|  |
| --- |
|  |
|  |  |
| **Программное обеспечение интеграции систем безопасности Insentry.Get**Руководство администратора |
|  |
|  |
| Москва 2021 |

**Содержание**

[Термины и сокращения 3](#_Toc72244047)

[1 Введение 4](#_Toc72244048)

[1.1 Наименование и обозначение Системы 4](#_Toc72244049)

[1.2 Область применения 4](#_Toc72244050)

[1.3 Краткое описание возможностей 4](#_Toc72244051)

[1.4 Уровень подготовки пользователя 4](#_Toc72244052)

[1.5 Перечень эксплуатационной документации 5](#_Toc72244053)

[2 Назначение и условия применения 6](#_Toc72244054)

[2.1 Назначение Системы 6](#_Toc72244055)

[2.2 Виды деятельности, функции, для автоматизации которых предназначена Система 6](#_Toc72244056)

[2.3 Условия применения 6](#_Toc72244057)

[2.3.1 Требования к техническим средствам Системы 6](#_Toc72244058)

[2.3.2 Требования к программным средствам Системы 6](#_Toc72244059)

[3 Подготовка к работе 8](#_Toc72244060)

[3.1 Состав и содержание дистрибутива 8](#_Toc72244061)

[3.1.1 Дистрибутив СПО ИШСБ 8](#_Toc72244062)

[3.2 Порядок загрузки данных и программ 8](#_Toc72244063)

[3.2.1 Установка программных компонентов ИШСБ 8](#_Toc72244064)

[4 Описание операций 12](#_Toc72244065)

[4.1 Управление параметрами передачи событий 12](#_Toc72244066)

[Подготовительные действия 12](#_Toc72244067)

[4.1.1 Формат файла конфигурации 12](#_Toc72244068)

[4.1.2 Применение настроек 13](#_Toc72244069)

[4.2 Управление источниками событий для ИШСБ 13](#_Toc72244070)

[Подготовительные действия 13](#_Toc72244071)

[4.2.1 Формат файла конфигурации 13](#_Toc72244072)

[4.2.2 Применение настроек 14](#_Toc72244073)

[5 Аварийные ситуации 15](#_Toc72244074)

[5.1 Действия в случаях несоблюдения технологического процесса 15](#_Toc72244075)

[5.2 Действия по восстановлению программ и/или данных при отказе носителей данных или обнаружении ошибок в данных 15](#_Toc72244076)

[5.3 Действия в случаях обнаружении несанкционированного вмешательства в данные 15](#_Toc72244077)

[6 Рекомендации по освоению 17](#_Toc72244078)

Термины и сокращения

В настоящем документе применяются термины и сокращения, приведенные с соответствующими определениями и расшифровкой в следующей таблице (см. Таблица 1).

Таблица 1 — Перечень терминов, обозначений и сокращений

| Термин/сокращение | Определение/расшифровка |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ИС | Информационная система |
| КТС | Комплекс технических средств |
| ОПО | Общее программное обеспечение |
| ПО | Программное обеспечение |
| Сервис | Программный компонент, реализующий определенные функции автоматизированной системы |
| СПО | Специальное программное обеспечение |

# Введение

## Наименование и обозначение Системы

Полное наименование системы: Интеграционная шина систем безопасности.

Краткое наименование системы: ИШСБ.

Условное обозначение подсистемы: Insentry.Get.

В настоящем документе для обозначения ИШСБ также используется термины Система или ПО (Программное обеспечение).

## Область применения

ПО Insentry.Get предназначено для автоматизированного сбора информации об инцидентах безопасности от систем охранной, пожарной сигнализации, контроля и управления доступом, досмотрового оборудования и иных программных и аппаратных средств, интегрированных в системы безопасности предприятий и дальнейшей передачи в программное обеспечение семейства Insentry для обработки, хранения и анализа

## Краткое описание возможностей

В ИШСБ предоставлены следующие основные возможности:

* + Подключение посредством открытых и проприетарных API к системам безопасности
	+ Получение данных от программных и аппаратных средств
	+ Отправка подтверждений и иных служебных сообщений в адрес систем безопасности, в том числе сообщений о просмотре события и снятии тревог
	+ Фильтрация полученных данных
	+ Кеширование полученных данных
	+ Преобразование данных во внутренний протокол обмена, используемый ПО семейства Insentry
	+ Передача событий в ПО семейства Insentry
	+ Передача данные

## Уровень подготовки пользователя

Администратор Системы должен обладать следующими знаниями и навыками:

* Знание нормативной базы, регулирующей вопросы информационной и технической безопасности, и владение прикладными программными и техническими средствами обеспечения информационной безопасности.
* Знание принципов работы клиент-серверных и веб-приложений с трехуровневой архитектурой.
* Навыки настройки, администрирования и наполнения контентом информационных систем.
* Навыки администрирования СУБД.
* Навыки администрирования серверных операционных систем.
* Навыки конфигурирования, настройки и администрирования локальных вычислительных сетей и системно-технических средств удаленного доступа.
* Навыки настройки и администрирования веб-серверов и серверов приложений.

## Перечень эксплуатационной документации

Перед началом работы с ИШСБ пользователю необходимо ознакомится со следующими документами:

* (настоящий документ).

Актуальная документация размещается в базе знаний, доступной онлайн: <https://kb.insentry.io/>.

# Назначение и условия применения

## Назначение Системы

Система по классу ПО относится к системам сбора, хранения, обработки, анализа и визуализации массивов данных.

Система предназначена для непрерывного круглосуточной обработки данных об обнаруженных угрозах безопасности с генерацией тревожных событий, сбора, обработки, хранения и передачи актуальной информации, необходимой для функционирования смежных информационных систем в рамках интегрированной системы безопасности.

## Виды деятельности, функции, для автоматизации которых предназначена Система

В ИШСБ обеспечена автоматизация следующих функций:

* Сбор и обработка информации об угрозах безопасности от взаимодействующих смежных ИС обеспечения безопасности.
* Передача во взаимодействующие смежные ИС обеспечения безопасности:
	+ сообщений о тревожных событиях;
	+ сообщений о состоянии технических и программных средств Системы;

## Условия применения

### Требования к техническим средствам Системы

Техническое обеспечение Системы должно состоять из технических средств сервера ИШСБ

Технические средства сервера ИШСБ должны отвечать требованиям, приведенным в следующей таблице (см. Таблица 2).

Таблица 2 — Требования к техническим средствам сервера видеонаблюдения

| Требование | Минимальное значение |
| --- | --- |
| Центральный процессор | x86 совместимый процессор, 2 и более ядер; 1,6 ГГц и выше тактовая частота |
| Оперативная память (RAM) | Не меньше 8 Гбайт |
| Дисковая подсистема | Не меньше 120 Гбайт |
| Сетевой адаптер | Не ниже Gigabit Ethernet |

### Требования к программным средствам Системы

Общее программное обеспечение (ОПО) Системы должно состоять из системных и прикладных программных средств сервера ИШСБ

ОПО сервера ИШСБ должно отвечать требованиям, приведенным в следующей таблице (см. Таблица 4).

Таблица 4 — Требования к ОПО сервера видеонаблюдения

| Требование | Минимальное значение |
| --- | --- |
| Операционная система | Ядро Linux версии 5.4 и выше, Windows 10 20H2 и новее |
| Среда исполнения Java | Open JDK 11 и выше |

# Подготовка к работе

## Состав и содержание дистрибутива

### Дистрибутив СПО ИШСБ

Дистрибутив специального программного обеспечения (СПО) ИШСБ поставляется в виде файла-архива Setup-InSentry.Get.<номер сборки>.exe.

## Порядок загрузки данных и программ

Загрузка данных и программных компонентов ПО ИШСБ на средства ИТ-инфраструктуры выполняется в следующей последовательности:

1. Установка программных компонентов ИШСБ (см. п. 3.2.1).

### Установка программных компонентов ИШСБ

Операция предназначена для установки программных компонентов СПО ИШСБ на сервер.

Условия выполнения операции

* Компьютер соответствует требованиям к техническим средствам и общему ПО, приведенным в подразделе 2.3 «Условия применения».
* Пользователь обладает правами администратора на сервере, предназначенном для установки ИШСБ.

Подготовительные действия

Скачайте дистрибутив ПО Insentry.Get с сайта <https://insentry.io/download/get>

Основные действия

Запустите на исполняемый файл из дистрибутива СПО ИШСБ. Установите компоненты СПО ИШСБ, следуя пошаговым инструкциям Мастера установки:

1. На навальном шаге убедитесь в соответствии версии ПО требуемой и нажмите «Далее» (см. Рисунок 2).



Рисунок 2 — Окно Мастер установки на начальном шаге

1. На шаге Выбора папки установки укажите расположение для устанавливаемого приложения (см. Рисунок 3).



Рисунок 3 — Окно Мастер установки на шаге Выбор папки установки

1. На шаге Установка… Мастер установки автоматически выполнит установку программных компонентов и документации СПО ИШСБ следующим образом:
	1. Распакует файлы с документацией и выбранными компонентами из сжатых двоичных файлов во временную папку.
	2. Выполнит поочередную установку компонентов.



Рисунок 4 — Окно Мастер установки на шаге Установка… 🡪 Завершение установки…

1. После завершения установки компонентов СПО ИШСБ Мастер установки выполнит следующие действия:
	1. Создаст службу Insentry.Get в оснастке «Службы и приложения»
	2. Откроет окно с сообщением о завершении установки СПО ИШСБ (см. Рисунок 5).



Рисунок 5 — Окно Мастер установки с сообщением о завершении установки ИШСБ

Заключительные действия

Завершите работу и закройте окно Мастера установки при помощи кнопки Завершить.

# Описание операций

Администратор использует конфигурационные файлы Системы для настройки процесса получения, обработки, хранения и предоставления информации.

## Управление параметрами передачи событий

Предназначен для

* Определения типов событий от внешних программных и аппаратных средств безопасности, подлежащих передаче в ИШСБ
* Указания серверов-получателей событий от СПО ИШСБ
* Задания технологических параметров

Подготовительные действия

Откройте в редакторе текстовый файл application.properties расположенный в каталоге C:\Program Files\InSentry\Get, используя системную учетную запись с правами, достаточными для сохранения файла

### Формат файла конфигурации

logging.file=${ProgramData}/InSentry/Get/InSentry.Get.log

logging.level.ru=DEBUG

logging.level.org.apache.http.wire=INFO

log4j.logger.org.apache.http.wire=INFO

logging.level.org.springframework.web=INFO

server.tomcat.access-log-enabled=true

server.tomcat.access-log-pattern=%h %l %u %t "%r" %s %b %D

spring.http.encoding.force=false

server.port=7350

message.ttl=2678400

data.folder=${ProgramData}/InSentry/Get/Data

aquarius.mqtt.persistence.storage=${ProgramData}/InSentry/Get/mqtt/aquarius/persistence

scpt.mqtt.persistence.storage=${ProgramData}/InSentry/Get/mqtt/scpt/persistence

auth.api.login=getApi

auth.api.pass=getPass

auth.user.login=admin

auth.user.pass=pass

skud.event.list=2,4,11,22,130,142

skud.error.list=8,26,27,28,29,32,38,233,234,235,236,237,238

skud.warning.list=147,180

skud.normal.list=1,23,39,129,131,134,141,148,181,232

rus-guard.event.list=73,13,21,3

stomp.max.message.size:524288

broker.stomp.addr=stomp://admin:admin@localhost:7561

broker.start.embedded=true

### Применение настроек

Перезапустите службу Insentry.Get в оснастке Управление – Службы и приложения – Службы

## Управление источниками событий для ИШСБ

Предназначен для определения списка внешних программных и аппаратных средств безопасности, выполняющих роль источников событий и параметров подключения СПО ИШСБ к ним, как к источникам.

Подготовительные действия

Откройте в редакторе текстовый файл *sources\_list.xml* расположенный в каталоге C:\Program Files\InSentry\Get, используя системную учетную запись с правами, достаточными для сохранения файла

### Формат файла конфигурации

<sources>

 <scpt>

 <sourceId>a4aa6b98-ae81-45e8-88ac-3410ea006c06</sourceId>

 <host>10.107.4.193</host>

 <httpPort>7350</httpPort>

 <mqttPort>1883</mqttPort>

 <login>armtbagent</login>

 <pass>D0ghjc0ndtn!</pass>

 </scpt>

 <aquarius>

 <sourceId>a4aa6b98-ae81-45e8-88ac-3410ea006c08</sourceId>

 <host>10.107.4.9</host>

 <httpPort>8080</httpPort>

 <mqttPort>1883</mqttPort>

 <login>next</login>

 <pass>5w86pTcTj6Tr</pass>

 </aquarius>

<integral>

 <sourceId>a4aa6b98-ae81-45e8-88ac-3410ea006c07</sourceId>

 <host>10.107.4.81</host>

 <port>8888</port>

 <path>/onvif/event\_services</path>

 <consumerHost>10.107.4.1</consumerHost>

 </integral>

<integral>

 <sourceId>a4aa6b98-ae81-45e8-88ac-3410ea006c09</sourceId>

 <host>10.107.4.96</host>

 <port>8888</port>

 <path>/onvif/event\_services</path>

 <consumerHost>10.107.4.1</consumerHost>

 </integral>

</sources>

### Применение настроек

Перезапустите службу Insentry.Get в оснастке Управление – Службы и приложения – Службы

# Аварийные ситуации

Программное обеспечение Системы обеспечивает корректную обработку аварийных ситуаций, вызванных неверными действиями пользователя, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система выдает пользователю соответствующие аварийные сообщения, после чего возвращается в рабочее состояние, которое предшествовало неверной (недопустимой) команде пользователя или некорректному вводу данных.

Надежность аппаратной платформы серверов и рабочих станций, операционных систем серверов и рабочих станций, систем управления базами данных обеспечивается их производителями.

## Действия в случаях несоблюдения технологического процесса

При несоблюдении технологического процесса Система реагирует путем выдачи соответствующих сообщений об ошибках.

В случае возникновения таких ошибок необходимо действовать в соответствии с рекомендациями, приведенными Системой в тексте сообщения об ошибке.

Примерами ошибок при несоблюдении технологического процесса могут быть следующие ошибки:

* Ошибка приема и /или обработки данных
* Неудачная попытка передачи данных

## Действия по восстановлению программ и/или данных при отказе носителей данных или обнаружении ошибок в данных

При отказах в работе носителей данных или обнаружении ошибок в данных Система выводит сообщение об ошибке, связанной с некорректной работой базы данных.

В случае возникновения подобных ситуаций необходимо обратиться в структурное подразделение, отвечающее за эксплуатацию технических средств, и сообщить полный текст сообщения об ошибке.

## Действия в случаях обнаружении несанкционированного вмешательства в данные

При подозрении в компрометации личного пароля (паролей), некорректном функционировании установленных на сервере или рабочей станции технических средств защиты, при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих работу с Системой, а также в случае возникновения других возможных проблем безопасности необходимо выполнить следующие действия:

1. Определить время несанкционированного вмешательства в работу Системы или в ее данные.
2. Устранить последствия вмешательства путем выполнения внеочередного технического обслуживания программных и/или технических средств Системы, а также иных действий по восстановлению Системы.
3. Выяснить способ и причину вмешательства путем анализа системных и прикладных журналов событий, а также иных действий.
4. Устранить способ и причину несанкционированного вмешательства путем настройки технических и программных средств Системы, сброса пароля или иных действий.

# Рекомендации по освоению

Данных, приведенных в настоящем руководстве и документах из перечня необходимой эксплуатационной документации (см. подраздел 1.5 «Перечень эксплуатационной документации»), достаточно для установки и настройки общего и специального программного обеспечения , а также администрирования программных компонентов ИШСБ при ее эксплуатации.