	Улучшение	Доработаны правила корреляции, добавлены события и отдельная локализация для изменения следующих параметров: – группы (когда нет понимания - удаление или добавление членства); – роли (аналогично группе); – ID УЗ;

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
			– имени УЗ; – домашней директории (для Linux); – оболочки (для Linux)
SIEMCONT-2180	GL_UM_ACC_S03_Changing_Password	Улучшение	Доработано правило корреляции – добавлена отдельная локализацию для пользователя root; – добавлена директива event
SIEMCONT-2010	GL_CONF_S05_Application_Compromised_By_Compromised_User	Улучшение	Доработано правило корреляции: добавлены исключения по полям subject.account.name, object.fullpath
SIEMCONT-1790	GL_OS_LIN_SUS_S06_Executed_Tool_For_Download_Files	Улучшение	Доработано правило корреляции: изменено условие фильтрации событий, добавлено обнаружение запуска следующих утилит: – axel – aria2 – httpie
SIEMCONT-1659	– GL_OS_WIN_REG_H01_Registry_Parameter_Rename – GL_OS_WIN_REG_H02_Registry_Parameter_Value_Modify – GL_OS_WIN_REG_H03_Registry_Parameter_Create – GL_OS_WIN_REG_H04_Registry_Parameter_Delete – GL_OS_WIN_REG_S05_Registry_Section_Has_Removed – GL_OS_WIN_REG_S06_Modify_Registry	Улучшение	Доработаны правила на реестр: – добавлен табличный список Windows_WL_Registry_Tracking_Exceptions, с возможностью вносить regex-исключения по полю object.fullpath для всех правил на реестр; – в правилах переработан запрос исключений
SIEMCONT-1546	– GL_FILES_S03_Viewed_File_Forbidden_To_View – GL_HV_VM_S02_Critical_VM_Configuration_Change – GL_HV_VM_S15_A_Critical_VM_Snapshot_Was_Deleted	Улучшение	Доработаны правила корреляции: изменен запрос к макросу с табличным списком исключений: – добавлено исключение по полю subject.account.name для правил GL_FILES_S03, GL_HV_VM_S02, GL_HV_VM_S15; – добавлено исключение по полям subject.account.name и object.account.name для правил GL_UM_ACC_S05 и GL_UM_ADM_S05.

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
	– GL_UM_ACC_S05_Rising_Privileges_Of_Tracked_User_Or_Group – GL_UM_ADM_S05_Account_Or_Group_Grant_Rights		См. также изменения по *SIEMCONT-1546 для пакета ПОРК*
SIEMCONT-1522	GL_AUTH_S02_Authenticating_Different_Accounts_From_One_Host	Улучшение	Доработано правило корреляции: в настройку макроса COMMON_Exceptions добавлена возможность фильтрации не только по src.host, но и по имени пользователя
SIEMCONT-1073	GL_BU_BCKP_S02_Deleting_A_Backup	Улучшение	Доработано правило корреляции: изменены условия исключения - добавлена возможность исключения по полю subject (колонка custom_exception_1) и полю subject.account.name (колонка custom_exception_2)
SIEMCONT-899	GL_AUTH_S02_Authenticating_Different_Accounts_From_One_Host	Улучшение	Доработано правило корреляции: изменены условия исключения - добавлена возможность исключения по полю object.account.name (колонка custom_exception_2)

SIEMCONT-815	правила корреляции UM	Улучшение	– Разработаны правила корреляции по подгруппам:
			  – Управление группами;
			  – Управление ролями;
			  – Управление учётными записями;
			– Во все правила корреляции UM добавлен макрос COMMON_Check_Event_Sources с обращением к списку с хранимой информации об источниках;
			– Во все правила корреляции UM, где речь идет о группе или о УЗ добавлены макросы COMMON_Check_Track_User и COMMON_Check_Track_Role_Or_Group.
			См. также изменения по *SIEMCONT-815 для пакета ПОРК*

SIEMCONT-781	GL_UM_S09_Frequent_Password_Changes	Улучшение	Разработано правило корреляции для выявления превышения допустимого количества смен пароля у пользователя. См. также изменения по *SIEMCONT-781 для пакета ПОРК*
SIEMCONT-779	GL_CONF_S13_Multiple_Policy_Modify	Улучшение	Разработано правило корреляции для множественного изменения политик DLP.
SIEMCONT-719	GL_MDL_S01_Critical_Module_Stop	Улучшение	Разработано правило корреляции для выключения критичных модулей. См. также изменения по *SIEMCONT-719 для пакета ПОРК*

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
SIEMCONT-699	GL_DB_ACT_S06_DB_Shutdown	Улучшение	Разработано правило корреляции для выявления событий выключения СУБД и баз данных. См. также изменения по *SIEMCONT-699 для пакета ПОРК*.
SIEMCONT-644	GL_CONF_S12_Multiple_Policy_Removal	Улучшение	Разработано правило корреляции для отслеживания трех и более событий удаления различных политик одним пользователем в защищаемой системе за указанный интервал времени. См. также изменения по *SIEMCONT-644 для пакета ПОРК*
Пакет обнаружения компьютерных атак (корпоративный сегмент), сборка_5.2.2			
SIEMCONT-2613	MTE_T1090.003_Proxy.Multi_hop_Proxy	Улучшение	Доработано правило корреляции: в событии Proxy_Hop доработан фильтр, который срабатывает только в случае исходящих успешных соединений на порты TOR
SIEMCONT-2580	MTE_T1059.005_Command_and_Scripting_Interpreter.Visual_Basic	Улучшение	Доработано правило корреляции: в фильтр правила прописаны дополнительные исключения по предоставленным данным и FP сработкам
SIEMCONT-2123	MTE_T1003.001_OS_Credential_Dumping.LSASS_Memory	Улучшение	Доработано правило корреляции: добавлен кейс удаленной реализации дампа LSASS - добавлено новое событие установки службы Windows (Windows_Service_Install)
SIEMCONT-2121	– MTE_T1087.001_Account_Discovery.Local_Account – MTE_T1548.003_Abuse_Elevation_Control_Mechanism.Sudo_and_Sudo_Caching	Улучшение	Доработаны правила корреляции: – исключено срабатывание на /etc/sudoers для MTE_T1087.001_Account_Discovery.Local_Account; – добавлена возможность исключения по object.fullpath.и добавлено срабатывание на действие чтения для MTE_T1548.003_Abuse_Elevation_Control_Mechanism.Sudo_and_Sudo_Caching
SIEMCONT-2103	MTE_T1087.001_Account_Discovery.Local_Account	Улучшение	Доработано правило корреляции: исправлена локализация
SIEMCONT-2049	MTE_T1049_System_Network_Connections_Discovery	Улучшение	Доработано правило корреляции: в условие добавлена необходимость наличия ключа a (-all) в cmdline
SIEMCONT-1649	MTE_T1489_Service_Stop	Улучшение	Доработано правило корреляции: – в фильтр события на процессы добавлено дополнительное условие по проверке службы в соответствии со списком критичных служб; – имя службы теперь проверяется в табличном списке COMMON_Critical_Services_On_Devices;

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
			– у макроса события выполнения блока сценария PowerShell удалены условия для команд, которые вызывали запуск процессов
SIEMCONT-1643	MTE_T1564.004_Hide_Artifacts.NTFS_File_Attributes	Улучшение	Доработано правило корреляции: в фильтре события уточнено условие на regex для предотвращения FP сработок на приведенные примеры
SIEMCONT-1641	MTE_T1505.003_Server_Software_Component.Web_Shell	Улучшение	Доработано правило корреляции: – расширено покрытие детектирования с использованием табличного списка MTE_Process_Web_Shell с привязкой используемого языка программирования – скорректированы условия отбора событий правила корреляции
SIEMCONT-704	MTE_T1558.001_Steal_or_Forge_Kerberos_Tickets.Golden_Ticket	Улучшение	Доработано правило корреляции: добавлено новое событие: запрос билета Kerberos (Windows_Ticket_Request)
Пакет общих ресурсов контента, сборка_5.2.0			
SIEMCONT-2760	– TTS_37_Network_Or_Host_Scan – TTS_38_Network_Or_Host_Scan_By_Compromised_Host – GL_FW_S04_Host_Port_Scan – GL_FW_S05_Network_Scan	Улучшение	Доработаны правила корреляции – в GL_FW_S04, GL_FW_S05 добавлена обработка полей src.port для набора событий, поступающих на вход правил; – в GL_FW_S04, GL_FW_S05, TTS_37 и TTS_38 добавлены варианты локализации при src.port != null, где инициатор сканирования указан в формате {src.ip}:{src.port}
	COMMON_WL_Network_Connections	Улучшение	Доработан табличный список: в шаблоне исключений расширены условия исключений для правил GL_FW_S04, GL_FW_S05, TTS_37 и TTS_38
SIEMCONT-2330	– TTS_02_Multiple_Errors_On_Objects – TTS_32_Bruteforce_Attempt – TTS_33_Distributed_Bruteforce_Attempt	Улучшение	Изменены описания и работа правил корреляции по умолчанию. По умолчанию будут работать следующему сценарию: – правило корреляции срабатывает при наступлении 10 событий; – во избежание спама после каждой сработки правила корреляции будет выдерживаться тайм-аут 10 минут. По желанию пользователя могут быть добавлены настройки для конкретного источника с явным значением vendor|title в колонке key_field. В таком случае настройки по умолчанию автоматически не будут применяться к данному источнику
	COMMON_General_Rules_Configuration_Parameters	Улучшение	Доработан табличный список: – добавлены предзаполненные строки с настройками правил:

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
			– TTS_02_Multiple_Errors_On_Objects; – TTS_32_Bruteforce_Attempt; – TTS_33_Distributed_Bruteforce_Attempt; – унифицированы наименования параметров, задаваемых в колонке param_description, для всех правил: – Event_Count - пороговое количество событий для сработки правила; – Rule_TimeOut — тайм-аут регистрации событий после сработки правила; – добавлена возможность указания значения «any|any» в колонке key_field, соответствующему параметру «vendor|title» в key_field_description
	– GL_AUTH_P01_Failed_Logging_Counter – GL_P02_Errors_Counter	Улучшение	Доработаны правила обогащения: – в инструкции enrich_fields изменены запросы к табличному списку COMMON_General_Rules_Configuration_Parameters, получающие значения параметров Event_Count и Rule_TimeOut для конкретного правила. – параметры приведены к новому унифицированному значению – добавлен механизм последовательной проверки параметров со следующей приоритизацией: – запрос параметров Event_Count и Rule_TimeOut по значению «evenc_src.vendor|evenc_src.title» в колонке key_field; – запрос параметров Event_Count и Rule_TimeOut по значению «any|any» в колонке key_field
SIEMCONT-1722	TTS_36_Modifying_Files_Prohibited_For_Editing	Улучшение	Доработано правило корреляции: – удален запрос к макросу COMMON_Track_Files_Actions; – добавлены прямые запросы к табличному списку COMMON_Files_Forbidden в порядке приоритета: – проверка на наличие в табличном списке строки, где значение колонки dst.fqdn/dst.hostname полностью соответствует значению в поле dst.fqdn/hostname нормализованного события;

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
			– при неуспешной проверке по условию выше выполняется поиск строки, где в колонке dst.fqdn/dst.hostname указано регулярное выражение, под которое подходит значение dst.fqdn/hostname нормализованного события. Также остается возможность указания в табличном списке COMMON_Files_Forbidden IP-адреса хоста в колонке dst.ip. Проверка по dst.ip будет выполняться, если не будут заполнены колонки dst.fqdn/hostname
	COMMON_Files_Forbidden	Улучшение	Доработан табличный список: изменен тип данных для колонок dst.hostname и dst.fqdn со string на regex - появилась возможность указывать как имя хоста/FQDN полностью, так и регулярное выражение
SIEMCONT-1677	GL_FW_S05_Network_Scan	Улучшение	Доработано правило корреляции: поле protocol исходного события добавлено в поле protocol корреляционного события через инструкцию on
SIEMCONT-1546	COMMON_Tracking_Exceptions	Улучшение	В рамках доработки изменено условие работы шаблона исключений для табличного списка
SIEMCONT-829	TTS_28_Configure_Security_Tool	Улучшение	Доработано правило корреляции: в строке вызова макроса реализована передача в параметры макроса $custom_exception_1 и $custom_exception_2 значения "none", если в полях события встретится null, через функцию coalese
	COMMON_Tracking_Exceptions	Улучшение	Доработан табличный список: в колонках custom_exception_1 и custom_exception_2 появилась возможность задать значение "none", для исключения событий по полям нормализованного события со значением null (поля не заполнены)
SIEMCONT-815	– COMMON_Add_Role_To_Group – COMMON_Check_Event_Sources – COMMON_Check_Track_Role_Or_Group – COMMON_Check_Track_User – COMMON_Delete_Role_From_Group – COMMON_Grant_Role_Rights – COMMON_Modify_Role	Улучшение	В рамках доработки правил UM для поддержки ролей. – добавлены макросы под роли; – макрос COMMON_Check_Track_User_or_Group удален: разделен на два макроса COMMON_Check_Track_User и COMMON_Check_Track_Role_Or_Group

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
	– COMMON_Modify_Role_Rights – COMMON_Role_Assignment_To_Group – COMMON_Role_Assignment_To_Role – COMMON_Role_Assignment_To_User – COMMON_Role_Creation – COMMON_Role_Deletion – COMMON_Role_Revocation_To_Group – COMMON_Role_Revocation_To_Role – COMMON_Role_Revocation_To_User COMMON_Users_Admin_Categories		
	– COMMON_Event_Sources – COMMON_Users_Configurating – COMMON_Temporary_Users	Улучшение	Доработаны табличные списки: изменен состав колонок, добавлены: – appliance - принадлежность источника к программно-аппаратному комплексу; label - метка источника данных; comment - любая информация – account_or_group.domain - домен объекта, для которого определяется категория; comment - поле для дополнительной информации; – account.domain - домен пользователя; account.id - идентификатор пользователя
	– GL_UM_L01_Temporary_Users_Creation – GL_UM_L02_Temporary_Users_Auth – GL_UM_L03_Deleting_User_Within_N_Hours_After_Creation	Улучшение	Доработаны правила обогащения: добавлены обращения к новым колонкам в табличных списках выше и обращения к новым правилам из пакета инфраструктурного контента

ID запроса	Наименование ресурса	Тип запроса	Описание изменения
	– GL_UM_L06_Password_Changed _Enrich		
SIEMCONT -781	GL_UM_L07_Password_Changes _Counter	Улучшение	Добавлено правило обогащения для учета количества изменений пароля у пользователя
	COMMON_Password_Changes _Counter_List	Улучшение	Добавлен динамический табличный список для ведения подсчета изменения пароля у пользователя
	COMMON_Threshold_Value_List	Улучшение	Доработан табличный список - в описание добавлены новые категории: – «changes_pass» - контроль смены пароля у пользователя (для поля category); – «pass» - пароль (для поля name _resource)
SIEMCONT -719	– COMMON_Critical_Modules – COMMON_Module_Stop	Улучшение	В рамках разработки правила корреляции GL_MDL_S01_Critical_Module_Stop для выключения критичных модулей добавлены: – табличный список для задания критичных модулей на хостах; – макрос для фильтрации событий остановки модуля
SIEMCONT -699	– COMMON_Critical_DB – COMMON_Stop_DB	Улучшение	В рамках разработки правила корреляции GL_DB_ACT_S06_DB_Shutdown для выявления событий выключения СУБД и баз данных добавлены: – табличный список для задания критичных баз данных на хостах; – макрос для фильтрации событий остановки СУБД
SIEMCONT -644	COMMON_Policy_Remove	Улучшение	В рамках разработки правила корреляции GL_CONF_S12_Multiple_Policy_Removal для отслеживания трех и более событий удаления различных политик одним пользователем в защищаемой системе за указанный интервал времени добавлен макрос для фильтрации событий удаления политики устройства

Приложение В
Перечень стандартных источников

В таблице В.1 представлен перечень стандартных источников, обработка событий которых поддерживается посредством механизмов обработки событий в пакете коннекторов для стандартных источников.

Таблица В.1 − Перечень стандартных источников событий

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
АСО	Aruba Networks	eCos	HP ProCurve 1810/eCos-2.0 P.1.17	eCos
	Aruba Networks	OS Switch	15.7	ArubaOS-Switch
	Cisco	IOS	12, 15, XE	IOS
	Cisco	IOS XE	2.x, 3.x	IOS 12.x, 15.x
	Hewlett Packard Enterprise	Comware Software	3, 5, 7	Comware Software

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Juniper	Junos	mx240	Junos OS
Инфр. ПО	Microsoft	DHCP	Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016	Windows
	Microsoft	DNS	2008, 2012	Windows
	Microsoft	Exchange	15.01.1913.007	Windows
	Microsoft	Internet Information Services	6.0 − 8.5	Windows
	Microsoft	System Center Configuration Manager (SCCM)	5.00.9068.1026, 5.00.9078.1014	Windows
	Microsoft	Terminal services	Windows Server 2019	Windows Server 2019

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Opensource	Apache	2.4	Linux
	Microsoft	Certification Authority	Windows Server 2008, 2008R2, 2012, 2012R2, 2016	Windows Server 2008, 2008R2, 2012, 2012R2, 2016
	Microsoft	NTP	Microsoft Windows Server 2019	Microsoft Windows Server 2019
	Microsoft	Active Directory	Microsoft Windows Server 2019, 2016, 2012, 2008	Microsoft Windows Server 2019, 2016, 2012, 2008
	Microsoft	Active Directory Federation Services	10.0.17763.4644	Windows Server 2019, 2016, 2012, 2008
ОС	AlmaLinux	OS	8.9	Linux
	FreeBSD Team	FreeBSD	11.0	Linux
	Microsoft	SysMon	8 - 15	Windows Server 2019

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Microsoft	Windows	Windows XP - 10, Windows Server 2000 - 2019	Windows XP - 10, Windows Server 2000 - 2019
	Oracle	Solaris	8 - 11	Solaris
	Red Hat	CentOS	6, 7	CentOS
	Red Hat	Red Hat Enterprise Linux	4.x, 5.x, 6.x, 7.x	Linux
	Базальт СПО	Альт Сервер 8 СП	10.1	Linux
	Базальт СПО	Альт Виртуализация	10.1	Linux
	РЕД СОФТ	РЕД ОС	7.1, 7.2, 7.3	Linux

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Русбитех	Astra Linux	1.6, 1.7	Linux
Гипервизоры	VMware	ESXi	5.x, 6.x	ESXI
	VMware	vCenter	5.5 - 7.0	ESXI
СрЗИ	Checkpoint	Connectra & Gaia & Endpoint Security Client	R76, R77.10, R77.20, R77.30, R81.10	Windows
	Cisco	ASA	8, 9	iOS
	Cisco	FWSM	8, 9	iOS
	Cisco	PIX	8, 9	iOS

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Positive Technologies	Application Firewall	3.7.x, 4.1.x	Linux
	Positive Technologies	Multiscanner	5.x	Linux
	Positive Technologies	Network Attack Discovery	11.x, 12.0-3	Linux
	Газинформ-сервис	Ankey SIEM NG	4.1, 5.2	Linux
	Лаборатория Касперского	Industrial Cybersecurity For Nodes	3.1	Windows, Linux
	Лаборатория Касперского	Security Center	8 - 14	Windows, Linux

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Positive Technologies	Application Inspector	4.8.0	Microsoft Windows 10; Microsoft Windows Server 2016 Debian 10, 11; CentOS 8; Ubuntu 18.04, 20.04, 21.04, 21.10, 22.04, 22.10; РЕД ОС 7.3; Astra Linux 1.7, 2.12
	Positive Technologies	Sandbox	5.15	Astra Linux 1.7; Debian 11
СУБД	Microsoft	SQL Server	2008+, 2000	Windows Server 2019 Standard, Windows XP
	Oracle	Database	11g, 19c	RHEL, Windows

Приложение Г
Перечень нестандартных источников

Перечень нестандартных источников, поддерживаемых ПК Ankey SIEM NG, приведен в таблице Г.1.

Таблица Г.1 − Перечень нестандартных источников событий

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
АСО	Allied Telesis	OS	AT-GS950 Series	Собственная ОС
	D-Link	OS	DGS-3120-24SC, DES3526, DES-3226S, DGS-1100-24, DES-1228/ME, DES-3018, DES-3026, DES-3200, DGS-3312SR, DES-1210	Собственная ОС
	Digital Solution	Integrity	DS Integrity NG-40G, DS Integrity NG-100G	Собственная ОС
	EdgeCore Networks	SONiC	ECS3510-28T	SONiC
	Eltex	Routing OS	Aggregation 10G Switch MES53xx Series, Aggregation 10G/40G Switch MES5448, Ethernet Access Switch MES11xx Series, Ethernet Access Switch MES14xx Series, Ethernet Access Switch MES21xx Series, Ethernet Access Switch MES23xx Series, Ethernet Access Switch MES24xx Series, Ethernet Aggregation Switch MES33xx Series, Industrial Switches MES35xx Series, MPLS Router ME5100, Service Gateway ESR-100,	Routing OS

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
			Service Gateway ERS-200, Service Gateway ESR-1000	
	Extreme Networks	EOS	A4H124-24FX, A4H254-8F8T, Matrix N3 Platinum	EOS
	Hirschmann	HiOS	ABB AFS650, ABB AFS675, Hirschmann MACH1000, Hirschmann MACH1020, Hirschmann RS20	HiOS
	Huawei	VRP	AR2240, AR2220E, AR2204, AR550, NetEngine 8000, S1720, S2700, S5700, S5720, S6720, S6730, S7706, S12700E, 6730, NE20, NE40	VRP
	Lenovo	Fabric OS	Fc5022, D610S	Fabric OS v8.2.1a, Fabric OS v8.2.1c
	Lenovo	Networking OS	RackSwitch and Flex System	Networking OS 8.2
	Mikrotik	RouterOS	6.30−7.6	RouterOS
	MOXA	OS	EDS-405A, EDS-408A, EDS-508A, EDS-510A, EDS-516A, EDS-510E, EDS-510E-3GTXSFP, EDS-408A-MM-SC, PT-G7828, PT-G7728, ioLogik E1242, ioLogik E1210, NPort IA5250AI, NPort IA5450A, NPort IA5150AI-T, NPort 5630-16, MGate MB3270, MGate MB3480, IKS-G6824A, UC-8410, IA-240	MOXA OS
	NetGear	NGOS	GS728TP	NGOS
	NsGate	NIS	NIS 3500-2408GE	NIS
	Phoenix Contact	OS	LM 4TX/2FX, MCS 14TX/2FX	Собственная ОС
	QTech	OS	QSW-3400, QSW-6500, QSW-8300 series	qtech os
	Siemens	OS	sn-OSM, sn-SCALANCE X200 (прошивка snMsps), sn-SCALANCE X300X400, sn-SCALANCE XB208, sn-SCALANCE X307	Собственная ОС

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Trei	OS	S301, S304	Собственная ОС
	Zelax	ZOS	ZES-20xx, ZES-22xx, ZES-30xx, ZES-32xx	ZOS
	Zyxel	ZynOS	VES1724-56B2	ZynOS
	НАТЕКС	OS	серии 5124G10, NXI-3000, NX-3408 NetXpert RT-3806, NetXpert NXI-3030	Собственная ОС
	Полигон	OS	2xxx, 3424GE, 3424 GE-U, 3424 GE-US (os version 2.3.20.4)	Собственная ОС
АСУ ТП	AdAstrA	Trace Mode	5.15, 6.0.6, 6.10.1	Windows
	ARC Informatique	PcVue	8.1/10	Windows
	AVEVA	System Platform	2014	Windows, MSSQL
	AVEVA	InTouch	7.1, 7.11, 8, 9, 9.5, 10, 10.1, 11.0	Windows 2019, MSSQL
	AVEVA & Advantech	Edge & Studio	InduSoft Web Studio 2020, Advantech Studio 6.0, Advantech Studio 6.1	Windows
	AVEVA & Advantech	Pi System	2017 sp2, 2018 sp3	Windows
	CCC	TrainTools & TrainView	6, 7, 11	Windows
	CCC	WOIS	1.08, 4, 4.3	Windows XP
	CODESYS Group	SCADA	3.5.x	Windows
	Emerson	DeltaV	3.1	Linux, Windows
	GE Digital	Cimplicity	6.1, 7.5, 8.1, 10	Windows
	GE Digital	iFIX	3.5, 4.0, 5.5	Windows XP, Windows Server 2003

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Honeywell	Experion PKS	R511	Windows Server 2016, MSSQL Server
	ICONICS	GENESIS32	7, 8, 9	Windows, MS Access, MSSQL
	MPS Soft	MasterSCADA	3x (Enterprise), 4D	3x: Windows 4D: Windows, Linux
	Pipe	SCADA	7.1, 7.2	Windows XP
	RealFlex Technologies	SCADA	4, 6	QNX
	Rockwell Automation	FactoryTalk	FactoryTalk View SE 6.10	Windows 7−10, Windows Server 2008−2012
	Schneider Electric	ClearSCADA	2007 R1.4, 2010 R2.1, 2013 R2.1	Windows XP, Windows Server 2008
	Schneider Electric	Foxboro	7.1	Windows, Linux
	Schneider Electric	Vijeo Citect (Citect SCADA)	5.42, 5.5	Windows
	Siemens	Simatic WinCC	7.4.0.1, 7.0, 6.0, 5.0	Windows7, Windows Server 2003/SQL Server 2005 (v7.0, v6.0), WindowsXP/SQL Server 2005, SQL Server 2000 (v7.0, v6.0), Windows7/SQL Server 2012 (v7.4.0.1)
	Verano	RTAP	Verano Visualiser 2.20	Windows
	Yokogawa	CENTUM VP	6.02	Windows
	Yokogawa	FAST/TOOLS	10.04	OS Windows 10
	АВИАТЭКС	ТопИнфо II	2.2.12.128	Windows
	Атомик Софт	Alpha.Platform	Alpha.Security 1.7.18	Astra Linux SE 1.7, Microsoft Windows Server 2016

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	ВегаМашПроект	КРАУС	20.11.2022	Astra Linux 1.7.3, PostgreSQL 11
	Газприборавто-матика	Зонд	Зонд 2006, Зонд 2015	Windows XP
	Газпром Автоматизация	Поток-ДУ	01.12.2021	Astra Linux SE 1.7
	Комита Цифровые технологии	СОЮЗ-ЕАМ	1.14.a	Astra Linux SE 1.7, PostgreSQL
	Космос-Нефть-Газ	ICS	3.15	Windows
	КРУГ	SCADA-2000	4.3, 4.2	Windows
	НПА Вира Реалтайм	Сириус-ИС	2.8 (Сириус-ИС), 2.8 (СПУРТ-Р), 2.9 (ПТК "Союз")	Linux
	РегЛаб	AstraRegul	2024.08.31.00	AstraLinux 1.7
	Система-Сервис	Аргус	7.7.1	Windows, Astra Linux
	ТеконАвтоматика	SCADA	2.8.3	Windows 7 (x86, x64)/8.1(x64)/10, Windows Server 2008 R2/2012 R2/2016
	ЭЗАН	Соната	1.3 (rev 7004 - 10411), 1.4 (rev 9604 - 12711)	v.1.3: Microsoft Windows 2012 R2 v.1.4: Microsoft Windows 2012 R2; Astra Linux 1.7.5
	Элеси	SCADA Infinity	4x	Windows 8.1 (x64) или старше, Microsoft Office 2007 (x86/x64) или старше
	Elesy	Integrity Scada	1.0.1	Astra Linux
	Rockwell Automation	RSView32	7.5	Microsoft Windows 2000, NT, 9x, XP
	Электронные информационные системы	EISCADA	2.4.3.2, 2.5.1, 2.5.2	Windows 2000/XP
	ЭЛНА	Комета	01.08.2024	Astra Linux SE 1.7

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
Гипервизоры	Proxmox	Virtual Environment	8.1.4	Debian GNU/Linux
	РЕД СОФТ	РЕД Виртуализация	7.3.0	Собственная ОС
	Базис	vControl	1.96	ПАК
	Microsoft	Hyper-V	6.3.9600, 10.0.14393	Windows Server 2008R, Windows Server 2012R, Windows Server 2016
	Microsoft	System Center Virtual Machine Manager	Microsoft SCVMM 2019	Microsoft Server 2019
	Red Hat	oVirt	4.3.3.7, 4.4.6, 4.4.9.5	Собственная ОС
	OrionSoft	zVirt	3.0, 4.2	Собственная ОС
Инфр. ПО	APC	StruxureWare Data Center Expert	7.9.1	Windows 10, Windows Server 2016
	Cisco	Unified Communication Manager	12.5	Linux
	Communigate Systems	CommuniGate	6.3	RedOS 7.3
	Eltex	EMS	3.24, 3.30	Linux
	ISC	BIND	BIND 9.18	Red Hat Enterprise Linux, RedOS 7.3, Server 7.9
	Microsoft	Windows Server Update Services	4.0, 5.0, 6.3.9600	Windows
	Opensource	iRedMail	1.3.2	Linux
	Opensource	Nginx	1.12, 1.24	Linux
	Opensource	Postfix	3.8.4	RedOS 7.3 (Муром)
	Opensource	Sendmail	8.14.7	RHEL 7.9

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Opensource	Zabbix	6.4, 5.4, 4.0, 3.2	– 3.2: Astra Linux 1.7.5 & MariaDB 5.5; – 4.0: Debian 11 & PostgreSQL 15 / MySQL 8.0; – 5.4: Ubuntu 20.05 & PostgreSQL 12,15 / MySQL 8.0 / MariaDB 10.3; – 6.0: Ubuntu 22.04 & PostgreSQL 15 / MySQL 8.0
	Veeam Software	Backup & Replication	9.5 Enterprise	Windows
	VK	WorkMail	1.18, 1.19, 1.20, 1.21	CentOS 7, РЕД ОС от 7.3 и выше
	Киберпротект	Кибер Бэкап	12.5, 15, 16.x, 17	– v.12.5: CentOS 7, Windows Server 2012; – v.15: Astra Linux 1.7, Windows Server 2016; – v.16.x: Astra Linux 1.7, Windows Server 2019; – v.17: Astra Linux 1.7, Astra Linux 1.8, РЕД ОС 8, Windows Server 2019
	Скала-Р	Мониторинг	3.11.85, 3.13.88	ALT Server 9.2
	УЦСБ	DATAPK ITM	v1.3, v1.4, v1.5, v1.6, v1.7	RedOS 7.3, CentOS 8

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Cloud Native Computing Foundation	Kubernetes	1.24.0, 1.26.0	Debian 11
	JBoss	KeyCloak	22.0.1	CentOS Stream 8, PostgreSQL 10.23
	РЕД СОФТ	РЕД АДМ	1.2.2	РЕД ОС Муром 7.3.5
	Opensource	FreeIPA	4.10.3	РЕД ОС 7.3
	VK	Teams	24.5	РЕД ОС Муром 7.3.2
	Eltex	ECCM	2.0	Ubuntu 20.04 & PostgreSQL 12.22
	ИНИТИ	СОЛО	3.05	РЕД ОС
	Протей	ВКС	15.1	Astra Linux 1.7
	Протей	imSwitch	4 (odbclog), 5 (odbclog), 5 (filemonitor)	Astra Linux 1.7.4
	Протей	SBC & ITG & MAK	4.2	Linux
ИТСО	Schrack Seconet	SecoLOG	2.5	Windows 7
	Болид	Орион Про	1.12.2	OS Windows, MS SQL SERVER
ОС	Blackberry	QNX	4.25, 6.5	Собственная ОС
ППО	1С	Enterprise	8.2, 8.3	Microsoft Windows, Linux
	ArtLebedev	Imprimatur	1	RED OS MUROM 7.3.4, MariaDB 10.11.4, nginx 1.25.1
	Directum	RX	4.6.39	Альт Сервер 10, Ubuntu 20.04 LTS/22.04 LTS/24.04 LTS, РЕД ОС 7.3/8.0, Astra Linux Special Edition 1.7.5 («Воронеж», «Орел», «Смоленск»)

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Grafana Labs	Grafana	10.3.5	RED OS MUROM 7.3.4
	ITPS	AVIST Oil&Gas	ПАКЦД.2.01.001.И3. 01	Astra Linux SE 1.7, PostgreSQL
	Opensource	Cacti	1.2.27	Linux
	SAP	BO	3.1, 4.2	– 3.1: SUSE Linux Enterprise Server 11 & Oracle Database 11.2; – 4.2: SUSE Linux Enterprise Server 12 & SQL Anywhere 17
	The Samba Team	DC	4.17.10	Linux (RedOs 7.3)
	Петровайзер Софт	Графики бурения	1.0	Linux РЕД ОС 7.3
	Фактор-ТС	Enterprise Service Bus	5.0.199	Astra Linux 1.7.4
	VK	Application Server	2.0 (by VK)	РЕД ОС 7.3 & ClickHouse 24.9
	SAP	Java	7.40.3301	SUSE Linux Enterprise Server 11 (x86_64), Microsoft Windows Server 2019
	SAP	ABAP	7.52 SP 7	SUSE Linux Enterprise Server 12 SP3
	TrueConf	Server	5.3.6	Astra Linux 1.7.3 & PostgreSQL 11
	Газпром ЦПС	Кабинет руководителя	2.0	Astra Linux
	OpenText	Archive Server	16.0.0	SLES11 & SAP HANA / Oracle / MS SQL

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	OpenText	Content Server	16.0.5	Linux & SAP HANA Windows & SAP HANA
	OpenText	Directory Server	1.18	Linux Windows
	1С-Битрикс	Битрикс24	23.300.100	Centos 7 & MySQL 5.7
	Газпром ЦПС	ИС ПНР	2.7	Linux
	РЕД СОФТ	РЕД DC	2.0.0	РЕД ОС 7.3
	СИНТЕЛЛЕКТ	TESSA	3.5	Astra Linux CE & PostgreSQL 14.4
	Sarex	SRX	1.1.12	CentOS 8 & PostgreSQL 10.23
СрЗИ	Dr.Web	Enterprise Security Suite	13.00.1	Linux
	Indeed	Certificate Manager	6.3.1.0	Microsoft Windows 2008 и выше
	Infotecs	VipNet Administrator Удостоверяющий и ключевой центр	4.6	Win
	Infotecs	VipNet Administrator Центр управления сетью	4.6.9, 3.2.9, 3.2.5, 3.2.4, 3.2.3	Windows Server 2012, MSSQL 2012
	Infotecs	VipNet IDS NS	3.x	ЗПС, функционирующая под управлением адаптированной 64-разрядной ОС на базе ядра Linux
	Infotecs	VipNet Policy Manager	4.3, 4.5	Linux

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Infotecs	VipNet Prime	1.7.2	Linux
	Infotecs	VipNet Prime. NVS	1.4.0	Linux
	Infotecs	VipNet StateWatcher	4.9.1, 4.9.2	OS Windows
	Infotecs	VipNet xFirewall & VipNet Coordinator	VipNet xFirewall: 5.0.1, 5.1.1-2652, 5.4, 5.6, VipNet Coordinator: 4.3.2, 4.5, 5.6, VipNet Coordinator IG	Linux
	InfoWatch	Device Monitor	7.10	Windows, PostgreSQL
	InfoWatch	Traffic Monitor.Incidents	7.1, 7.6, 7.7, 7.10	– v.7.1: Astra Linux 1.6 & PostgreSQL 9.6; – v.7.6: Astra Linux 1.7 & PostgreSQL 9.6; – v.7.7, v.7.10: РЕД ОС 7.3 & PostgreSQL 13.8
	InfoWatch	Traffic Monitor.Internal	7.1, 7.6, 7.7, 7.10	– v.7.1: Astra Linux 1.6 & PostgreSQL 9.6; – v.7.6: Astra Linux 1.7 & PostgreSQL 9.6; – v.7.7, v.7.10: РЕД ОС 7.3 & PostgreSQL 13.8
	RSA	Archer GRC	6.1	MS Windows, MS SQL
	S-Terra	VPN Gate	4.1, 4.2, 4.6	Linux
	S-Terra	VPN KP	4.5	Windows
	S-Terra Bel	Bel VPN KP	4.5	Windows
	S-Terra Bel	Bel VPN Gate	4.1, 4.2, 4.5	Linux

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	UserGate	UGOS	5(частично), 6, 7(частично)	Windows; ПАК
	Varonis	DatAdvantage	6.0	Windows
	Xello	Deception	4.9.4, 5.2.8	Windows
	Zecurion	DLP. Incidents	6, 10, 11	Windows
	Zecurion	DLP. Internal	6, 10, 11, 12	Microsoft Windows 7,8,10 & Microsoft SQL Server 2008,2008 R2,2012,2014,2016,2017 / PostgreSQL 9.6, 10; Microsoft Windows Server 2008 R2,2012,2012 R2,2016 & Microsoft SQL Server 2008,2008 R2,2012,2014,2016,2017 / PostgreSQL 9.6, 10
	АйТи Бастион	СКДПУ НТ. Мониторинг и аналитика	2.1.56, 2.2.8	Astra Linux 1.6 Special Edition
	АйТи Бастион	СКДПУ НТ. Шлюз доступа	7.0.14, 7.0.16	Astra Linux 1.6 Special Edition
	Аладдин РД	Enterprise Certification Authority	2.0.1.367, 2.2.1.286	RedOs 7.3, Astra Linux 1.7.5 / PostgreSQL 11.21, Jatoba
	Аладдин РД	JaCarta Management System	2.0, 3.7, 4.1	– v.2.0: Microsoft Windows server 2008-2012 & PostgreSQL 9.6.20 / MS SQL 2008-2019;

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
				– v.3.7: Microsoft Windows server 2008-2012 & PostgreSQL 9.6.20 / MS SQL 2008-2019; – v.4.1: Astra Linux 1.6,1.7,2.12 & PostgreSQL 9.6.10 / MS SQL 2008-2019 / Jatoba 1.9; РЕД ОС 7.2,7.3 & PostgreSQL 9.6.10 / MS SQL 2008-2019 / Jatoba 1.9; ALT Linux 8 & PostgreSQL 9.6.10 / MS SQL 2008-2019 / Jatoba 1.9
	Аладдин РД	SecurLogon	2.0.1.247_ro7.3_x64	RedOS
	АЛТЭКС-СОФТ	RedCheck	2.6.1, 2.6.9, 2.7.0.194	– v. 2.6.1: Microsoft Windows Server 2019 & MSSQL 2020; – v. 2.6.9: Microsoft Windows Server 2019; – v. 2.7.0.194: Debian 10
	АТОМ БЕЗОПАСНОСТЬ	StaffCop. Incidents	4.10, 5.0, 5.2	Linux
	АТОМ БЕЗОПАСНОСТЬ	StaffCop. Internal	4.10, 5.0, 5.2	Linux
	Газинформсервис	Ankey ASAP	1.0.5, 1.0.8	Linux

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
	Газинформсервис	Ankey IDM	1.6, 1.7, 1.8, 1.9	Linux
	Газинформсервис	Ankey SIEM	3.x, 4.x	Linux
	Газинформсервис	Efros ACS	3.0.0	Astra Linux Special Edition 1.6 Смоленск
	Газинформсервис	Efros CI	4.5, 4.7, 4.9, 4.10	Windows, Linux
	Газинформсервис	SafeERP PS	AA 740 4.8.9	Linux
	Газинформсервис	АУЗНИ	5.2, 6.0	Windows
	Газинформсервис	Блокхост-Сеть	4.2	Windows
	КИТ	Eplat4m	1.0.5.2	Windows, Linux
	Код Безопасности	Континент	3.7, 3.9, 4	Windows, Собственная ОС
	Лаборатория Касперского	Secure Mail GateWay	1.1.2, 2.0.0	Linux
	Лаборатория Касперского	Security For Linux Mail Server	8.0.3.30	Linux
	СОЛАР СЕКЬЮРИТИ	Dozor. Incidents	7.7.0	Linux
	СОЛАР СЕКЬЮРИТИ	Dozor. Internal	7.7.0	Linux
	СОЛАР СЕКЬЮРИТИ	webProxy	3.8	CentOS 7.9
	УЦСБ	DATAPK	1.16, 1.17, 1.18, 1.19	CentOS 7.6/7.7
	Газинформсервис	SafeERP CS	AA 740 4.8.9	Linux
	Газинформсервис	SafeERP CS EM	4.9.5	РЕД ОС & PostgreSQL 9.6.4 & Container
	R-Vision	SOAR	5.4	Astra Linux 1.7
СУБД	Firebird Foundation	DBMS	2.5.1	Windows
	MariaDB Corporation	DBMS	10.11.4	РЕД ОС 7.3
	Oracle	MySQL	5.1.24r, 5.7.21	CentOS 7 64-bit
	PostgreSQL	NativeLog	PostgreSQL 9.6, 11, 12, 14.5, 15.5 Postgres Pro 16	Windows Server R1/R2 2012, 2016, 2019, Astra Linux 1.6 (SE),

Тип источника	Производитель	Наименование источника	Версия ПО/ Модель оборудования	Окружение
				CentOS 7.8/8.2, Ред ОС Муром 7.2
	SAP	ASE	16.0 SP03	Linux
	SAP	HANA	2.00.040.00.1553674765	Linux
	Газинформсервис	Jatoba	1.14, 4.5, 5.8.1 (ja_seceventlog)	Windows Server R1/R2 2012, 2016, 2019, Astra Linux 1.6 (SE), CentOS 7.8/8.2, Ред ОС Муром 7.2, Ред ОС Муром 7.3, AlmaLinux 8.9, Astra Linux 1.7
	Opensource	ClickHouse	22.1.3.7	Debian 11