Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

САВРУС

Руководство администратора

ИННОВАЦИОННАЯ КОМПАНИЯ

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

АННОТАЦИЯ

Настоящий документ представляет собой руководство оператора системы анализа и визуализации рисков в управленческих системах (далее САВРУС).

Руководство описывает порядок действий при работе с системой по созданию, просмотру и редактированию основных средств анализа, визуализации и отчётности, предоставляемых системой.

Перед работой пользователя с САВРУС рекомендуется внимательно ознакомиться с настоящим руководством.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

СОДЕРЖАНИЕ

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

СОКРАЩЕНИЯ И ТЕРМИНЫ

Сокращение/ термин	Расшифровка/ описание
АК	Активный канал
АЛ	Активный лист
ИБ	Информационная безопасность
ЛКМ	Левая кнопка мыши
ОС	Операционная система
ПКМ	Правая кнопка мыши
ПМ	Пункт меню
УЗ	Учётная запись
Правила	Правила корреляции событий

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

АРХИТЕКТУРА СИСТЕМЫ

1. Описание компонентов

Архитектура система САВРУС представлена на рисунке ниже.

Система САВРУС (включая все её компоненты) может работать полностью автономно, без доступа к сети Интернет.

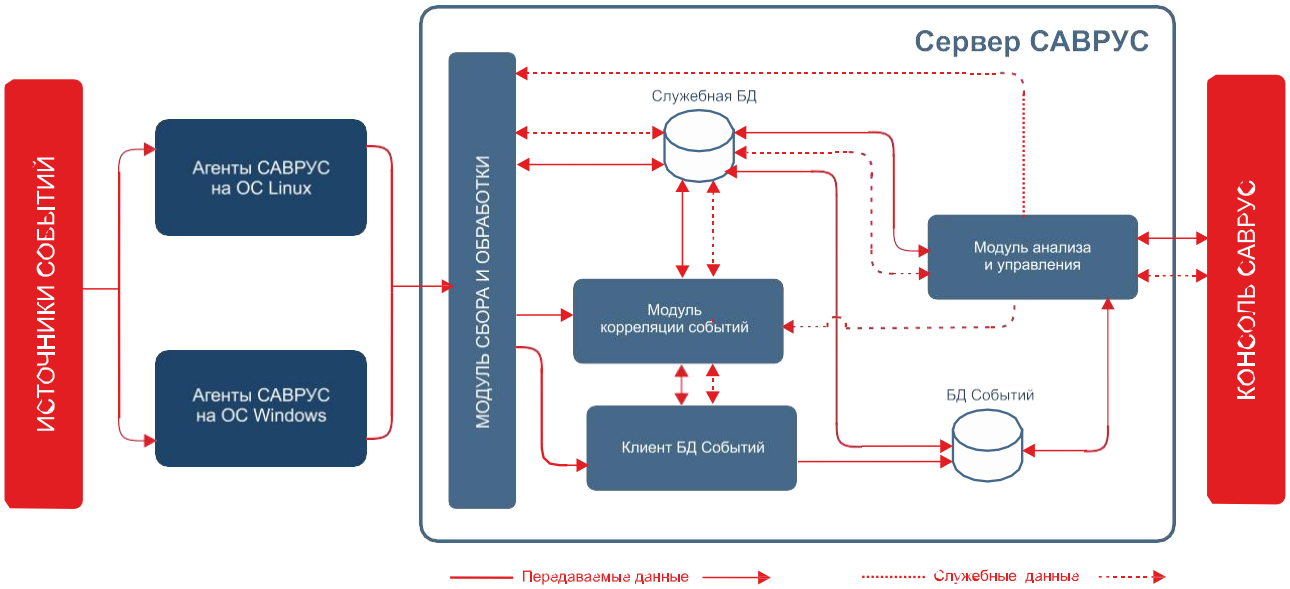

Рисунок 1. Архитектура САВРУС

Описание компонентов системы САВРУС представлено в таблице ниже. Все компоненты таже могут развёртываться в системах виртуализации (VMWare и т.д.)

Таблица 1. Компоненты САВРУС

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

№	Компонент	Описание	Поддерживаемые ОС/СУБД
1.	Агент	Предназначены сбора (активный/пассивный), нормализации и обогащения событий безопасности с целевых систем. В низко нагруженных инсталляциях возможна установка all-in-one включая установку агентов на сервере с ядром системы	Windows Server 2016 / 2019 / 2022 RHEL / CenOS OracleLinux 8.x / 9.x RedOS 8 Опционально: AstraLinux 1.7.5 / 1.8 Debian 10 / 12
2.	Модуль сбора и обработки событий (Inforter)	Предназначен для: • приёма и обработки входящего потока данных с агентов; • кэширования событий безопасности; • обработки (нормализацию и категоризацию данных) с последующим преобразованием и подготовке к записи в формате БД событий безопасности (в том числе событий с кириллицей); • отправки событий безопасности в БД событий безопасности; • отправки событий безопасности на корреляцию.	ОС RHEL CenOS OracleLinux 8.x / 9.x RedOS 8 Опционально: AstraLinux 1.7.5 / 1.8 Debian 10 / 12
3.	Модуль корреляции событий (InforterCE)	Предназначен для аналитической обработки событий безопасности в режиме реального времени.	ОС RHEL CenOS OracleLinux 8.x / 9.x RedOS 8 Опционально: AstraLinux 1.7.5 / 1.8 Debian 10 / 12
4.	Модуль анализа и управления (SavrusCore)	Предназначен для • управление запросами пользователей к БД со стороны Консоли управления;	ОС RHEL CenOS OracleLinux 8.x / 9.x RedOS 8

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

		• взаимодействие и мониторинг работы компонентов САВРУС.	Опционально: AstraLinux 1.7.5 / 1.8 Debian 10 / 12
5.	Консоль САВРУС	Консоль управление САВРУС, обеспечивает управление компонентами и настройками Системы, выполняет функции визуализаций, анализа и отчётности результатов пользовательских запросов к Системе.	Microsoft Windows 10
6.	Клиент ClickHouse	Предназначен для взаимодействия с колоночной БД Событий безопасности.	RedHat/CentOS 8.x/9.x; Astra Linux Special Edition 1.7; AstraLinux 2.12.45; Debian 10.
7.	БД Событий безопасности	Предназначена для хранения данных о событиях безопасности и инцидентах	ClickHouse client version 22.2.2, server version 22.2.2 revision 54455;
8.	БД Служебных настроек	Предназначена для хранения данных служебных настроек.	Jatoba; PostgreSQL из состава Astra Linux Special Edition 1.7; Postgres Pro Enterprise; Maria DB 10.3.28-MariaDB MariaDB Serve

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

ИНСТАЛЛЯЦИЯ СИСТЕМЫ

1. Установка консоли

Консоль САВРУС предназначен для управления компонентами и настройками Системы, выполняет функции визуализаций, анализа и отчётности результатов пользовательских запросов к Системе.

Установка консоли системы осуществляется без доступа к сети Интернет.

Для инсталляции консоли на рабочее место пользователя системы необходимо воспользоваться инсталлятором. Для этого следует запустить файл «setup.exe»

Откроется следующее окно (см. Рисунок 2) с установкой компонентов необходимых для функционирования консоли.

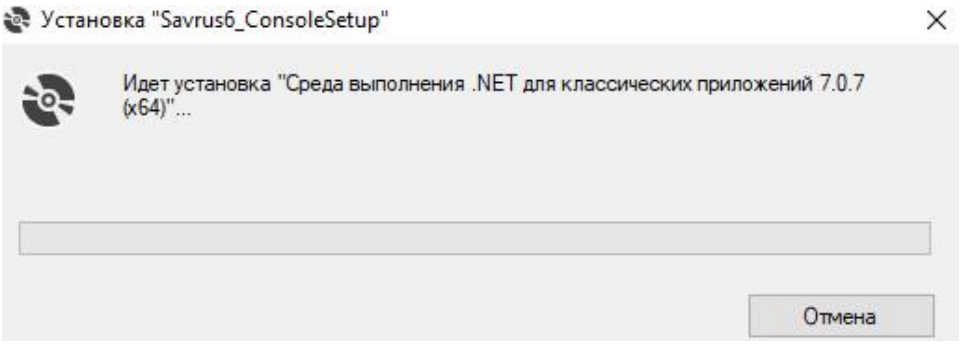

Рисунок 2. Установка компонентов .net

После чего откроется диалоговое окно с мастером установки консоли САВРУС в нем необходимо нажать кнопку «Далее» (см. Рисунок 3).

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

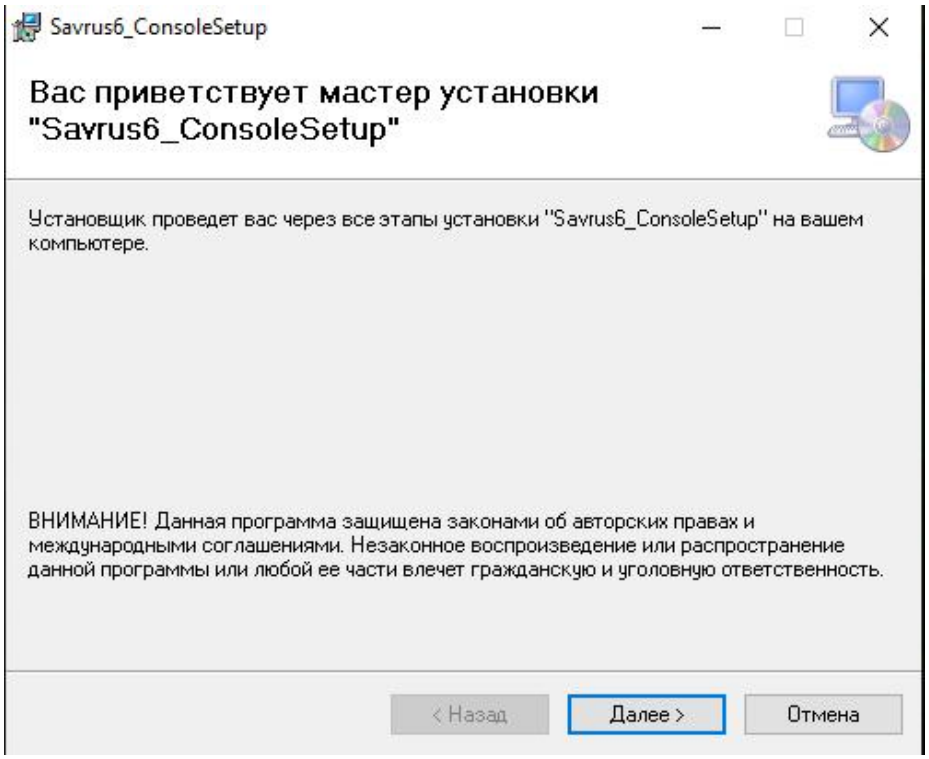

Рисунок 3. Мастер установки

После чего необходимо выбрать каталог, в котором будет располагаться консоль. При необходимости можно выбрать пользователей рабочей станции, которым необходимо установить консоль (см. Рисунок 4).

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

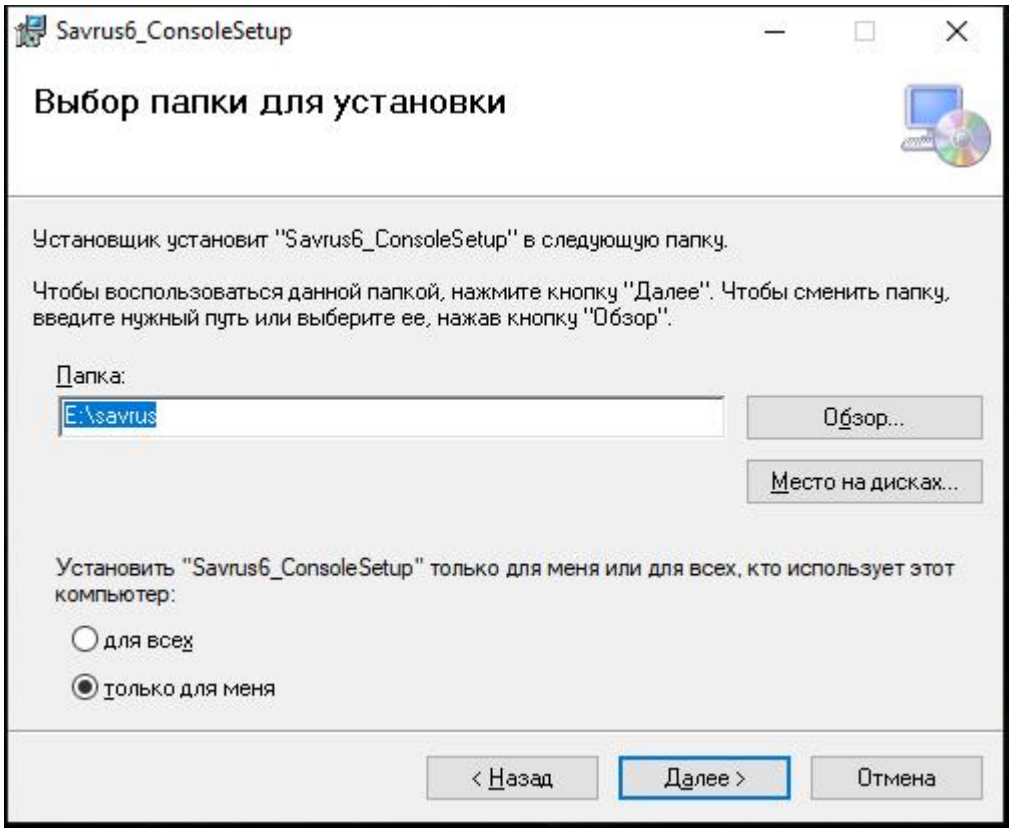

Рисунок 4. Указание каталога

Далее необходимо подтвердить установку консоли, для этого следует нажать на кнопку «Далее» (см. Рисунок 5).

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

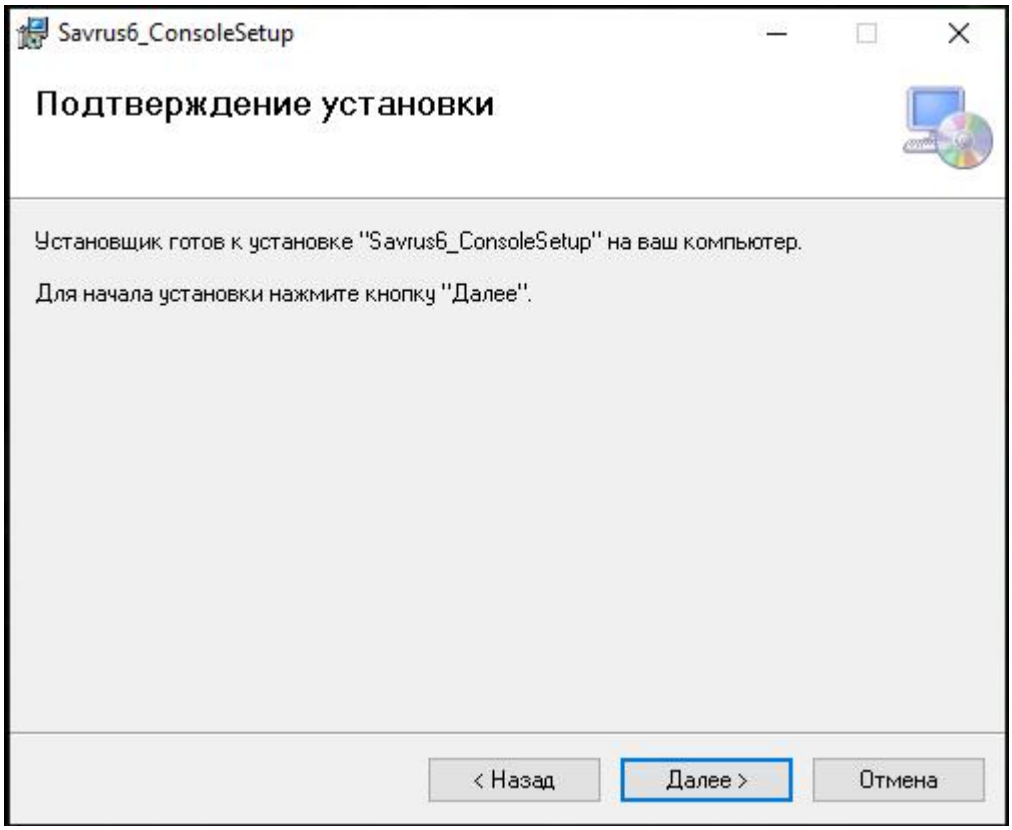

Рисунок 5. Подтверждение установки

Процесс установки может занять некоторое время. При необходимости процесс установки можно прервать, для этого следует нажать на кнопку «Отмена» (см. Рисунок 6).

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

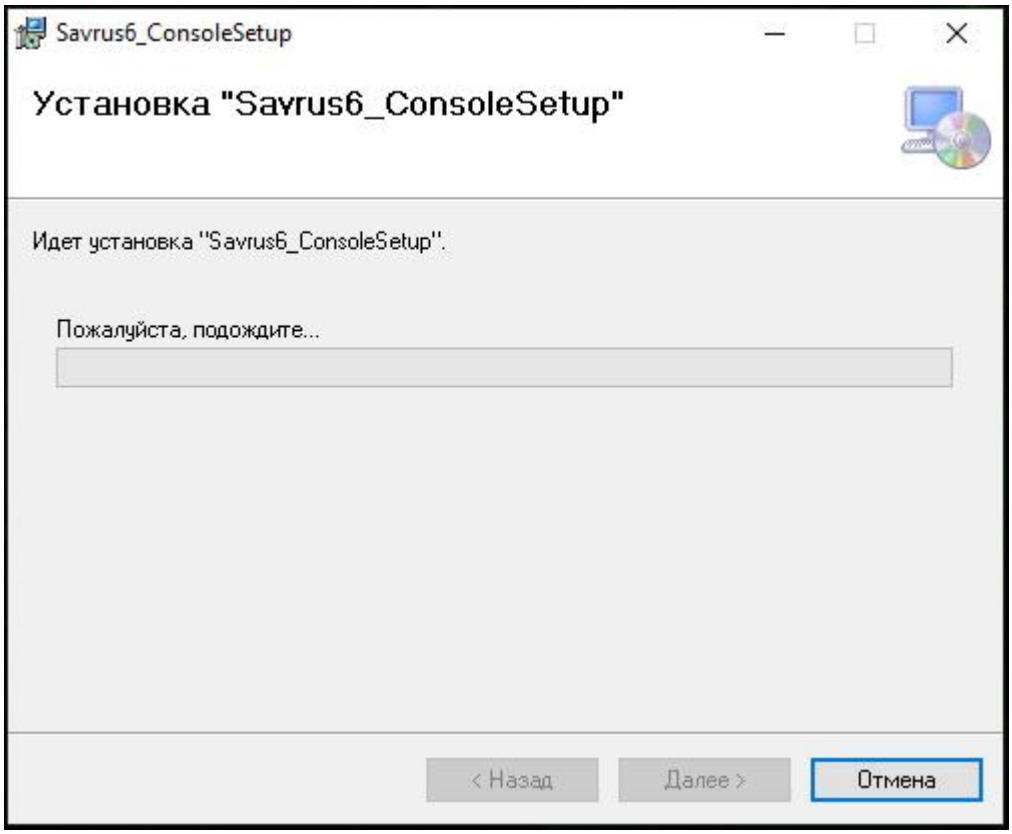

Рисунок 6. Установка консоли

После успешной установки консоли САВРУС откроется диалоговое окно завершения установки (см. Рисунок 7). Для завершения процесса следует нажать на кнопку «Закрыть». Консоль САВРУС успешно установилась на рабочее место и ярлык для работы с системой должен быть автоматически расположен на рабочем столе.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

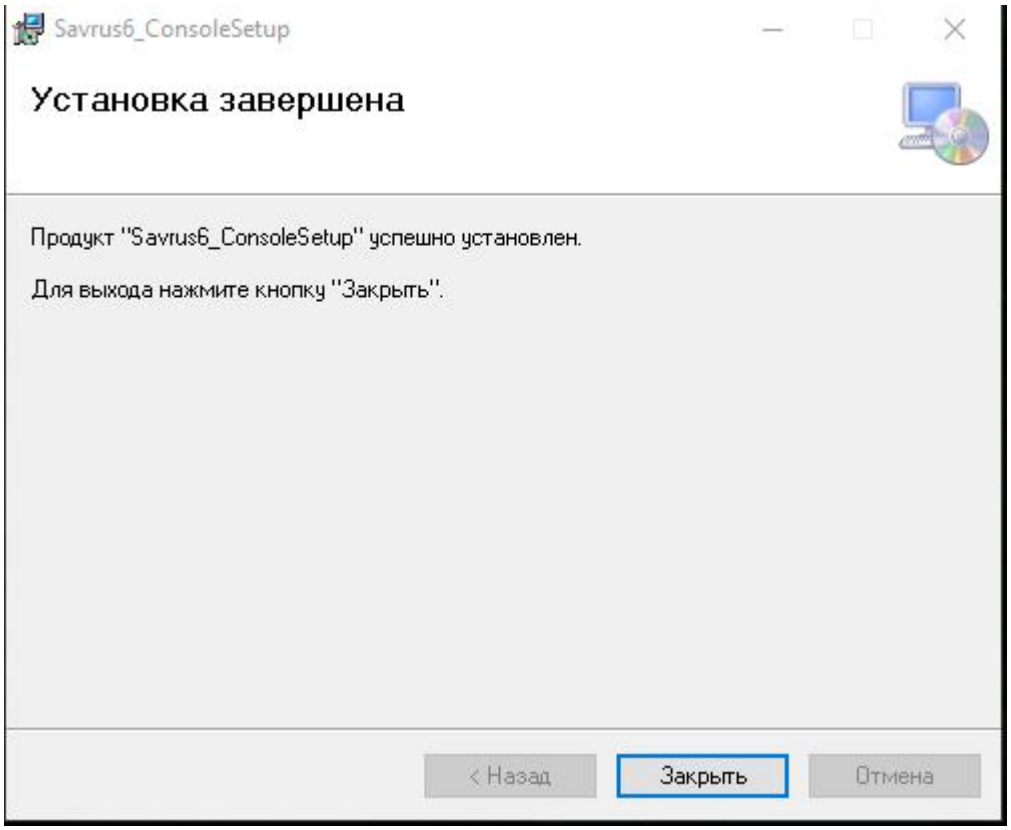

Рисунок 7. Завершение установки

2. Установка серверной части

Установка ядра системы осуществляется без доступа к сети Интернет.

Для установки ядра системы необходимо подготовить сервер (физический или виртуальный). Инсталяция должна производиться на чистом и обновленном сервере.

Для корректной работы системы необходимо произвести разметку диска на сервере. Ниже представлен пример разметки диска.

Разметка диска:

- /boot (sda2) – 1Gb
- /boot/efi (efi) – 500Mb
- / (ext4) – max
- /boot и /boot/efi – загрузочные разделы
- /boot/efi нужен только в случае, если сервер имеет поддержку UEFI

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Размер swap не важен, в боевом режиме swap нужно отключать.

Далее необходимо загрузить на подготовленный сервер дистрибутив с инсталлятором САВРУС (savrus_install XX_XX_XX) и запустить его.

Далее необходимо с помощью команды `./savrus_install` запустить установку серверной части. При необходимости записи логов установки можно использовать команду `./savrus_install 0` . При вводе данной команды будет создан файл savrus_install.log в котором будет храниться весь лог установки.

После ввода команды будет запущена проверка совместимости инсталлятора с операционной системой. По завершению проверки, при положительном результате, необходимо согласиться с продолжением установки.

Далее появится меню с выбором типа установки

1. **Setup All-in-one** – установка всех компонентов (Clickhouse, MariaDB, inforter, inforter_ce, dotnet, savruscore). При запуске происходит проверка директорий. Если директории были найдены, то они будут удалены с уничтожением всех хранимых файлов и пересозданы.
2. **All-in-one Distributed** – установка всех компонентов на главный сервер с распределенной таблицей кликхауса (многонодовая конфигурация для подключения шардов и реплик). При установке данным способом необходимо будет задать параметры и IP адреса шародов/реплик. Развернутое описание установки указано в пункте «**3. Distributed w/o correlation**», но при выборе данного типа не нужно будет указывать IP адрес сервера с модулем корреляции.
3. **Distributed w/o correlation** – установка компонентов без модуля корреляции на сервер с распределенной таблицей кликхауса (многонодовая конфигурация).

При установке данным способом необходимо будет задать IP адреса шародов/реплик и сервера с модулем корреляции.

После установки необходимых компонентов система предложит ввести IP адреса первого шарда.

Рисунок 8. Предложение о вводе IP адреса первого шарда.

Далее система предложит ввести IP адреса для первой реплики первого шарда.

Рисунок 9. Предложение о вводе IP адреса для первой реплики первого шарда.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Если добавить реплику, то система предложит ввести IP адрес для второй реплики и тд. Если отказаться (N/n) от указания реплики, то система отправит запрос о продолжении настройки для внесения данных о следующем шарде.

Рисунок 10. Предложение о настройки следующего шарда.

При ответе (Y/y) система продолжит процедуру внесения данных для следующих шародов/реплик. Процесс настройки будет таким же, как и при настройке первого шарда.

При ответе (N/n) система начнет установку недостающих компонентов, после которой предложит ввести IP адрес машины, на которой находится модуль корреляции.

Рисунок 11. Предложение о вводе IP адреса машины с модулем корреляции.

После введения IP адреса коррелятора система доустановит необходимые файлы и процесс установки будет завершен.

4. **Setup Shard/Replica** – установка шардов/реплик для многонодовой конфигурации.
5. **Setup Correlation module** – установка модуля корреляции на отдельный сервер.
6. **Uninstall services** – удаление компонентов. Система сама определяет расположение необходимых к удалению файлов.

Список доступных компонентов для удаления:

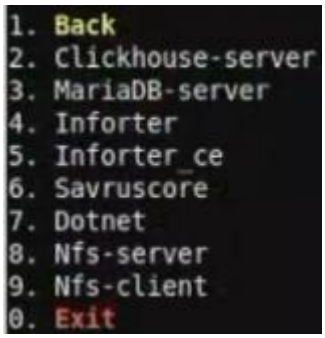

Рисунок 12. Список доступных компонентов для удаления.

7. **Update services** – обновление компонентов. При обновлении сравниваются текущая версия компонента, с версией заложенной в инсталяторе. Конфигурационные файлы компонентов не затрагиваются, кроме конфиг файла Savruscore, он будет перезаписан.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Список доступных компонентов для обновления:

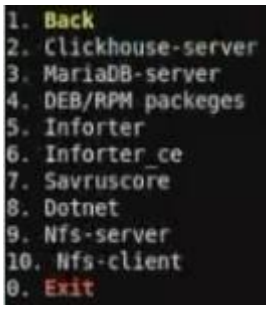

Рисунок 13. Список доступных компонентов для обновления.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

КОНФИГУРИРОВАНИЕ СИСТЕМЫ

1. Конфигурирование компонентов системы

В каждом компоненте Системы есть собственные файлы конфигурации. Изменение параметров конфигураций должно осуществляться квалифицированным специалистом администрирования САВРУС, т.к. может привести к неработоспособности отдельных компонентов или всей Системы в целом.

Перечень конфигурационных файлов (приводятся пути расположения компонентов по-умолчанию):

- для компонента «Inforter» файл конфигурации расположен в /opt/inforter с названием «config.xml»;
- для компонента «Inforter_CE» файл конфигурации расположен в /opt/inforter_ce с названием «config.xml»;
- для компонента «savruscore» файлы конфигурации и настройки параметров логирования расположены в /opt/savruscore/config с названием «appsettings.json» и «log4net.config»;
- конфигурационный файл СУБД ClickHouse расположен в /etc/clickhouse-server/ с названием «config.xml». Внесение изменений в этот файл не рекомендуется без участия вендора (САВРУС) и может привести к неработоспособности компонента;
- конфигурационные файлы СУБД MyriaDB расположены в /etc/my.cnf.d/*.*.

Внесение изменений в эти файлы не рекомендуется без участия вендора (САВРУС) и может привести к неработоспособности компонента.

Примеры с описанием параметров конфигурации приведены ниже:

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

1.1. Модуль сбора и обработки событий

```
<?xml version="1.0"?>
<inforter master="true" threads="128">
    <clickhouse config="/etc/clickhouse-server/config.xml" drop_percentage="20" db_version="3" drop_part="false" enable="true" merge="true" merge_count="100" merge_max_size="500">
        <destination host="127.0.0.1" port="9000" user="" password="" database="savrus" table="data" />
    </clickhouse>
    <parse noncef_fields="false" logging="false" />
    <logging level="1" size="10" heartbeat_interval="120" splitting_logs="false" />
    <ce enable="true" folder="/opt/inforter/data" />
    <cef port="514" granulation="5" enable="true" event_max_size="0" />
    <geoipv4 enable="false" locale="ru" />
    <mysql host="localhost" user="savrus" password="" database="savrus6" port="3306" />
    <metrics enable="false" />
    <jatoba drop_percentage="10" enable="false">
        <destination host="127.0.0.1" port="5432" user="" password="" database="savrus" table="data" />
    </jatoba>
    <assets enable="true" />
    <ssl certificate_file="/opt/inforter/certs/server.pem" privatekey_file="/opt/inforter/certs/server.key" />
    <https enable="true" port="8443" />
    <cefssl enable="true" port="515" granulation="10" />
    <cluster enable="false" name="savrus" internal_replication="false" />
    <savruscore folder="/opt/savruscore6/" />
    <cache delay="600" />
    <cepp rules_optimization="false" />
    <forwarding>
        <destination host="127.0.0.1" port="514" type="cefsyslog" protocol="UDP" cefver="0.1">
            <BasicCondition Operator="EQ" Column="deviceVendor" Value="AST" />
        </destination>
        <destination type="ceffile" folder="/opt/inforter/forwarding/cef" prefix="forwarding" cefver="0.1">
            <BasicCondition Operator="EQ" Column="deviceVendor" Value="AST" />
        </destination>
    </forwarding>
</inforter>
```

Рисунок 14. Пример конфигурационного файла Inforter

Описание параметров конфигурационного файла представлено в таблице ниже.

Таблица 2. Поля конфигурационного файла Inforter

№	Наименование	Описание	Значение по умолчанию	Примечание
Inforter – параметры модуля сбора и обработки				
1.	master	Режим работы модуля сбора и обработки	true	true – стандартный режим с отправкой событий на корреляцию false – контроль свободного места на шардах СУБД ClickHouse
2.	threads	Количество потоков	128	
Clickhouse – настройки взаимодействия с базой данных. Система САВРУС может работать с СУБД Jatoba вместо СУБД ClickHouse				
3.	config	Расположение конфигурационного файла	/etc/clickhouse-server/config.xml	
4.	drop_part	Способ отчистки базы данных	false	true – удаление партов в партициях false – удаление партиций

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

5.	enable	Использование СУБД ClickHouse	true	true-включено false-выключено
6.	merge	Объединение пакетов	true	true-включено false-выключено; При частой вставке небольших пакетов в СУБД ClickHouse, скорость обработки становится меньше
7.	merge_count	Максимальное кол-во пакетов для единоразовой вставки	100	
8.	merge_max_size	Максимальный размер одного пакета	500	Значение в мегабайтах
Clickhouse destination – параметры расположения базы данных				
9.	host	Узел нахождения базы данных	127.0.0.1	
10.	port	Порт	9000	
11.	user	Имя пользователя	-	
12.	password	Пароль	-	
13.	database	Наименование базы данных	savrus	
14.	table	Наименование таблицы	data	
Jatoba – настройка взаимодействия с СУБД Jatoba **Система САВРУС может работать с СУБД Jatoba вместо СУБД ClickHouse**				
15.	drop_percentage	Порог удаления старых партиций в базе данных	20	
16.	enable	Использование СУБД Jatoba	false	true-включено false-выключено
Jatoba destination – Параметры расположения базы данных Jatoba				
17.	host	Узел	127.0.0.1	
18.	port	Порт	5432	
19.	user	Имя пользователя	-	
20.	password	Пароль	-	
21.	database	Наименование базы данных	savrus	
22.	table	Таблица	data	
Parse – работа с событиями вне формата CEF				

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

23.	noncef_fields	Включение парсинга событий вне формата CEF	false	true-включено (при включении данного параметра возрастает нагрузка на inforter) false-выключено
24.	logging	Логирование событий вне формата CEF	false	true-включено false-выключено
Logging – параметры настройки логирования				
25.	logging_level	Уровень логирования	1	Подробнее см. раздел «Логирование в системе»
26.	size	Размер одного лог файла	10	Значение в Мбайтах
27.	heartbeat_interval	Интервал сообщений о состоянии inforter'a	120	Значение в секундах
28.	splitting_logs	Разделение логирования каждого потока	false	true-включено false-выключено Необходимо для отладки системы
Savruscore – параметры расположения модуля анализа и управления				
29.	folder	Путь к каталогу с savruscore для получения флагов	/opt/savruscore6/	Параметр необходим для получения данных о изменении ресурсов системы (флаги)
Metrics – параметры настройки метрик inforter'a				
30.	enable	Служебные события inforter'a	false	true-включено false-выключено
Mysql – параметры расположения базы данных Savrus				
31.	host	Узел	localhost	
32.	user	Имя пользователя		
33.	password	Пароль		
34.	database	Наименование базы данных	savrus6	
35.	port	Порт	3306	
CE– параметры настройки взаимодействия с модулем корреляции				
36.	enable	Перенаправление событий на модуль корреляции	true	true-включено false-выключено
37.	folder	Путь к папке, в которой лежат события	/opt/inforter/data	Папка хранения файлов с

		для направления на корреляцию		событиями для модуля корреляции
cepp				
38.	rules_optimization	Оптимизация правил	false	true-включено false-выключено
CEF – параметры настройки CEF файлов				
39.	port	Порт для приёма CEF файлов	514	
40.	granulation	Грануляция принимаемых событий	5	Значение в секундах
41.	enable	Приём данных в формате CEF	true	true-включено false-выключено
42.	event_max_size	Максимальный размер одного события	0	Значение 0 означает, что события не буду обрезаться и целиком попадут в систему.
geoipv4 – параметры настройки геолокации				
43.	enable	Геолокация	false	true-включено false-выключено Если на сервере с Inforter меньше 32 Гб оперативной памяти, геолокация будет автоматически отключаться. Подробнее см. раздел «Геолокация и сетевая модель»
44.	locale	Язык локализация	Ru	En-Английский Ru-Русский
Assets – параметр для работы с сетевой моделью				
45.	enable	Использование ассетов	true	true-включено false-выключено
Cluster - работы с шардами ClickHouse				
46.	enable	Для работы с шардами ClickHouse	false	true-включено false-выключено
47.	name	Название кластера	savrus	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

48.	internal_replication	Включение записи напрямую в шарду с помощью inforter	false	true-включено false-выключено. При значении true ClickHouse самостоятельно распределяет данные по шардам, ри - false inforter самостоятельно распределяет данные по шардам
Cache				
49.	delay	Контроль переполнения папки «data»	600	Значение в секундах. Данные событий от агентов/источников сначала записываются в папку «data», а потом перенаправляются на хранение в БД событий. Если возраст файл с данными превышает указанное значение, то данные из папки «data» удаляются
ssl – параметры ssl сертификатов				
50.	certificate_file	Расположение файлов сертификата	/opt/inforter/certs/server.pem	
51.	privatekey_file	Расположение файла ключа	/opt/inforter/certs/server.key	
Cefssl				
52.	enable	Приём данных в формате CEF по протоколу SSL	false	true-включено false-выключено
53.	port	Порт	515	
54.	granulation	Грануляция принимаемых событий	10	Значение в секундах
https – веб-интерфейс и API				

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

55.	enable	Включение/отключение веб-интерфейса	true	true-включено false-выключено Необходим для отладки правил корреляции
56.	port	Порт	8443	
forwarding – условия пересылки входящих событий по фильтру (кол-во целей пересылки неограниченно)				
destination – первая цель пересылки событий (указанный удаленный сервер)				
57.	host	Узел назначения пересылаемых событий	127.0.0.1	
58.	port	Порт	514	
59.	type	Формат пересылки событий	cefsyslog	
60.	protocol	Протокол передачи	UPD	
61.	cefver	Версия формата CEF	0.1	
BasicCondition – условие срабатывания пересылки для данной цели				
62.	Operator	Оператор сравнения	EQ	EQ-равно NE-не равно GT-болшьше GE-больше или равно LT-меньше LE-меньше или равно EndsWith-заканчивается с Contains-содержит StartWith-начинается с
63.	Column	Столбец, по которому производится сравнение	deviceVendor	
64.	Value	Значение, с которым будет происходить сравнение	AST	
destination – вторая цель пересылки событий (сохранение в файле на локальном диске)				
65.	type	Формат сохранения событий	ceffile	
66.	folder	Папка, в которую будут сохраняться файлы	/opt/inforter/forwardin/cef	
67.	prefix	Префикс, который будет добавлен к именам файлов	forwarding	
68.	cefver	Версия формата CEF	0.1	

BasicCondition – условие срабатывания пересылки для данной цели				
69.	Operator	Оператор сравнения	EQ	EQ-равно NE-не равно GT-болшьше GE-больше или равно LT-меньше LE-меньше или равно EndsWith-заканчивается с Contains-содержит StartWith-начинается с
70.	Column	Столбец, по которому производится сравнение	deviceVendor	
71.	Value	Значение, с которым будет происходить сравнение	AST	

1.2. Модуль корреляции событий

```
<?xml version="1.0"?>
<inforter_ce threads="64" vendor="Savrus">
    <logging logging_level="1" size="5" heartbeat_interval="120" splitting_logs="false"
    <ce folder="/opt/inforter/data/" rules_matches="200" rules_disable_threshold="3" ru
    <mysql host="localhost" user="savrus" password="sBknC7tM/OMhYR2B6fQIvA==" database="
    <email from="savrus@ast-security.ru" url="smtps://smtp.yandex.ru:465" user="savrus@a
    <savruscore folder="/opt/savruscore6/" />
    <metrics enable="true" />
    <ssl certificate_file="/opt/inforter/certs/server.pem" privatekey_file="/opt/inforte
    <https enable="true" port="8444" send_events="true" />
    <clickhouse>
        <destination host="127.0.0.1" port="9000" user="" password="" database="savrus"
    </clickhouse>
    <audit rules_threshold="true" rules_delay="true" />
    <rrules check="false" check_interval="60" />
    <rules granulation_enable="true" />
</inforter_ce>
```

Рисунок 15. Пример конфигурационного файла InforterCE

Описание параметров конфигурационного файла представлено в таблице ниже.

Таблица 3. Поля конфигурационного файла InforterCE

№	Наименование	Описание	Значение по умолчанию	Примечание

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Inforter_ce				
1.	threads	Количество потоков	64	
2.	vendor	Наименование вендора для указания в полях событий	Savrus	
Logging – параметры настройки логирования				
3.	logging_level	Уровень логирования	1	Подробнее см. раздел «Логирование в системе»
4.	size	Размер одного лог файла	5	Значение в Мегабайтах
5.	heartbeat_interval	Интервал сообщений о состоянии inforter CE	120	Значение в секундах
6.	splitting_logs	Разделение логирования каждого потока	false	true-включено false-выключено Необходимо для отладки системы
7.	max_string_size	Максимальный размер строки лога	16384	
ce				
8.	folder	Путь к папке с событиями от модуля сбора и обработки	/opt/inforter/data/	Папка с файлами событий безопасности
9.	rules_matches	Предельное количество срабатываний одного правила в секунду	1000	При превышении значения правило выключается
10.	rules_disable_threshold	Ограничение для отключения правил	1	Значение 1 означает что правило потребляет 100% ресурсов одного ядра процессора. Можно использовать или этот параметр или max_cpu_usage_percentage

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

11.	rules_optimization	Оптимизация правил	false	true-включено false-выключено
12.	max_cpu_usage_percentage	Максимальная нагрузка правила на процессор	90	Значение в процентах нагрузка всего процессора. При превышении параметра система отключает самые тяжёлые для обработки правила
13.	rules_action_colleration_event_fields	Выбор значений при выполнении действий в правилах	false	true- берётся значение из корреляционного события false- берётся значение из базового события
Mysql – параметры расположения базы данных Savrus				
14.	host	Узел	localhost	
15.	user	Имя пользователя		
16.	password	Пароль		
17.	database	Наименование базы данных	savrus6	
18.	port	Порт	3306	
19.	delay	Задержка времени синхронизации с базой данных	1	
20.	max_allowed_packet	Максимальный пакет, который можно от править в базу за сессию	1073741824	Значение в байтах
Email – параметры настройки оповещений				
21.	from	Отправитель оповещения		
22.	url	Адрес почтового сервиса		
23.	user	Имя пользователя		
24.	password	Пароль		
25.	encryption	Тип шифрования		
Savruscore – параметры расположения savruscore (модуля управления и анализа)				
26.	folder	Расположение savruscore (модуля управления и анализа)	/opt/savruscore6/	
Metrics – параметры настройки метрик inforter_ce'a				

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

27.	enable	Служебные события модуля корреляции	true	true-включено false-выключено
ssl – расположение ssl сертификатов				
28.	certificate_file	Расположение файлов сертификата	/opt/inforter/certs/server.pem	
29.	privatekey_file	Расположение файла ключа	/opt/inforter/certs/server.key	
https				
30.	enable	Включение/отключение веб-интерфейса	true	true-включено false-выключено Необходим для отладки правил корреляции
31.	port	Порт	8444	
Clickhouse destination – настройки взаимодействия с базой данных				
32.	host	Узел нахождения базы данных	127.0.0.1	
33.	port	Порт	9000	
34.	user	Имя пользователя		
35.	password	Пароль		
36.	database	Наименование базы данных	savrus	
37.	table	Наименование таблицы	data	
Audit – аудит работы правил корреляции				
38.	rules_threshold	Порог срабатывания правил	false	true-включено false-выключено
39.	rules_delay	Аудит задержки срабатывания правила	false	true-включено false-выключено
RRules – параметры взаимодействия с ретроспективными правилами				
40.	check	Включает проверку длительности выполнения ретроправил	false	true-включено false-выключено
41.	check_interval	Время, по истечении которого поступает событие о превышении времени	60	Значение в секундах

		выполнения правила		
Rules – параметры взаимодействия с правилами				
42.	granulation_enable	Включение/отключение грануляции	false	true-включено false-выключено

1.3. Модуль анализа и управления

Конфигуратор настроек ядра

Функционал конфигурирования настроек ядра системы САВРУС представляет из себя консольное приложение, позволяющее администратору системы установить нужные значения параметров конфигурации с помощью удобного текстового меню с гибкой и интуитивно понятной навигацией.

Этот функционал совмещает в себе удобный доступ к параметрам конфигурации, развернутое описание параметров конфигурации и валидацию вводимых значений.

Для того, чтобы войти в режим конфигурирования ядра системы САВРУС необходимо:

Перейти в директорию установки ядра системы САВРУС с помощью команды вида:

```
#cd /opt/savruscore
```

Запустить конфигуратор с помощью команды:

```
#dotnet SavrusService.dll -console -setup
```

После выполнения указанных команд будет показано меню, в котором отражены основные пункты настройки конфигурации:

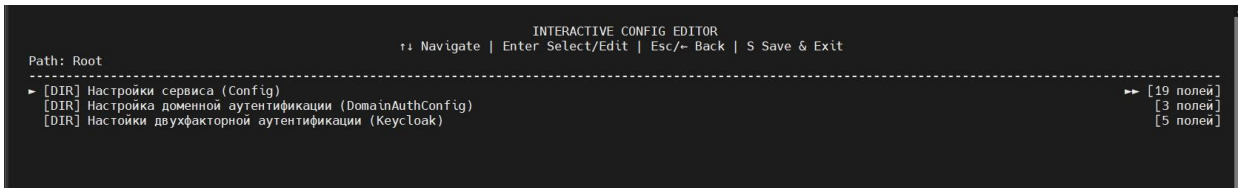

Рисунок 16. Основное меню настройки конфигурации.

- Настройки сервиса.
- Настройка доменной аутентификации.
- Настройка двухфакторной аутентификации.

В меню присутствуют несколько типов пунктов с обозначениями:

- **[DIR]** – Директория (элемент, содержащий вложенные пункты).

- **[VAL]** – Параметр (конечный элемент конфигурации, содержащий конкретное значение).
- **[ARR]** – Массив параметров (массив элементов, содержащих одинаковый набор параметров).

При редактировании элемента типа **[ARR]** появляется дополнительный пункт меню, позволяющий добавить элемент массива и пункт в навигации (горячая клавиша **«Delete»**), позволяющий удалить элемент массива.

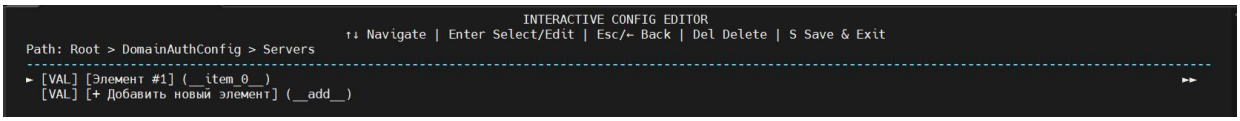

Рисунок 17. Пункт меню «Настройки параметров сервера аутентификации».

Редактирование элементов массива ничем не отличается от редактирования других пунктов конфигурации.

Для сохранения конфигурации и выхода из конфигуратора необходимо нажать горячую клавишу **«S»** в режиме навигации, для выхода из конфигуратора без сохранения конфигурации необходимо несколько раз нажать **«ESC»** до получения соответствующего оповещения.

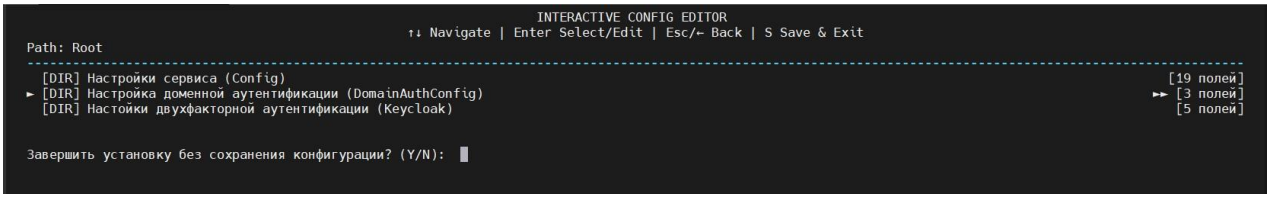

Рисунок 18. Оповещение о завершении установки без сохранения в основном меню настройки.

Пункт «Настройки сервиса»

Данный пункт содержит в себе основные параметры настроек ядра с их подробным описанием текущими значениями. При выборе параметра конфигурации для редактирования будет отображено соответствующее меню, где отражен тип параметра конфигурации, признак того – будет ли храниться его значение в зашифрованном виде, текущее значение параметра. Если конфигурация создается «с нуля» - будет указано значение по умолчанию. При вводе параметров, которые должны храниться в зашифрованном виде, вводимые символы замещаются символом **«*».**

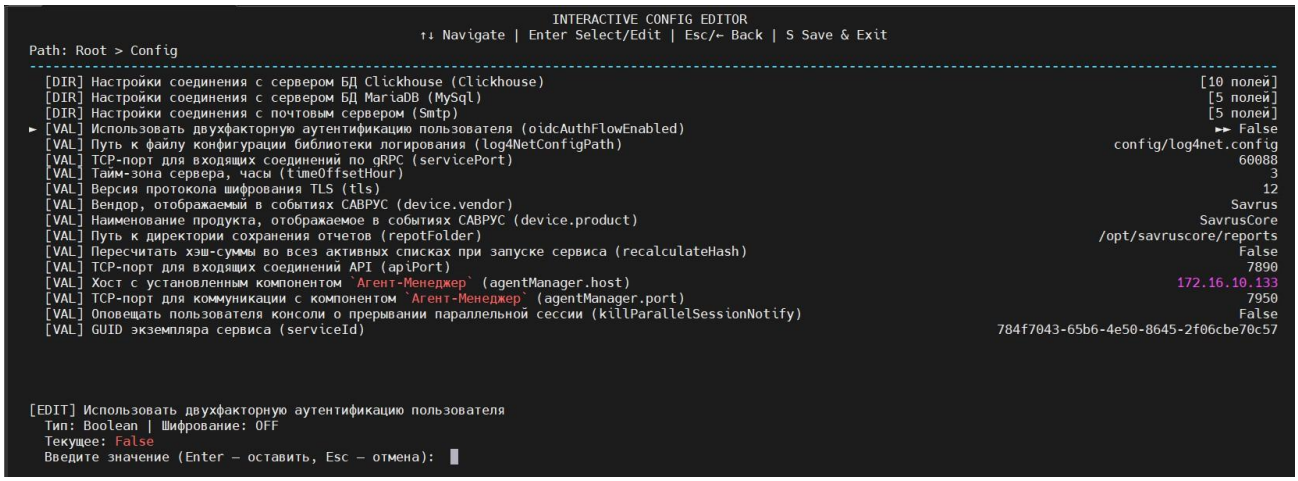

Рисунок 19. Пункт меню «Настройки сервиса».

Пункт «Настройки доменной аутентификации»

Позволяет включить/отключить режим доменной аутентификации со стороны ядра, задать период проверки доменных учетных записей доменных пользователей, имеющих активные сессии на ядре, и задать настройки сервера доменной аутентификации.

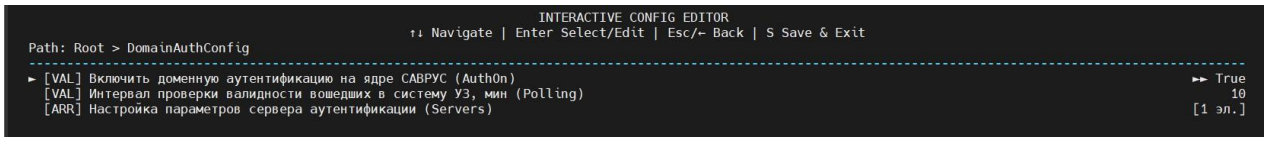

Рисунок 20. Пункт меню «Настройки доменной аутентификации».

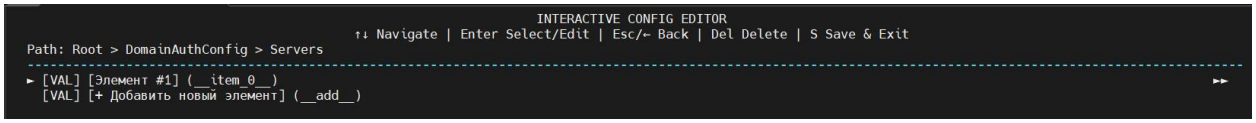

Рисунок 21. Пункт меню «Настройки параметров сервера аутентификации».

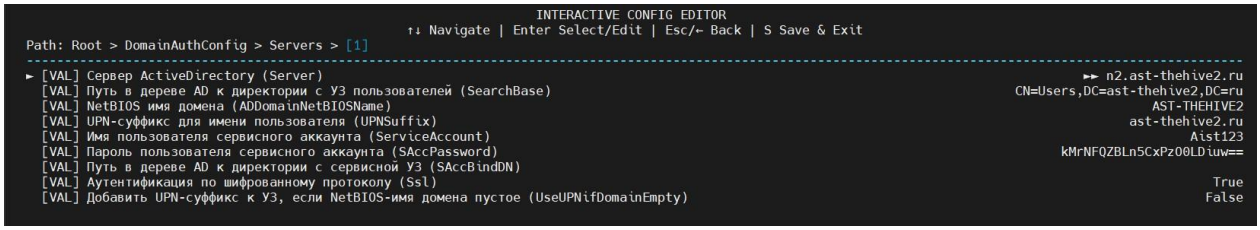

Рисунок 22. Настройки элемента сервера аутентификации.

Пункт «Настройка двухфакторной аутентификации»

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Позволяет задать значения параметров конфигурации для настройки доступа к серверу «**Keycloack**» при режиме работы с двухфакторной аутентификацией.

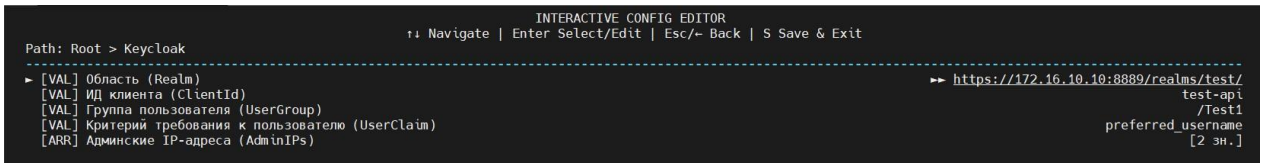

Рисунок 23. Пункт меню «Настройки двухфакторной аутентификации».

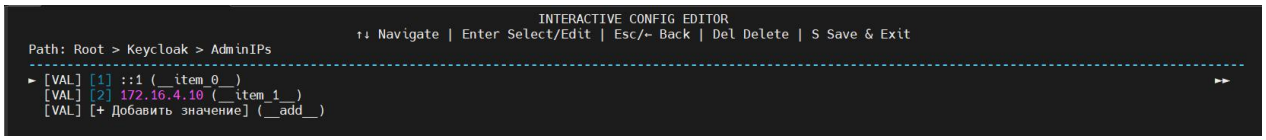

Рисунок 24. Пункт меню «Адинские IP-адреса».

Параметры настроечного файла модуля анализа и управления

```
"DomainAuthConfig":
  { "AuthOn": true,
  "Polling": 10,
  "Servers": [
    {
      "Server": "",
      "SearchBase": "",
      "ADDomainNetBIOSName": "",
      "UPNSuffix": "",
      "ServiceAccount": "",
      "SAccPassword": "",
      "SAccBindDN": "",
      "Ssl": true,
      "UseUPNifDomainEmpty": false
    }
  ]
},
"Config":
  { "Clickhouse": {
    "ch.host": "localhost",
    "ch.port": 9000,
    "ch.user": "default",
    "ch.pass": "",
    "ch.db": "savrus",
    "ch.table": "data",
    "ch.table.incidents": "incidents",
    "ch.Timeout": 100000,
    "ch.Ssl": false,
    "ch.CertificatePath": "certs/server.pem"
  },
  "MySql": {
    "mysql.host": "localhost",
```

```
      "mysql.port":,
      "mysql.user": "",
      "mysql.pass": "",
      "mysql.db": "savrus"
    },
    "Smtp":
      { "smtp.host": "",
      "smtp.from": "",
      "smtp.username": "",
      "smtp.pass": "",
      "smtp.encryption": "ssl"
    },
    "oidcAuthFlowEnabled": false,
    "log4NetConfigPath": "config/log4net.config",
    "servicePort": 7888,
    "timeOffsetHour": 3,
    "tls": 12, "device.vendor":
    "Savrus",
    "device.product": "SavrusCore",
    "repotFolder": "Reports/",
    "recalculateHash": false,
    "apiPort": 7890,
    "agentManager.host": "localhost",
    "agentManager.port": 7950,
    "killParallelSessionNotify": true,
    "serviceId": "784f7043-65b6-4e50-8645-2f06cbe70c57"
  },
  "Keycloak":
    { "Realm": "",
    "ClientId": "",
    "UserGroup": "",
    "UserClaim": "",
    "AdminIPs": [
      "::1",
      "127.0.0.1"
```

Рисунок 25. Пример конфигурационного файла SavrusCore

Таблица 4. Поля конфигурационного файла SavrusCore

№	Наименование	Описание	Примечание
DomainAuthConfig - настройка доменной аутентификации			
1.	AuthOn	Включить доменную аутентификацию на ядре САВРУС	
2.	Polling	Интервал проверки валидности вошедших в систему УЗ, мин	
3.	Servers	Настройка параметров сервера аутентификации	
4.	Server	Сервер ActiveDirectory	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

5.	SearchBase	Путь в дереве AD к директории с УЗ пользователей	
6.	ADDomainNetBIOS Name	NetBIOS имя домена	
7.	UPNSuffix	UPN-суффикс для имени пользователя	
8.	ServiceAccount	Имя пользователя сервисного аккаунта	
9.	SAccPassword	Пароль пользователя сервисного аккаунта	
10.	SAccBindDN	Путь в дереве AD к директории с сервисной УЗ	
11.	Ssl	Аутентификация по шифрованному протоколу	
12.	UseUPNifDomainEmpty	Добавить UPN-суффикс к УЗ, если NetBIOS-имя домена пустое	
		Config – настройки SavrusCore	
13.		Clickhouse - Настройки соединения с сервером БД Clickhouse	
14.	ch.host	Хост, на котором расположена СУБД ClickHouse	Если все компоненты расположены на одном сервере, то рекомендуемый параметр 127.0.0.1
15.	ch.port	Порт подключения СУБД ClickHouse	
16.	ch.user	Пользователь СУБД ClickHouse	
17.	ch.pass	Пароль СУБД ClickHouse	
18.	ch.db	Наименование базы данных СУБД ClickHouse	
19.	ch.table	Наименование таблицы с данными о событиях безопасности СУБД ClickHouse	
20.	ch.table.incidents	Имя таблицы хранения инцидентов	
21.	ch.Timeout	Таймаут соединения с СУБД ClickHouse	
22.	ch.Ssl	Использовать защищенное соединение	
23.	ch.CertificatePath	Путь к SSL-сертификату	
24.		MySql - Настройки соединения с сервером БД MariaDB	
25.	mysql.host	хост, на котором расположена СУБД MariaDB	Если все компоненты расположены на одном сервере, то рекомендуемый параметр 127.0.0.1
26.	mysql.port	Порт подключения СУБД MariaDB	
27.	mysql.user	Пользователь СУБД MariaDB	
28.	mysql.pass	Пароль СУБД MariaDB	
29.	mysql.db	Наименование базы данных СУБД MariaDB	
30.		Smtp - Настройки соединения с почтовым сервером	
31.	smtp.host	Почтовый сервер SMTP	
32.	smtp.from	Учетная запись отправителя	
33.	smtp.username	Имя пользователя сервера SMTP	
34.	smtp.pass	Пароль пользователя сервера SMTP	
35.	smtp.encryption	Протокол шифрования сообщений	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

36.	oidcAuthFlowEnabled	Использовать двухфакторную аутентификацию пользователя	
37.	log4NetConfigPath	Путь к файлу конфигурации библиотеки логирования	
38.	servicePort	TCP-порт для входящих соединений по gRPC	Значение 7888
39.	timeOffsetHour	Тайм-зона сервера, часы	
40.	tls	Версия протокола шифрования TLS	
41.	device.vendor	Вендор, отображаемый в событиях САВРУС	
42.	device.product	Наименование продукта, отображаемое в событиях САВРУС	
43.	repotFolder	Путь к директории сохранения отчетов	
44.	recalculateHash	Пересчитать хэш-суммы во всез активных списках при запуске сервиса	
45.	apiPort	TCP-порт для входящих соединений API	
46.	agentManager.host	Хост с установленным компонентом Агент-Менеджер	
47.	agentManager.port	TCP-порт для коммуникации с компонентом Агент-Менеджер	
48.	killParallelSessionNotify	Оповещать пользователя консоли о прерывании параллельной сессии	
49.	serviceId	GUID экземпляра сервиса	
50.		Keycloak - Настойки двухфакторной аутентификации	
51.	Realm	Область	
52.	ClientId	ID клиента	
53.	UserGroup	Группа пользователя	
54.	UserClaim	Критерий требования к пользователю	
55.	AdminIPs	Адмиские IP-адреса	

Настроечный файл библиотеки логирования log4net представлен ниже.

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
  <appender name="DebugAppender" type="log4net.Appender.DebugAppender" >
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date %-5level %logger - %message%newline" />
    </layout>
  </appender>
  <appender name="RollingFile" type="log4net.Appender.RollingFileAppender">
    <file value="logs/savrusmgrsvc.log" />
    <appendToFile value="true" />
    <maximumFileSize value="100KB" />
    <maxSizeRollBackups value="2" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date %5level: %message%newline %exception" />
    </layout>
  </appender>
  <appender name="ErrorFile" type="log4net.Appender.RollingFileAppender">
    <file value="logs/errors.log"/>
    <appendToFile value="true"/>
    <maximumFileSize value="5MB"/>
    <maxSizeRollBackups value="10"/>
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%d %level %thread %logger - %message%newline"/>
    </layout>
    <filter type="log4net.Filter.LevelRangeFilter">
      <levelMin value="ERROR"/>
      <levelMax value="FATAL"/>
    </filter>
  </appender>
  <appender name="RemoteLogAppender" type="SavrusService.RemoteLogAppender, SavrusService">
    <sendProtocol value="tcp"/>
    <hostAddress value="127.0.0.1"/>
    <hostPort value="514"/>
    <basicSet value="true"/>
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%d [%level] %thread %logger - %message"/>
    </layout>
  </appender>
  <root>
    <level value="ALL"/>
    <appender-ref ref="DebugAppender" />
    <appender-ref ref="RollingFile" />
    <appender-ref ref="ErrorFile"/>
    <appender-ref ref="RemoteLogAppender"/>
  </root>
</log4net>
```

Рисунок 26. Пример конфигурационного файла библиотеки логирования log4net.

1.4. СУБД ClickHouse

В конфигурационном файле ClickHouse необходимо раскомментировать строки: «max_table_size_to_drop», «max_partition_size_to_drop».

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

```
<max_table_size_to_drop>0</max_table_size_to_drop>
<max_partition_size_to_drop>0</max_partition_size_to_drop>
```

Рисунок 27. Строки конфигурационного файла

Внесение других изменений в конфигурационный файл не рекомендуется, т. к. может привести к неработоспособности системы.

1.5. СУБД MariaDB

При установке компонентов (модуль сбора и обработки, модуля управления и анализа, ClickHouse) на одном сервере, внесение изменений в конфигурационный файл не рекомендуется, т. к. может привести к неработоспособности системы. При другом размещении компонентов необходимо обратится за консультацией к вендору.

1.6. Консоль «САВРУС»

Конфигурационный файл консоли «САВРУС» находится в папке с файлами консоли и называется «Savrus.dll.config»

Описание назначения параметров конфигурационного файла консоли «САВРУС»

```
<userSettings>
    <Savrus.Properties.Settings>
```

Тип используемого gRPC-протокола, используемого для канала связи консоли и ядра.

- 1 – gRPC
- 2 – gRPC Web

```
<setting name="TypeConnection" serializeAs="String">
    <value>1</value>
</setting>
```

Версия используемого протокола TLS, используемого для канала связи консоли и ядра.

- 3 – TLS 1.2
- 4 – TLS 1.3

```
<setting name="TLS" serializeAs="String">
    <value>4</value>
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

```
        </setting>
```

Перечень IPv4-адресов серверов с установленным ядром системы, используется для быстрого переключения соединения.

```
        <setting name="ServiceAddressList" serializeAs="Xml">
            <value>
                <ArrayOfString
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                    <string>localhost</string>
                </ArrayOfString>
            </value>
        </setting>
```

Порт, открытый на стороне ядра, для установки gRPC-соединения. Сохраняется последнее значение при успешном соединении.

```
        <setting name="ServicePort" serializeAs="String">
            <value>7889</value>
        </setting>
```

IPv4-адрес сервера с установленным ядром системы, на который было установлено последнее успешное соединение.

```
        <setting name="ServiceAddress" serializeAs="String">
            <value>localhost</value>
        </setting>
```

Язык интерфейса консоли.

- 0 – русский
- 1 - английский

```
        <setting name="Lang" serializeAs="String">
            <value>0</value>
        </setting>
```

Установленный визуальный стиль оформления пользовательского интерфейса.

```
        <setting name="DefaultSkin" serializeAs="String">
            <value>0</value>
        </setting>
```

Признак доменной аутентификации при входе пользователя в систему. Сохраняется последнее значение при успешном соединении

```
        <setting name="ADAuth" serializeAs="String">
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

```
    <value>False</value>
</setting>
```

Набор параметров, отвечающих за период срабатывания таймера обновления активного канала.

Кол-во строк в активном канале: 1000, 10000

```
<setting name="IntervalRenewShort" serializeAs="String">
    <value>120</value>
</setting>
```

Кол-во строк в активном канале: 25000

```
<setting name="IntervalRenewMiddle" serializeAs="String">
    <value>120</value>
</setting>
```

Кол-во строк в активном канале: 50000, 100000

```
<setting name="IntervalRenewLong" serializeAs="String">
    <value>240</value>
</setting>
```

Значение по умолчанию кол-ва строк в активном канале при создании канала

```
<setting name="DefaultCountActiveChannel" serializeAs="String">
    <value>10000</value>
</setting>
```

Параметры, отвечающие за отображение диаграмм (положение легенды, размещение итогов и т.д) – в данный момент не используются.

```
<setting name="PieSetting" serializeAs="String">
    <value />
</setting>
<setting name="BarSetting" serializeAs="String">
    <value />
</setting>
```

Хранит настройку по умолчанию отображения полей активного канала (порядок, ширина поля) – в данный момент используется хранение макетов объектов в БД.

```
<setting name="Fields" serializeAs="String">
    <value />
</setting>
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Имя домена, использованное при последнем удачном входом в систему с использованием доменной аутентификации.

```
<setting name="DomainName" serializeAs="String">
    <value>""</value>
</setting>
```

Набор полей по умолчанию при создании активного канала.

```
<setting name="DefaultSQLAV" serializeAs="String">
    <value>type, _seid, srt, name, deviceAddress,
deviceHostName, severity, destinationAddress, destinationUserName,
sourceAddress, sourceUserName, deviceVendor, deviceProduct,
agentAddress, endTime</value>
</setting>
```

Интервал проверки валидности доменной учетной записи пользователя, вошедшего в систему с использованием доменной аутентификации. В версии с аутентификацией пользователя на ядре системы – не используется.

```
<setting name="IntervalDomainAccountEnableCheck"
serializeAs="String">
    <value>600</value>
</setting>
```

Символ-разделитель, используемый по умолчанию в операциях импорта и экспорта данных активного списка.

```
<setting name="CSVExportDelimiter" serializeAs="String">
    <value>;</value>
</setting>
```

Значение по умолчанию интервала фильтра получения событий при создании активного канала.

- 0 – произвольный
- 1 – 30 минут
- 2 – 1 час
- 3 – 4 часа
- 4 – 12 часов
- 5 – 1 день
- 6 – 2 дня
- 7 – 1 неделя

```
<setting name="DefaultIntervalOnAcCreate" serializeAs="String">
    <value>1</value>
</setting>
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Вкл/выкл SSL-шифрование при проверке данных учетной записи пользователя при использовании доменной аутентификации.

```
<setting name="UseLDAPS" serializeAs="String">
    <value>True</value>
</setting>
```

Вкл/выкл механизм работы с филиалами, отображение связанных элементов управления.

```
<setting name="UseTenants" serializeAs="String">
    <value>False</value>
</setting>
```

Вкл/выкл механизм работы с менеджерами агентов, отображение связанных элементов управления.

```
<setting name="UseConnectors" serializeAs="String">
    <value>False</value>
</setting>
```

Таймаут ожидания ответа сервера ядра при проверке его доступности, при превышении которого будет показываться форма повторного входа в систему.

```
<setting name="CoreStatusCheckTimeoutSec" serializeAs="String">
    <value>2</value>
</setting>
```

URL для обращения к хранилищу ключей при использовании двухфакторной аутентификации.

```
<setting name="OidcAuthority" serializeAs="String">

<value>https://<keycloak_address>:8889/realms/<my_realm>/</value>
</setting>
```

ИД клиента области хранилища ключей при использовании двухфакторной аутентификации.

```
<setting name="OidcClientId" serializeAs="String">
    <value><my_client_id></value>
</setting>
```

Вкл/выкл режима использования двухфакторной аутентификации при входе в систему.

```
<setting name="OidcAuthFlow" serializeAs="String">
    <value>True</value>
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

```
        </setting>
```

URL обратного вызова подтверждения JWT-токена при использовании двухфакторной аутентификации. На этот URL должен быть сгенерирован доверенный сертификат.

```
        <setting name="OidcRedirectUrl" serializeAs="String">
            <value>https://localhost:8627/callback</value>
        </setting>
```

Область разрешений (scope) клиента хранилища ключей при использовании двухфакторной аутентификации.

```
        <setting name="OidcScope" serializeAs="String">
            <value>openid</value>
        </setting>
```

Таймаут обращения к хранилищу ключей при использовании двухфакторной аутентификации.

```
        <setting name="OidcAuthFlowTimeout" serializeAs="String">
            <value>00:01:00</value>
        </setting>
```

Отпечаток сертификата для поиска в хранилище при использовании двухфакторной аутентификации.

```
        <setting name="CertThumbprint" serializeAs="String">
            <value />
        </setting>
```

Срок истечения действия сертификата при использовании двухфакторной аутентификации.

```
        <setting name="CertExpirationThreshold" serializeAs="String">
            <value>30.00:00:00</value>
        </setting>
    </Savrus.Properties.Settings>
</userSettings>
```

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

2. Описание баз данных

2.1. Служебная БД

В служебной базе данных, реализованной на СУБД MariaDB, имеются таблицы, описанные в таблице ниже. Подробное описание таблиц представлено в Приложение 1. Описание таблиц MariaDB.

Таблица 5. Поля служебной БД

№	Наименование таблицы	Описание	Примечание
1.	SAV_ALC_CustomZones	Используется для хранения данных о геолокации	
2.	SAV_ALC_NetModel_Asset	Используется для хранения данных о внутренней структуре организации	
3.	SAV_ALC_NetModel_Network	Используется для хранения данных о внутренней структуре организации	
4.	SAV_ALC_NetModel_Zone	Используется для хранения данных о внутренней структуре организации	
5.	SAV_ALC_RVision_Incidents	Используется для хранения данных о инцидентах	
6.	SAV_ALD_<название>	Используется для хранения активных списков, создаваемых пользователями в системе САВРУС	
7.	actualresources	Используется для хранения данных о ресурсах системы	Правила, активные листы, папки и т.д.
8.	config_properties	Используется для хранения параметров парольной политики	
9.	core_properties	Используется для хранения служебных данных, характерных для всех пользователей сервиса.	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

10.	roles	Используется для хранения данных о наименовании роли	
11.	roles_access	Используется для хранения данных о правах ролей	
12.	roles_resources	Используется для хранения данных о доступах ролей	
13.	user_auth_attempts	Используется для хранения данных о неудачных попытках входа пользователя в систему	
14.	users	Используется для хранения данных о пользователях	
15.	userspasswords	Используется для хранения данных о паролях пользователей	

2.2. БД событий

В базе данных событий, реализованной на СУБД ClickHouse, имеются таблицы, описанные в таблице ниже.

Таблица 6. Поля БД событий

№	Наименование таблицы	Описание	Примечание
Служебные таблицы			
1.	GeoLite2CityBlocksIPv4	Используется для хранения данных о геолокации и сети. Используется для обогащения событий безопасности данными геолокации.	
2.	GeoLite2CityLocationsEN	Используется для хранения данных о геолокации на английском языке.	
3.	GeoLite2CityLocationsRU	Используется для хранения данных о геолокации на русском языке	
4.	ZonesIPv4	Используется для хранения данных о территориальных зонах	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

5	mv_deviceProduct	Материализованное представление, служащее для отрисовки данных в выпадающих списках	
6	mv_deviceVendor	Материализованное представление, служащее для отрисовки данных в выпадающих списках	
7.	mv_destinstionUserName	Материализованное представление, использующееся в контекстном поиске	
8.	mv_sourceUserName	Материализованное представление, использующееся в контекстном поиске	
Основные таблицы			
9.	data	Используется хранения информации о событиях безопасности	
10.	View_data	Представление таблицы data	
Таблицы для визуализации			
11.	mv_agent_events	Материализованное представление, служащее для отрисовки данных	
12.	mv_start_Cache	Материализованное представление, служащее для отрисовки данных	
13.	mv_start_EPS_Agent_H	Материализованное представление, служащее для отрисовки данных	
14.	mv_start_EPS_DB_H	Материализованное представление, служащее для отрисовки данных	
15.	mv_start_RCname	Материализованное представление, служащее для отрисовки данных	
16.	mv_start_Rule_name	Материализованное представление, служащее для отрисовки данных	
17.	mv_start_Rule_Vendor	Материализованное представление, служащее для отрисовки данных	
18.	mv_start_activelists	Материализованное представление, служащее для отрисовки данных	

19.	mv_start_agent_EPS	Материализованное представление, служащее для отрисовки данных	
20.	mv_start_database_info	Материализованное представление, служащее для отрисовки данных	
21.	mv_start_destinationAddress	Материализованное представление, служащее для отрисовки данных	
22.	mv_start_destinationHostName	Материализованное представление, служащее для отрисовки данных	
23.	mv_start_destinationUserName	Материализованное представление, служащее для отрисовки данных	
24.	mv_start_deviceAddress	Материализованное представление, служащее для отрисовки данных	
25.	mv_start_deviceProduct	Материализованное представление, служащее для отрисовки данных	
26.	mv_start_deviceVendor	Материализованное представление, служащее для отрисовки данных	
27.	mv_start_main	Материализованное представление, служащее для отрисовки данных	
28.	mv_start_name	Материализованное представление, служащее для отрисовки данных	
29.	mv_start_resources	Материализованное представление, служащее для отрисовки данных	
30.	mv_start_severity	Материализованное представление, служащее для отрисовки данных	
31.	mv_start_sourceAddress	Материализованное представление, служащее для отрисовки данных	
32.	mv_start_sourceHostName	Материализованное представление, служащее для отрисовки данных	
33.	mv_start_sourceUserName	Материализованное представление, служащее для отрисовки данных	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

34.	mv_start_type	Материализованное представление, служащее для отрисовки данных	

3. Геолокация и сетевая модель

Система позволяет производить обогащение событий ИБ данными геолокации и отображать сетевую модель организации.

Для корректной работы функционала геолокации необходимо выделение достаточного объёма оперативной памяти на сервере системы, не менее 32 Гб. В случает нехватки оперативной памяти геолокация будет автоматически выключаться.

Функционал геолокации включается в конфигурационном файле модуля сбора и обработки в параметре geoipv4 (подробнее см. раздел «Модуль сбора и обработки событий» настоящего руководства).

Для геолокации используются следующие таблицы (подробнее в «Таблица 6. Поля БД событий»):

- БД событий:
  - GeoLite2CityBlocksIPv4;
  - GeoLite2CityLocationsEN;
  - GeoLite2CityLocationsRU;
  - ZonesIPv4.
- Служебная БД:
  - SAV_ALC_CustomZones.

Для реализации сетевой модели организации используются следующие таблицы, которые в консоли САВРУС представлены Активными списками:

- SAV_ALC_NetModel_Asset;
- SAV_ALC_NetModel_Network;
- SAV_ALC_NetModel_Zone.

Таблицы сетевой модели необходимы для обогащения событий безопасности данными сетевой модели организации. Данное обогащение происходит после обогащения событий безопасности геолокацией.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Сетевую модель можно заполнять вручную или же с помощью Импорта, по аналогии с обычными Активными списками. Единственное отличие при работе с ними проводится проверка на пересечение подсетей, чего нет в других Активных списках. Подробнее о работе с Активными списками см. «Руководство пользователя САВРУС» раздел «Активные списки».

Рекомендуется заполнять сетевую модель в следующем порядке: сначала SAV_ALC_NetModel_Zone, потом SAV_ALC_NetModel_Network и последним SAV_ALC_NetModel_Asset.

4. Запуск/остановка компонентов

В случае неактивности одного из модулей, можно осуществить запуск компонентов в ручном режиме в указанной выше последовательности. Останов компонентов, при необходимости, должен осуществляться в обратном порядке.

Если при запуске компонентов один из них автоматически не запустился, перед его запуском в ручном режиме необходимо в обратной последовательности остановить работу следующих за ним компонентов.

Остановка компонентов осуществляется командами:

```
systemctl stop <ИмяКомпонента>
```

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

Запуск компонентов осуществляется командами:

```
Systemctl start <ИмяКомпонента>
```

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

Проверка статуса компонентов осуществляется командами:

```
systemctl status <имя компонента>
```

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

В случае возникновения вопросов, обратитесь в службу поддержки вендора.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

5. Логирование в системе

Логирование в системе САВРУС осуществляется на агентах, модуле сбора и обработки событий (Inforter), модуле корреляции событий (InforterCE), модуле управления и анализа (SavrusCore) и в консоли САВРУС.

Каждый компонент системы осуществляет логирование локально в log-файлы. Компоненты Inforter, InforterCE и SavrusCore также направляют данные мониторинга в БД реализованную на СУБД ClickHouse. Для этого в конфигурационных файлах Inforter, InforterCE необходимо включить опцию метрики, а в SavrusCore в опциях device.vendor и device.product указать желаемое наименование. После этого в Консоли САВРУС можно будет построить Активный канал (а также любой вид визуализации данных) по служебным событиям компонентов системы, для этого следует в условии АК в полях device.vendor и device.product необходимый компонент.

5.1. Логирование агентов

Настройка

Настройка логирования агентов производится в конфигурационных файлах (config.xml). В параметре «logging_level» необходимо указать желаемый уровень логирования.

```
<?xml version="1.0"?>
<agent type="syslog" id="0" logging_level="1" servicename="inforter_agent_syslog"
```

Рисунок 28. Пример конфигурационного файла

Агент поддерживает 7 уровней логирования:

- 0 уровень логирования TRACE - логирование всех операций и выше;
- 1 уровень логирования DEBUG - логирование отладочной информации и выше;
- 2 уровень логирования INFO - логирование информационных сообщений и выше;
- 3 уровень логирования WARN - логирование предупреждений и выше;
- 4 уровень логирования ERROR - логирование ошибок и выше;
- 5 уровень логирования CRITICAL - логирование только критических ошибок;
- 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

Просмотр лог-файлов

Лог-файлы агентов хранятся в папке: `/opt/agent/logs`

5.2. Логирование Модуля сбора и обработки событий (Inforter)

Настройка

Настройка логирования inforter производится в конфигурационных файлах (config.xml). В параметре «logging_level» необходимо указать желаемый уровень логирования.

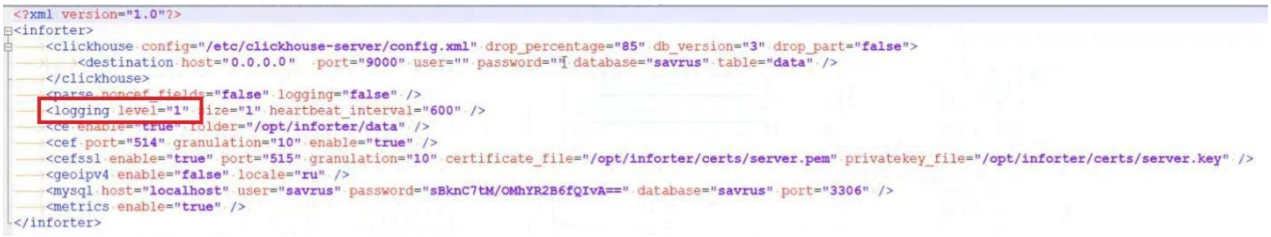

Рисунок 29. Пример конфигурационного файла

Inforter поддерживает 7 уровней логирования:

- 0 уровень логирования TRACE - логирование всех операций и выше;
- 1 уровень логирования DEBUG - логирование отладочной информации и выше;
- 2 уровень логирования INFO - логирование информационных сообщений и выше;
- 3 уровень логирования WARN - логирование предупреждений и выше;
- 4 уровень логирования ERROR - логирование ошибок и выше;
- 5 уровень логирования CRITICAL - логирование только критических ошибок;
- 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

Просмотр лог-файлов

Лог-файлы inforter хранятся в папке:`/opt/inforter/logs/`

5.3. Логирование Модуля корреляции событий (InforterCE)

Настройка

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Настройка логирования InforterCE производится в конфигурационных файлах (config.xml). В параметре «logging_level» необходимо указать желаемый уровень логирования.

InforterCE поддерживает 7 уровней логирования:

- 0 уровень логирования TRACE - логирование всех операций и выше;
- 1 уровень логирования DEBUG - логирование отладочной информации и выше;
- 2 уровень логирования INFO - логирование информационных сообщений и выше;
- 3 уровень логирования WARN - логирование предупреждений и выше;
- 4 уровень логирования ERROR - логирование ошибок и выше;
- 5 уровень логирования CRITICAL - логирование только критических ошибок;
- 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

Просмотр лог-файлов

Лог-файлы inforter хранятся в папке:`/opt/inforter_ce/logs/`

5.4. Логирование Модуля управления и анализа (SavrusCore)

Логирование модуля управления и анализа построено на использовании библиотеки log4net. SavrusCore поддерживает следующие способы логирования:

- логирование в консоль отладки;
- логирование ошибок в файл `/logs/errors.log`;
- логирование потока выполнения приложения в файл `/logs/savrusmgrsvc.log`;
- логирование событий приложения в систему Savrus.

Настройка

Настройки параметров логирования, уровней логирования и формата сообщений находятся в соответствующем разделе файла конфигурации /config/log4net.config.

```
<log4net>
        <appender name="DebugAppender" type="log4net.Appender.DebugAppender" >
          <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%date %-5level %logger - %message%newline" />
          </layout>
        </appender>
        <appender name="RollingFile" type="log4net.Appender.RollingFileAppender">
          <file value="logs/savrusmgrsvc.log" />
          <appendToFile value="true" />
          <maximumFileSize value="100KB" />
          <maxSizeRollBackups value="2" />
          <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%date %5level: %message%newline %exception" />
          </layout>
        </appender>
        <appender name="ErrorFile" type="log4net.Appender.RollingFileAppender">
          <file value="logs/errors.log"/>
          <appendToFile value="true"/>
          <maximumFileSize value="5MB"/>
          <maxSizeRollBackups value="10"/>
          <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%d %level %thread %logger - %message%newline"/>
          </layout>
          <filter type="log4net.Filter.LevelRangeFilter">
            <levelMin value="ERROR"/>
            <levelMax value="FATAL"/>
          </filter>
        </appender>
        <appender name="RemoteLogAppender" type="SavrusService.RemoteLogAppender, SavrusService">
          <sendProtocol value="tcp"/>
          <hostAddress value="333.33.33.333"/>
          <hostPort value="514"/>
          <basicSet value="true"/>
          <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%d [%level] %thread %logger - %message"/>
          </layout>
        </appender>
        <root>
          <level value="ALL"/>
          <appender-ref ref="DebugAppender" />
          <appender-ref ref="RollingFile" />
          <appender-ref ref="ErrorFile"/>
          <appender-ref ref="RemoteLogAppender"/>
        </root>
      </log4net>
```

Рисунок 30. Пример конфигурационного файла

За функционал логирования отвечает класс RemoteLogAppender, унаследованный от шаблонного библиотечного класса, класс LogObject, содержащий определение наборов событий и отвечающий за формирование раздела Extension строки сообщения в формате CEF.

В разделе конфигурации имеются настраиваемые параметры, отвечающие за выбор отправляемых событий и доставку сообщений:

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

- `<sendProtocol value="tcp"/>` – протокол передачи сообщений в систему САВРУС, допускаются значения "`udp`" и "`tcp`";
- `<hostAddress value="127.0.0.1"/>` – IPv4 адрес приёмника сообщений;
- `<hostPort value="514"/>` – порт, на котором приёмник ожидает поток сообщений;
- `<basicSet value="true"/>` – выбор набора логируемых событий: типовой/расширенный, допускаются значения "`true`" и "`false`".

Описание логируемых событий

Модуль поддерживает два набора событий: типовой и расширенный.

Типовой набор событий (name, deviceEventClassId)

Таблица 7. Типовой набор событий

Наименование события	Код
Начало работы (запуск) системы	10001
Окончание(остановка) работы системы	10002
Вход пользователя в систему	10101
Выход пользователя из системы	10102
Неуспешный вход в систему	10103
Неверное имя при входе в систему.	10104
Неверный пароль при входе в систему.	10105
Отключение пользователя\сессии по тайм-ауту	10106
Создание учетной записи	10201
Удаление учетной записи	10202
Блокировка(отключение) учетной записи	10203
Разблокировка(включение) учетной записи	10204
Смена пароля учетной записи	10205
Смена пароля пользователя Администратором системы.	10206
Создание группы(роли) пользователей	10301
Удаление группы(роли) пользователей	10302
Изменение прав группы(роли) пользователей	10303
Назначение\исключение прав пользователя на объект	10304
Исключение пользователя из состава группы(роли).	10401
Включение пользователя в состав группы(роли).	10402
Очистка журнала событий	10501
Изменение настроек аудита (включение\отключение, изменение уровня логирования)	10502
Изменение конфигурации системы (конфигурационных файлов, настроек СУБД, настроек ПО)	10503

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Включение правила консолью	10601
Выключение правила консолью	10602
Файл отчета сформирован	10701
Отчет отправлен по E-mail	10702
Файл отчета удален	10703
Включение отчета консолью	10704
Выключение отчета консолью	10705
Добавление записи в АЛ в консоли	10801
Удаление записи из АЛ в консоли	10802
Изменение записи АЛ в консоли	10803
Очистка АЛ в консоли	10804
Превышение лимита записи в АЛ при операции в консоли	10805

Расширенный набор событий (name, deviceEventClassId):

Таблица 8. Расширенный набор событий

Наименование события	Код
Создание объекта (при необходимости детального аудита)	20301
Удаление объекта (при необходимости детального аудита)	20302
Изменение объекта (при необходимости детального аудита)	20303
Чтение объекта (при необходимости детального аудита)	20304
Копирование объекта (при необходимости детального аудита)	20305
Установка прав доступа на объект (при необходимости детального аудита)	20306
Изменение прав доступа на объект (при необходимости детального аудита)	20307
Пометка объекта на удаление (при необходимости детального аудита)	20308
Снятие пометки объекта на удаление (при необходимости детального аудита)	20309
Вход пользователя в подсистему	20201
Выход пользователя из подсистемы	20202
Запуск\восстановление подсистемы (компонент, сервисов, инстансов)	20501
Остановка\сбой подсистемы (компонент, сервисов, инстансов)	20502
События успешного\неуспешного контроля целостности файлов\объектов	20503
Неуспешная валидация данных	20504
Архивирование данных (при необходимости детального аудита)	20505
Попытка удаления журналов аудита	20506
Выполнение SQL-запроса к базе MySQL	20601

Просмотр лог-файлов

Лог-файлы потока выполнения приложения находится по пути: `/opt/savruscore/logs/savrusmgrsvc.log`, логирование ошибок ведётся в файле `errors.log`. Также имеется возможность посмотреть их в консоли САВРУС.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Для просмотра логов компонента SavrusCore необходимо в консоли САВРУС в разделе «Администрирование» выбрать вкладку «Лог». Обновление лога можно осуществлять путем нажатия на кнопку «Обновить лог» в верхней части окна.

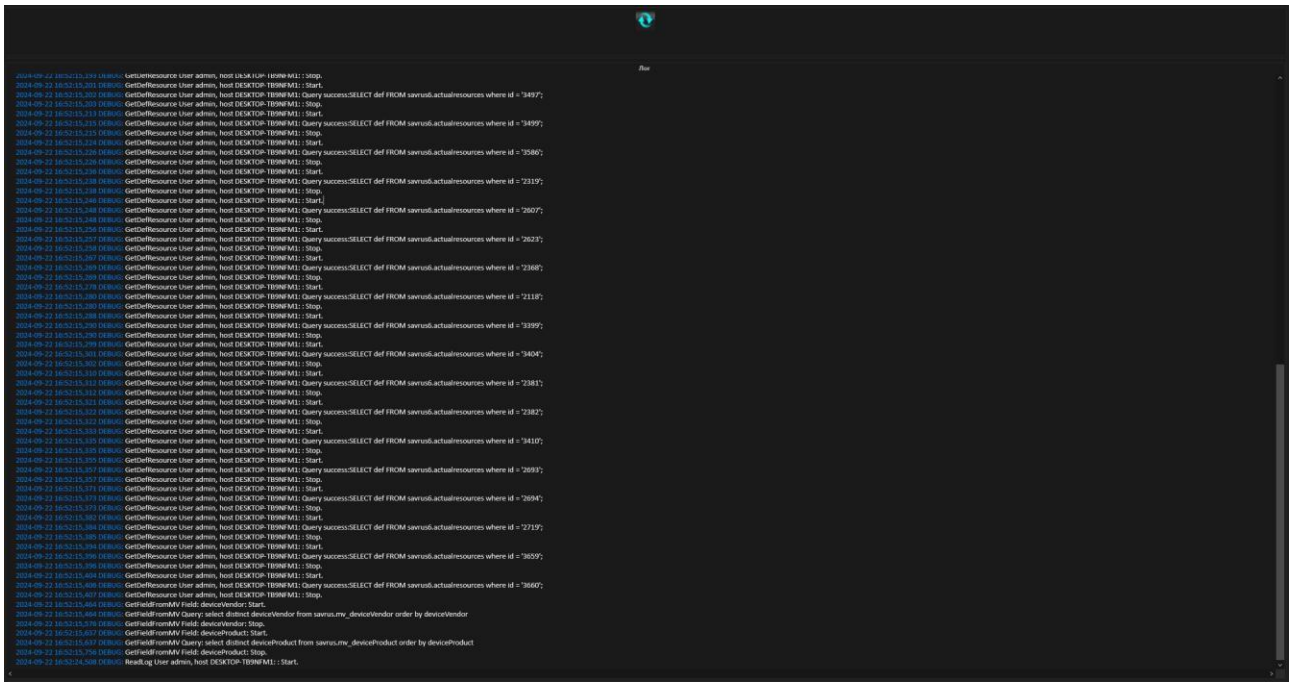

Рисунок 31. Пример логов системы

5.5. Логирование консоли САВРУС

Логирование консоли САВРУС построено на использовании библиотеки log4net. Консоль САВРУС поддерживает следующие способы логирования:

- логирование ошибок в файл `/logs/errors.log`;
- логирование потока выполнения приложения в файл `/logs/ savrus.log`.

Настройки параметров логирования, уровней логирования и формата сообщений находятся в файле конфигурации `log4net.config`.

```
<log4net>
        <appender name="LogFileAppender" type="log4net.Appender.RollingFileAppender">
          <param name="File" value="logs\savrus.log"/>
          <param name="AppendToFile" value="true"/>
          <maxSizeRollBackups value="10"/>
          <maximumFileSize value="5MB"/>
          <lockingModel type="log4net.Appender.FileAppender+MinimalLock"/>
          <layout type="log4net.Layout.PatternLayout">
            <param name="ConversionPattern" value="%d  %-5p %m%n"/>
          </layout>
        </appender>
        <appender name="ErrorFile" type="log4net.Appender.RollingFileAppender">
          <file value="logs\errors.log"/>
          <appendToFile value="true"/>
          <maximumFileSize value="5MB"/>
          <maxSizeRollBackups value="10"/>
          <layout type="log4net.Layout.PatternLayout">
            <conversionPattern value="%d %level %thread %logger - %message%newline"/>
          </layout>
          <filter type="log4net.Filter.LevelRangeFilter">
            <levelMin value="ERROR"/>
            <levelMax value="FATAL"/>
          </filter>
        </appender>
        <logger name="LOGGER">
          <appender-ref ref="LogFileAppender"/>
          <appender-ref ref="ErrorFile"/>
        </logger>
    </log4net>
```

Рисунок 32. Пример конфигурационного файла

Параметры ротации лог-файлов настраиваются в разделах:

- `<maxSizeRollBackups value="10"/>`
- `<maximumFileSize value="5MB"/>`

6. Требования к АРМ администратора/оператора

Для работы Консоли САВРУС необходимо рабочее место под управлением ОС семейства MS Windows и сетевым доступом к серверу управления САВРУС TCP/7889 (по умолчанию), TCP/22 (для администрирования).

6.1. Запуск консоли управления

Для входа в Консоль САВРУС необходимо запустить ярлык «Savrus6» на рабочем столе.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

При первом запуске Консоли САВРУС необходимо осуществить настройку подключения к серверам/компонентам САВРУС. В случае поставки САВРУС в виде виртуальной машины используются значения полей, заявленные по умолчанию.

Для настройки подключения и запуска Консоли САВРУС необходимо обеспечить заполнение следующих полей:

Таблица 9. Поля для заполнения при входе в консоль

№	Название поля	Данные для наполнения
1.	Адрес менеджера	IP Адрес или Имя сервера Модуля управления и анализа
2.	Порт менеджера	Порт (по умолчанию TCP/7888) – для соединения и взаимодействия с Модулем управления и анализа
3.	Тип подключения	GRPC или GRPC-WEB. Рекомендуется использовать GRPC
4.	TLS	1.0 / 1.1 / 1.2 / 1.3. Рекомендуется использовать 1.2
5.	Имя пользователя	Имя пользователя/администратора для авторизации
6.	Пароль	Пароль от учетной записи

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

ОБНОВЛЕНИЕ КОМПОНЕНТОВ СИСТЕМЫ

В случае выпуска мажорных версий обновления системы – обновление осуществляется с помощью инсталлятора. В случае выпуска минорных версий обновлений системы – обновление обеспечивается отдельных компонентов системы согласно положениям ниже. Дополнительно необходимо учитывать рекомендуемые параметры конфигурации компонентов системы (см. раздел «Конфигурирование компонентов системы»).

1. Обновление модуля сбора и обработки событий

Для обновления необходимо произвести следующие действия:

1. Скопировать в `/opt` папку «`inforter_<date>`».
2. Переименовать старую папку «`inforter`», например в «`inforter_old`».
3. Переименовать новую скопированную папку «`inforter_<date>`» в «`inforter`».
4. Добавить права для запуска файла (пользователем с привилегиями root) `/opt/inforter/chmod +x inforter`.
5. При наличии памяти на сервере более 32 Gb для работы может быть активирована работа компонента встроенной геолокации, для этого в `/opt/inforter/config.xml` правится строчка:

   `<geoipv4 enable="false" locale="ru" />` в `<geoipv4 enable="true" locale="ru" />`
6. Проверьте в файле `config.xml` уровень логирования. Параметр `logging_level` должен быть установлен в значение 1 или 2. Установка уровня 0 может привести к чрезмерной нагрузке на систему из-за избыточного объёма логов.
7. После обновления компонента или параметров его необходимо перезагрузить (`restart`).

2. Обновление модуля корреляции событий

Для обновления необходимо произвести следующие действия:

1. Скопировать в `/opt` папку «`inforter_ce_<date>`».

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

2. Переименовать старую папку «`inforter_ce`», например в «`inforter_ce_old`».
3. Переименовать новую скопированную папку «`inforter_ce_<date>`» в «`inforter_ce`».
4. Добавить права для запуска файла (пользователем с привилегиями root) `/opt/inforter_ce/chmod +x inforter_ce`.
5. Проверить в файле «`config.xml`» уровень логирования. «`logging_level`» должен быть выставлен в значение 1 или 2 (не 0 !!!).
6. После обновления компонента или параметров его необходимо перезагрузить (`restart`).

3. Обновление модуля анализа и управления

Для обновления необходимо произвести следующие действия:

1. Скопировать в `/opt` папку «`savruscore_<date>`».
2. Переименовать старую папку «`savruscore`», например в «`savruscore_old`».
3. Переименовать новую скопированную папку «`savruscore_<date>`» в «`savruscore`».
4. Проверить выставлено ли в файле `config/appsettings.json` корректное значение параметра `ch.table` источника данных (по умолчанию `data`).
5. После обновления компонента или параметров его необходимо перезагрузить (`restart`).

4. Обновление консоли САВРУС

Обновление ядра как правило требует установки соответствующего релиза консоли САВРУС. Для обновления консоли необходимо загрузить и развернуть соответствующий релиз. Для доступности прежних стартовых дашбордов для каждого инстанса необходимо перенести файлы конфигурации стартовых дашбордов из предыдущего релиза.

5. Проверка работоспособности компонентов

Система САВРУС и её компоненты рассчитаны на беспрерывную работу. В случае плановый перезагрузки серверов, где располагаются компоненты, Система автоматически

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

продолжит работу в штатном режиме. Для контроля работоспособности компонентов можно осуществить ряд контрольных процедур.

Все процедуры проводятся пользователем с правами root на уровне ОС (где установлены соответствующие компоненты). Для проведения контрольных и сервисных процедур необходима организация SSH соединения с компонентами Системы (RDP соединения для серверов под управлением ОС Windows, при наличии).

Проверка работоспособности Агентов осуществляется путём анализа лог-файлов, располагающихся в директориях установки агентов – `agent*.log`. Кастомизация параметров Агентов осуществляется с помощью настроечных файлов в директориях установки агентов – `agent.properties`.

6. Модуль сбора и обработки событий

Для проверки работоспособности Модуль сбора и обработки событий (Inforter) выполняется следующая команда:

```
systemctl status inforter
```

```
[root@savrus ~]# systemctl status inforter
● inforter.service - Inforter daemon
   Loaded: loaded (/usr/lib/systemd/system/inforter.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-01-15 13:20:30 MSK; 1 months 0 days ago
 Main PID: 94795 (inforter)
   CGroup: /system.slice/inforter.service
           └─94795 /opt/inforter/inforter
```

Рисунок 33. Проверка статуса работы Inforter

В случае корректной работы модуля должен быть возвращён результат «`Started Inforter daemon`»

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в `/opt/inforter/inforter.log.*`

6.1. БД Событий безопасности

Для проверки работоспособности выполняется следующая команда:

```
systemctl status clickhouse-server.service
```

В случае корректной работы модуля должен быть возвращён результат `active (exited)`, аналогично представленному на рисунке ниже:

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

```
[root@co7ch ~]# systemctl status clickhouse-server.service
● clickhouse-server.service - LSB: Yandex clickhouse-server daemon
   Loaded: loaded (/etc/rc.d/init.d/clickhouse-server; bad; vendor preset: disabled)
   Active: active (exited) since Wed 2019-07-24 21:38:11 MSK; 11h ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4986 ExecStart=/etc/rc.d/init.d/clickhouse-server start (code=exited, status=0/SUCCESS)
```

Рисунок 34.Проверка статуса работы ClickHouse

6.2. БД Служебных настроек

Для проверки работоспособности выполняется следующая команда:

`systemctl status mariadb.service или systemctl status mysqld.service`

(в зависимости от того, какая БД была установлена и поддерживается ОС)

В случае корректной работы модуля должен быть возвращён результат `active (running)`, аналогично представленному на рисунках ниже:

```
[root@co7ch ~]# systemctl status mariadb.service
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-07-24 21:38:13 MSK; 11h ago
  Process: 5081 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCES
S)
  Process: 4980 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
 Main PID: 5080 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─5080 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─5422 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/l...
```

Рисунок 35. Проверка статуса работы MariaDB

```
[root@savrus ~]# systemctl status mysqld.service
● mysqld.service - MySQL Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-11-02 19:42:25 MSK; 3 months 13 days ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
 Main PID: 103373 (mysqld)
   CGroup: /system.slice/mysqld.service
           └─103373 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid
```

Рисунок 36. Проверка статуса работы MySQL

6.3. Модуля управления и анализа

Для проверки работоспособности Модуля управления и анализа (компонента управления) выполняется следующая команда:

`systemctl status savruscore`

В случае корректной работы модуля должен быть возвращён результат `active (running)`, аналогично представленному на рисунке ниже:

```
[root@savrus ~]# systemctl status savruscore
● savruscore.service - Core3.1 Savrus Manager daemon
   Loaded: loaded (/usr/lib/systemd/system/savruscore.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2021-02-10 11:58:15 MSK; 5 days ago
 Main PID: 102118 (dotnet)
   CGroup: /system.slice/savruscore.service
           └─102118 /usr/bin/dotnet /opt/savruscore/SavrusService.dll --nossl
```

Рисунок 37. Проверка статуса работы SavrusCore

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в `/opt/savruscore/logs/*.*`

6.4. Модуля корреляции событий

Для проверки работоспособности Модуль корреляционной обработки событий (Inforter_ce) (в режиме реального времени) выполняется следующая команда:

```
systemctl status inforter_ce
```

В случае корректной работы модуля должен быть возвращён результат `Started Inforter CE daemon`, аналогично представленному на рисунке ниже:

```
[root@savrusl14 ~]# systemctl status inforter_ce
● inforter_ce.service - Inforter CE daemon
   Loaded: loaded (/etc/systemd/system/inforter_ce.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-07-19 17:06:46 MSK; 46s ago
 Main PID: 31081 (inforter_ce)
   CGroup: /system.slice/inforter_ce.service
           └─31081 /opt/inforter_ce/inforter_ce
```

Рисунок 38. Проверка статуса работы InforterCE

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в /opt/inforter_ce/inforter_ce.log.*

АДМИНИСТРИРОВАНИЕ

1. Управление ролями и правами доступа

Система САВРУС поддерживает ролевую модель доступа к ресурсам системы, для управления ролями в меню ресурсов на вкладке «Администрирование» предусмотрен раздел «Роли пользователей» (см. Рисунок 39).

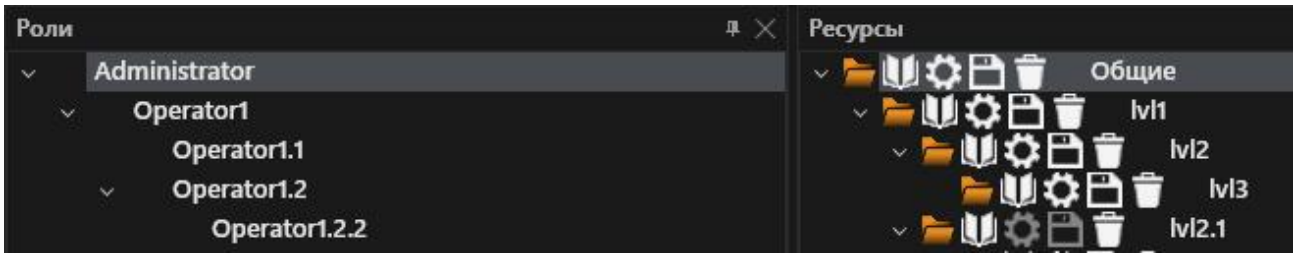

Рисунок 39. Окно управления ролями

1.1. Создание роли

Для добавления новой роли в систему необходимо нажать ЛКМ на кнопку «Добавить роль»  Или кликнуть ПКМ на роль и в контекстном меню выбрать пункт «Добавить роль».

В открывшемся диалоговом окне следует ввести имя добавляемой роли (см. Рисунок 40) и нажать кнопку «Сохранить».

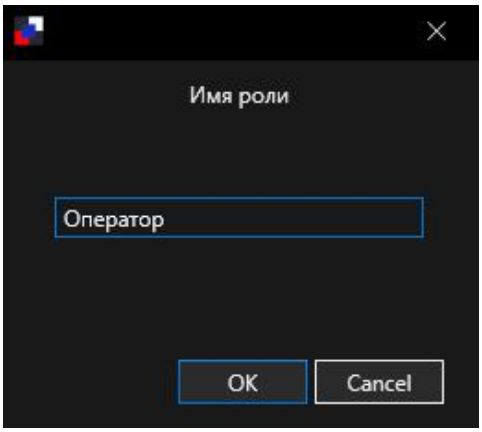

Рисунок 40. Диалоговое окно "Имя роли"

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

1.2. Настройка прав доступа

Для предоставления прав по разным категориям необходимо нажать на выпадающий список. После чего появиться перечень доступных категорий (см. Рисунок 41). Подробное описание ресурсов представлено в «Руководстве пользователя САВРУС».

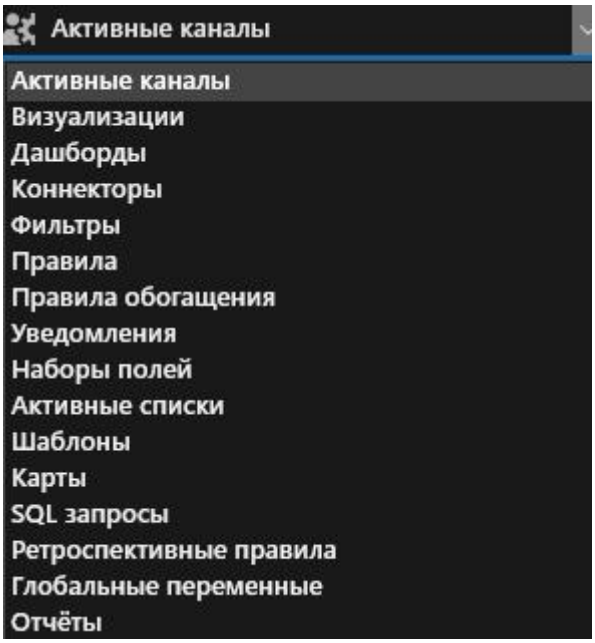

Рисунок 41. Список доступных ресурсов

После выбора необходимо задать полномочия для всех доступных ресурсов (см. Рисунок 42).

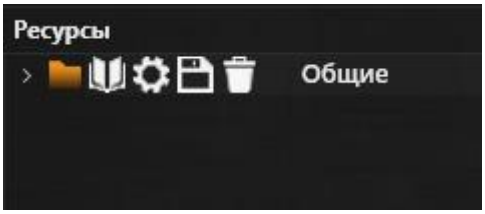

Рисунок 42. Доступные ресурсы

Можно выдать права на чтение ресурса  , редактирование  , сохранение  и удаление  . Для этого необходимо нажать на необходимую кнопку и сделать её активной.

Для права «Open» предусмотрена каскадная модель доступа. А для прав «Create», «Save», «Delete» свободное назначение.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Так же можно настроить права доступа к личным ресурсам каждой роли. Для этого необходимо задать полномочия для ресурсов, находящихся в папке «Личные» (см. Рисунок 43). Доступ к данным ресурсам имеется только у выбранной роли и администратора системы.

Рисунок 43. Меню настройки прав личных ресурсов.

1.3. Редактирование роли

Для редактирования роли необходимо выбрать её из выпадающего списка и внести изменения. После чего сохранить изменения нажатием на кнопку  . Чтобы переименовать роль следует использовать кнопку  . Или кликнуть ПКМ на роль и в контекстном меню выбрать соответствующий пункт.

1.4. Фильтры

При необходимости можно разграничивать доступ к ресурсам с помощью фильтров. Для использования фильтров следует выбрать необходимую роль из ранее созданных в системе (см. Рисунок 44).

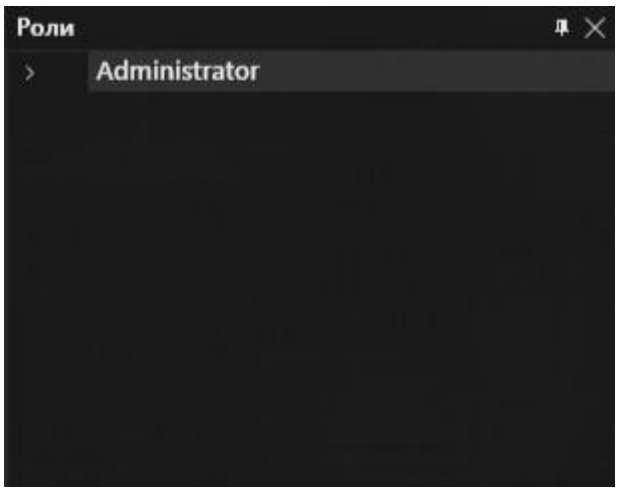

Рисунок 44. Список ролей

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Далее, следует выбрать необходимый фильтр из ранее созданных в системе (создание и редактирование фильтров подробно описано Руководстве пользователя). Для этого следует нажать на кнопку и в появившемся выпадающем списке выбрать нужный фильтр (см. Рисунок 45).

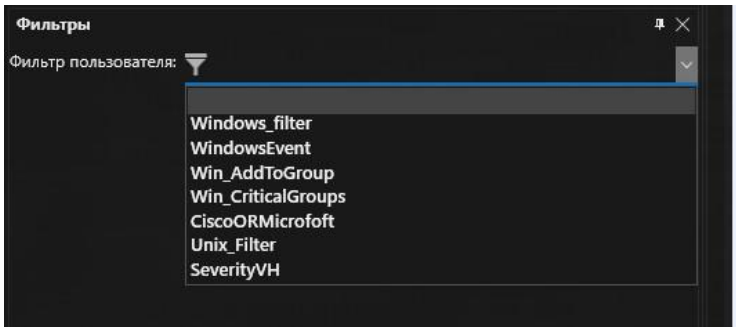

Рисунок 45. Список фильтров

После чего выбранная роль будут доступны события только в соответствии с выбранным фильтром.

1.5. Расширенные привилегии

САВРУС позволяет назначить необходимой роль расширенные привилегии администратора ИБ для проведения аудита. Для этого в меню редактирования роли пользователя необходимо соответствующем разделе нажать на кнопку и в появившемся списке выбрать необходимое (см. Рисунок 46).

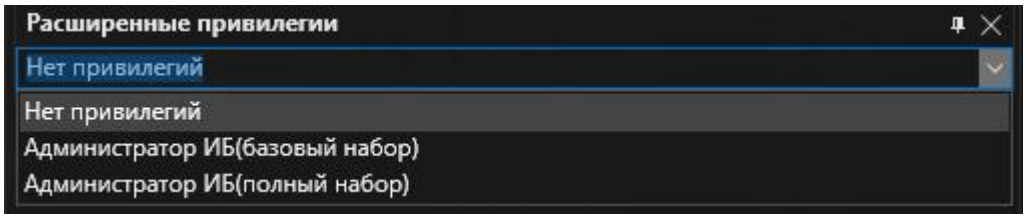

Рисунок 46. Список расширенных привилегий

2. Управление пользователями

Система САВРУС поддерживаем многопользовательский режим работы. Для управления УЗ пользователей в меню ресурсов на вкладке «Администрирование» предусмотрен раздел «Пользователи» (см. Рисунок 47).

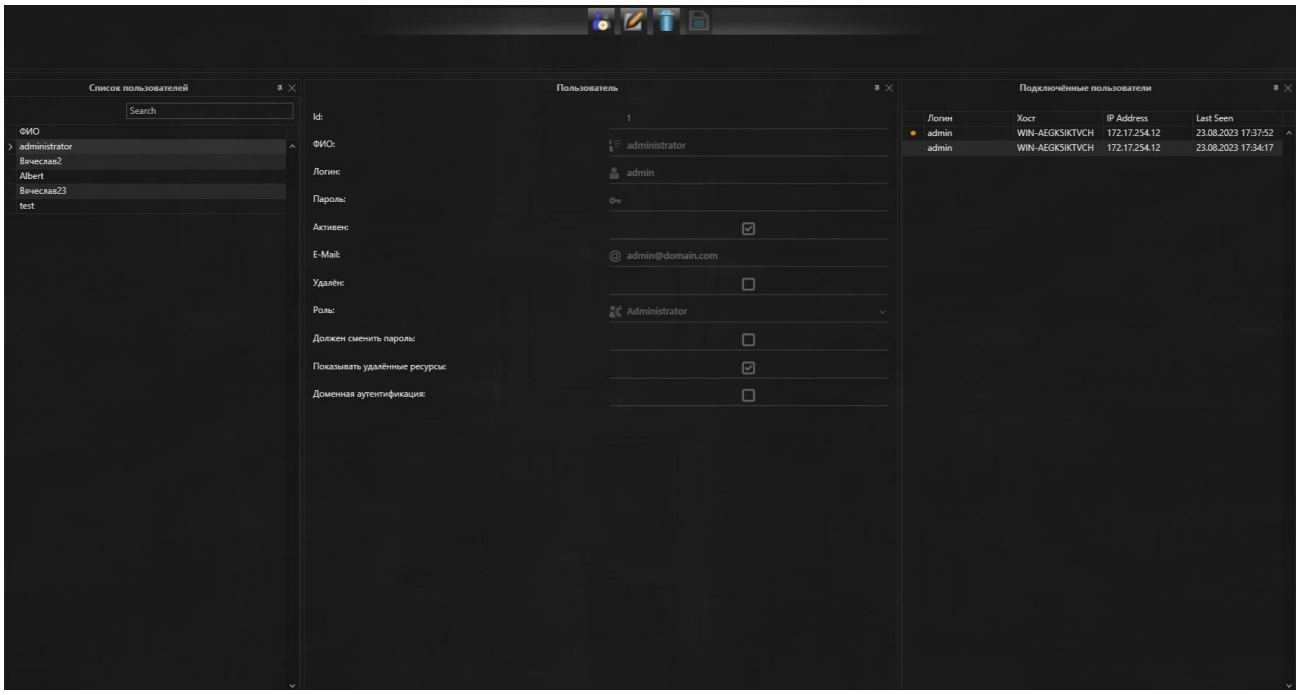

Рисунок 47. Окно управления УЗ пользователей

3. Создание УЗ

Для создания новой УЗ пользователя необходимо нажать ЛКМ на кнопку «новый пользователь»  . Или в панели слева (под списком пользователей) формы управления УЗ пользователей щёлкнуть ПКМ и в контекстном меню выбрать соответствующий пункт. В появившейся форме (см. Рисунок 48) необходимо заполнить поля перечисленные в таблице Таблица 10.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

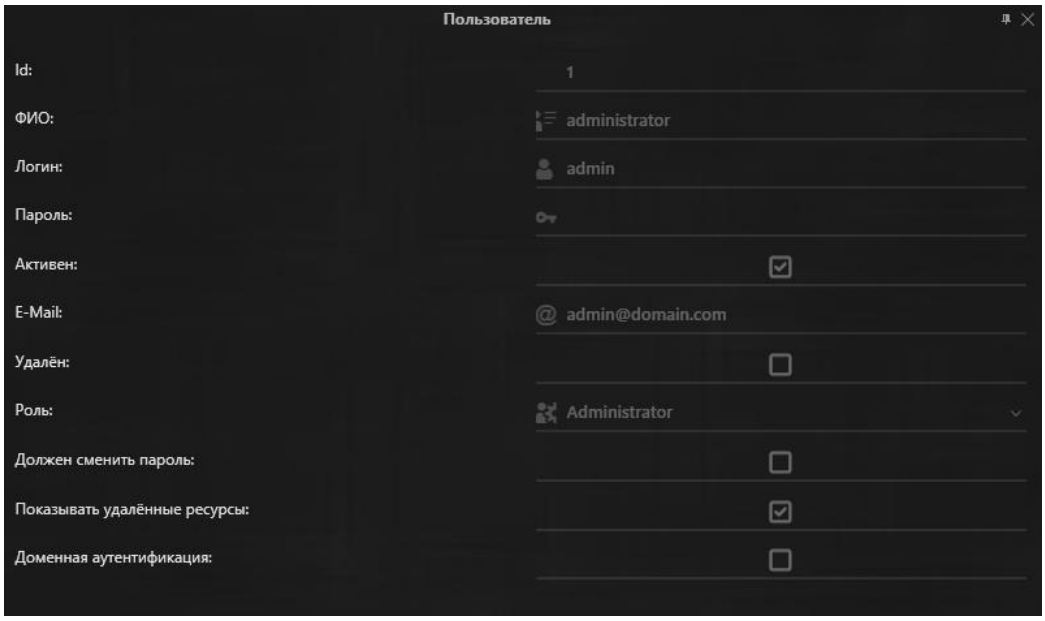

Рисунок 48. Форма создания нового пользователя

При работе с пользователями определяются следующие параметры, описанные в таблице ниже.

Таблица 10. Поля формы создания нового пользователя

Название поля	Описание	Примечание
ФИО	ФИО пользователя – владельца УЗ	
Логин	Логин создаваемой УЗ пользователя	
Пароль	Пароль создаваемой УЗ пользователя	Требования к паролю устанавливаются в соответствие с парольной политикой
Активный	Признак активности УЗ пользователя	Используется в целях временной блокировки УЗ пользователя в системе
E-mail	Электронная почта владельца УЗ пользователя	
Удалён	Признак удаления УЗ пользователя	Используется в случае удаления УЗ пользователя из системы
Роль	Роль создаваемой УЗ пользователя	Создание и редактирование ролей представлено в разделе «АДМИНИСТРИРОВАНИЕ »

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Должен сменить пароль	Признак необходимости смены пароля при первичном входе в Систему	
Показывать удалённые ресурсы	Признак возможности УЗ пользователя управлять удалёнными ресурсами	Рекомендуется только для авторизованных пользователей Системы
Доменная аутентификация	Признак необходимости входа в систему с помощью доменной аутентификации	

3.1. Внесение изменений в УЗ

Для редактирования УЗ пользователя необходимо выбрать её и перейти в режим редактирования, нажав на кнопку  или из контекстного меню, вызываемого ПКМ. В основном окне отобразятся параметры УЗ, которые можно будет скорректировать. Для применения изменений необходимо нажать кнопку  . Возможна опция удаления УЗ пользователя из Системы при нажатии кнопки  , для этого предварительно необходимо удалить или перенести ресурсы УЗ удаляемого профиля. Также в нижней части окна доступна история изменений выбранной учетной записи.

3.2. Мониторинг пользователей в системе

Для мониторинга пользователей в системе следует в меню ресурсов на вкладке «Администрирование» выбрать раздел «Пользователи». В правой части окна располагается раздел для отслеживания подключенных пользователей в системе (см. Рисунок 49). Для отключения пользователя необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «отключить».

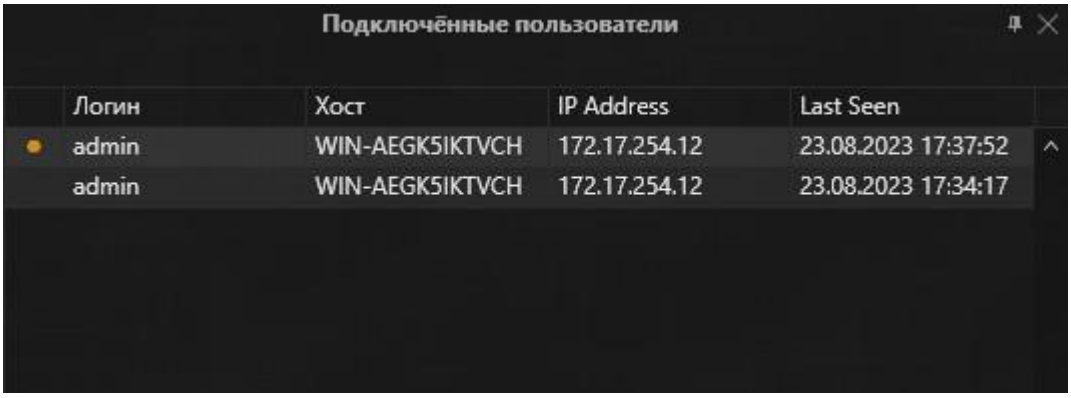

Рисунок 49. Подключенные пользователи

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

4. Логирование

Для просмотра логов системы САВРУС необходимо в разделе «Администрирование» перейти на вкладку «Лог». Подробнее об уровнях логирования написано в разделе «Логирование в системе».

5. Настройка парольной политики

Для настройки парольной политики необходимо во вкладке «Администрирование» выбрать раздел «Парольная политика».

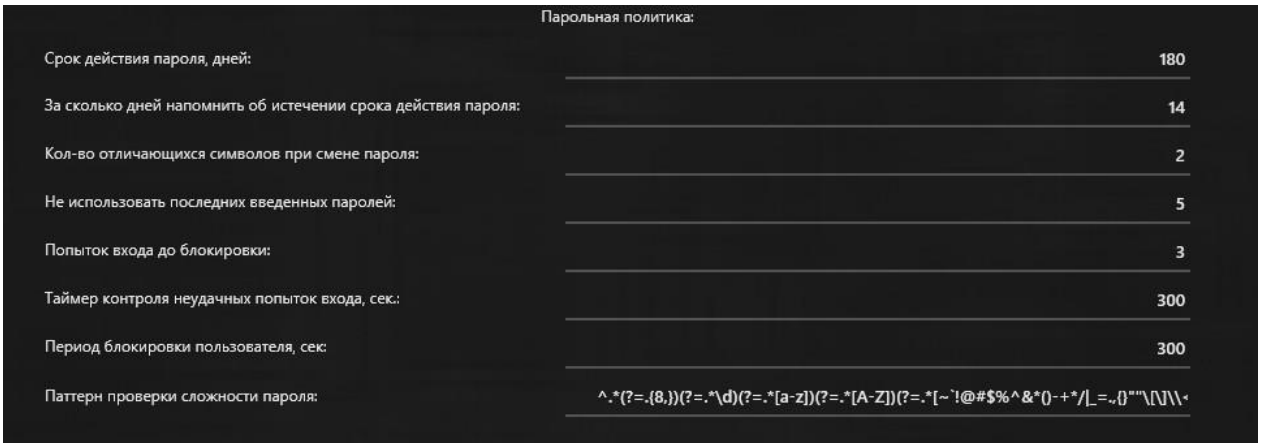

Рисунок 50. Окно настройки парольной политики

Для редактирования парольной политики необходимо нажать на кнопку «Режим редактирования»  и внести изменения в пункты парольной политики.

После завершения редактирования необходимо нажать кнопку «Сохранить»  .

Описание требований парольных политик, поддерживаемых системой, указаны в таблице ниже.

Таблица 11. Требования парольных политик

№	Наименование	Значение
1	Срок действия пароля, дней	Диапазон значений от 0-180
2	За сколько дней необходимо напомнить об истечении срока действия пароля	Диапазон значений от 0-180
3	Кол-во отличающихся символов при смене пароля	Диапазон значений от 0-50
4	Не использовать последних введённых паролей	Диапазон значений от 0-50
5	Попыток входа для блокировки	Диапазон значений от 3-10
6	Таймер контроля неудачных попыток ввода, сек	Диапазон значений от 0-900

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

7	Период блокировки пользователя, сек	Диапазон значений от 180-900
8	Паттерн проверки сложности пароля	Настраиваемое регулярное выражение

6. Подключение филиалов

Для работы с филиалами сначала требуется активировать соответствующий режим. В меню ресурсов следует перейти на вкладку Администрирование, затем открыть раздел Параметры программы и установить флажок «Использовать филиалы».

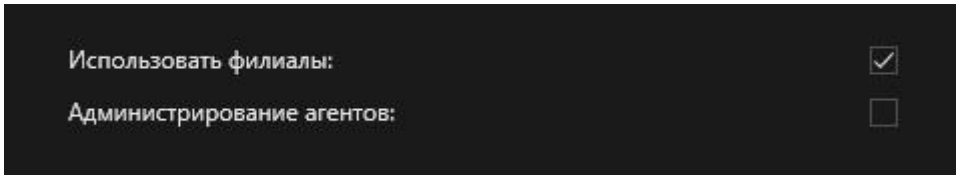

Рисунок 51. Параметры программы

После этого необходимо перейти на вкладку «Филиалы» через меню ресурсов. Для добавления нового филиала используется кнопка «Создать».

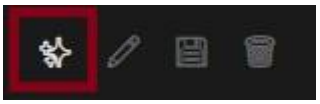

Рисунок 52. Кнопка «Создать»

В открывшемся окне требуется заполнить следующие поля:

1. Имя
2. IP-адрес
3. Порт
4. Логин
5. Пароль

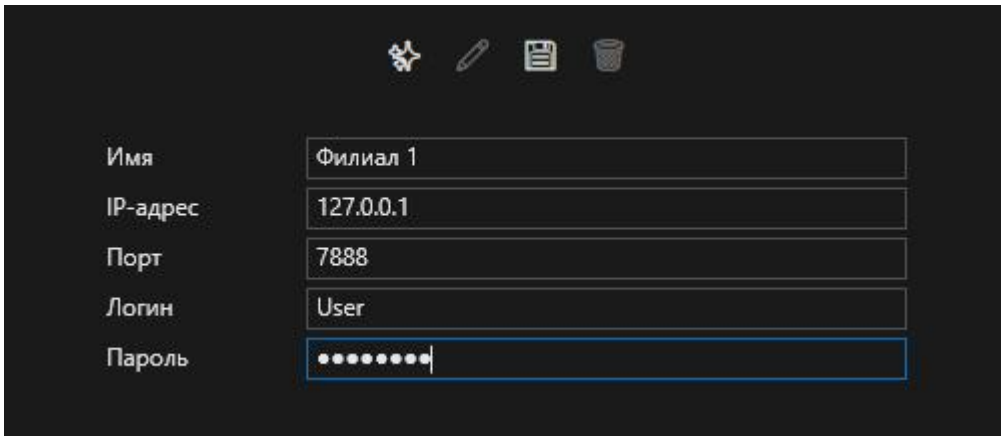

Рисунок 53. Окно параметров филиала

После ввода всех данных выполняется сохранение с помощью кнопки «Сохранить». Добавленный филиал отображается в списке слева.

Рисунок 54. Список филиалов

Переключение между филиалами осуществляется через выпадающий список, расположенный в левой верхней части приложения.

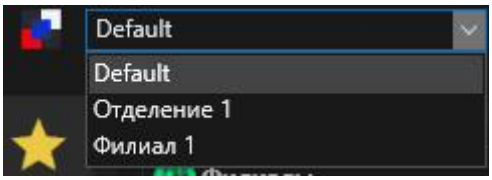

Рисунок 55. Выпадающий список филиалов

Для удаления филиала нужно выбрать его из списка на вкладке «Филиалы» и нажать кнопку «Удалить».

7. Интеграция с почтовым сервером

Для подключения к почтовому серверу используется библиотека Curl.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Настройка отправки сообщений выполняется в модуле корреляции событий. Для этого необходимо запустить inforterCE следующей командой:

```
./inforter_ce setup
```

В открывшемся меню выбираем пункт 1.

```
1 - change config
2 - test MySQL settings
3 - test Email settings
4 - save and exit
0 - exit
```

Далее выбираем пункт 2

```
1 - change MySQL settings
2 - change Email settings
0 - exit
```

После чего вводим необходимые настройки.

- `Email from`: user1@domain.ru (адрес отправителя почты)
- `Email url`: smtp://smtp.domain.ru:25 (сервер отправки почты и порт)
- `Email user`: user1 (логин почтового ящика)
- `Email password`: ********* (пароль)
- `Email encryption`: No (указываем ”SSL”, если требуется шифрование)

После настройки имеется возможность протестировать отправку сообщений. Для этого в корневом меню необходимо выбрать пункт 3

```
1 - change config
2 - test MySQL settings
3 - test Email settings
4 - save and exit
0 - exit
```

Далее при необходимости выбираем просмотр логов отправки и вводим адрес получателя сообщения.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

- `Show mail log? (Y/N)` — отображение журнала отправки сообщений
- `Enter email of recipient` — получатель тестового сообщения, например ”`root@localhost`”

После успешной проверки отобразится сообщение «`Email test is OK!`» или "`Email test failed!`" при не успешной.

Применённый настройки будут отображаться в конфигурационном файле модуля корреляции.

```
<email from="savrus@savrus.ru" url="smtp://localhost" user="" password="" encryption="" />
```

Рисунок 56. Пример конфигурационного файла

Для проверки отправки почты посредством Curl необходимо выполнить следующие действия:

1. Перейдите в рабочую директорию `cd /opt/inforter_ce`
2. Создайте файл с телом письма. Запустите редактор `nano` для создания файла `test.txt` с помощью команды: `nano test.txt`
3. Приведите файл test.txt к следующему виду:

```
From: "User Name" <user1@domain.ru>

To: <user2@domain.ru>

Subject: This is a test mail

Hello...

This is a test message sent via curl.
```

4. Сохраните файл
5. Отправьте письмо с помощью curl, выполнив следующую команду:

```
curl -k -vvv \
  --url 'smtp://smtp.domain.ru:25' \
  --mail-from 'user1@domain.ru' \
  --mail-rcpt 'user2@domain.ru' \
  --upload-file test.txt \
```

```
--user 'user1@domain.ru'
```

8. Параметры сервера

В данном разделе настраивается ограничение на максимальное количество строк в активном списке и таймаут бездействия пользователя.

Ограничение на количество строк в активном списке необходимо для балансировки нагрузки на систему.

Для редактирования параметров необходимо нажать на кнопку «Режим редактирования»  и внести необходимые изменения.

Для сохранения изменений следует нажать на кнопку «Сохранить»  .

9. Ограничение количества одновременных (параллельных) сессий пользователей

Данный функционал представляет из себя набор параметров конфигурации, позволяющий управлять поведение системы «САВРУС» в момент входа пользователя в систему.

За реализацию разных вариантов поведения системы отвечают следующие параметры конфигурации:

- «Лимит соединения пользователей с одного хоста»
- «Разрешены параллельные сессии»
- «killParallelSessionNotify»

«Лимит соединения пользователей с одного хоста»

Расположен в консоли «САВРУС» по пути: «Администрирование» - «Параметры сервера».

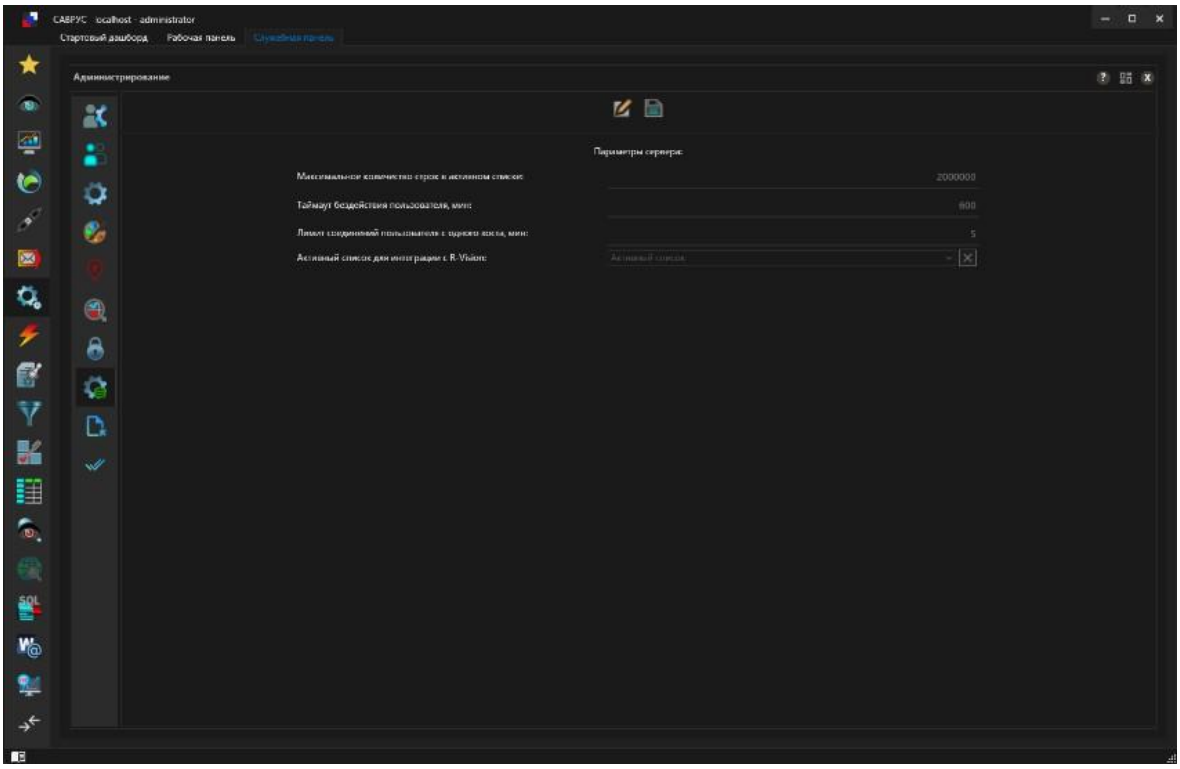

Рисунок 57. Окно модуля «Параметры сервера»

- Может принимать целые значения от 1 до 100.
- Ограничивает кол-во сессий с одинаковыми значениями параметров: UserLogin, Domain, Host или IpAddress.
- Зависит от значения параметра «Разрешены параллельные сессии», установленного для пользователя. Имеет меньший приоритет.

«Разрешены параллельные сессии»

Расположен в панели редактирования атрибутов пользователя системы по пути: «Администрирование» - «Пользователи».

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

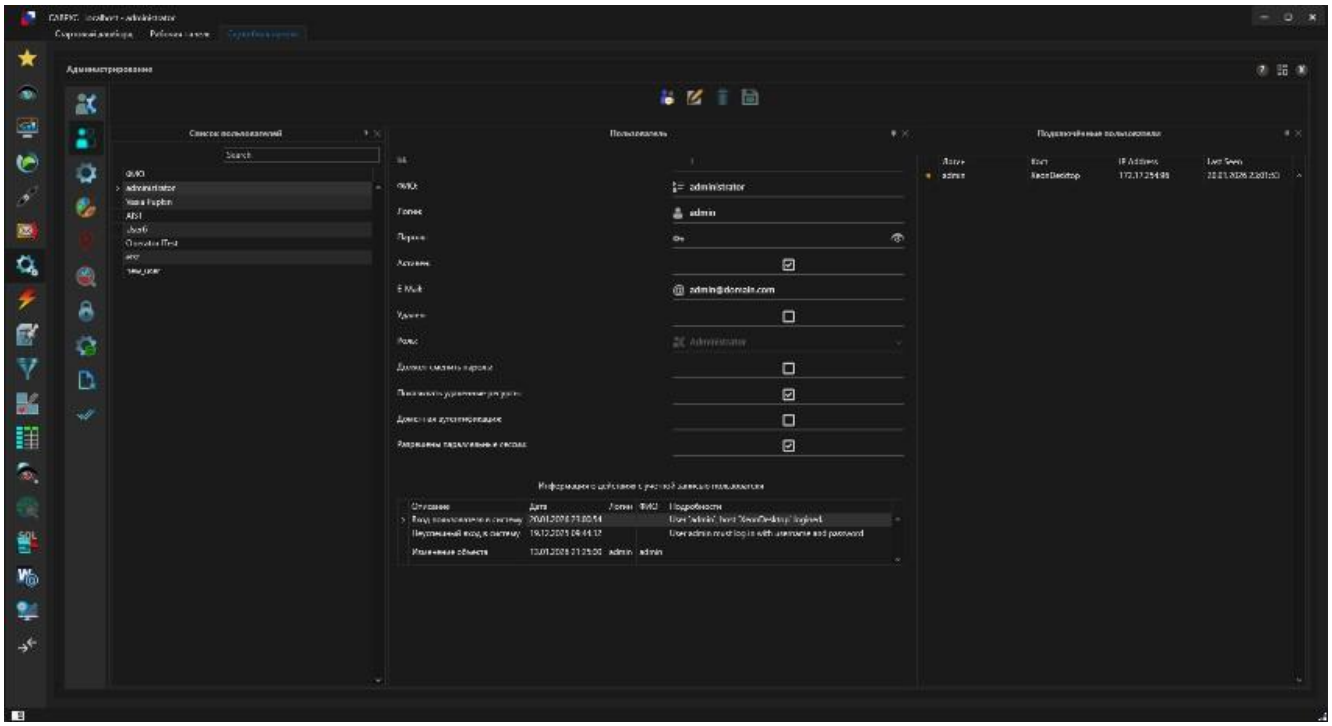

Рисунок 58. Окно модуля «Пользователи»

- Может принимать значения «вкл»/«откл»
- Значение «откл» устанавливает ограничение в размере единственной сессии пользователя с одинаковыми значениями параметров UserLogin, Domain
- Настраивается для каждого пользователя системы, имеет высший приоритет по отношению к параметру «Лимит соединений пользователя с одного хоста»

«killParallelSessionNotify»

Расположен на стороне ядра системы «САВРУС» в файле: .../config/appsettings.json в секции “Config”.

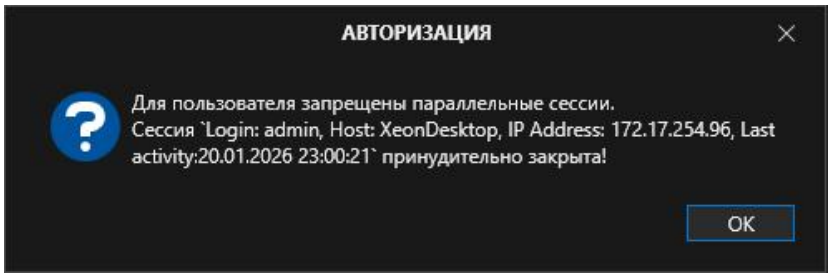

Рисунок 59. Предупреждение о завершении сессии

- Может принимать значения «0» и «1»

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

- Значение «1» устанавливает режим оповещения пользователя консоли, осуществляющего вход в систему, о том, что уже существует и будет принудительно завершена открытая сессия с идентичными указанными параметрами UserLogin, Domain. Пользователю консоли будет показано диалоговое окно с соответствующей информацией.
- При установленном в **«0»** значении параметра существующая открытая сессия будет принудительно закрыта без какого-либо оповещения.

При установленном в значение «вкл» параметре «Разрешены параллельные сессии» и превышении допустимого количества открытых сессий пользователю консоли будет показано окно, отображающее данные сессии с самым большим временем неактивности. Нажатие на кнопку «ОК» закроет эту сессию и процесс входа продолжится. Нажатие «Cancel» прервет вход в систему «САВРУС».

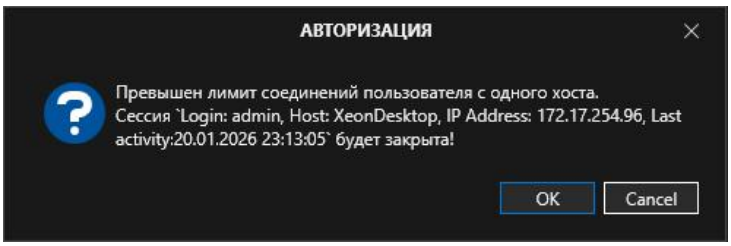

Рисунок 60. Окно подтверждения закрытия сессии

10. Список автозагрузки

В данном разделе реализован функционал создания, редактирования и сохранения списка ресурсов, которые будут автоматически открыты в режиме редактирования при старте консоли «САВРУС».

Модуль позволяет формировать персональный список ресурсов для автозагрузки с хранением списка в БД, что обеспечивает доступность списка с любых рабочих мест.

Модуль расположен в разделе «Администрирование» и доступен для пользователей с любой ролью.

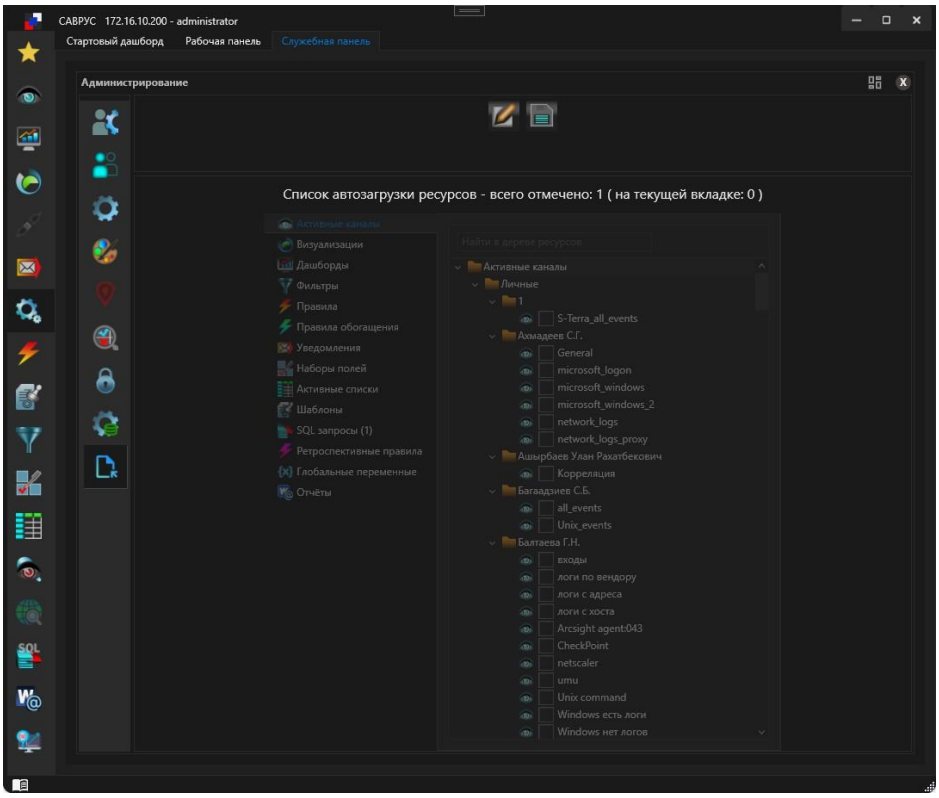

Рисунок 61. Окно «Автозагрузка» в режиме просмотра

При открытии модуля на экран консоли «САВРУС» выводится окно, содержащее список всех типов ресурсов, доступных в системе и иерархическое представление ресурсов соответствующих типов.

В окне отображается информация о выбранных ресурсах (всего и на выбранной вкладке), дополнительно, рядом с названием типа ресурса системы отображается количество выбранных ресурсов этого типа.

После нажатия на кнопку  «Режим редактирования» можно вносить изменения в список, отмечая ресурсы в дереве ресурсов выбранного типа.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

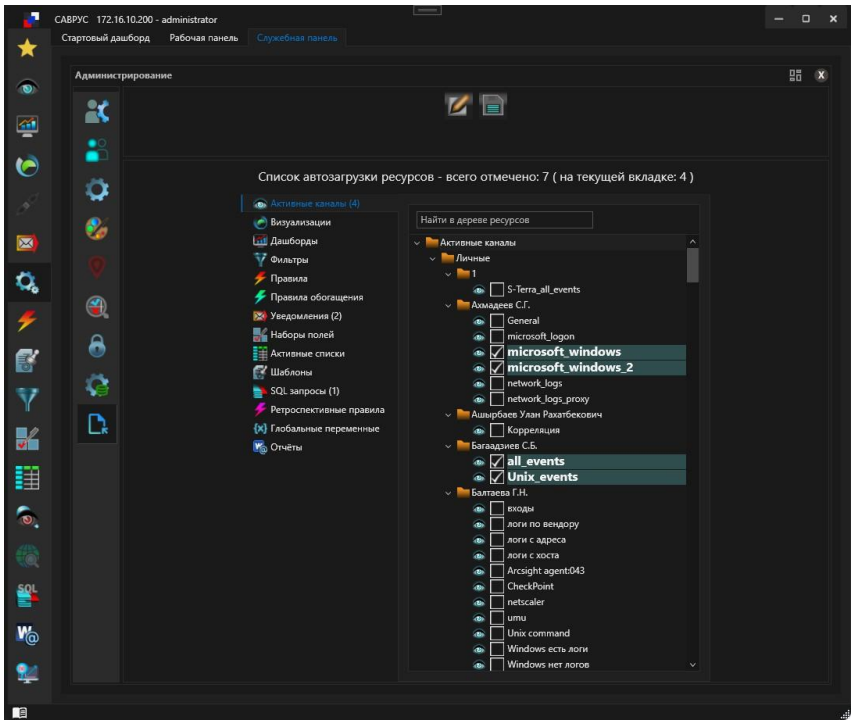

Рисунок 62. Окно «Автозагрузка» в режиме редактирования

После нажатия кнопки «Сохранить», список автозагрузки авторизированного пользователя консоли «САВРУС» будет сохранен в БД MySql в таблице `resource_user_settings`, поле `autoload`.

При следующем запуске консоли «САВРУС», выбранные ресурсы будут загружены и доступны во вкладке «Рабочая панель».

На стороне сервиса SavrusCore за обновление списка отвечает метод

```
/// <summary>
/// обновляет признак Autoload для списка ресурсов пользователя
/// </summary>
public override async Task<Protos.Status>
UpdateCustomUserAutoLoadResourceList(ResourceUserSettings request,
ServerCallContext context)
```

Значения для полей аргумента request:

- AuthToken – токен аутентификации
- UserId – ИД пользователя, для которого создается список
- Filter – список ИД ресурсов с разделителем `|`
- Autoload – состояние признака, устанавливаемое для всех ресурсов с ИД из списка, переданного в поле Filter

Метод вызывается дважды – для установки и сброса признака с соответствующим списком ИД ресурсов.

11. Проверка ресурсов

Данный инструмент предназначен для автоматической валидации ресурсов системы.

Модуль расположен в разделе «Администрирование» - «Проверка ресурсов».

Рабочая панель инструмента «Проверка ресурсов» выглядит следующим образом.

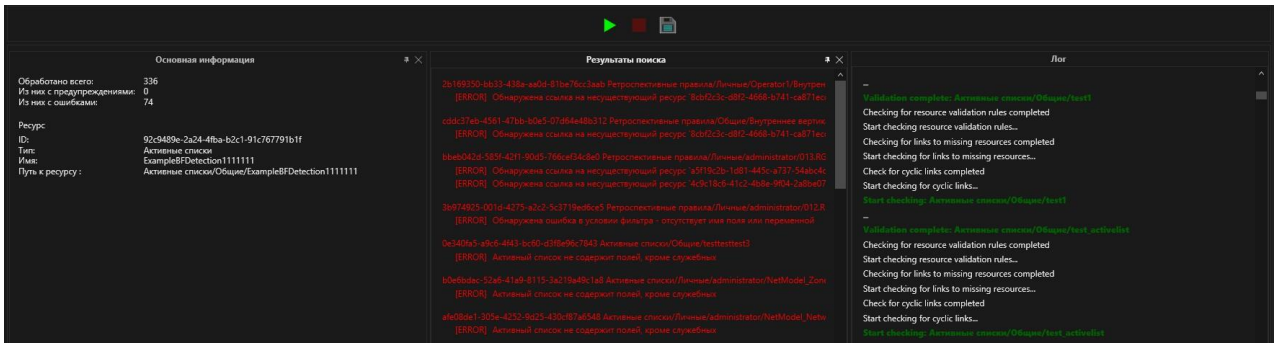

Рисунок 63. Рабочая панель модуля «Проверка ресурсов»

В верхней части находится панель управления, которая содержит 3 активных кнопки:

- Запустить – запускает проверку всех ресурсов системы.
- Остановить – останавливает проверку ресурсов.
- Сохранить как… – сохраняет файл логов содержащий информацию из окна «Результаты поиска».

Окно «Основная информация», находящееся в левой части рабочей панели содержит информацию о количестве проверенных ресурсов, найденных ресурсов с предупреждениями и ошибками, а так же информацию о проверенном ресурсе.

Центральное окно «Результаты поиска» содержит информацию о всех ресурсах, содержащих предупреждения или ошибки обнаруженные при прохождении проверки.

В окне «Лог», в правой части рабочей панели отображается подробная информация о процессе проверки каждого ресурса.

Так же реализована возможность запустить точечную проверку необходимого ресурса. Для этого необходимо нажать «ПКМ» в дереве ресурсов по выбранному ресурсу, далее в выпадающем меню выбрать пункт «Проверка ресурса».

Проверка ресурсов происходит в 3 этапа.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

1. Проверка ресурса на зацикливание. Проверяется наличие в ресурсе ссылок на самого себя или наличие другого ресурса, содержащего циклические ссылки.
2. Проверка связей. Проверяется, что ресурс не ссылается на удаленные или перемещённые объекты.
3. Проверка правил валидации. Данная проверка осуществляется на основе наборов правил валидаторов подготовленных для каждого типа ресурсов. По мимо ручной проверки, данный этап проверка автоматически запускается при сохранении любого ресурса.

12. Восстановление бэкапа базы данных событий

Для начала восстановления данных из бэкапа БД Событий необходимо поместить файлы бэкапа в доступную директорию. Далее необходимо запустить файл `cl-restore.sh`, который по умолчанию находится в папке `/opt/backup/`. Затем выполнить команду вида:

```
./cl-restore.sh -t "Название таблицы" -l "Директория с бэкапами/"
```

В названии таблицы указывается таблица базы данных Событий, в которую будут восстановлены данные. В директории с бэкапами указывается директория, в которой будет производиться поиск бэкапов для восстановления. Важно, чтобы название директории обязательно заканчивалось на «/».

Рисунок 64. Пример команды

После выполнения команды появляется список доступных для восстановления бэкапов и меню действий:

- 0 – восстановление всех бэкапов;
- 1-9 – восстановление конкретного бэкапа;
- 10 – отмена восстановления.

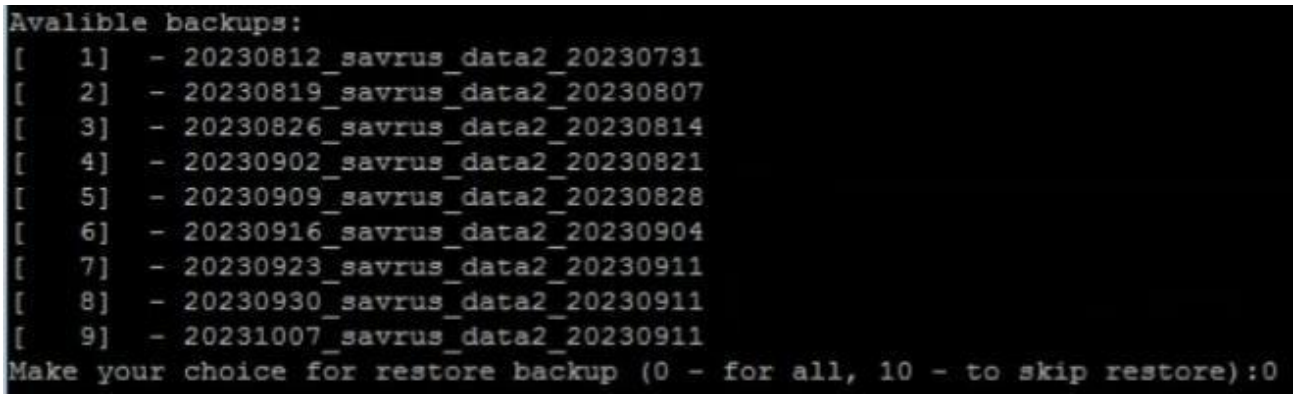

Рисунок 65. Выбор бэкапа для восстановления

В случае, если во время восстановления будет обнаружена ранее восстановленная партиция, появится оповещение, которое будет предупреждать о дублировании партиций. В случае появления данной проблемы предусмотрены следующие варианты:

- Skip – произойдёт пропуск партиции с сохранением прошлой версии партиции в таблице;
- Continue – произойдёт дублирование партиции в таблице;
- Detach partition – произойдёт удаление старой партиции из таблицы и загрузка новой.

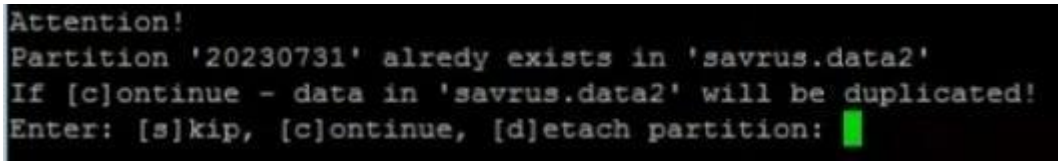

Рисунок 66. Дублирование бэкапов

В случае ошибок выполнение команды приостанавливается с выводом кода ошибки.

Рисунок 67. Пример ошибки

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Приложение 1. Описание таблиц MariaDB

1.1. SAV_ALC_CustomZones

Хранимые данные: служащее для хранения данных о геолокации.

Структура таблицы представлена ниже.

Таблица 12. SAV_ALC_CustomZones

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	subnet	varchar(512)	Подсеть	
3.	zonename	varchar(512)	Имя зоны	
4.	country	varchar(512)	Страна	
5.	region	varchar(512)	Регион	
6.	city	varchar(512)	Город	
7.	description	varchar(512)	Описание	
8.	creationTime	bigint(20)	Время создания	
9.	lastModifiedTime	bigint(20)	Время последнего изменения файла.	
10.	count	int(11)	Количество	
11.	hashCode	bigint(20)	Хэш код	

1.2. SAV_ALC_NetModel_Asset

Хранимые данные: служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 13. SAV_ALC_NetModel_Asset

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	IPAddress	varchar(512)	IP адрес	
3.	Customer	varchar(512)	Клиент	
4.	Asset	varchar(512)	Выделенные сервера	
5.	Description	varchar(512)	Описание	
6.	creationTime	bigint(20)	Время создания	
7.	lastModifiedTime	bigint(20)	Время последнего изменения файла.	
8.	count	int(11)	Количество	

9.	hashCode	bigint(20)	Хэш код	

1.3. SAV_ALC_NetModel_Network

Хранимые данные: служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 14. SAV_ALC_NetModel_ Network

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	Subnet	varchar(512)	Подсеть	
3.	Customer	varchar(512)	Клиент	
4.	Network	varchar(512)	Сеть	
5.	Country	varchar(512)	Страна	
6.	Region	varchar(512)	Регион	
7.	City	varchar(512)	Город	
8.	Description	varchar(512)	Описание	
9.	creationTime	bigint(20)	Время создания	
10.	lastModifiedTime	bigint(20)	Время последнего изменения файла.	
11.	count	int(11)	Количество	
12.	hashCode	bigint(20)	Хэш код	

1.4. SAV_ALC_NetModel_Zone

Хранимые данные: служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 15. SAV_ALC_NetModel_Zone

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	Subnet	varchar(512)	Подсеть	
3.	Customer	varchar(512)	Клиент	
4.	Zone	varchar(512)	Зона	
5.	Description	varchar(512)	Описание	
6.	creationTime	bigint(20)	Время создания	
7.	lastModifiedTime	bigint(20)	Время последнего изменения файла.	

8.	count	int(11)	Количество	
9.	hashCode	bigint(20)	Хэш код	

1.5. SAV_ALC_RVision_Incidents

Хранимые данные: служащее для для интеграции с RVision.

Ниже представлено описание полей таблицы.

Таблица 16. SAV_ALC_RVision_Incidents.

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	seid	bigint(20)	Уникальный идентификатор события	
3.	status	int(11)	Статус	
4.	status_desc	text	Описание	
5.	logging	text	Время логирования	
6.	eventId	text	Уникальный идентификатор, который присваивает значение каждому событию.	
7.	startTime	bigint(20)	Время, когда началось действие, на которое ссылается событие	
8.	endTime	bigint(20)	Время, когда закончилось действие, на которое ссылается событие	
9.	externalId	text	Идентификатор, используемый исходным устройством.	
10.	severity	int(11)	Уровень критичности	
11.	name	text	Название события	
12.	message	text	Произвольное сообщение, содержащее более подробную информацию о событии.	
13.	sourceUserName	text	Идентифицирует исходного пользователя по имени.	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

14.	sourceUserId	text	Идентифицирует исходного пользователя по идентификатору.	
15.	sourceUserPrivileges	text	Определяет привилегии исходного пользователя.	
16.	sourceNtDomain	text	Доменное имя Windows для исходного адреса.	
17.	sourceAddress	varchar(40)	Определяет источник, на который ссылается событие в IP-сети.	
18.	sourceHostName	text	Определяет источник, на который ссылается событие в IP-сети.	
19.	sourceMacAddress	text	Шесть шестнадцатеричных чисел, разделенных двоеточием.	
20.	sourcePort	int(11)	Порт источника события.	
21.	sourceZoneUri	text	URI для зоны, которой был назначен исходный ресурс	
22.	sourceServiceName	text	Служба, которая отвечает за генерацию этого события.	
23.	destinationUserName	text	Идентифицирует конечного пользователя по имени.	
24.	destinationUserId	text	Идентифицирует конечного пользователя по ID.	
25.	destinationUserPrivileges	text	Представляет привилегии конечного пользователя.	
26.	destinationNtDomain	text	Доменное имя Windows для адреса назначения.	
27.	destinationAddress	varchar(40)	Определяет адрес назначения, на который ссылается событие в IP - сети. Формат представляет собой IPv4 -адрес.	
28.	destinationHostName	text	Определяет пункт назначения, к которому относится событие в IP-сети.	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

29.	destinationMacAddress	text	Шесть шестнадцатеричных чисел, разделенных двоеточием.	
30.	destinationPort	int(11)	Номер порта	
31.	destinationZoneUri	text	URI для зоны, в которой был назначен целевой ресурс	
32.	destinationServiceName	text	Сервис, на который направлено данное событие. Пример: "sshd"	
33.	destinationProcessName	text	Имя процесса назначения события.	
34.	deviceProcessName	text	Имя процесса, связанного с событием.	
35.	fileId	text	Идентификатором, связанным с файлом	
36.	fileHash	text	Хэш файла.	
37.	fileName	text	Имя файла.	
38.	filePath	text	Полный путь к файлу, включая само имя файла.	
39.	oldFileId	text	Полный путь к старому файлу, включая само имя файла.	
40.	oldFileHash	text	Хэш старого файла.	
41.	requestUrlHost	text	Получение текущего имени домена	
42.	flexDate1	text	Пользовательское поле временной метки	
43.	reason	text	Причина, по которой было сгенерировано событие аудита.	
44.	deviceCustomDate1	bigint(20)	Пользовательское временное поле	
45.	deviceCustomDate2	bigint(20)	Пользовательское временное поле	
46.	deviceCustomString1	text	Пользовательское строковое поле	
47.	deviceCustomString2	text	Пользовательское строковое поле	
48.	deviceCustomString3	text	Пользовательское строковое поле	
49.	deviceCustomString4	text	Пользовательское строковое поле	
50.	deviceCustomString5	text	Пользовательское строковое поле	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

51.	deviceCustomString6	text	Пользовательское строковое поле	
52.	deviceDomain	text	Полное доменное имя	
53.	devicePayloadId	text	Уникальный идентификатор для полезной нагрузки, связанной с событием.	
54.	creationTime	bigint(20)	Время создания	
55.	lastModifiedTime	bigint(20)	Время последнего изменения файла.	
56.	count	int(11)	Количество	
57.	hashCode	bigint(20)	Хэш код	

1.6. Actualresources

Хранимые данные: Данная таблица служит для хранение созданных в системе САВРУС ресурсов.

Ниже представлено описание полей таблицы.

Таблица 17. actualresources

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор	
2.	parentId	int(11)	Идентификатор родительского ресурса	
3.	type	int(11)	Тип	
4.	name	varchar(512)	Имя ресурса	
5.	def	mediumtext	XML файл, описывающий структуру и состав ресурса	
6.	subType	int(11)	Подтип	
7.	isSystem	tinyint(1)	Системный	
8.	shared	tinyint(1)	Общий	
9.	personal	tinyint(1)	Персональный	
10.	deleted	tinyint(1)	Ресурс помечен на удаление	
11.	userId	int(11)	Уникальный идентификатор пользователя	
12.	resourceId	varchar(50)	Уникальный идентификатор ресурса	
13.	Disabled	tinyint(1)	Выключенный	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

14.	DateCreation	datetime	Дата создания	
15.	DateChanged	datetime	Дата последнего изменения	
16.	status	varchar(512)	Статус	
17.	uri	text	Идентификатор ресурса	

1.7. config_properties

Хранимые данные: хранит параметры парольной политики.

Ниже представлено описание полей таблицы.

Таблица 18. config_properties

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор записи	
2.	pwd_sym_to_change	int(11)	кол-во символов, на которое новый пароль пользователя должен отличаться от старого при смене пароля пользователем	
3.	pwd_exp_days	int(11)	срок действия пароля пользователя в днях	
4.	pwd_ban_last_used	int(11)	кол-во последних введенных паролей, запрещенных к использованию при смене пароля пользователем	
5.	max_auth_attempts	int(11)	максимальное кол-во попыток входа в систему, после которого блокируется учетная запись пользователя	
6.	auth_attempts_timer	int(11)	время фиксации последовательных неудачных попыток входа пользователя в систему, в секундах	
7.	user_ban_timer	int(11)	время, на которое блокируется учетная запись пользователя после превышения максимального	

			количества неудачных попыток входа, в секундах	
8.	pwd_pattern	varchar(300)	REGEXP-выражение, описывающее минимально допустимый набор символов и минимальную длину пароля пользователя при создании нового пользователя или смене пароля пользователем	
9.	pwd_exp_days_remind	int(11)	за сколько дней необходимо начать напоминать пользователю об истечении пароля	

1.8. report_scheduler

Хранимые данные: Отвечает за график формирования отчетов.

Ниже представлено описание полей таблицы.

Таблица 19. report_scheduler

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор	
2.	res_id	int(11)	ИД ресурса (отчета)	
3.	recipient_id	int(11)	ИД получателя	
4.	path	varchar(255)	Путь к файлу отчета	
5.	next_date	datetime	Дата и время формирования и отправки следующего отчёта	
6.	formed	tinyint(1)	Флаг, указывающий, сформирован ли отчёт	
7.	template_id	int(11)	ИД шаблона с текстом и темой письма	

1.9. resource_history

Хранимые данные: История изменений ресурса.

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

Ниже представлено описание полей таблицы.

Таблица 20. resource_history

№	Имя поля	Формат поля	Описание	Примечание
1.	id	begint(20)	Уникальный идентификатор	
2.	res_id	int(20)	ИД ресурса	
3.	user_id	int(20)	ИД пользователя	
4.	olddef	mediumtext	Предыдущее значение изменяемого поля	
5.	nwedef	mediumtext	Новое значение изменённого поля	
6.	datechanged	datetime	Дата и время внесения изменения	
7.	host_address	varchar(40)	ИД хоста с которого были внесены изменения	

1.10. resource_user_layout

Хранимые данные: Шаблон настроек для группы ресурсов.

Ниже представлено описание полей таблицы.

Таблица 21. resource_user_layout

№	Имя поля	Формат поля	Описание	Примечание
1.	id	begint(20)	Уникальный идентификатор	
2.	user_id	int(11)	ИД пользователя	
3.	resource_type	int(11)	Тип ресурса	
4.	name	varchar(512)	Название шаблона	
5.	select_order	mediumtext	Список полей необходимых для взятия из БД	
6.	sort_order	mediumtext	Правила сортировки	
7.	filter_order	mediumtext	Условия фильтрации	
8.	layout	mediumtext	Конфигурация отображения шаблона	
9.	columns_order	mediumtext	Порядок и видимость колонок в таблице	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

10.	is_default	tinyint(1)	Шаблон по умолчанию	

1.11. resource_user_settings

Хранимые данные: Шаблон настроек ресурса для каждого пользователя.

Ниже представлено описание полей таблицы.

Таблица 22. resource_user_settings

№	Имя поля	Формат поля	Описание	Примечание
1.	user_id	int(11)	ИД пользователя	
2.	resource_id	int(11)	ИД ресурса	
3.	favorite	tinyint(1)	Флаг, отмечающий, добавлен ли ресурс в избранное	
4.	select_order	mediumtext	Список полей необходимых для взятия из БД	
5.	sort_order	mediumtext	Правила сортировки	
6.	filter_order	mediumtext	Условия фильтрации	
7.	layout	mediumtext	Конфигурация отображения шаблона	
8.	columns_order	mediumtext	Порядок и видимость колонок в таблице	
9.	autoload	tinyint(1)	Флаг , определяет, должны ли ресурс открываться автоматически при старте консоли	

1.12. core_properties

Хранимые данные: используется для хранения служебных данных, характерных для всех пользователей сервиса.

Ниже представлено описание полей таблицы.

Таблица 23. core_properties

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор записи	
2.	al_rows_limit_default	int(11)	Лимит количества записей активного списка	
3.	user_inactivity_timeout	int(11)	Таймаут бездействия пользователя в сессии	
4.	rvision_al_id	varchar(50)	Идентификатор записи журнала изменений	

1.13. roles

Хранимые данные: Данная таблица служит хранения данных о существующих в системе САВРУС ролях пользователей.

Ниже представлено описание полей таблицы.

Таблица 24. roles

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор	
2.	Name	varchar(128)	Имя роли	
3.	parent_id	int(11)	Ссылка на родителя	
4.	roleFilter	varchar(50)	Идентификатор фильтра, прикрепленного к роли	
5.	rolePermission	int(11)	Дополнительные привилегии роли	

1.14. roles_resources

Хранимые данные: служащее для описания прав роли пользователя на выполнение действий над определенным типом ресурсов.

Ниже представлено описание полей таблицы.

Таблица 25. roles_resources

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

№	Имя поля	Формат поля	Описание	Примечание
1.	role_id	int(11)	Уникальный идентификатор роли	Роль пользователя
2.	res_id	int(11)	ИД ресурса	Ресурса, на который определяются права (папка в дереве ресурсов)
3.	CREATE	tinyint(1)	Создан	Право роли выполнять команду «Создать»
4.	OPEN	tinyint(1)	Открыт	Право роли выполнять команду «Открыть»
5.	SAVE	tinyint(1)	Сохранён	Право роли выполнять команду «Сохранить»
6.	DEL	tinyint(1)	Удален	Право роли выполнять команду «Удалить»

1.15. trigger_unlock

Хранимые данные: Служебная таблица для отключения изменений в первых 500 строках таблицы Actualresources.

Ниже представлено описание полей таблицы.

Таблица 26. Trigger_unlock

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(10) unsigned	Уникальный идентификатор	
2.	allow_ar_update	tinyint(1)	Флаг, разрешающий или запрещающий обновление записей	
3.	allow_ar_delete	tinyint(1)	Флаг, разрешающий или запрещающий удаление записей	

1.16. user_auth_attempts

Хранимые данные: используется для хранения данных о неудачных попытках входа пользователя в систему.

Ниже представлено описание полей таблицы.

Таблица 27. user_auth_attempts

№	Имя поля	Формат поля	Описание	Примечание
1.	user_id	int(11)	Уникальный идентификатор пользователя	
2.	attempts_count	int(11)	Количество неудачных попыток входа за контролируемый промежуток времени	
3.	attempts_start	timestamp	Время первой неудачной попытки	
4.	banned_until	timestamp	Время окончания блокировки входа по количеству неудачных попыток входа	

1.17. user_history

Хранимые данные: История действий с учетной записью пользователя

Ниже представлено описание полей таблицы.

Таблица 28. user_history

№	Имя поля	Формат поля	Описание	Примечание
1.	id	bigint(20)	Уникальный идентификатор	
2.	user_id	int(11)	ИД пользователя	
3.	event_time	datetime	Дата и время события	
4.	login	varchar(45)	Логин пользователя	
5.	fio	varchar(45)	ФИО	
6.	event_type	int(11)	Тип события	
7.	message	longtext	Подробное описание события	

1.18. users

Хранимые данные: служащее для описания пользователей.

Ниже представлено описание полей таблицы.

Таблица 29. users

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор	
2.	FIO	varchar(45)	Фамилия имя отчество	
3.	UserLogin	varchar(45)	Логин пользователя	

Общество с ограниченной ответственностью
«Актуальные Технологии Безопасности»
107113, г. Москва, ул. Лобачика, д. 17, эт. 8, каб.7
ИНН 7733742415, КПП 771801001
ОКПО 67955435, ОГРН 1107746637228
тел: +7 499 648 7548
https://ast-security.ru/

4.	Active	tinyint(1)	Является ли пользователь активным	
5.	EMail	varchar(255)	Электронная почта пользователя	
6.	Deleted	tinyint(1)	Является ли пользователь удалённым	
7.	Pwd	varchar(300)	Хэш пароля пользователя	
8.	userRole	int(11)	Роль пользователя	
9.	needChangePass	tinyint(1)	Признак необходимости смены пароля пользователем	
10.	showDeletedResources	tinyint(1)	Показывать ли пользователю удалённые ресурсы	
11.	adAuth	tinyint(1)	Пользователь использует доменную аутентификацию	
12.	userFilter	varchar(50)	Фильтр пользователя	Сейчас не используется

1.19. usersPasswords

Хранимые данные: служащее для хранения хэш значения введенных ранее паролей. Используется для реализации требования парольной политики не допускать использование последних N введенных паролей.

Ниже представлено описание полей таблицы.

Таблица 30. userPasswords

№	Имя поля	Формат поля	Описание	Примечание
1.	id	int(11)	Уникальный идентификатор пароля	
2.	userId	int(11)	Уникальный идентификатор пользователя	
3.	pwd	varchar(300)	Хэш пароля	
4.	dateCreation	timestamp	Дата создания	
5.	dateExpiration	timestamp	Дата истечения пароля	
6.	active	int(11)	Пароль активен	Текущий используемый хэш пароля