РГДП.58.29.14.000-001-04 РП

Информационная безопасность

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Редакция 2
Соответствует версии Astra.Security 1.4.14.1
Соответствует версии Astra.HMI.SecurityConfigurator 2.2.2.1
Соответствует версии Astra.HMI.Security 2.0.7.1
Соответствует версии Astra.HMI.IntegrityControl 2.1.1.1

СПИСОК ИЗМЕНЕНИЙ

Редакция	Список изменений
Редакция 2	- Добавлен раздел Настройка защищенного соединения с LDAP-сервером. - Добавлен раздел Блокировка сочетаний клавиш. - Добавлен раздел Запуск сервисов (для ОС Linux). - Добавлен раздел Доступ из проекта HMI к правам Astra.HMI.SecurityConfigurator. - Добавлен раздел Шаблоны прав приложений.

ОГЛАВЛЕНИЕ

1. Информационная безопасность

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.
В условиях цифровизации экономики и увеличения количества целевых атак на промышленные предприятия тема кибербезопасности АСУ ТП требует повышенного внимания.

Основные угрозы безопасности информации АСУ ТП:

1. Несанкционированный доступ к данным (искажение данных).
2. Перехват управления (навязывание команд, выведение из строя устройств).
3. Подмена устройств (передача некорректных данных, нарушение стабильной работы сети устройств).
4. Перепрошивка устройств (воздействие на объект управления).

1.1. Общие сведения

1.1.1. Требования к информационной безопасности в АСУ ТП

Требования к обеспечению безопасности автоматизированных систем управления технологическими процессами приведены в Федеральном законе от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской федерации».

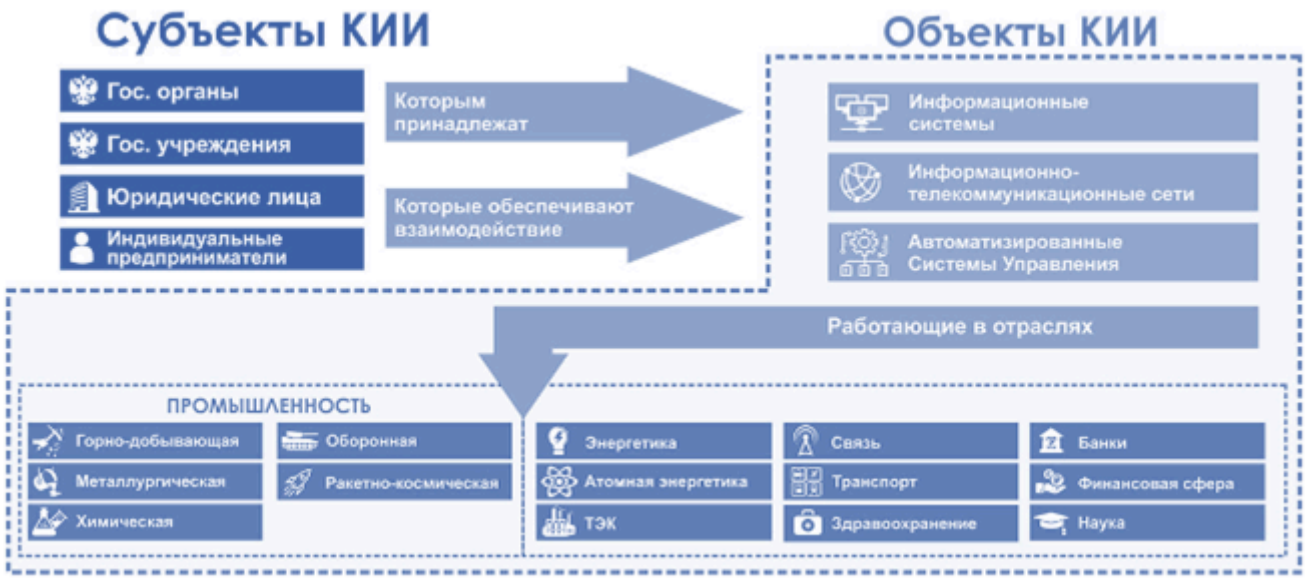
Основные требования ИБ для АСУ ТП:

- Идентификация и аутентификация, управление доступом.
- Аудит безопасности.
- Контроль целостности.
- Наложенные средства безопасности.

В соответствии с Указом Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

К объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере:

- здравоохранения;
- науки;
- транспорта;
- связи;
- энергетики;
- банковской и иных сферах финансового рынка;
- топливно-энергетического комплекса;
- атомной энергии;
- оборонной и ракетно-космической промышленности;
- горнодобывающей, металлургической и химической промышленности.



Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры.

ПК AstraRegul включен в реестр российского ПО.

1.1.2. Общие рекомендации

Чтобы избежать сбоев в работе компонентов ПТК AstraRegul и снизить вероятность возникновения уязвимостей проекта автоматизации технологического процесса, следуйте рекомендациям по безопасному администрированию:

- Ограничивайте доступ к техническим средствам.
- Используйте IPSec.
- Ограничивайте число портов, используемых DCOM.
- Используйте антивирусное ПО и обновляйте антивирусные базы.
- Отключайте автоматическое обновление ПО.
- Блокируйте доступ к информации на внешнем накопителе.
- Ограничивайте права и количество учетных записей пользователей.
- Ограничивайте права доступа к системным папкам.
- Используйте системы контроля версий.
- Используйте пароли для доступа к Astra.Server и Astra.AccessPoint.

Несоблюдение рекомендаций может повлечь:

- потерю технологических данных;
- подачу ложных команд управления технологическому оборудованию;
- возникновение аварийных ситуаций;
- несвоевременное оповещение о наступивших событиях и авариях;
- потерю контроля над ходом технологического процесса;
- остановку технологического оборудования;
- нарушение безопасности производства;
- действие вредоносных программ.

Ограничение доступа к техническим средствам

Чтобы предотвратить несанкционированный доступ посторонних лиц и негативное воздействие окружающей среды (пыль, влага), рекомендуем размещать технические средства (серверы, АРМ, сетевое оборудование) в серверных шкафах.

Несоблюдение данной рекомендации может привести к прекращению или сбоям в работе компонентов ПТК в результате:

- отключения оборудования;
- отсоединения кабелей;
- порчи или кражи оборудования;
- прочих физических воздействий, приводящих к отключению или поломке технических средств.

Использование IPSec

Чтобы предотвратить несанкционированный доступ к сети и перехват пакетов данных, передаваемых по межсетевому протоколу IP, рекомендуем использовать IPSec в туннельном режиме для организации безопасного сетевого взаимодействия между удаленными компонентами ПК AstraRegul.

Несоблюдение данной рекомендации несет угрозу перехвата, просмотра, изменения и прочих нежелательных действий с пакетами данных, передаваемыми между удаленными компонентами ПК AstraRegul.

Ограничение числа портов DCOM

Чтобы предотвратить несанкционированный доступ и повысить безопасность сетевого взаимодействия между удаленными компонентами ПК AstraRegul, рекомендуем ограничивать число портов, используемых DCOM, до определенного диапазона. Затем рекомендуем настраивать межсетевой экран (брандмауэр):

запретить входящий трафик на узел OPC;

разрешить входящий трафик определенных узлов OPC через порт TCP 135;

разрешить входящий трафик определенных узлов OPC через некоторый диапазон портов TCP.

Несоблюдение данной рекомендации несет угрозу несанкционированного подключения к сети, сетевых атак, проникновения вредоносных программ и других сетевых угроз, способных вызвать серьезные сбои в работе компонентов ПК AstraRegul.

Антивирусное ПО

Чтобы избежать заражения серверов и АРМ компьютерными вирусами, рекомендуем использовать антивирусное ПО и регулярно обновлять антивирусные базы.

Несоблюдение данной рекомендации может привести к серьёзным сбоям в работе компьютеров при заражении вирусами, например:

- внезапная перезагрузка или невозможность включения;
- вывод на экран посторонних сообщений;
- блокировка компьютера;
- замедление работы;
- удаление или изменение файлов приложений;
- форматирование жесткого диска;
- другие непредсказуемые ситуации.

Сбои в работе компьютеров приводят к замедлению, сбоям и прекращению работы компонентов ПК AstraRegul.

Отключение автоматического обновления ПО

Чтобы избежать сбоев в работе серверов и АРМ, рекомендуем отключать автоматическое обновление ОС и антивирусного ПО.

Обновлять ОС, антивирусное ПО, компоненты ПК AstraRegul и ППО проекта автоматизации рекомендуем во время плановых работ по техническому обслуживанию и ремонту.

Несоблюдение данной рекомендации повышает вероятность сбоя в работе компонентов ПК AstraRegul.

Ограничение доступа к информации на внешнем накопителе

Чтобы предотвратить несанкционированное использование внешних накопителей, рекомендуем блокировать порты USB и приводы оптических дисков для учетных записей пользователей.

Подключив к системному блоку внешний накопитель, пользователь не увидит его в папке Мой компьютер или доступ к нему будет запрещён.

Несоблюдение данной рекомендации может привести к заражению компьютеров вредоносными программами, содержащимися на накопителях, а также утечке конфиденциальной информации предприятия.

Ограничение прав и количество учетных записей пользователей

Чтобы предотвратить несанкционированный доступ к ПО серверов и АРМ, рекомендуем включать только учетные записи пользователей, предусмотренные проектом автоматизации.

Для каждой учетной записи:
- устанавливайте сложные пароли;
- ограничивайте права пользователя в использовании ПО рамками должностных обязанностей.

Несоблюдение данной рекомендации несет угрозу несанкционированного доступа к ПО пользователей, не обладающих необходимыми знаниями, что может привести к ошибкам в работе с ПО, компонентами ПК AstraRegul и управлении технологическим процессом.

Ограничение доступа к системным папкам

Чтобы предотвратить несанкционированный доступ к файлам ОС и компонентов ПК AstraRegul, рекомендуем ограничивать права доступа к системным папкам.

Не рекомендуем изменять права доступа к каталогам, в которые устанавливаются компоненты ПК AstraRegul.

Дистрибутивы компонентов ПК AstraRegul не изменяют стандартные права доступа к системным каталогам.

Несоблюдение данной рекомендации несет угрозу подмены компонентов ПК AstraRegul вредоносными программами, что может привести к серьёзным сбоям в работе проекта автоматизации и всего технологического процесса.

Рекомендации, применимые для компонентов ПК AstraRegul.

Системы контроля версий

Чтобы избежать утраты исходных файлов ПО проекта автоматизации, рекомендуем использовать системы контроля версий для хранения и контроля версионности исходных файлов проекта автоматизации.

Несоблюдение данной рекомендации повышает риск использования устаревших версий исходных файлов проекта автоматизации для доработок и корректировок.

Пароли для доступа к Astra.Server и Astra.AccessPoint

Чтобы предотвратить несанкционированный доступ из сервисных приложений Конфигуратор, Статистика и Управляющий, настоятельно рекомендуем использовать пароли для доступа к Astra.Server и Astra.AccessPoint.

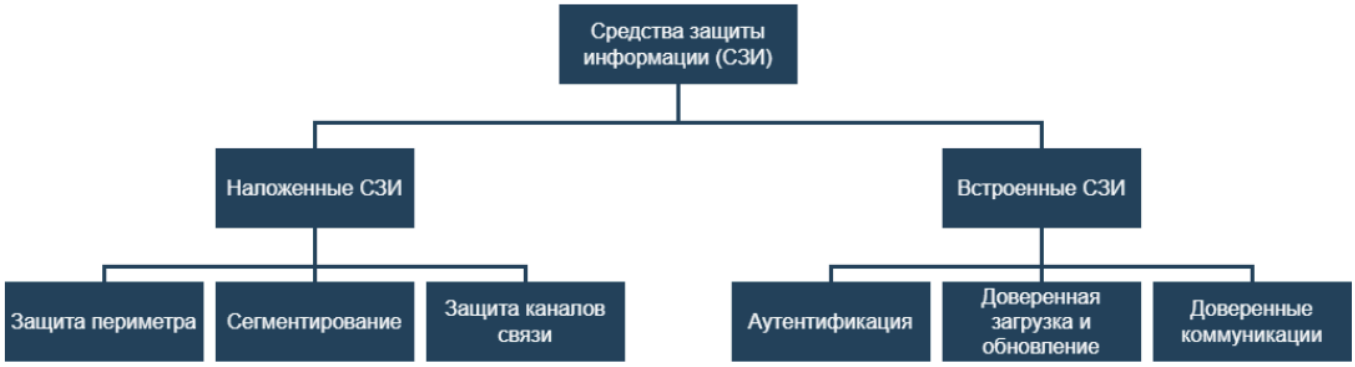
Несоблюдение данной рекомендации несет угрозу несанкционированных действий:

- изменение конфигураций;
- просмотр статистики;
- управление сервером или резервной парой серверов;
- несанкционированный обмен данными.

Несанкционированный доступ и действия могут стать причиной серьёзных сбоев в работе компонентов ПТК, проекта автоматизации и всего технологического процесса.

1.1.3. Средства защиты информации

Средства защиты информации (СЗИ) – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.



1.1.3.1. Наложенные СЗИ

Подсистема межсетевого экранирования на периметре АСУТП

CheckPoint	https://checkpoint.com
UserGate	https://usergate.com
Eltex	https://eltex-co.ru
НПО «Эшелон»	https://npo-echelon.ru

Средства обнаружения вторжений (СОВ)

Эти СЗИ мониторят и анализируют множество данных в корпоративной сети, чтобы вовремя обнаружить факт несанкционированного доступа.

CheckPoint	https://checkpoint.com
UserGate	https://usergate.com
АО «РНТ»	https://www.rnt.ru/ru
НПО «Эшелон»	https://npo-echelon.ru
S-Terra	https://www.s-terra.ru
ViPNet IDS	https://infotecs.ru/product/setevye-komponenty/vipnet-ids/
«Рубикон»	https://npo-echelon.ru/

Подсистема межсетевого экранирования в сети АСУТП

Эти СЗИ защищают корпоративную сеть от попыток проникновения. Иногда их называют также файрволами или брандмауэрами.

Eltex	https://eltex-co.ru

UserGate	https://usergate.com
S-Terra	https://www.s-terra.ru
TrustAccess	https://www.securitycode.ru/

Подсистема однонаправленной передачи данных

АПК InfoDiode	http://www.amt.ru/web/ru/infodiode
ProfiDiode	http://oreol-security.ru

Подсистема криптографической защиты каналов связи

Эти СЗИ защищают уже не доступ к информации, а ее саму — с помощью криптографии. То есть, вся она передается в зашифрованном виде и декодируется с помощью криптографических ключей. Без них злоумышленник не сможет понять смысла данных, даже если перехватит их.

АПКШ Континент	https://www.securitycode.ru/products/apksh_kontinent/
ПАК ViPNet	https://infotecs.ru/product/setevye-komponenty/vipnet-coordinator-hw/
ПАК S-Terra	https://www.s-terra.ru/products/catalog/s-terra-shlyuz-4-2/

Подсистема профилирования

Kaspersky Industrial CyberSecurity for Networks	https://www.kaspersky.ru/enterprise-security/industrial
PT Industrial Security Incident Manager	https://www.ptsecurity.com/ru-ru/products/isim/

Подсистема анализа защищенности

MaxPatrol 8 / MaxPatrol VM	https://www.ptsecurity.com/ru-ru/products/mp8/
Nessus	https://www.tenable.com/products/nessus/nessus-professional
Open VAS	https://openvas.ru/

Подсистема антивирусной защиты

Kaspersky Endpoint Security	https://www.kaspersky.ru
Kaspersky Industrial CyberSecurity for Nodes	https://www.kaspersky.ru/enterprise-security/industrial
Symantec Endpoint Protection	https://symantec.com/
PT Sandbox	https://www.ptsecurity.com/ru-ru/products/sandbox/

Подсистема контроля действий привилегированных пользователей

SafeInspect	https://www.newinfosec.ru/content/safeinspect
СКДПУ	http://it-bastion.com

Подсистема идентификации, аутентификации

MS AD	https://www.microsoft.com
Secret Net	https://www.securitycode.ru/products/secret-net-studio/

Подсистема контроля конфигурации

Efros Config Inspector	https://www.gaz-is.ru
AUVESY VersionDog	https://www.versiondog.ru
Tufin Network Security Policy Management	https://www.tufin.com

Подсистема регистрации событий безопасности (SIEM)

SIEM (Security information and event management) - управление информацией о безопасности и событиями ИБ. Система может оперативно обнаружить внешние и внутренние атаки, анализировать инциденты и события, оценивать уровень защиты информационной системы, формировать отчеты и другую аналитику.

Positive Technologies MaxPatrol SIEM	https://www.ptsecurity.com/ru-ru/products/mpsiem/

CYBERLYMPHA	https://datapk.ru
Kaspersky Unified Monitoring and Analysis Platform	https://www.kaspersky.ru/enterprise-security/unified-monitoring-and-analysis-platform
RuSIEM	https://rusiem.com

Подсистема управления ИБ

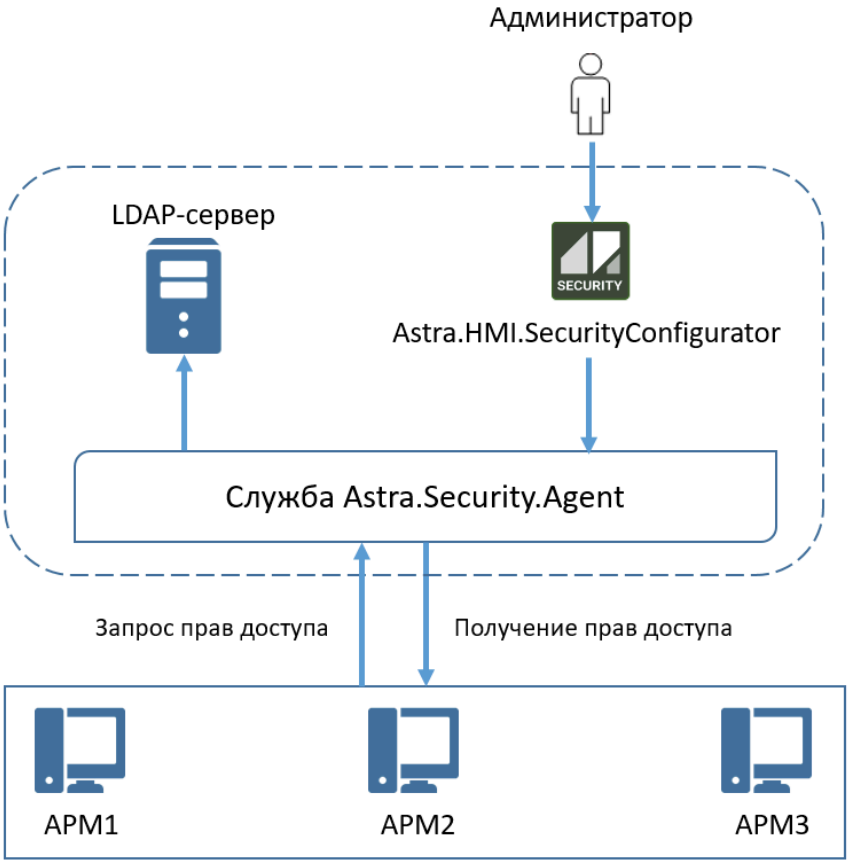
ePlat4m Security GRC	http://eplat4m.ru
R-vision SGRC	https://r-vision.pro

1.2. Подсистема безопасности

Основная функция подсистемы безопасности - разграничение прав доступа пользователей.

Подсистема безопасности построена на протоколе доступа к сетевым каталогам LDAP.

Компонент	Версия	Описание
Astra.Security.Agent	1.4.14.1	Агент безопасности
OpenLDAP	2.5.5	Сервер для хранения учетных записей и прав доступа
Astra.HMI.SecurityConfigurator	2.2.2.1	Конфигуратор для администрирования учетных записей и прав доступа
Astra.HMI.Security	2.0.7.1	Библиотека Astra.HMI для использования прав доступа



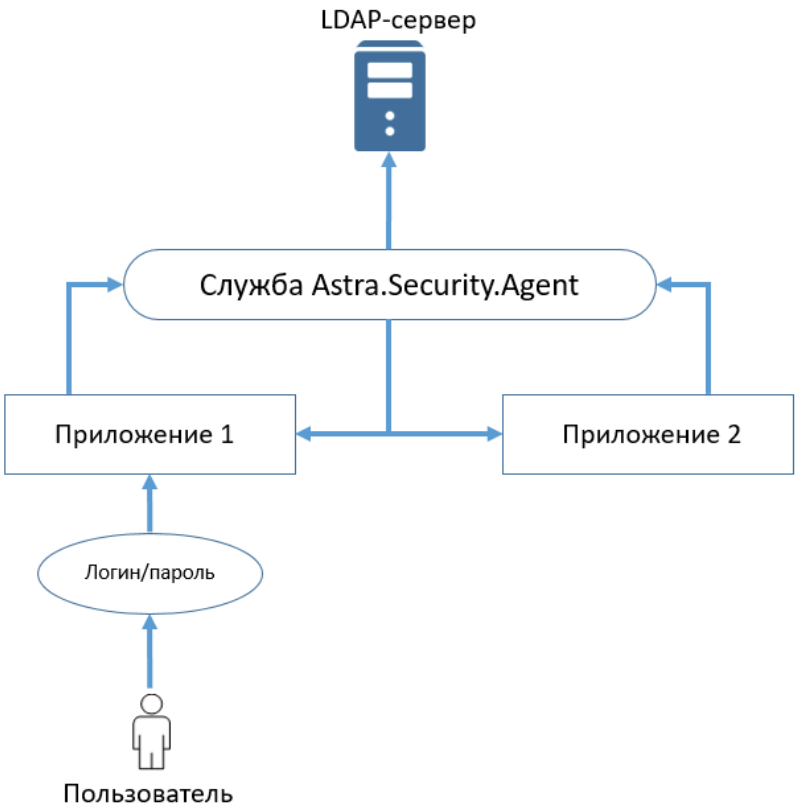
После некорректной установки компонентов или возникновении ошибок с подключением к серверу OpenLDAP, самый простой способ восстановить штатную работу – переустановить Astra.Security.

1.2.1. Astra.Security.Agent

Astra.Security.Agent – служба, отправляющая информацию приложениям о состоянии безопасности на рабочем месте и информацию о значениях прав, запрашиваемых прав приложений, для текущего пользователя подсистемы безопасности.

Алгоритм работы агента безопасности можно представить в виде 5 пунктов:

1. При входе в приложение пользователь вводит свой логин и пароль.
2. Приложение отправляет запрос службе Astra.Security.Agent, которая переадресует запрос LDAP-серверу.
3. LDAP-сервер проверяет, существует ли такой пользователь в базе данных.
4. Если пользователь существует, LDAP-сервер передает информацию о правах пользователя службе Astra.Security.Agent.
5. Служба Astra.Security.Agent, в свою очередь, уведомляет все приложения, которые к ней подключены, что пользователь с определенными правами прошел авторизацию на LDAP-сервере.



Если пользователь, в рамках своей пользовательской сессии, решит войти в другое приложение, которое подключено к службе Astra.Security.Agent и к которому у пользователя также есть доступ, то ему не придется заново вводить логин и пароль, данную информацию приложение уже получит от службы Astra.Security.Agent.

1.2.1.1. Настройка

Для использования защищенного соединения необходимо отредактировать конфигурационный файл "astra.security.agent.xml", расположенный в директории установки Astra.Security:

ОС Windows:

C:\Program Files\AstraRegul\Astra.Security.

ОС Linux:

/opt/AstraRegul/Astra.Security.

После изменения настроек нужно перезапустить службу Astra.Security.Agent

Пример конфигурационного файла

```
<Astra.Security.Agent>
    <EntryPointNetAgent Address="127.0.0.1" Port="1010"/>
    <LdapHosts>
        <LDAPServer Address="127.0.0.1" Port="389"/>
    </LdapHosts>
    <LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>
    <LdapPassword value="RWxHK5e2yzqRm38glUuOOsToGpZIUnY7XqA8O3JfqAQukcFbDiADJ/V0uU2UgPAetUUmMXIKLdAN5pzNYfV+J5synx7OfXHNgN0f9KOEedI
+PaQFOyYzCK15+PcVIJcE2WVzWhzIzPOtU9+YsKoa7YsKSMBAve4Eo"/>
    <LdapSecure value="False"/>
    <SecurityDn value="ou=AstraSecurity,dc=maxcrc,dc=com"/>
    <DefaultUser value=""/>
    <DefaultUserPassword value=""/>
    <GuestDisplayName value=""/>
```

```
    <mesPrefix value=""/>
    <AuditLogConsumers TraceAudit="0">
      <OpcDaLogConsumer>
          <Server Host="127.0.0.1" Type="OPC" ProgId="AstraRegul.OPCDAServer" TCPServerPort="4388" HostTcpReserve="" MasterPasswordCipher="">
        <SeverityMap>
          <Severity Category="Critical" Value="800" Sound=""/>
          <Severity Category="Important" Value="200" Sound=""/>
          <Severity Category="Info" Value="100" Sound=""/>
          <Severity Category="Debug" Value="0" Sound=""/>
        </SeverityMap>
        <SignalMap>
          <Signal Name="DynEvents.NormalDynSignal" Mode="DynamicEvent" Type="Normal"/>
          <Signal Name="DynEvents.AdminDynSignal" Mode="DynamicEvent" Type="Admin"/>
          <Signal Name="DynEvents.UserNameDynSignal" Mode="DynamicEvent" Type="UserName"/>
          <Signal Name="DynEvents.DisplayNameDynSignal" Mode="DynamicEvent" Type="DisplayName"/>
          <Signal Name="DynEvents.GroupNameDynSignal" Mode="DynamicEvent" Type="GroupName"/>
          <Signal Name="DynEvents.WorkstationNameDynSignal" Mode="DynamicEvent" Type="WorkstationName"/>
          <Signal Name="DynEvents.NormalMessage" Mode="Value" Type="Normal"/>
          <Signal Name="DynEvents.AdminMessage" Mode="Value" Type="Admin"/>
          <Signal Name="DynEvents.UserNameMessage" Mode="Value" Type="UserName"/>
          <Signal Name="DynEvents.DisplayNameMessage" Mode="Value" Type="DisplayName"/>
          <Signal Name="DynEvents.GroupNameMessage" Mode="Value" Type="GroupName"/>
          <Signal Name="DynEvents.WorkstationNameMessage" Mode="Value" Type="WorkstationName"/>
        </SignalMap>
      </Server>
    </OpcDaLogConsumer>
  </AuditLogConsumers>
  <Options LoggerLevel="2" ICMode="1" kbDriverString="0x1D+0x38+0x53;0x1D+0x2A+0x01;" UseRightsCacheStorage="0" />
</Astra.Security.Agent>
```

1.2.1.1.1. Настройка связи с узлами сети Astra.Net

Эта настройка выполняется в случае, если Net-агент и агент безопасности установлены на разных компьютерах.

Чтобы установить связь Astra.Security с Net-агентом, в конфигурационном файле укажите адрес точки доступа Astra.Net.Agent:

<EntryPointNetAgent **Address**="127.0.0.1" **Port**="1010"/>

- Address – IP-адрес Net-агента;
- Port – порт для подключения.

1.2.1.1.2. Настройка соединения с LDAP-сервером

Эта настройка выполняется в случае, если OpenLDAP и агент безопасности установлены на разных компьютерах.

Чтобы установить связь между Агент Astra.Security и LDAP-сервером, установленным на другом компьютере, укажите адрес и порт LDAP-сервера:

```
<LdapHosts>
    <LDAPServer Address="127.0.0.1" Port="389"/>
</LdapHosts>
```

1.2.1.1.2.1. Настройка защищенного соединения с LDAP-сервером

Чтобы установить защищенную связь между Агент Astra.Security и LDAP-сервером, установите значение порта LDAP-сервера равным 636:

```
<LdapHosts>
    <LDAPServer Address="127.0.0.1" Port="636"/>
</LdapHosts>
```

Также у тега **<LdapSecure>** установите значение параметра равным "True":

```
<LdapSecure value="True"/>
```

1.2.1.1.3. Настройка администратора LDAP

По умолчанию указана стандартная учетная запись администратора LDAP, создающаяся автоматически при установке Astra.Security. Если необходимо, можно указать другую учетную запись администратора LDAP, указав здесь же пароль для нее.

По умолчанию администратором является пользователь Manager, пароль администратора задается при установке OpenLDAP.

В конфигурационном файле имя администратора запишите в качестве значения тега **<LdapUser>** в указанном виде:

<LdapUser value="cn=Manager,dc=maxcrc,dc=com"/>

"**dc=maxcrc,dc=com**" – домен LDAP-сервера, указываемый для связи с Агент Astra.Security. Это значение **менять нельзя**.

"**cn="логин-администратора",dc="домен-базы-данных**""– формат указания каталога, принятый для OpenLDAP.

Здесь же укажите пароль администратора в зашифрованном виде в качестве значения тега <LdapPassword>:

<LdapPassword **value**="VuZyuLC...JFchMHvKXNeztHoFpe24v2Wl9viv"/>

Когда необходимо зашифровать пароль, используйте приложение **astra.security.crypter**, расположенное в /AstraRegul/Astra.Security/Utils.

1. Запустите приложение через командную строку от имени администратора.
2. Введите шифруемый пароль и нажмите Enter.
3. Зашифрованное значение скопируйте и вставьте в качестве значения тега **<LdapPassword>** в конфигурационный файл.

Пароли шифруются с использованием алгоритма Salted SHA-1 и хранятся в виде необратимых хэш-значений.

1.2.1.1.4. Настройка пользователя по умолчанию

Можно указать пользователя по умолчанию – пользователя, чьи права используются, когда нет активной пользовательской сессии.

Пользователем по умолчанию может быть любой пользователь из созданных при конфигурировании подсистемы. В целях безопасности не указывайте пользователя, у которого есть права на редактирование конфигурации подсистемы безопасности.

Задайте имя пользователя в конфигурационном файле в качестве значения тега **<DefaultUser>**:

```
<DefaultUser value="ИМЯПОЛЬЗОВАТЕЛЯ"/>
```

Здесь же укажите пароль пользователя по умолчанию в зашифрованном виде в качестве значения тега **<DefaultUserPassword>**:

```
<DefaultUserPassword
value="VuZyuLC...JFchMHvKXNeztHoFpe24v2Wl9viv"/>
```

1.2.1.1.5. Настройка каталога (корневой папки)

Этот параметр менять не нужно, если на LDAP-сервере всего один каталог и Вы создавали его с помощью конфигуратора Astra.HMI.SecurityConfigurator.

Если же на LDAP-сервере хранится несколько разных каталогов (корневых папок), и подключаться по умолчанию нужно только к одному из них, укажите название нужного каталога в качестве значения тега **<SecurityDn>**:

<SecurityDn value="ou=**AstraSecurity**,dc=maxcrc,dc=com"/>,
где **AstraSecurity** – название каталога по умолчанию.

"**dc=maxcrc,dc=com**" – домен LDAP-сервера, указываемый для связи с Агент Astra.Security. Это значение **менять нельзя**.

"**cn="логин-администратора",dc="домен-базы-данных**""– формат указания каталога, принятый для OpenLDAP.

1.2.1.1.6. Настройка логирования

Чтобы изменить уровень логирования, назначьте атрибуту LoggerLevel тега <Options> значение:

- 0 – чтобы выводить в лог минимум информации;
- 2 – чтобы выводить в лог всю необходимую информацию о работе Astra.Security;
- 5 – чтобы выводить в лог дополнительную информацию о работе Astra.Security.

Рекомендуемое значение = "**2**". Значение = "**5**" следует использовать только при поиске и анализе ошибок.

<Options **LoggerLevel**="2" ICMode="1" kbDriverString="0x1D +0x38+0x53;0x1D+0x2A+0x01;" UseRightsCacheStorage="0" />

1.2.1.1.7. Настройка источника данных о правах

Флаг **UseRightsCacheStorage** используется для выбора источника данных о правах:

- 1 – права пользователя не запрашиваются с LDAP-сервера по необходимости, используются кэшированные значения прав;
- 0 – права пользователя запрашиваются с LDAP-сервера всегда.

<Options LoggerLevel="2" ICMode="1" kbDriverString="0x1D +0x38+0x53;0x1D+0x2A+0x01;" **UseRightsCacheStorage**="0" />

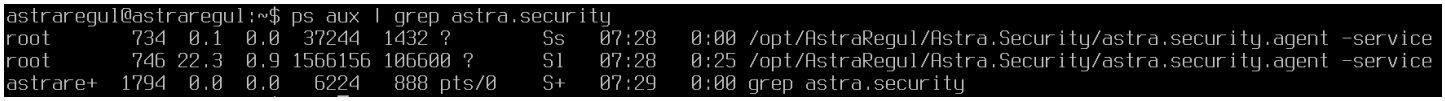
1.2.1.1.8. Запуск сервисов на ОС Linux

1.2.1.1.8.1. Запуск сервиса astra.security.useractivity.service

Сервис предназначен для обслуживания сессий пользователя. Именно этот сервис позволяет отследить длительность сессии и время бездействия пользователя. Благодаря ему происходит автоматический выход пользователя из системы, если длительность сессии или время бездействия достигло установленного лимита.

По умолчанию сервис запускается автоматически. Чтобы посмотреть список запущенных сервисов, используйте команду "ps aux". Для удобства поиска отфильтруйте результаты с помощью команды "grep":

```
ps aux | grep astra.security
```



Если в списке не будет сервиса "astra.security.useractivity.service", необходимо будет запустить его вручную.

Сервис запускается для каждого пользователя отдельно. Чтобы запустить сервис для конкретного пользователя, необходимо редактировать файл "astra.security.useractivity.sh", расположенный в /opt/AstraRegul/Astra.Security. Для этого выполните следующие действия:

1. Откройте файл в текстовом редакторе, вызвав команду:

```
sudo nano /opt/AstraRegul/Astra.Security/astra.security.useractivity.sh
```

```
#!/bin/sh
# Установите правильный адрес дисплея для графического сервера в переменной окружения DISPLAY.
# Пример: ":0".
export DISPLAY=":0"
# Установите правильный путь к файлу авторизации для графического сервера
# (для того пользователя, от которого выполняется вход в графическую систему).
# Пример: "/home/user1/.Xauthority".
export XAUTHORITY="/home/<имя_пользователя>/.Xauthority"
# Укажите имя пользователя для запуска команды от его имени.
sudo -u <имя_пользователя> /opt/Automiq/Astra.Security/astraa.security.useractivity
```

2. Укажите значение "DISPLAY", зависящее от количества и конфигурации мониторов. Чтобы узнать значение, вызовите команду:

```
export |grep DISPLAY
```

```
astraregul@astraregul:~$ export  | grep DISPLAY
declare -x DISPLAY=":0"
```

3. Укажите имя пользователя, под которым необходимо запускать сервис. Затем нажмите сочетание клавиш "Ctrl + O", чтобы сохранить изменения, и сочетание клавиш "Ctrl + X", чтобы выйти из редактора.

После этого стоит перезапустить систему. Проверьте список запущенных сервисов с помощью команды "ps aux". Сервис "astra.security.useractivity.service" будет запущен от имени указанного пользователя.

Если же необходимо, чтобы сервис следил за сессией еще одного пользователя, необходимо добавить этого пользователя в конфигурацию сервиса. Для этого перейдите к файлу "astra.security.useractivity.add.anotheruser.sh", расположенному в "/opt/AstraRegul/Astra.Security", и следуйте инструкции, описанной в нем.

```
#!/bin/sh
echo Данный файл поможет создать службу useractivity
echo для еще одного пользователя графической системы.
echo Сначала отредактируйте данный файл:
echo замените anotheruser на нужное имя пользователя.
echo Затем выполните следующие команды.
#cp /lib/systemd/system/astra.security.useractivity.service /lib/systemd/system/astra.security.useractivity.anotheruser.service
#cp /opt/AstraRegul/Astra.Security/astra.security.useractivity.sh /opt/AstraRegul/Astra.Security/astra.security.useractivity.anotheruser.sh
echo Далее, отредактируйте файл /opt/AstraRegul/Astra.Security/astra.security.useractivity.anotheruser.sh
echo для того, чтобы установить правильные значения
echo переменных окружения DISPLAY и XAUTHORITY.
echo Далее, отредактируйте файл /lib/systemd/system/astra.security.useractivity.anotheruser.service
echo  для того, чтобы в нем было указано правильное название
echo  файла /opt/AstraRegul/Astra.Security/astra.security.useractivity.anotheruser.sh
echo Затем выполните следующие команды.
#systemctl enable astra.security.useractivity.anotheruser.service
#systemctl start astra.security.useractivity.anotheruser.service
```

Замените "anotheruser" на "<имя_пользователя>".

Импорт настроек модулей мониторинга

Эту настройку необходимо выполнить для того, чтобы модули мониторинга отслеживали длительность сессий и блокировок пользователей.

Перейдите в папку установки Astra.Security:

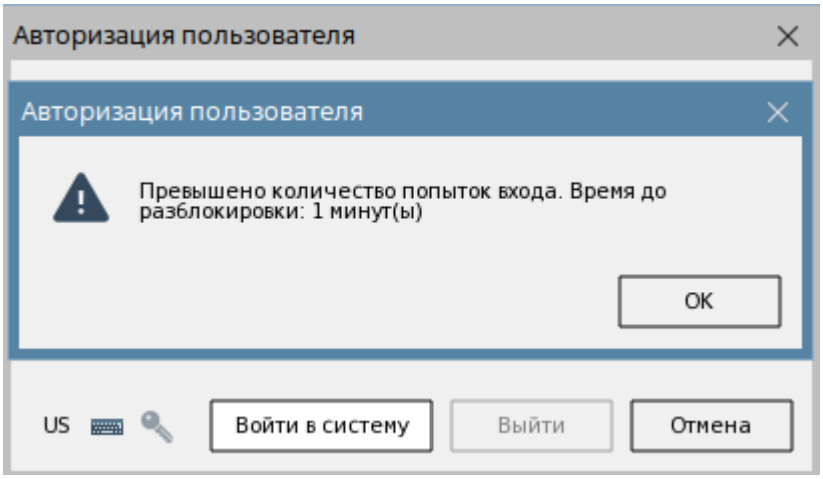
```
cd /opt/AstraRegul/Astra.Security/
```

Примените настройки модулей с помощью команд:

```
sudo sh ./monitor.export.sh
sudo sh ./addLockTime.sh
```

```
astraregul@astraregul:/opt/AstraRegul/Astra.Security$ sudo sh ./monitor.export.sh
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config"

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcDatabase={2}Monitor,cn=config"

astraregul@astraregul:/opt/AstraRegul/Astra.Security$ sudo sh ./addLockTime.sh
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn={4}astra,cn=schema,cn=config"

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn={4}astra,cn=schema,cn=config"
```

Теперь если ввести несколько раз неправильный пароль блокировка будет временной.


Авторизация пользователя
Авторизация пользователя
Превышено количество попыток входа. Время до разблокировки: 1 минут(ы)
OK
US
Войти в систему
Выйти
Отмена

1.2.1.1.8.2. Запуск сервисов от имени непривилегированного пользователя

Сервисы **astra.security.service** и **astra.security.useractivity.service**, как правило, запущены от имени суперпользователя root.

Чтобы посмотреть, от чьего имени запущен сервис, используйте команду "ps aux". Для удобства поиска отфильтруйте результаты с помощью команды "grep":

```
ps aux | grep astra.security
```

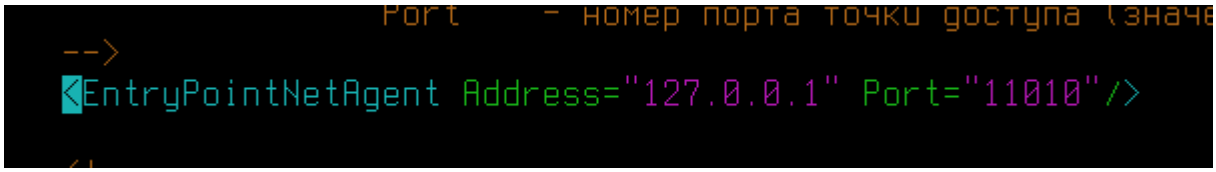
Однако в некоторых случаях бывает необходимо разрешить запуск сервиса от имени непривилегированного пользователя. Для этого выполните следующие шаги:

1. Перейдите к папке, где хранятся конфигурационные файлы агента безопасности – /opt/AstraRegul/Astra.Security, выполнив команду:

```
cd /opt/AstraRegul/Astra.Security
```

2. Замените в конфигурационном файле "astra.security.agent.xml" номер порта Net-агента на новое значение.

Измените номер порта Net-агента на значение выше 10000 (например, 11010). Это необходимо, потому что непривилегированным пользователям нельзя "прослушивать" порты с малыми номерами.



3. Перейдите в каталог, где хранятся конфигурационные файлы astra.Domain , выполнив команду:

```
cd /opt/AstraRegul/Astra.Domain
```

4. Укажите новое значение порта в конфигурационных файлах "astra.net.agent.xml" и "astra.domain.agent.xml".

```
<Astra.Net.Agent Name="local" NetEnterPort="11010" ParentAgentPort="11020">
```

```
-->
<EntryPointNetAgent Name="local" Address="127.0.0.1" Port="11010"/>
<!--
```

5. Перейдите к папке, содержащей юнит-файлы, выполнив команду:

```
cd /lib/systemd/system/
```

6. В файлах **astra.security.service** и **astra.security.useractivity.service** замените значение "root" в строчках "User=root" и "Group=root" на имя непривилегированного пользователя, например "User=test" и "Group=test".

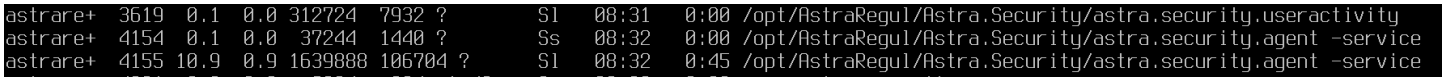
```
User=astraregul_new
Group=astraregul_new
```

7. Убедитесь в том, что непривилегированный пользователь имеет права на чтение и запись:

- папки установки Astra.Security;
- папок и файлов, для которых выполняется контроль целостности;
- кэша конфигурации Astra.Domain.

8. Перезапустите систему.

9. Проверьте список запущенных сервисов с помощью команды "ps aux". Сервисы "astra.security.service" и "astra.security.useractivity.service" будут запущены от имени указанного пользователя.



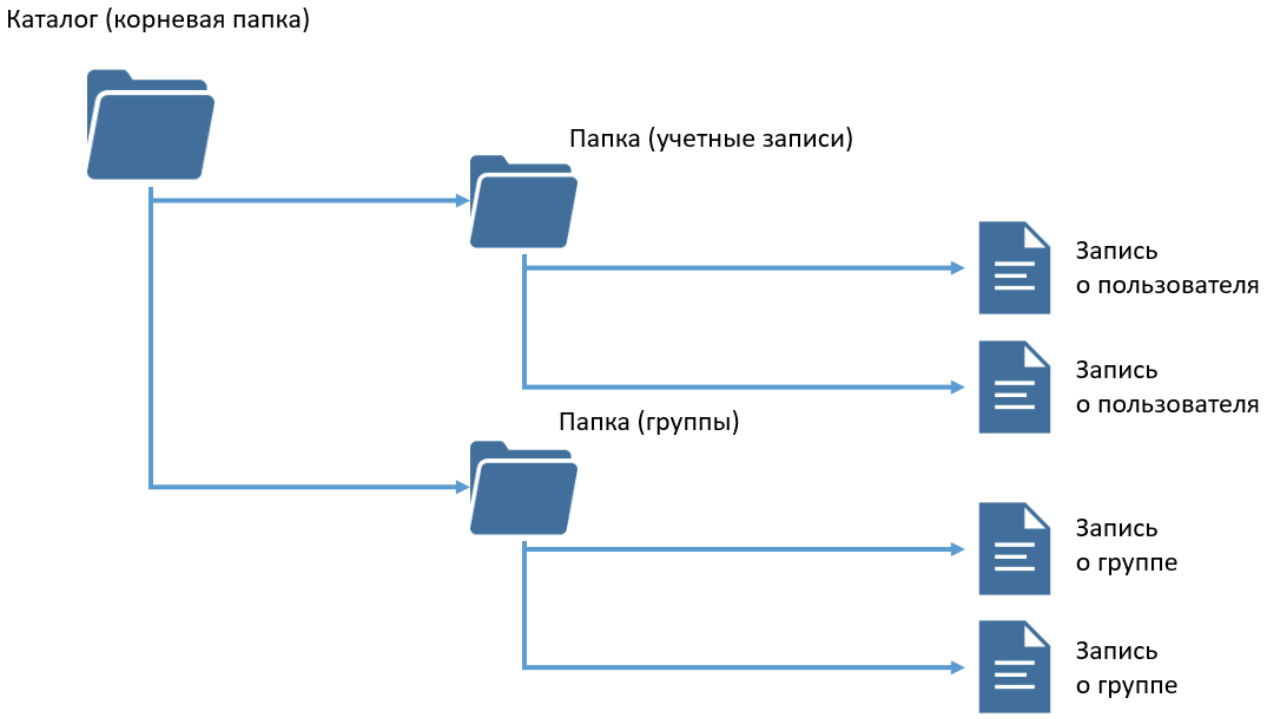
1.2.2. OpenLDAP

LDAP-сервер – это хранилище каталогов LDAP.

Каталоги предназначены для хранения записей об:

- учетных записях пользователей;
- группах пользователей;
- правах и приложениях, в которые объединяются права;
- рабочих местах и станциях.

Каталог имеет вид дерева: корневой узел содержит записи, которые могут быть объединены в папки.



Подсистема безопасности Astra.Security построена на протоколе доступа к описанным каталогам – LDAP.

> В качестве LDAP-сервера Astra.Security использует продукт OpenLDAP.

1.2.2.1. Базовая настройка

AstraLinux
РЕД ОС

Базовая настройка для ОС Windows не выполняется.

1.2.2.1.1. AstraLinux

Переименование домена базы данных LDAP
Определение структуры каталогов на LDAP-сервере
Добавление шаблона политики контроля доступа

1.2.2.1.1.1. Переименование домена базы данных LDAP

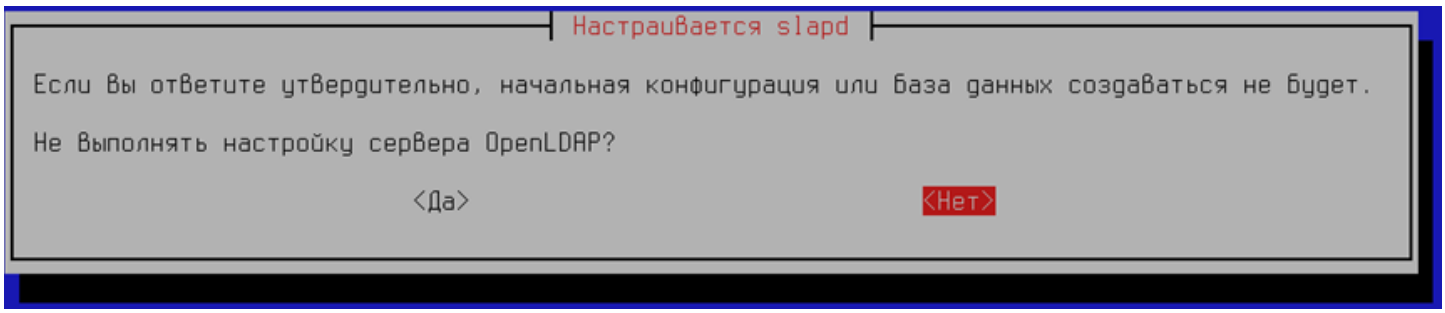
При установке OpenLDAP в качестве имени домена по умолчанию используется значение nodomain. Значение имени домена по умолчанию для компонентов Astra.Security: maxcrc.com.

Чтобы создать учетную запись администратора LDAP-сервера выполните следующие действия:

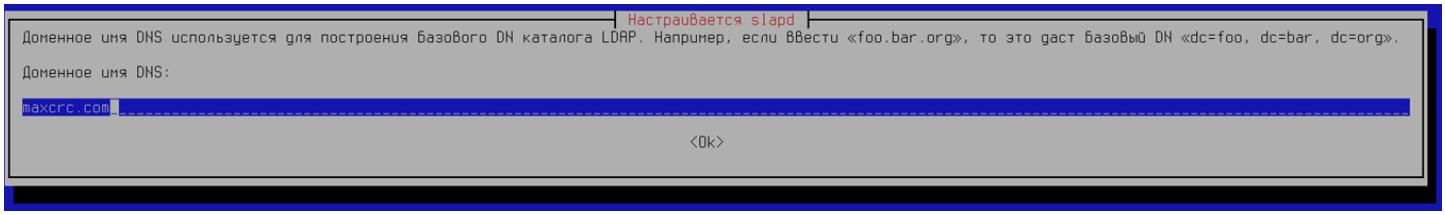
1. Чтобы изменить имя домена, используйте команду:

```
sudo dpkg-reconfigure slapd
```

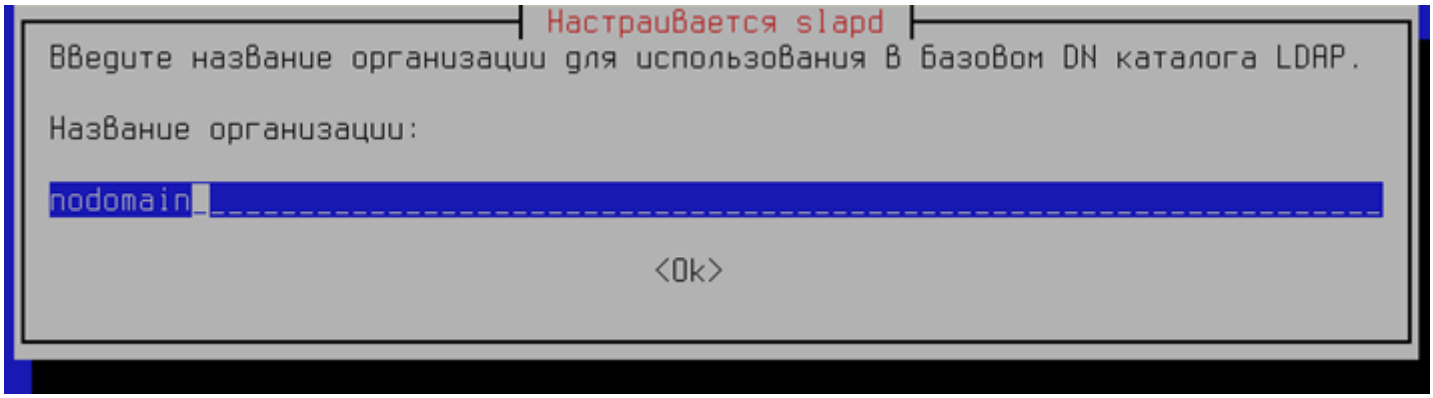
2. В открывшемся окне на вопрос "Не выполнять настройку сервера OpenLDAP?" ответьте No (Нет). Запустится конфигуратор LDAP-сервера. В конфигураторе:



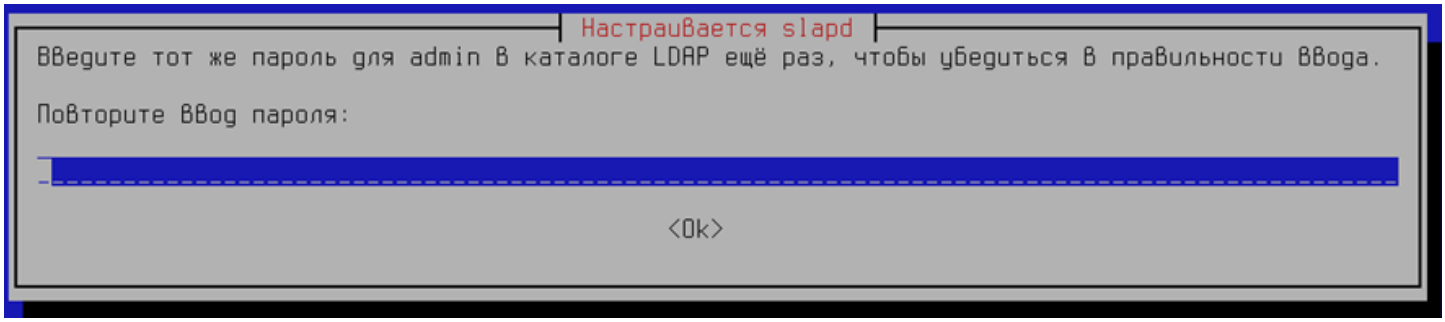
3. В качестве имени домена задайте строку maxcrc.com:



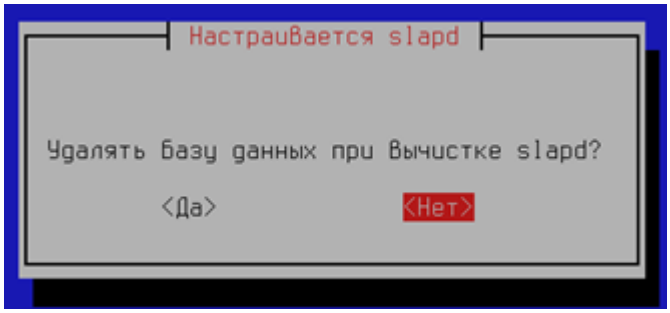
4. Название организации может быть произвольным:



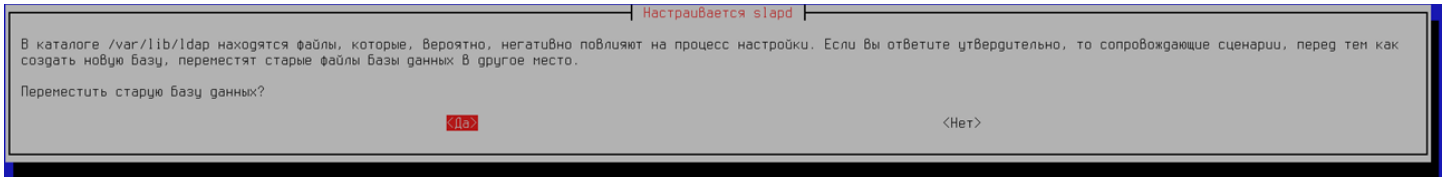
5. Укажите пароль администратора:



6. На вопрос : "Удалять базу данных при удалении slapd?" можете отвечать выборочно, в зависимости от требований и удобства:



7. На вопрос: "Переместить старую базу данных?" ответьте Да, если есть файлы старой базы данных.



8. После настройки пакета должно появиться окно терминала со следующим содержанием:

```
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.57+dfsg-3~bpo10+1.astra1+b1... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
```

9. Перезапустите OpenLDAP Service следующей командой:

sudo systemctl restart slapd

```
user@astra:~$ sudo systemctl restart slapd
```

1.2.2.1.1.2. Определение структуры каталогов на LDAP-сервере

После установки OpenLDAP структура каталогов на сервере еще не определена. Эту настройку **обязательно нужно выполнить**.

Чтобы сформировать структуру данных внутри каталогов LDAP, нужно применить файлы схемы. Необходимые файлы схемы **astra.security.ldif** и shell-скрипт **astra.security.schema.export.sh** устанавливаются вместе с пакетом Astra.Security.

Чтобы применить схемы выполните следующие команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./astra.security.schema.export.sh
```

```
user@astra:/opt/AstraRegul/Astra.Security$
user@astra:/opt/AstraRegul/Astra.Security$ cd /opt/AstraRegul/Astra.Security
user@astra:/opt/AstraRegul/Astra.Security$ sudo sh ./astra.security.schema.export.sh
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=astra,cn=schema,cn=config"
```

Перезапустите OpenLDAP Service следующей командой:

```
sudo systemctl restart slapd
```

```
user@astra:/opt/AstraRegul/Astra.Security$ sudo systemctl restart slapd
user@astra:/opt/AstraRegul/Astra.Security$
```

1.2.2.1.1.3. Добавление шаблона политики контроля доступа

Чтобы содержимое каталогов можно было просматривать и редактировать, нужно настроить политики контроля доступа. Для этого следует создать файл-шаблон с описанием прав доступа к OpenLDAP и применить его.

1. Создайте файл-шаблон **access.ldif** командой:

```
sudo nano access.ldif
```

2. Добавьте в файл **access.ldif** следующие строки:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by users write by * read
```

3. После этого сохраните файл и выйдите с помощью комбинации Ctrl + O и Ctrl + X.

4. Примените созданный файл-шаблон командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f access.ldif
```

1.2.2.1.2. РЕД ОС

Создание учетной записи администратора LDAP-сервера
Добавление шаблона политики контроля доступа
Создание базы данных LDAP
Определить структуру каталогов на LDAP-сервере
Переименование домена базы данных LDAP

1.2.2.1.2.1. Создание учетной записи администратора LDAP-сервера

Если при установке OpenLDAP было предложено придумать пароль для создаваемой учетной записи администратора OpenLDAP, этот шаг можно пропустить и перейти к следующему пункту Переименовать домен базы данных LDAP.

Чтобы создать учетную запись администратора LDAP-сервера выполните следующие действия:

1. Сгенерируйте шифрованное значение пароля для учетной записи администратора с помощью команды:

slappasswd

Шифрованное значение имеет вид {SSHA}строка_символов.

```
[root@localhost AstraRegul]# slappasswd
New password:
Re-enter new password:
{SSHA}YVWxXjb4W+tWQjoZtKQhe9Tx01ejidok
[root@localhost AstraRegul]#
```

Сохраните полученное значение для следующих шагов настройки.

2. Перейдите в папку /opt/AstraRegul, следующей командой:

cd /opt/AstraRegul

```
[root@localhost Astra.Security]# cd /opt/AstraRegul/
```

3. Создайте файл **config.ldif**:

sudo nano config.ldif

```
[root@localhost AstraRegul]# cd /opt/AstraRegul/
[root@localhost AstraRegul]# sudo nano config.ldif
```

В данном примере для создания и редактирования текстовых файлов на ОС Linux предлагается использовать редактор NANO. Команда nano позволяет открыть существующий или создать новый файл с указанным именем. В результате вызова команды файл откроется в соответствующем редакторе.

Если используете редактор NANO, то:

- чтобы сохранить файл, нажмите сочетание клавиш Ctrl + O;
- чтобы выйти из редактора, нажмите сочетание клавиш Ctrl + X;
- чтобы вызвать справку, нажмите сочетание клавиш Ctrl + G.

4. Добавьте в файл **config.ldif** следующие строчки:

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}/gXAjQ0eerpfXsIoH1iCKSJlimiYzJlq

```
 GNU nano 4.3
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}0Or1IEEMJQ1UC+sgZmmMt2EElvN64DYS
```

› **olcDatabase** – указывает конкретное имя экземпляра базы данных и обычно находится в /etc/ldap/slapd.d/cn=config;
› **cn=config** – указывает глобальные параметры конфигурации;
› **{SSHA}строка_символов** – шифрованное значение пароля.

5. Сохраните файл, нажав сочетание клавиш Ctrl + O, и выйдите из редактора, нажав сочетание клавиш Ctrl + X.

6. Добавьте запись администратора в LDAP командой, указав URI со ссылкой на LDAP-сервер и файл, созданный ранее:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f config.ldif
```

В случае успешного изменения должно появиться следующее сообщение:

```
[root@localhost AstraRegul]# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f config.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

1.2.2.1.2.2. Добавление шаблона политики контроля доступа

Чтобы содержимое каталогов можно было просматривать и редактировать, нужно настроить политики контроля доступа. Для этого следует создать файл-шаблон с описанием прав доступа к OpenLDAP и применить его.

Файл, создаваемый в инструкции, для анонимных пользователей делает доступным чтение, для зарегистрированных пользователей – редактирование каталогов.

Чтобы добавить шаблон политики контроля доступа выполните следующие действия:

1. Создайте файл-шаблон **access.ldif**

sudo nano access.ldif

```
[root@localhost AstraRegul]# sudo nano access.ldif
```

2. Добавьте в файл access.ldif следующие строчки:

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by users write by * read

```
 GNU nano 4.3
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by users write by * read
```

3. Сохраните файл, нажав сочетание клавиш Ctrl + O, и выйдите из редактора, нажав сочетание клавиш Ctrl + X.

4. Примените изменения командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f access.ldif
```

В случае успешного изменения должно появиться следующее сообщение:

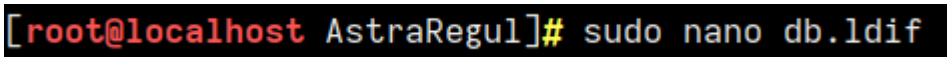
```
[root@localhost AstraRegul]# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f config.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

1.2.2.1.2.3. Создание базы данных LDAP

Чтобы создать базы данных LPAD выполните следующие действия:

1. Создайте файл-шаблон **db.ldif**

sudo nano db.ldif



2. Добавьте в файл db.ldif следующие строчки:

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}/gXAjQ0eerpfXsIoH1iCKSJlimiYzJlq
Где {SSHA}/gXAjQ0eerpfXsIoH1iCKSJlimiYzJlq – зашифрованный пароль, сгенерированный в пункте "**Создать учетную запись администратора LDAP-сервера**".

```
 GNU nano 4.3
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=maxcrc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}0Or1IEEMJQ1UC+sgZmmMt2EElvN64DYS
```

3. Сохраните файл, нажав сочетание клавиш Ctrl + O, и выйдите из редактора, нажав сочетание клавиш Ctrl + X.

4. Примените изменения командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f db.ldif
```

В случае успешного изменения должно появиться следующее сообщение:

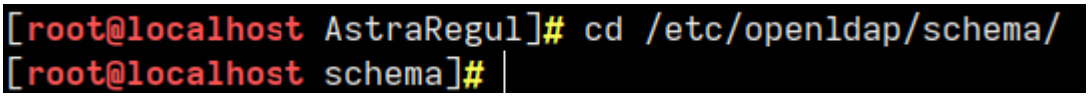
```
[root@localhost AstraRegul]# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f db.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}mdb,cn=config"

modifying entry "olcDatabase={2}mdb,cn=config"

modifying entry "olcDatabase={2}mdb,cn=config"
```

1.2.2.1.2.4. Определить структуру каталогов на LDAP-сервере

После установки OpenLDAP структура каталогов на сервере еще не определена. Эту настройку обязательно нужно выполнить.
Чтобы сформировать структуру данных внутри каталогов LDAP, выполните следующие действия:

1. Перейдите в директорию /etc/openldap/schema/

```
cd /etc/openldap/schema/
```



2. Примените схемы в следующем порядке:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f collective.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f corba.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cosine.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f duaconf.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f dyngroup.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f inetorgperson.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f java.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f misc.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f nis.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f openldap.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f pmi.ldif
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ppolicy.ldif
```

После каждой команды, должно появляться сообщение об успешном применении схемы:

```
[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f collective.ldif
adding new entry "cn=collective,cn=schema,cn=config"

[root@localhost schema]# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f corba.ldif
adding new entry "cn=corba,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cosine.ldif
adding new entry "cn=cosine,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f duaconf.ldif
adding new entry "cn=duaconf,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f dyngroup.ldif
adding new entry "cn=dyngroup,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f inetorgperson.ldif
adding new entry "cn=inetorgperson,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f java.ldif
adding new entry "cn=java,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f misc.ldif
adding new entry "cn=misc,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f nis.ldif
adding new entry "cn=nis,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f openldap.ldif
adding new entry "cn=openldap,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f pmi.ldif
adding new entry "cn=pmi,cn=schema,cn=config"

[root@localhost schema]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ppolicy.ldif
adding new entry "cn=ppolicy,cn=schema,cn=config"
```

3. Перейдите в директорию /opt/AstraRegul/Astra.Security

```
cd /opt/AstraRegul/Astra.Security
```

```
[root@localhost schema]# cd /opt/AstraRegul/Astra.Security/
[root@localhost Astra.Security]#
```

4. Примените последнюю схему, командой:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f astra.security.ldif
```

В случае успешного изменения должно появиться следующее сообщение:

```
[root@localhost Astra.Security]# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f astra.security.ldif
adding new entry "cn=astra,cn=schema,cn=config"

[root@localhost Astra.Security]#
```

1.2.2.1.2.5. Переименование домена базы данных LDAP

При установке OpenLDAP в качестве имени домена по умолчанию используется значение **nodomain**. Значение имени домена по умолчанию для компонентов Astra.Security – **maxcrc.com**. Эту настройку обязательно нужно выполнить.

Чтобы переименовать домен базы данных LDAP выполните следующие действия:

1. Перейдите в директорию /opt/AstraRegul:

```
[root@localhost AstraRegul]# cd /opt/AstraRegul/
```

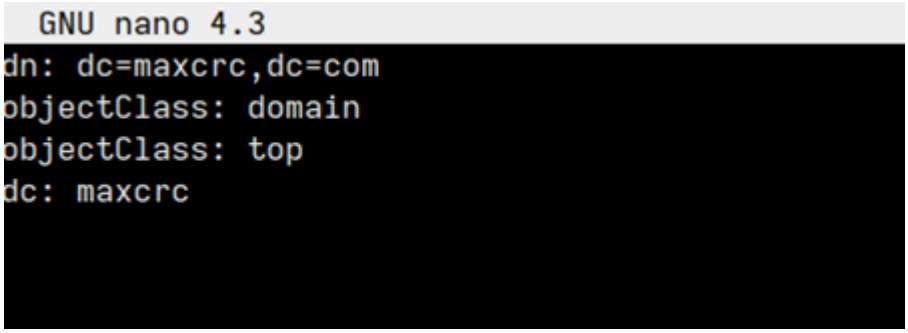
2. Создайте файл **empty.ldif**

sudo nano empty.ldif

```
[root@localhost AstraRegul]# sudo nano empty.ldif
```

3. Добавьте в файл empty.ldif следующие строчки:

dn: dc=maxcrc,dc=com
objectClass: domain
objectClass: top
dc: maxcrc

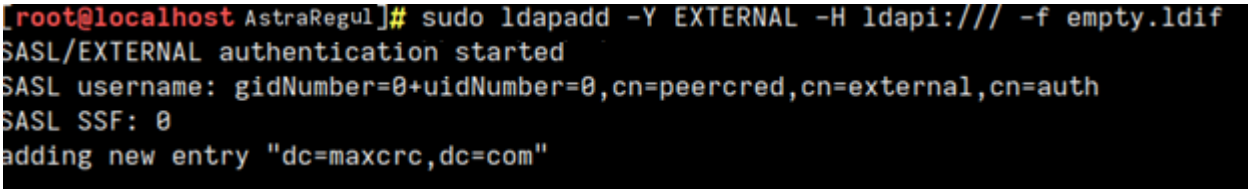


4. Сохраните файл, нажав сочетание клавиш Ctrl + O, и выйдите из редактора, нажав сочетание клавиш Ctrl + X.

5. Примените изменения командой:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f empty.ldif
```

В случае успешного изменения должно появиться следующее сообщение:



1.2.2.2. Резервирование

Резервирование (репликация) LDAP-сервера позволяет синхронизировать конфигурации двух и более серверов.

Резервирование может быть:

- однонаправленным – в этом случае конфигурация одного сервера (поставщика) тиражируется на другие сервера (приемники);
- разнонаправленным – в этом случае синхронизируются конфигурации нескольких серверов.

1.2.2.2.1. Windows

- Однонаправленное резервирование
- Разнонаправленное резервирование

1.2.2.2.1.1. Однонаправленное резервирование

Чтобы настроить однонаправленное резервирование:

1. Определите, какой из LDAP-серверов будет поставщиком, а какие – приемниками.

2. Настройте сервер-поставщик:

2.1. Перейдите к файлу конфигурации OpenLDAP **slapd.conf**, расположенному в папке:

C:\ProgramData\OpenLDAP\openldap

2.2 Раскомментируйте конструкцию syncprov:

```
# Раскоментируйте этот блок, если данный LDAP-сервер является Поставщиком (главным сервером)
#overlay syncprov
#syncprov-checkpoint 100 10
#syncprov-sessionlog 100
#index entryCSN eq
#index entryUUID eq
```

2.3. Перезапустите службу **OpenLDAP**.

3. Настройте сервера-приемники:

Описанные в пункте действия выполните на каждом из серверов-приемников.

3.1. Перейдите к файлу конфигурации OpenLDAP **slapd.conf**, расположенному в папке:

C:\Program Files\OpenLDAP

3.2 Раскомментируйте конструкцию syncrepl:

```
# Раскоментируйте этот блок, если данный LDAP-сервер является
    Потребителем (подчиненный сервером)
#syncrepl rid=1
#    provider=ldap://172.16.13.167:389
#    type=refreshAndPersist
#    retry="60 10 300 +"
#    searchbase="dc=maxcrc,dc=com"
#    filter="(objectClass=*)"
#    scope=sub
#    attrs="*,+"
#    schemachecking=off
#    bindmethod=simple
#    sizelimit=2147483648
#    timelimit=2147483648
#updateref ldap://172.16.13.167:389
```

3.3. Укажите IP-адрес и порт сервера-поставщика в значениях параметров **provider** и **updateref** вместо значения по умолчанию «**172.16.13.167:389**».

3.4. Перезапустите службу **OpenLDAP**.

3.5. Повторите описанные в пункте действия на всех серверах-приемниках.

4. Откройте конфигурационный файл **astra.security.agent.xml**, расположенному по следующему пути:

```
C:\Program Files\AstraRegul\AstraSecurity
```

5. Добавьте в секцию тега **<LdapHosts>** строки с IP-адресами и портами всех подчиненных серверов:

```
<LdapHosts>
    <LDAPServer Address="127.0.0.1" Port="389"/>
```

```
        <!-- <LDAPServer Address="199.99.99.111" Port="389"/> -->
    </LdapHosts>
```

6. Сохраните изменения в файле и перезапустите службу Astra.Security.Agent.

1.2.2.2.1.2. Разнонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Отключите все возможные репликации баз и серверов.

2. Убедитесь, что содержимое баз резервируемых серверов идентично.

3. Остановите все программы, взаимодействующие с серверами OpenLDAP.

4. Убедитесь, что системное время резервируемых серверов одинаковое, иначе синхронизация изменений будет работать в одну сторону.

5. На время настройки резервирования одного из серверов остановите остальные резервируемые сервера OpenLDAP.

Чтобы настроить разнонаправленное резервирование:

Описанные ниже действия выполните на каждом из резервируемых серверов.

1. Измените файл конфигурации OpenLDAP **slapd.conf**, расположенный в папке:

C:\ProgramData\OpenLDAP\openldap

1.1. Перед определением базы добавьте уникальный идентификатор сервера:

```
############################
# mdb database definitions
############################

ServerID 001

database        mdb
suffix          "dc=maxcrc,dc=com"
```

```
rootdn          "cn=Manager,dc=maxcrc,dc=com"
```

ServerID должен быть уникальным для каждого сервера.

1.2. Раскомментируйте всю конструкцию **syncrepl**, кроме последней строки:

```
syncrepl rid=1
    provider=ldap://172.16.13.167:389
    type=refreshAndPersist
    retry="60 10 300 +"
    searchbase="dc=maxcrc,dc=com"
    filter="(objectClass=*)"
    scope=sub
    attrs="*,+"
    schemachecking=off
    bindmethod=simple
    sizelimit=2147483648
    timelimit=2147483648
#updateref ldap://172.16.13.167:389
```

Конструкция **syncrepl** описывает один из резервируемых серверов. Добавьте столько конструкций **syncrepl**, сколько серверов участвуют в резервировании помимо текущего.

Внутри одного сервера параметры rid разных конструкций syncrepl должны иметь уникальные значения.

1.3. В каждой конструкции **syncrepl** укажите **IP-адрес** и **порт** сервера, который она описывает. Для этого в строке параметра **provider** замените по умолчанию «172.16.13.167:389» на нужное значение.

1.4. В конце файла добавьте запись:

```
mirrormode TRUE
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
index entryCSN eq
index entryUUID eq
```

2. Перезапустите службу OpenLDAP Service.

3. Повторите описанные выше действия на каждом из резервируемых серверов.

После настройки **последовательно включите** все сервера OpenLDAP.

4. Подключитесь напрямую к каждой базе и убедитесь, что ошибок не возникло.

Для проверки внесите изменения в конфигурацию на одном из серверов. Убедитесь, что эти изменения появились и на других серверах.

Первая синхронизация может занимать более 10 секунд.

1.2.2.2.2. Linux

- Однонаправленное резервирование
- Разнонаправленное резервирование

1.2.2.2.2.1. Однонаправленное резервирование

Прежде чем перейти к настройкам резервирования:
1. Убедитесь, что типы баз данных всех серверов – «mdb», с помощью команды:

```
sudo slapcat -n0
```

Если тип БД отличается, то во всех дальнейших командах нужно заменить mdb на текущий тип БД.

2. Сделайте бэкап конфигурации и БД сервера-поставщика в текущей папке с помощью команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

Чтобы настроить однонаправленное резервирование:

1. Определите, какой из LDAP-серверов будет поставщиком, а какие – приемниками.

2. Настройте сервера-приемники:

Описанные в пункте действия выполните на каждом из серверов-приемников.

2.1. Ознакомьтесь с файлом openldap-enable-syncrepl-consumer.ldif, устанавливаемым в составе Astra.Security:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
#delete: olcSyncrepl
add: olcSyncrepl
olcSyncrepl:
  rid=001
  provider=ldap://192.168.56.1
  binddn="cn=admin,dc=maxcrc,dc=com"
  bindmethod=simple
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  type=refreshAndPersist
  timeout=0
  network-timeout=0
  retry="60 +"

dn: olcDatabase={1}mdb,cn=config
changetype: modify
#delete: olcUpdateRef
add: olcUpdateRef
olcUpdateRef: ldap://192.168.56.1
```

Отступ в каждой строке внутри конструкции **olcSyncRepl** обязательно должен содержать по два пробела.

2.2. Измените следующие строки:

- «dn: olcDatabase={1}mdb,cn=config» – замените «mdb» на текущий тип БД, если он отличается;
- «provider=ldap://192.168.56.1» – замените значение по умолчанию «192.168.56.1» на адрес сервера-поставщика данных;
- «credentials="secret"» – если меняли пароль администратора OpenLDAP, замените «secret» на актуальное значение;
- «olcUpdateRef: ldap://192.168.56.1» – замените значение по умолчанию «192.168.56.1» на адрес сервера-поставщика данных;
- «binddn="cn=admin,dc=maxcrc,dc=com"» – замените на «binddn="cn=admin,dc=nodomain"», если не выполняли переименование домена;
- «searchbase="dc=maxcrc,dc=com"» – замените на «searchbase="dc=nodomain"», если не выполняли переименование домена.

В файлах .ldif порядок и количество пробелов имеют важное значение

2.3. Для применения внесенных изменений выполните команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-enable-syncrepl-consumer.sh
```

2.4. Перезапустите службу OpenLDAP Service:

```
sudo systemctl restart slapd
```

3. Настройте сервер-поставщик:

3.1. Ознакомьтесь с файлом **openldap-enable-syncrepl-provider.ldif**, устанавливаемым в составе Astra.Security:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpCheckpoint: 100 10
olcSpSessionlog: 100

dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq
```

3.2. Замените «mdb» на текущий тип БД, если он отличается, в строках:

- «dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config»;
- «dn: olcDatabase={1}mdb,cn=config»,

3.3. Для применения внесенных изменений выполните команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-enable-syncrepl-provider.sh
```

3.4. Перезапустите службу OpenLDAP Service:

```
sudo systemctl restart slapd
```

4. Настройте Агент Astra.Security:

4.1. Перейдите к файлу конфигурации **astra.security.agent.xml**, расположенному по следующему пути:

```
/opt/AstraRegul/Astra.Security
```

4.2 Добавьте в секцию тега <**LdapHosts**> строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
    <LDAPServer Address="127.0.0.1" Port="389"/>
    <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

4.3. Перезапустите службу:

```
sudo systemctl restart Astra.Security
```

1.2.2.2.2.2. Разнонаправленное резервирование

Прежде чем перейти к настройкам резервирования:

1. Убедитесь, что типы баз данных всех серверов – «mdb», с помощью команды:

```
sudo slapcat -n0
```

Если тип БД отличается, то во всех дальнейших командах нужно заменить mdb на текущий тип БД.

2. Отключите все возможные репликации баз и серверов.

3. Убедитесь, что содержимое баз резервируемых серверов идентично.

4. Сделайте бэкап конфигурации и БД сервера-поставщика в текущей папке с помощью команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-conf-and-data-backup.sh
```

Для восстановления конфигурации и БД OpenLDAP в случае ошибок резервирования, выполните команды:

```
cd /opt/AstraRegul/Astra.Security
sudo sh ./openldap-conf-and-data-restore.sh
```

5. Остановите все программы, взаимодействующие с серверами OpenLDAP.

6. Убедитесь, что системное время резервируемых серверов одинаковое, иначе синхронизация изменений будет работать в одну сторону.

7. На время настройки резервирования одного из серверов остановите остальные резервируемые сервера OpenLDAP.

Чтобы настроить разнонаправленное резервирование:

1. На любом из резервируемых серверов создайте файл конфигурацииopenldap-enable-syncreplmultiprovider-server.ldif со следующим содержанием:

```
##############################################################
# Check/modify database type (bdb/hdb/mbd/...), server ID (unique number),
# address of provider, binddn, credentials, searchbase.
##############################################################

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: syncprov.la

##############################################################

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100

##############################################################

dn: cn=config
changetype: modify
replace: olcServerID
olcServerID: 1

dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncRepl
```

```
olcSyncRepl:
  rid=001
  provider=ldap://192.168.56.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
olcSyncRepl:
  rid=002
  provider=ldap://192.168.57.102:389
  bindmethod=simple
  binddn="cn=admin,dc=maxcrc,dc=com"
  credentials="secret"
  searchbase="dc=maxcrc,dc=com"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
-
add: olcMirrorMode
olcMirrorMode: TRUE

dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Отступ в каждой строке внутри конструкции olcSyncRepl обязательно должен содержать по два пробела.

2. Измените файл конфигурации следующим образом:

2.1. В строке **olcServerID: 1** придумайте и укажите идентификатор сервера;

olcServerID должен быть уникальным для каждого резервируемого сервера.

2.2. Замените **«mdb»** на текущий тип БД, если он отличается, в строках:

- «dn: olcDatabase={1}mdb,cn=config»;
- «dn: olcDatabase={1}mdb,cn=configdn: olcDatabase={1}mdb,cn=config»;
- «dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config»

2.3. Добавьте столько конструкций **olcSyncRepl**, сколько серверов участвуют в резервировании помимо текущего. Каждая конструкция **olcSyncRepl** описывает один из резервируемых серверов.

Внутри одного сервера параметры **rid** разных конструкций **olcSyncRepl** должны иметь уникальные значения.

2.4. В каждой конструкции **olcSyncRepl** укажите **IP-адрес** и **порт** сервера, который она описывает, в строке параметра **provider**.

2.5. Замените «"dc=maxcrc,dc=com"» на «"dc=nodomain"», если не выполняли переименование домена, в строках:

- «binddn="cn=admin,dc=maxcrc,dc=com"»;
- «searchbase="dc=maxcrc,dc=com"».

3. Для применения внесенных изменений выполните команду:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f openldap-enable-syncrepl-multiproviderserver.ldif
```

4. Перезапустите сервер:

```
sudo systemctl restart slapd
```

5. Повторите все описанные действия на каждом из резервируемых серверов.

6. Настройте Агент Astra.Security:

6.1. Перейдите к файлу конфигурации **astra.security.agent.xml**, расположенному по следующему пути:

/opt/AstraRegul/Astra.Security

Добавьте в секцию тега <**LdapHosts**> строки с IP-адресами и портами всех резервируемых серверов:

```
<LdapHosts>
    <LDAPServer Address="127.0.0.1" Port="389"/>
    <LDAPServer Address="172.16.13.167" Port="389"/>
</LdapHosts>
```

6.2. Перезапустите службу:

```
sudo systemctl restart Astra.Security
```

После настройки **последовательно включите** все сервера OpenLDAP.

Подключитесь напрямую к каждой базе и убедитесь, что ошибок не возникло.

Для проверки внесите изменения в конфигурацию на одном из серверов. Убедитесь, что эти изменения появились и на других серверах.

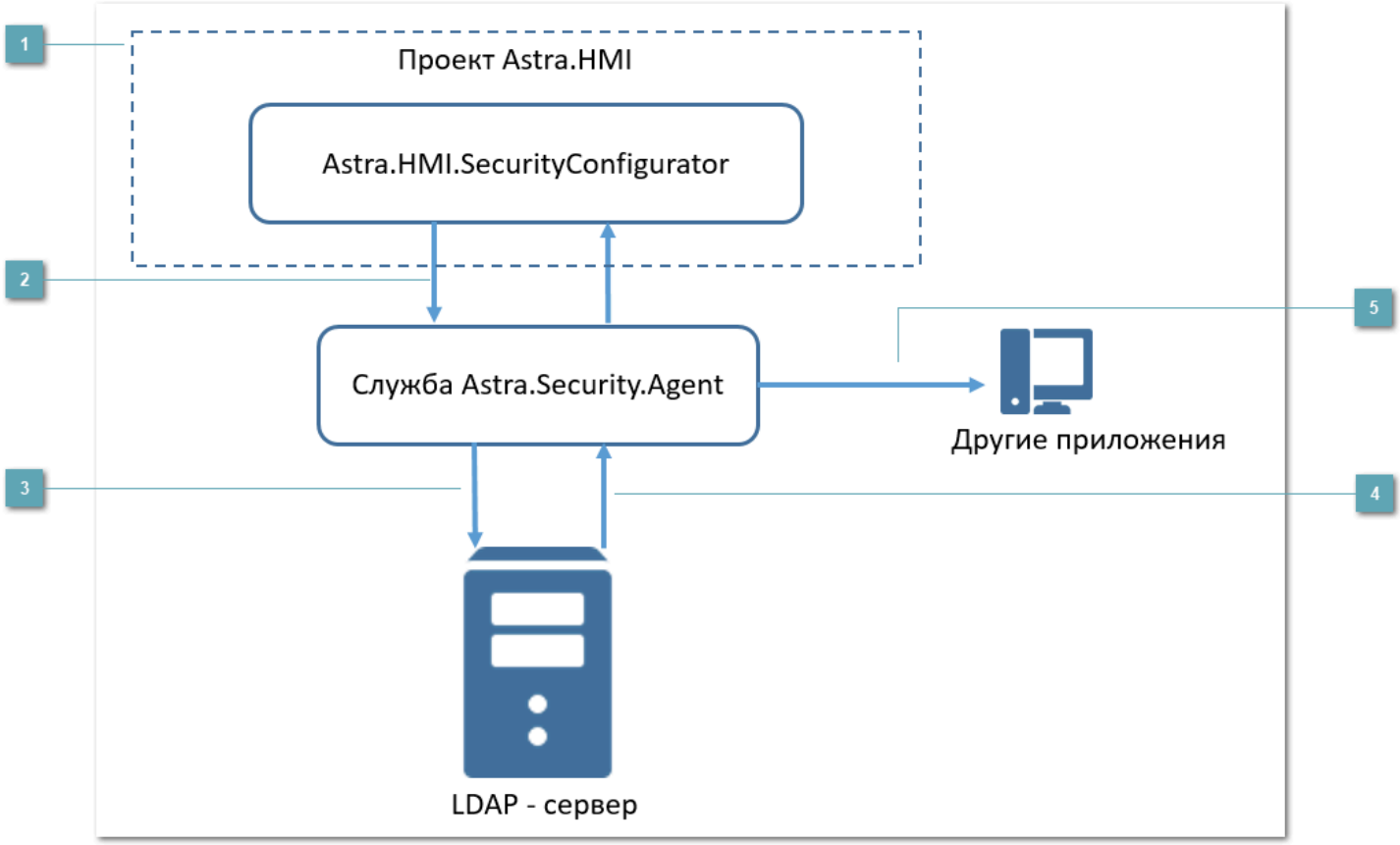
1.2.3. Astra.HMI.SecurityConfigurator

Astra.HMI.SecurityConfigurator – приложение, предназначенное для конфигурирования подсистемы безопасности Astra.Security.

Под конфигурированием подсистемы безопасности подразумевается:

- создание учетных записей пользователей для предоставления им доступа к возможностям проекта;
- объединение пользователей в группы для предоставления им одинаковых возможностей;
- создание прав доступа к возможностям проекта и группировка прав в приложения;
- создание ролей и назначение их пользователям или группам;
- назначение прав пользователям, группам и/или ролям.

Используйте Astra.HMI.SecurityConfigurator как самостоятельное приложение, или встраивайте его в проекты автоматизации, разработанные в Astra.HMI.



1 Astra.HMI.SecurityConfigurator

Astra.HMI.SecurityConfigurator встраивается в проект автоматизации, реализованный в среде разработки Astra.HMI, или вызывается как самостоятельное приложение.

2 Astra.HMI.SecurityConfigurator –> Astra.Security

С помощью Astra.HMI.SecurityConfigurator меняется конфигурация подсистемы безопасности Astra.Security. Новая конфигурация передается Агент Astra.Security.

3 Агент Astra.Security –> LDAP-сервер

Агент Astra.Security записывает на LDAP-сервер конфигурацию, где она хранится в виде каталогов LDAP.

4 LDAP-сервер –> Агент Astra.Security

LDAP-сервер по запросу предоставляет информацию о пользователях, группах, ролях и их возможностях Агент Astra.Security.

5 Агент Astra.Security –> Приложения

Агент Astra.Security предоставляет информацию всем приложениям, запрашивающим ее.

Требования к окружению

Для работы Astra.HMI.SecurityConfigurator должны быть установлены:

- Astra.HMI – среда разработки проектов автоматизации;
- Astra.Security – подсистема безопасности, которую можно конфигурировать в соответствии с нуждами проекта;

- Astra.Domain – компонент, обеспечивающий взаимодействие между Astra.HMI и Astra.Security;
- Astra.HMI.Security – компонент, обеспечивающее взаимодействие приложения с Astra.Security;
- Astra.HMI.Tables – компонент, обеспечивающий отображение компонентов приложения в проекте в режиме исполнения.

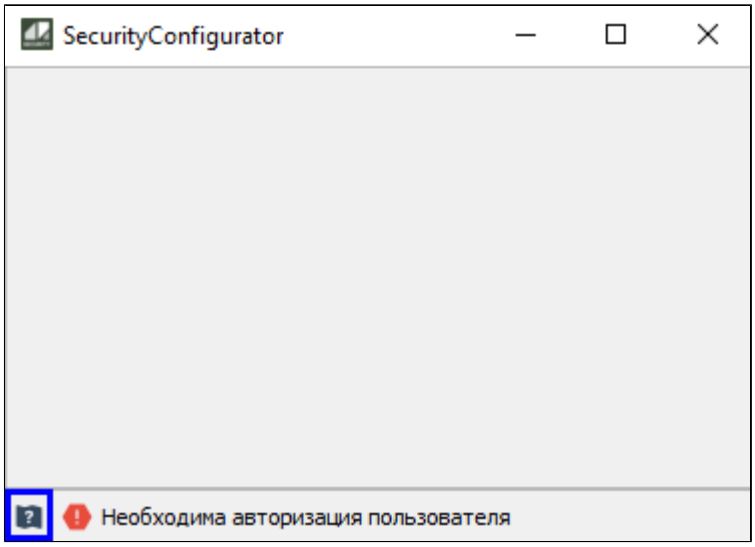
Если приложение встраивается в проект Astra.HMI в качестве расширения, потребуется библиотека Astra.HMI.CommonLib.

Если приложение используется в веб-версии проекта автоматизации, то установите дополнительно:

- Astra.HMI.WebViewer – для просмотра проектов Astra.HMI в веб-интерфейсе;
- Astra.HMI.Security.WebViewer – для работы компонентов Astra.HMI.Security в веб-интерфейсе;
- Astra.HMI.Tables.WebViewer – для работы компонентов Astra.HMI.Tables в веб-интерфейсе.

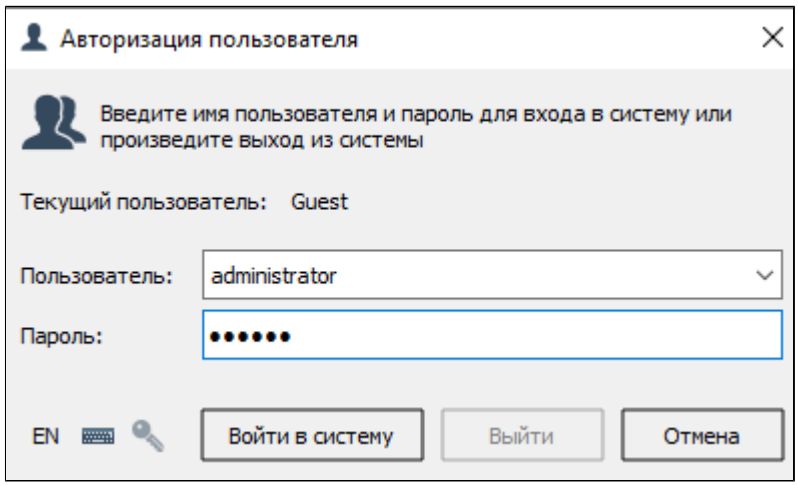
1.2.3.1. Вход с учетными данными

Чтобы приступить к работе, необходимо авторизоваться. Для авторизации нажмите на иконку в левом нижнем углу.

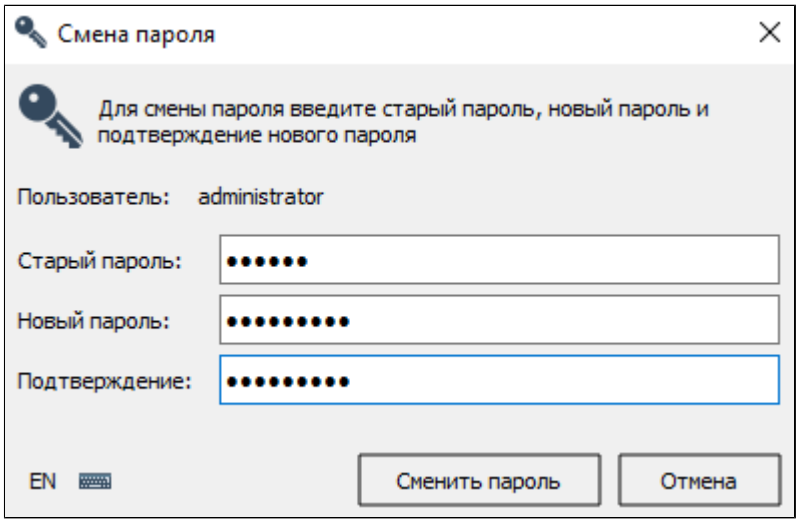


По умолчанию, если конфигурация Astra.Security не создана, каталог на LDAP-сервере и учетная запись администратора Astra.Security создадутся при первом запуске конфигуратора.

Имя каталога	AstraSecurity
Логин	administrator
Пароль	задается при установке LDAP-сервера (по умолчанию - secret)

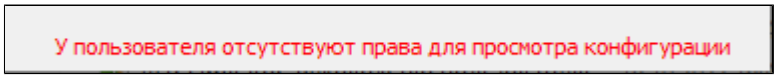


Введите указанные учетные данные и нажмите Войти в систему. Появится диалоговое окно, требующее обновления пароля. Нажмите ОК и в открывшемся окне введите новый пароль.



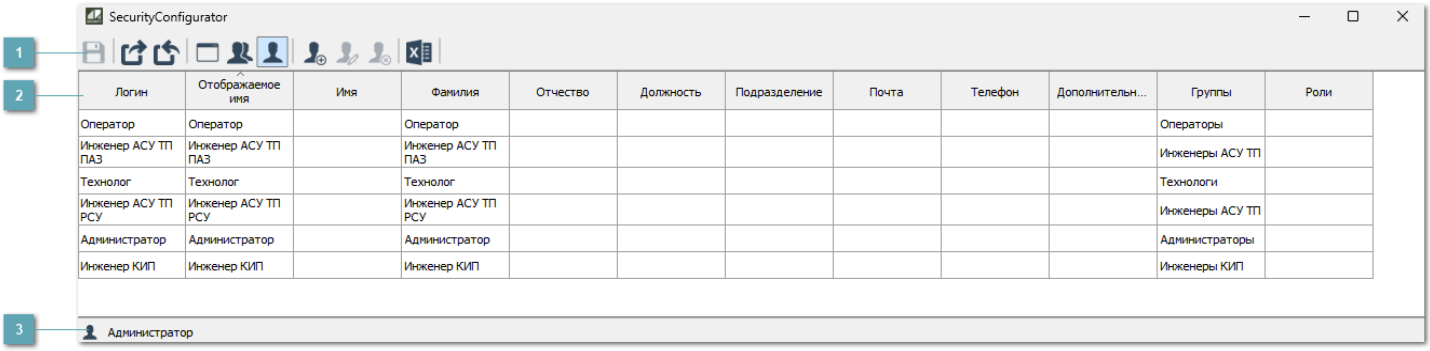
Если же необходимо конфигурировать созданный ранее каталог и использовать имеющуюся учетную запись администратора, настройте Агент Astra.Security. Настройка Агент Astra.Security описана в документе на подсистему безопасности Astra.Security.

Если введены учетные данные пользователя, обладающего правами на просмотр и изменение конфигурации, соответствующие действия будут доступны. В противном случае доступ будет отклонен, и в окне конфигуратора появится сообщение об этом.



Вы можете создать собственную учетную запись администратора, наделив его правами на просмотр и изменение конфигурации, а затем удалить учетную запись «administrator».

1.2.3.2. Интерфейс



1 Панель инструментов

Содержит функциональные кнопки.

2 Список пользователей

Отображает список созданных пользователей.

3 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных приложений.

Показать группы пользователей

Отображение списка созданных групп пользователей.

Показать список пользователей

Отображение списка созданных пользователей.

Добавить учетную запись пользователя

Добавление учетной записи пользователя.

Редактировать учетную запись пользователя

Редактирование учетной записи пользователя.

Удалить учетную запись пользователя

Удаление учетной записи пользователя.

Экспортировать в файл

Экспорт списка пользователей в файл.

1.2.3.2.1.1. Сохранить изменения

После редактирования прав настроек Astra.HMI.SecurityConfigurator нажмите Сохранить изменения.

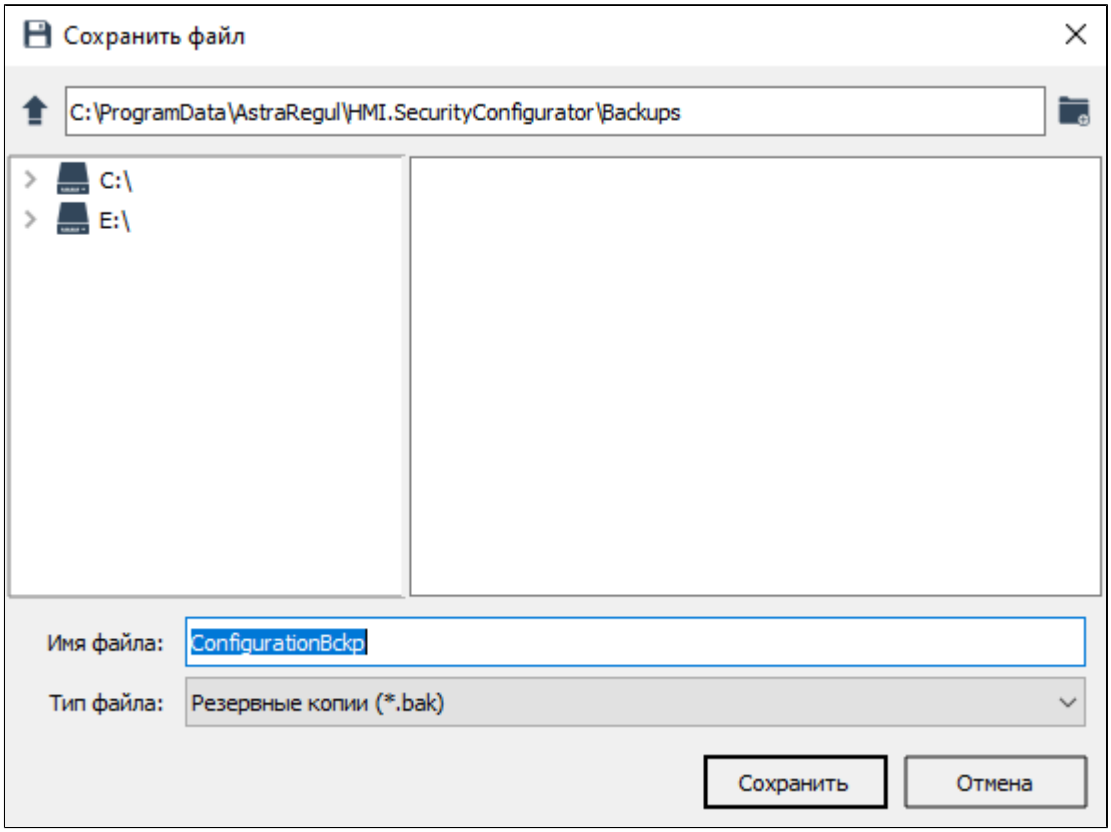
Если вы не выполните сохранение изменений, по завершении редактирования настроек Security.Configurator предложит сохранить изменения.

1.2.3.2.1.2. Сохранить резервную копию конфигурации

Для сохранения текущей конфигурации подсистемы безопасности можно создать ее резервную копию. При необходимости сохраненную конфигурацию можно восстановить из резервной копии.

Чтобы создать резервную копию текущей конфигурации, нажмите кнопку "Сохранить резервную копию конфигурации".

Откроется диалоговое окно, где будет предложено ввести полный путь к папке для хранения резервной копии и имя резервной копии. Укажите оба параметра и нажмите Сохранить.



› Чтобы перейти к папке на уровень выше, нажмите .

› Чтобы создать в указанном расположении новую папку, нажмите  .

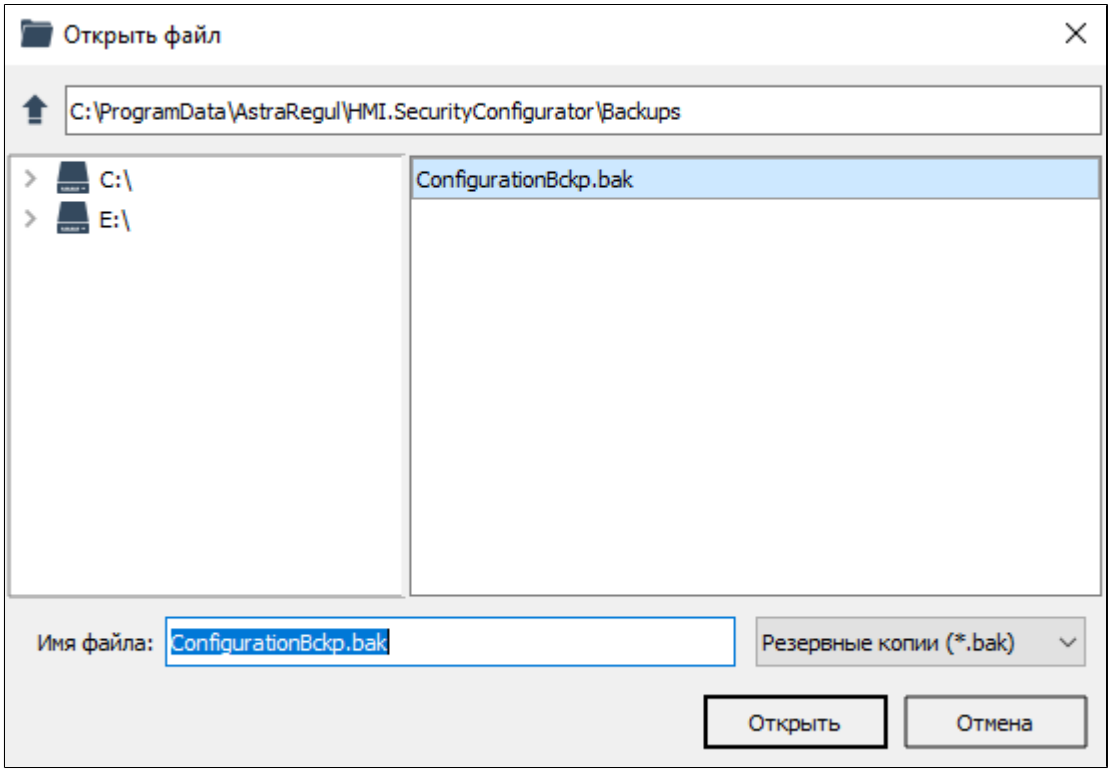
Для создания резервной копии нужно обладать правами на чтение, создание и изменение файлов в указанной папке.

Путь к папке для хранения резервных копий конфигурации указывается в свойстве BackupsPath компонента SecurityConfigurator. Если значение не указано, то по умолчанию используется путь к папке Backups, создающейся в папке проекта при первом сохранении резервной копии. Подробнее свойство описано в Справочнике API.

1.2.3.2.1.3. Восстановить конфигурацию из резервной копии

Чтобы восстановить конфигурацию из резервной копии, нажмите кнопку "Восстановить конфигурацию из резервной копии".

Откроется диалоговое окно, где будет предложено ввести полный путь к файлу резервной копии и полное имя резервной копии. Укажите оба параметра и нажмите Открыть.



Для создания резервной копии нужно обладать правами на чтение, создание и изменение файлов в указанной папке.

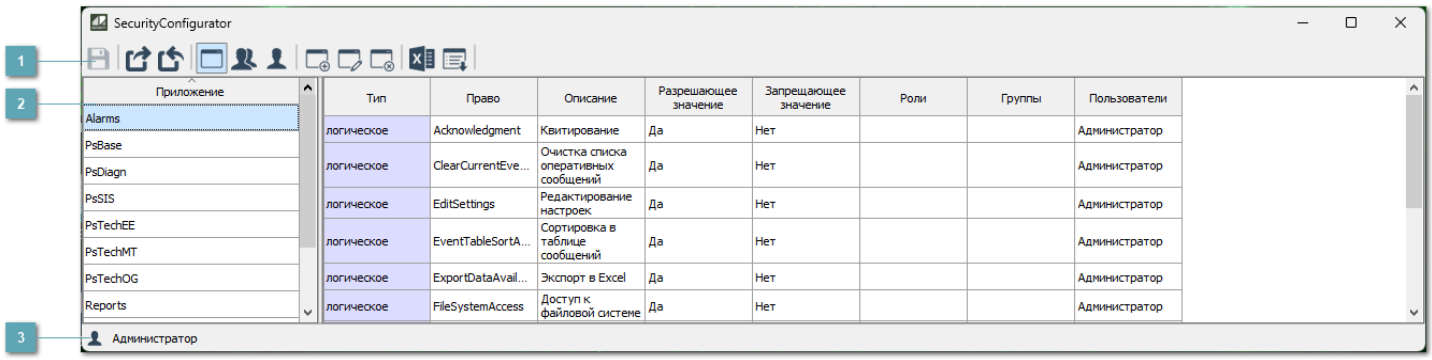
Удаленная учетная запись вновь появится в списке учетных записей, а удаленное приложение – в списке приложений.

1.2.3.2.1.4. Показать список приложений

Возможности пользователей в проекте определяются наличием у них разрешений и запретов на определенные действия. Информация о том, разрешено или запрещено пользователю какое-либо действие, хранится в праве. Для удобства права сгруппированы в приложения.

Создание и редактирование приложений и прав ведется в окне редактирования приложений. Чтобы открыть окно, нажмите кнопку "Показать список приложений" на панели инструментов.

Откроется следующее окно:



1 Панель инструментов

Содержит функциональные кнопки.

2 Список приложений

Отображает список созданных приложений и таблицу с описанием прав.

3 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1.4.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных приложений.

Показать группы пользователей

Отображение списка созданных групп пользователей.

Показать список пользователей

Отображение списка созданных пользователей.

Добавить приложение

Добавление нового приложения.

 Редактировать приложение

Редактирование приложения.

 Удалить приложение

Удаление приложения.

 Экспортировать в файл

Экспорт списка прав приложения в файл.

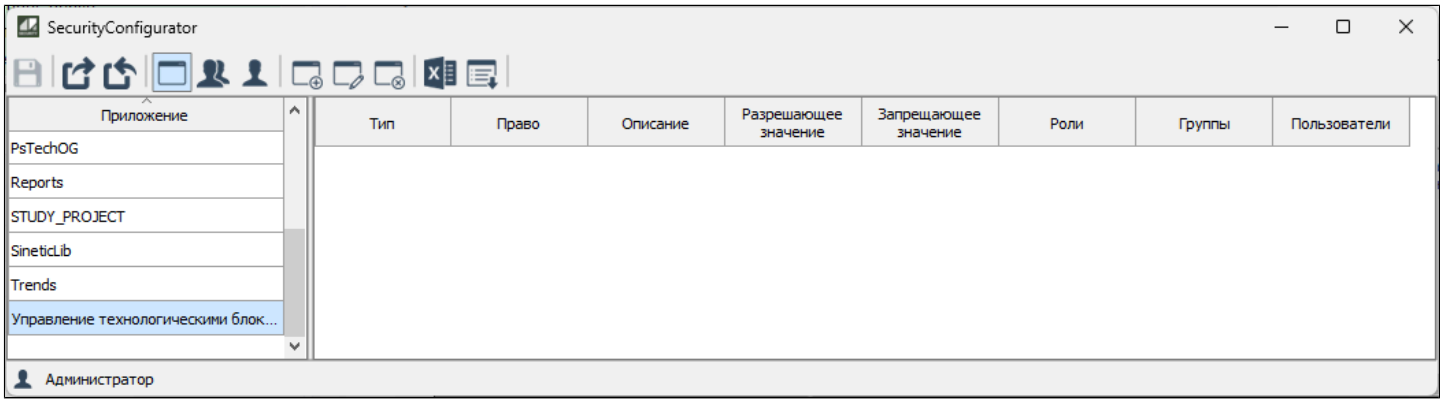
 Импортировать приложение из файла

Импорт приложения из файла.

1.2.3.2.1.4.1.1. Добавить приложение

Чтобы создать новое приложение нажмите кнопку "Добавить приложение" на панели инструментов.

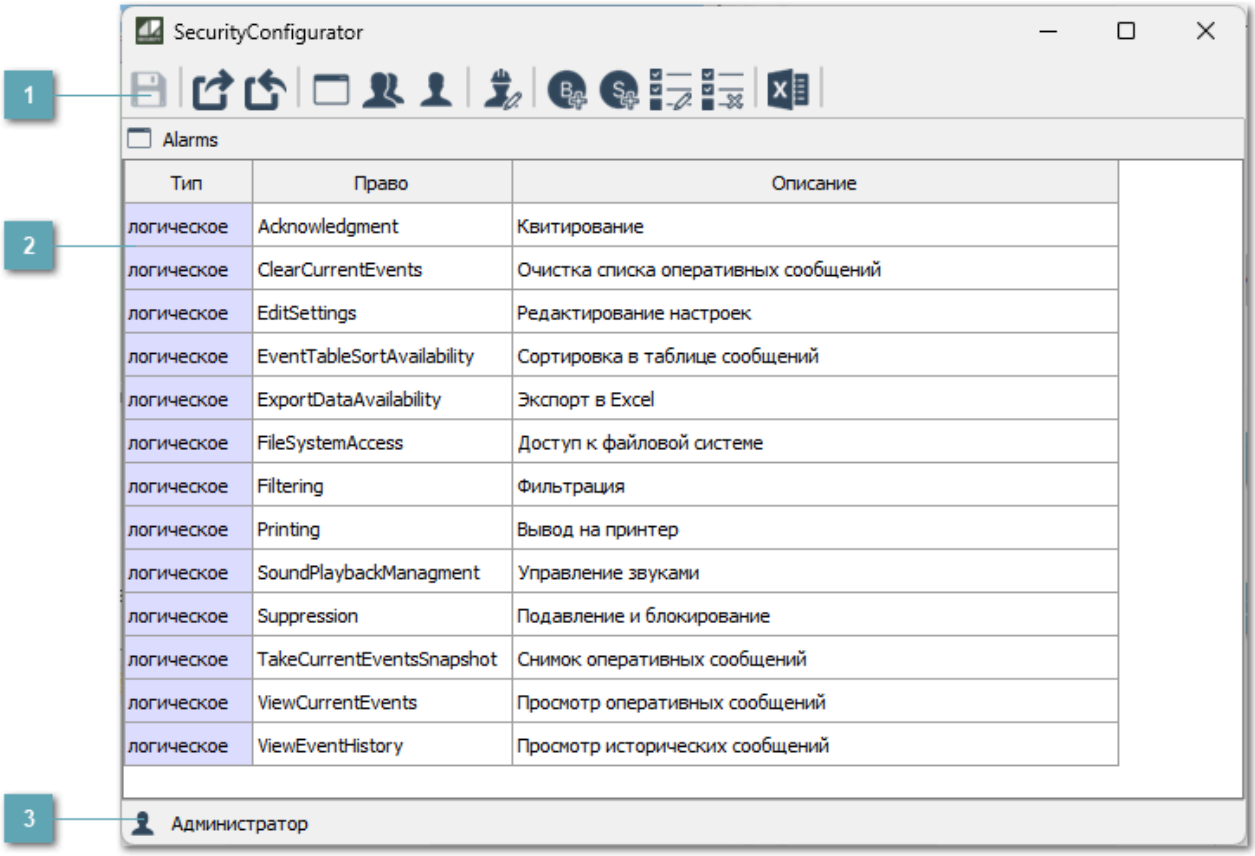
В открывшемся окне введите название приложения и нажмите кнопку "ОК". Приложение будет создано и появится в списке приложений.



1.2.3.2.1.4.1.2. Редактировать приложение

Для добавления прав в приложение нажмите кнопку "Редактировать приложение" на панели инструментов или дважды кликните по строке приложения в списке.

Откроется окно добавления прав.



1 Панель инструментов

Содержит функциональные кнопки.

2 Список прав

Отображает список прав, относящихся к приложению.

3 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1.4.1.2.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных приложений.

Показать группы пользователей

Отображение списка созданных групп пользователей.

Показать список пользователей

Отображение списка созданных пользователей.

Редактирование ролей

Редактирование ролей.

Добавить логическое право

Добавление логического права.

Добавить строковое право

Добавление строкового плана.

Изменить выделенное право

Редактирование выделенного права.

Удалить выделенное право

Удаление выделенного права.

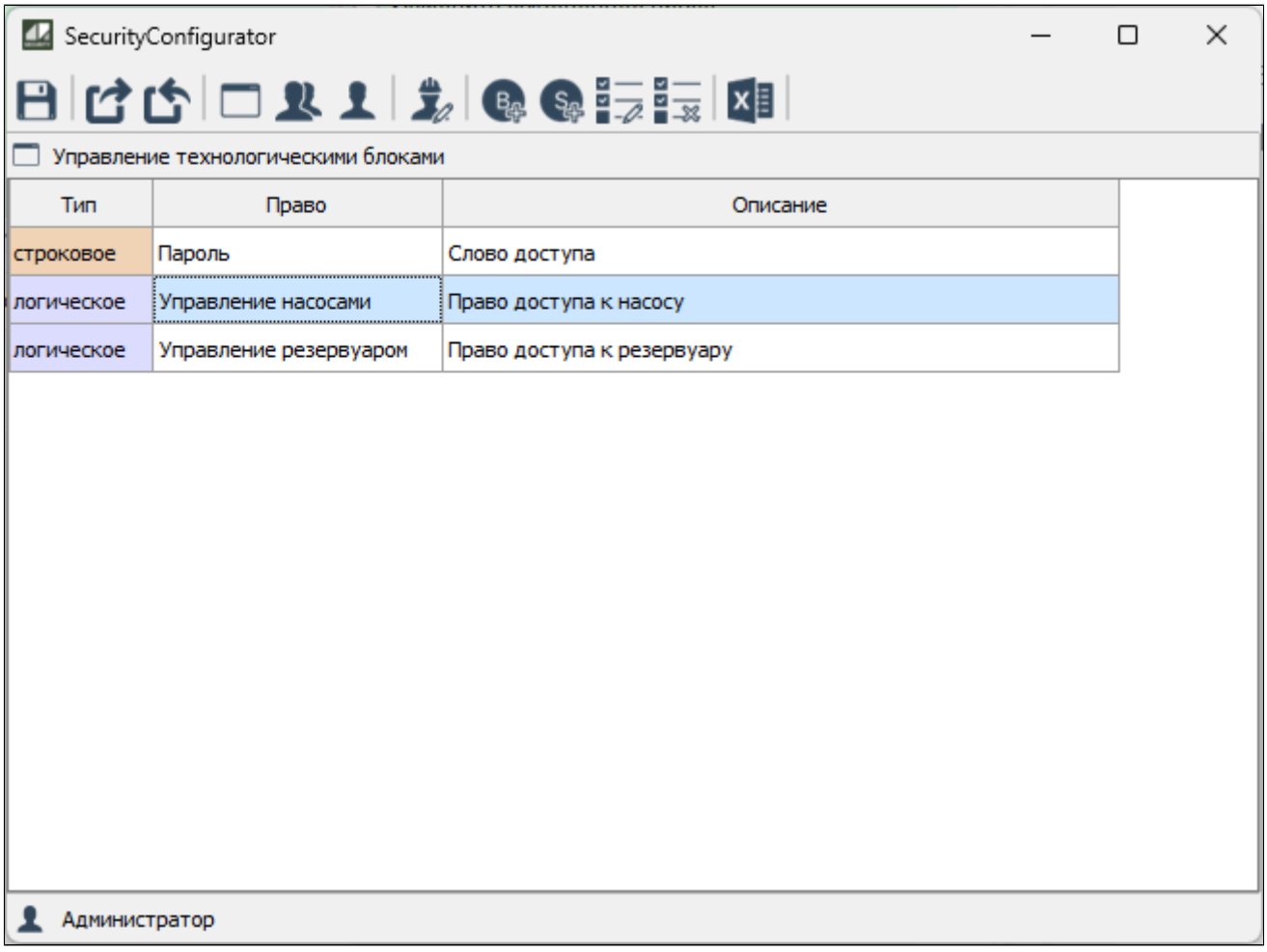
Экспортировать в файл

Экспорт списка прав приложения в файл.

1.2.3.2.1.4.1.2.1.1. Добавить логическое право

Чтобы разграничить доступ будущих пользователей к технологическим объектам, необходимо создать право доступа. Для этого нажмите кнопку "Добавить логическое право" на панели инструментов.

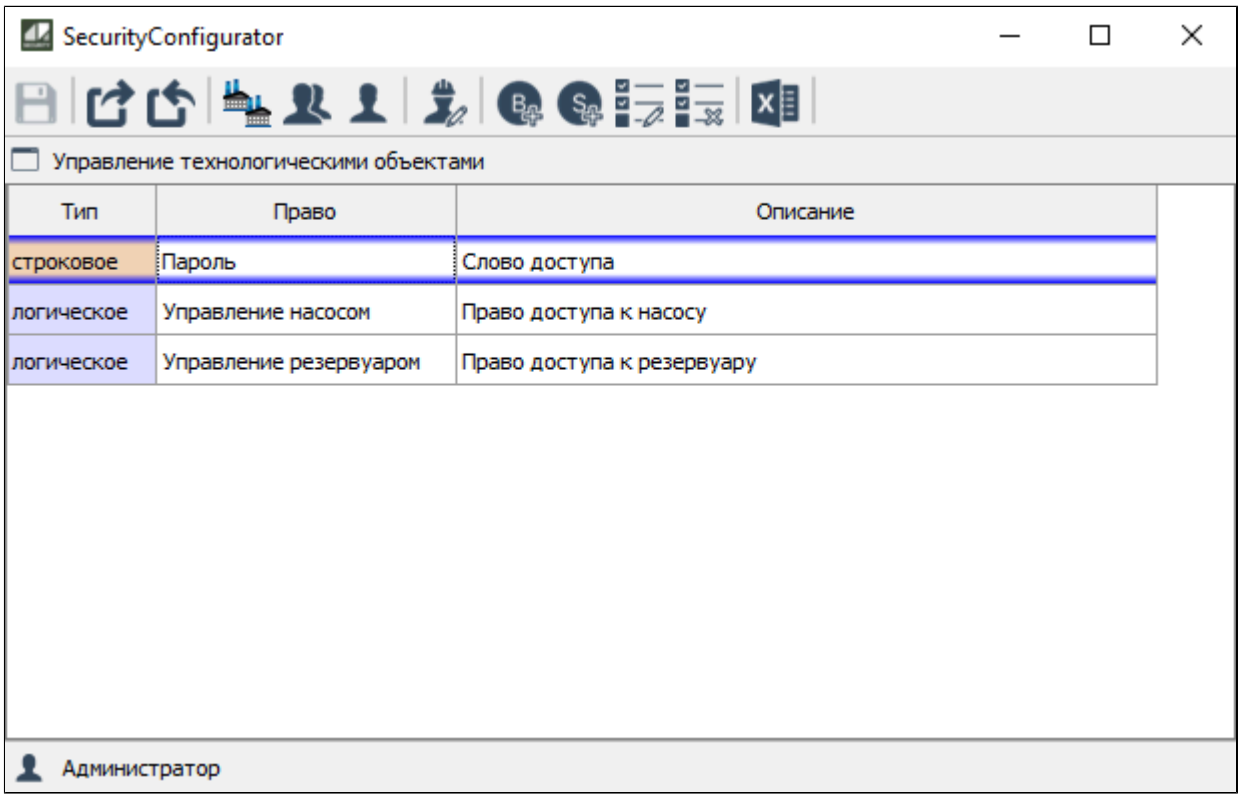
В открывшемся окне введите название права и его описание и нажмите кнопку "Добавить". Право будет создано и появится в списке прав приложения.



1.2.3.2.1.4.1.2.1.2. Добавить строковое право

Чтобы добавить строковое право, нажмите кнопку "Добавить строковое право" на панели инструментов.

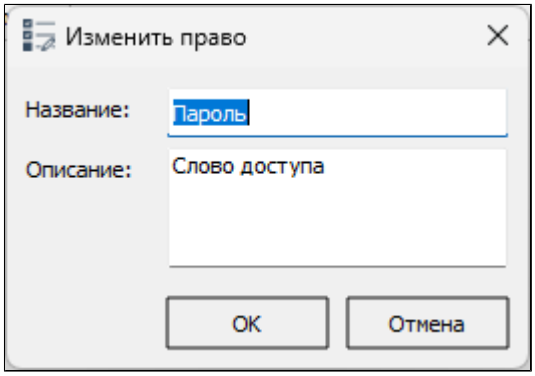
В открывшемся окне введите название права и его описание и нажмите кнопку "Добавить". Право будет создано и появится в списке прав приложения.



1.2.3.2.1.4.1.2.1.3. Изменить выделенное право

Чтобы изменить название и/или описание выделенного права, нажмите кнопку "Изменить выделенное право" на панели управления.

В открывшемся окне внесите необходимые изменения и нажмите кнопку "ОК".



1.2.3.2.1.4.1.2.1.4. Удалить выделенное право

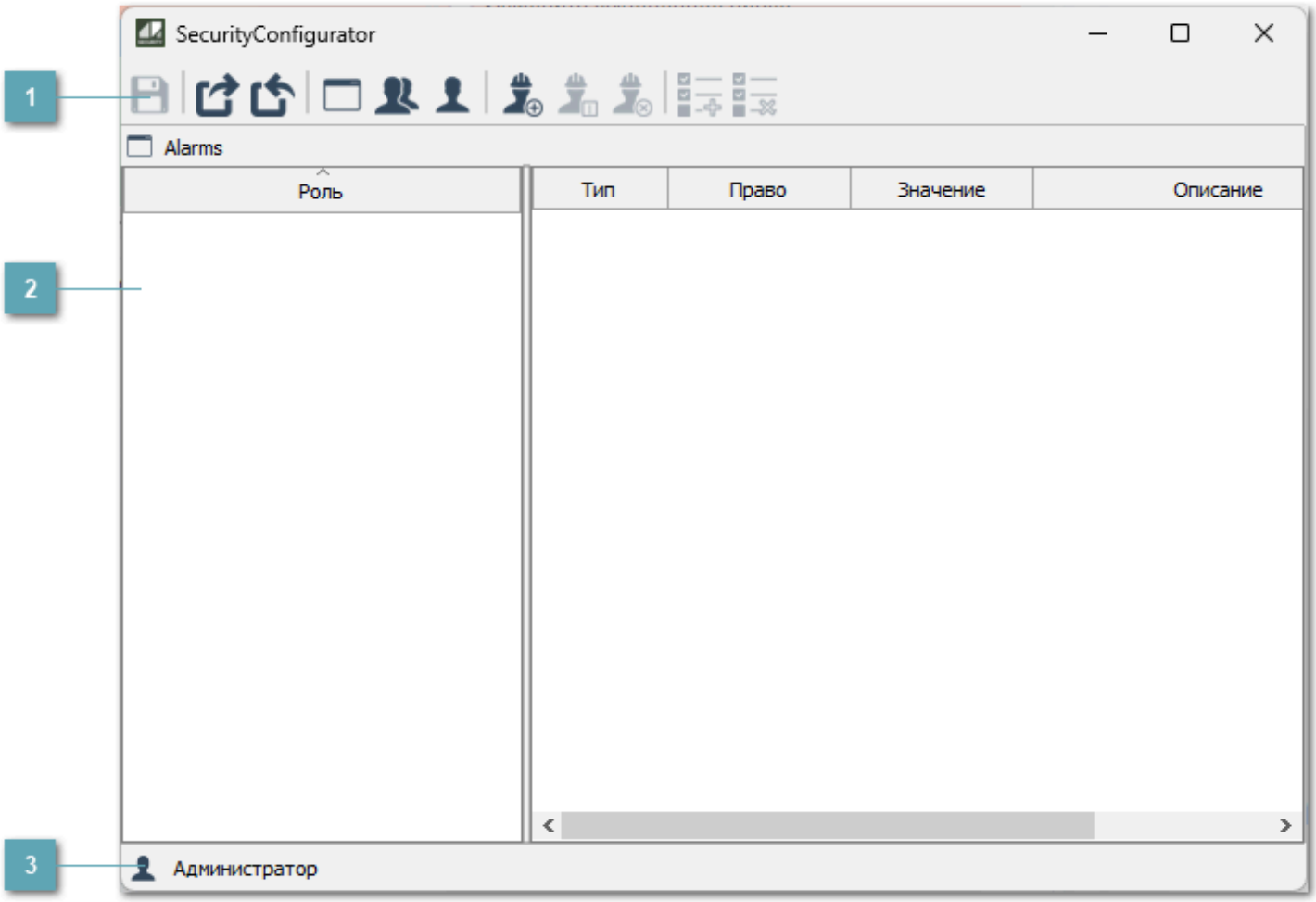
Чтобы удалить выделенное право, нажмите кнопку "Удалить выделенное право" на панели инструментов.

1.2.3.2.1.4.1.2.1.5. Редактирование ролей

Внутри приложения можно создать роль. Роль – это совокупность значений каждого права приложения. Роль может быть назначена как пользователю, так и группе.

Чтобы добавить роль нажмите Редактирование ролей на панели инструментов.

Откроется окно редактирования ролей.



1 Панель инструментов

Содержит функциональные кнопки.

2 Список ролей

Отображает список ролей (с описанием назначенных прав), относящихся к приложению.

3 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1.4.1.2.1.5.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных групп пользователей.

Показать группы пользователей

Отображение списка созданных пользователей.

Показать список пользователей

Добавление учетной записи пользователя.

Добавить роль

Добавление роли.

 Сменить имя роли

Изменение имени роли.

 Удалить роль

Удаление роли.

 Добавить права

Добавление прав роли.

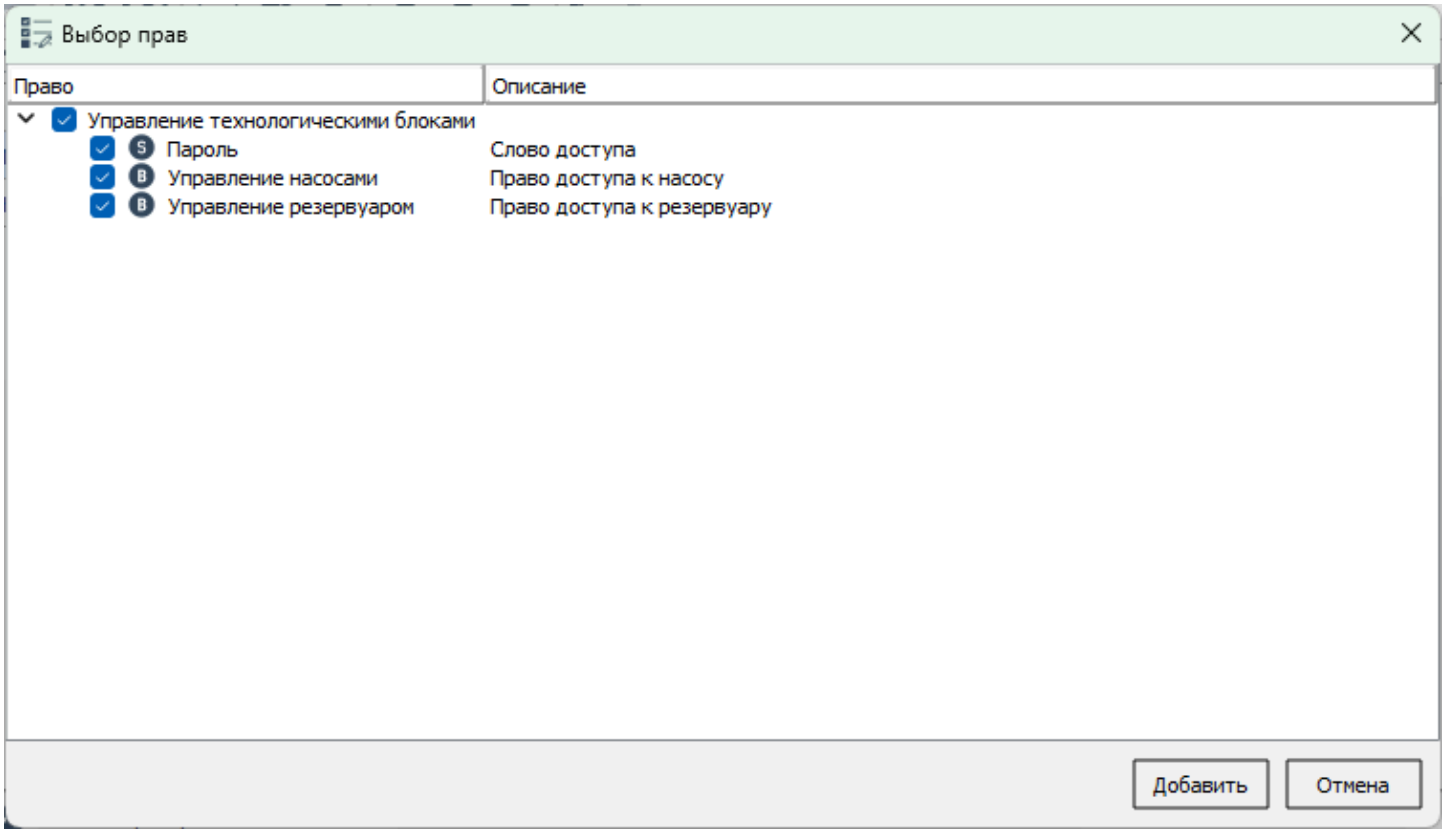
 Удалить права

Удаление прав роли.

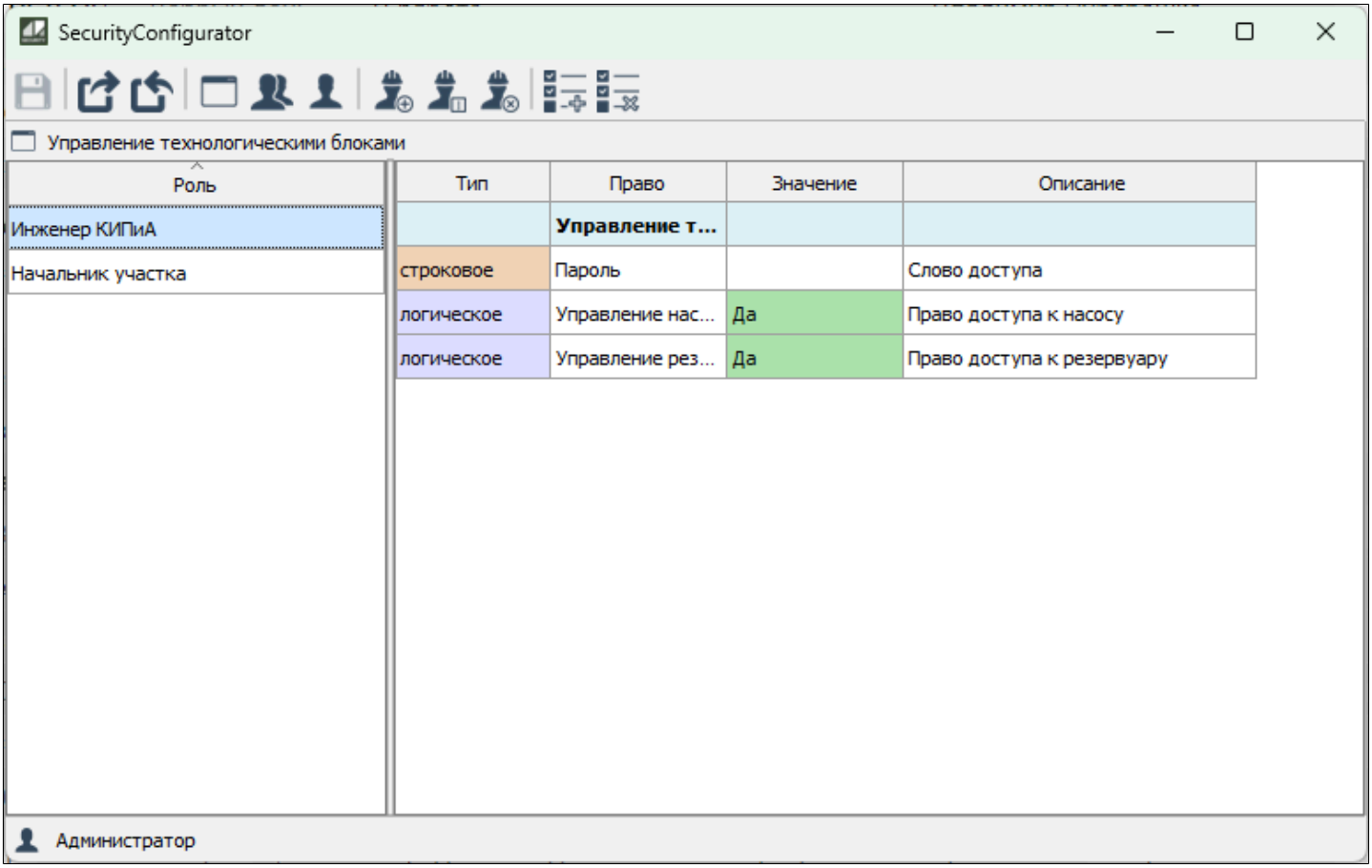
1.2.3.2.1.4.1.2.1.5.1.1. Добавить роль

Чтобы создать новую роль, нажмите кнопку "Добавить роль" на панели инструментов.

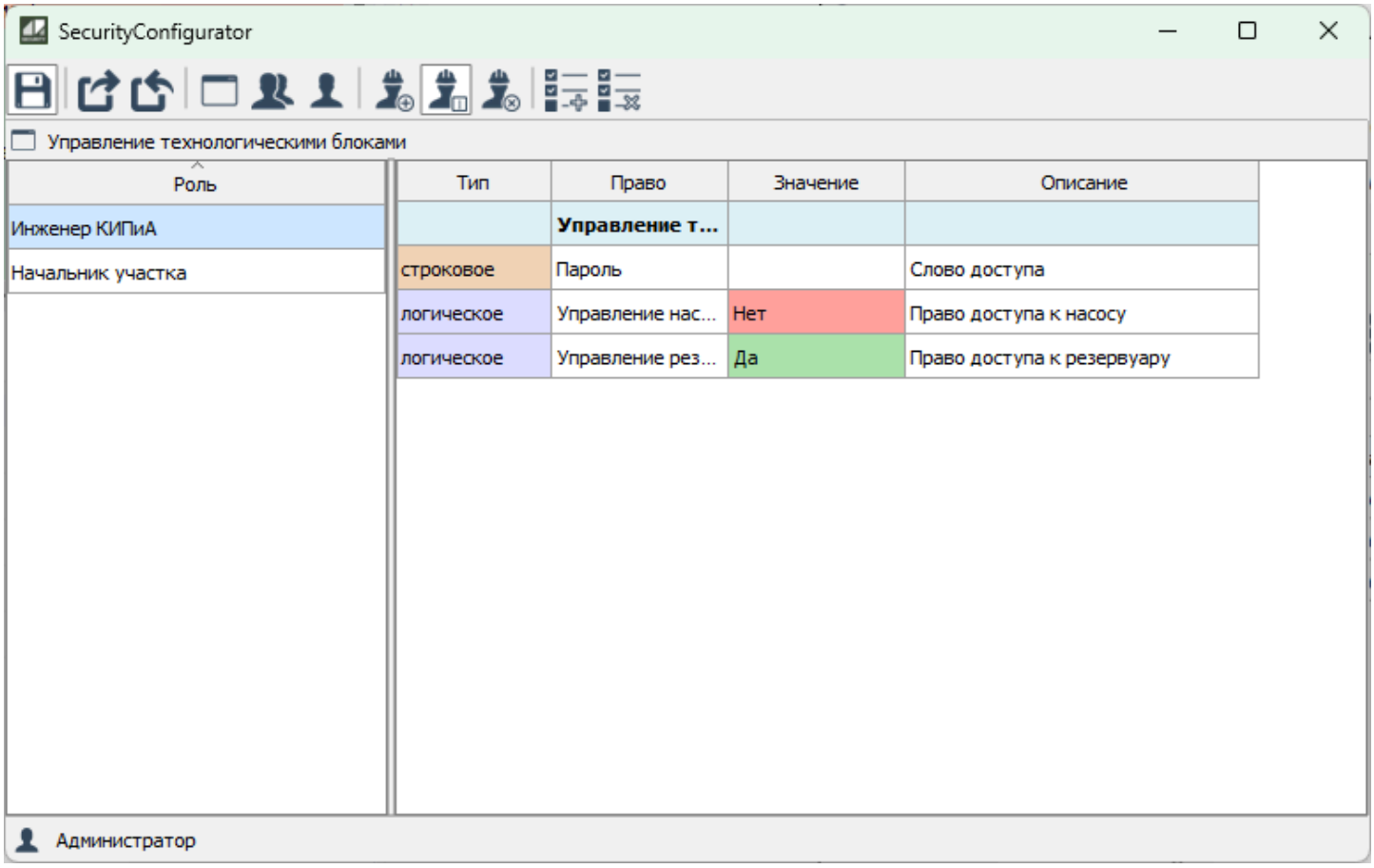
В открывшемся окне введите название роли и нажмите ОК. Роль появится в списке ролей. Для назначения прав роли необходимо нажать Добавить права.



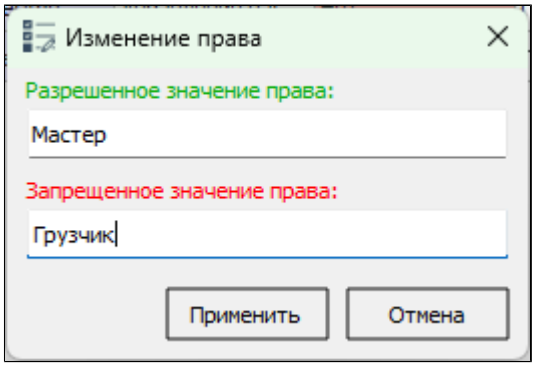
Укажите разрешающие значения для обоих прав роли.



Вы можете изменять права роли, изменяя разрешающее значение. Для этого дважды кликните по значению логического права. Для логического права значение изменится автоматически на противоположное.



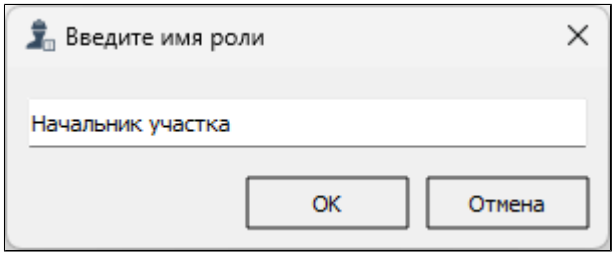
Для строкового права вы можете задать разрешенное и запрещенное значения права. Для этого дважды кликните по значению строкового права. В открывшемся окне введите разрешенное и запрещенное значения.



1.2.3.2.1.4.1.2.1.5.1.2. Сменить имя роли

Чтобы изменить имя роли, нажмите кнопку "Сменить имя роли" на панели инструментов.

В открывшемся окне введите новое имя роли и нажмите кнопку "ОК".



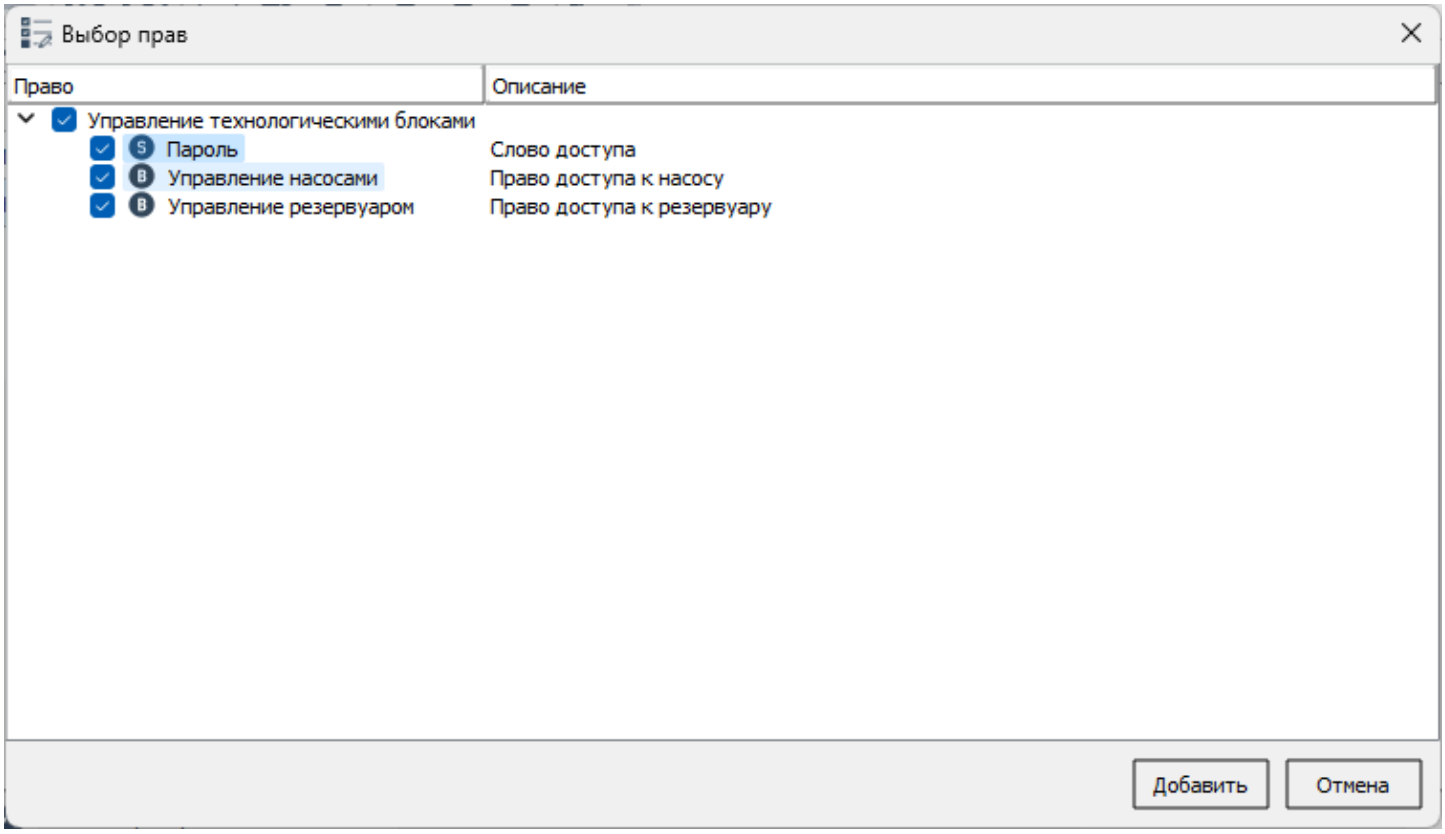
1.2.3.2.1.4.1.2.1.5.1.3. Удалить роль

Чтобы удалить роль, нажмите кнопку "Удалить роль" на панели инструментов.

1.2.3.2.1.4.1.2.1.5.1.4. Добавить права

Чтобы добавить права роли, нажмите кнопку "Добавить права" на панели инструментов.

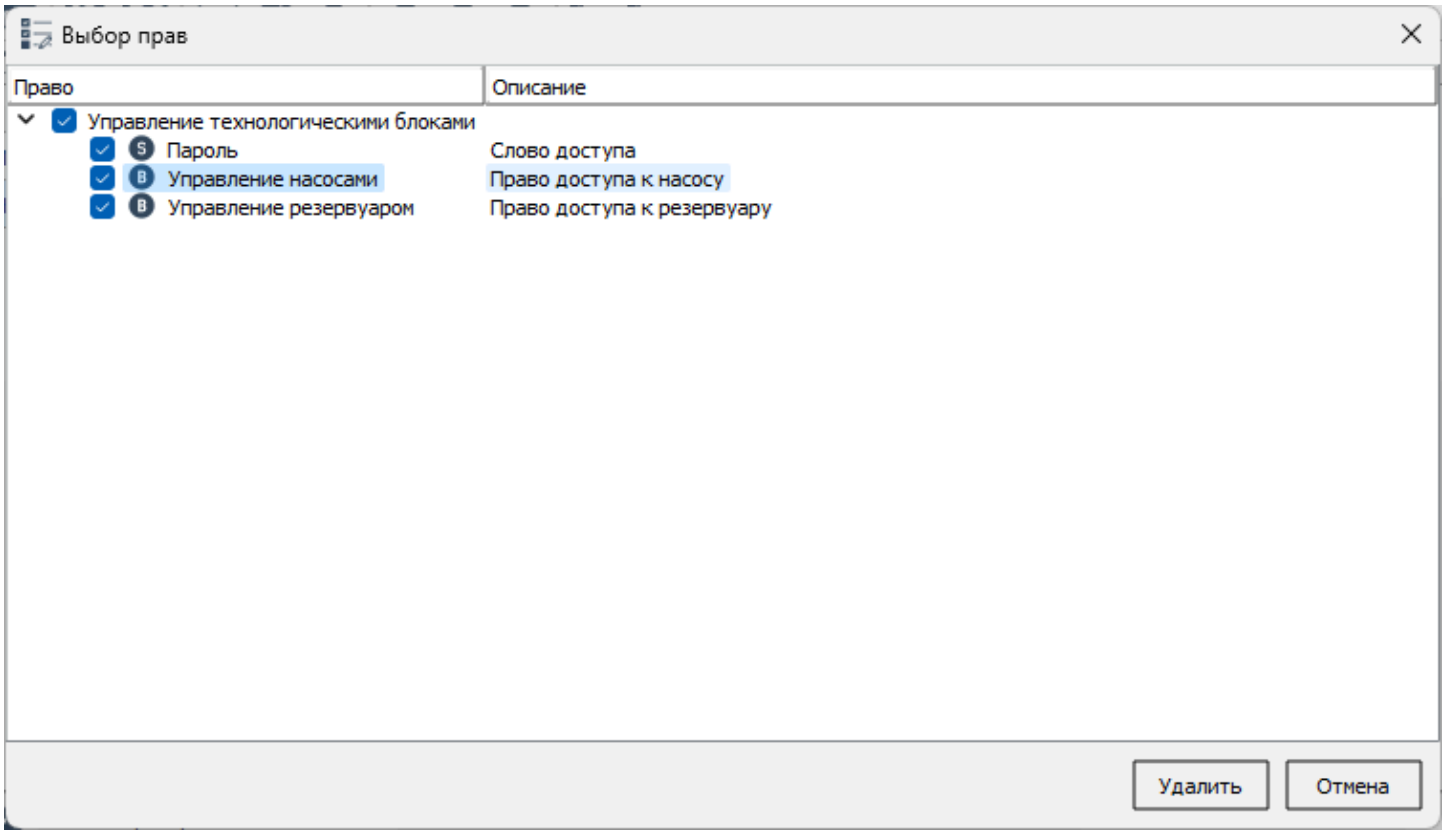
В открывшемся окне выберите права, которые необходимо добавить роли.



1.2.3.2.1.4.1.2.1.5.1.5. Удалить права

Чтобы удалить права роли, нажмите кнопку "Удалить права" на панели инструментов.

В открывшемся окне выберите права, которые необходимо удалить.



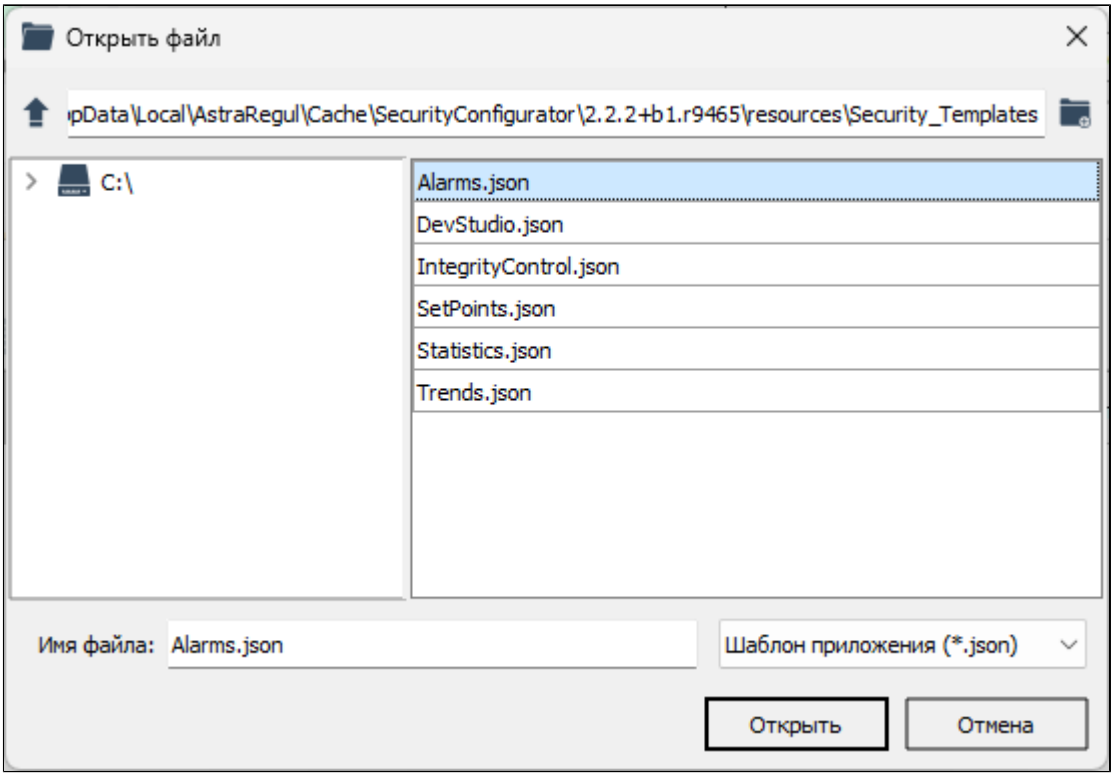
1.2.3.2.1.4.1.3. Удалить приложение

Чтобы удалить созданное приложение, выделите его, нажмите кнопку "Удалить приложение на панели инструментов" и подтвердите удаление.

1.2.3.2.1.4.1.4. Импортировать приложение из файла

Чтобы импортировать приложение из файла, нажмите кнопку "Импортировать приложение из файла" на панели инструментов.

В открывшемся окне выберите файл с приложением для импорта.



Шаблоны прав приложений

- Astra.Security
- Astra.HMI.Alarms
- Astra.HMI.Trends
- Astra.HMI.IntegrityControl
- Astra.HMI.Statistics

Права стандартного приложения Astra.Security

Право	Название	Описание
AttempsTimeOut	Таймаут при превышении количества попыток входа, мин	Длительность блокировки пользователя при превышении количества неудачных попыток, указанных в MaxAttempsCount
ConfigurationAccess	Редактирование конфигурации	Предоставляет доступ к редактированию конфигурации Astra.Security. Этим правом наделяется администратор Astra.Security
EditSettings	Изменение настроек	Предоставляет доступ к настройкам Astra.HMI.SecurityConfigurator. Не применяется в текущей версии Astra.HMI.SecurityConfigurator
InteractiveLogon	Интерактивный вход	Разрешает/запрещает пользователю вход. Устаревшее право Astra.Security, функцию которого выполняет блокировка. Для разрешения или запрета входа используйте блокировку учетной записи пользователя
LowerCount	Количество в пароле символов в нижнем регистре	Устанавливает минимально допустимое количество символов в нижнем регистре в пароле
MaxAttempsCount	Количество попыток входа, шт	Устанавливает количество неудачных попыток входа для пользователя. Если

		пользователь не войдет за указанное количество попыток, то блокируется на время, указанное в AttempsTimeOut
MaxIdleTime	Максимальное время бездействия, мин	Устанавливает время бездействия пользователя. Таймер сбрасывается при каждом взаимодействии пользователя с АРМ – щелчком или движением мыши, вводом текста с клавиатуры и т.д. Если же за указанное время пользователь не взаимодействует с АРМ, происходит автоматический выход пользователя из системы. Эффективным значением права является максимальное значение
NumberCount	Количество цифровых символов в пароле	Устанавливает минимально допустимое количество цифр в пароле
PasswordAge	Срок действия пароля, дней	Устанавливает границы срока действия пароля. До истечения минимального срока действия обновить пароль нельзя. После истечения максимального срока действия пароля попытки входа со старыми учетными данными будут отклоняться. Эффективным значением минимального срока является максимальное значение.

		Эффективным значением максимального срока является минимальное значение
PasswordComplexity	Сложность пароля	Обязательность использования в пароле следующих видов символов: › цифры › буквы нижнего регистра › буквы верхнего регистра › специальные символы
PasswordMinLength	Минимальная длина пароля	Устанавливает минимально допустимое количество символов в пароле
PasswordNotifyForChange	Уведомление о смене пароля, дней	Позволяет создать напоминание об истечении срока действия пароля для пользователя. За указанное до истечения пароля время будет отправлено напоминание о скором истечении срока действия пароля. Эффективным значением является максимальное значение
PasswordsInHistory	Количество паролей в истории	Устанавливает количество хранимых в истории паролей. Обновить пароль на такой же, как в истории паролей, не получится. Эффективным значением является максимальное значение
SessionDurationLimit	Максимальное время сессии, мин	Устанавливает длительность сессии пользователя. После истечения указанного времени происходит автоматический

<table>
<tr><td></td><td></td><td>выход пользователя из системы. Эффективным значением является минимальное значение</td></tr>
<tr><td>SpecialCount</td><td>Количество специальных символов в пароле</td><td>Устанавливает минимально допустимое количество специальных символов в пароле. К специальным символам относятся следующие символы:<table><tr><td>?</td><td>!</td><td>@</td><td>#</td><td>$</td><td>%</td><td>^</td><td>&</td><td>№</td><td><</td><td>></td></tr><tr><td>_</td><td>-</td><td>=</td><td>+</td><td>*</td><td>(</td><td>)</td><td>[</td><td>]</td><td>{</td><td>}</td></tr><tr><td>.</td><td>,</td><td>:</td><td>;</td><td>~</td><td>`</td><td>'</td><td>"</td><td>\</td><td>|</td><td>/</td></tr></table></td></tr>
<tr><td>UpperCount</td><td>Количество в пароле символов в верхнем регистре</td><td>Устанавливает минимально допустимое количество символов в верхнем регистре в пароле</td></tr>
<tr><td>ViewConfiguration</td><td>ViewConfiguration</td><td>Предоставляет доступ к просмотру конфигурации Astra.Security без возможности редактирования</td></tr>
<tr><td>WinKeysShortcutAccess</td><td>Доступ к сочетаниям клавиш Windows</td><td>Блокирует использование сочетаний клавиш (так называемых Hotkeys). Чтобы запретить использование сочетаний клавиш, укажите их в конфигурационном файле Агент Astra.Security. Подробнее об этом в документе на Astra.Security, в разделе, описывающем настройку агента</td></tr>
</table>

Права приложения Astra.HMI.Alarms

Право	Название	Описание
Acknowledgment	Квитирование	Доступ к возможностям квитирования
ClearCurrentEvents	Очистка списка оперативных сообщений	Доступ к функции очистки списка оперативных сообщений
EditSettings	Редактирование настроек	Предоставляет доступ к настройкам Astra.HMI.Alarms.
EventTableSortAvailability	Сортировка в таблице сообщений	Доступ к функциям сортировки таблицы событий
ExportDataAvailability	Экспорт в Excel	Доступ к функции экспорта событий в табличный файл
FileSystemAccess	Доступ к файловой системе	Доступ к файловой системе. Если "false", то включен режим ограничения доступа к файловой системе.
Filtering	Фильтрация	Если право задано: › не открывается окно "Фильтр пользователя" при перетаскивании сигнала в таблицу из Astra.Trends; › скрыты: › кнопка "Показывать подавленные сообщения" на панели инструментов; › кнопка "Фильтр отображения на панели инструментов" и соответствующая

		команда в контекстном меню; › команда "Расширенный фильтр" в выпадающем меню кнопки "Запросить данные"; › команды "Фильтр по объекту", "Фильтр по событию" и "Фильтр на основе буфера обмена" в контекстном меню таблицы; › команды "Отобразить события по объекту" и "Отобразить события" по всем объектам в контекстном меню объектов и сигналов в дереве сигналов.
Printing	Вывод на принтер	Доступ к функциям печати
SoundPlaybackManagment	Управление звуками	Доступ к управлению очередью звуков
Suppression	Подавление и блокирование	Доступ к функциям подавления и блокирования
TakeCurrentEventsSnapshot	Снимок оперативных сообщений	Доступ к функции снимка
ViewCurrentEvents	Просмотр оперативных сообщений	Доступ к оперативному режиму

ViewEventHistory	Просмотр исторических сообщений	Доступ к историческому режиму

Права приложения Astra.HMI.Trends

Право	Название	Описание
EditSettings	Редактирование настроек	Предоставляет доступ к настройкам Astra.HMI.Trends.
FileSystemAccess	Доступ к файловой системе	Доступ к файловой системе. Если "false", то включен режим ограничения доступа к файловой системе.

Права приложения Astra.HMI.IntegrityControl

Право	Название	Описание
CheckFiles	Проверка файлов	Доступ к проверке файлов.
CreateEtalon	Создание эталонных значений	Доступ к созданию эталонных значений.
FileSystemAccess	Доступность файловой системы	Доступ к файловой системе. Если "false", то включен режим ограничения доступа к файловой системе.

Права приложения Astra.HMI.Statistics

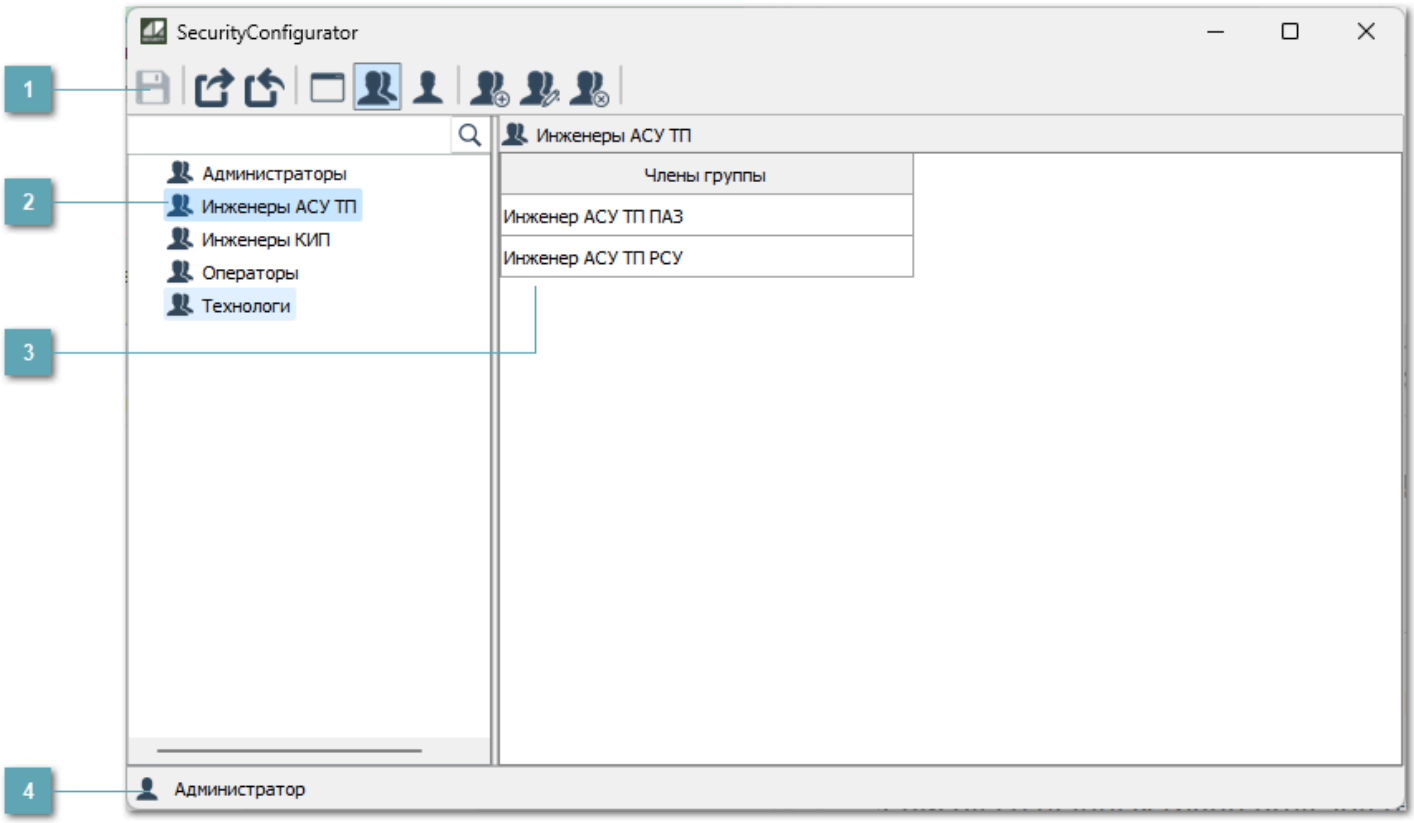
Право	Название	Описание
FileSystemAccess	Доступность файловой системы	Доступ к файловой системе. Если "false", то включен режим ограничения доступа к файловой системе.

1.2.3.2.1.5. Показать группы пользователей

Пользователей можно объединять в группы для удобства. Это помогает назначать одинаковые разрешения и запреты нескольким пользователям одновременно.

Чтобы посмотреть список созданных групп пользователей, нажмите кнопку "Показать группы пользователей" на панели инструментов.

Откроется окно, в котором будут отображены все созданные ранее группы.



1 Панель инструментов

Содержит функциональные кнопки.

2 Группы пользователей

Список созданных групп пользователей.

3 Члены группы

Список пользователей, относящихся к группе.

4 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1.5.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных приложений.

Показать группы пользователей

Отображение списка созданных групп пользователей.

Показать список пользователей

Отображение списка созданных пользователей.

Добавить группу

Добавление новой группы пользователей.

 Редактировать группу

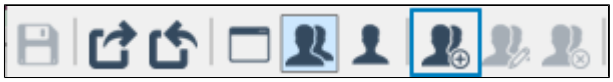
Редактирование группы пользователей.

 Удалить группу

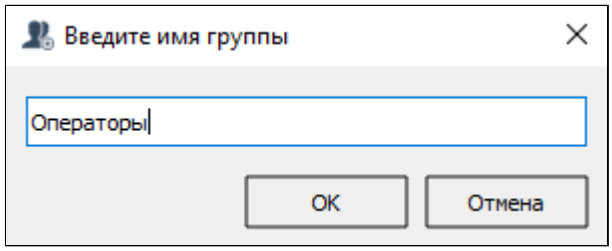
Удаление группы пользователей.

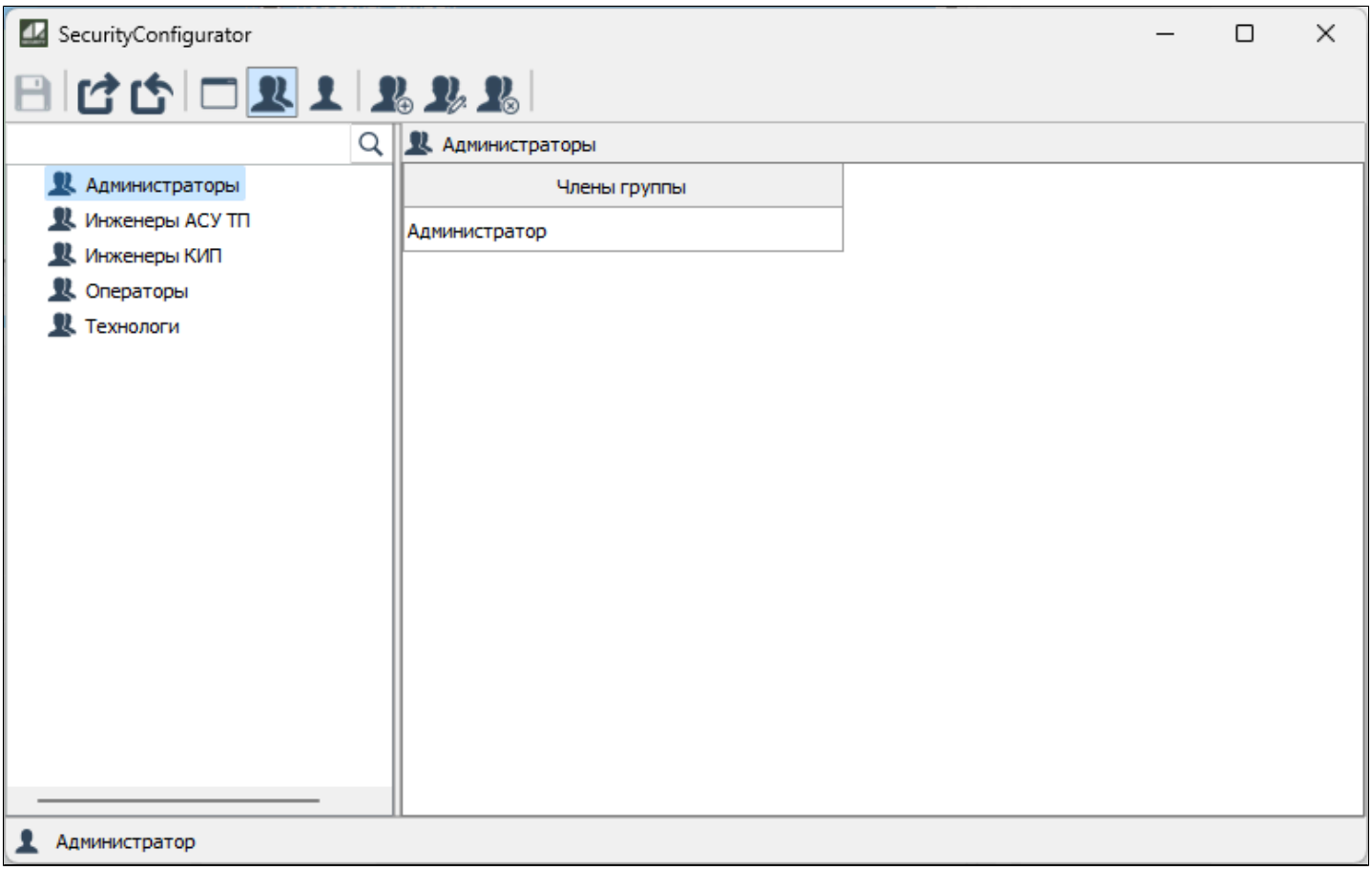
1.2.3.2.1.5.1.1. Добавить группу

Чтобы создать новую группу, нажмите кнопку "Добавить группу" на панели инструментов.



В открывшемся окне введите название группы и нажмите кнопку "ОК". Группа появится в списке групп.

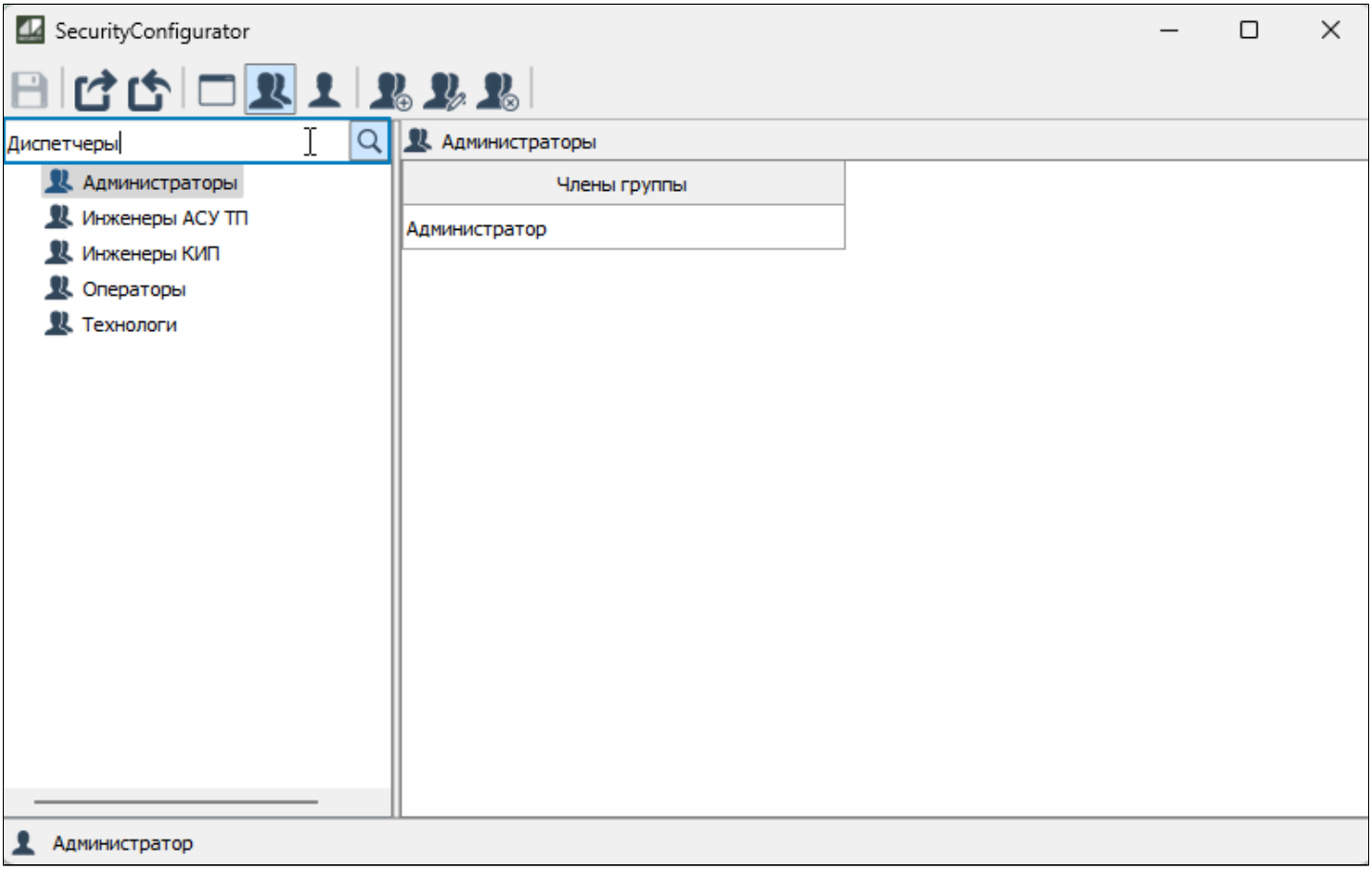




1.2.3.2.1.5.1.2. Редактировать группу

Чтобы редактировать группу, нажмите кнопку "Редактировать группу" на панели инструментов или дважды кликните по строке группы в списке.

Чтобы найти группу в списке групп по названию, воспользуйтесь панелью поиска над списком.



Для сортировки списка пользователей, состоящих в группе, нажмите на заголовок списка Члены группы. Первое нажатие сортирует список по возрастанию, второе - по убыванию, третье нажатие отключает сортировку.

1.2.3.2.1.5.1.3. Удалить группу

Чтобы удалить группу, выберите группу и нажмите кнопку "Удалить группу" на панели инструментов.

1.2.3.2.1.6. Показать список пользователей

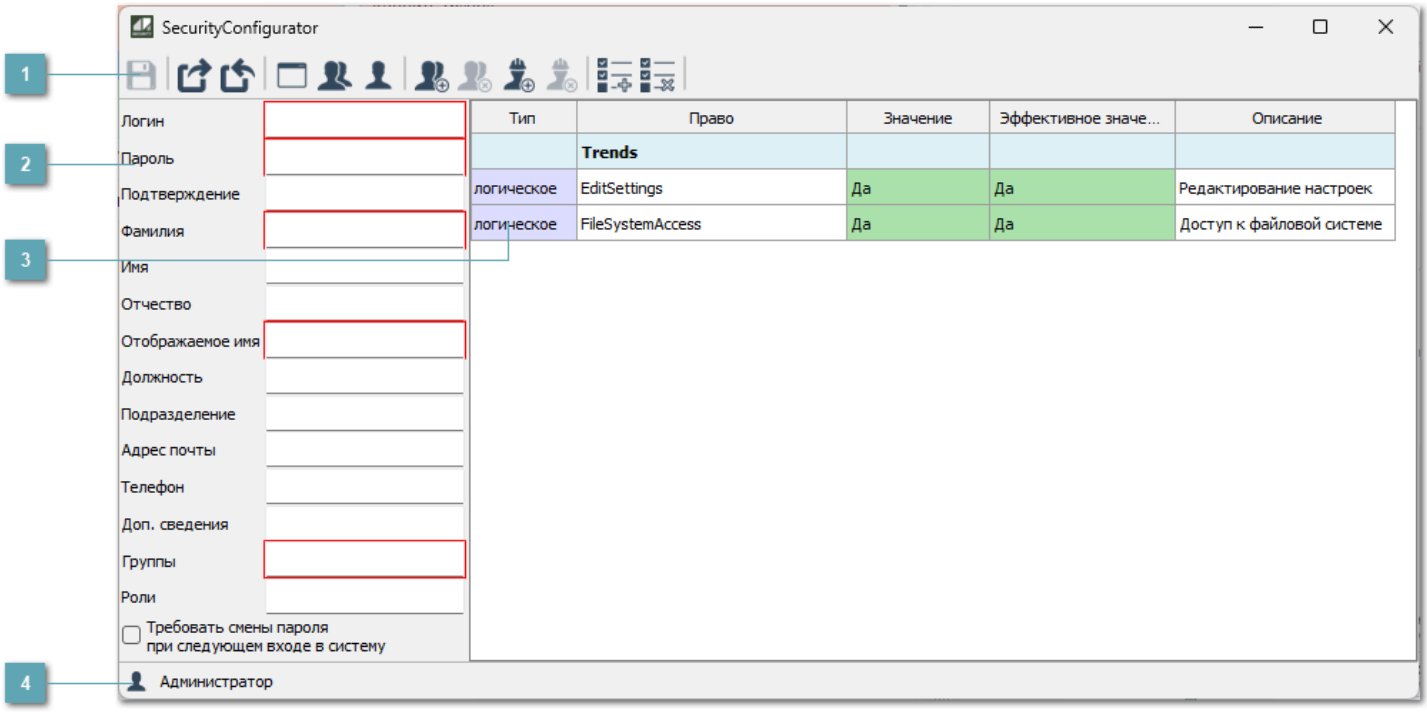
Создание и редактирование списка учетных записей ведется в окне редактирования учетных записей. Чтобы открыть окно, нажмите кнопку "Показать список пользователей на панели инструментов".

Появится список всех учетных записей, существующих в подсистеме безопасности Astra.Security.

1.2.3.2.1.7. Добавить учетную запись пользователя

Чтобы создать новую учетную запись пользователя, нажмите кнопку "Добавить учетную запись пользователя" на панели инструментов.

Откроется окно создания и редактирования учетной записи. Заполните все необходимые поля. Поля, выделенные красной рамкой, являются обязательными для заполнения.



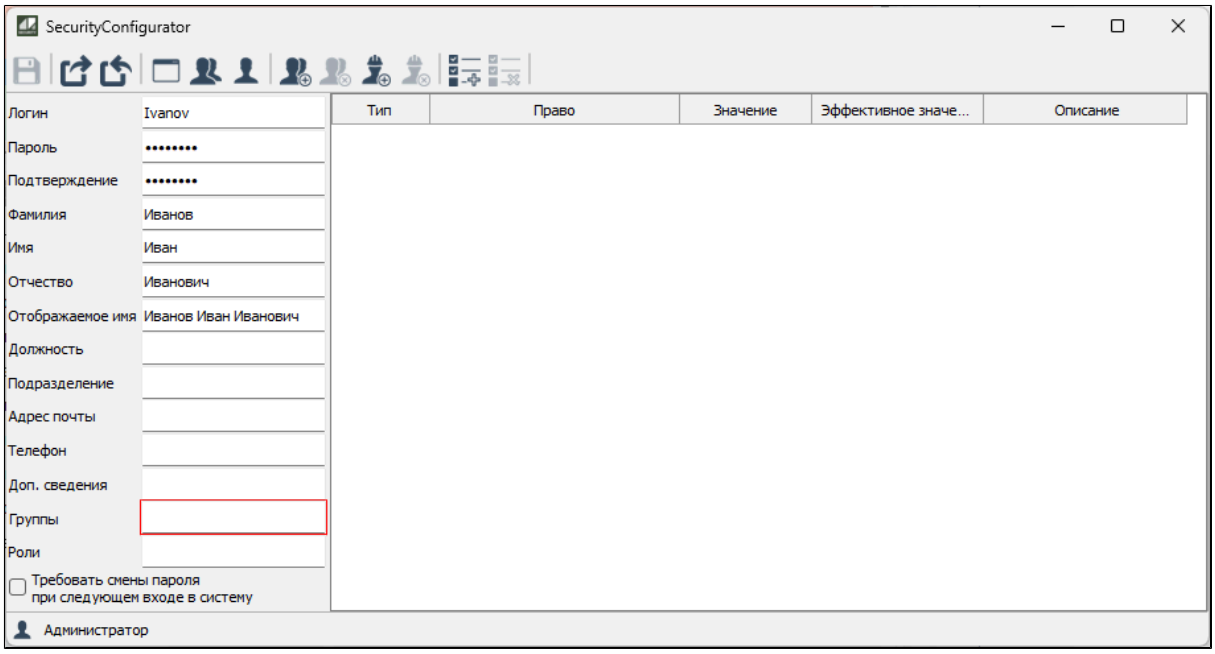
1 Панель инструментов

Содержит функциональные кнопки.

2 Данные учетной записи пользователя

Область добавления данных новых пользователей при регистрации.

Поле Отображаемое имя заполняется автоматически, его значение состоит из введенных фамилии, имени и отчества. Однако значение отображаемого имени можно менять.



Необходимость добавления пользователя хотя бы в одну группу регулируется свойством UserInAtLeastOneGroup компонента SecurityConfigurator:

- Если при разработке свойству указано значение «true», каждого создаваемого пользователя нужно будет добавлять в группу.
- Если же свойству указано значение «false», добавление в группу не будет обязательным, и, соответственно, поле Группы не будет выделено красной рамкой.

3 Список прав пользователя

Отображает список прав, которые будут доступны новому пользователю.

4 Строка состояния

Содержит информацию об авторизации пользователя.

1.2.3.2.1.7.1. Панель инструментов

Сохранить изменения

Сохранение внесенных изменений.

Сохранить резервную копию конфигурации

Сохранение резервной копии конфигурации.

Восстановить конфигурацию из резервной копии

Восстановление конфигурации из резервной копии.

Показать список приложений

Отображение списка созданных приложений.

Показать группы пользователей

Отображение списка созданных групп пользователей.

Показать список пользователей

Отображение списка созданных пользователей.

Добавить в группу

Добавление пользователя в группу.

 Удалить из группы

Удаление пользователя из группы.

 Добавить роли пользователю

Добавление роли пользователю.

 Лишить пользователя ролей

Лишение ролей пользователя.

 Добавить права

Добавление прав пользователю.

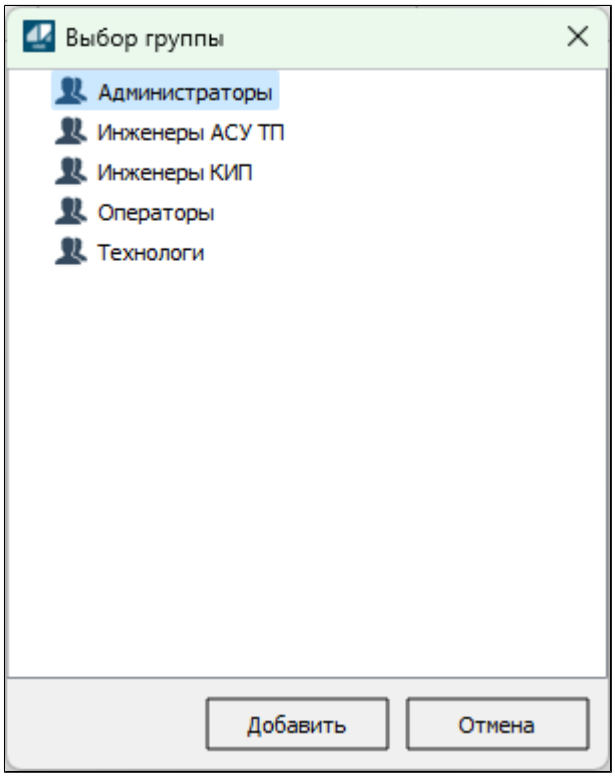
 Удалить права

Удаление прав пользователя.

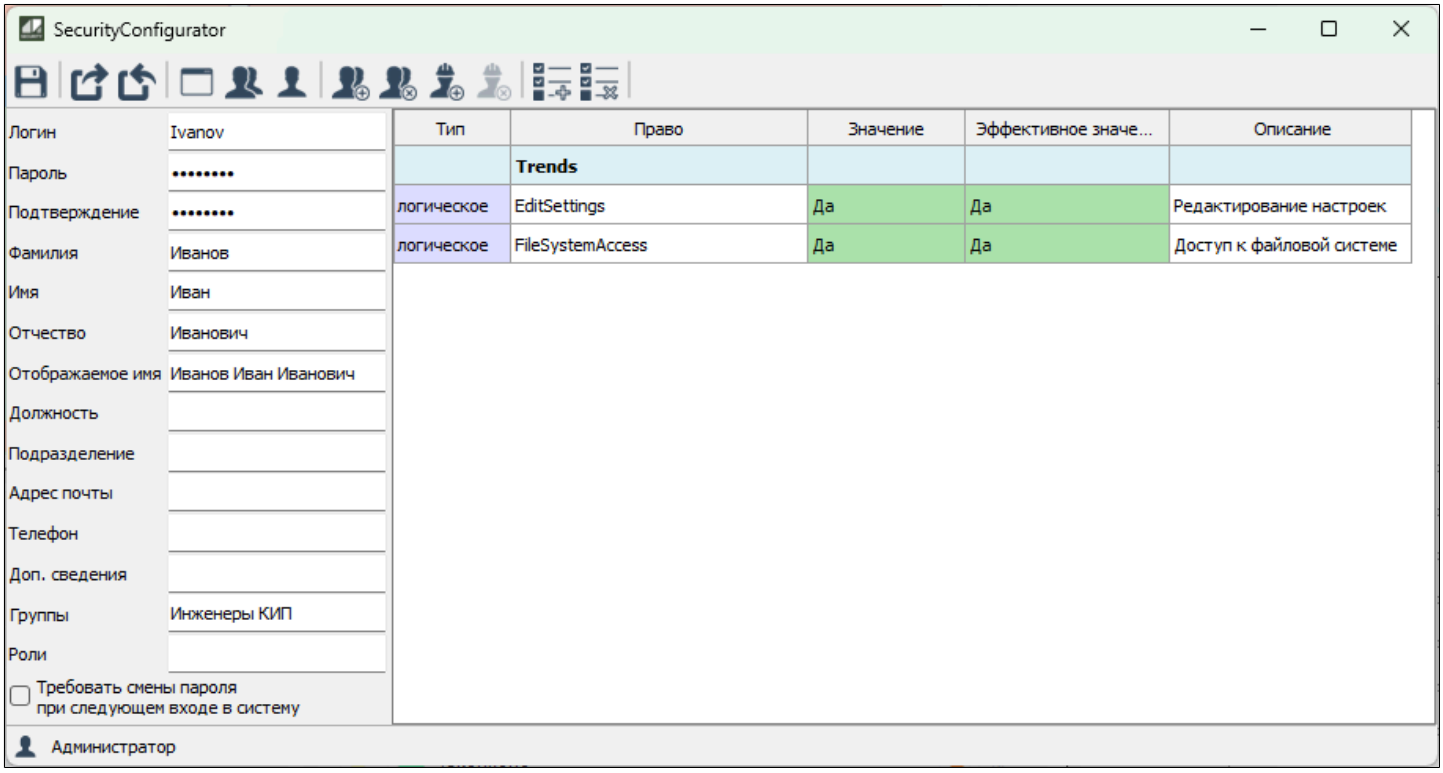
1.2.3.2.1.7.1.1. Добавить в группу

Чтобы добавить пользователя в группу нажмите кнопку "Добавить в группу" на панели инструментов.

В открывшемся окне выберите нужную группу и нажмите кнопку "Добавить".

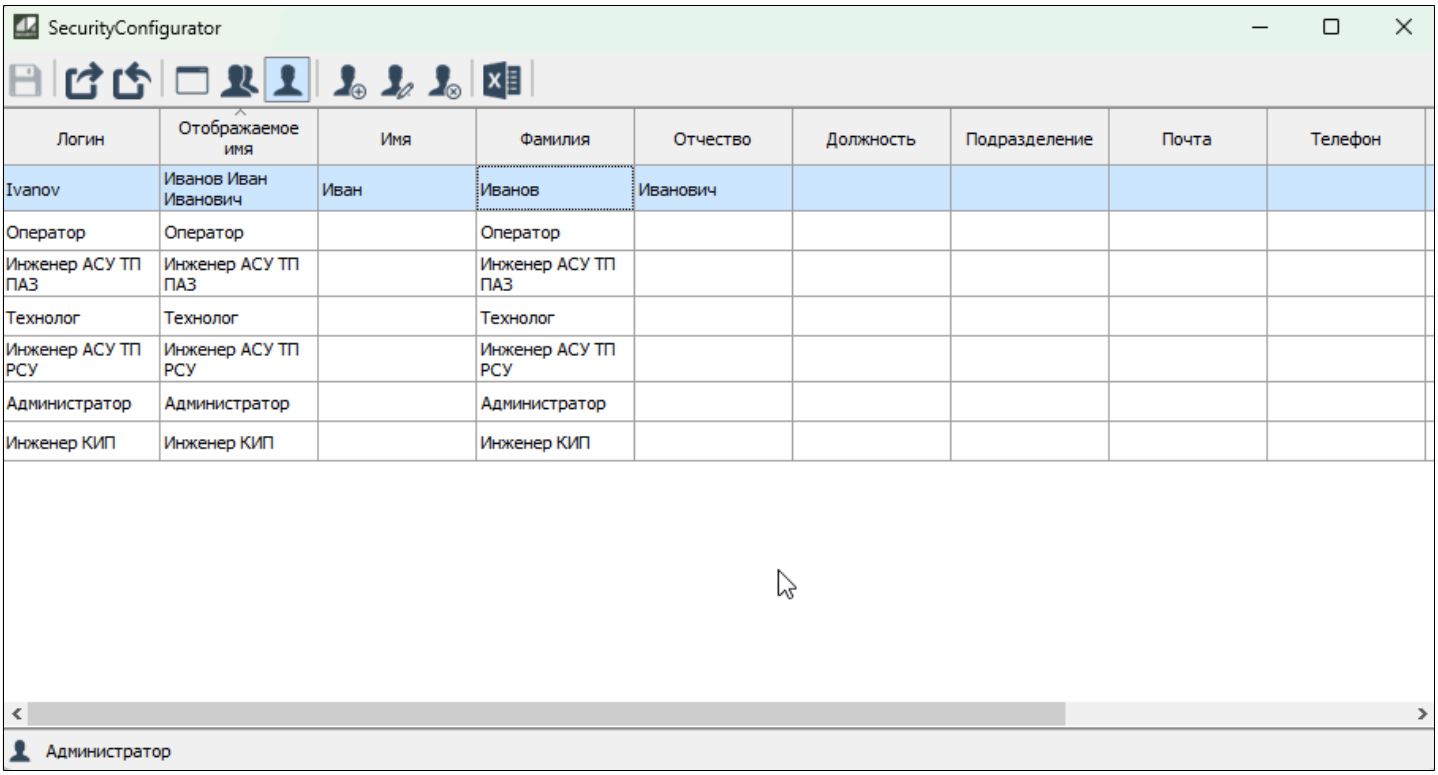


У пользователя появятся разрешения и запреты, назначенные группе, в которую он был добавлен.



Значения прав записаны в столбец Эффективное значение. Это связано с тем, что права унаследованы от группы.

Добавленный пользователь будет отображен в списке пользователей.



Количество групп, в которые пользователь может быть добавлен одновременно, связано со свойством UserInOnlyOneGroup компонента SecurityConfigurator:

- Если при разработке свойству указано значение «true», каждый пользователь сможет состоять только в одной группе.
- Если же свойству указано значение «false», каждого пользователя можно будет добавить в несколько групп.

После добавления учетной записи пользователя на панели управления добавятся специальные команды.

Команда	Кнопка	Описание
Блокировать группу пользователей		Используется, когда необходимо ограничить доступ в систему всем пользователям, состоящим в группе. Пока группа заблокирована, попытки входа участников отклоняются подсистемой безопасности. Чтобы разблокировать заблокированную группу, нажмите  Блокировка группы, в которой находится текущий пользователь, невозможна.
Завершить сессию пользователя на указанных АРМ		Предоставляет администратору возможность завершить сессии выбранного пользователя на указанных АРМ. Наличие команды связано со свойством DomainNodesList компонента SecurityConfigurator
Задать пароль пользователя		Предоставляет администратору возможность сменить пароль пользователя

Получение эффективных значений прав

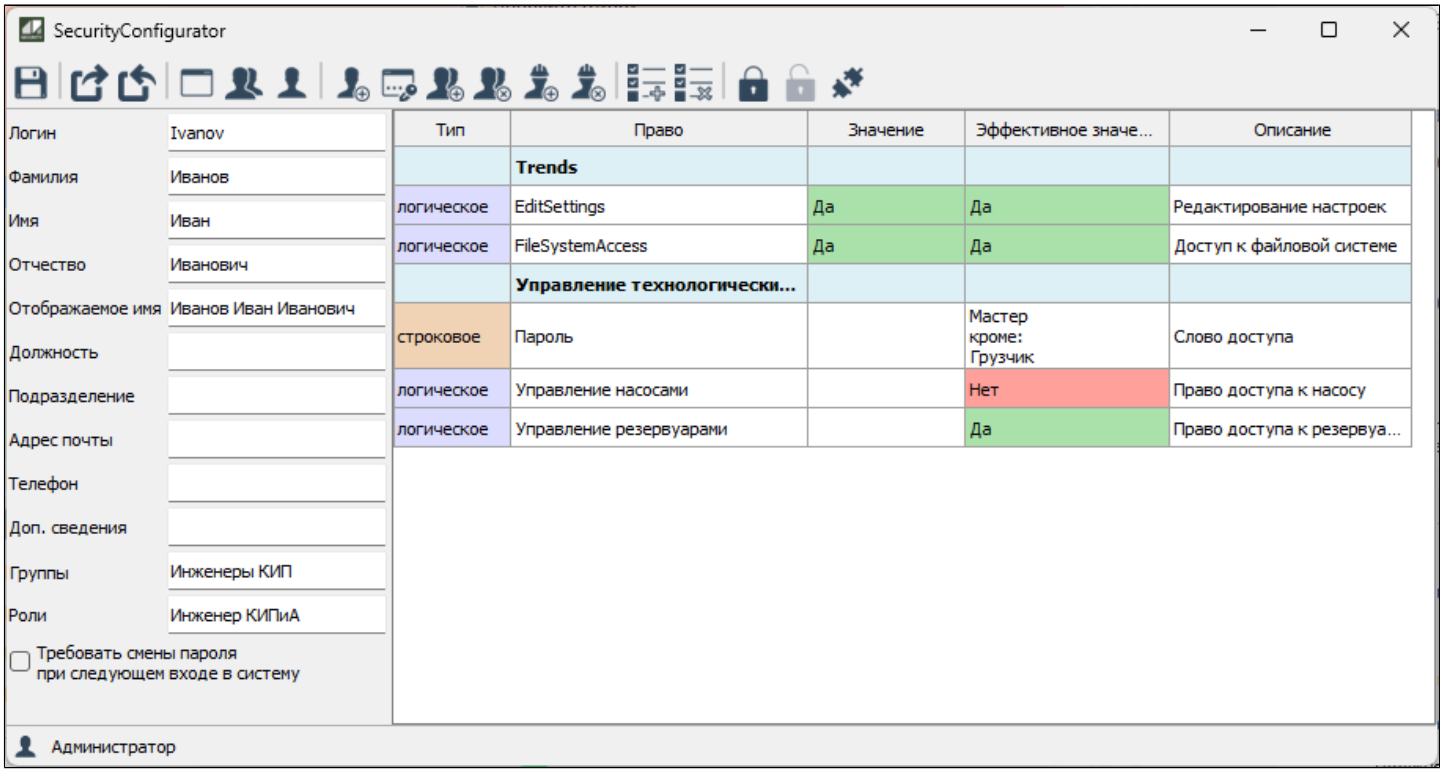
Значение одного и того же права может быть назначено:

- пользователю лично;
- группе пользователей;
- роли.

Значение права для пользователя зависит от того, в каких группах он состоит, какие роли ему назначены, и какое значение права назначено пользователю лично. Итоговое значение называется эффективным значением права.

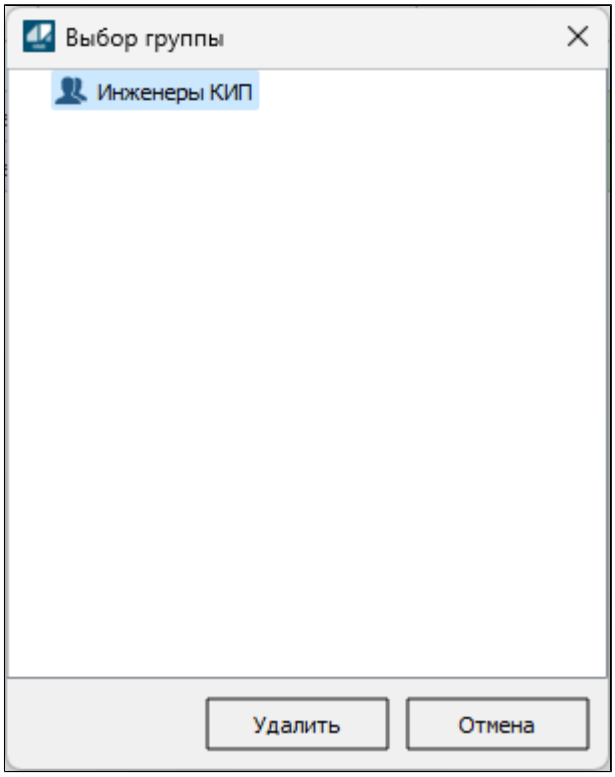
Правила определения эффективного значения права:

- Для логического права:
  - если есть хоть одно разрешающее значение и нет запрещающих, эффективное значение разрешающее;
  - если есть хоть одно запрещающее значение, эффективное значение запрещающее.
- Для строковых прав эффективное значение складывается из всех наследованных прав. Строковые права отображаются списком.



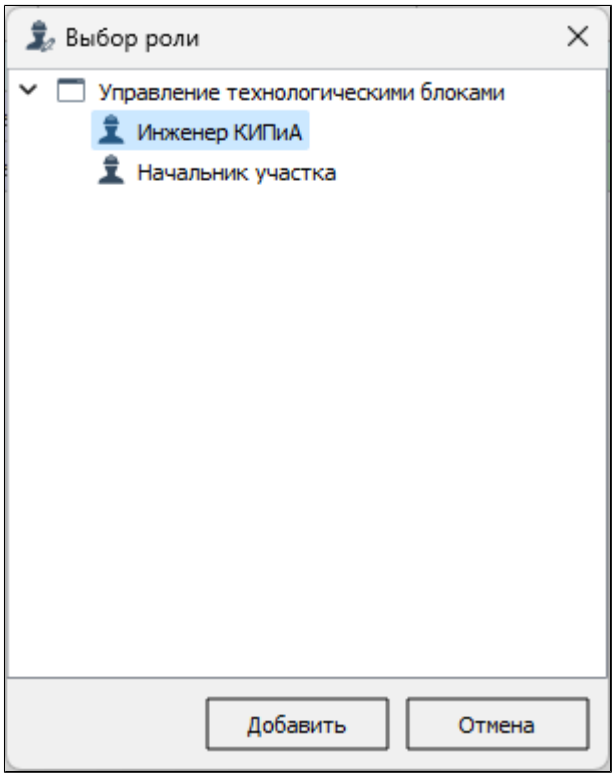
1.2.3.2.1.7.1.2. Удалить из группы

Чтобы удалить пользователя из группы, нажмите кнопку "Удалить из группы" на панели инструментов и выберите группу, из которой необходимо исключить пользователя.



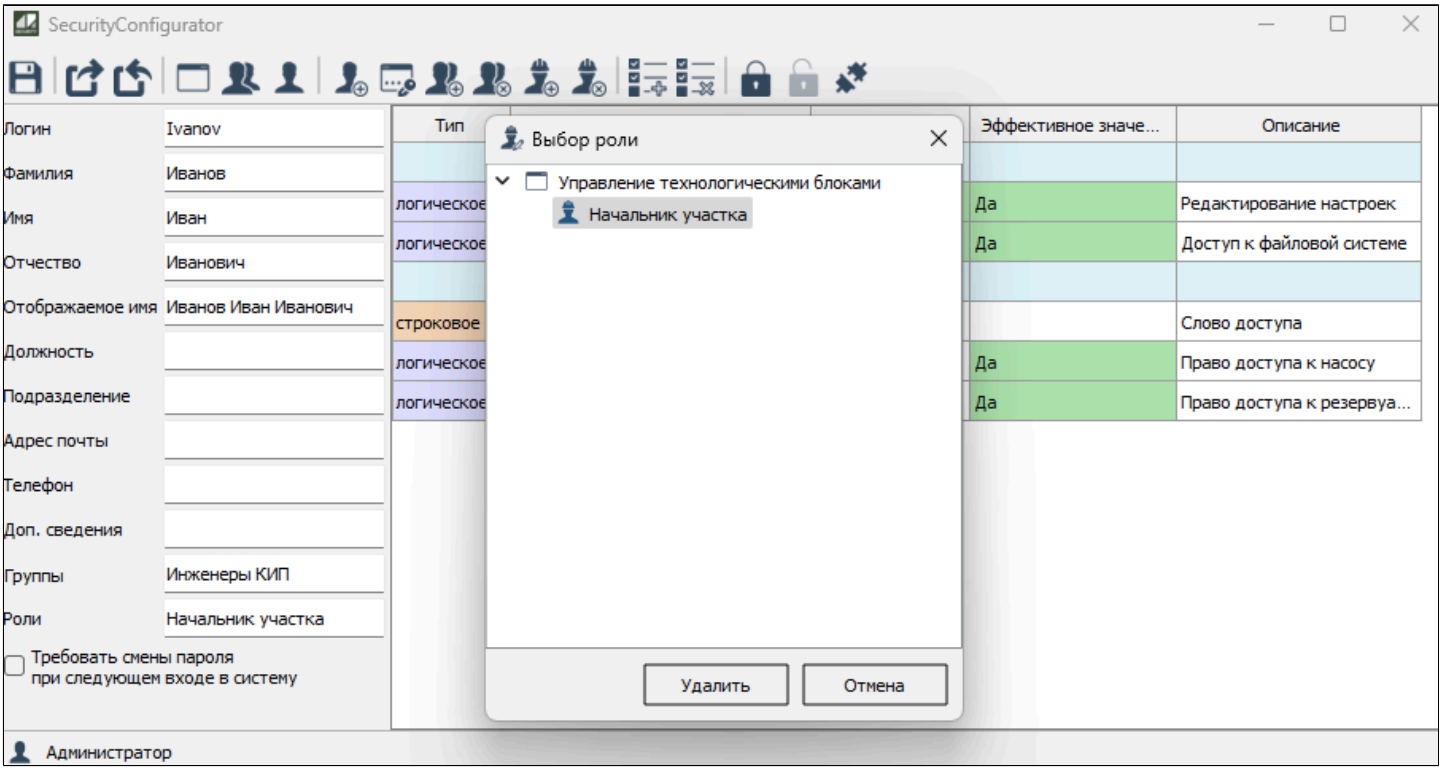
1.2.3.2.1.7.1.3. Добавить роли пользователю

Чтобы назначить пользователю роль, нажмите кнопку "Добавить роли пользователю" на панели инструментов и в открывшемся окне из списка доступных ролей выберите необходимые.



1.2.3.2.1.7.1.4. Лишить пользователя ролей

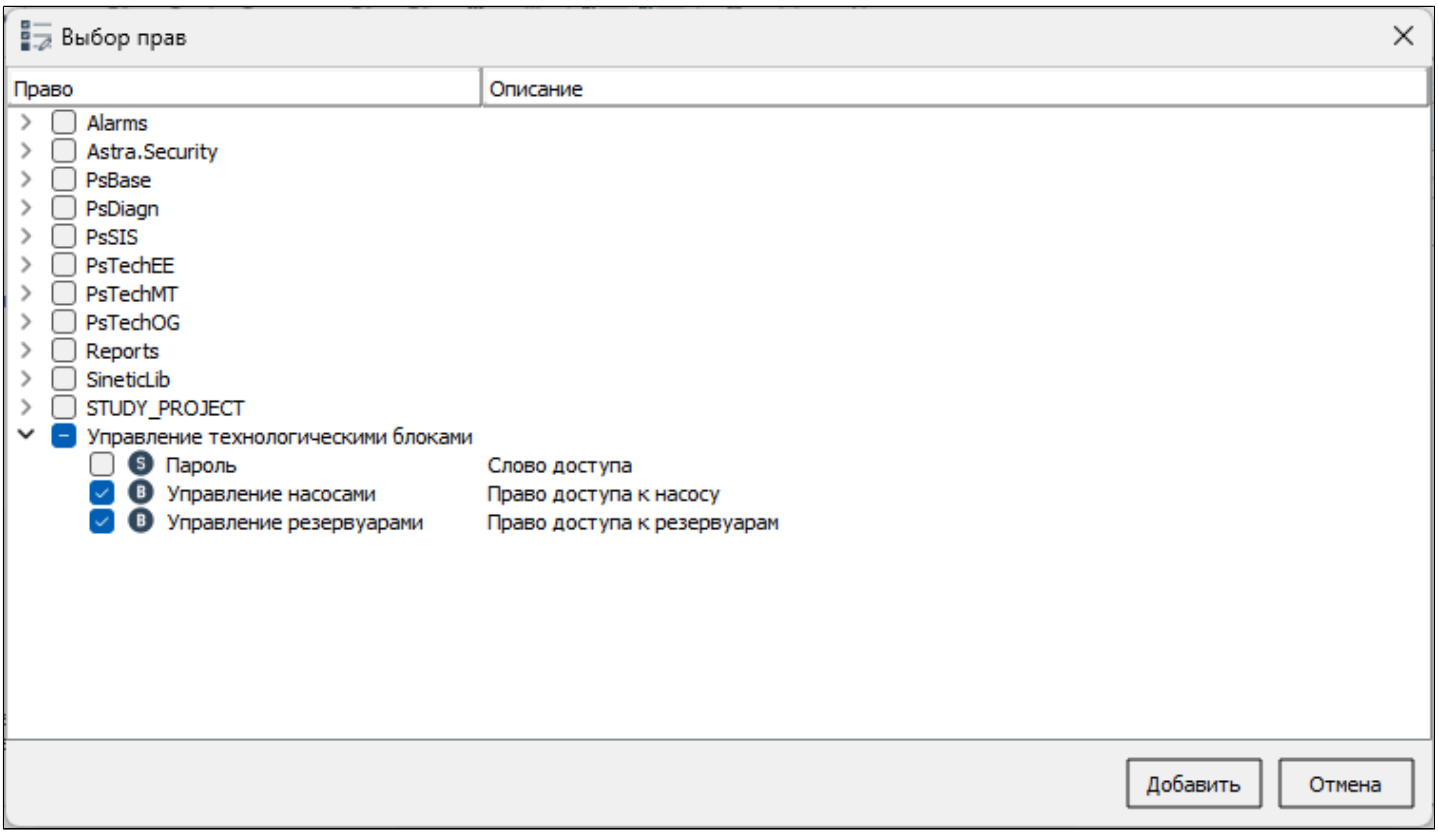
Чтобы удалить у пользователя роль, нажмите кнопку "Лишить пользователя ролей" на панели инструментов, в открывшемся окне из списка доступных ролей выберите необходимые и нажмите кнопку "Удалить".



1.2.3.2.1.7.1.5. Добавить права

Чтобы добавить пользователю права, нажмите кнопку "Добавить права" на панели инструментов.

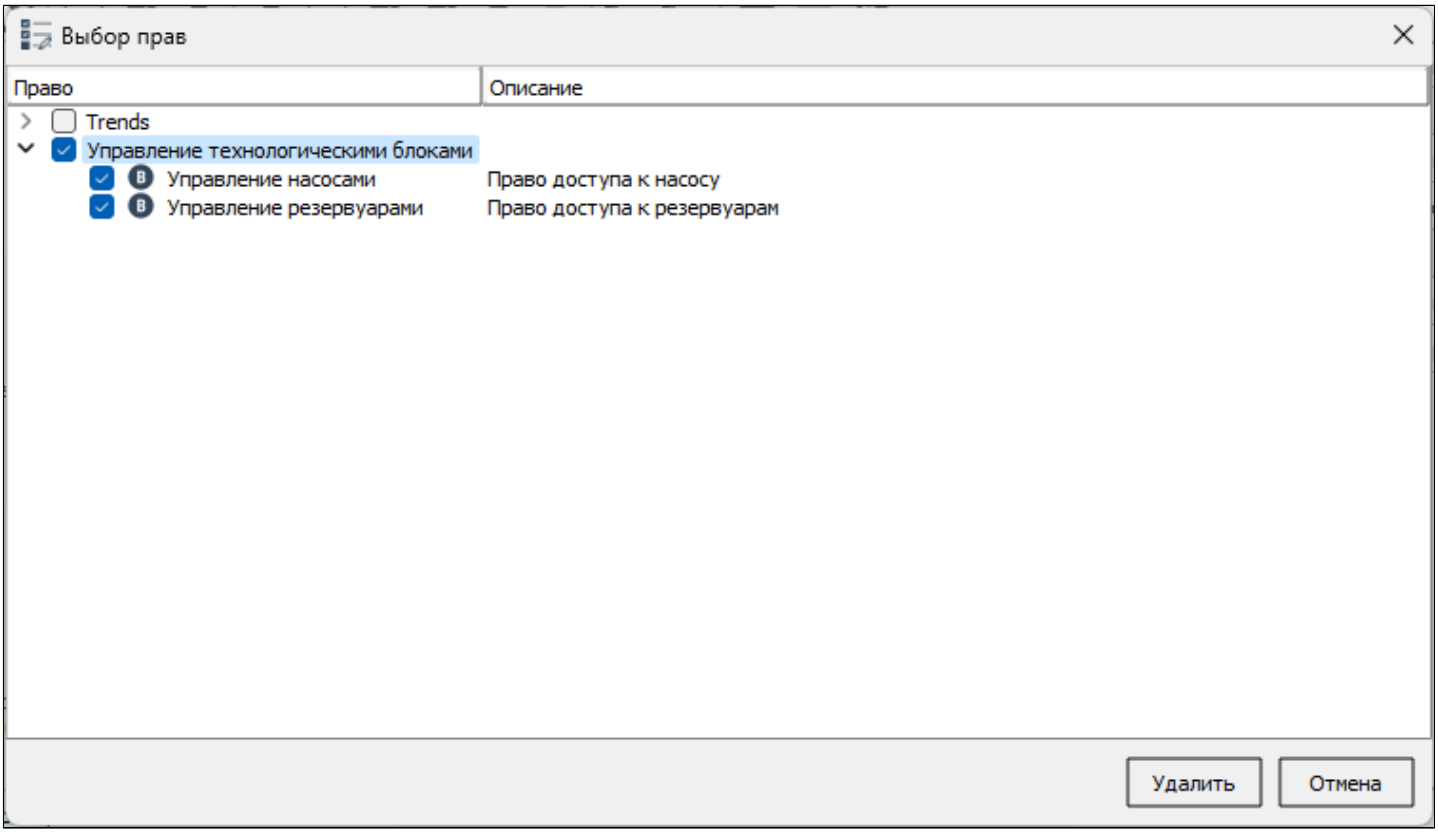
Откроется окно выбора прав. Выберите права, которые необходимо назначить пользователю, и нажмите кнопку "Добавить".



1.2.3.2.1.7.1.6. Удалить права

Чтобы удалить права пользователя, нажмите кнопку "Удалить права" на панели инструментов.

Откроется окно выбора прав пользователя. Выберите права, которые необходимо удалить и нажмите кнопку "Удалить".



1.2.3.2.1.8. Редактировать учетную запись пользователя

Чтобы внести изменения в учетную запись пользователя, выберите пользователя из списка и нажмите кнопку "Редактировать учетную запись пользователя" на панели инструментов или дважды кликните по строке учетной записи в списке.

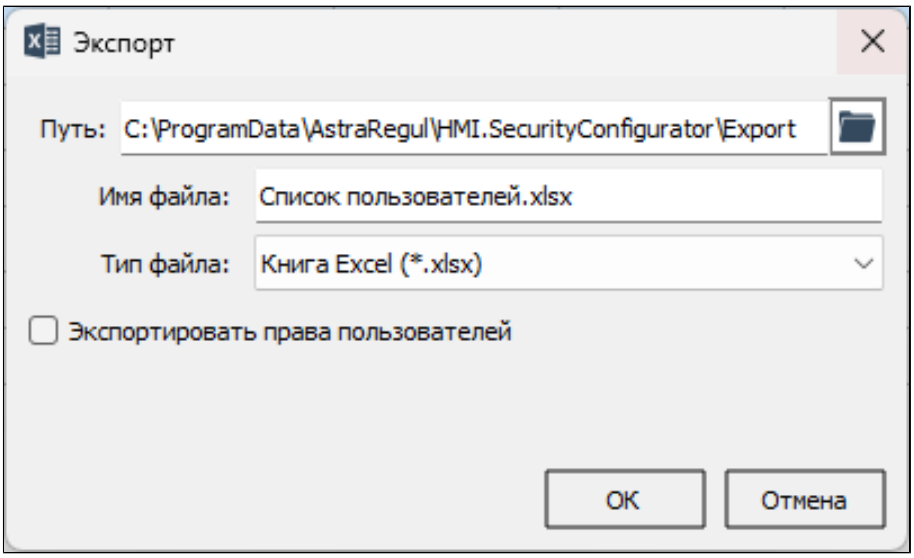
1.2.3.2.1.9. Удалить учетную запись пользователя

Чтобы удалить учетную запись пользователя, выберите пользователя из списка и нажмите кнопку "Удалить учетную запись пользователя" на панели инструментов.

1.2.3.2.1.10. Экспортировать в файл

Чтобы экспортировать список пользователей или список прав, нажмите кнопку "Экспортировать в файл" на панели инструментов.

Откроется окно с настройками параметров экспорта. Укажите путь, задайте название файла и выберите формат данных, затем нажмите кнопку "Сохранить".



Установите флаг Экспортировать права пользователя для экспорта прав каждого пользователя в отдельный файл.

Экспорт списка пользователей выполняется в файл формата *.csv, *.xlsx или *.pdf.
Экспорт списка прав выполняется в файл формата *.json, *.csv, *.xlsx или *.pdf.

1.2.3.3. Встраивание в проект

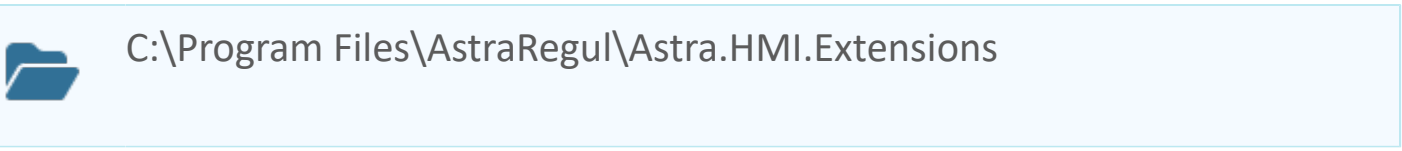
Чтобы встроить Astra.HMI.SecurityConfigurator в проект и начать работу с приложением:

1. Подключите Astra.HMI.SecurityConfigurator к проекту как внешний модуль.
2. Добавьте экземпляр типа SecurityConfigurator в проект.

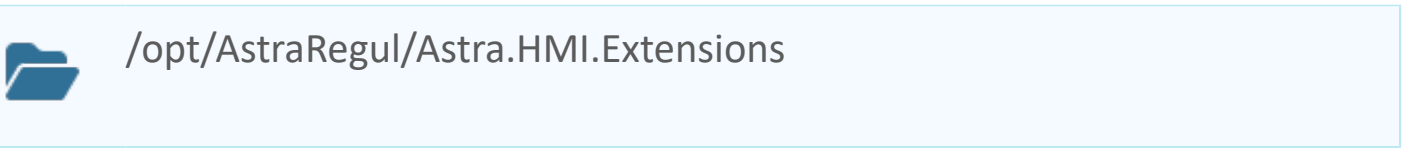
В интерфейсе отобразится дерево карт уставок из указанного конфигурационного файла. Вы сможете переключаться между картами и редактировать значения уставок.

Подключение внешнего модуля Astra.HMI.SecurityConfigurator

Чтобы подключить Astra.HMI.SecurityConfigurator как внешний модуль, выполните следующие действия:
1. Создайте в папке своего проекта папку externals, в которой нужно размещать файлы всех подключаемых внешних модулей.
2. Перейдите к папке, в которую устанавливаются все приложения Astra.HMI:
   - ОС Windows:

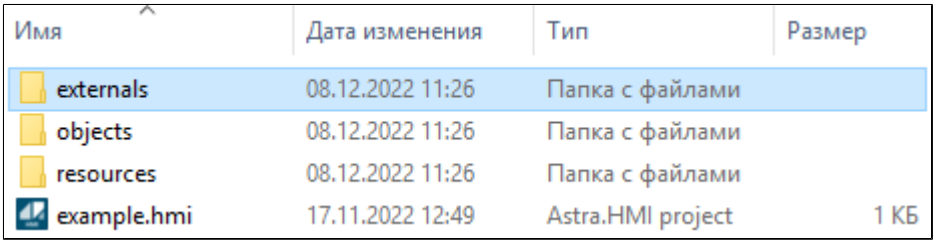


   - ОС Linux:



В папке уже должна быть папка SecurityConfigurator, появившаяся после установки Astra.HMI.SecurityConfigurator.

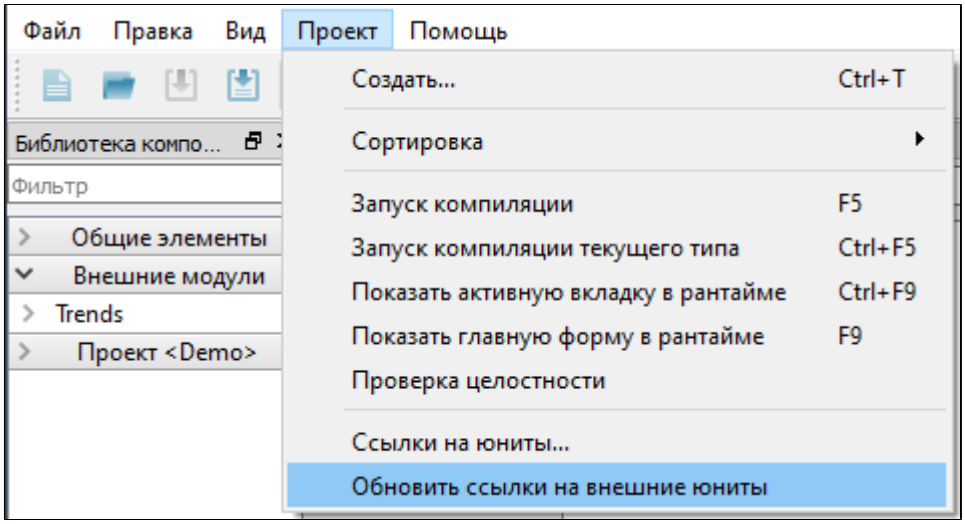
3. Скопируйте эту папку SecurityConfigurator и папку библиотеки Commonlib в созданную вами папку **externals**.



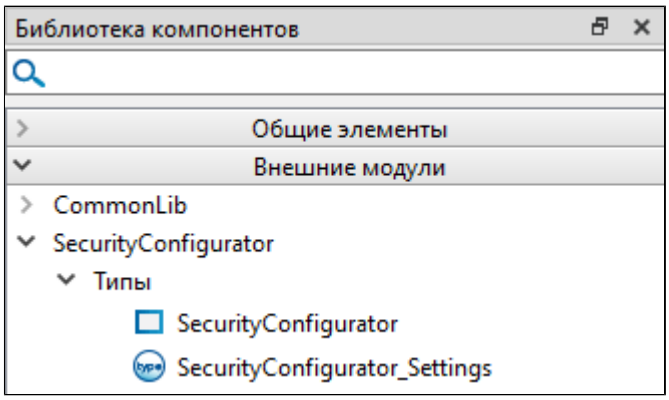
Для использования Astra.HMI.SecurityConfigurator в проекте Astra.HMI, необходимо установить библиотеку Astra.HMI.CommonLib.

4. Откройте свой проект в дизайнере Astra.HMI.

5. Перейдите в меню Проект и выберите команду **Обновить ссылки на внешние юниты**.



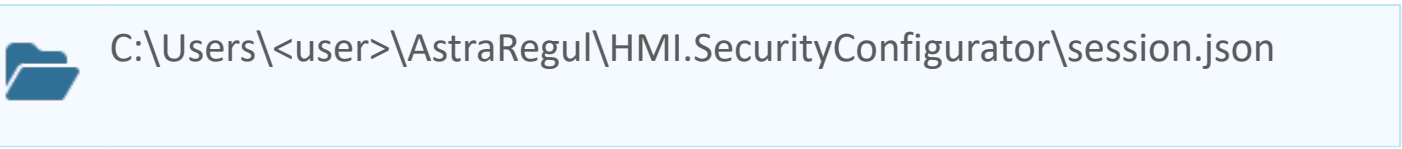
Так вы обновите список внешних модулей своего проекта, и новый модуль SecurityConfigurator появится в библиотеке компонентов.



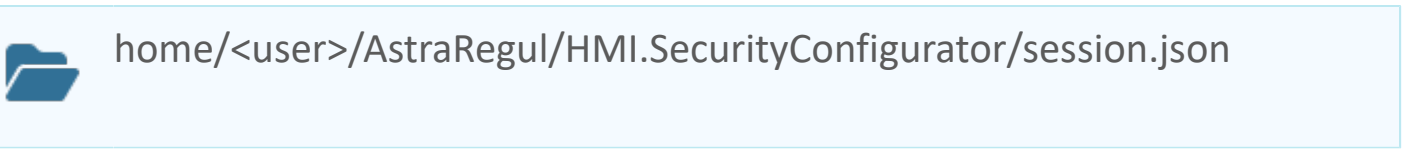
Настройка вида приложения

Чтобы внешний вид и положение окна конфигуратора не менялись после перезапуска приложения, эта информация сохраняется в конфигурационном файле session.json. Чтобы ознакомиться с файлом, перейдите к его расположению:

- ОС Windows:



- ОС Linux:



SecurityConfigurator

Экранная форма SecurityConfigurator – основной компонент приложения Astra.HMI.SecurityConfigurator. В режиме исполнения является полноценным конфигуратором SecurityConfigurator подсистемы безопасности Astra.Security и позволяет:

- создавать, редактировать и удалять учетные записи пользователей;
- создавать, редактировать и удалять группы пользователей;
- добавлять пользователей в группы и удалять их из групп;
- создавать, редактировать и удалять приложения и права, назначать права пользователям и группам;
- создавать роли в приложениях и назначать их пользователям и группам;
- сохранять резервные копии конфигурации и восстанавливать конфигурацию из резервной копии.

1.2.3.3.1. Настройки

Экземпляр типа Astra.HMI.SecurityConfigurator, добавленный в проект Astra.HMI имеет следующие параметры настройки:

Параметр	Описание
Список узлов домена	Список имен АРМ, на которых можно завершить сессию пользователя
Пользователь может быть только в одной группе	Количество групп, в которых пользователь может состоять одновременно
Пользователь должен быть в группе	Обязательность добавления пользователя в группу
Путь к резервным копиям базы	Путь к резервным копиям базы
Путь для экспорта таблиц	Полный путь к папке для хранения экспортированных таблиц
Путь к шаблонам приложений	Путь к шаблонам приложений

1.2.3.3.1.1. Список узлов домена

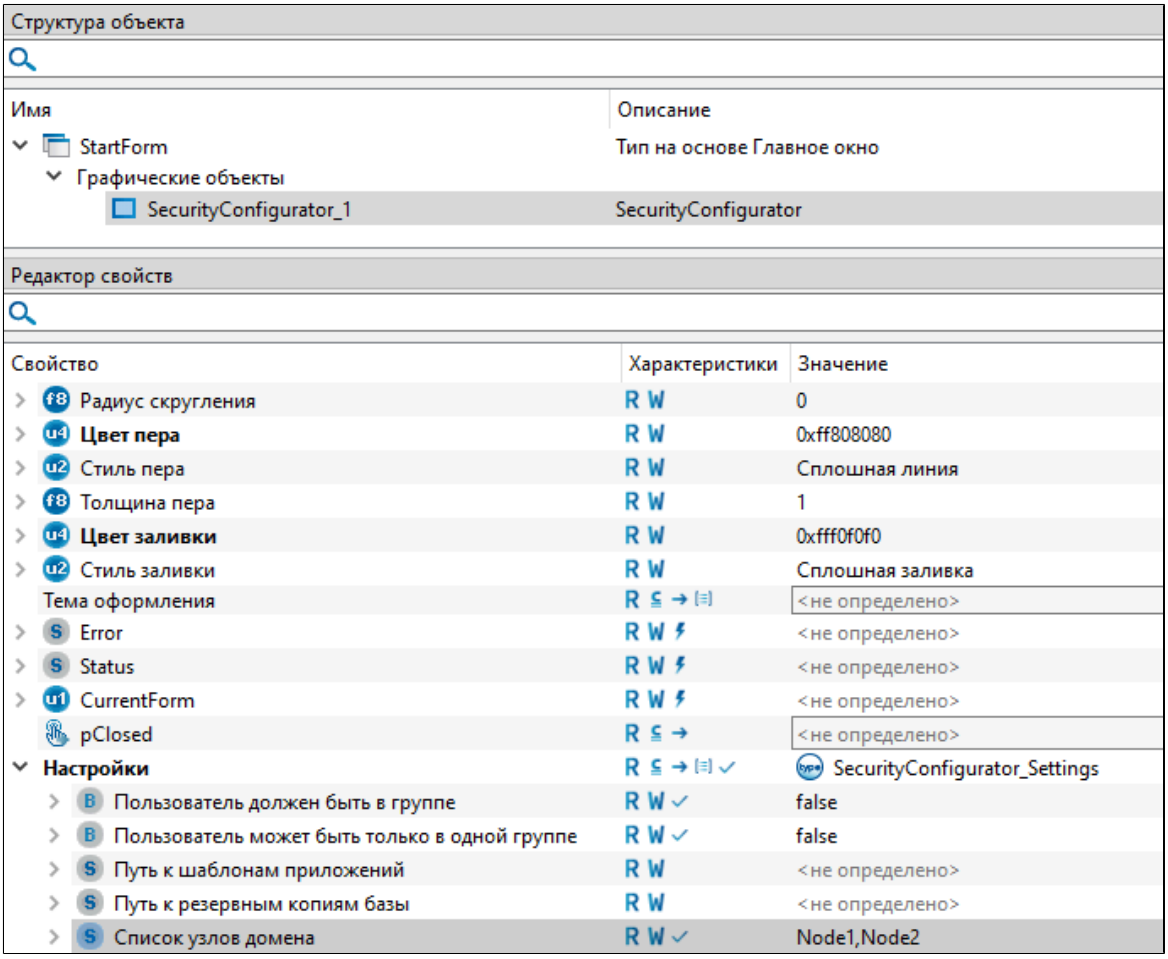
Список имен APM, на которых можно завершить сессию пользователя.

string DomainNodes

Если указать хотя бы одно имя APM в сети Astra.Net, в окне редактирования учетной записи пользователя появится команда на завершение сессии. Результат применения свойства описан в Специальные команды редактирования учетных записей).

Примеры

Построена простейшая сеть Astra.Net, в которой все узлы подчинены центральному узлу сети. В сеть включены три APM: CentralNode, Node1 и Node2. Необходимо иметь возможность завершать пользовательские сессии на узлах Node1 и Node2 из конфигуратора на центральном узле CentralNode. Тогда в качестве значения свойства DomainNodesList указывается список имен Node1 и Node2.


Структура объекта
Имя
Описание
StartForm
Тип на основе Главное окно
Графические объекты
SecurityConfigurator_1
SecurityConfigurator
Редактор свойств
Свойство
Характеристики
Значение
Радиус скругления
R W
0
Цвет пера
R W
0xff808080
Стиль пера
R W
Сплошная линия
Толщина пера
R W
1
Цвет заливки
R W
0xfff0f0f0
Стиль заливки
R W
Сплошная заливка
Тема оформления
R
<не определено>
Error
R W
<не определено>
Status
R W
<не определено>
CurrentForm
R W
<не определено>
pClosed
R
<не определено>
Настройки
R
SecurityConfigurator_Settings
Пользователь должен быть в группе
R W
false
Пользователь может быть только в одной группе
R W
false
Путь к шаблонам приложений
R W
<не определено>
Путь к резервным копиям базы
R W
<не определено>
Список узлов домена
R W
Node1,Node2

1.2.3.3.1.2. Пользователь может быть только в одной группе

Регулирует количество групп, в которых пользователь может состоять одновременно.

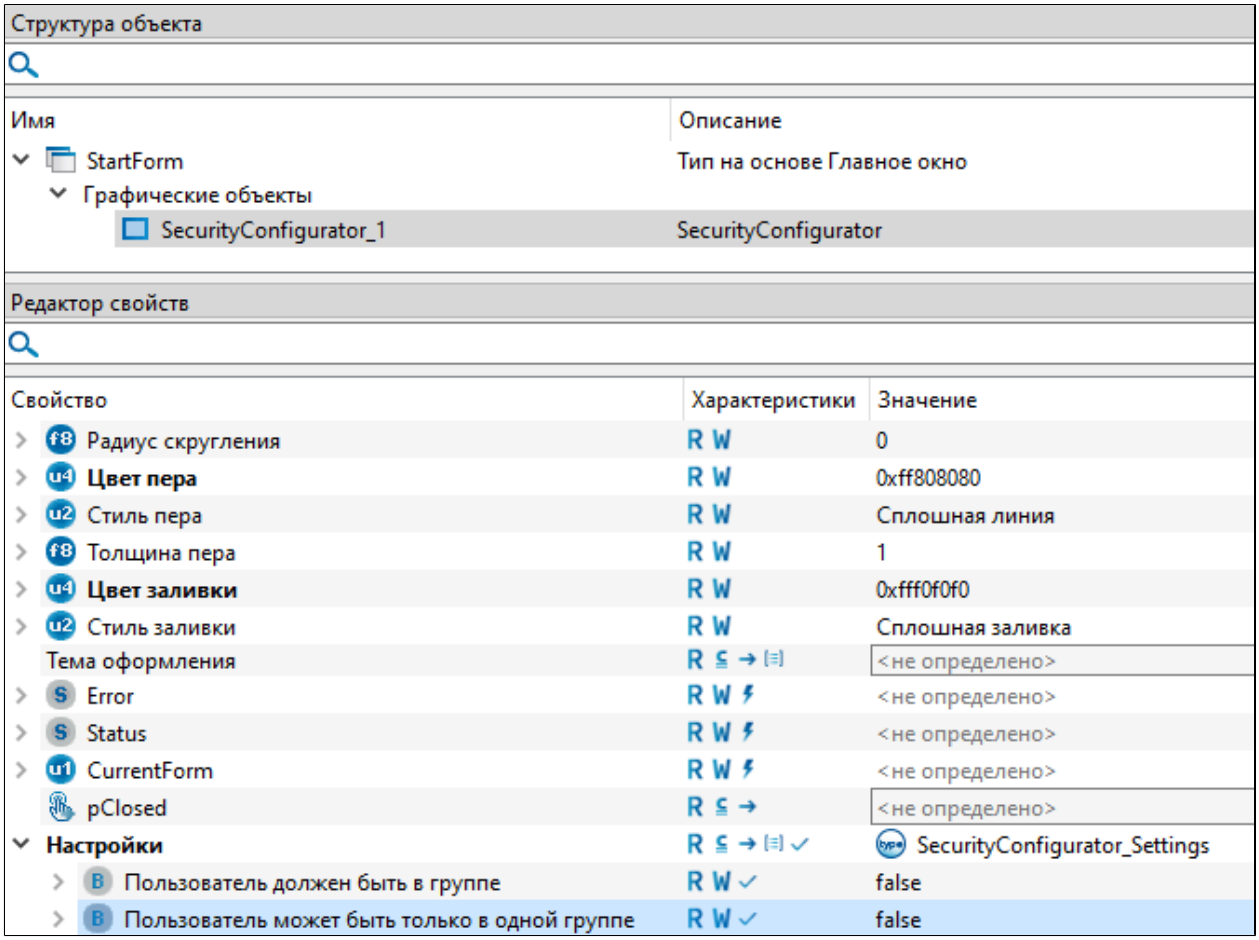
bool UserInOnlyOneGroup

Значение

Значение	Описание
true	Пользователя можно добавить только в одну группу
false	Пользователя можно добавить в несколько групп

Примеры

//Установить возможность добавлять пользователей в несколько групп.



1.2.3.3.1.3. Пользователь должен быть в группе

Регулирует обязательность добавления пользователя в группу.

bool UserInAtLeastOneGroup

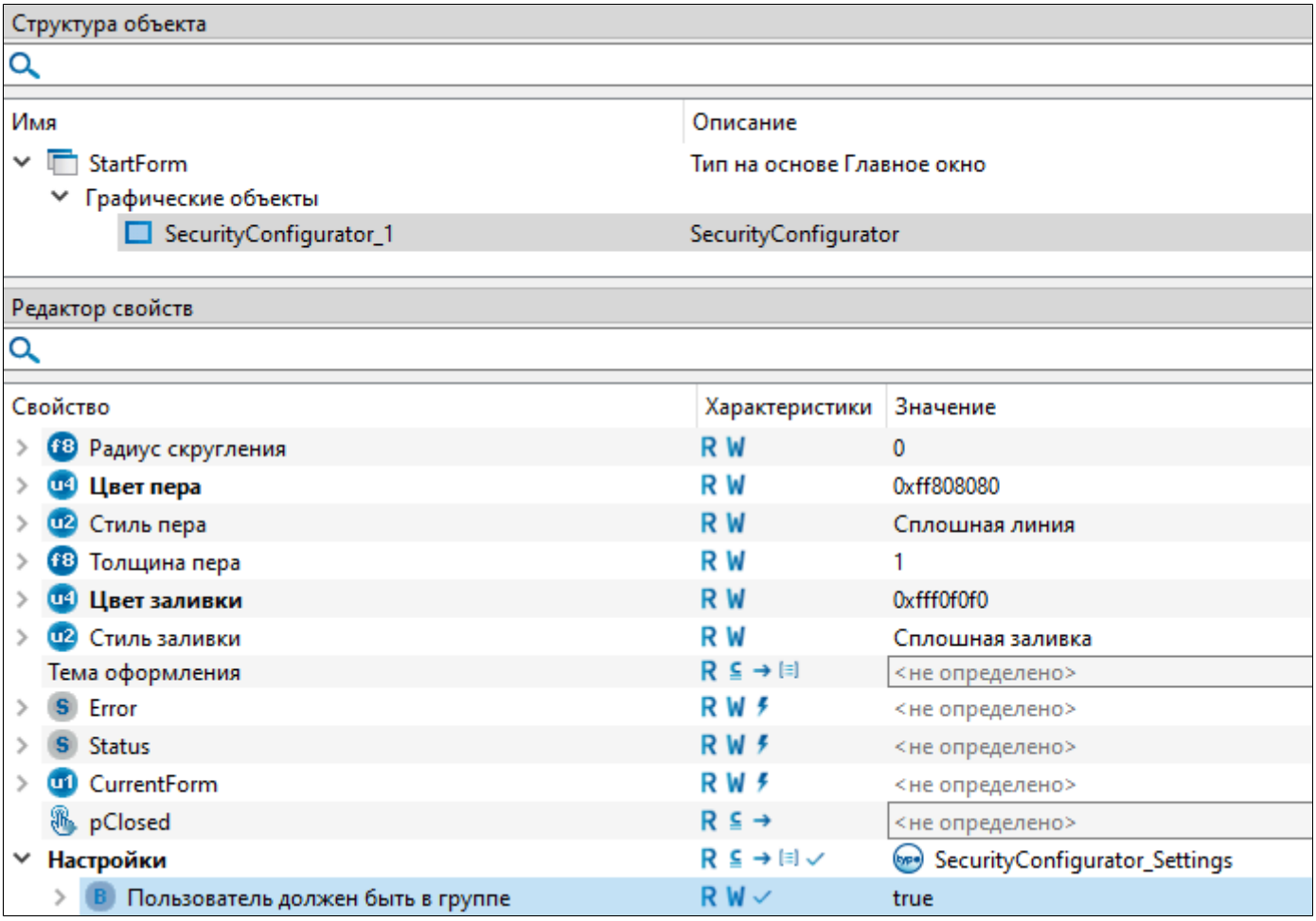
Значение

Значение	Описание
true	Пользователь должен состоять хотя бы в одной группе
false	Пользователя необязательно добавлять в группу (группы)

Требование обязательного нахождения пользователя в группе может исходить из Astra.HMI.Security. В таком случае не удастся сохранить запись пользователя без указания группы, даже если для свойства указано значение false. Решение этого противоречия находится в разработке.

Примеры

//Установить требование нахождения пользователя хотя бы в одной в группе.



1.2.3.3.1.4. Путь к резервным копиям базы

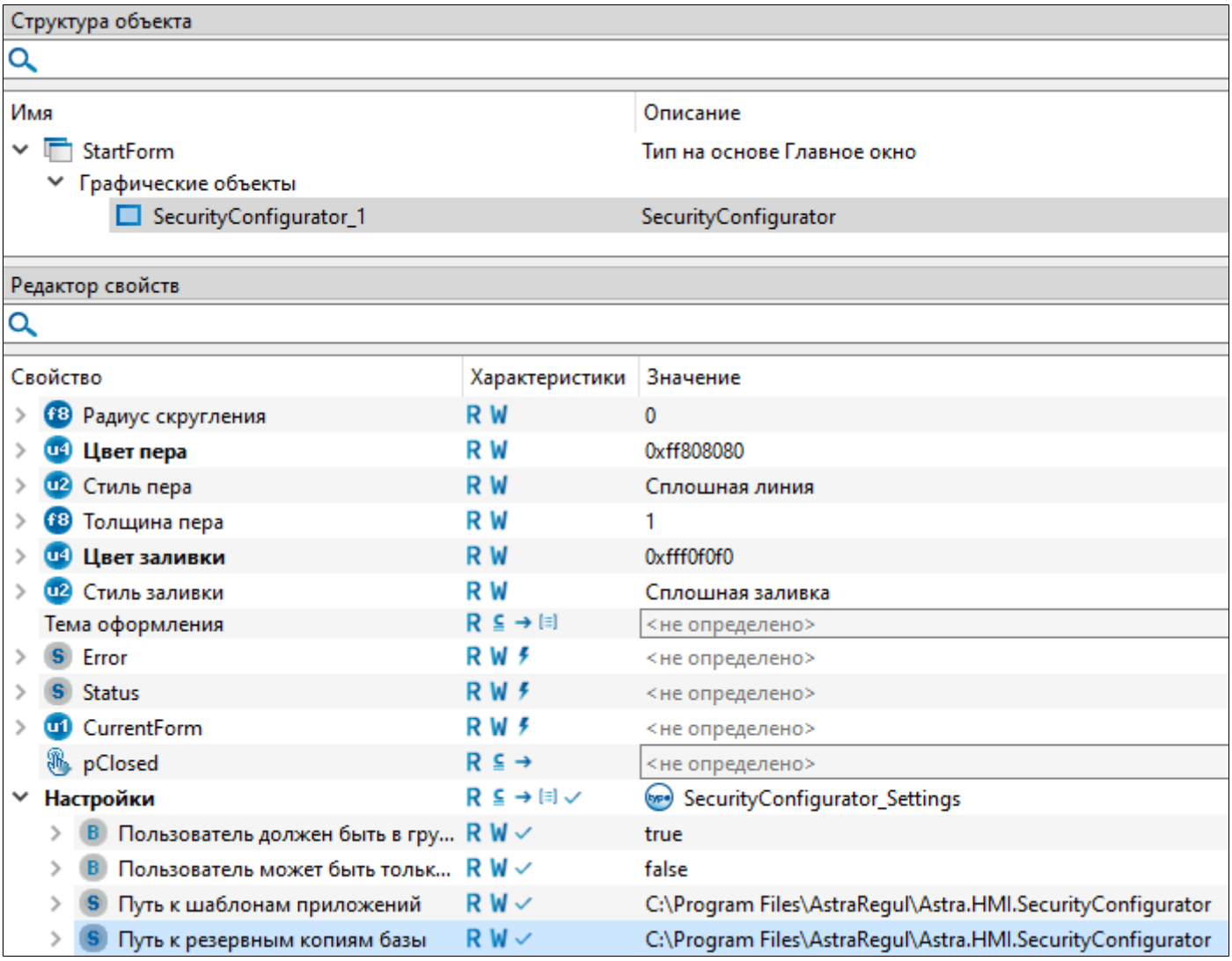
Полный путь к папке для хранения резервных копий конфигурации подсистемы безопасности.

string BackupsPath

Если не указывать значение свойства, то при сохранении резервной копии или восстановлении из резервной копии будет предложен путь к папке по умолчанию. Папкой по умолчанию является папка Backups, создающаяся в папке проекта при первом сохранении резервной копии.

Примеры

//Установить следующий путь к папке для хранения резервной копии конфигурации подсистемы безопасности: C:\Program Files\AstraRegul\Astra.HMI.SecurityConfigurator.



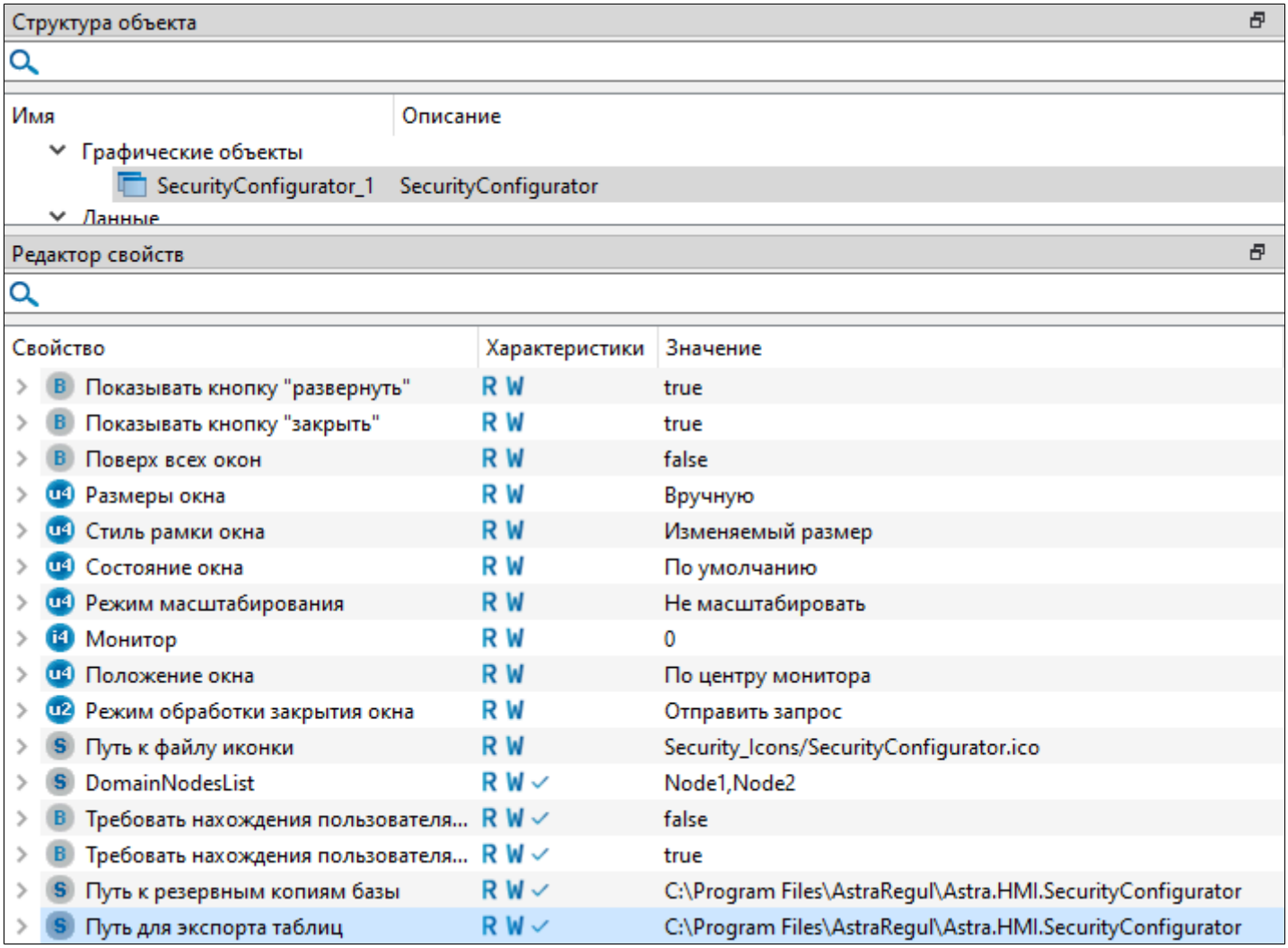
1.2.3.3.1.5. Путь для экспорта таблиц

Полный путь к папке для хранения экспортированных таблиц.

string ExcelExportPath

Примеры

//Установить следующий путь к папке для экспорта таблиц: C:\Program Files\AstraRegul\Astra.HMI.SecurityConfigurator.



1.2.3.3.1.6. Путь к шаблонам приложений

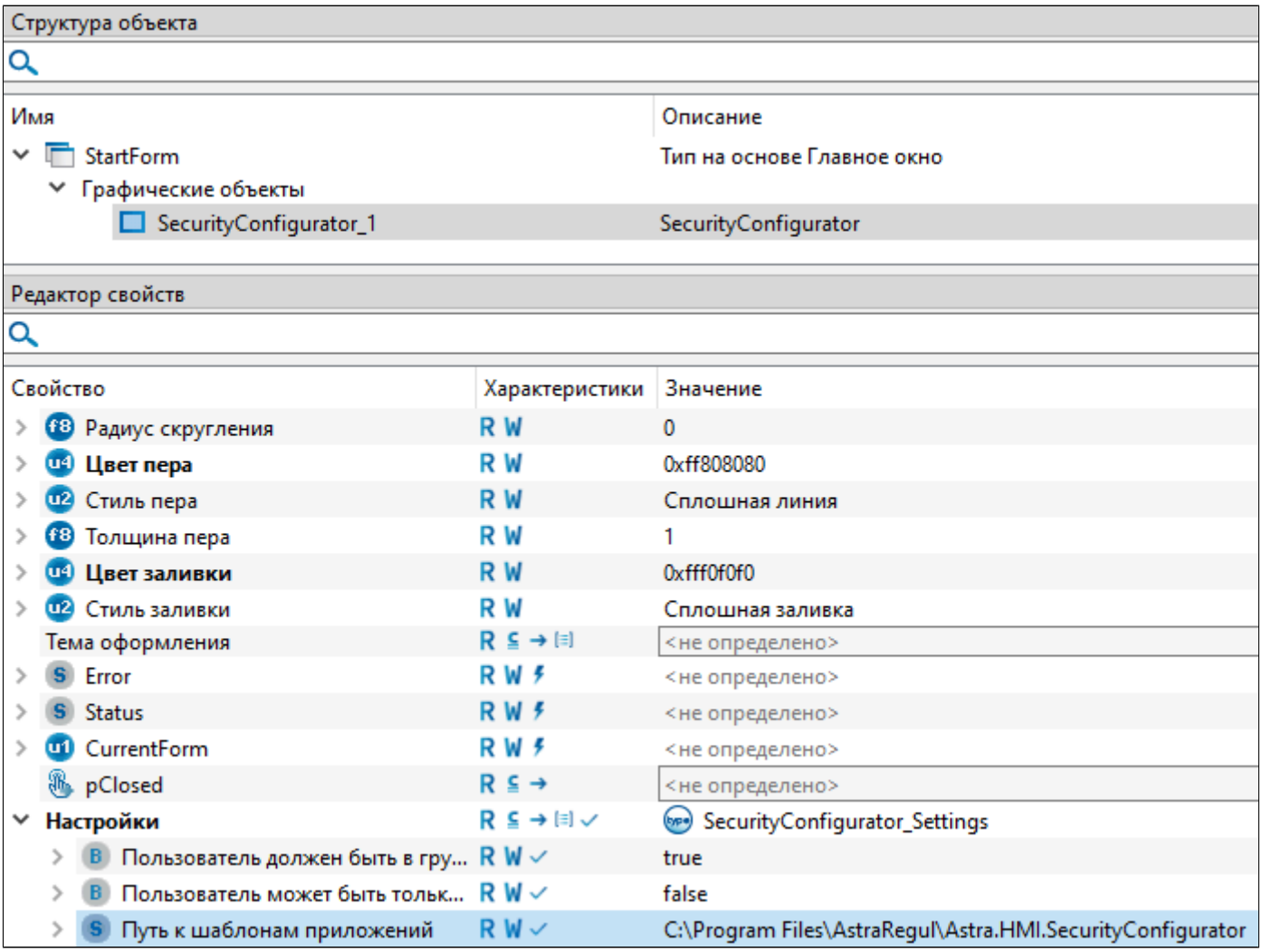
Полный путь к папке для хранения шаблонов приложений.

string AppTemplatesPath

Если не указывать значение свойства, то при импорте приложений будет предложен путь к папке по умолчанию. Папкой по умолчанию является папка Security_Templates в папке проекта.

Примеры

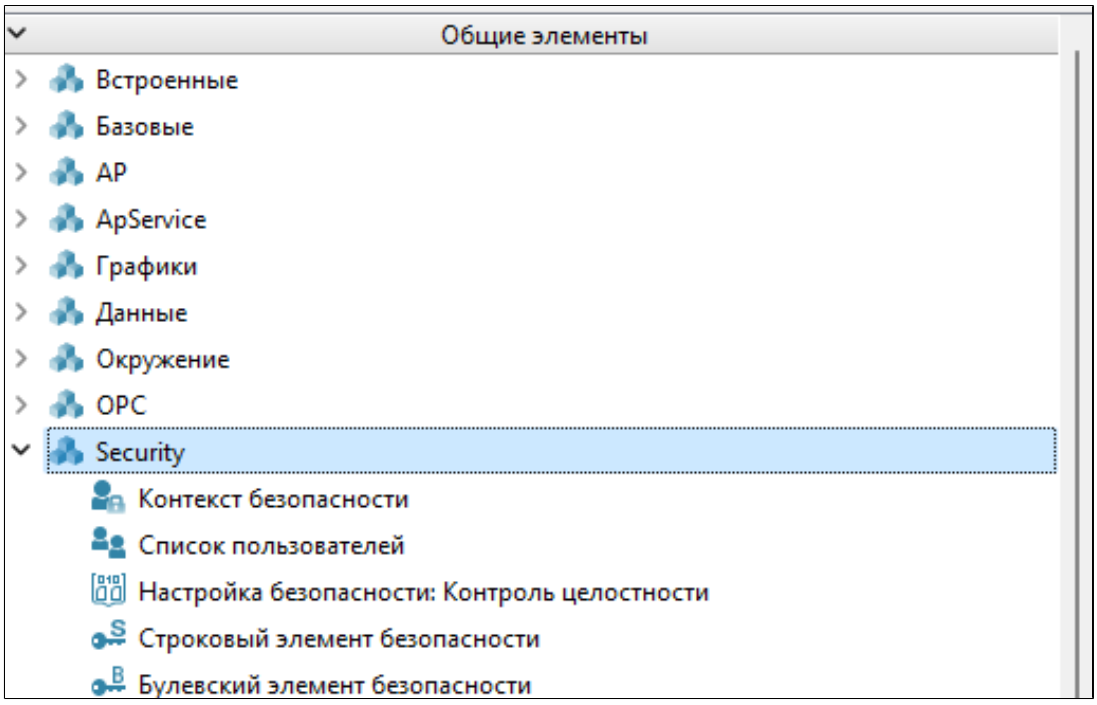
//Установить следующий путь к папке для хранения шаблонов приложений: C:\Program Files\AstraRegul\Astra.HMI.SecurityConfigurator.

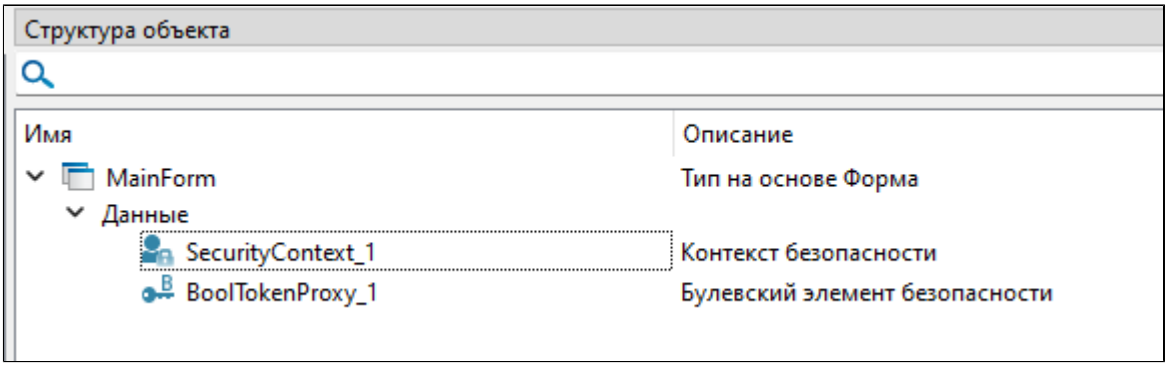


1.2.3.4. Доступ из проекта HMI к правам Astra.HMI.SecurityConfigurator

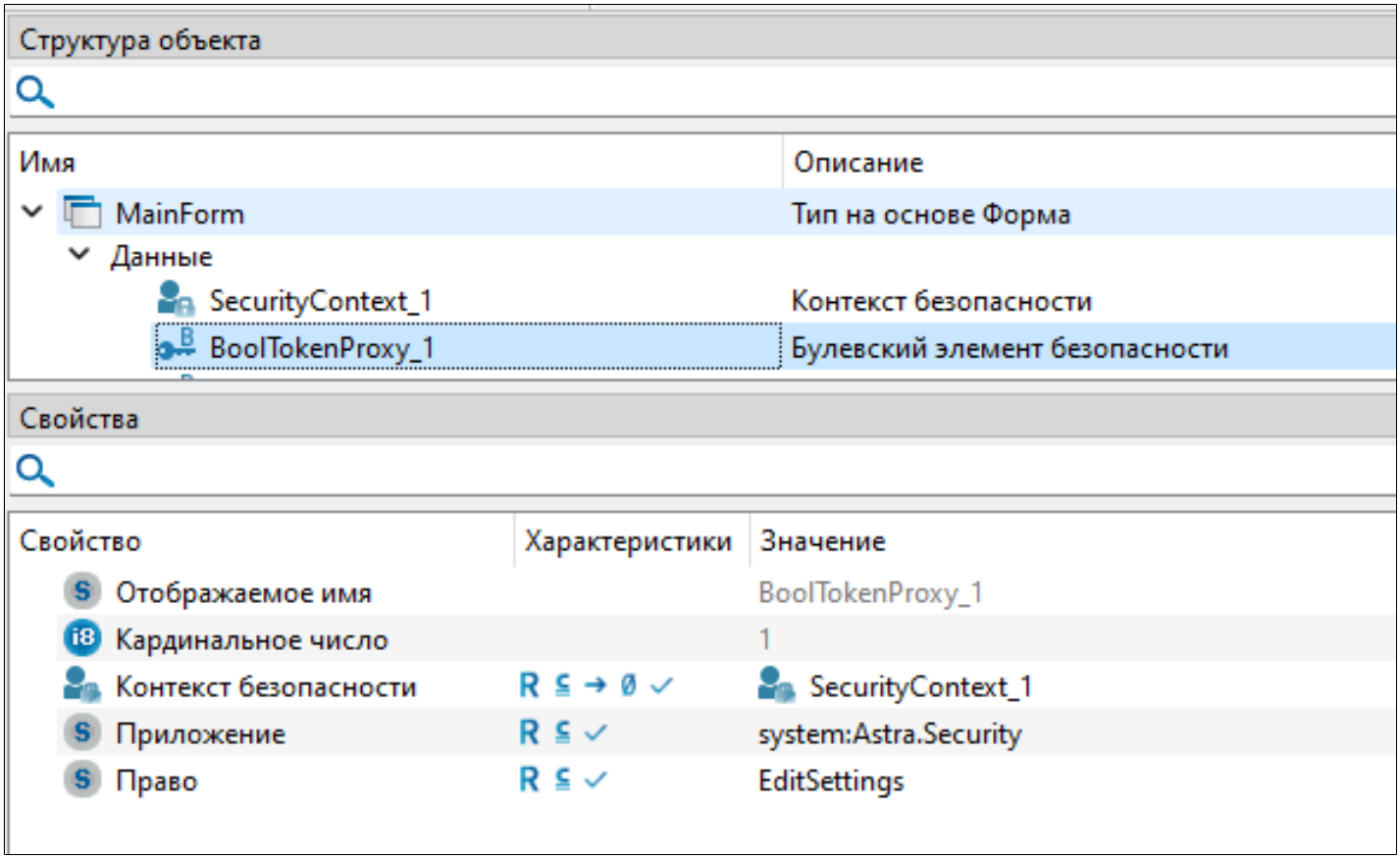
Для получения доступа к правам Astra.HMI.SecurityConfigurator из проекта HMI необходимо выполнить следующие действия:

1. Добавьте на форму объекты "Контекст безопасности" и "Булевский элемент безопасности" из раздела "Общие элементы".

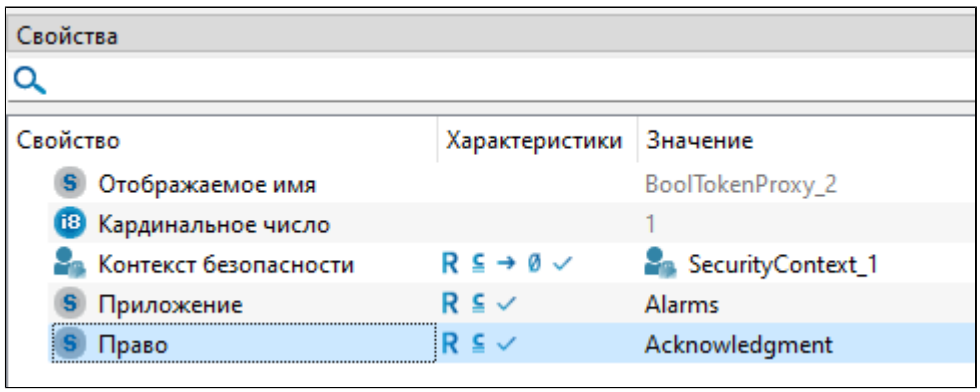




2. Выберите в структуре объектов Булевский элемент безопасности и в свойстве "Приложение" укажите "system:Astra.Security". Затем укажите "Контекст безопасности" и выберите право, которое необходимо получить.



Для получения прав из других приложений (Astra.HMI.Trends, Astra.HMI.Alarms и т.д.) в свойстве "Приложение" необходимо указать полное имя приложения.



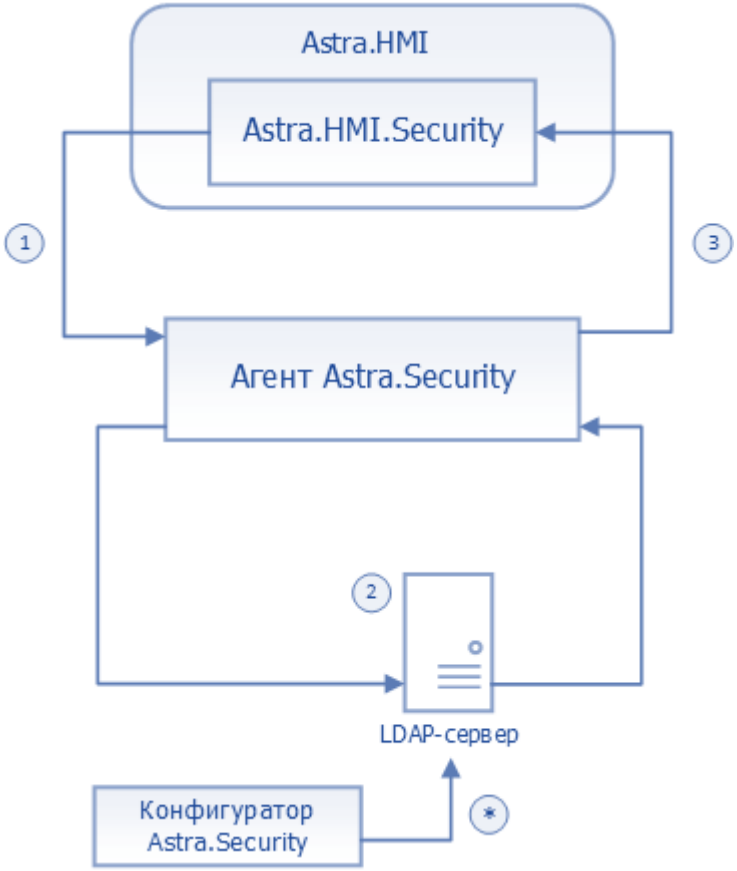
1.2.4. Astra.HMI.Security

Astra.HMI.Security – библиотека компонентов для графического редактора Astra.HMI, позволяющих взаимодействовать с подсистемой безопасности Astra.Security.

Функции:

- регистрация пользователя в подсистеме безопасности (вход) с использованием учетных данных;
- просмотр и изменение текущей конфигурации подсистемы безопасности Astra.Security;
- получение информации о статусе операций пользователя;
- выход из подсистемы безопасности.

Компоненты расширения Astra.HMI.Security обращаются к подсистеме безопасности Astra.Security с помощью API: свойств, функций и событий



1. Компонент Astra.HMI.Security отправляет запрос на просмотр или изменение конфигурации подсистемы безопасности в Агент Astra.Security.
2. Агент Astra.Security находит нужную информацию на LDAP-сервере или записывает новую конфигурацию на LDAP-сервер.
3. Агент Astra.Security предоставляет результат операции в проект Astra.HMI с помощью компонентов Astra.HMI.Security.

Информация на LDAP-сервере также может быть изменена с помощью Конфигуратор Astra.Security.

1.2.4.1. Компоненты

Компонент	Описание
Контекст безопасности	Предназначен для взаимодействия с подсистемой безопасности Astra.Security
Список пользователей	Позволяет извлекать и обновлять список пользователей подсистемы безопасности Astra.Security
Настройка безопасности: Контроль целостности	Компонент позволяет контролировать целостность указанных файлов и папок
Строковый элемент безопасности	Обеспечивает связь со строковым правом подсистемы безопасности Astra.Security
Булевский элемент безопасности	Обеспечивает связь с логическим правом подсистемы безопасности Astra.Security
Настройка безопасности: Менеджер	Используется для конфигурирования подсистемы безопасности Astra.Security из проектов Astra.HMI
Настройка безопасности: Приложение	Предназначен для загрузки информации о приложении
Настройка безопасности: Пользователь	Предназначен для загрузки информации об учетной записи
Настройка безопасности: Группа	Предназначен для загрузки информации о группе
Мастер конфигурирования Security	Предназначен для чтения и обновления конфигурации службы Агент Astra.Security
Информация лицензирования: Получение	Компонент предназначен для получения информации о лицензировании

1.2.4.1.1. Контекст безопасности

Компонент позволяет взаимодействовать с подсистемой безопасности Astra.Security.

1.2.4.1.1.1. События

Событие	Описание
LoginRejected	Отклонение аутентификации пользователя
PasswordExpiration	Истечение срока действия пароля пользователя или приближение к времени истечении срока действия пароля
ConnectedChanged	Изменение текущего подключения к Astra.Net.Agent
CurrentUserChanged	Смена текущего пользователя
LoginStarted	Начало аутентификации пользователя
LoginFailed	Появление ошибки при аутентификации пользователя
AuditFailed	Сигнал об ошибке логгирования сообщения
ForceStopUserSessionFinished	Сигнал об успешном принудительном завершении сеанса пользователя
ResetUserFailedLoginCounterFinished	Сигнал об успешном сбросе таймаута по превышению количества неуспешных попыток ввода пароля
RemoteGetLoggedUsersFinished	Получение списка текущих пользователей на удаленной рабочей станции в сети Astra.Net
RemoteGetLoggedUsersFailed	Не удалось получить список текущих пользователей на удаленной рабочей станции в сети Astra.Net

1.2.4.1.1.1.1. LoginRejected

Отклонение попытки входа подсистемой безопасности Astra.Security.

Активируется в момент входа при:

- вводе неверных учетных данных;
- истечении срока действия пароля;
- отсутствии прав на вход.

Параметры

Параметр	Тип	Описание
errorMessage	string	Сообщение с причиной отклонения входа

1.2.4.1.1.1.2. PasswordExpiration

Уведомление об истечении срока действия пароля.

Активируется при входе с учетными данными в случае, если оставшееся время действия пароля находится внутри срока уведомления о смене пароля.

Параметры

Параметр	Тип	Описание
timeRemain	int4	Время, оставшееся до окончания действия пароля.

Событие можно использовать при наличии у текущего пользователя права Уведомление о смене пароля, дней (PasswordNotifyForChange). Назначить право можно в Конфигуратор Astra.Security.

1.2.4.1.1.1.3. ConnectedChanged

Изменение текущего подключения к Astra.Net.Agent.

Активируется в момент разрыва или появления соединения с Агент Astra.Security.

Параметры

Параметр	Тип	Описание
connected	bool	Новое состояние подключения

Значение

Значение	Описание
true	Есть соединение с Агент Astra.Security
false	Нет соединения с Агент Astra.Security

1.2.4.1.1.1.4. CurrentUserChanged

Смена текущего пользователя.

Активируется в момент регистрации подсистемой безопасности нового текущего пользователя.

Параметры

Параметр	Тип	Описание
user	string	Имя нового пользователя

Возвращаемое значение

Возвращает логин текущего пользователя в параметр user.

1.2.4.1.1.1.5. LoginStarted

Запуск попытки аутентификации пользователя.

Активируется в момент передачи введенных учетных данных подсистеме безопасности Astra.Security.

1.2.4.1.1.1.6. LoginFailed

Возникновение ошибки при попытке входа.

Активируется при проблемах соединения с Агент Astra.Security.

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.1.1.7. AuditFailed

Данный сигнал уведомляет об ошибке логирования сообщения пользователя в аудит.

Аудит – это запись сообщений в базу данных на сервере.

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.1.1.8. ForceStopUserSessionFinished

Текущая сессия пользователя завершена.

Активируется в случае успешного завершения операции ForceStopUserSession().

1.2.4.1.1.1.9. ResetUserFailedLoginCounterFinished

Счетчик неудачных попыток входа пользователя сброшен.

Активируется в случае успешного завершения операции ResetUserFailedLoginCounter().

1.2.4.1.1.1.10. RemoteGetLoggedUsersFinished

Получен список текущих пользователей на удаленной рабочей станции в сети Astra.Net.

Активируется в случае успешного завершения операции RemoteGetLoggedUsersList(). Список помещается во внутреннее хранилище компонента.

Чтобы воспользоваться данными из списка, используйте функции GetRemoteLoggedUserCount() и GetRemoteLoggedUserByIndex().

1.2.4.1.1.1.11. RemoteGetLoggedUsersFailed

Не удалось получить список текущих пользователей на удаленной рабочей станции в сети Astra.Net.

Активируется в случае неуспешного завершения операции RemoteGetLoggedUsersList().

Значение

Значение	Описание
1	Не удалось отправить запрос на удаленную машину
2	Имя удаленной машины совпадает с именем локальной

1.2.4.1.1.2. Функции

Функция	Описание
GroupDisplayName	Возвращает отображаемое имя группы по указанному индексу
Group	Возвращает идентификатор группы по указанному индексу группы
Logout	Выход пользователя из подсистемы безопасности
ChangePassword	Меняет пароль текущего пользователя
AsyncLoginWithPasswordChange	Асинхронная авторизация пользователя в подсистеме безопасности с последующей сменой пароля
AsyncLogin	Асинхронная авторизация пользователя в подсистеме безопасности по логину и паролю
Login	Авторизация пользователя в подсистеме безопасности
LogAudit	Логировать сообщение пользователя
LogAuditExt	Логировать сообщение пользователя
ForceStopUserSession	Принудительно завершить пользовательскую сессию
ResetUserFailedLoginCounter	Сброс таймаута по превышению количества неуспешных попыток ввода пароля
RemoteGetLoggedUsersList	Запрашивает список текущих пользователей на удаленной рабочей станции в сети Astra.Net
GetRemoteLoggedUserCount	Возвращает количество текущих пользователей на удаленной рабочей станции

GetRemoteLoggedUserByIndex	Возвращает логин одного из текущих пользователей на удаленной рабочей станции

1.2.4.1.1.2.1. GroupDisplayName

Возвращает отображаемое имя группы по указанному индексу.

GroupDisplayName(Index)

Параметры

Параметр	Тип	Описание
Index	uint8	Индекс группы

Нумерация групп пользователя в списке начинается с 0.

Примеры

Вызов: SecurityContext.GroupDisplayName(0)

1.2.4.1.1.2.2. Group

Возвращает идентификатор группы по указанному индексу группы.

Group(Index)

Параметры

Параметр	Тип	Описание
Index	uint8	Индекс группы

Нумерация групп пользователя в списке начинается с 0.

Примеры

Вызов: SecurityContext.Group(0)

1.2.4.1.1.2.3. Logout

Выход пользователя из подсистемы безопасности. Функция не требует входных параметров.

void Logout()

Примеры

Вызов: SecurityContext.Logout()
Результат: завершение сессии. Текущим пользователем становится дефолтный пользователь.

1.2.4.1.1.2.4. ChangePassword

Меняет пароль текущего пользователя.

ChangePassword (OldPassword, NewPassword)

Параметры

Параметр	Тип	Описание
OldPassword	string	Пароль пользователя
NewPassword	string	Новый пароль пользователя

Изменить пароль нельзя, если не истек минимальный срок действия пароля, указанный в праве Срок действия пароля, дней (PasswordAge).

Примеры

Вызов: SecurityContext.ChangePassword("OldPassword", "NewPassword")
Результат:

- пароль изменен;
- пароль не изменен.

1.2.4.1.1.2.5. AsyncLoginWithPasswordChange

Асинхронная авторизация пользователя в подсистеме безопасности с последующей сменой пароля. Активирует событие LoginStarted.

AsyncLoginWithPasswordChange (string Login, string OldPassword, NewPassword)

Параметры

Параметр	Тип	Описание
Login	string	Логин пользователя
OldPassword	string	Старый пароль пользователя
NewPassword	string	Новый пароль пользователя

Изменить пароль нельзя, если не истек минимальный срок действия пароля, указанный в праве Срок действия пароля, дней (PasswordAge).

Примеры

Вызов: SecurityContext.AsyncLoginWithPasswordChange("Login", "OldPassword", "NewPassword")
Результат:

- пароль изменен, вход произведен;
- пароль не изменен, вход не произведен.

1.2.4.1.1.2.6. AsyncLogin

Асинхронная авторизация пользователя в подсистеме безопасности по логину и паролю.

AsyncLogin(string Login, string Password)

Параметры

Параметр	Тип	Описание
Login	string	Логин пользователя
Password	string	Пароль пользователя

Примеры

Вызов: SecurityContext.AsyncLogin("Login", "Password")
Результат:

- вход произведен;
- вход не произведен.

1.2.4.1.1.2.7. Login

Авторизация пользователя в подсистеме безопасности. Активирует событие LoginStarted.

Login(string Login, string Password)

Параметры

Параметр	Тип	Описание
Login	string	Логин пользователя
Password	string	Пароль пользователя

Исполнение функции останавливает другие процессы в проекте до тех пор, пока вход не будет выполнен или не возникнет ошибка входа. Поэтому проект в режиме исполнения может зависать. Для входа лучше использовать функцию AsyncLogin.

Примеры

Вызов: SecurityContext.Login("Login", "Password")
Результат:

- вход произведен;
- вход не произведен.

1.2.4.1.1.2.8. LogAudit

Функция, записывающая сообщение аудита с указанной важностью.

Аудит – это запись сообщений от подсистемы безопасности в базу данных на сервере.

void LogAudit(string message, uint4 improtrance)

Параметры

Параметр	Тип	Описание
message	string	Сообщение, которое необходимо отправить на аудит
improtrance	uint4	Уровень важности сообщения, оцененный по четырехбальной шкале, где 0 – наиболее важное сообщение, 3 – наименее важное сообщение

Примеры

Вызов: SecurityContext.LogAudit("Обновил запись в журнале",2)

1.2.4.1.1.2.9. LogAuditExt

Функция, записывающая сообщение аудита с указанными важностью и типом.

Аудит – это запись сообщений от подсистемы безопасности в базу данных на сервере.

void LogAuditExt(string message, uint4 improtrance, string type)

Параметры

Параметр	Тип	Описание
message	string	Сообщение, которое необходимо отправить на аудит
improtrance	uint4	Уровень важности сообщения, оцененный по четрехбальной шкале, где 0 – наиболее важное сообщение, 3 – наименее важное сообщение
type	string	Тип сообщения. Здесь следует указать одно из значений, описанных при настройке аудита в конфигурационном файле Astra.Security - astra.security.agent.xml. По умолчанию - Normal или Admin

Примеры

Вызов: SecurityContext.LogAuditExt("Обновил запись в журнале",2,"Normal")

1.2.4.1.1.2.10. ForceStopUserSession

Завершает текущую сессию пользователя.

Завершить сессию можно как на локальном АРМ, так и на удаленном АРМ, входящем в сеть Astra.Net.

void ForceStopUserSession(string Login, string NetName)

Параметры

Параметр	Тип	Описание
Login	string	Логин учетной записи пользователя
NetName	string	Имя узла в сети Astra.Net. Для завершения сессии на локальном АРМ имя узла в сети Astra.Net указывать не нужно

Примеры

Вызов: SecurityContext.ForceStopUserSession("login","NetName")

1.2.4.1.1.2.11. ResetUserFailedLoginCounter

Сбрасывает счетчик неудачных попыток входа пользователя.
Сбросить счетчик можно как для попыток входа на локальном АРМ, так и на удаленном АРМ, входящем в сеть Astra.Net.

void ResetUserFailedLoginCounter(string Login, string NetName)

Параметры

Параметр	Тип	Описание
Login	string	Логин учетной записи пользователя
NetName	string	Имя узла в сети Astra.Net. Для сброса счетчика на локальном АРМ имя узла в сети Astra.Net указывать не нужно

Для использования счетчика неудачных попыток входа пользователю должно быть назначено право Количество неуспешных попыток входа до временной блокировки, шт (MaxAttemptsCount).

Примеры

Вызов: ResetUserFailedLoginCounter("Login","NetName")

1.2.4.1.1.2.12. RemoteGetLoggedUsersList

Запрашивает список текущих пользователей на удаленной рабочей станции в сети Astra.Net.

void RemoteGetLoggedUsersList(string NetName)

В случае успешной активации события RemoteGetLoggedUsersFinished список поместится во внутреннее хранилище компонента. Чтобы воспользоваться данными из списка, используйте функции GetRemoteLoggedUserCount() и GetRemoteLoggedUserByIndex().

Параметры

Параметр	Тип	Описание
NetName	string	имя узла в сети Astra.Net. Для завершения сессии на локальном АРМ имя узла в сети Astra.Net указывать не нужно

Примеры

Вызов: RemoteGetLoggedUsersList("NetName")
Результат:

- в случае успешного завершения операции активируется событие RemoteGetLoggedUsersFinished;
- в случае неуспешного завершения операции активируется событие RemoteGetLoggedUsersFailed.

1.2.4.1.1.2.13. GetRemoteLoggedUserCount

Возвращает количество текущих пользователей на удаленной рабочей станции. Может использоваться только после вызова функции RemoteGetLoggedUsersList().

Функция не требует входных параметров.

uint4 GetRemoteLoggedUserCount()

В случае успешной активации события RemoteGetLoggedUsersFinished список поместится во внутреннее хранилище компонента. Чтобы воспользоваться данными из списка, используйте функции GetRemoteLoggedUserCount() и GetRemoteLoggedUserByIndex().

Примеры

Вызов: SecurityContext.GetRemoteLoggedUserCount()

1.2.4.1.1.2.14. GetRemoteLoggedUserByIndex

Возвращает логин одного из текущих пользователей на удаленной рабочей станции. Может использоваться только после вызова функции RemoteGetLoggedUsersList.

string GetRemoteLoggedUserByIndex(uint4 index)

Нумерация пользователей в списке начинается с 0.

Параметры

Параметр	Тип	Описание
index	uint4	Порядковый номер пользователя в списке, полученном в результате вызова функции RemoteGetLoggedUsersList()

Примеры

Вызов: SecurityContext.GetRemoteLoggedUserByIndex(4)

1.2.4.1.1.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта (поля объекта)
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
GroupCount	Свойство, которое отображает количество групп текущего пользователя
PasswordChangeError	Текст ошибки последней операции смены пароля пользователя
LoginRejectReason	Причина отклонения последней авторизации пользователя в подсистеме безопасности
LoginError	Текст ошибки при неудачной попытке авторизации
PasswordExpiresIn	Остаток времени действия пароля пользователя в секундах
PasswordExpiresSoon	Свойство уведомляет о скором сроке истечения действия пароля пользователя
PasswordExpires	Наличие ограничений на минимальный / максимальный срок действия пароля
SessionExpiresIn	Остаток времени сессии пользователя в секундах
SessionDurationLimit	Максимальная длительность сессии пользователя в секундах
SessionStartTime	Метка времени подключения текущего пользователя к подсистеме безопасности
ConnectionError	Текст ошибки установки связи с Astra.Net.Agent
Connected	Состояние подключения к Astra.Net.Agent
GuestMode	Текущее состояние гостевого режима

CurrentUserDisplayName	Отображаемое имя текущего пользователя подсистемы безопасности
CurrentUserId	Уникальный идентификатор текущего пользователя подсистемы безопасности
CurrentUser	Логин текущего пользователя, авторизованного в подсистеме безопасности
InactiveRemainTime	Оставшееся время неактивности пользователя

1.2.4.1.1.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.1.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.1.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.1.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.1.3.5. GroupCount

Свойство, которое отображает количество групп текущего пользователя.

uint8 GroupCount

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityContext.GroupCount
Пример значения: 2.

1.2.4.1.1.3.6. PasswordChangeError

Текст ошибки последней операции смены пароля пользователя.

string PasswordChangeError

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityContext.PasswordChangeError
Пример значения: Не вышел минимальный срок действия пароля.

1.2.4.1.1.3.7. LoginRejectReason

Причина отклонения последней авторизации пользователя в подсистеме безопасности.

string LoginRejectReason

Доступно только для чтения в режиме рантайма.

Подсистема безопасности отклоняет вход при:

- вводе неверных учетных данных;
- истечении срока действия пароля;
- отсутствии прав на вход.

Примеры

Вызов: SecurityContext.LoginRejectReason
Пример значения: Неверные учетные данные.

1.2.4.1.1.3.8. LoginError

Текст ошибки при неудачной попытке авторизации.

string LoginError

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityContext.LoginError
Пример значения: На узле 'LOCAL' зафиксирована ошибка: Служба 'SECURITYAGENT' не зарегистрирована.

1.2.4.1.1.3.9. PasswordExpiresIn

Остаток времени действия пароля пользователя в секундах. Если срок действия пароля неограничен, свойство равно 0.

uint4 PasswordExpiresIn

Доступно только для чтения в режиме рантайма.

В момент, когда пользователь меняет пароль, запускается таймер, отсчитывающий оставшееся время действия пароля.
Значение срока действия пароля для текущего пользователя указано в праве Срок действия пароля, дней (PasswordAge). Назначить право можно в Конфигуратор Astra.Security.
По истечении указанного в праве времени попытки входа пользователя отклоняются подсистемой безопасности Astra.Security. Узнать о том, что срок действия пароля истек, можно с помощью события LoginRejected компонента Контекст безопасности.

Примеры

Вызов: SecurityContext.PasswordExpiresIn

1.2.4.1.1.3.10. PasswordExpiresSoon

Свойство уведомляет о скором сроке истечения действия пароля пользователя. Свойство связано с параметром PasswordNotifyForChange подсистемы безопасности Astra.Security.

bool PasswordExpiresSoon

Доступно только для чтения в режиме рантайма.

Значение свойства связано со значениями прав Срок действия пароля, дней (PasswordAge) и Уведомление о смене пароля, дней (PasswordNotifyForChange) текущего пользователя. Оставшееся время действия пароля сравнивается со сроком уведомления о смене пароля.
Назначить права можно в Конфигуратор Astra.Security.

Значение

Значение	Описание
true	Оставшееся время действия пароля пользователя меньше или равно параметру PasswordNotifyForChange подсистемы безопасности Astra.Security
false	Оставшееся время действия пароля пользователя больше параметра PasswordNotifyForChange подсистемы безопасности Astra.Security

Примеры

Вызов: SecurityContext.PasswordExpiresSoon

1.2.4.1.1.3.11. PasswordExpires

Наличие ограничений на минимальный/максимальный срок действия пароля.

bool PasswordExpires

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Ограничения есть
false	Ограничений нет

Примеры

Вызов: SecurityContext.PasswordExpires

1.2.4.1.1.3.12. SessionExpiresIn

Остаток времени сессии пользователя в секундах.

uint4 SessionExpiresIn

Доступно только для чтения в режиме рантайма.

В момент, когда пользователь совершает вход с личными учетными данными, запускается таймер, отсчитывающий оставшееся время до завершения сессии.
Значение максимального времени длительности сессии для текущего пользователя указано в праве Максимальное время сессии, мин (SessionDurationLimit). Назначить право можно в Конфигуратор Astra.Security.
По истечении указанного в праве времени сессия текущего пользователя автоматически завершается.

Примеры

Вызов: SecurityContext.SessionExpiresIn

1.2.4.1.1.3.13. SessionDurationLimit

Максимальная длительность сессии пользователя в секундах. По истечении указанного времени сессия пользователя завершится.

uint4 SessionDurationLimit

Доступно только для чтения в режиме рантайма.

Значение максимальной длительности сессии для текущего пользователя указано в праве Максимальное время сессии, мин (SessionDurationLimit). Назначить право можно в Конфигуратор Astra.Security.

Примеры

Вызов: SecurityContext.SessionDurationLimit
Пример значения: 120.

1.2.4.1.1.3.14. InactiveRemainTime

Оставшееся время неактивности пользователя, с.

uint4 InactiveRemainTime

Только для чтения в режиме рантайма.

В момент, когда пользователь перестает взаимодействовать с АРМ, запускается таймер, отсчитывающий оставшееся время неактивности.

Значение максимального времени неактивности для текущего пользователя указано в праве Максимальное время бездействия, мин (MaxIdleTime). Назначить право можно в Конфигуратор Astra.Security.

По истечении указанного в праве времени сессия текущего пользователя автоматически завершается.

Для отслеживания активности должен выполняться процесс Astra.Security CheckActivity Executable, запускаемый утилитой astra.security.useractivity.exe.

Примеры

Вызов: SecurityContext.InactiveRemainTime

1.2.4.1.1.3.15. SessionStartTime

Метка времени подключения текущего пользователя к подсистеме безопасности.

timestamp SessionStartTime

Доступно только для чтения в режиме рантайма.

Примеры

Пример вызова: Text_Msg.Text = DateTime.ToString(SecurityContext.SessionStartTime)
Пример значения: 13.08.2021 09:20:14 после применения функции DateTime.ToString().

1.2.4.1.1.3.16. ConnectionError

Текст ошибки установки связи с Astra.Net.Agent.

string ConnectionError

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityContext.ConnectionError
Пример значения: Соединение с Net агентом разорвано. Код ошибки1.

1.2.4.1.1.3.17. Connected

Состояние подключения к Astra.Net.Agent.

bool Connected

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Связь установлена
false	Связь не установлена

Примеры

Вызов: SecurityContext.Connected

1.2.4.1.1.3.18. GuestMode

Текущее состояние гостевого режима.

bool GuestMode

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Пользователь использует подсистему безопасности как гость
false	Пользователь вошел в подсистему безопасности по логину и паролю

Примеры

Вызов: SecurityContext.CurrentUser

1.2.4.1.1.3.19. CurrentUserDisplayName

Отображаемое имя текущего пользователя подсистемы безопасности.

string CurrentUserDisplayName

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityContext.CurrentUserDisplayName
Пример значения: Иванов.

1.2.4.1.1.3.20. CurrentUserId

Уникальный идентификатор текущего пользователя подсистемы безопасности.

string CurrentUserId

Доступно только для чтения в режиме рантайма.

Уникальный идентификатор формируется подсистемой безопасности в момент создания учетной записи.

Примеры

Вызов: SecurityContext.CurrentUserId
Вид значения: astra:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Пример значения: astra:c3a997b1-326e-42ee-8907-e359fc17feb7.

1.2.4.1.1.3.21. CurrentUser

Логин текущего пользователя, авторизованного в подсистеме безопасности.

string CurrentUser

Доступно только для чтения в режиме рантайма.

С момента ввода корректных учетных данных подсистема безопасности регистрирует вошедшего как текущего пользователя. Для всех свойств, функций и событий предоставляется контекст текущего пользователя.

Примеры

Вызов: SecurityContext.CurrentUser
Пример значения: ivanov.

1.2.4.1.2. Список пользователей

Компонент позволяет:

- извлекать список пользователей подсистемы безопасности Astra.Security;
- обновлять извлеченный список пользователей.

1.2.4.1.2.1. События

Событие	Описание
UpdateFinished	Завершение обновления списка пользователей
UpdateStarted	Запуск обновления списка пользователей

1.2.4.1.2.1.1. UpdateFinished

Извлечение или обновление списка пользователей завершено.

1.2.4.1.2.1.2. UpdateStarted

Запущено извлечение или обновление списка пользователей.

Активируется в результате успешного завершения операции BeginUpdate().

1.2.4.1.2.2. Функции

Компонент	Описание
GetLoginName	Предоставляет логин пользователя по номеру в списке
GetDisplayName	Предоставляет имя пользователя по номеру в списке
BeginUpdate	Запускает извлечение или обновление списка пользователей

1.2.4.1.2.2.1. GetLoginName

Предоставляет логин пользователя по номеру в списке.

string GetLoginName(uint8 number)

Параметры

Параметр	Тип	Описание
number	uint8	Порядковый номер логина пользователя в списке

Нумерация логинов пользователей в списке начинается с 0.

Примеры

Вызов: UserList.GetLoginName(0)

```
i: var = 0;
while (i < Count)
//для всех учетных записей (Count)
{
ComboBox_UserList.AddItem(GetLoginName(i));
//добавление в выпадающий список всех логинов пользователей
i+=1;
}
```

1.2.4.1.2.2.2. GetDisplayName

Предоставляет имя пользователя по номеру в списке.

string GetDisplayName(uint8 number)

Параметры

Параметр	Тип	Описание
number	uint8	Порядковый номер имени пользователя в списке

Нумерация имен пользователей в списке начинается с 0.

Примеры

```
Вызов: UserList.GetDisplayName(0)
i: var = 0;
while (i < Count)
//для всех учетных записей (Count)
{
ComboBox_UserList.AddItem(GetDisplayName(i));
//добавление в выпадающий список всех имен пользователей
i+=1;
}
```

1.2.4.1.2.2.3. BeginUpdate

Запускает извлечение или обновление списка пользователей.

Функция не требует входных параметров.

void BeginUpdate()

1.2.4.1.2.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта (поля объекта)
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
Error	Текст ошибки при работе со списком пользователей
HasError	Признак наличия ошибки при работе со списком пользователей
IsUpdatePending	Статус выполнения процедуры обновления списка пользователей
Count	Возвращает количество пользователей в списке

1.2.4.1.2.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.2.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.2.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.2.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.2.3.5. Контекст безопасности

Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом. Указывается на вкладке Редактор свойств.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.2.3.6. Error

Текст ошибки при работе со списком пользователей. Например, ошибка во время запроса.

string Error

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: UserList.Error

1.2.4.1.2.3.7. HasError

Наличие ошибок при извлечении или обновлении списка пользователей.

bool HasError

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: UserList.HasError

1.2.4.1.2.3.8. IsUpdatePending

Статус обновления списка пользователей.

bool IsUpdatePending

Значение

Значение	Описание
true	Список пользователей обновляется
false	Список пользователей не обновляется

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: UserList.IsUpdatePending

1.2.4.1.2.3.9. Count

Количество пользователей в списке, извлеченном из подсистемы безопасности.

uint8 Count

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: UserList.Count

1.2.4.1.3. Настройка безопасности: Контроль целостности

Подсистема безопасности Astra.Security позволяет контролировать целостность указанных файлов и папок. На основе контрольной суммы файлов и папок создается эталон состояния. Когда необходимо проверить их целостность, считается текущая контрольная сумма и сравнивается с эталонным значением.

Компонент Настройка безопасности: Контроль целостности предназначен для:

- создания эталона состояния файлов и папок;
- выполнения проверок состояния файлов и папок;
- получения информации об изменениях в файлах и папках.

1.2.4.1.3.1. События

Событие	Описание
GetListFailed	Появление ошибки получения списка контролируемых файлов
ListIsReady	Завершение подготовки списка контролируемых файлов
CreateFailed	Появление ошибки при создании эталонного файла
CreateFinished	Завершение создания эталонного файла
UpdateFailed	Появление ошибки при обновлении списка контролируемых файлов
UpdateFinished	Завершение обновления списка контролируемых файлов
RemoteUpdateFinished	Сигнал о завершении обновления контрольных значений на удаленном ноде
RemoteUpdateFailed	Сигнал о неуспешном завершении операции обновления контрольных значений на удаленном ноде
RemoteCreateFinished	Сигнал о завершении создания эталонного файла на удаленном ноде
RemoteCreateFailed	Сигнал о неуспешном завершении операции создания эталона на удаленном ноде
RemoteListIsReady	Результат проверки целостности файлов на удаленной рабочей станции в сети Astra.Net получен
RemoteGetListFailed	Результат проверки целостности файлов на удаленной рабочей станции в сети Astra.Net не получен

1.2.4.1.3.1.1. GetListFailed

Не удалось получить результат проверки целостности файлов.

Активируется в случае неуспешного завершения операции Get_IC_List().

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.1.2. ListIsReady

Получен результат проверки целостности файлов.

Активируется в случае успешного завершения операции Get_IC_List().

Возвращает данные в JSON-формате в переменную IC_List_JSON.

1.2.4.1.3.1.3. CreateFailed

Не удалось создать эталон состояния файлов.

Активируется в случае неуспешного завершения операции Create_IC_Etalon().

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.1.4. CreateFinished

Создан эталон состояния файлов.

Активируется в случае успешного завершения операции Create_IC_Etalon().

1.2.4.1.3.1.5. UpdateFailed

Не удалось выполнить проверку целостности файлов.

Активируется в случае неуспешного завершения операции Update_IC().

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.1.6. UpdateFinished

Выполнена проверка целостности файлов.

Активируется в случае успешного завершения операции Update_IC().

1.2.4.1.3.1.7. RemoteUpdateFinished

Выполнена проверка целостности файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае успешного завершения операции UpdateRemote_IC().

1.2.4.1.3.1.8. RemoteUpdateFailed

Не удалось выполнить проверку целостности файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае неуспешного завершения операции UpdateRemote_IC().

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.1.9. RemoteCreateFinished

Создан эталон состояния файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае успешного завершения операции CreateRemote_IC_Etalon.

1.2.4.1.3.1.10. RemoteCreateFailed

Не удалось создать эталон состояния файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае неуспешного завершения операции CreateRemote_IC_Etalon.

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.1.11. RemoteListIsReady

Получен результат проверки целостности файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае успешного завершения операции GetRemote_IC_List.

Возвращает данные в JSON-формате в переменную IC_List_JSON.

1.2.4.1.3.1.12. RemoteGetListFailed

Не удалось получить результат проверки целостности файлов на удаленной рабочей станции в сети Astra.Net.

Активируется в случае неуспешного завершения операции GetRemote_IC_List.

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.3.2. Функции

Компонент	Описание
Create_IC_Etalon	Создает эталонный файл
Get_IC_List	Вычисляет контрольную сумму файлов
Update_IC	Вычисляет контрольную сумму файлов
UpdateRemote_IC	Вычисляет контрольные суммы на удаленном рабочем месте
GetRemote_IC_List	Получить список контролируемых файлов с удаленного рабочего места
CreateRemote_IC_Etalon	Создать эталонный файл на удаленном рабочем месте

1.2.4.1.3.2.1. Create_IC_Etalon

Создает эталонный файл.

void Get_IC_Etalon()

Создает эталон на основе текущего состояния файлов и папок:

- вычисляет текущую контрольную сумму;
- сохраняет значение в качестве эталонного.

Функция не требует входных параметров.

Примеры

Вызов: SecurityIntegrityControl.Create_IC_Etalon()
Результат:

- в случае успешного завершения операции активируется событие CreateFinished;
- в случае неуспешного завершения операции активируется событие CreateFailed.

1.2.4.1.3.2.2. Get_IC_List

Запрашивает результат проверки целостности файлов и папок.

Функция не требует входных параметров.

void Get_IC_List()

Примеры

Вызов: SecurityIntegrityControl.Get_IC_List()
Результат:

- в случае успешного завершения операции активируется событие ListIsReady;
- в случае неуспешного завершения операции активируется событие GetListFailed.

1.2.4.1.3.2.3. Update_IC

Вычисляет контрольную сумму файлов.

void Update_IC()

Выполняет проверку целостности файлов и папок:

- вычисляет текущую контрольную сумму;
- сравнивает результат с эталонным значением.

Функция не требует входных параметров.

Примеры

Вызов: SecurityIntegrityControl.Update_IC()
Результат:

- в случае успешного завершения операции активируется событие UpdateFinished;
- в случае неуспешного завершения операции активируется событие UpdateFailed.

1.2.4.1.3.2.4. UpdateRemote_IC

Вычисляет контрольные суммы на удаленном рабочем месте.

void UpdateRemote_IC(string netName)

Параметры

Параметр	Тип	Описание
netName	string	Имя рабочей станции в сети Astra.Net

Примеры

Вызов: SecurityIntegrityControl.UpdateRemote_IC("Netname")
Результат:

- в случае успешного завершения операции активируется событие RemoteUpdateFinished;
- в случае неуспешного завершения операции активируется событие RemoteUpdateFailed.

1.2.4.1.3.2.5. GetRemote_IC_List

Получить список контролируемых файлов с удаленного рабочего места. Аналогично функции Get_IC_List(), но на удаленной рабочей станции в сети Astra.Net.

void GetRemote_IC_List(string netName)

Параметры

Параметр	Тип	Описание
netName	string	Имя рабочей станции в сети Astra.Net

Примеры

Вызов: SecurityIntegrityControl.GetRemote_IC_List("Netname")
Результат:

- в случае успешного завершения операции активируется событие RemoteListIsReady;
- в случае неуспешного завершения операции активируется событие RemoteGetListFailed.

1.2.4.1.3.2.6. CreateRemote_IC_Etalon

Создать эталонный файл на удаленном рабочем месте. Аналогично функции Create_IC_Etalon(), но на удаленной рабочей станции в сети Astra.Net.

void CreateRemote_IC_Etalon(string netName)

Параметры

Параметр	Тип	Описание
netName	string	Имя удаленного рабочего места

Примеры

Вызов: SecurityIntegrityControl.CreateRemote_IC_Etalon("Netname")
Результат:

- в случае успешного завершения операции активируется событие RemoteCreateFinished;
- в случае неуспешного завершения операции активируется событие RemoteCreateFailed.

1.2.4.1.3.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
IC_List_JSON	Список контролируемых файлов в формате JSON

1.2.4.1.3.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.3.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.3.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.3.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.3.3.5. Контекст безопасности

Ссылка на элемент типа Контекст безопасности, обеспечивающий взаимодействие с подсистемой безопасности Astra.Security. Указывается на вкладке Редактор свойств.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.3.3.6. IC_List_JSON

Список контролируемых файлов в формате JSON.

JSON IC_List_JSON

Доступно только для чтения в режиме рантайма.

Примеры


```
{
"date_last_check": "01.01.2021 00:00:01",
"creator": "Guest(name)",
"date_etalon_created": "01.01.2021 00:00:00",
"data": [
 {
  "ID": "0",
  "ParentID": "-1",
  "Dir": "1",
  "hasRefValue": "0",
  "name": "C:\\Users\\controled objects",
  "MD5_onStart": "",
  "date_onStart": "01.01.2021 00:00:00",
  "status": "4",
  "MD5_current": "",
  "date_current": "",
  "MD5_etalon": "",
  "date_etalon": ""
 },
 {
  "ID": "1",
```

```
 "ParentID": "0",
 "Dir": "0",
 "hasRefValue": "0",
 "name": "ex1.txt",
 "MD5_onStart": "cadf2174b6ff3f2d027ee2393ff0a392",
 "date_onStart": "01.01.2021 00:00:00",
 "status": "4",
 "MD5_current": "cadf2174b6ff3f2d027ee2393ff0a392",
 "date_current": "01.01.2021 00:00:00",
 "MD5_etalon": "",
 "date_etalon": ""
 }
]
}
```


Основной является следующая информация:

- date_last_check – дата последней проверки целостности;
- date_etalon_created – дата создания эталона;
- Dir – флаг директории:
  - 1: проверяемый объект – директория;
  - 0: проверяемый объект – файл;
- status – состояние проверяемого объекта:
  - 0 – ошибок нет;
  - 4 – файл не существует;
  - 8 – нарушена целостность файла (контрольные суммы не совпадают).

1.2.4.1.4. Строковый элемент безопасности

Компонент, обеспечивающий связь со строковым правом подсистемы безопасности Astra.Security.

Связь позволяет получать разрешения и запреты для текущего пользователя.

1.2.4.1.4.1. События

Событие	Описание
ConnectedChanged	Изменение подключения между Security context и Astra.Security.Agent
ValueChanged	Изменение значения права при входе пользователя

1.2.4.1.4.1.1. ConnectedChanged

Смена состояния подписки на право.

Параметры

Параметр	Тип	Описание
connected	bool	Текущее значение

1.2.4.1.4.1.2. ValueChanged

Смена текущего значения права.

Параметры

Параметр	Тип	Описание
value	bool	Текущее значение

1.2.4.1.4.2. Функции

Компонент	Описание
GetForbidden	Возвращает запрет строкового права по индексу запрета
GetAllowed	Возвращает разрешение строкового права по индексу разрешения

1.2.4.1.4.2.1. GetForbidden

Предоставляет запрет текущего пользователя из права, связанного с элементом.

string GetForbidden(uint8 number)

Нумерация запретов начинается с 0.

Параметры

Параметр	Тип	Описание
number	uint8	Порядковый номер запрета в списке запретов текущего пользователя

1.2.4.1.4.2.2. GetAllowed

Предоставляет разрешение текущего пользователя из права, связанного с элементом.

string GetAllowed(uint8 number)

Нумерация разрешений начинается с 0.

Параметры

Параметр	Тип	Описание
number	uint8	Порядковый номер разрешения в списке разрешений текущего пользователя

1.2.4.1.4.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта (поля объекта)
Кардинальное число	Преобразует объект в массив и задает размер массива
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Error	Отображает ошибки, связанные с токеном
Connected	Свойство, которое отражает состояние подключения
ForbiddenCount	Количество запрещений в строковом праве
AllowedCount	Количество разрешений в строковом праве
Право	Название булевского или строкового права в подсистеме Astra.Security
Приложение	Приложение подсистемы Astra.Security, относительно которого применимо право

1.2.4.1.4.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.4.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.4.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.4.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.4.3.5. Контекст безопасности

Ссылка на элемент типа Контекст безопасности, обеспечивающий взаимодействие с подсистемой безопасности Astra.Security. Указывается на вкладке Редактор свойств.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.4.3.6. Приложение

Приложение подсистемы Astra.Security, относительно которого применимо право.

string Application

Примеры

Вызов: StringTokenProxy.Application

1.2.4.1.4.3.7. Право

Имя права, с которым связан элемент.

string Right

Примеры

Вызов: StringTokenProxy.Right

1.2.4.1.4.3.8. Error

Ошибка подписки.

string Error

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: StringTokenProxy.Error
Пример значения: Не удалось получить значение токена права. Объект не найден в хранилище LDAP

1.2.4.1.4.3.9. Connected

Состояние подписки на право.

Подписка – это состояние соединения элемента с указанным правом.

bool Connected

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Связь между Security context и Astra.Security.Agent установлена
false	Связи между Security context и Astra.Security.Agent нет

Примеры

Вызов: StringTokenProxy.Connected

1.2.4.1.4.3.10. ForbiddenCount

Количество запретов текущего пользователя в праве, связанном с элементом.

uint4 ForbiddenCount

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: StringTokenProxy.ForbiddenCount
Пример значения: 2.

1.2.4.1.4.3.11. AllowedCount

Количество разрешений текущего пользователя в праве, связанном с элементом.

uint4 AllowedCount

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: StringTokenProxy.AllowedCount
Пример значения: 1.

1.2.4.1.5. Булевский элемент безопасности

Компонент, обеспечивающий связь с логическим правом подсистемы безопасности Astra.Security.

Связь позволяет отслеживать изменение значения права для текущего пользователя.

1.2.4.1.5.1. События

Событие	Описание
ConnectedChanged	Изменение подключения между Security context и Astra.Security.Agent
ValueChanged	Изменение значения права при входе пользователя

1.2.4.1.5.1.1. ConnectedChanged

Смена состояния подписки на право.

Параметры

Параметр	Тип	Описание
connected	bool	Текущее значение

1.2.4.1.5.1.2. ValueChanged

Смена текущего значения права.

Параметры

Параметр	Тип	Описание
value	bool	Текущее значение

1.2.4.1.5.2. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта (поля объекта)
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
Error	Отображает ошибки, связанные с токеном
Connected	Свойство, которое отражает состояние подключения
Value	Значение булевского права, которое определено на сервере безопасности для текущего пользователя
Право	Название булевского или строкового права в подсистеме Astra.Security
Приложение	Приложение подсистемы Astra.Security, относительно которого применимо право

1.2.4.1.5.2.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.5.2.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.5.2.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.5.2.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.5.2.5. Контекст безопасности

Ссылка на элемент типа Контекст безопасности, обеспечивающий взаимодействие с подсистемой безопасности Astra.Security.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.5.2.6. Приложение

Приложение подсистемы Astra.Security, относительно которого применимо право.

string Application

Примеры

Вызов: BoolTokenProxy.Application
Пример значения: Управление состоянием оборудования.

1.2.4.1.5.2.7. Право

Название булевского или строкового права в подсистеме Astra.Security.

string Right

Примеры

Вызов: BoolTokenProxy.Right
Пример значения: Управление насосом.

1.2.4.1.5.2.8. Error

Ошибка подписки.

string Error

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: BoolTokenProxy.Error
Пример значения: Не удалось получить значение токена права. Объект не найден в хранилище LDAP

1.2.4.1.5.2.9. Connected

Состояние подписки на право.

bool Connected

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Связь между Security context и Astra.Security.Agent установлена
false	Связи между Security context и Astra.Security.Agent нет

Примеры

Вызов: BoolTokenProxy.Connected

1.2.4.1.5.2.10. Value

Значение булевского права, которое определено на сервере безопасности для текущего пользователя.

bool Value

Доступно только для чтения в режиме рантайма.

Значение

Значение	Описание
true	Разрешено
false	Запрещено

Примеры

Вызов: BoolTokenProxy.Value

1.2.4.1.6. Настройка безопасности: Менеджер

Компонент предназначен для:

- получения списков учетных записей, групп пользователей и приложений;
- удаления учетных записей, групп пользователей и приложений;
- создания и восстановления резервных копий конфигурации Astra.Security.

Используется для конфигурирования подсистемы безопасности Astra.Security из проектов Astra.HMI.

1.2.4.1.6.1. События

Событие	Описание
AgentStatusChanged	Изменение состояния Astra.Security.Agent
DeleteUserFailed	Появление ошибки при выполнении удаления пользователя
DeleteGroupFailed	Появление ошибки при выполнении удаления группы
DeleteApplicationFailed	Появление ошибки при выполнении удаления приложения
DeleteUserComplete	Завершение удаления пользователя
DeleteGroupComplete	Завершение удаления группы
DeleteApplicationComplete	Завершение удаления приложения
RequestUsersListFailed	Появление ошибки при выполнении запроса списка пользователей
RequestGroupListFailed	Появление ошибки при выполнении запроса списка групп
RequestAppListFailed	Появление ошибки при выполнении запроса списка приложений
RequestGroupListComplete	Завершении выполнения запроса списка групп
RequestUsersListComplete	Завершение выполнения запроса списка пользователей
RequestAppListComplete	Завершение выполнения запроса списка приложений
GetConfigurationFinished	Сигнал о завершении экспорта конфигурации LDAP
GetConfigurationFailed	Сигнал об ошибке в процессе выполнения экспорта конфигурации LDAP
SetConfigurationFinished	Сигнал о завершении импорта конфигурации LDAP

SetConfigurationFailed	Сигнал об ошибке в процессе выполнения импорта конфигурации LDAP
LastActionError	Ошибка выполнения последнего действия

1.2.4.1.6.1.1. AgentStatusChanged

Изменение текущего состояния Агент Astra.Security.

Все возможные состояния Агент Astra.Security описаны в свойстве AgentStatus.

1.2.4.1.6.1.2. DeleteUserFailed

Ошибка при удалении учетной записи из подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции DeleteUser().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.3. DeleteGroupFailed

Ошибка при удалении группы пользователей из подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции DeleteGroup().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.4. DeleteApplicationFailed

Ошибка при удалении приложения из подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции DeleteApplication().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.5. DeleteUserComplete

Учетная запись удалена из подсистемы безопасности Astra.Security.

Активируется в случае успешного завершения операции DeleteUser().

1.2.4.1.6.1.6. DeleteGroupComplete

Группа пользователей удалена из подсистемы безопасности Astra.Security.

Активируется в случае успешного завершения операции DeleteGroup().

1.2.4.1.6.1.7. DeleteApplicationComplete

Приложение удалено из подсистемы безопасности Astra.Security.

Активируется в случае успешного завершения операции DeleteApplication().

1.2.4.1.6.1.8. RequestUsersListFailed

Ошибка при получении списка пользователей подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции RequestUsersList().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.9. RequestGroupListFailed

Ошибка при получении списка групп пользователей подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции RequestGroupList().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.10. RequestAppListFailed

Ошибка при получении списка приложений подсистемы безопасности Astra.Security.

Активируется в случае неуспешного завершения операции RequestAppList().

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.6.1.11. RequestGroupListComplete

Получен список групп пользователей, имеющихся в подсистеме безопасности Astra.Security.

Активируется в случае успешного завершения операции RequestGroupList().

Параметры

Параметр	Тип	Описание
JSONAppList	string	Список групп в JSON формате

1.2.4.1.6.1.12. RequestUsersListComplete

Получен список пользователей, имеющихся в подсистеме безопасности Astra.Security.

Активируется в случае успешного завершения операции RequestUsersList().

Параметры

Параметр	Тип	Описание
JSONAppList	string	Список пользователей в JSON формате

1.2.4.1.6.1.13. RequestAppListComplete

Получен список приложений, имеющихся в подсистеме безопасности Astra.Security.

Активируется в случае успешного завершения операции RequestAppList().

Параметры

Параметр	Тип	Описание
JSONAppList	string	Список приложений в JSON формате

1.2.4.1.6.1.14. GetConfigurationFinished

Файл резервной копии конфигурации Astra.Security создан (или перезаписан) успешно.

Активируется в случае успешного завершения операции ExportConfiguration().

1.2.4.1.6.1.15. GetConfigurationFailed

Ошибка при создании (или перезаписи) файла резервной копии конфигурации Astra.Security.

Активируется в случае неуспешного завершения операции ExportConfiguration().

Возвращает код ошибки в переменную FailReason, если код ошибки равен:

- 2 – не удалось экспортировать конфигурацию из LDAP (например, не существует корневого каталога и т.д.);
- 3 – нет права на чтение конфигурации;
- 4 – не удалось открыть файл для записи конфигурации.

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки

1.2.4.1.6.1.16. SetConfigurationFinished

Резервная копия конфигурации Astra.Security восстановлена успешно.

Активируется в случае успешного завершения операции ImportConfiguration().

1.2.4.1.6.1.17. SetConfigurationFailed

Не удалось восстановить резервную копию конфигурации Astra.Security.

Активируется в случае неуспешного завершения операции ImportConfiguration().

Возвращает код ошибки в переменную FailReason, если код ошибки равен:

- 1 – файл резервной копии поврежден;
- 2 – не удалось зачистить базу данных LDAP перед применением конфигурации;
- 3 – произошла внутренняя ошибка LDAP;
- 4 – произошла непредвиденная ошибка на стороне агента;
- 5 – у пользователя нет права на редактирование конфигурации;
- 6 – другие ошибки;
- 7 – не удается открыть файл с конфигурацией.

1.2.4.1.6.1.18. LastActionError

Ошибка выполнения последнего действия.

Активируется в результате внесения в конфигурацию подсистемы безопасности таких изменений, которые могут привести к нарушению работы Astra.Security. Таким действием является, например, удаление учетной записи единственного администратора.

Параметры

Параметр	Тип	Описание
errorMessage	string	Текст ошибки

1.2.4.1.6.2. Функции

Компонент	Описание
GetErrorDescriptionByCode	Возвращает описание ошибки по коду
DeleteUser	Удаляет пользователя
DeleteGroup	Удаляет группу
DeleteApplication	Удаляет приложение
RequestUsersList	Запрашивает список пользователей
RequestGroupList	Запрашивает список групп
RequestAppList	Запрашивает список приложений
ExportConfiguration	Экспортировать конфигурацию
ImportConfiguration	Импортировать конфигурацию

1.2.4.1.6.2.1. GetErrorDescriptionByCode

Возвращает текстовое описание ошибок, возникающих при запросе и удалении приложений, групп пользователей и учетных записей.

string GetErrorDescriptionByCode(uint1 FailReason)

Параметры

Параметр	Тип	Описание
FailReason	uint1	Код ошибки из любого события, говорящего об ошибке

1.2.4.1.6.2.2. DeleteUser

Удаляет четную запись из подсистемы безопасности.

void DeleteUser(string UserUID)

Параметры

Параметр	Тип	Описание
UserUID	string	Уникальный идентификатор (uid) учетной записи

Удаление учетных записей доступно только пользователям с правами администратора.

Примеры

Вызов: SecurityManager.DeleteUser("astra:d01969e0-ae05-4548-9375-2533b326a588")

Результат:

- в случае успешного завершения операции активируется событие DeleteUserComplete();
- в случае неуспешного завершения операции активируется событие DeleteUserFailed().

1.2.4.1.6.2.3. DeleteGroup

Удаляет группу пользователей из подсистемы безопасности.

void DeleteGroup(string GroupUID)

Параметры

Параметр	Тип	Описание
GroupID	string	Уникальный идентификатор (uid) группы

Удаление групп пользователей доступно только пользователям с правами администратора.

Примеры

Вызов: SecurityManager.DeleteGroup("astra:d01969e0-ae05-4548-9375-2533b326a588")
Результат:

- в случае успешного завершения операции активируется событие DeleteGroupComplete;
- в случае неуспешного завершения операции активируется событие DeleteGroupFailed.

1.2.4.1.6.2.4. DeleteApplication

Удаляет приложение.

void DeleteApplication(string appName)

Параметры

Параметр	Тип	Описание
appName	string	Имя приложения

Примеры

Вызов: SecurityManager.DeleteApplication("Управление состоянием оборудования")
Результат:

- в случае успешного завершения операции активируется событие DeleteApplicationComplete;
- в случае неуспешного завершения операции активируется событие DeleteApplicationFailed.

1.2.4.1.6.2.5. RequestUsersList

Запрашивает список всех учетных записей, имеющихся в подсистеме безопасности Astra.Security.

Функция не требует входных параметров.

void RequestUsersList()

Просмотр списка учетных записей доступен только пользователям с правами администратора.

Примеры

Вызов: SecurityManager.RequestUsersList()
Результат:

- в случае успешного завершения операции активируется событие RequestUsersListComplete;
- в случае неуспешного завершения операции активируется событие RequestUsersListFailed.

1.2.4.1.6.2.6. RequestGroupList

Запрашивает список всех групп пользователей, имеющихся в подсистеме безопасности Astra.Security.

Функция не требует входных параметров.

void RequestGroupList()

Просмотр списка групп пользователей доступен только пользователям с правами администратора.

Примеры

Вызов: SecurityManager.RequestGroupList()
Результат:

- в случае успешного завершения операции активируется событие RequestGroupListComplete;
- в случае неуспешного завершения операции активируется событие RequestGroupListFailed.

1.2.4.1.6.2.7. RequestAppList

Запрашивает список всех приложений, имеющихся в подсистеме безопасности Astra.Security.

Функция не требует входных параметров.

void RequestAppList()

Примеры

Вызов: SecurityManager.RequestAppList()
Результат:

- в случае успешного завершения операции активируется событие RequestAppListComplete;
- в случае неуспешного завершения операции активируется событие RequestAppListFailed.

1.2.4.1.6.2.8. ExportConfiguration

Создает (или перезаписывает) файл резервной копии текущей конфигурации Astra.Security в указанном месте.

void ExportConfiguration(string fullPath)

Параметры

Параметр	Тип	Описание
fullPath	string	Полный путь к создаваемому файлу вместе с именем файла

Примеры

Вызов: SecurityManager.ExportConfiguration("D:/export.ldb")
Результат:

- в случае успешного завершения операции активируется событие GetConfigurationFinished;
- в случае неуспешного завершения операции активируется событие GetConfigurationFailed.

1.2.4.1.6.2.9. ImportConfiguration

Восстанавливает резервную копию конфигурации Astra.Security из указанного файла.

void ImportConfiguration(string fullPath)

Параметры

Параметр	Тип	Описание
fullPath	string	Полный путь к файлу резервной копии вместе с именем файла

Примеры

Вызов: SecurityManager.ImportConfiguration("D:/export.ldb")
Результат:

- в случае успешного завершения операции активируется событие SetConfigurationFinished;
- в случае неуспешного завершения операции активируется событие SetConfigurationFailed.

1.2.4.1.6.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
AgentStatus	Текущее состояние Astra.Security.Agent

1.2.4.1.6.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.6.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.6.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.6.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.6.3.5. Контекст безопасности

Ссылка на элемент типа Контекст безопасности, обеспечивающий взаимодействие с подсистемой безопасности Astra.Security.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.6.3.6. AgentStatus

Текущее состояние Astra.Security.Agent.

uint1 AgentStatus

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityManager.AgentStatus.

1.2.4.1.7. Настройка безопасности: Приложение

Компонент предназначен для загрузки информации о приложении:

- имеющемся в подсистеме безопасности – для просмотра и изменения этой информации;
- созданном из проекта Astra.HMI – для дальнейшей отправки в подсистему безопасности.

1.2.4.1.7.1. События

Событие	Описание
SaveFailed	Появление ошибки при сохранении приложения
SaveComplete	Завершение сохранения приложения
LoadFailed	Появление ошибки при загрузке приложения
LoadComplete	Завершение выполнения загрузки приложения

1.2.4.1.7.1.1. SaveFailed

Информация о приложении не сохранена в подсистему безопасности Astra.Security.

Активируется в случае неуспешного завершения операции Save().

Параметры

Параметр	Тип	Описание
FailReasonCode	string	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.7.1.2. SaveComplete

Информация о приложении сохранена в подсистему безопасности Astra.Security.

Активируется в случае успешного завершения операции Save().

1.2.4.1.7.1.3. LoadFailed

Информация о приложении не загружена в элемент.

Активируется в случае неуспешного завершения операции Load().

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.7.1.4. LoadComplete

Информация о приложении загружена в элемент.

Активируется в случае успешного завершения операции Load().

1.2.4.1.7.2. Функции

Компонент	Описание
GetErrorDescriptionByCode	Возвращает описание ошибки по коду
RoleDeleteRight	Удаляет значение права приложения подсистемы безопасности
RoleChangeRight	Изменяет значение права приложения подсистемы безопасности
RoleAddRight	Шаблон описания
DeleteRole	Удаляет одну из ролей приложения подсистемы безопасности
ChangeRole	Изменяет имя одной из ролей приложения подсистемы безопасности
CreateRole	Добавляет новую роль для приложения подсистемы безопасности
DeleteToken	Удаляет право приложения подсистемы безопасности
ChangeToken	Изменяет значение одного из прав приложения подсистемы безопасности
CreateToken	Добавляет новое право для приложения подсистемы безопасности
New	Создает новое приложение подсистемы безопасности
GetRoleRights	Возвращает список прав одной из роли приложения подсистемы безопасности
GetRolesList	Возвращает список ролей, добавленных в приложение подсистемы безопасности
GetTokensList	Возвращает список прав, настроенных для приложения
Save	Сохраняет данные приложения подсистемы безопасности

Load	Загружает данные приложения подсистемы безопасности

1.2.4.1.7.2.1. GetErrorDescriptionByCode

Возвращает текстовое описание ошибок, возникающих при загрузке и сохранении приложений.

string GetErrorDescriptionByCode(uint1 FailReasonCode)

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Код ошибки из любого события, говорящего об ошибке

1.2.4.1.7.2.2. RoleDeleteRight

Удаляет значение права приложения подсистемы безопасности.

void RoleDeleteRight(string AppName, string RoleID, string RightName)

Параметры

Параметр	Тип	Описание
AppName	string	Имя приложения
RoleID	string	Уникальный идентификатор (uid) роли
RightName	string	Имя права

Примеры

SecurityManagerApplication.RoleDeleteRight("appname","astra:4ce9483e-e137-41c2-bf1c-343e9b731f20","pravo")

1.2.4.1.7.2.3. RoleChangeRight

Изменяет значение права приложения подсистемы безопасности.

void RoleChangeRight(string AppName, string RoleID, string RightName, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppName	string	Имя приложения
RoleID	string	Уникальный идентификатор (uid) роли
RightName	string	Имя права
AllowedValue	string	Новое разрешающее значение права
ForbidenValue	string	Новое запрещающее значение права

Примеры

SecurityManagerApplication.RoleChangeRight("appname","astra:4ce9483e-e137-41c2-bf1c-343e9b731f20","pravo","закрыто","открыто")

1.2.4.1.7.2.4. RoleAddRight

Предоставляет для указанной роли право приложения, загруженного в элемент.

void RoleAddRight(string AppName, string RoleID, string RightName, uint1 RightType, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppName	string	Имя приложения
RoleID	string	Уникальный идентификатор (uid) роли
RightName	string	Имя права
RightType	uint1	Тип права. Значение: › 0 – тип string › 1 – тип bool
AllowedValue	string	Разрешающее значение права
ForbidenValue	string	Запрещающее значение права

Примеры

Sample: SecurityManagerApplication.RoleAddRight("appname","astra:4ce9483e-e137-41c2-bf1c-343e9b731f20","pravo",0,"открыто","закрыто")

1.2.4.1.7.2.5. DeleteRole

Удаляет одну из ролей приложения подсистемы безопасности.

void DeleteRole(string RoleID)

Параметры

Параметр	Тип	Описание
RoleID	string	Уникальный идентификатор (uid) роли

Примеры

Вызов: SecurityManagerApplication.DeleteRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20")

1.2.4.1.7.2.6. ChangeRole

Переименовывает роль из приложения, загруженного в элемент.

void ChangeRole(string RoleID, string RoleName)

Параметры

Параметр	Тип	Описание
RoleID	string	Уникальный идентификатор (uid) роли
RoleName	string	Новое имя роли

Примеры

Вызов: SecurityManagerApplication.ChangeRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20","newrolename")

1.2.4.1.7.2.7. CreateRole

Создает роль в указанном приложении.

void CreateRole(string RoleName, string AppName)

Параметры

Параметр	Тип	Описание
RoleName	string	Имя роли
AppName	string	Имя приложения, в котором создается роль

Примеры

Вызов: SecurityManagerApplication.CreateRole("role","app")

1.2.4.1.7.2.8. DeleteToken

Удаляет токен из приложения, загруженного в элемент.

void DeleteToken(string TokenID)

Параметры

Параметр	Тип	Описание
TokenID	string	ID токена

Примеры

Вызов: SecurityManagerApplication.DeleteToken("right")

1.2.4.1.7.2.9. ChangeToken

Меняет тип, имя и описание токена в приложении, загруженном в элемент.

void ChangeToken(string TokenID, uint1 TokenType, string TokenName, string Description)

Параметры

Параметр	Тип	Описание
TokenID	string	ID токена
TokenName	string	Новое имя токена
TokenType	uint1	Тип токена. Значение: › 0 – тип bool › 1 – тип string
Description	string	Новое описание токена

Входной параметр тип токена не будет требоваться в будущих версиях.

Примеры

Вызов: SecurityManagerApplication.ChangeToken("tokenID",1,"newname","new

1.2.4.1.7.2.10. CreateToken

Создает токен в приложении, загруженном в элемент.

void CreateToken(uint1 TokenType, string TokenName, string Description)

Параметры

Параметр	Тип	Описание
TokenType	uint1	Тип токена. Значение: › 0 – тип bool › 1 – тип string
TokenName	string	Имя токена
Description	string	Описание

Примеры

Вызов: SecurityManagerApplication.CreateToken(1,"right","description")

1.2.4.1.7.2.11. New

Освобождает элемент от загруженной в него информации для создания нового приложения.

Функция не требует входных параметров.

void New()

После создания нового приложения не забудьте загрузить его в подсистему безопасности с помощью функции Save().

Примеры

Вызов: SecurityManagerApplication.New()

1.2.4.1.7.2.12. GetRoleRights

Предоставляет список прав, назначенных текущей роли.

Возвращает данные в JSON-формате.

string GetRoleRights(stringroleUID)

Параметры

Параметр	Тип	Описание
roleUID	string	Уникальный идентификатор (uid) роли

1.2.4.1.7.2.13. GetRolesList

Предоставляет список ролей из приложения, загруженного в элемент.

Функция не требует входных параметров..

Возвращает данные в JSON-формате.

string GetRolesList()

Примеры

Вызов: SecurityManagerApplication.GetRolesList()

1.2.4.1.7.2.14. GetTokensList

Предоставляет список токенов и прав из приложения, загруженного в элемент.

Функция не требует входных параметров.

Возвращает данные в JSON-формате.

string GetTokensList()

Примеры

Вызов: SecurityManagerApplication.GetTokensList()

1.2.4.1.7.2.15. Save

Отправляет информацию о приложении в подсистему безопасности после:

- редактирования ранее выгруженного из подсистемы безопасности приложения;
- создания приложения из проекта Astra.HMI с помощью функции New() и свойств элемента.

Функция не требует входных параметров.

void Save()

Примеры

Вызов: SecurityManagerApplication.Save()
Результат:

- в случае успешного завершения операции активируется событие SaveComplete;
- в случае неуспешного завершения операции активируется событие SaveFailed.

1.2.4.1.7.2.16. Load

Загружает данные приложения подсистемы безопасности.

void Load(string appID)

Параметры

Параметр	Тип	Описание
appID	string	ID приложения

Примеры

Вызов: SecurityManagerApplication.Load("Управление состоянием оборудования")
Результат:

- в случае успешного завершения операции активируется событие LoadComplete;
- в случае неуспешного завершения операции активируется событие LoadFailed.

1.2.4.1.7.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта (поля объекта)
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
IsChanged	Признак наличия изменений в параметрах приложения подсистемы безопасности
ApplicationID	Символьный идентификатор приложения подсистемы безопасности
Имя приложения	Имя приложения подсистемы безопасности
Менеджер конфигурирования безопасности	Ссылка на компонент Настройка безопасности: Менеджер

1.2.4.1.7.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.7.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.7.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.7.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.7.3.5. Менеджер конфигурирования безопасности

Ссылка на элемент типа Настройка безопасности: Менеджер, обеспечивающий работу с учетными записями, группами пользователей и приложениями.

Содержит свойство Контекст безопасности для указания ссылки на элемент типа Контекст безопасности.
Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.7.3.6. Имя приложения

Имя приложения, загруженного в элемент.

string ApplicationName

Примеры

Вызов: SecurityManagerApplication.ApplicationName.

1.2.4.1.7.3.7. IsChanged

Уведомление об изменении в приложении, загруженном в элемент.

bool IsChanged

Доступно только для чтения в режиме рантайма.

Принимает значение false при:

- загрузке приложения в элемент;
- сохранении приложения в подсистему безопасности.

Примеры

Вызов: SecurityManagerApplication.IsChanged.
Значение:

- true – приложение было изменено;
- false – нет изменений в приложении.

1.2.4.1.7.3.8. ApplicationID

Идентификатор (ID) приложения, загруженного в элемент.

Совпадает с именем приложения.

string ApplicationID

Доступно только для чтения в режиме рантайма.

Примеры

Вызов: SecurityManagerApplication.ApplicationID.

1.2.4.1.8. Настройка безопасности: Пользователь

Компонент предназначен для загрузки информации об учетной записи:

- имеющейся в подсистеме безопасности – для просмотра и изменения этой информации;
- созданной из проекта Astra.HMI – для дальнейшей отправки в подсистему безопасности.

1.2.4.1.8.1. События

Событие	Описание
SaveFailed	Появление ошибки при сохранении приложения
SaveComplete	Завершение сохранения приложения
LoadFailed	Появление ошибки при загрузке приложения
LoadComplete	Завершение выполнения загрузки приложения

1.2.4.1.8.1.1. SaveFailed

Информация об учетной записи не загружена в элемент.

Активируется в случае неуспешного завершения операции Load().

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.8.1.2. SaveComplete

Информация об учетной записи сохранена в подсистему безопасности Astra.Security.

Активируется в случае успешного завершения операции Save().

1.2.4.1.8.1.3. LoadFailed

Информация об учетной записи не загружена в элемент.

Активируется в случае неуспешного завершения операции Load().

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.8.1.4. LoadComplete

Информация об учетной записи загружена в элемент.

Активируется в случае успешного завершения операции Load().

1.2.4.1.8.2. Функции

Компонент	Описание
GetErrorDescriptionByCode	Возвращает описание ошибки по коду
DeleteRight	Удаляет значение права пользователя подсистемы безопасности
ChangeRight	Изменяет значение права пользователя подсистемы безопасности
AddRight	Добавляет новое право пользователю подсистемы безопасности
DeleteGroup	Удаляет пользователя подсистемы безопасности из группы
AddGroup	Добавляет пользователя подсистемы безопасности в группу
DeleteRole	Удаляет одну из ролей пользователя подсистемы безопасности
AddRole	Добавляет новую роль для пользователя подсистемы безопасности
New	Создает нового пользователя подсистемы безопасности
GetEffectiveRights	Возвращает список эффективных прав пользователя подсистемы безопасности
GetRights	Возвращает список прав пользователя подсистемы безопасности
GetRoles	Возвращает список ролей, назначенных пользователю подсистемы безопасности
GetApplicationsList	Возвращает список приложений, на которые у пользователя подсистемы безопасности есть права
GetGroupsList	Возвращает список групп, в которых состоит пользователь подсистемы безопасности

ValidatePassword	Проверяет пароль на соответствие назначенным парольным политикам
SetPassword	Задает пароль пользователя подсистемы безопасности
Save	Сохраняет данные пользователя подсистемы безопасности
Load	Загружает данные пользователя подсистемы безопасности

1.2.4.1.8.2.1. GetErrorDescriptionByCode

Возвращает текстовое описание ошибок, возникающих при загрузке и сохранении пользователей.

string GetErrorDescriptionByCode(uint1 FailReasonCode)

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Код ошибки из любого события, говорящего об ошибке

1.2.4.1.8.2.2. DeleteRight

Лишает права пользователя, чья учетная запись загружена в элемент.

void DeleteRight(string AppID, string RightName)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права

Примеры

Вызов: SecurityManagerUser.DeleteRight("Управление состоянием оборудования","Управление насосом")

1.2.4.1.8.2.3. ChangeRight

Меняет значения прав пользователя, чья учетная запись загружена в элемент.

void ChangeRight(string AppID, string RightName, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права
AllowedValue	string	Новое разрешающее значение права
ForbidenValue	string	Новое запрещающее значение права

Примеры

Вызов: SecurityManagerUser.ChangeRight("Управление состоянием оборудования","Управление насосом","false","true")

1.2.4.1.8.2.4. AddRight

Назначает право пользователю, чья учетная запись загружена в элемент.

void AddRight(string AppID, string RightName, uint1 RightType, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права
RightType	uint1	Тип права. Значение: › 0 – тип string › 1 – тип bool
AllowedValue	string	Разрешающее значение права
ForbidenValue	string	Запрещающее значение права

Примеры

Вызов: SecurityManagerUser.AddRight("Управление состоянием оборудования","Управление насосом",1,"true","false")

1.2.4.1.8.2.5. DeleteGroup

Удаляет пользователя подсистемы безопасности из группы.

void DeleteGroup(string GroupUID)

Параметры

Параметр	Тип	Описание
GroupUID	string	Уникальный идентификатор (uid) группы

Примеры

Вызов: SecurityManagerUser.DeleteGroup("astra:ffdad1f9-ae36-4980-82b8-c7180a63b451")

1.2.4.1.8.2.6. AddGroup

Добавляет в указанную группу пользователя, чья учетная запись загружена в элемент.

void AddGroup(string GroupUID)

Параметры

Параметр	Тип	Описание
GroupUID	string	Уникальный идентификатор (uid) группы

Примеры

Вызов: SecurityManagerUser.AddGroup("astra:ffdad1f9-ae36-4980-82b8-c7180a63b451")

1.2.4.1.8.2.7. DeleteRole

Лишает указанной роли пользователя, чья учетная запись загружена в элемент.

DeleteRole(string RoleID)

Параметры

Параметр	Тип	Описание
RoleID	string	Уникальный идентификатор (uid) роли

Примеры

Вызов: SecurityManagerUser.DeleteRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20")

1.2.4.1.8.2.8. AddRole

Назначает указанную роль пользователю, чья учетная запись загружена в элемент.

void AddRole(string RoleID)

Параметры

Параметр	Тип	Описание
RoleID	string	Уникальный идентификатор (uid) роли

Примеры

Вызов: SecurityManagerUser.AddRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20")

1.2.4.1.8.2.9. New

Освобождает элемент от загруженной в него информации для создания нового приложения.

Функция не требует входных параметров.

void New()

После создания новой учетной записи не забудьте загрузить её в подсистему безопасности с помощью функции Save().

Примеры

Вызов: SecurityManagerUser.New()

1.2.4.1.8.2.10. GetEffectiveRights

Возвращает список эффективных прав пользователя подсистемы безопасности.

string GetEffectiveRights(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список эффективных прав

1.2.4.1.8.2.11. GetRights

Предоставляет список личных прав пользователя, чья учетная запись загружена в элемент, из указанного приложения.

Возвращает данные в JSON-формате.

string GetRights(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список прав

Примеры

Вызов: SecurityManagerUser.GetRights("Управление состоянием оборудования")

1.2.4.1.8.2.12. GetRoles

Предоставляет список ролей пользователя, чья учетная запись загружена в элемент, в указанном приложении.

Возвращает данные в JSON-формате.

string GetRoles(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список ролей

Примеры

Вызов: SecurityManagerUser.GetRoles("Управление состоянием оборудования")

1.2.4.1.8.2.13. GetApplicationsList

Предоставляет список приложений с правами пользователя, чья учетная запись загружена в элемент.

Функция не требует входных параметров.

Возвращает данные в JSON-формате.

string GetApplicationsList()

Примеры

Вызов: SecurityManagerUser.GetApplicationsList()

1.2.4.1.8.2.14. GetGroupsList

Предоставляет список групп, в которых состоит пользователь учетной записи, загруженной в элемент.

Функция не требует входных параметров.

Возвращает данные в JSON-формате.

string GetGroupsList()

Примеры

Вызов: SecurityManagerUser.GetGroupsList()

1.2.4.1.8.2.15. ValidatePassword

Проверить пароль на соответствие назначенным парольным политикам.

uint2 ValidatePassword(string_1)

Параметры

Параметр	Тип	Описание
string_1	string	Пароль

1.2.4.1.8.2.16. SetPassword

Устанавливает пароль для учетной записи, загруженной в элемент.

uint2 SetPassword(string Password)

Параметры

Параметр	Тип	Описание
Password	string	Пароль

Подсистема безопасности Astra.Security не накладывает требований к содержанию пароля.

Примеры

Вызов: SecurityManagerUser.SetPassword("password")
Результат:

- в случае успешного завершения операции активируется событие SaveComplete;
- в случае неуспешного завершения операции активируется событие SaveFailed.

1.2.4.1.8.2.17. Save

Отправляет информацию о приложении в подсистему безопасности после:

- редактирования ранее выгруженного из подсистемы безопасности приложения;
- создания приложения из проекта Astra.HMI с помощью функции New() и свойств элемента.

Функция не требует входных параметров.

void Save()

Примеры

Вызов: SecurityManagerUser.Save()
Результат:

- в случае успешного завершения операции активируется событие SaveComplete;
- в случае неуспешного завершения операции активируется событие SaveFailed.

1.2.4.1.8.2.18. Load

Загружает информацию об учетной записи из подсистемы безопасности в элемент.

void Load(string UserID)

Параметры

Параметр	Тип	Описание
UserID	string	уникальный идентификатор (uid) учетной записи

Примеры

Вызов: SecurityManagerUser.Load("astra:ab5cc552-a515-48ab-9e82-436aabf6bdfc")
Результат:

- в случае успешного завершения операции активируется событие LoadComplete;
- в случае неуспешного завершения операции активируется событие LoadFailed.

1.2.4.1.8.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Менеджер конфигурирования безопасности	Ссылка на компонент Настройка безопасности: Менеджер
IsChanged	Признак наличия изменений в параметрах учетной записи пользователя подсистемы безопасности
UserID	Символьный идентификатор пользователя подсистемы безопасности
Смена пароля при следующем входе	Требование смены пароля при следующем входе пользователя в подсистему безопасности
Комментарий	Комментарий к учетной записи пользователя подсистемы безопасности
Номер телефона	Номер телефона пользователя подсистемы безопасности
Адрес электронной почты	Электронная почта пользователя подсистемы безопасности
Подразделение	Подразделение пользователя подсистемы безопасности
Должность	Должность пользователя подсистемы безопасности
Отображаемое имя	Отображаемое имя пользователя подсистемы безопасности
Фамилия	Фамилия пользователя подсистемы безопасности
Логин пользователя	Логин пользователя подсистемы безопасности
Имя	Имя пользователя подсистемы безопасности

Пользователь заблокирован	Пользователь заблокирован
Отчество	Отчество пользователя

1.2.4.1.8.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.8.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.8.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.8.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.8.3.5. Менеджер конфигурирования безопасности

Ссылка на элемент типа Настройка безопасности: Менеджер, обеспечивающий работу с учетными записями, группами пользователей и приложениями.

Содержит свойство Контекст безопасности для указания ссылки на элемент типа Контекст безопасности.
Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.8.3.6. Логин пользователя

Логин пользователя подсистемы безопасности.

string Login

1.2.4.1.8.3.7. Имя

Имя пользователя подсистемы безопасности.

string Name

1.2.4.1.8.3.8. Фамилия

Фамилия пользователя подсистемы безопасности.

string Surname

1.2.4.1.8.3.9. Отчество

Отчество пользователя.

string MidName

1.2.4.1.8.3.10. Отображаемое имя

Отображаемое имя пользователя подсистемы безопасности.

string DisplayName

1.2.4.1.8.3.11. Должность

Должность пользователя подсистемы безопасности.

string Position

1.2.4.1.8.3.12. Подразделение

Подразделение пользователя подсистемы безопасности.

string Unit

1.2.4.1.8.3.13. Адрес электронной почты

Электронная почта пользователя подсистемы безопасности.

string Email

1.2.4.1.8.3.14. Номер телефона

Номер телефона пользователя подсистемы безопасности.

string Phone

1.2.4.1.8.3.15. Комментарий

Комментарий к учетной записи пользователя подсистемы безопасности.

string Comment

1.2.4.1.8.3.16. Смена пароля при следующем входе

Требование смены пароля при следующем входе пользователя в подсистему безопасности.

bool ForcePassChange

Примеры

Вызов: SecurityManagerUser.ForcePassChange
Значение:

- true – требовать смену пароля;
- false – не требовать смену пароля.

1.2.4.1.8.3.17. Пользователь заблокирован

Хранит информацию о том, заблокирован ли пользователь.

bool Disabled

Примеры

Вызов: SecurityManagerUser.Disabled
Значение:

- true – пользователь заблокирован;
- false – пользователь не заблокирован.

1.2.4.1.8.3.18. IsChanged

Уведомление об изменении в учетной записи, загруженной в элемент.

bool IsChanged

Только для чтения в режиме рантайма.

Принимает значение false при:

- загрузке учетной записи в элемент;
- сохранении учетной записи в подсистему безопасности.

Примеры

Вызов: SecurityManagerUser.IsChanged
Значение:

- true – учетная запись была изменена;
- false – нет изменений в учетной записи.

1.2.4.1.8.3.19. UserID

Уникальный идентификатор (uid) учетной записи, загруженной в элемент.

string UserID

Только для чтения в режиме рантайма.

Примеры

Вызов: SecurityManagerUser.UserID
Вид значения: astra:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Пример значения: astra:ab5cc552-a515-48ab-9e82-436aabf6bdfc.

1.2.4.1.9. Настройка безопасности: Группа

Компонент предназначен для загрузки информации о группе:

- имеющейся в подсистеме безопасности – для просмотра и изменения этой информации;
- созданной из проекта Astra.HMI – для дальнейшей отправки в подсистему безопасности.

1.2.4.1.9.1. События

Событие	Описание
SaveFailed	Появление ошибки при сохранении приложения
SaveComplete	Завершение сохранения приложения
LoadFailed	Появление ошибки при загрузке приложения
LoadComplete	Завершение выполнения загрузки приложения

1.2.4.1.9.1.1. SaveFailed

Информация о группе не сохранена в подсистему безопасности Astra.Security.

Активируется в случае неуспешного завершения операции Save().

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.9.1.2. SaveComplete

Информация о группе сохранена в подсистему безопасности Astra.Security.

Активируется в случае успешного завершения операции Save().

1.2.4.1.9.1.3. LoadFailed

Информация о группе не загружена в элемент.

Активируется в случае неуспешного завершения операции Load().

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Номер ошибки

Получить текст ошибки можно, вызвав функцию GetErrorDescriptionByCode().

1.2.4.1.9.1.4. LoadComplete

Информация о группе загружена в элемент.

Активируется в случае успешного завершения операции Load().

1.2.4.1.9.2. Функции

Компонент	Описание
GetErrorDescriptionByCode	Возвращает описание ошибки по коду
DeleteRight	Удаляет значение права пользователя подсистемы безопасности
ChangeRight	Изменяет значение права пользователя подсистемы безопасности
AddRight	Добавляет новое право пользователю подсистемы безопасности
DeleteRole	Удаляет одну из ролей пользователя подсистемы безопасности
AddRole	Добавляет новую роль для пользователя подсистемы безопасности
New	Создает нового пользователя подсистемы безопасности
GetApplicationsList	Возвращает список приложений, на которые у пользователя подсистемы безопасности есть права
Save	Сохраняет данные пользователя подсистемы безопасности
Load	Загружает данные пользователя подсистемы безопасности
GroupEffectiveRights	Возвращает список эффективных прав группы подсистемы безопасности
GroupRights	Возвращает список прав группы подсистемы безопасности
GroupRoles	Возвращает список ролей, назначенных группе подсистемы безопасности
GetMembersList	Возвращает список пользователей, состоящих в группе

1.2.4.1.9.2.1. GetErrorDescriptionByCode

Возвращает текстовое описание ошибок, возникающих при загрузке и сохранении групп.

string GetErrorDescriptionByCode(uint1 FailReasonCode)

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Код ошибки из любого события, говорящего об ошибке

1.2.4.1.9.2.2. DeleteRight

Лишает права группу, загруженную в элемент.

void DeleteRight(string AppID, string RightName)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права

Примеры

Вызов: SecurityManagerGroup.DeleteRight("Управление состоянием оборудования","Управление насосом")

1.2.4.1.9.2.3. ChangeRight

Меняет значения прав группы, загруженной в элемент.

void ChangeRight(string AppID, string RightName, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права
AllowedValue	string	Новое разрешающее значение права
ForbidenValue	string	Новое запрещающее значение права

Примеры

Вызов: SecurityManagerGroup.ChangeRight("Управление состоянием оборудования","Управление насосом","false","true")

1.2.4.1.9.2.4. AddRight

Назначает право группе, загруженной в элемент.

void AddRight(string AppID, string RightName, uint1 RightType, string AllowedValue, string ForbidenValue)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, содержащего право
RightName	string	Имя права
RightType	int	Тип права. Значение: › 0 – тип string › 1 – тип bool
AllowedValue	string	Разрешающее значение права
ForbidenValue	string	Запрещающее значение права

Примеры

Вызов: SecurityManagerGroup.AddRight("Управление состоянием оборудования","Управление насосом",1,"true","false"

1.2.4.1.9.2.5. DeleteRole

Лишает указанной роли группу, загруженную в элемент.

void DeleteRole(string RoleID)

Параметры

Параметр	Тип	Описание
RoleID	string	Уникальный идентификатор (uid) роли

Примеры

Вызов: SecurityManagerGroup.DeleteRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20")

1.2.4.1.9.2.6. AddRole

Назначает указанную роль группе, загруженной в элемент.

void AddRole(string RoleUID)

Параметры

Параметр	Тип	Описание
RoleUID	string	Уникальный идентификатор (uid) роли

Примеры

Вызов: SecurityManagerGroup.AddRole("astra:4ce9483e-e137-41c2-bf1c-343e9b731f20")

1.2.4.1.9.2.7. New

Освобождает элемент от загруженной в него информации для создания новой группы.

Функция не требует входных параметров.

void New()

После создания нового приложения не забудьте загрузить его в подсистему безопасности с помощью функции Save().

Примеры

Вызов: SecurityManagerGroup.New()

1.2.4.1.9.2.8. GetApplicationsList

Предоставляет список приложений с правами группы, загруженной в элемент.

Функция не требует входных параметров.

Возвращает данные в JSON-формате.

string GetApplicationsList()

Примеры

Вызов: SecurityManagerGroup.GetApplicationsList()

1.2.4.1.9.2.9. Save

Отправляет информацию о приложении в подсистему безопасности после:

- редактирования ранее выгруженного из подсистемы безопасности приложения;
- создания приложения из проекта Astra.HMI с помощью функции New() и свойств элемента.

Функция не требует входных параметров.

void Save()

Примеры

Вызов: SecurityManagerGroup.Save()
Результат:

- в случае успешного завершения операции активируется событие SaveComplete;
- в случае неуспешного завершения операции активируется событие SaveFailed.

1.2.4.1.9.2.10. Load

Загружает информацию о группе из подсистемы безопасности в элемент.

void Load(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	Уникальный идентификатор (uid) группы

Примеры

Вызов: SecurityManagerGroup.Load("astra:d01969e0-ae05-4548-9375-2533b326a588")
Результат:

- в случае успешного завершения операции активируется событие LoadComplete;
- в случае неуспешного завершения операции активируется событие LoadFailed.

1.2.4.1.9.2.11. GroupEffectiveRights

Предоставляет список эффективных прав группы, загруженной в элемент, из указанного приложения.

Возвращает данные в JSON-формате.

string GroupEffectiveRights(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список эффективных прав

Примеры

Вызов: SecurityManagerGroup.GroupEffectiveRights("Управление состоянием оборудования")

1.2.4.1.9.2.12. GroupRights

Предоставляет список прав группы, загруженной в элемент, из указанного приложения.

Возвращает данные в JSON-формате.

string GroupRights(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список прав

Для получения списка эффективных прав используйте функцию GroupEffectiveRights().

Примеры

Вызов: SecurityManagerGroup.GroupRights("Управление состоянием оборудования")

1.2.4.1.9.2.13. GroupRoles

Предоставляет список ролей группы, загруженной в элемент, в указанном приложении.

Возвращает данные в JSON-формате.

string GroupRoles(string AppID)

Параметры

Параметр	Тип	Описание
AppID	string	ID приложения, из которого требуется получить список ролей

Примеры

Вызов: SecurityManagerGroup.GroupRoles("Управление состоянием оборудования")

1.2.4.1.9.2.14. GetMembersList

Предоставляет список участников группы, загруженной в элемент.

Функция не требует входных параметров.

Возвращает данные в JSON-формате.

string GetMembersList()

Примеры

Вызов: SecurityManagerGroup.GetMembersList()

1.2.4.1.9.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Менеджер конфигурирования безопасности	Ссылка на компонент Настройка безопасности: Менеджер
IsChanged	Признак наличия изменений в параметрах группы подсистемы безопасности
GroupID	Символьный идентификатор группы подсистемы безопасности
Описание группы	Описание группы подсистемы безопасности
Имя группы	Имя группы подсистемы безопасности
Группа заблокирована	Пользователь заблокирован

1.2.4.1.9.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.9.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.9.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.9.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.9.3.5. Менеджер конфигурирования безопасности

Ссылка на элемент типа Настройка безопасности: Менеджер, обеспечивающий работу с учетными записями, группами пользователей и приложениями.

Содержит свойство Контекст безопасности для указания ссылки на элемент типа Контекст безопасности.
Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.9.3.6. Имя группы

Название группы, загруженной в элемент.

string GroupName

Примеры

Вызов: SecurityManagerGroup.GroupName
Пример значения: dispatchers.

1.2.4.1.9.3.7. Описание группы

Описание группы, загруженной в элемент.

string GroupDescription

Примеры

Вызов: SecurityManagerGroup.GroupDescription

1.2.4.1.9.3.8. Группа заблокирована

Хранит информацию о том, заблокирована ли группа.

bool Disabled

Примеры

Вызов: SecurityManagerGroup.Disabled
Значение:

- true – группа заблокирована;
- false – группа не заблокирована.

1.2.4.1.9.3.9. IsChanged

Уведомление об изменении в группе, загруженной в элемент.

bool IsChanged

Доступно только для чтения в режиме рантайма.

Принимает значение false при:

- загрузке группы в элемент;
- сохранении группы в подсистему безопасности.

Примеры

Вызов: SecurityManagerGroup.IsChanged
Значение:

- true – группа была изменена;
- false – нет изменений в группе.

1.2.4.1.9.3.10. GroupID

Уникальный идентификатор (uid) группы, загруженной в элемент.

string GroupID

Доступно только для чтения в режиме рантайма.

Уникальный идентификатор формируется подсистемой безопасности в момент создания группы.

Примеры

Вызов: SecurityManagerGroup.GroupID
Вид значения: astra:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Пример значения: astra:d01969e0-ae05-4548-9375-2533b326a588.

1.2.4.1.10. Мастер конфигурирования Security

Компонент предназначен для чтения и обновления конфигурации службы Агент Astra.Security.

После установки подсистемы безопасности Astra.Security необходимо настроить ее компоненты – в том числе, службу Агент Astra.Security. Вносить изменения в конфигурационный файл можно вручную, либо из проекта Astra.HMI с помощью свойств, функций и событий экземпляра Мастер конфигурирования Security.

Компонент следует использовать следующим образом:

- Для чтения конфигурации необходимо вызвать функцию Read(). Она поместит данные из конфигурационного файла в компонент. После этого можно будет обратиться к данным, прочитав значения свойств компонента или вызвав функции, название которых начинается с Get (GetLdapHost(), GetLdapPort() и пр.).
- Для создания новой конфигурации необходимо сначала указать новые данные, поместив их в значения свойств и во входные параметры функций, название которых начинается с Add (AddLdap(), AddLogConsumer() и пр.). После этого следует вызвать функцию Generate(), которая создаст текст нового конфигурационного файла.

1.2.4.1.10.1. События

Событие	Описание
ConsumersListChanged	Изменение списка потребителей аудита
LdapListChanged	Изменение списка LDAP-серверов
ReadingFailure	Появление ошибки считывания конфигурации Astra.Security.Agent
ReadingFinished	Завершение считывания конфигурации Astra.Security.Agent
ReadingStarted	Начало считывания конфигурации Astra.Security.Agent
GenerationFailure	Появление ошибки генерации конфигурации Astra.Security.Agent
GenerationFinished	Завершение генерации конфигурации Astra.Security.Agent
GenerationStarted	Начало генерации конфигурации Astra.Security.Agent

1.2.4.1.10.1.1. ConsumersListChanged

Изменен список серверов-потребителей сообщений аудита во внутреннем массиве компонента.

Активируется в результате успешного выполнения одной из функций – AddLogConsumer() или ClearLogConsumersList().

1.2.4.1.10.1.2. LdapListChanged

Изменен список LDAP-серверов во внутреннем массиве компонента.

Активируется в результате успешного выполнения одной из функций – AddLdap() или ClearLdapList().

1.2.4.1.10.1.3. ReadingFailure

Не удалось прочитать конфигурационный файл Агент Astra.Security.

Активируется в результате неуспешного выполнения функции Read().

Чтобы ознакомиться с текстом ошибки, обратитесь к значению внутренней переменной Error этого события, либо к значению свойства Ошибка чтения (ReadError) компонента.

1.2.4.1.10.1.4. ReadingFinished

Чтение конфигурационного файла Агент Astra.Security завершено успешно.

Активируется в результате успешного выполнения функции Read().

Чтобы ознакомиться с полученными настройками, обратитесь к значениям свойств компонента.

1.2.4.1.10.1.5. ReadingStarted

Начато чтение конфигурационного файла Агент Astra.Security.

Активируется сразу после вызова функции Read().

1.2.4.1.10.1.6. GenerationFailure

Не удалось создать текст конфигурационного файла Агент Astra.Security.

Активируется в результате неуспешного выполнения функции Generate().

Чтобы ознакомиться с текстом ошибки, обратитесь к значению внутренней переменной Error этого события, либо к значению свойства Ошибка конфигурирования компонента.

1.2.4.1.10.1.7. GenerationFinished

Создан текст конфигурационного файла Агент Astra.Security. Результат помещен в свойство GeneratedString.

Активируется в результате успешного выполнения функции Generate().

1.2.4.1.10.1.8. GenerationStarted

Начато создание текста конфигурационного файла Агент Astra.Security.

Активируется сразу после вызова функции Generate().

1.2.4.1.10.2. Функции

Компонент	Описание
AddSignal	Добавляет новый сигнал потребителю аудита
AddSeverity	Добавляет новую категорию важности потребителю аудита
AddLogConsumer	Добавляет нового потребителя аудита в конфигурацию Astra.Security.Agent
ClearLogConsumersList	Очищает список потребителей аудита
GetSignalMode	Возвращает режим сигнала аудита по индексу сервера аудита и индексу сигнала
GetSignalName	Возвращает имя сигнала аудита по индексу сервера аудита и индексу сигнала
GetSeverityValue	Возвращает значение важности аудита по индексу сервера аудита и индексу категории
GetSeverityCategory	Возвращает категорию важности аудита по индексу сервера аудита и индексу категории
GetSignalsCount	Возвращает количество сигналов аудита по индексу сервера аудита
GetSeverityCount	Возвращает количество категорий аудита по индексу сервера аудита
GetServerType	Предоставляет информацию о типе одного из указанных в конфигурационном файле серверов-потребителей аудита
GetServerProgId	Возвращает программный идентификатор (ProgId) сервера аудита по индексу
GetAuditServerPort	Возвращает порт сервера аудита по индексу
GetAuditServerHost	Возвращает IP адрес или имя компьютера с сервером аудита по индексу
GetLdapPort	Возвращает порт LDAP-сервера по индексу

GetLdapHost	Возвращает IP адрес или имя компьютера с LDAP-сервером по индексу
ClearLdapList	Очищает список LDAP-серверов в конфигурации Astra.Security.Agent
AddLdap	Добавляет новый LDAP-сервер в конфигурацию Astra.Security.Agent
Read	Запускает чтение конфигурации Astra.Security.Agent
Generate	Запускает генерацию конфигурации Astra.Security.Agent
GetSignalType	Предоставляет название типа сообщений в указанном сигнале для указанного сервера-потребителя

1.2.4.1.10.2.1. AddSignal

Добавляет в компонент информацию о сигнале, предназначенном для записи сообщений, для указанного сервера-потребителя.

bool AddSignal(int4 ConsumerIndex, string SignalName, int4 SignalMode, string SignalType)

Параметры

Параметр	Тип	Описание
ConsumerIndex	int4	Индекс сервера-потребителя во внутреннем массиве компонента
SignalName	string	Название сигнала
SignalMode	int4	Режим записи сообщения в сигнал: › 1 – соответствует DynamicEvent (запись сообщения с xml-конструкцией, описывающей динамическое событие) › 2 – соответствует Value (обычная запись сообщения)
SignalType	string	Тип сообщений, записывающихся в сигнал

Функция возвращает результат добавления информации о сигнале в компонент:

› true – информация добавлена;

› false – информацию не удалось добавить. В таком случае следует проверить значение индекса – оно может быть больше, чем размер массива в компоненте.

1.2.4.1.10.2.2. AddSeverity

Добавляет в компонент категорию важности сообщений для указанного сервера-потребителя.

bool AddSeverity(int4 ConsumerIndex, string SeverityCategory, int4 SeverityValue)

Параметры

Параметр	Тип	Описание
ConsumerIndex	int4	Индекс сервера-потребителя во внутреннем массиве компонента
SeverityCategory	string	Название категории важности
SeverityValue	int4	Значение категории важности

Функция возвращает результат добавления категории в компонент:

- true – категория добавлена;
- false – категорию не удалось добавить. В таком случае следует проверить значение индекса – оно может быть больше, чем размер массива в компоненте.

1.2.4.1.10.2.3. AddLogConsumer

Добавляет описание сервера-потребителя аудита сообщений. Добавленное описание хранится во внутреннем массиве компонента.

В случае успешного завершения операции активируется событие ConsumersListChanged.

void AddLogConsumer(string Host, string HostTcpReserve, int4 TCPServerPort, string ProgID, string Type)

Параметры

Параметр	Тип	Описание
Host	string	Имя или IP-адрес сервера
HostTcpReserve	string	Имя или IP-адрес сервера для резервного канала связи с сервером TCP (значение может быть пустым)
TCPServerPort	int4	Порт для подключения к TCP-серверу (если выбран TCP-сервер)
ProgID	string	Строковый идентификатор OPC-сервера (если выбран OPC-сервер)
Type	string	Тип сервера: › для Windows возможны значения OPC (по умолчанию) и TCP › для других ОС допустимо только TCP

1.2.4.1.10.2.4. ClearLogConsumersList

Очищает внутренний массив серверов-потребителей в компоненте.

Функция не требует входных параметров.

В случае успешного завершения операции активируется событие ConsumersListChanged.

void ClearLogConsumersList()

1.2.4.1.10.2.5. GetSignalMode

Возвращает режим сигнала аудита по индексу сервера аудита и индексу сигнала.

int4 GetSignalMode(ServerIndex, SignalIndex)

Параметры

Параметр	Тип	Описание
ServerIndex	int4	Индекс сервера аудита
SignalIndex	int4	Индекс сигнала

1.2.4.1.10.2.6. GetSignalName

Предоставляет информацию о режиме записи сообщения в указанный сигнал в указанном сервере-потребителе.

string GetSignalName(int4 i, int4 k)

Параметры

Параметр	Тип	Описание
i	int4	Индекс сервера аудита
k	int4	Индекс категории важности

Возвращает значение в числовом виде, где:

- 1 – соответствует DynamicEvent (запись сообщения с xml-конструкцией, описывающей динамическое событие);
- 2 – соответствует Value (обычная запись сообщения).

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, каждый из них описывается в компоненте в виде элемента массива A[i]. Каждый элемент массива A[i] представляет собой массив B, каждый элемент B[i,k] которого описывает один из сигналов в описываемом сервере A[i].

Массив A, описывающий сервера-потребители = [[Массив B, описывающий первый сервер], [Массив B, описывающий второй сервер]]
Массив B, описывающий первый сервер = [[Описание первой категории важности], [Описание второй категории важности]]
Массив B, описывающий второй сервер = [[Описание первой категории важности], [Описание второй категории важности]]

Обратиться к конкретному сигналу можно по номеру элемента в массивах A и B (i, k).

Каждый элемент массива B[i,k] соответствует одному из значений атрибута Mode xml-элемента <Signal>, вложенного в xml-элемент <SignalMap> одного из xml-элементов <OpcDaLogConsumer> в конфигурационном файле агента безопасности.

Пример использования приведен в описании функции GetSignalType().

1.2.4.1.10.2.7. GetSeverityValue

Предоставляет числовое значение выбранной категории важности сообщений.

int4 GetSeverityValue(int4 i, int4 k)

Параметры

Параметр	Тип	Описание
i	int4	Индекс сервера аудита
k	int4	Индекс категории важности

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, каждый из них описывается в компоненте в виде элемента массива A[i]. Каждый элемент массива A[i] представляет собой массив B, каждый элемент B[i,k] которого описывает одну из категорий важности описываемого сервера A[i].

Массив A, описывающий сервера-потребители = [[Массив B, описывающий первый сервер], [Массив B, описывающий второй сервер]]
Массив B, описывающий первый сервер = [[Описание первой категории важности], [Описание второй категории важности]]
Массив B, описывающий второй сервер = [[Описание первой категории важности], [Описание второй категории важности]]

Обратиться к конкретной категории важности можно по номеру элемента в массивах A и B (i, k).

Каждый элемент массива B[i,k] соответствует одному из значений атрибута Value xml-элемента <Severity>, вложенного в xml-элемент <SeverityMap> одного из xml-элементов <OpcDaLogConsumer> в конфигурационном файле агента безопасности.

Примеры

Допустим, в конфигурационном файле описан один сервер-потребитель сообщений (один элемент <OpcDaLogConsumer>), для которого описано четыре категории важности сообщений аудита:

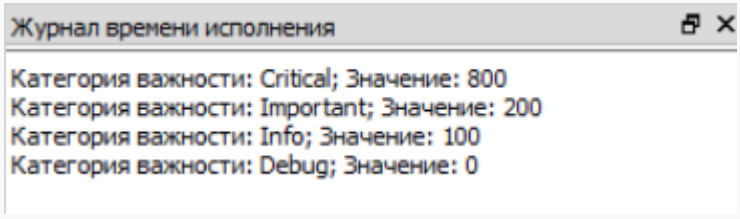
```
<AuditLogConsumers TraceAudit="1">
 <OpcDaLogConsumer>
  <Server Host="127.0.0.1" Type="OPC" ...>
   <SeverityMap>
      <Severity Category="Critical"
   Value="800"/>
      <Severity
   Category="Important"
   Value="200"/>
      <Severity
   Category="Info"
   Value="100"/>
      <Severity
   Category="Debug"
   Value="0"/>
    </SeverityMap>
   </Server>
  </OpcDaLogConsumer>
 </AuditLogConsumers
```

Чтобы получить список категорий важности сообщений с их значениями в каждом сервере-потребителе, вызовите нужные функции в коде, выполняющемся в случае успешного чтения конфигурации Агент Astra.Security (например, в обработчике

события ReadingFinished). Укажите в качестве входных параметров индексы i (индекс в массиве серверов-потребителей) и k (индекс в массиве категорий важности). Приведенный ниже пример написан на языке Astra.Om, в нем итоговый список записывается в лог:

```
i: int4 = 0;
while (i < Configurator.ConsumersCount) //цикл выполняется, пока в массиве A не будут описаны все сервера-потребители
{
  k: int4 = 0;
  while (k < Configurator.GetSeverityCount(i)) //цикл выполняется, пока в массив B не будут записаны все категории важности i-го сервера-потребителя
  {
      DebugTool.Log("Категория важности: "+Configurator.GetSeverityCategory(i,k)+"; Значение: "+String.ToString(Configurator.GetSeverityValue(i,k))); //в Журнал времени исполнения записываются названия и значения категорий важности для i-го сервера
    k += 1;
  }
  i += 1;
}
```

В результате вызова функций в Журнал времени исполнения запишутся названия категорий важности с их значениями:



1.2.4.1.10.2.8. GetSeverityCategory

Возвращает категорию важности аудита по индексу сервера аудита и индексу категории.

string GetSeverityCategory(int4 i, int4 k)

Параметры

Параметр	Тип	Описание
i	int4	Индекс сервера аудита
k	int4	Индекс категории важности

Предоставляет название выбранной категории важности сообщений.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, каждый из них описывается в компоненте в виде элемента массива A[i]. Каждый элемент массива A[i] представляет собой массив B, каждый элемент B[i,k] которого описывает одну из категорий важности описываемого сервера A[i].

Массив A, описывающий сервера-потребители = [[Массив B, описывающий первый сервер], [Массив B, описывающий второй сервер]]
Массив B, описывающий первый сервер = [[Описание первой категории важности], [Описание второй категории важности]]
Массив B, описывающий второй сервер = [[Описание первой категории важности], [Описание второй категории важности]]

Обратиться к конкретной категории важности можно по номеру элемента в массивах A и B (i, k).

Каждый элемент массива B[i,k] соответствует одному из значений атрибута Category xml-элемента <Severity>, вложенного в xml-элемент <SeverityMap> одного из xml-элементов <OpcDaLogConsumer> в конфигурационном файле агента безопасности.

Пример использования приведен в описании функции GetSeverityValue().

1.2.4.1.10.2.9. GetSignalsCount

Предоставляет количество сигналов, предназначенных для записи сообщений аудита, в одном из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, значение для каждого из них записывается в компонент в виде элемента массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует количеству элементов <Signal> внутри элемента <SignalMap>, вложенного в один из элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

int4 GetSignalsCount(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.10. GetSeverityCount

Предоставляет количество категорий важности сообщений для одного из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, значение от каждого из них записывается в компонент в виде элемента массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует количеству элементов <Severity> внутри элемента <SeverityMap>, вложенного в один из элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

int4 GetSeverityCount(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.11. GetServerType

Предоставляет информацию о типе одного из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, перечень их типов записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута Type xml-элемента <Server>, вложенного в один из xml-элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

string GetServerType(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.12. GetServerProgId

Предоставляет ProgID (строковый идентификатор) одного из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, перечень их ProgID записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута ProgId xml-элемента <Server>, вложенного в один из xml-элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

string GetServerProgId(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.13. GetAuditServerPort

Предоставляет порт для подключения к одному из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, перечень портов для подключения к ним записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута TCPServerPort xml-элемента <Server>, вложенного в один из xml-элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

int4 GetAuditServerPort(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.14. GetAuditServerHost

Предоставляет IP-адрес одного из указанных в конфигурационном файле серверов-потребителей аудита.

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, перечень их IP-адресов записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута Host xml-элемента <Server>, вложенного в один из xml-элементов <OpcDaLogConsumer>, в конфигурационном файле агента безопасности.

string GetAuditServerHost(int Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс сервера аудита

1.2.4.1.10.2.15. GetLdapPort

Предоставляет номер порта для подключения к одному из указанных в конфигурационном файле LDAP-серверов.

Поскольку в конфигурационном файле может быть указано несколько LDAP-серверов, перечень портов для подключения к ним записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута Port одного из xml-элементов <LDAPServer>, вложенного в xml-элемент <LdapHosts>, в конфигурационном файле агента безопасности.

int4 GetLdapPort(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс LDAP-сервера

1.2.4.1.10.2.16. GetLdapHost

Предоставляет IP-адрес одного из указанных в конфигурационном файле LDAP-серверов.

Поскольку в конфигурационном файле может быть указано несколько LDAP-серверов, перечень их IP-адресов записывается в компонент в виде массива. Обратиться к конкретному значению можно по номеру его записи в массив.

Каждый элемент массива соответствует значению атрибута Address одного из xml-элементов <LDAPServer>, вложенного в xml-элемент <LdapHosts>, в конфигурационном файле агента безопасности.

string GetLdapHost(int4 Index)

Параметры

Параметр	Тип	Описание
Index	int4	Индекс LDAP-сервера

1.2.4.1.10.2.17. ClearLdapList

Очищает внутренний массив LDAP-серверов компонента.

Функция не требует входных параметров.

В случае успешного завершения операции активируется событие LdapListChanged.

void ClearLdapList()

1.2.4.1.10.2.18. AddLdap

Добавляет описание LDAP-сервера, к которому должен подключаться агент безопасности. Добавленное описание хранится во внутреннем массиве компонента.

bool AddLdap(string LDAPHost, int4 LDAPPort)

Параметры

Параметр	Тип	Описание
LDAPHost	string	IP адрес или имя компьютера, где расположен добавляемый LDAP-сервер
LDAPPort	int	Порт для подключения к добавляемому LDAP-серверу

Значение

Значение	Описание
true	Информация добавлена
false	Информацию не удалось добавить

В случае успешного завершения операции активируется событие LdapListChanged.

1.2.4.1.10.2.19. Read

Выполняет чтение конфигурации из конфигурационного файла Агент Astra.Security.

void Read(string XML)

Параметры

Параметр	Тип	Описание
XML	string	Строка, содержащая полный текст конфигурационного файла Агент Astra.Security в xml-формате

Чтобы получить такую строку из файла с помощью компонентов Astra.HMI, используйте функцию ReadTextFile() компонента Окружение: файлы (File System). В качестве входного параметра функции укажите полный путь к файлу конфигурации.

Результат:

- сразу после вызова функции активируется событие ReadingStarted;
- в случае успешного завершения операции активируется событие ReadingFinished;
- в случае неуспешного завершения операции активируется событие ReadingFailure.

Примеры

```
Configurator.Read(FileSystem.ReadTextFile("C:/Program Files/
AstraRegul/Astra.Security/astra.security.agent.xml"));
```

1.2.4.1.10.2.20. Generate

Создает текст конфигурационного файла Агент Astra.Security.

int4 Generate(bool ActivationFlag)

Параметры

Параметр	Тип	Описание
ActivationFlag	bool	Параметр отвечает за совместимость создаваемой конфигурации со старыми версиями Astra.Security. В качестве значения следует указывать true.

Результат:

- сразу после вызова функции активируется событие GenerationStarted;
- в случае успешного завершения операции активируется событие GenerationFinished, а строка-результат записывается в свойство GeneratedString;
- в случае неуспешного завершения операции активируется событие GenerationFailure.

Для создания конфигурации должны быть заполнены все обязательные поля. Обязательно следует указать:

- адрес и порт Net-агента – в соответствующих свойствах;
- параметры хотя бы одного LDAP-сервера – с помощью функции AddLdap();
- учетную запись администратора LDAP (в стандартном для LDAP виде) и пароль;
- пароль пользователя, чья учетная запись используется по умолчанию;
- адрес корневой папки LDAP-сервера;
- защищено ли соединение агента безопасности с LDAP-сервером.

Если в процессе создания конфигурации возникнет ошибка, функция вернет ее код. Чтобы ознакомиться с текстом ошибки, обратитесь ко значению

свойства Ошибка конфигурирования (Error) компонента, либо ко значению внутренней переменной Error события GenerationFailure.

1.2.4.1.10.2.21. GetSignalType

Предоставляет название типа сообщений в указанном сигнале для указанного сервера-потребителя.

string GetSignalType(int4 i, int4 k)

Параметры

Параметр	Тип	Описание
i	int4	Индекс сервера аудита
k	int4	Индекс категории важности

Поскольку в конфигурационном файле может быть указано несколько серверов-потребителей, каждый из них описывается в компоненте в виде элемента массива A[i]. Каждый элемент массива A[i] представляет собой массив B, каждый элемент B[i,k] которого описывает один из сигналов в описываемом сервере A[i].

Массив A, описывающий сервера-потребители = [[Массив B, описывающий первый сервер], [Массив B, описывающий второй сервер]]
Массив B, описывающий первый сервер = [[Описание первой категории важности], [Описание второй категории важности]]
Массив B, описывающий второй сервер = [[Описание первой категории важности], [Описание второй категории важности]]

Обратиться к конкретному сигналу можно по номеру элемента в массивах A и B (i, k).

Каждый элемент массива B[i,k] соответствует одному из значений атрибута Type xml-элемента <Signal>, вложенного в xml-элемент <SignalMap> одного из xml-элементов <OpcDaLogConsumer> в конфигурационном файле агента безопасности..

Примеры

Допустим, в конфигурационном файле описан один сервер-потребитель сообщений (один элемент <OpcDaLogConsumer>), в котором для записи сообщений аудита предназначено несколько сигналов:

```
<AuditLogConsumers TraceAudit="1">
 <OpcDaLogConsumer>
  <Server Host="127.0.0.1" Type="OPC" ...>
   <SignalMap>
      <Signal Name="DynEvents.NormalDynSignal"
    Mode="DynamicEvent"
    Type="Normal"/>
                    <Signal     Name="DynEvents.AdminDynSignal"
    Mode="DynamicEvent" Type="Admin"/>
                 <Signal    Name="DynEvents.UserNameDynSignal"
    Mode="DynamicEvent" Type="UserName"/>
              <Signal    Name="DynEvents.DisplayNameDynSignal"
    Mode="DynamicEvent" Type="DisplayName"/>
               <Signal    Name="DynEvents.GroupNameDynSignal"
    Mode="DynamicEvent" Type="GroupName"/>
         <Signal  Name="DynEvents.WorkstationNameDynSignal"
    Mode="DynamicEvent" Type="WorkstationName"/>
     <Signal Name="DynEvents.NormalMessage" Mode="Value"
    Type="Normal"/>
      <Signal Name="DynEvents.AdminMessage" Mode="Value"
    Type="Admin"/>
```

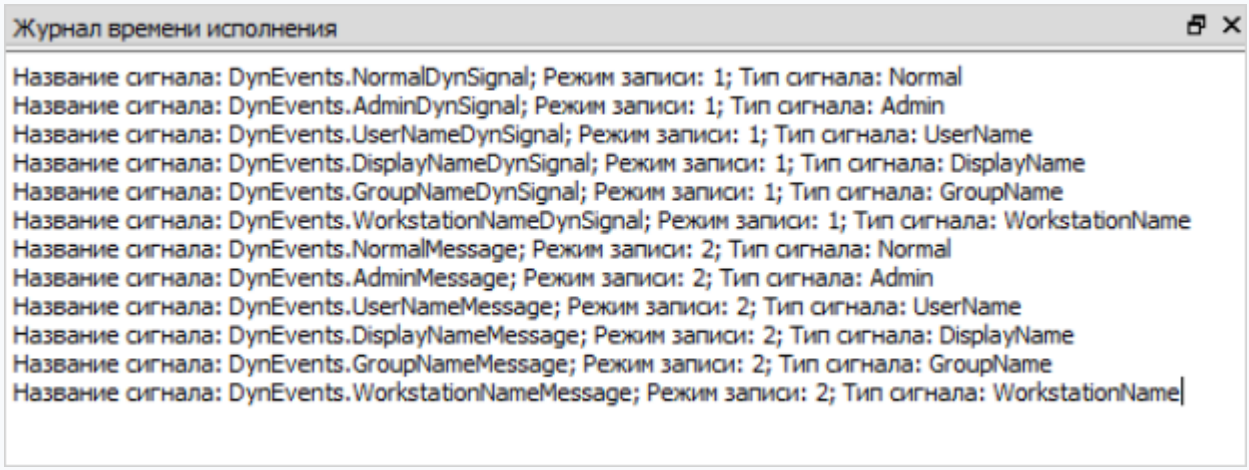
```
                    <Signal    Name="DynEvents.UserNameMessage"
    Mode="Value" Type="UserName"/>
                <Signal    Name="DynEvents.DisplayNameMessage"
    Mode="Value" Type="DisplayName"/>
                 <Signal    Name="DynEvents.GroupNameMessage"
    Mode="Value" Type="GroupName"/>
           <Signal  Name="DynEvents.WorkstationNameMessage"
    Mode="Value" Type="WorkstationName"/>
      </SignalMap>
     </Server>
    </OpcDaLogConsumer>
   </AuditLogConsumers>
```

Чтобы получить список параметров сигналов в каждом сервере-потребителе, вызовите нужные функции в коде, выполняющемся в случае успешного чтения конфигурации Агент Astra.Security (например, в обработчике события ReadingFinished()). Укажите в качестве входных параметров индексы i (индекс в массиве серверов-потребителей) и k (индекс в массиве сигналов). Приведенный ниже пример написан на языке Astra.Om, в нем список сигналов с их параметрами записывается в лог:

```
i: int4 = 0;
while (i < Configurator.ConsumersCount) //цикл выполняется, пока в массиве A не будут описаны все сервера-потребители
{
  k: int4 = 0;
  while (k < Configurator.GetSignalsCount(i)) //цикл выполняется, пока в массив B не будут записаны все сигналы i-го сервера-потребителя
  {
```

```
    DebugTool.Log("Название сигнала:
"+Configurator.GetSignalName(i,k)+"; Режим записи:
"+String.ToString(
Configurator.GetSignalMode(i,k))+"; Тип сообщения: "+
Configurator.GetSignalType(i,k)); //в Журнал времени
исполнения записывается список сигналов i-го сервера
    k += 1;
  }
  i += 1;
}
```

В результате вызова функций в Журнал времени исполнения запишется список сигналов с их параметрами:



1.2.4.1.10.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
ConsumersCount	Количество потребителей аудита, указанных в конфигурации Astra.Security.Agent
LdapCount	Количество LDAP-серверов, указанных в конфигурации Astra.Security.Agent
ReadError	Текст ошибки, возникшей при чтении конфигурации Astra.Security.Agent
GeneratedString	Текст готовой конфигурации Astra.Security.Agent в формате .xml
Error	Текст ошибки, возникшей при конфигурировании Astra.Security.Agent
Уровень логирования	Степень вывода сообщений о работе в журал приложений
Пароль пользователя по умолчанию	Пароль учетной записи, используемой по умолчанию
Пользователь по умолчанию	Любой пользователь, существующий на LDAP-сервере
Имя гостевой УЗ	Произвольное имя гостевой учетной записи
Адрес папки системы безопасности	Путь к папке с конфигурацией системы безопасности на LDAP-сервере
Пароль пользователя LDAP	Пароль пользователя для подключения к LDAP-серверу

Пользователь LDAP	Путь к пользовательской папке на LDAP-сервере
Режим работы контроля целостности	Включение/выключение режима работы системы контроля целостности файлов и папок
Использование защищенного соединения	Использование/отказ от использования защищенного соединения при подключении к LDAP-серверу
Порт LDAP сервера	Порт для подключения к LDAP-серверу
Адрес LDAP сервера	IP адрес или имя компьютера, где расположен LDAP-сервер
Порт Net агента	Порт для подключения к Astra.Net.Agent
Адрес Net агента	IP адрес или имя компьютера, где расположен Astra.Net.Agent
Комбинации блокировок	Комбинация клавиш, блокируемые драйвером клавиатуры
Трассировка аудита	Логировать ли сообщения аудита в журнал приложений
Кэш прав пользователя	Использовать ли кэширование значения прав текущего пользователя
Префикс сообщений аудита	Префикс для сообщений аудита для идентификации источника

1.2.4.1.10.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.10.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.10.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.10.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.10.3.5. Адрес Net агента

IP-адрес или имя компьютера, на котором установлен Net-агент, к которому подключается агент безопасности. Под Net-агентом подразумевается служба Astra.Net.Agent (на ОС Windows) или Astra.Net.service (на ОС Linux).

Зачастую Net-агент установлен на локальном компьютере.

Значение свойства соответствует значению атрибута Address элемента <EntryPointNetAgent> в конфигурационном файле агента безопасности.

string NetHost

1.2.4.1.10.3.6. Порт Net агента

Номер порта для подключения к Net-агенту, к которому подключается агент безопасности.

Значение свойства соответствует значению атрибута Port элемента <EntryPointNetAgent> в конфигурационном файле агента безопасности.

int4 NetPort

1.2.4.1.10.3.7. Адрес LDAP сервера

IP-адрес или имя компьютера, на котором развернут LDAP-сервер, к которому подключается агент безопасности.

Свойство устарело. Теперь при настройке агента может быть указано несколько LDAP-серверов, поэтому значения адресов записываются в компонент в виде массива.

Чтобы прочитать конкретное значение в массиве:

1. Вызовите функцию Read(), предназначенную для записи текущей конфигурации агента в массив.
2. Вызовите функцию GetLdapHost(), указав в качестве входного параметра номер элемента в массиве.

Количество элементов в массиве (LDAP-серверов) записывается в значение свойства LdapCount. Каждый элемент массива соответствует значению атрибута Address одного из элементов <LDAPServer> в конфигурационном файле агента безопасности.
Чтобы добавить описание нового LDAP-сервера, используйте функцию AddLdap().

string LdapHost

1.2.4.1.10.3.8. Порт LDAP сервера

Номер порта для подключения к LDAP-серверу.

Свойство устарело. Теперь при настройке агента может быть указано несколько LDAP-серверов, поэтому значения портов записываются в компонент в виде массива.

Чтобы прочитать конкретное значение в массиве:

1. Вызовите функцию Read(), предназначенную для записи текущей конфигурации агента в массив.
2. Вызовите функцию GetLdapPort(), указав в качестве входного параметра номер элемента в массиве.

Количество элементов в массиве (LDAP-серверов) записывается в значение свойства LdapCount. Каждый элемент массива соответствует значению атрибута Port одного из элементов <LDAPServer> в конфигурационном файле агента безопасности.

Чтобы добавить описание нового LDAP-сервера, используйте функцию AddLdap().

string LdapPort

1.2.4.1.10.3.9. Использование защищенного соединения

Указывает агенту безопасности необходимость использования защищенного соединения с LDAP-сервером.

Значение свойства соответствует значению атрибута value элемента <LdapSecure> в конфигурационном файле агента безопасности.

bool UseSecureConnection

1.2.4.1.10.3.10. Режим работы контроля целостности

Указывает, включен ли режим контроля целостности файлов и папок.

bool ICMode

Значение свойства соответствует значению атрибута ICMode элемента <Options> в конфигурационном файле агента безопасности:

- 0 – контроль целостности отключен, значение свойства – fasle;
- 1 – контроль целостности включен, значение свойства – true.

1.2.4.1.10.3.11. Пользователь LDAP

Учетная запись администратора LDAP-сервера.

string LdapUser

Поскольку учетная запись хранится на LDAP-сервере в виде каталога, обращение к ней происходит в стандартном для LDAP виде:

cn=ЛогинПользователя,dc=ДоменLDAPсервера

Значение свойства соответствует значению атрибута value элемента <LdapUser> в конфигурационном файле агента безопасности.

Примеры

Пример значения: cn=Manager,dc=maxcrc,dc=com

1.2.4.1.10.3.12. Пароль пользователя LDAP

Пароль учетной записи администратора LDAP-сервера.

Поскольку пароли являются секретной информацией, просмотреть текущее значение при чтении конфигурации нельзя. При создании новой конфигурации свойство используется для записи нового значения. Значение пароля, введенное в открытом виде, будет зашифровано.

string LdapUserPass

1.2.4.1.10.3.13. Адрес папки системы безопасности

Название корневого каталога на LDAP-сервере.

string LdapDN

Обращение к каталогу происходит в стандартном для LDAP виде:

ou=НазваниеПапки,dc=ДоменLDAPсервера

Значение свойства соответствует значению атрибута value элемента <SecurityDn> в конфигурационном файле агента безопасности.

Примеры

Пример значения: ou=AstraSecurity,dc=maxcrc,dc=com

1.2.4.1.10.3.14. Имя гостевой УЗ

Имя гостевой учетной записи – записи, чьи права используются, когда нет активной пользовательской сессии.

Значение свойства соответствует значению атрибута value элемента <GuestDisplayName> в конфигурационном файле агента безопасности.

string GuestName

1.2.4.1.10.3.15. Пользователь по умолчанию

Имя учетной записи пользователя по умолчанию – пользователя, чья сессия становится активной, если другие пользователи не авторизовались в подсистеме.

Значение свойства соответствует значению атрибута value элемента <DefaultUser> в конфигурационном файле агента безопасности.

string DefaultUser

1.2.4.1.10.3.16. Пароль пользователя по умолчанию

Пароль пользователя по умолчанию.

Значение свойства соответствует значению атрибута value элемента <DefaultUserPassword> в конфигурационном файле агента безопасности.

string DefaultUserPass

1.2.4.1.10.3.17. Уровень логирования

Означает количество информации, выводимой в лог подсистемы безопасности.

Значение свойства соответствует значению
атрибута LoggerLevel элемента <Options> в конфигурационном файле агента безопасности:

- 0 – в лог выводится минимум информации;
- 2 – в лог выводится вся основная информация о работе Astra.Security;
- 5 – в лог выводится дополнительная информация о работе Astra.Security помимо основной.

string LoggerLevel

1.2.4.1.10.3.18. Комбинации блокировки

Перечень клавиш, заблокированных для использования пользователем.

Заблокированные сочетания указаны в виде SCAN-кодов клавиш, разделенных внутри сочетания символом "+", а между сочетаниями – символом ";".

Значение свойства соответствует значению атрибута kbDriverString элемента <Options> в конфигурационном файле агента безопасности.

string DriverString

Примеры

Пример значения: 0x1D+0x38+0x53;0x1D+0x2A+0x01;
В данном примере заблокированы сочетания Ctrl+Alt+Del и Ctrl+Shift+Esc.

1.2.4.1.10.3.19. Трассировка аудита

Включает трансляцию сообщений аудита в системный журнал.

Значение свойства соответствует значению атрибута TraceAudit элемента <AuditLogConsumers> в конфигурационном файле агента безопасности:

- 0 – сообщения не транслируются в системный журнал, значение свойства – fasle;
- 1 – сообщения транслируются в системный журнал, значение свойства – true.

bool TraceAudit

1.2.4.1.10.3.20. Кэш прав пользователя

Указывает, используются ли кэшированные значения прав пользователя.

Значение свойства соответствует значению
атрибута UseRightsCacheStorage элемента <Options> в конфигурационном файле агента безопасности:

- 0 – актуальные значения прав пользователя запрашиваются с LDAP-сервера постоянно, значение свойства – false;
- 1 – значения прав пользователя запрашиваются с LDAP-сервера только в момент входа пользователя в подсистему, а в процессе его работы значения запрашиваются из кэша. Значение свойства в таком случае – true.

bool UseRightsStorageCache

1.2.4.1.10.3.21. Префикс сообщений аудита

Префикс сообщений аудита.

Значение свойства соответствует значению атрибута value элемента <mesPrefix> в конфигурационном файле агента безопасности.

string MesPrefix

1.2.4.1.10.3.22. UnderfinedListItems

Список полей (свойств), для которых обязательно указать значение для создания новой конфигурации Агент Astra.Security с помощью функции Generate().

string UnderfinedListItems

Доступно только для чтения в режиме рантайма.

1.2.4.1.10.3.23. ConsumersCount

Количество серверов-потребителей аудита, указанных в конфигурационном файле Агент Astra.Security.

int4 ConsumersCount

Доступно только для чтения в режиме рантайма.

1.2.4.1.10.3.24. LdapCount

Количество LDAP-серверов, указанных в конфигурационном файле Агент Astra.Security.

int4 LdapCount

Доступно только для чтения в режиме рантайма.

1.2.4.1.10.3.25. ReadError

Текст ошибки, возникшей при попытке чтения конфигурации Агент Astra.Security с помощью функции Read().

string ReadError

Доступно только для чтения в режиме рантайма.

1.2.4.1.10.3.26. GeneratedString

Полный текст конфигурационного файла Агент Astra.Security в xml-формате, созданного в результате вызова функции Generate().

string GeneratedString

Доступно только для чтения в режиме рантайма.

1.2.4.1.10.3.27. Error

Текст ошибки, возникшей при попытке создания новой конфигурации Агент Astra.Security с помощью функции Generate().

string Error

Доступно только для чтения в режиме рантайма.

1.2.4.1.11. Информация лицензирования: Получение

Компонент предназначен для получения информации о лицензировании.

1.2.4.1.11.1. События

Событие	Описание
RequestLicenseInfoComplete	Сигнал об успешном получении LicenseInfo, определенной сервером лицензирования на устройстве
RequestRemoteLicenseInfoComplete	Сигнал об успешном получении LicenseInfo, определенной сервером лицензирования на устройстве с удаленного узла
RequestLicenseInfoFailed	Сигнал об ошибке в процессе получения LicenseInfo, определенной сервером лицензирования на устройстве
RequestRemoteLicenseInfoFailed	Сигнал об ошибке в процессе получения LicenseInfo, определенной сервером лицензирования на устройстве с удаленного узла

1.2.4.1.11.1.1. RequestLicenseInfoComplete

Сигнал об успешном получении LicenseInfo, определенной сервером лицензирования на устройстве.

1.2.4.1.11.1.2. RequestRemoteLicenseInfoComplete

Сигнал об успешном получении LicenseInfo, определенной сервером лицензирования на устройстве с удаленного узла.

1.2.4.1.11.1.3. RequestLicenseInfoFailed

Сигнал об ошибке в процессе получения LicenseInfo, определенной сервером лицензирования на устройстве.

1.2.4.1.11.1.4. RequestRemoteLicenseInfoFailed

Сигнал об ошибке в процессе получения LicenseInfo, определенной сервером лицензирования на устройстве с удаленного узла.

1.2.4.1.11.2. Функции

Функция	Описание
RequestLicenseInfo	Асинхронный запрос на получение лицензионной информации
RequestRemoteLicenseInfo	Асинхронный запрос на получение лицензионной информации с удаленного узла
GetErrorDescriptionByCode	Возвращает текстовое описание ошибок, возникающих при загрузке и сохранении приложений

1.2.4.1.11.2.1. RequestLicenseInfo

Асинхронный запрос на получение лицензионной информации.

void RequestLicenseInfo(string jsonRequest)

Параметры

Параметр	Тип	Описание
jsonRequest	string	Запрос

1.2.4.1.11.2.2. RequestRemoteLicenseInfo

Асинхронный запрос на получение лицензионной информации с удаленного узла.

void RequestRemoteLicenseInfo(string jsonRequest, string aNetNode)

Параметры

Параметр	Тип	Описание
jsonRequest	string	Запрос
aNetNode	string	Имя удаленного узла

1.2.4.1.11.2.3. GetErrorDescriptionByCode

Возвращает текстовое описание ошибок, возникающих при загрузке и сохранении приложений.

string GetErrorDescriptionByCode(uint1 FailReasonCode)

Параметры

Параметр	Тип	Описание
FailReasonCode	uint1	Код ошибки из любого события, говорящего об ошибке

1.2.4.1.11.3. Свойства

Свойство	Описание
Отображаемое имя	Описание объекта
Кардинальное число	Преобразует объект в массив и задает размер массива
Length	Размер массива (количество элементов в массиве)
Index	Индекс элемента в массиве
Контекст безопасности	Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом
LicenseInfo	Уведомление об изменении в группе, загруженной в элемент

1.2.4.1.11.3.1. Отображаемое имя

Описание объекта (поля объекта). Позволяет указать произвольное (например, русскоязычное) имя для узнаваемости объекта (поля объекта) в проекте. Не мешает использованию базового англоязычного имени объекта (поля объекта) для обращения в коде.

1.2.4.1.11.3.2. Кардинальное число

Преобразует объект в массив и задает размер массива (количество элементов в массиве).

Значение

Значение	Описание
1	Одиночный объект
>1	Массив соответствующей размерности

1.2.4.1.11.3.3. Length

Размер массива (количество элементов в массиве).

int8 Length

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

```
//Записать в текстовое поле длину массива:
TextEdit_1.Text = String.ToString (SW_1.Length);
```

1.2.4.1.11.3.4. Index

Индекс элемента в массиве. Позволяет отследить у какого элемента сработало то или иное событие.

int8 Index

Есть только у массивов и доступно только для чтения в режиме рантайма.

Примеры

//Записать в текстовое поле индекс элемента массива, у которого сработало событие изменения значения:
TextEdit_2.Text = String.ToString(Index);

//Записать в текстовое поле текущее значение элемента массива, у которого сработало событие изменения значения:
TextEdit_3.Text = String.ToString(penwidth[Index]);

//В зависимости от индекса элемента в массиве вывести в текстовое поле запись о включении соответствующего режима работы задвижки:

```
if (SW_1.Mode.Index == 0)  {
    TextEdit_1.Text = "Включен режим 1";}
else
    {TextEdit_1.Text = "Включен режим 2";}
```

1.2.4.1.11.3.5. Контекст безопасности

Ссылка на компонент Контекст безопасности, относительно которого будет происходить дальнейшая работа с компонентом. Указывается на вкладке Редактор свойств.

Необходимо заполнить для взаимодействия с подсистемой безопасности Astra.Security.

1.2.4.1.11.3.6. LicenseInfo

Уведомление об изменении в группе, загруженной в элемент.

string LicenseInfo

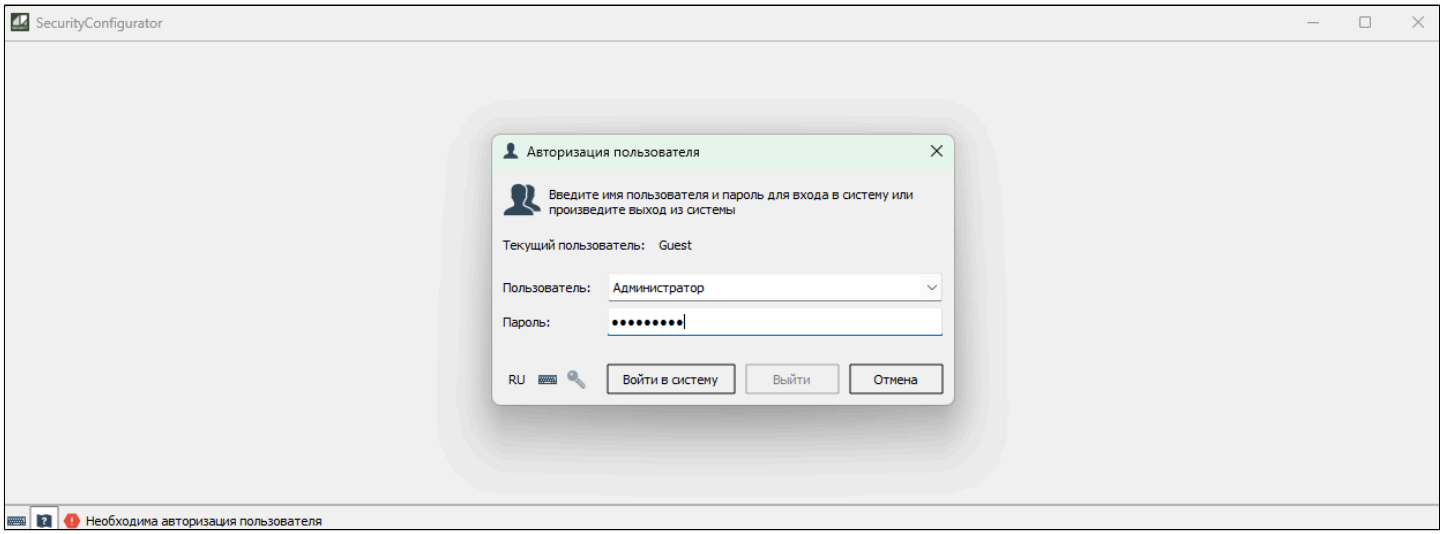
1.2.5. Блокировка сочетаний клавиш

Windows
AstraLinux
РЕД ОС 7.3
РЕД ОС 8

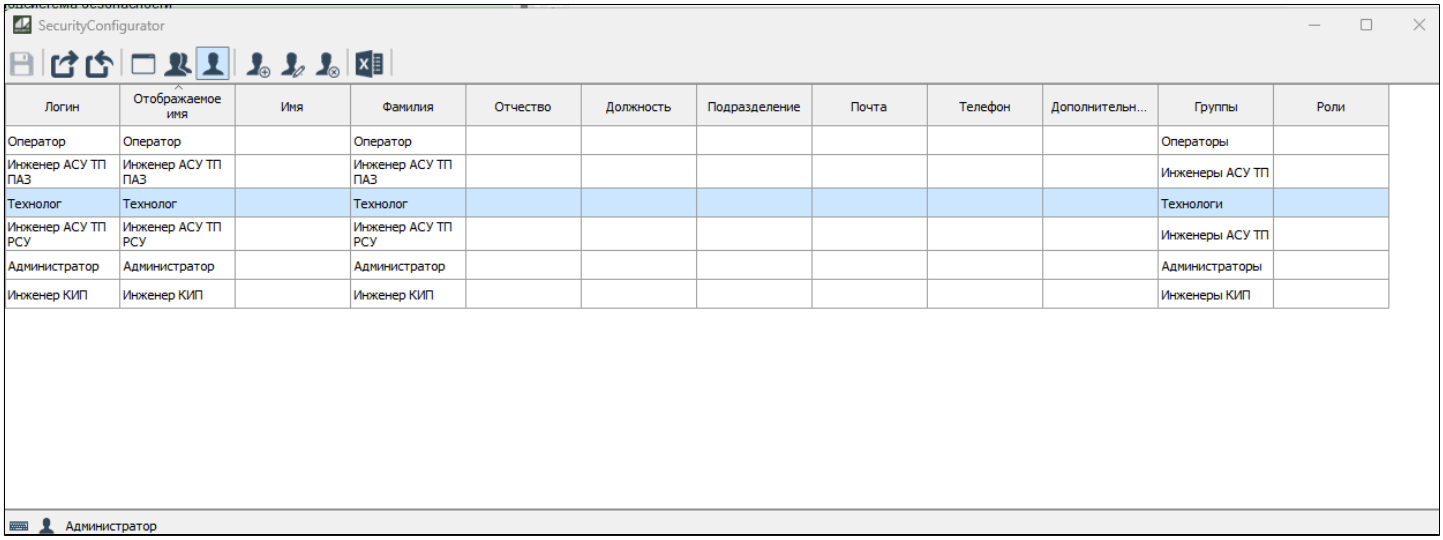
1.2.5.1. Windows

Для блокировки сочетания клавиш на ОС Windows необходимо выполнить следующие действия:

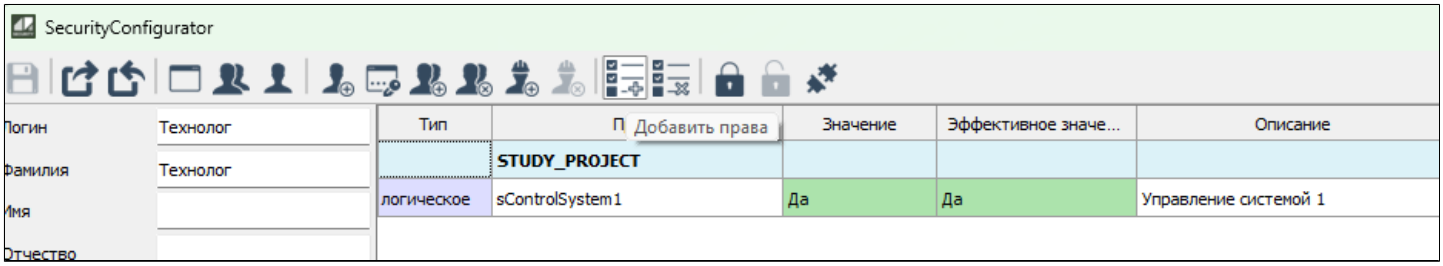
1. Запустите Astra.HMI.SecurityConfigurator и зайдите под пользователем, который обладает правами просмотра и изменение конфигурации системы безопасности:



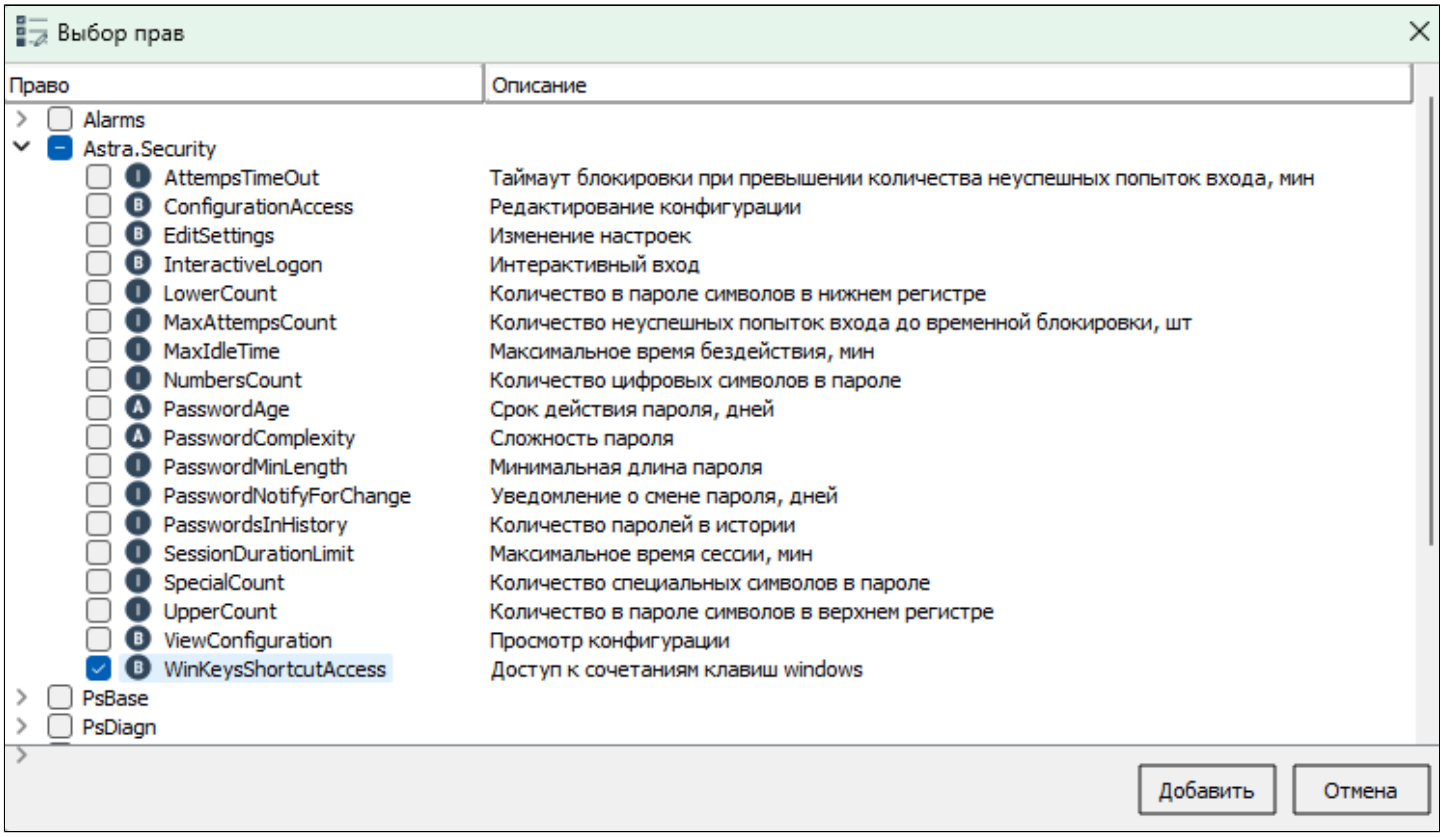
2. Выберите пользователя, которому необходимо заблокировать сочетание клавиш:



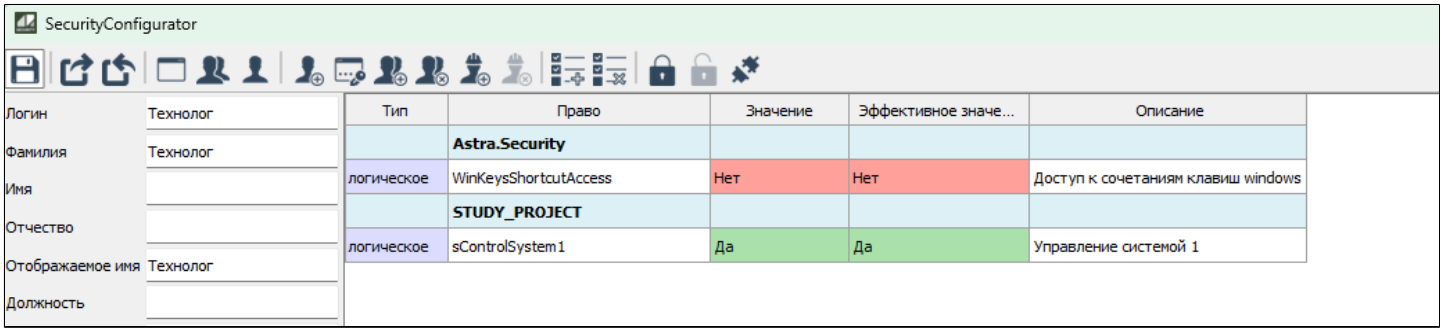
3. Нажмите кнопку "Добавить права".



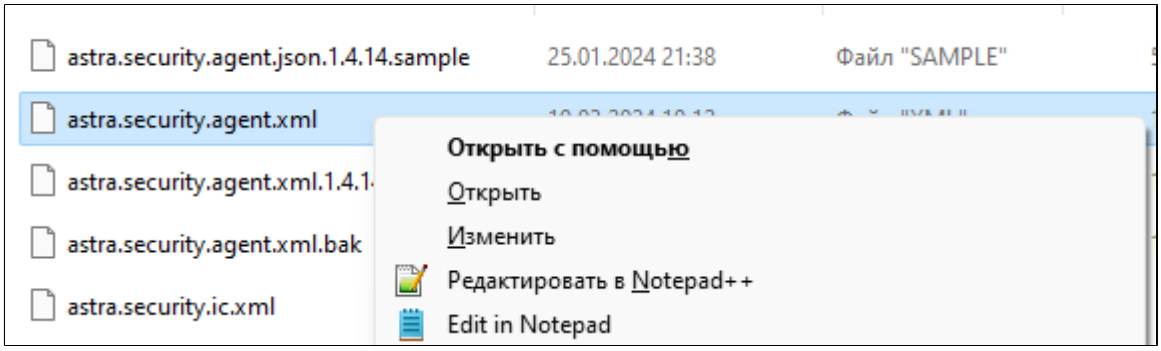
4. В списке прав выберите приложение "Astra.Security" и раскройте его. Выберите право "WinKeysShortcutAccess" и нажмите кнопку "Добавить".



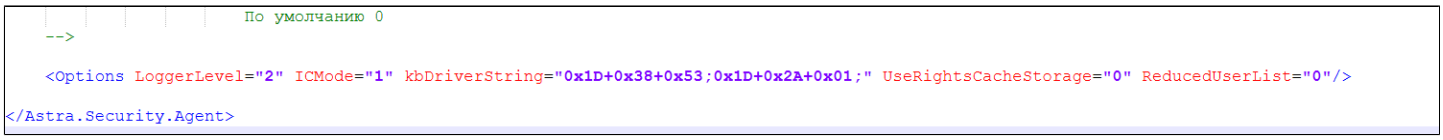
5. Укажите значение "Нет" двойным щелчком мыши по праву и нажмите кнопку "Сохранить":



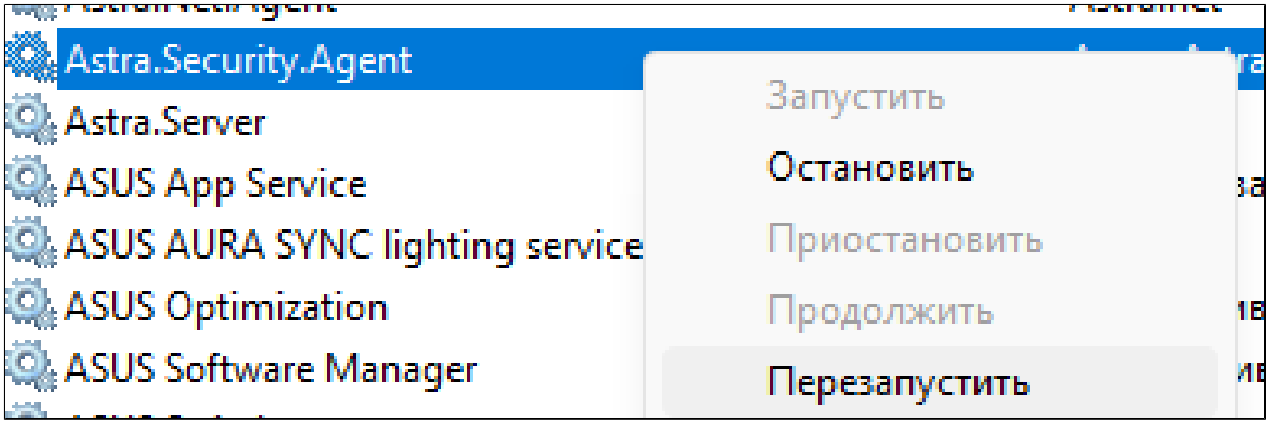
6. Перейдите в каталог Astra.Security по пути C:\Program Files\AstraRegul \Astra.Security и откройте конфигурационный файл "astra.security.agent.xml" с помощью текстового редактора:



7. В конце файла у параметра "Options" аттрибут "kbDriverString" отвечает за блокируемое сочетание клавиш. Скан коды клавиш разделяются внутри сочетанием "+", а сами сочетания ";".



8. Сохраните файл конфигурации и перезапустите службу "Astra.Security.Agent".



1.2.5.2. AstraLinux

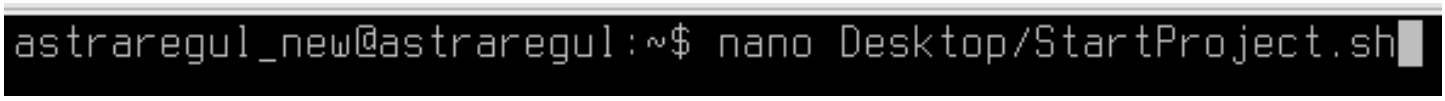
Для блокировки сочетания клавиш на ОС AstraLinux используется режим киоска.

1. Создайте пользователя с ограниченными правами, который будет работать в режиме киоска.

> Пошаговая инструкция приведена в разделе "Создание пользователя с ограниченными правами" документа "Администрирование. Руководство пользователя".

2. Авторизуйтесь под созданным пользователем и создайте скрипт запуска Astra.HMI.Viewer с блокировкой сочетания клавиш, выполнив команду:

> nano Desktop/StartProject.sh



3. В созданном файле напишите следующую конструкцию:

> #!/bin/bash
> cd <директория проекта>
> astra.hmi.viewer <Название проекта>

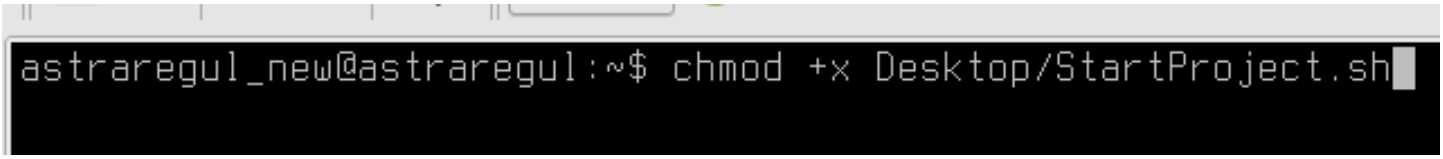
Для сохранения и выхода нажмите комбинацию клавиш "Ctrl+x". Для подтверждения изменений нажмите клавишу "y" и нажмите клавишу "Enter".

Скрипт и проект должны находиться в папке пользователя киоска.

С помощью этого скрипта будет запускаться проект с которым пользователь будет работать в киоске.

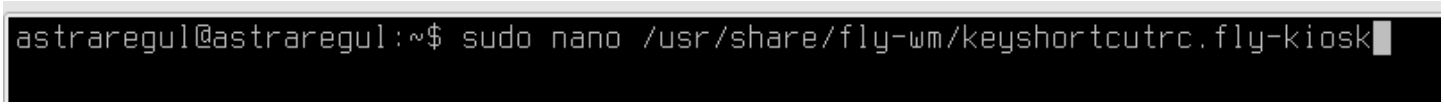
4. Для возможности запуска скрипта выполните команду:

chmod +x Desktop/StartProject.sh

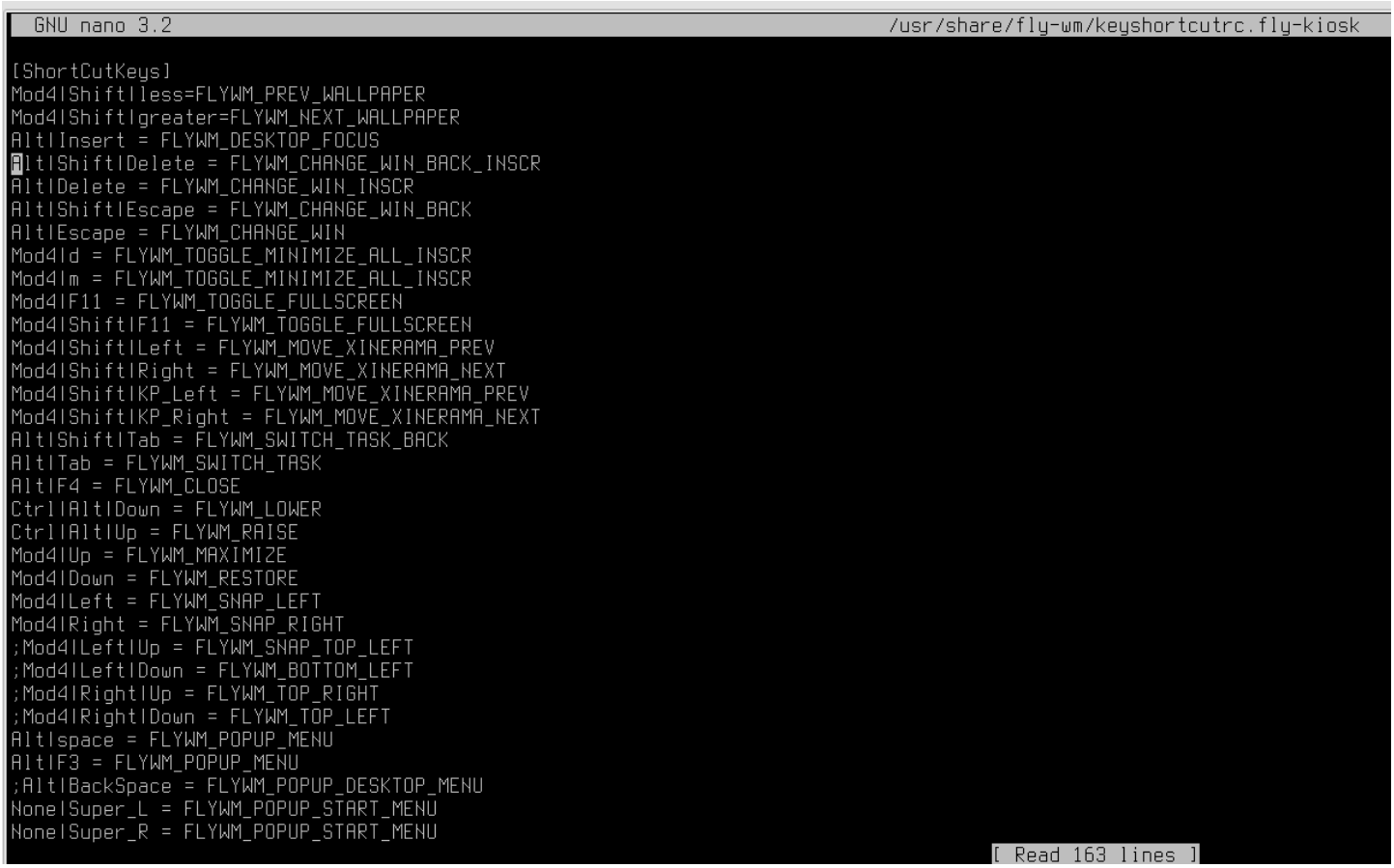


5. Зайдите в учетную запись с правами администратора.
6. Для отключения сочетаний клавиш в режиме киоска выполните команду:

sudo nano /usr/share/fly-wm/keyshortcutrc.fly-kiosk



У вас откроется графический редактор с сочетаниями клавиш

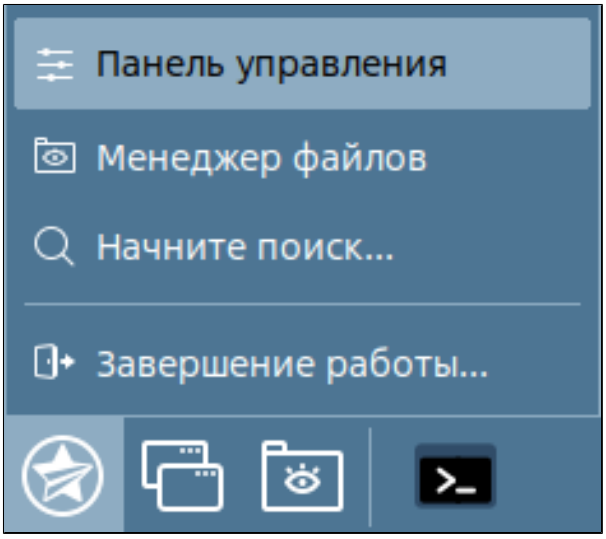



```
[ShortCutKeys]
Mod4|Shift|less=FLYWM_PREV_WALLPAPER
Mod4|Shift|greater=FLYWM_NEXT_WALLPAPER
Alt|Insert = FLYWM_DESKTOP_FOCUS
Alt|Shift|Delete = FLYWM_CHANGE_WIN_BACK_INSCR
Alt|Delete = FLYWM_CHANGE_WIN_INSCR
Alt|Shift|Escape = FLYWM_CHANGE_WIN_BACK
Alt|Escape = FLYWM_CHANGE_WIN
Mod4|d = FLYWM_TOGGLE_MINIMIZE_ALL_INSCR
Mod4|m = FLYWM_TOGGLE_MINIMIZE_ALL_INSCR
Mod4|F11 = FLYWM_TOGGLE_FULLSCREEN
Mod4|Shift|F11 = FLYWM_TOGGLE_FULLSCREEN
Mod4|Shift|Left = FLYWM_MOVE_XINERAMA_PREV
Mod4|Shift|Right = FLYWM_MOVE_XINERAMA_NEXT
Mod4|Shift|KP_Left = FLYWM_MOVE_XINERAMA_PREV
Mod4|Shift|KP_Right = FLYWM_MOVE_XINERAMA_NEXT
Alt|Shift|Tab = FLYWM_SWITCH_TASK_BACK
Alt|Tab = FLYWM_SWITCH_TASK
Alt|F4 = FLYWM_CLOSE
Ctrl|Alt|Down = FLYWM_LOWER
Ctrl|Alt|Up = FLYWM_RAISE
Mod4|Up = FLYWM_MAXIMIZE
Mod4|Down = FLYWM_RESTORE
Mod4|Left = FLYWM_SNAP_LEFT
Mod4|Right = FLYWM_SNAP_RIGHT
;Mod4|Left|Up = FLYWM_SNAP_TOP_LEFT
;Mod4|Left|Down = FLYWM_BOTTOM_LEFT
;Mod4|Right|Up = FLYWM_TOP_RIGHT
;Mod4|Right|Down = FLYWM_TOP_LEFT
Alt|space = FLYWM_POPUP_MENU
Alt|F3 = FLYWM_POPUP_MENU
;Alt|BackSpace = FLYWM_POPUP_DESKTOP_MENU
None|Super_L = FLYWM_POPUP_START_MENU
None|Super_R = FLYWM_POPUP_START_MENU
```

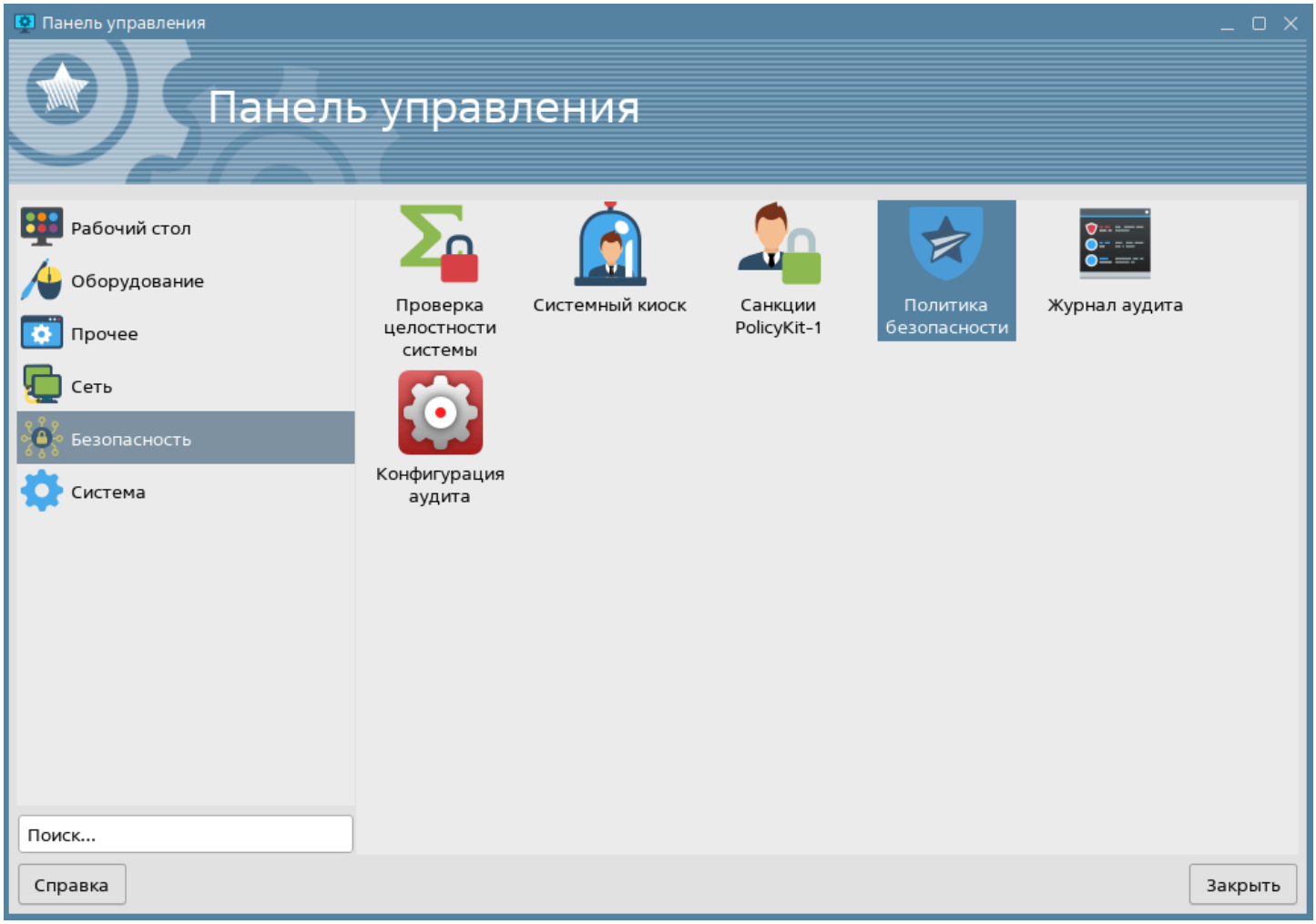
7. Удалите или закомментируйте сочетания клавиш, которые вы хотите заблокировать и сохраните файл.

```
Mod4|t = "x-terminal-emulator"
#Alt|Ctrl|Delete = "ksysguard --autosu"
#Alt|Ctrl|KP_Delete = "ksysguard --autosu"
#Shift|Ctrl|Escape = "ksysguard --autosu"
None|Print = "spectacle -f"
```

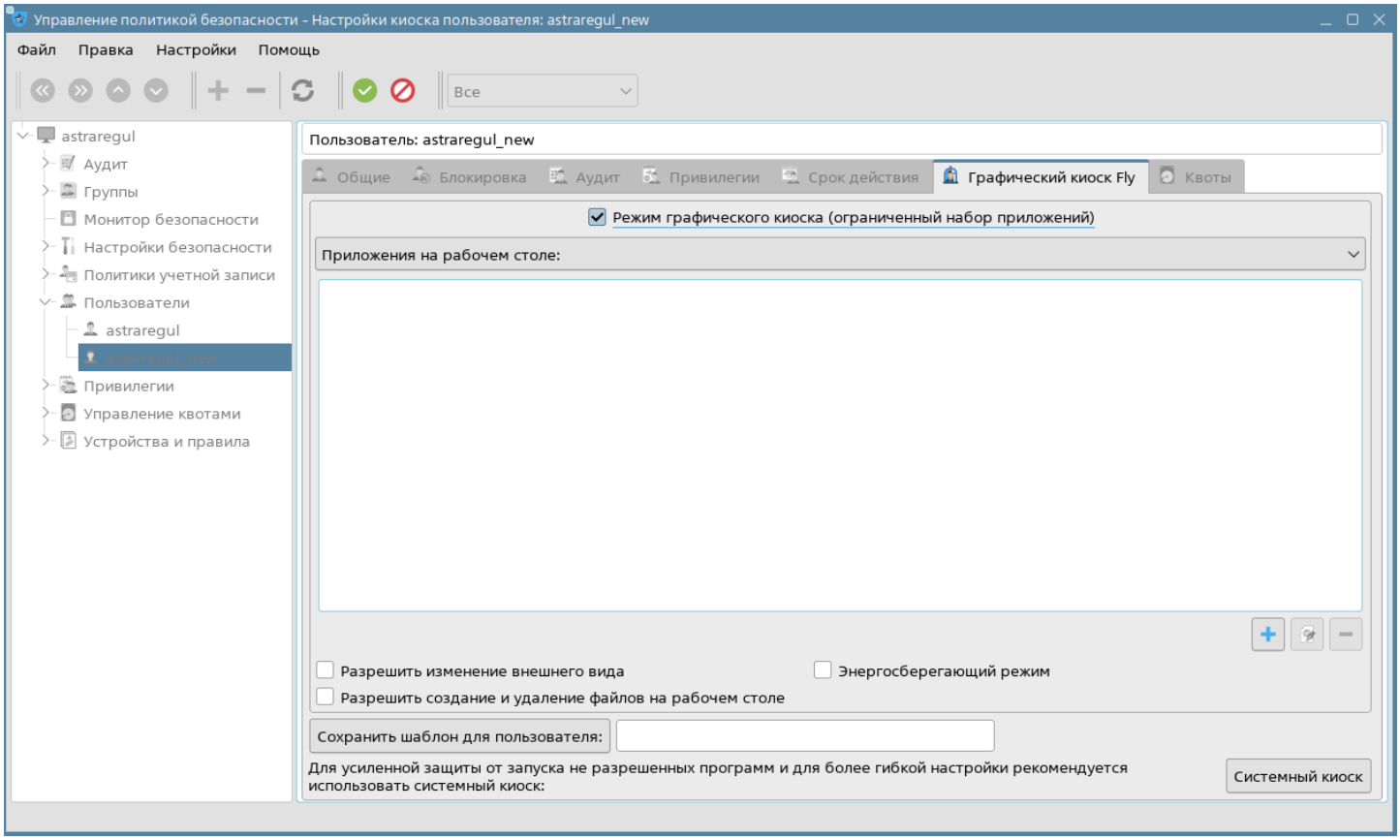
8. Откройте панель управления.



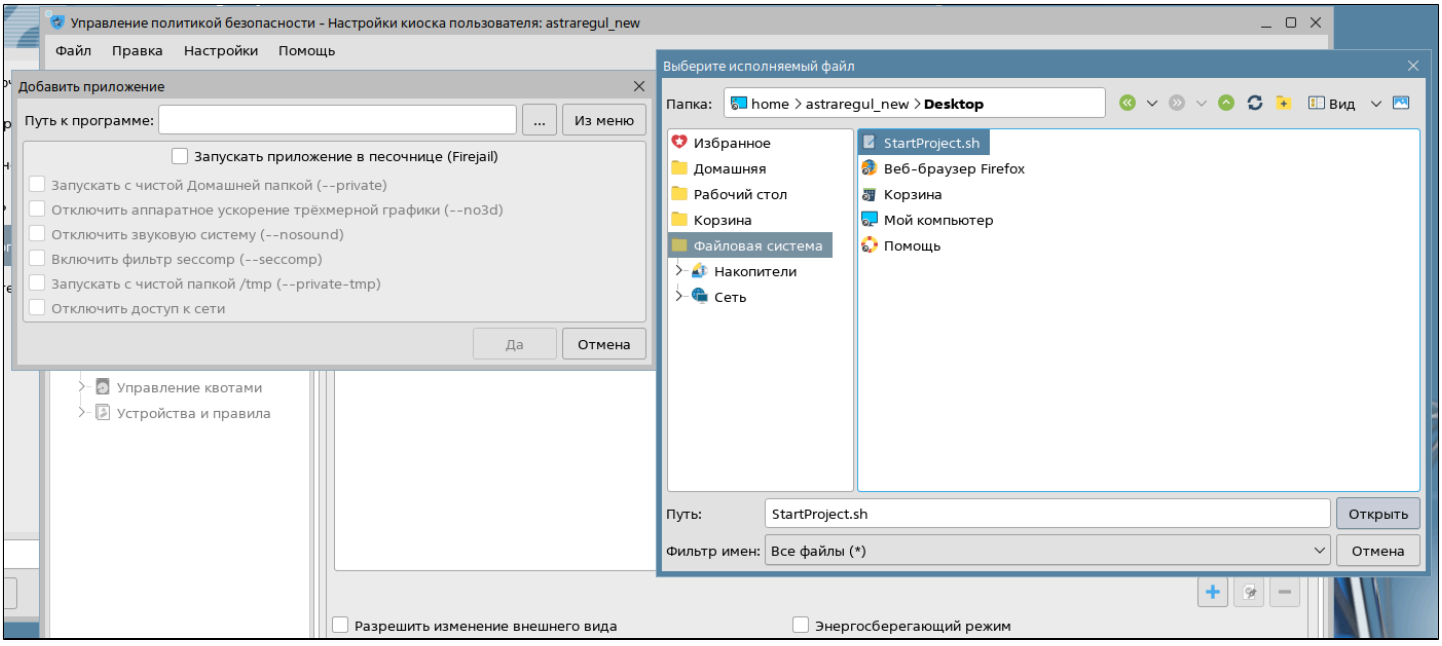
9. Перейдите в группу "Безопасность". Откройте раздел "Политика безопасности", режим графического киоска.



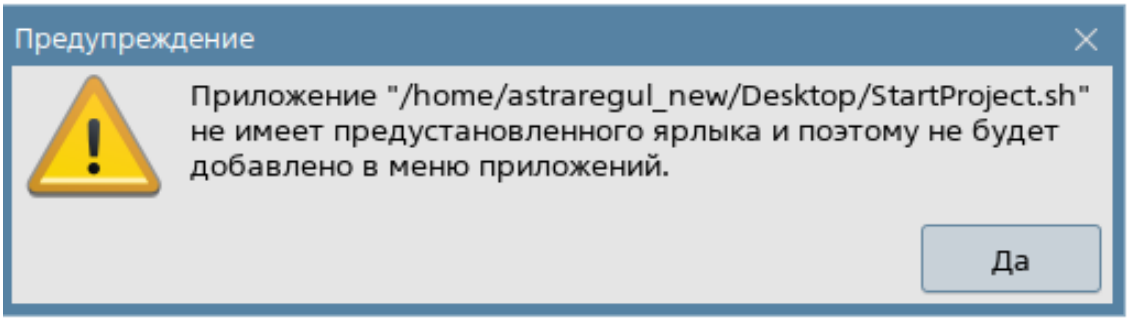
10. Выберите пользователя для режима киоска, перейдите во вкладку "Графический киоск Fly" и отметьте режим графического киоска.



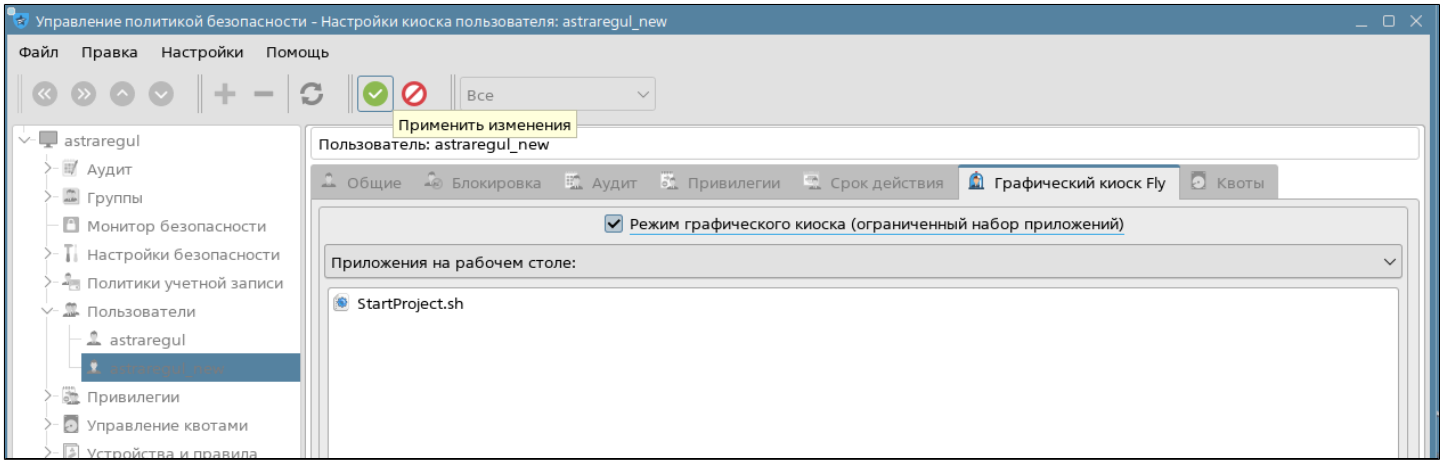
11. Добавьте созданный скрипт, который будет запускаться в киоске. Для этого нажмите кнопку "+", далее на кнопку "многоточие" и выберите путь до скрипта в папке пользователя с ограниченными правами и нажмите кнопку "Открыть".



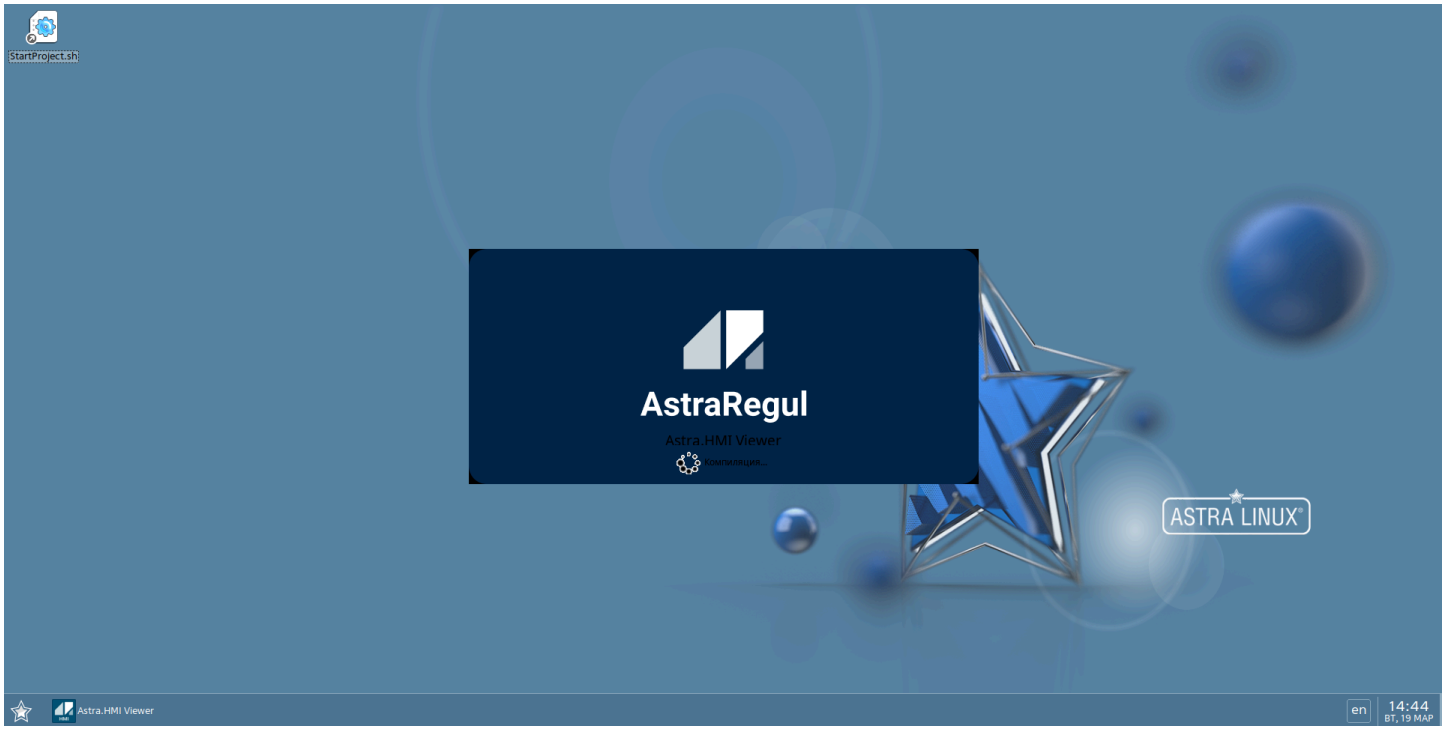
12. При открытии окна с предупреждениями нажмите кнопку "Да".



13. Сохраните настройки нажав кнопку "Применить изменения" и перезапустите ПК.



14. Войдете под пользователем, который был выбран для режима киоска. Файл скрипта будет расположен на рабочем столе. Запустите его двойным нажатием левой кнопкой мыши.



В режиме киоска недоступны команды, которые были удалены или закомментированы в файле "keyshortcutrc.fly-kiosk".

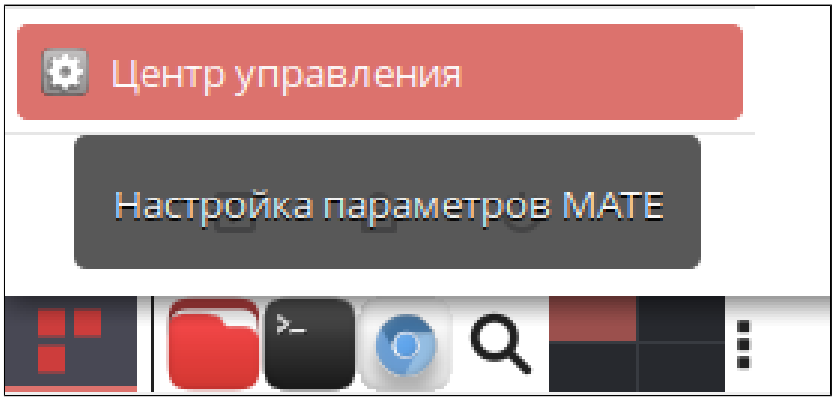
1.2.5.3. РЕД ОС 7.3

Для блокировки сочетания клавиш на ОС РЕД 7.3 используется редактор сочетания клавиш клавиатуры.

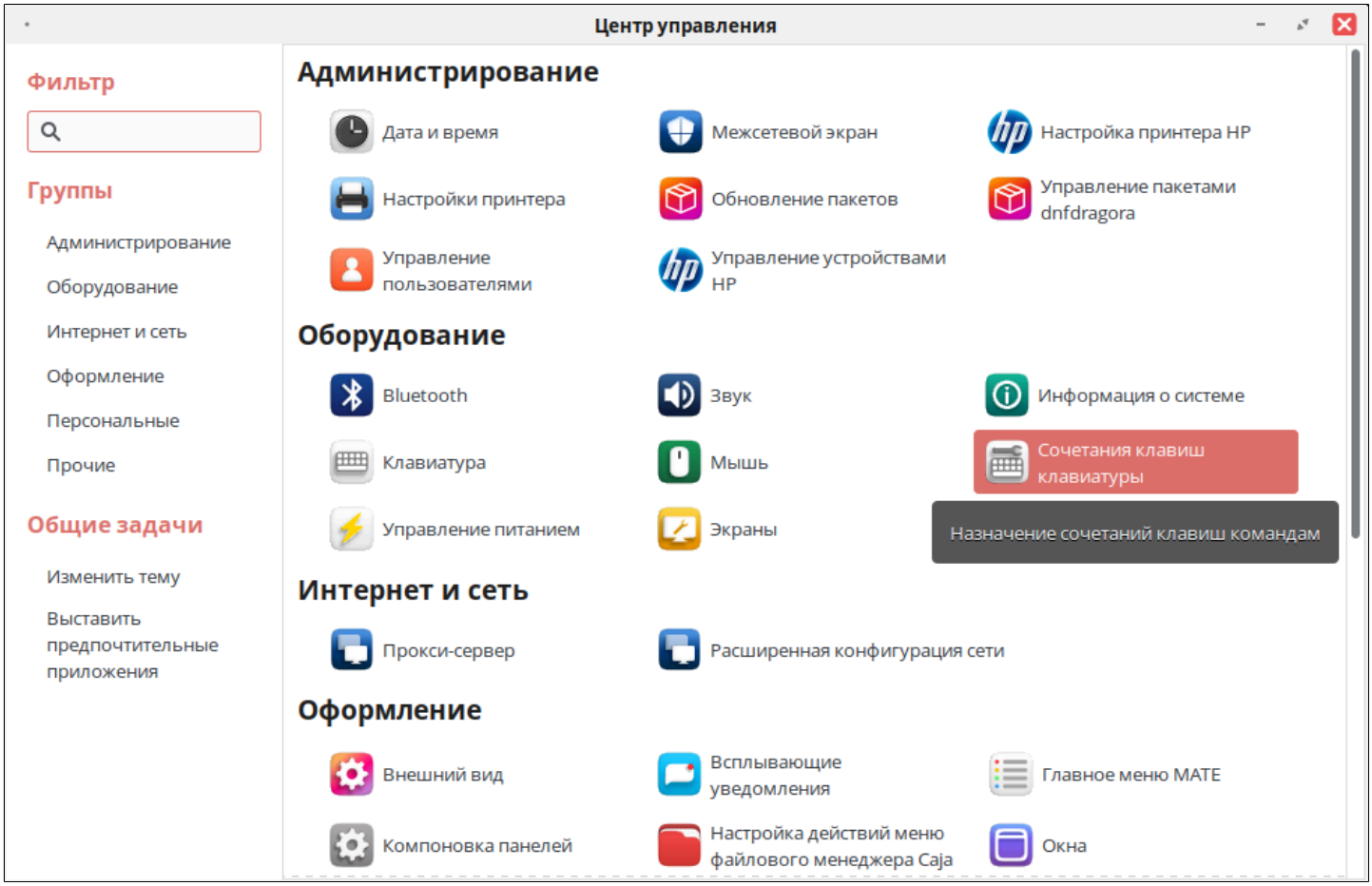
1. Создайте пользователя с ограниченными правами, у которого необходимо заблокировать сочетания клавиш.

> Пошаговая инструкция приведена в разделе "Создание пользователя с ограниченными правами" документа "Администрирование. Руководство пользователя".

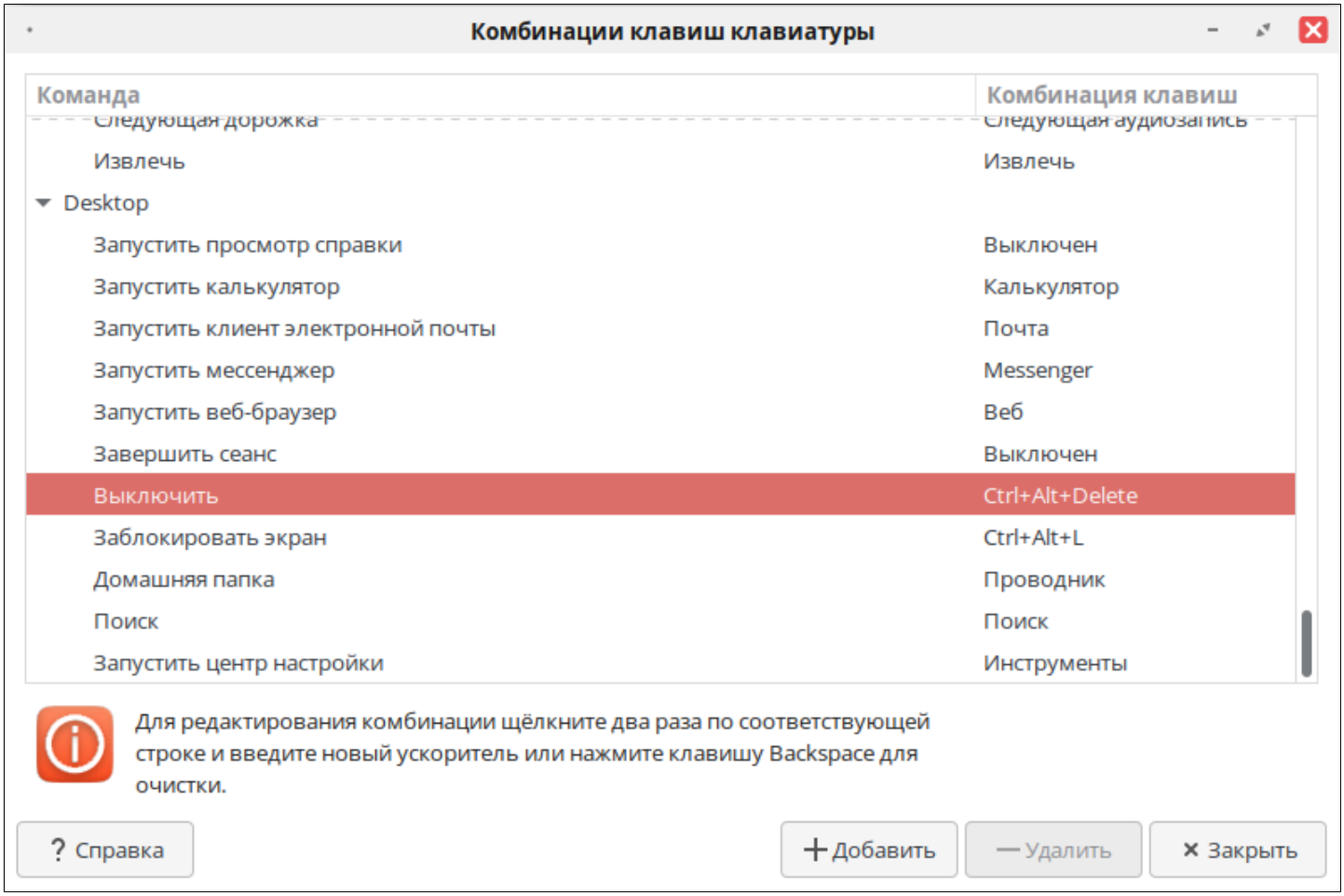
2. Авторизуйтесь под созданным пользователем и откройте "Центр управления".



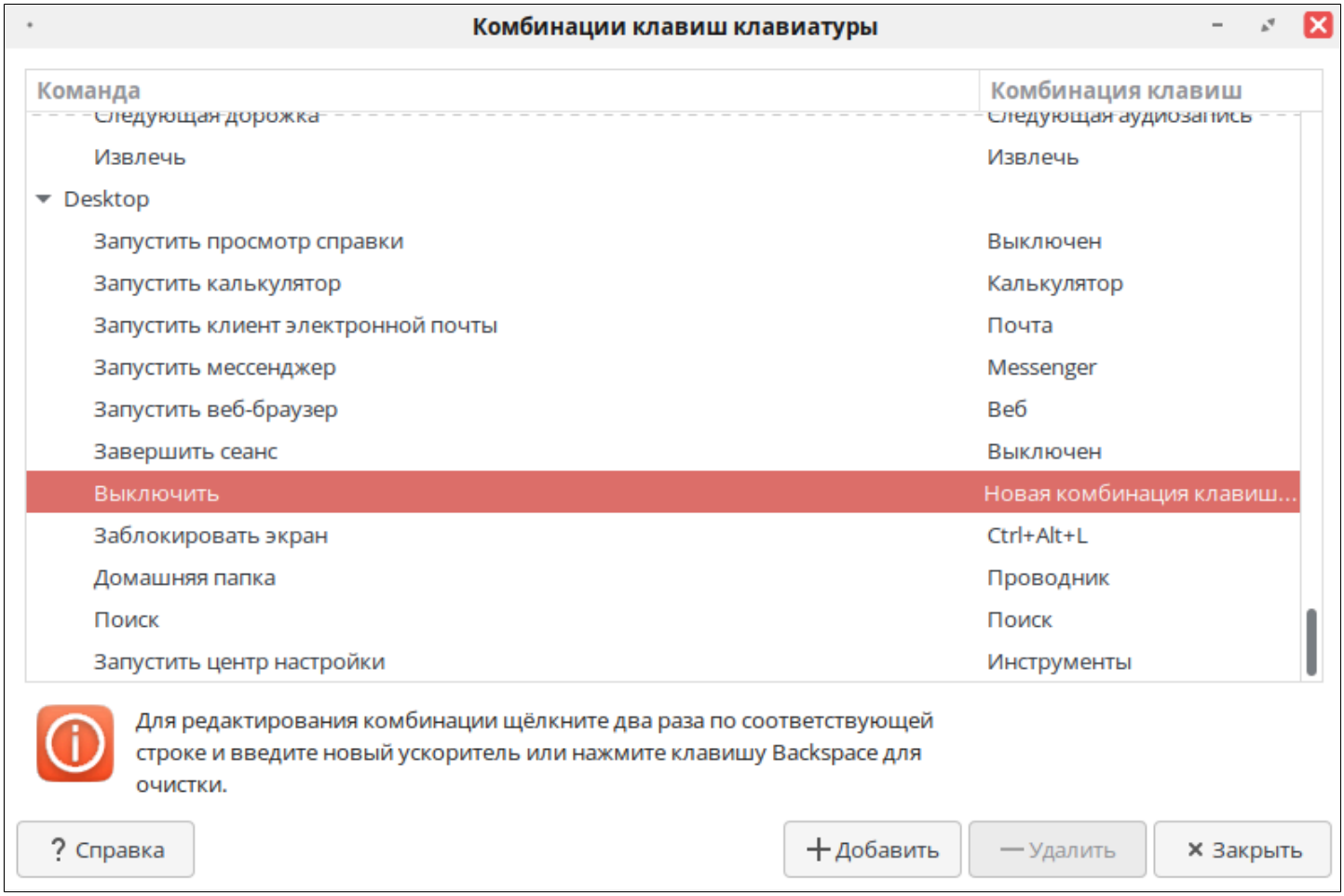
3. В разделе "Оборудование" выберите "Сочетание клавиш клавиатуры".



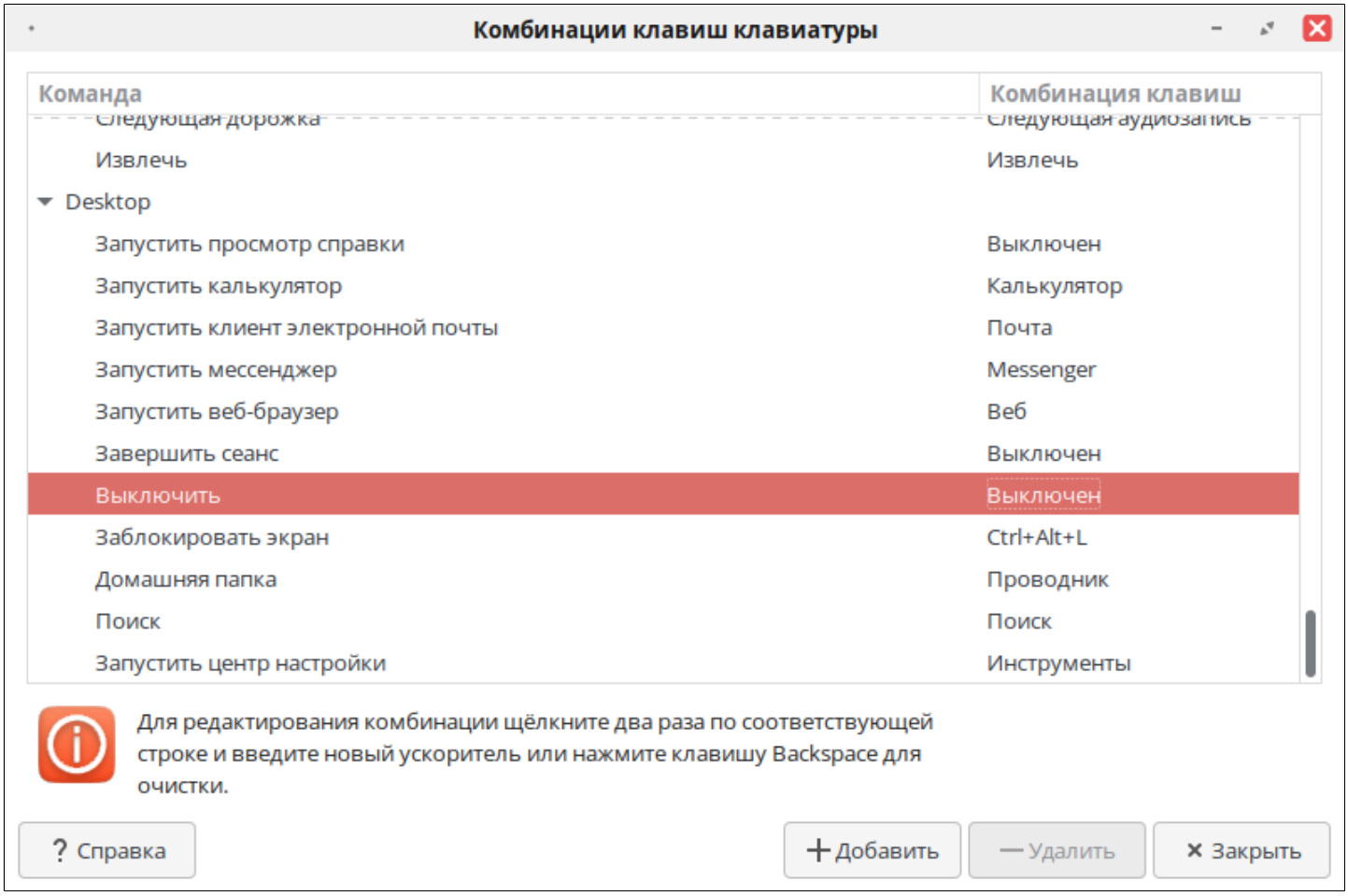
4. Выберите комбинацию клавиш клавиатуры, которую необходимо заблокировать и нажмите на неё левой кнопкой мыши.



5. Когда в строке с комбинацией отобразится сообщение "Новая комбинация клавиш..." нажмите клавишу "Backspace".



6. Комбинация клавиш для выключения ПК будет заблокирована.


Комбинации клавиш клавиатуры
Команда
Комбинация клавиш
Следующая дорожка
Следующая аудиозапись
Извлечь
Извлечь
Desktop
Запустить просмотр справки
Выключен
Запустить калькулятор
Калькулятор
Запустить клиент электронной почты
Почта
Запустить мессенджер
Messenger
Запустить веб-браузер
Веб
Завершить сеанс
Выключен
Выключить
Выключен
Заблокировать экран
Ctrl+Alt+L
Домашняя папка
Проводник
Поиск
Поиск
Запустить центр настройки
Инструменты
Для редактирования комбинации щёлкните два раза по соответствующей строке и введите новый ускоритель или нажмите клавишу Backspace для очистки.
Справка
Добавить
Удалить
Закрыть

1.2.5.4. РЕД ОС 8

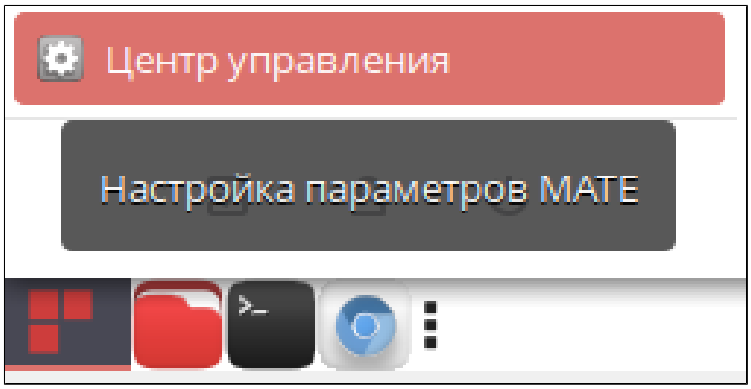
Для блокировки сочетания клавиш на ОС РЕД 8.0 используется редактор сочетания клавиш клавиатуры.

Графическая оболочка MATE

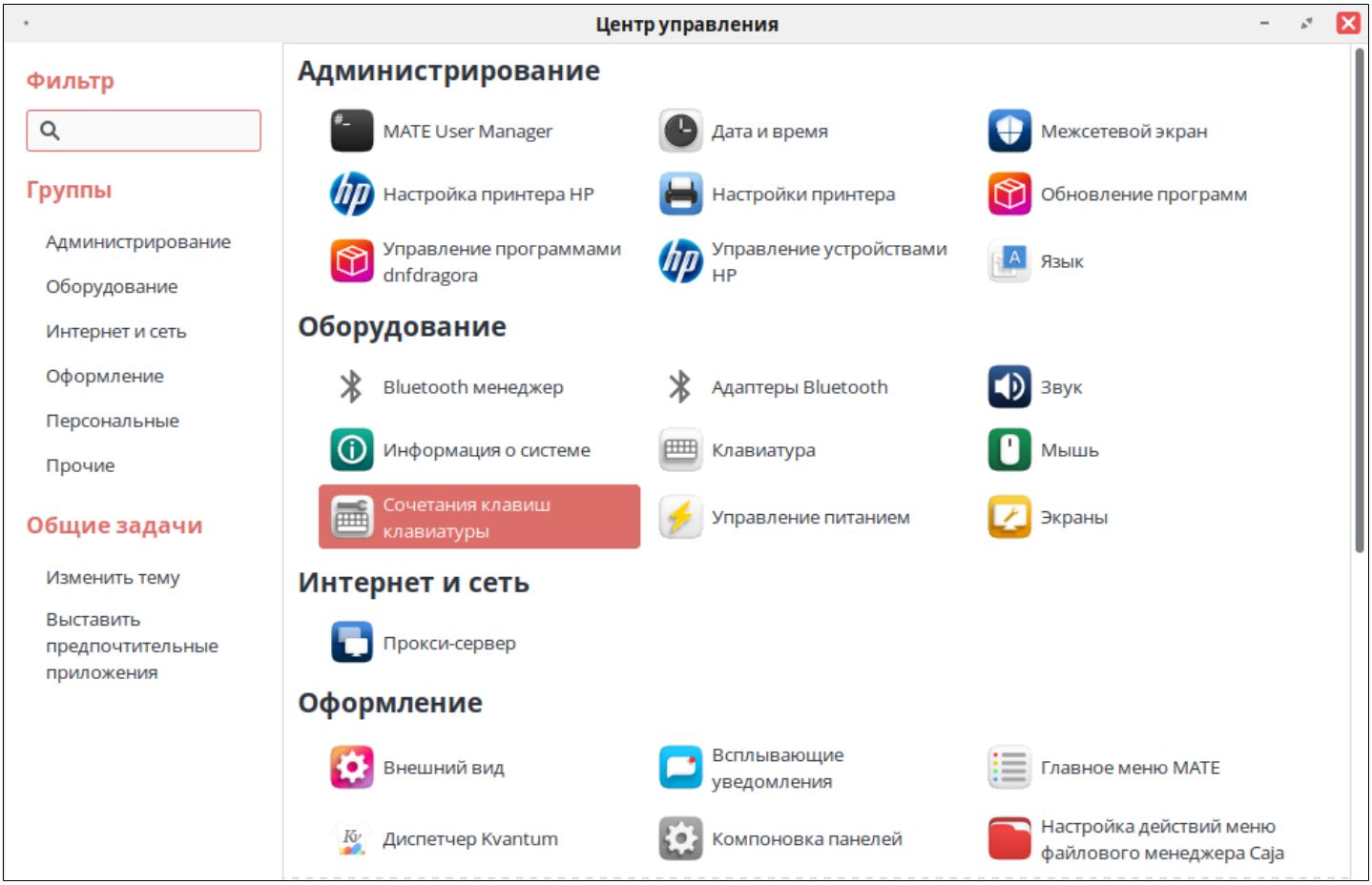
1. Создайте пользователя с ограниченными правами, у которого необходимо заблокировать сочетания клавиш.

> Пошаговая инструкция приведена в разделе "Создание пользователя с ограниченными правами" документа "Администрирование. Руководство пользователя".

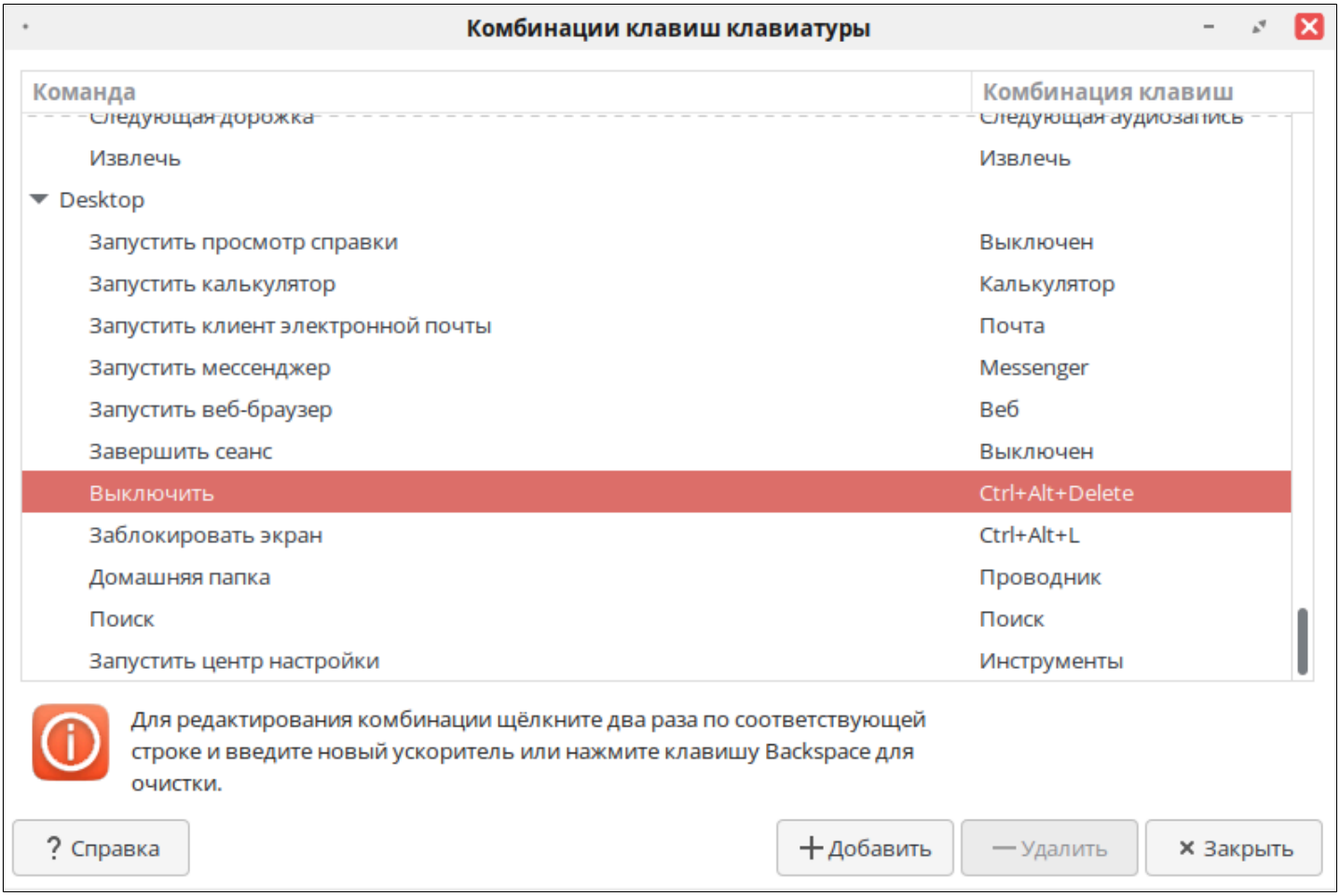
2. Авторизуйтесь под созданным пользователем в графической оболочкой MATE и откройте "Центр управления".



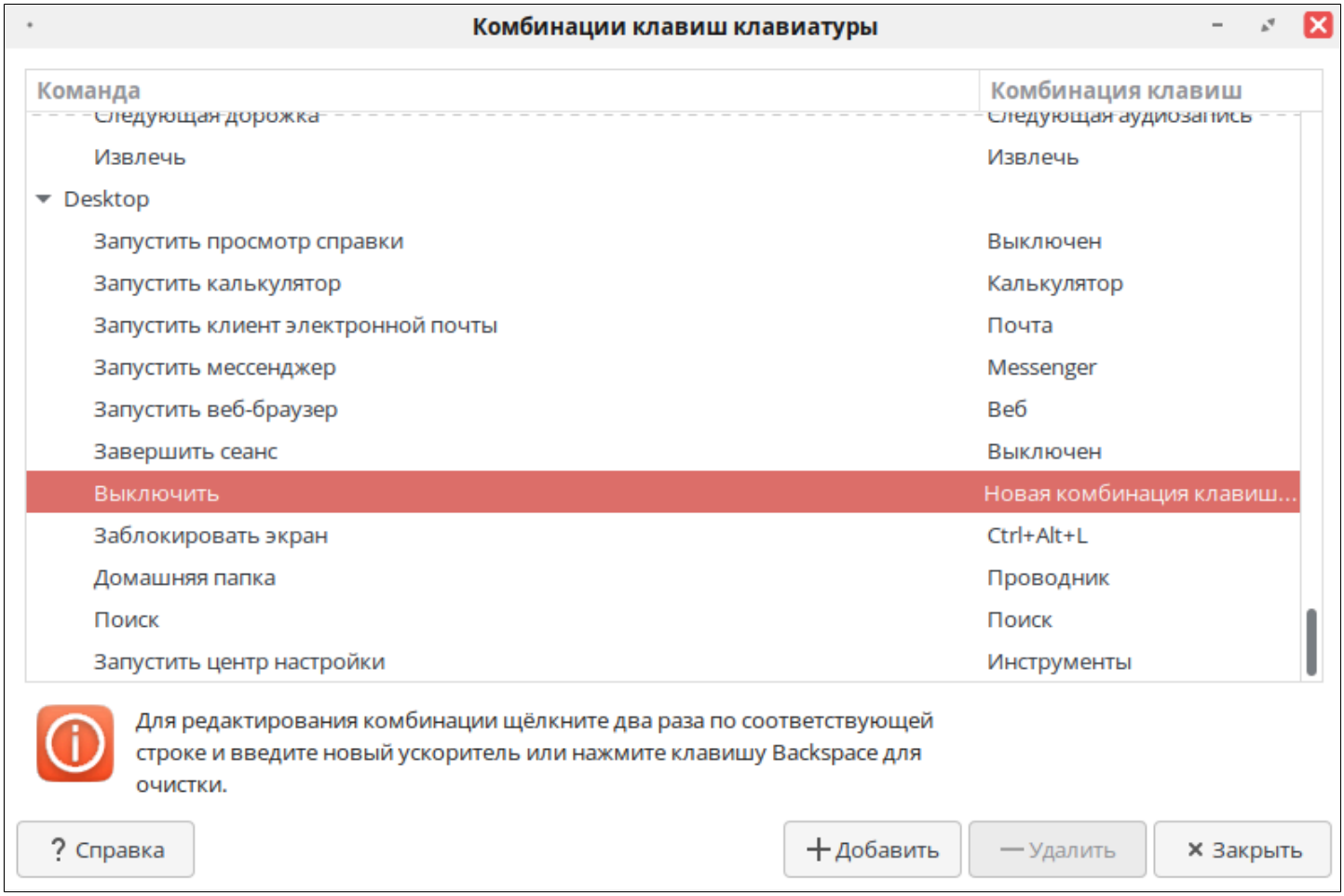
3. В разделе "Оборудование" выберите "Сочетание клавиш клавиатуры".



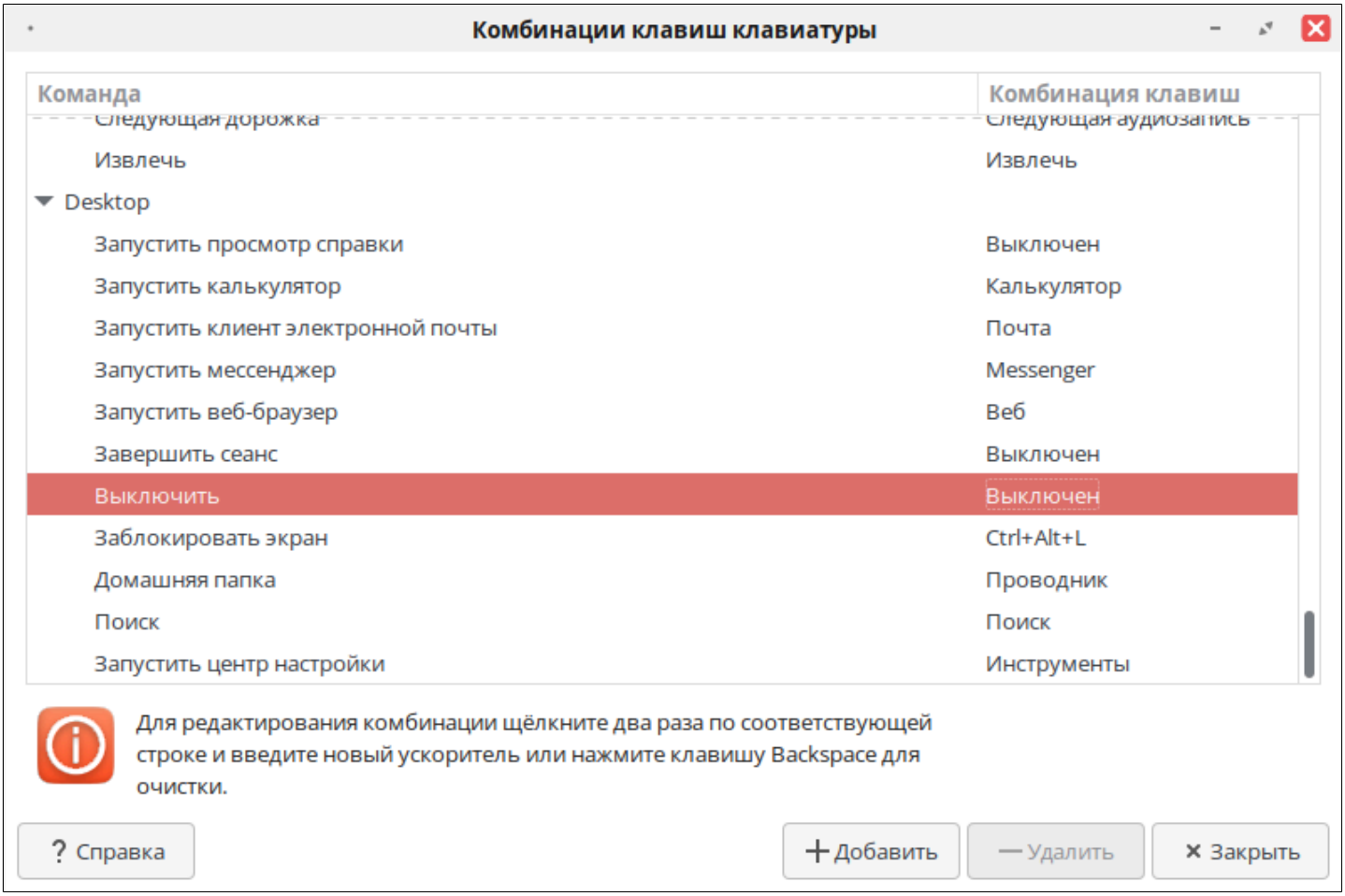
4. Выберите комбинацию клавиш клавиатуры, которую необходимо заблокировать и нажмите на неё левой кнопкой мыши.



5. Когда в строке с комбинацией отобразится сообщение "Новая комбинация клавиш..." нажмите клавишу "Backspace".



6. Комбинация клавиш для выключения ПК будет заблокирована.



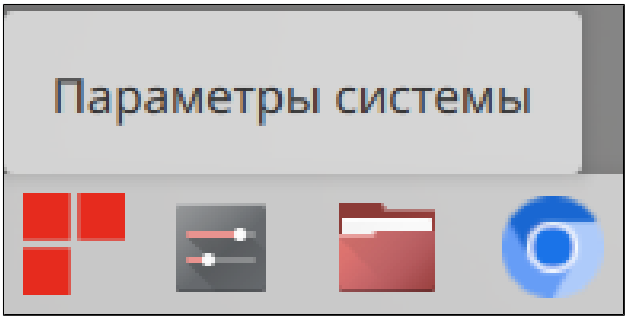
Графическая оболочка KDE Plasma

1. Создайте пользователя с ограниченными правами, у которого необходимо заблокировать сочетания клавиш.

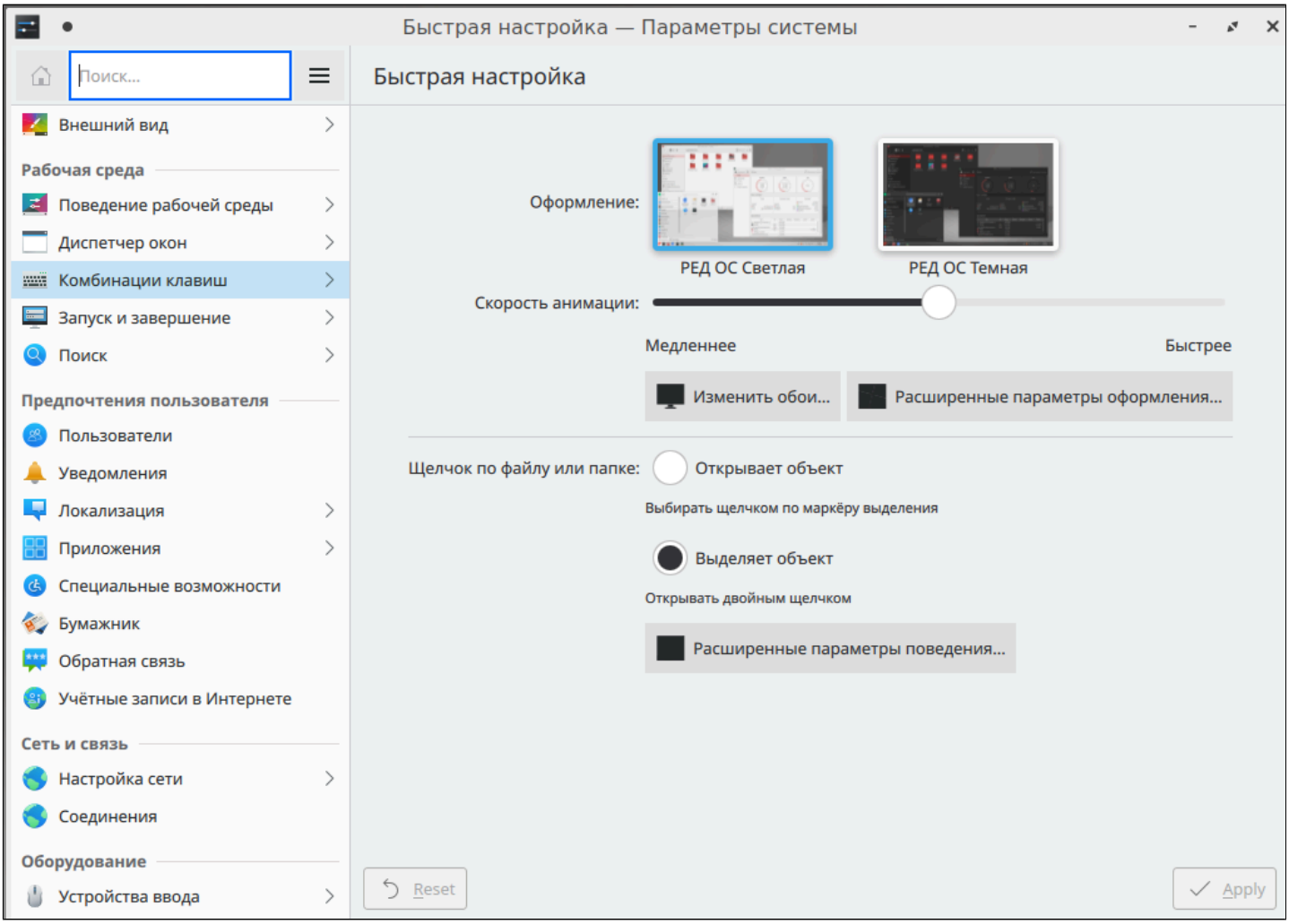
> Пошаговая инструкция приведена в разделе "Создание пользователя с ограниченными правами" документа "Администрирование. Руководство пользователя".

2. Авторизуйтесь под созданным пользователем в графической оболочке KDE и откройте "Параметры системы".

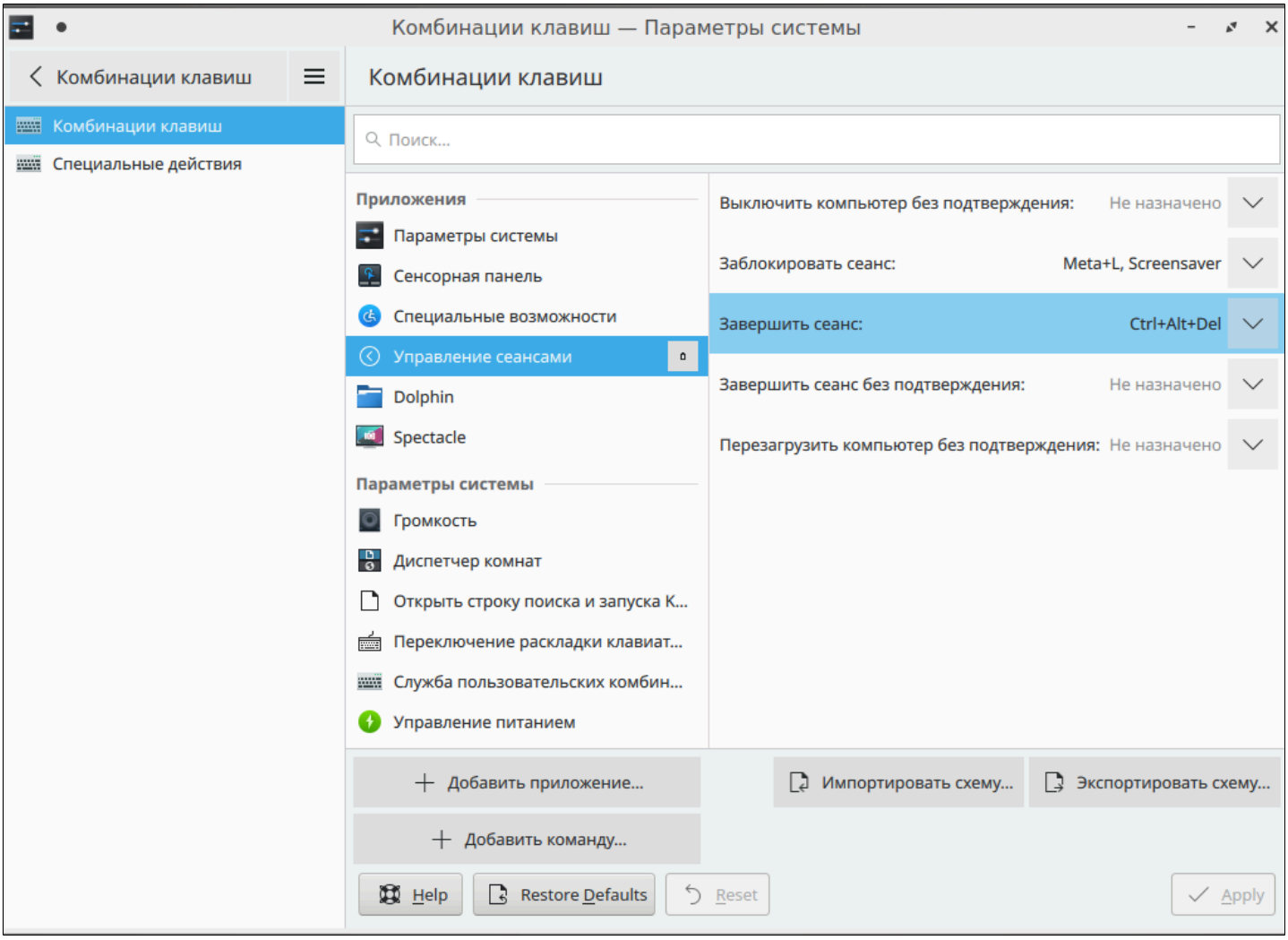
> Пошаговая инструкция по авторизации пользователя в графической оболочке KDE Plasma приведена в разделе "Отображение кнопки закрытия окна на РЕД ОС" документа "Администрирование. Руководство пользователя".



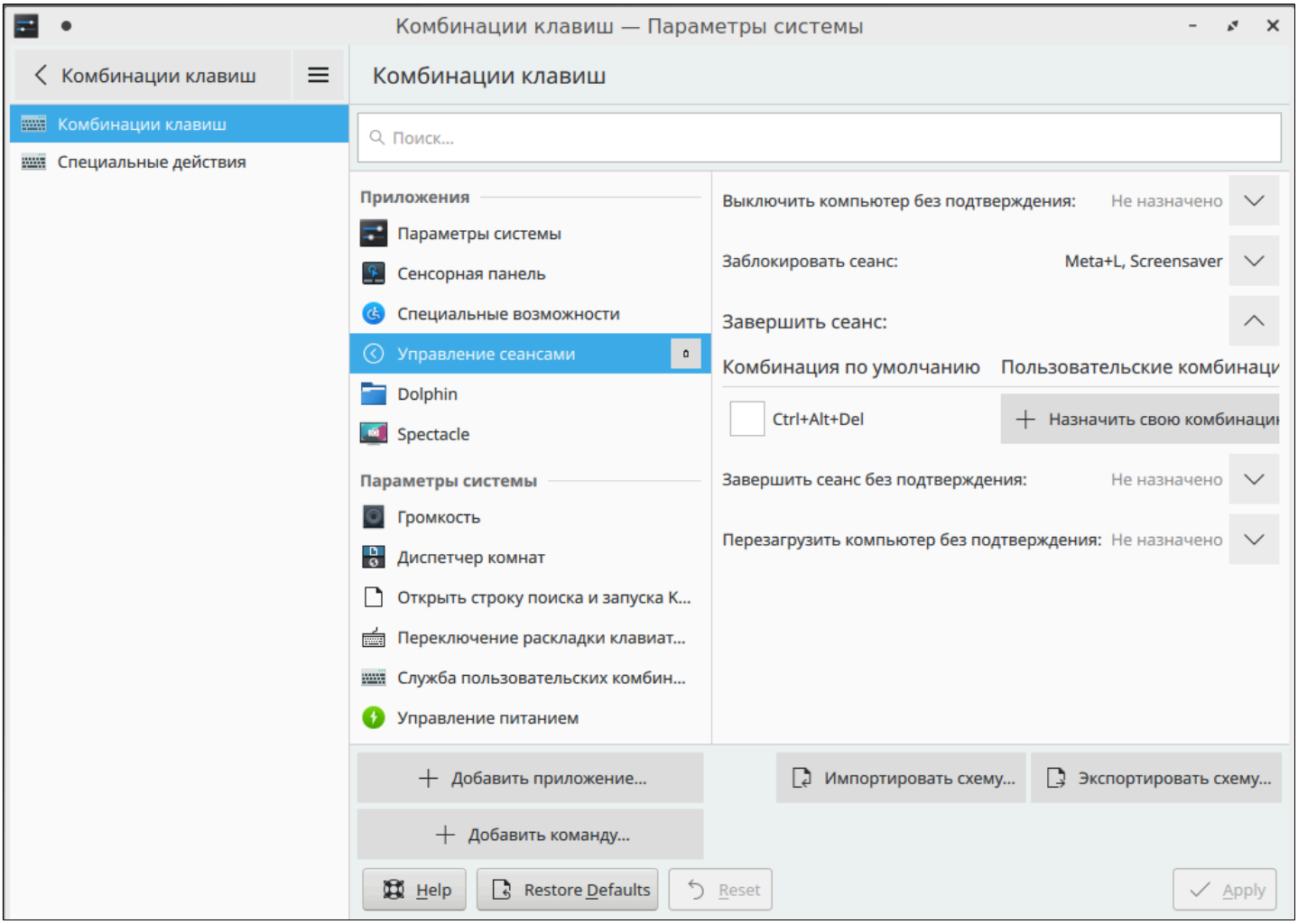
3. В разделе "Рабочая среда" выберите "Комбинации клавиш".



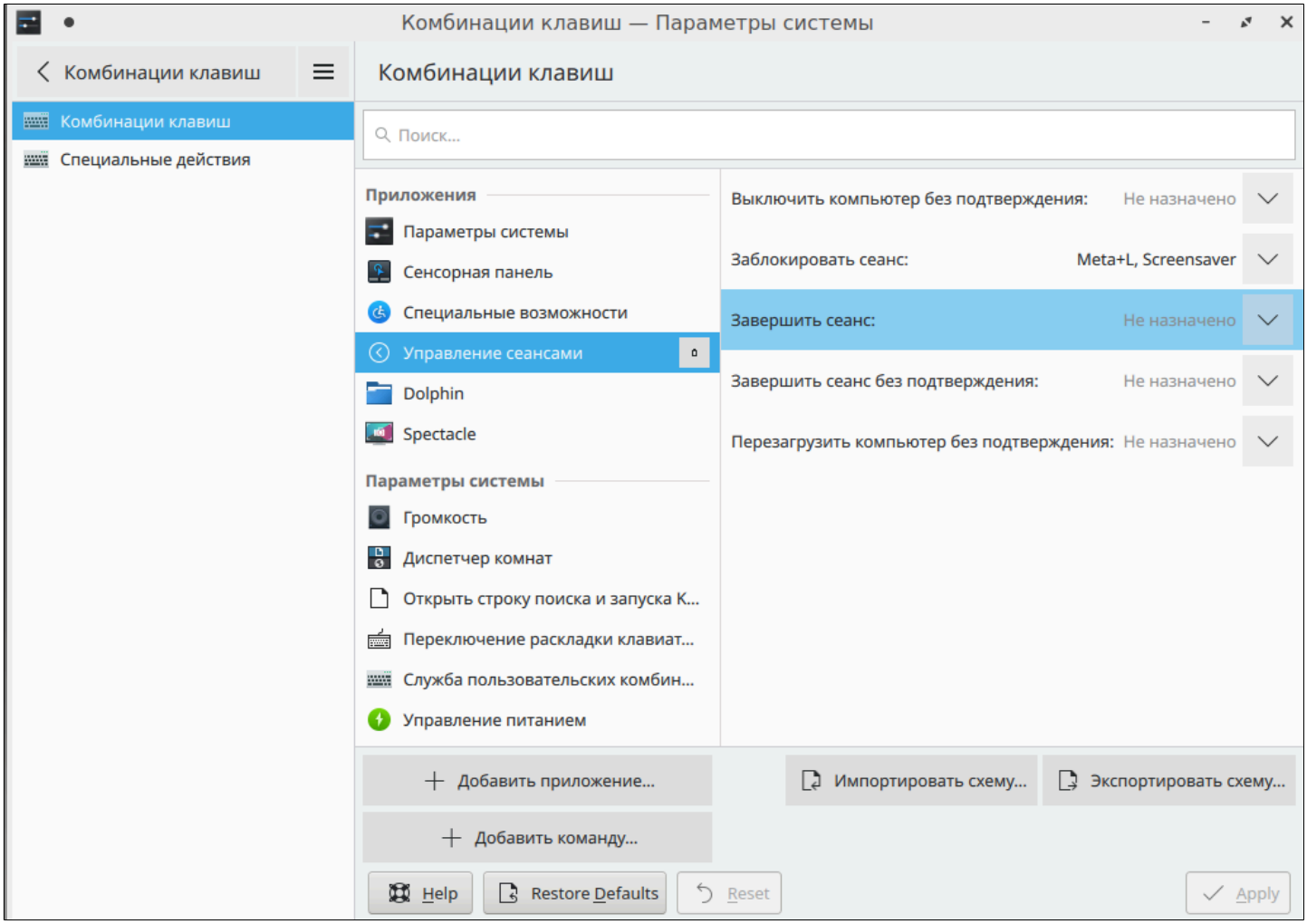
4. Выберите комбинацию клавиш клавиатуры, которую необходимо заблокировать и нажмите на неё левой кнопкой мыши.



5. В раскрывшемся меню снимите флаг с комбинации клавиш и нажмите кнопку "Apply".



6. Комбинация клавиш для завершения сеанса будет заблокирована.


Комбинации клавиш — Параметры системы
Комбинации клавиш
Комбинации клавиш
Специальные действия
Комбинации клавиш
Поиск...
Приложения
Параметры системы
Сенсорная панель
Специальные возможности
Управление сеансами
Dolphin
Spectacle
Параметры системы
Громкость
Диспетчер комнат
Открыть строку поиска и запуска K...
Переключение раскладки клавиат...
Служба пользовательских комбин...
Управление питанием
Выключить компьютер без подтверждения: Не назначено
Заблокировать сеанс: Meta+L, Screensaver
Завершить сеанс: Не назначено
Завершить сеанс без подтверждения: Не назначено
Перезагрузить компьютер без подтверждения: Не назначено
Добавить приложение...
Импортировать схему...
Экспортировать схему...
Добавить команду...
Help
Restore Defaults
Reset
Apply

1.3. Контроль целостности файлов

Компонент	Версия	Описание
Astra.HMI.IntegrityControl	2.1.1.1	Приложение для контроля целостности файлов

1.3.1. Astra.HMI.IntegrityControl

Astra.HMI.IntegrityControl – приложение для контроля целостности файлов и папок на локальных и удаленных узлах.

Контроль целостности выполняется с помощью подсистемы безопасности Astra.Security.

Astra.HMI.IntegrityControl можно запускать как отдельное приложение, либо встраивать его в прикладные проекты, разработанные в Astra.HMI.

1.3.1.1. Настройка

Перед использованием Astra.HMI.IntegrityControl выполните следующие действия:

1. Если вы планируете подключаться к удаленным узлам, обязательно объедините свой компьютер и удаленные узлы в сеть Astra.Net.

> Как организовать сеть Astra.Net описано в руководстве пользователя на Astra.Domain.

2. На тех компьютерах, где будет выполняться контроль целостности, в Astra.Security:

- Включите режим контроля целостности.
- Укажите контролируемые файлы и папки.
- Если нужно, включите периодическую автоматическую проверку контроля целостности.

1.3.1.1.1. Настройка системы безопасности Astra.Security

По умолчанию контроль целостности не выполняется.

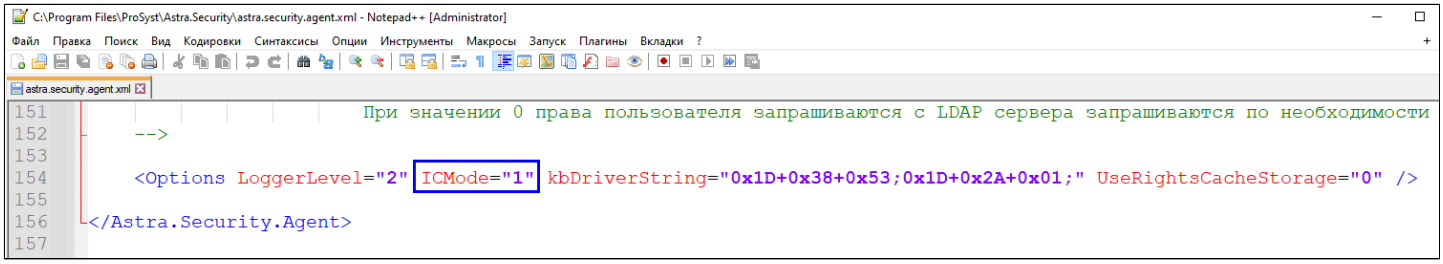
Чтобы выполнять контроль целостности выполните следующие действия:

1. Перейдите к файлу конфигурации astra.security.agent.xml, расположенному в папке:

C:\Program Files\AstraRegul\AstraSecurity

2.В конфигурационном файле astra.security.agent.xml назначьте атрибуту **ICMode** тега **<Options>** значение:

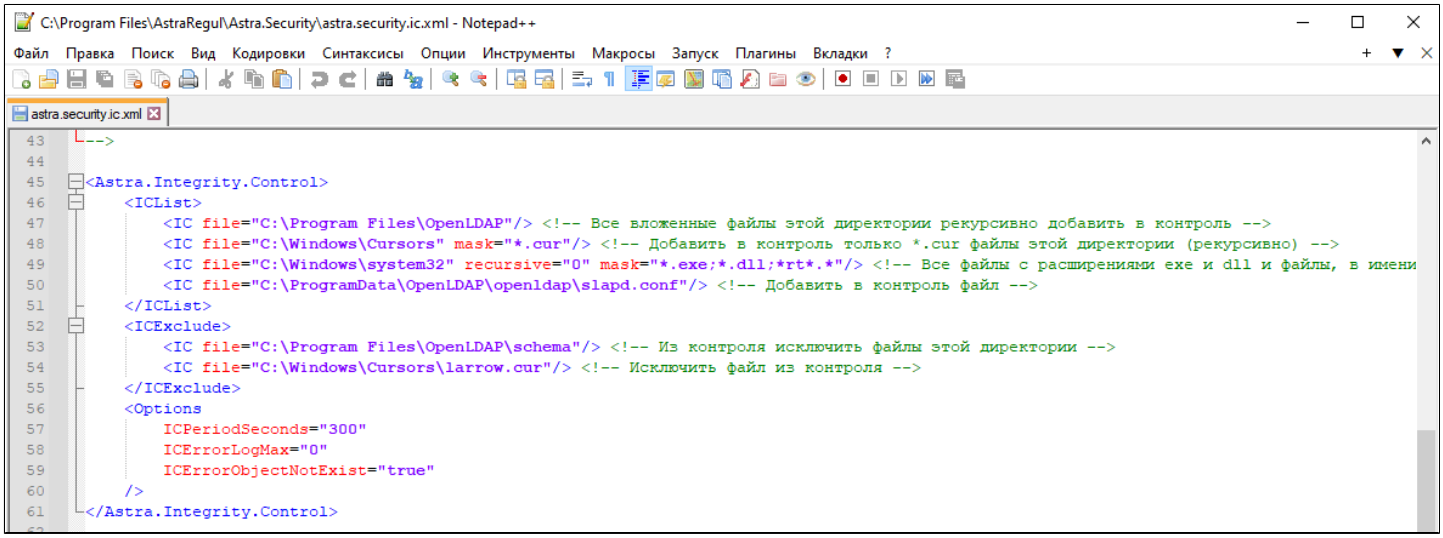
- 1 – для включения контроля целостности;
- 0 – для отключения контроля целостности.



3. Перейдите к файлу конфигурации astra.security.ic.xml, расположенному в папке:

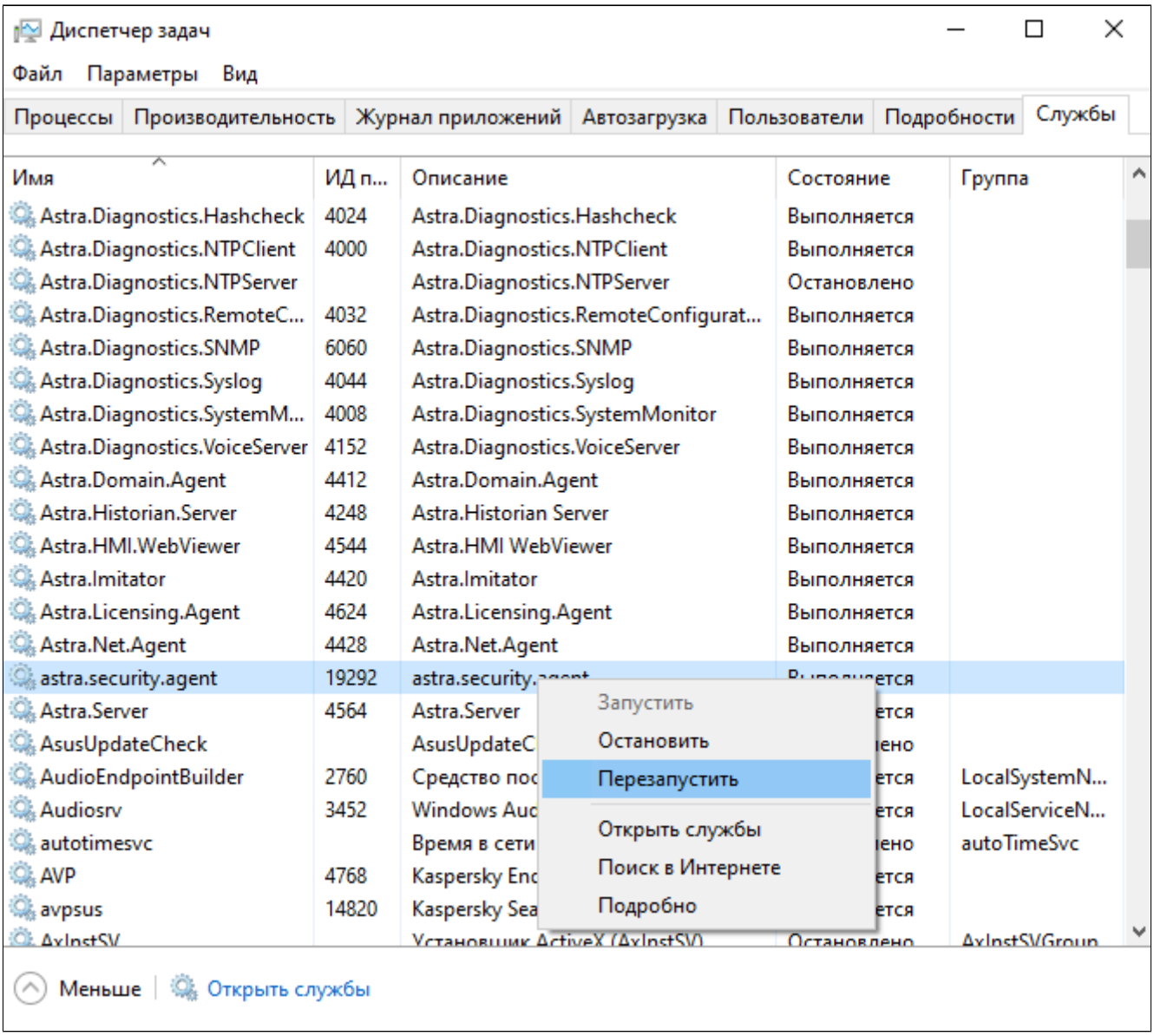
C:\Program Files\AstraRegul\AstraSecurity

4. Назначьте атрибуту **IC file** тега **<ICList>** значение, являющееся полным путем к контролируемой папке.



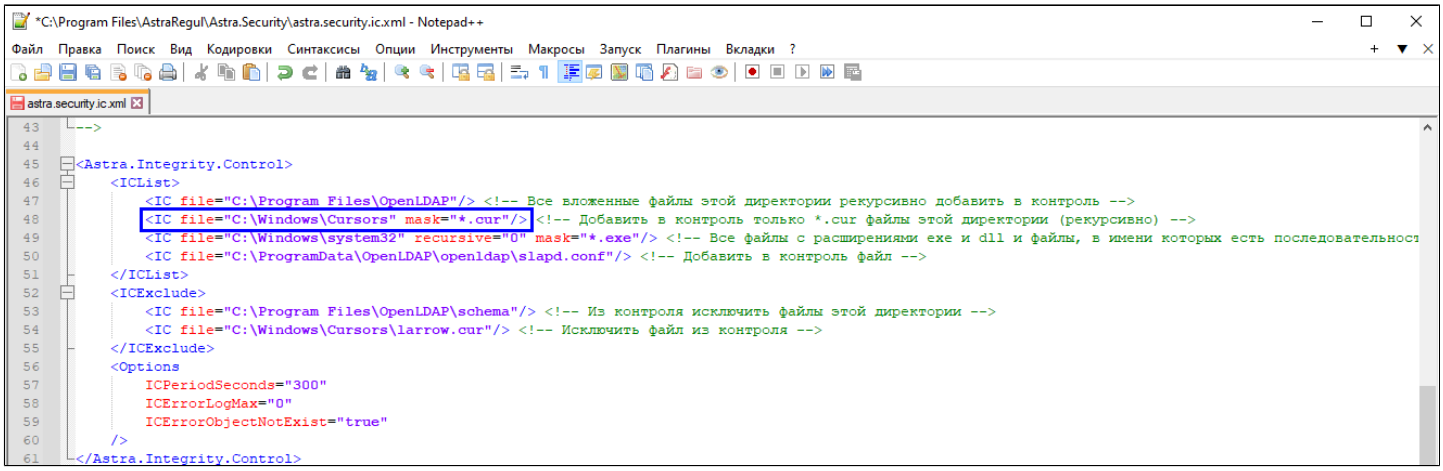
5. Назначьте атрибуту **ICPeriodSeconds** тега **<Options>** длительность интервала проверок в секундах. Если необходимо, чтобы проверка проводилась только по запросу пользователя, удалите тег **<Options>** из файла.

6. Перезагрузите службу **astra.security.agent**

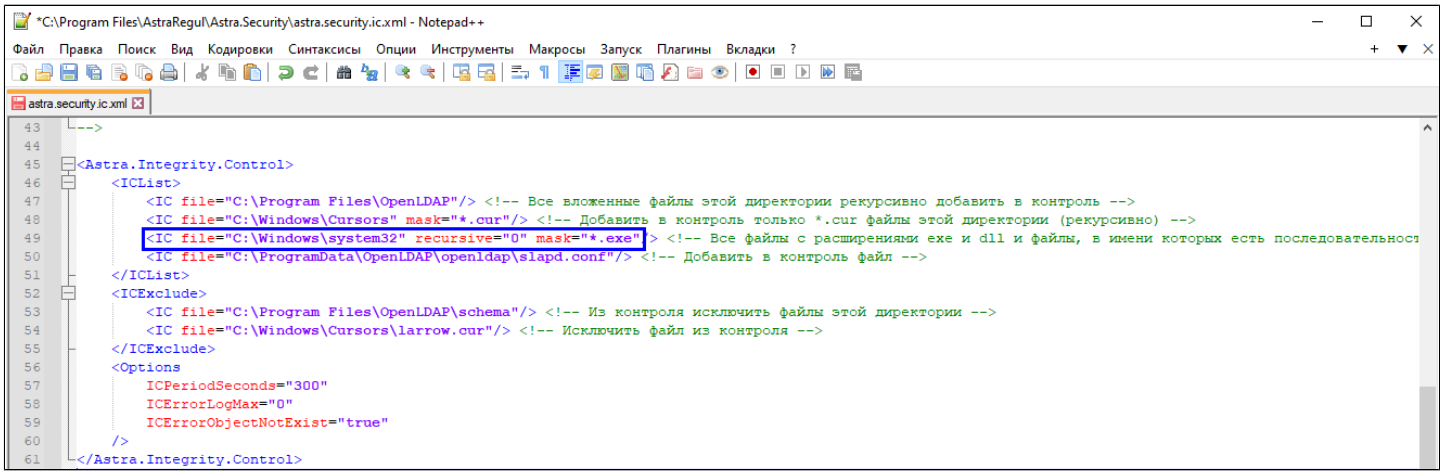


Настройка списка контролируемых файлов

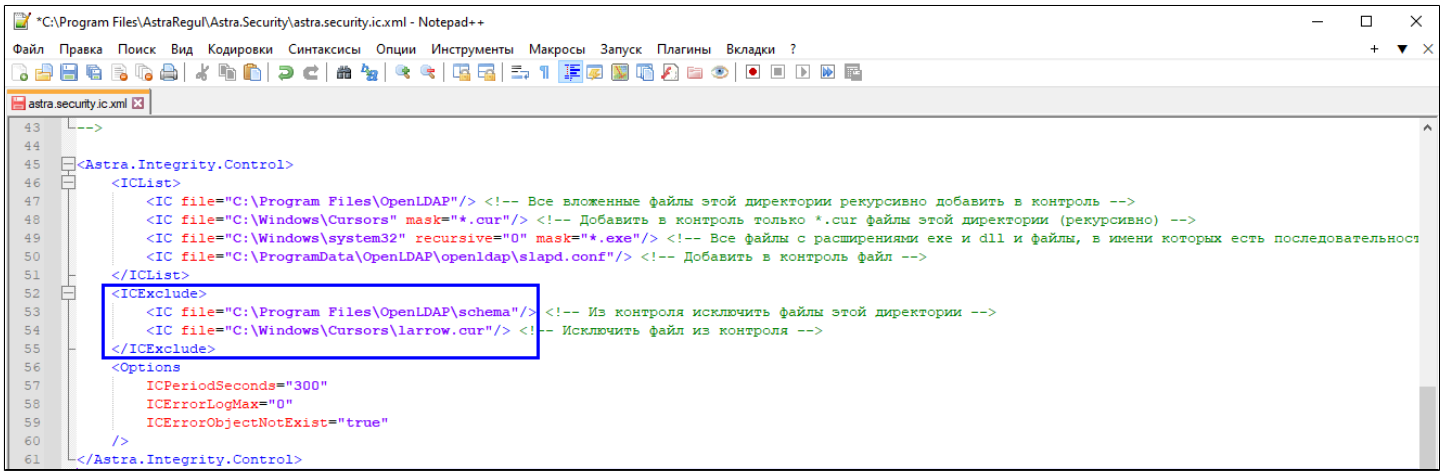
Можно фильтровать, какие именно файлы следует контролировать, с помощью маски. Для этого укажите значение атрибута **mask** тега **<IC file>**. Таким образом можно контролировать, например, только файлы с определенным расширением.



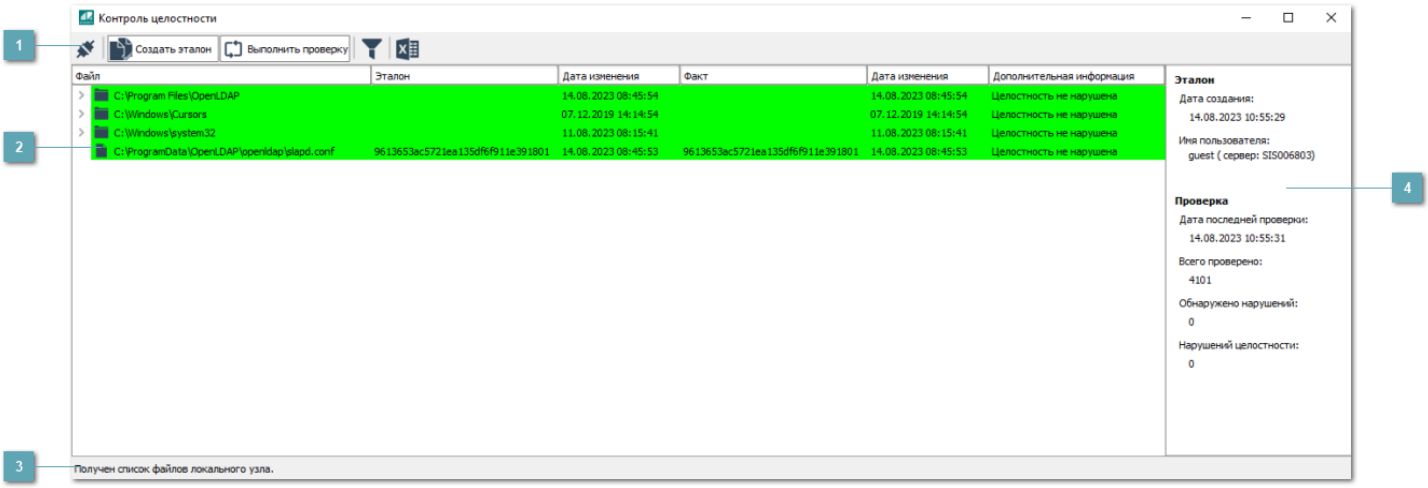
Можно исключить из контроля целостности все папки, вложенные в контролируемую папку, и их содержимое. Чтобы контроль целостности не выполнялся для вложенных папок и их содержимого, укажите значение "0" для атрибута **recursive** тега **<IC file>**.



Можно исключить из контроля целостности конкретный файл или папку, вложенную в контролируемую папку, и ее содержимое. Для этого укажите полный путь к исключаемым файлам и папкам здесь же в качестве значения атрибута **IC file** тега **<ICExclude>**.



1.3.1.2. Интерфейс



1 Панель инструментов

Область, содержащая функциональные кнопки.

2 Список контролируемых файлов

При подключении к узлу в данной области будет отображен список контролируемых файлов.

3 Строка состояния

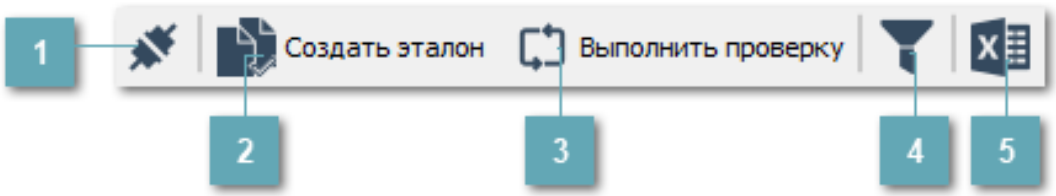
Содержит результат получения списка контролируемых файлов.

4 Информационное окно

Содержит информацию о контролируемом файле:

- эталон, по которому проводится контроль целостности;
- информация о последней проведенной проверке.

1.3.1.2.1. Панель инструментов



1 Выполнить подключение к узлу

Подключение к локальному узлу или любому удаленному узлу, входящему вместе с вашим локальным узлом в сеть Astra.Net.

2 Создать эталон

Создание эталонного файла на основе текущего состояния файла.

3 Выполнить проверку

Выполнение проверки целостности файлов.

4 Показать только файлы с нарушением целостности

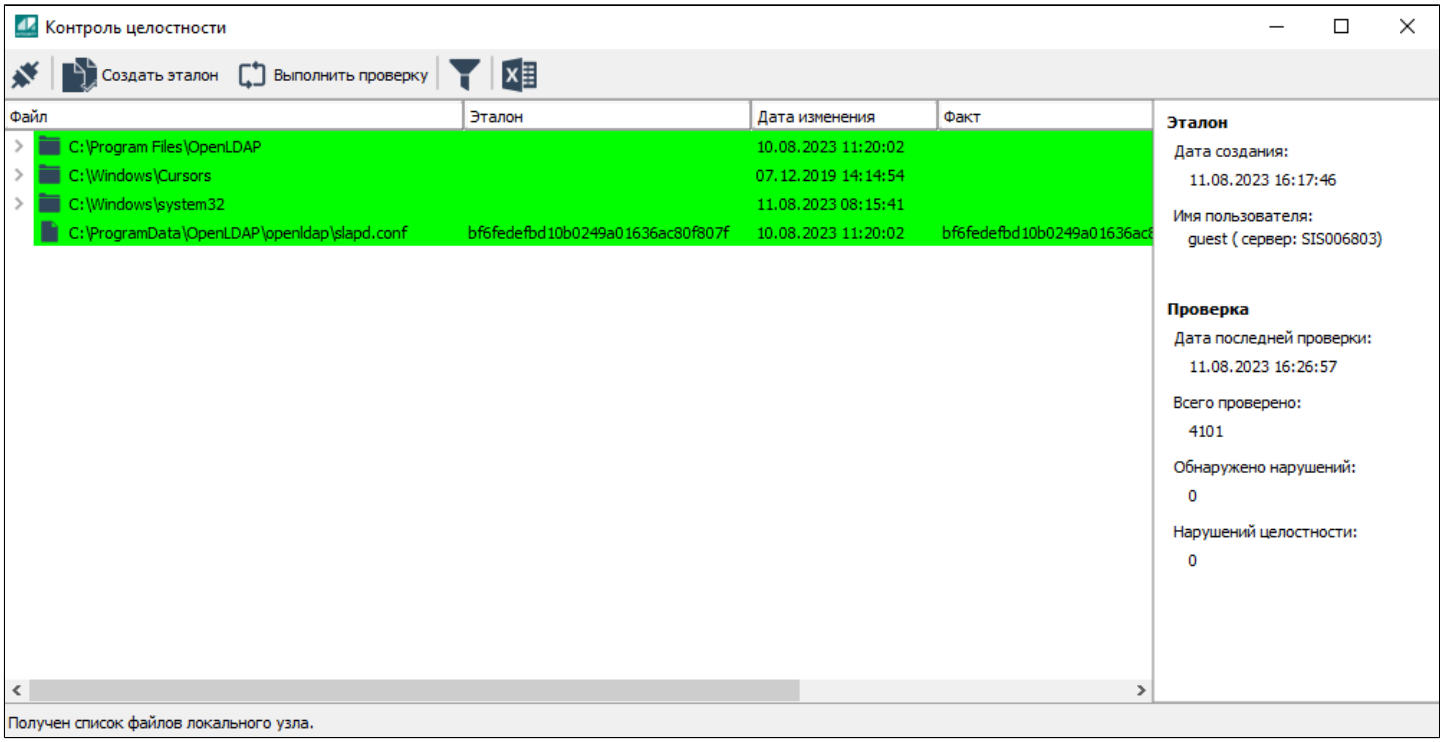
Включение фильтра отображения файлов. При включении фильтрации в списке контролируемых файлов останутся только файлы с нарушением целостности.

5 Экспорт в файл

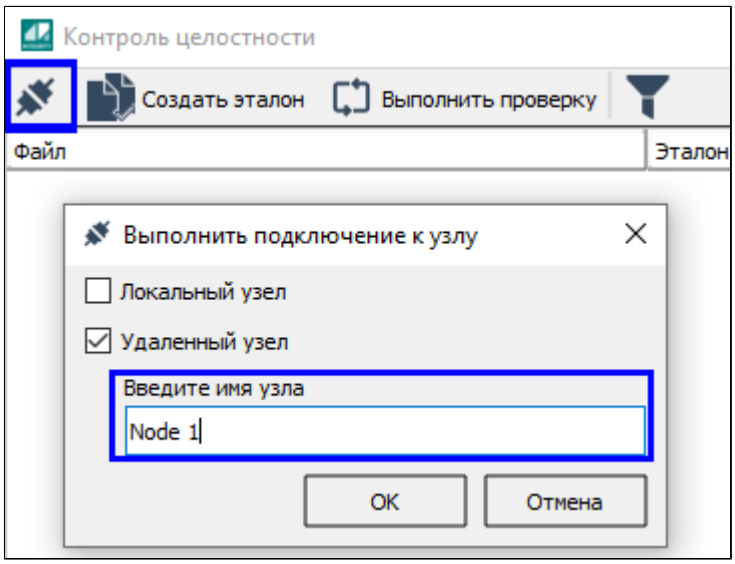
Экспорт списка контролируемых файлов.

1.3.1.2.1.1. Подключение к узлу

По умолчанию приложение подключено к вашему локальному компьютеру, на котором и выполняется контроль целостности.



Чтобы подключиться к любому удаленному узлу (входящему вместе с вашим локальным узлом в сеть Astra.Net), нажмите кнопку "Выполнить подключение к узлу" на панели инструментов и введите имя узла в открывшемся окне.

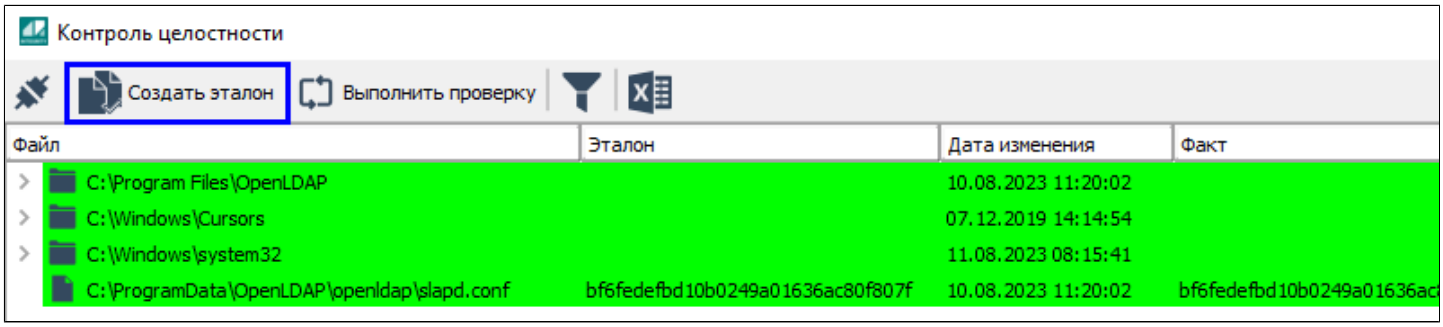


1.3.1.2.1.2. Создание эталонного файла

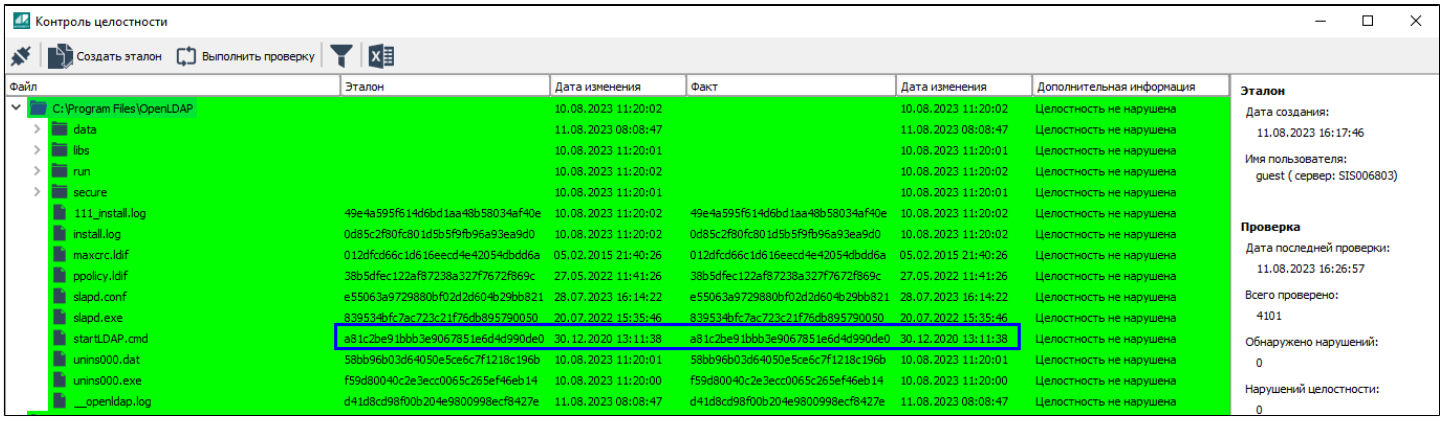
Под эталоном понимается срез текущего состояния (контрольных сумм) по каждому файлу, с которым будет сравниваться состояние файлов при следующей проверке.

Для того, чтобы создать эталон, необходимо привести файлы в нужное состояние, а затем создать эталон на основе текущего состояния файлов.

Чтобы создать эталон на основе текущего файла, нажмите кнопку "**Создать эталон**" на панели инструментов.



Для каждого файла вы можете увидеть эталонную контрольную сумму и дату изменения эталона.

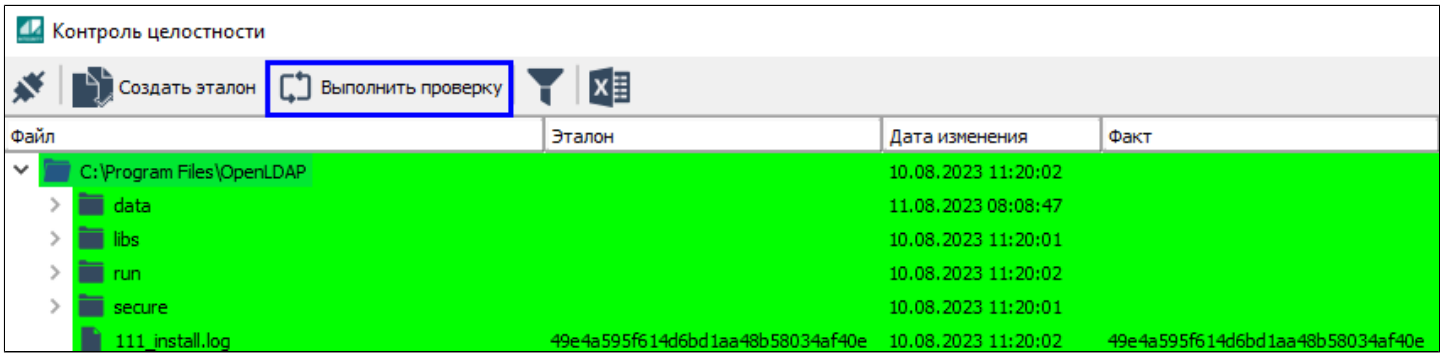


1.3.1.2.1.3. Проверка целостности

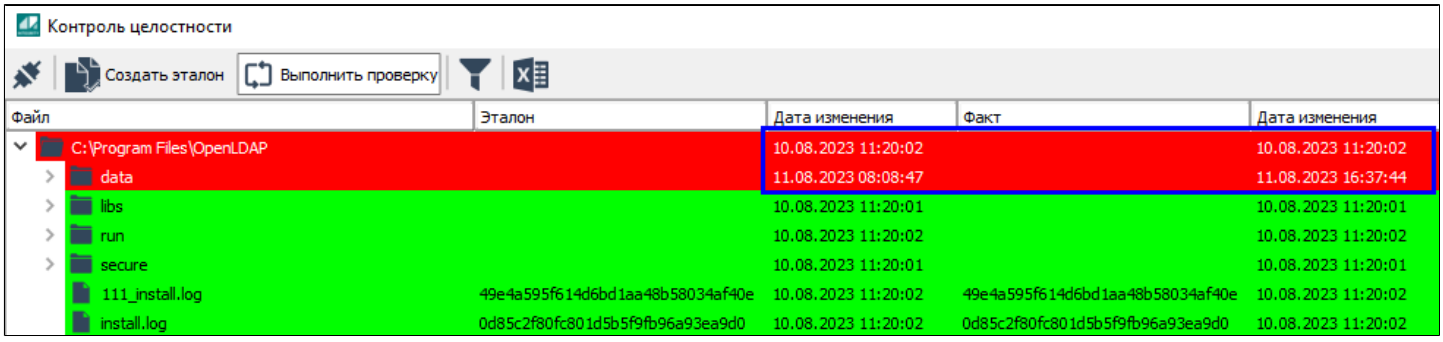
При проверке целостности проверяется соответствие контрольных сумм файлов и эталонных контрольных сумм. Список контролируемых файлов формируется заранее в конфигурационном файле службы Astra.Security.Agent.

Проверка может выполняться автоматически с заданным периодом, если это указано при настройке службы Astra.Security.Agent.

Чтобы вручную запустить проверку целостности на подключенном узле, нажмите кнопку "**Выполнить проверку**" на панели инструментов.

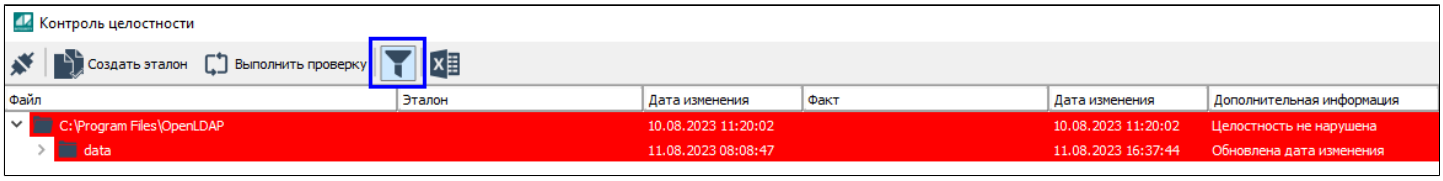


В результате проверки по каждому файлу вы можете отследить был ли изменен файл, и когда он был изменен.



1.3.1.2.1.4. Фильтр

Чтобы отобразить только файлы с изменениями, нажмите кнопку "Показать файлы с нарушением целостности" на панели инструментов.

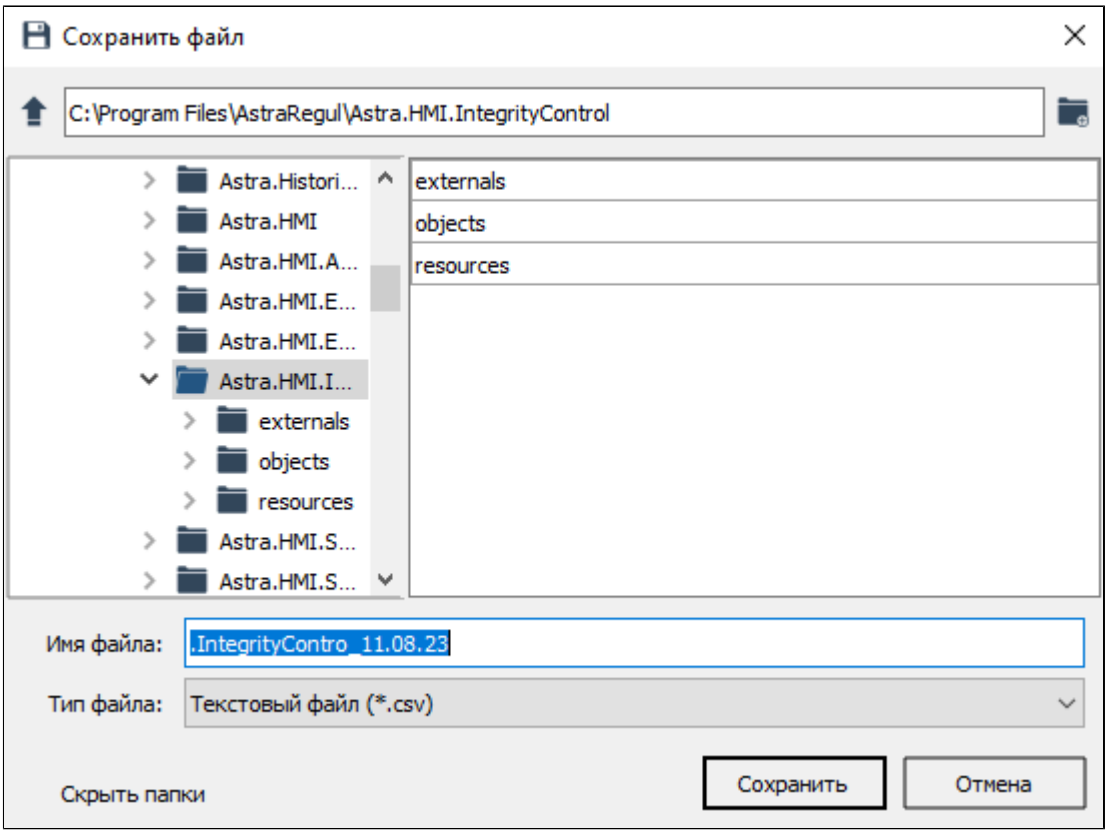


Чтобы снова отобразить все файлы, повторно нажмите кнопку "Показать файлы с нарушением целостности".

1.3.1.2.1.5. Экспорт в файл

Для того, чтобы экспортировать список контролируемых файлов в файл формата *.csv и *.xlsx нажмите на панели инструментов кнопку "Экспорт в файл".

Откроется окно с настройками параметров экспорта. Укажите путь, задайте название файла и выберите формат данных, затем нажмите кнопку "Сохранить".



Подключение внешнего модуля Astra.HMI.IntegrityControl

Чтобы подключить Astra.HMI.IntegrityControl как внешний модуль, выполните следующие действия:

1. Создайте в папке своего проекта папку **externals**, в которой нужно размещать файлы всех подключаемых внешних модулей.

2. Перейдите к папке, в которую устанавливаются все приложения Astra.HMI:

- **ОС Windows**:

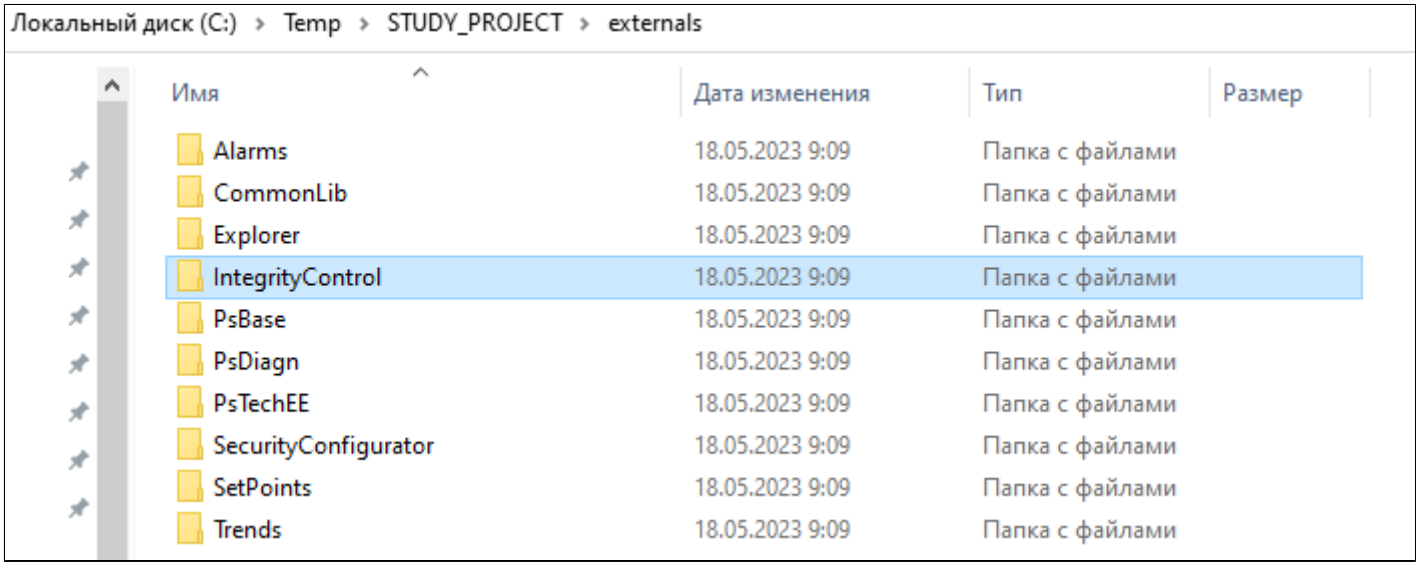
C:\Program Files\AstraRegul\Astra.HMI.Extensions

- **ОС Linux**:

/opt/AstraRegul/Astra.HMI.Extensions

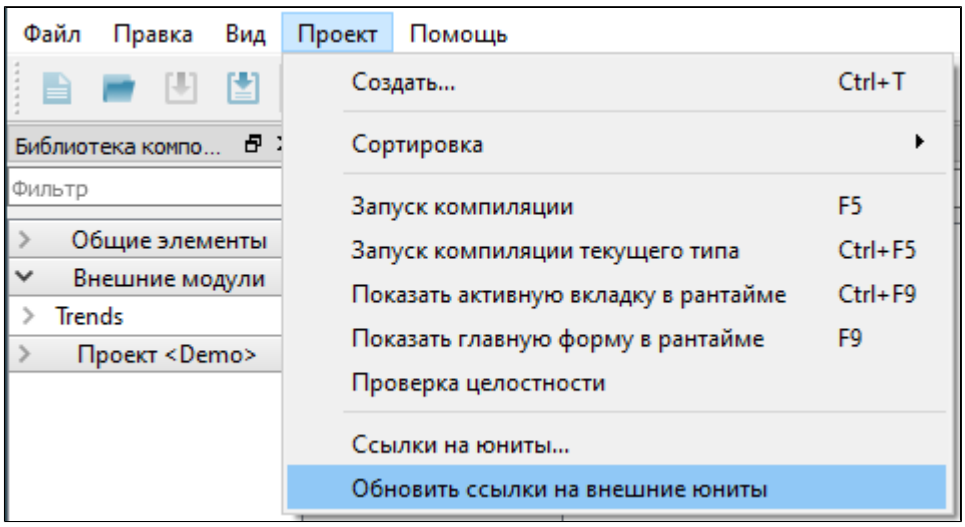
В папке уже должна быть папка IntegrityControl, появившаяся после установки Astra.HMI.IntegrityControl.

3. Скопируйте эту папку IntegrityControl в созданную вами папку externals.

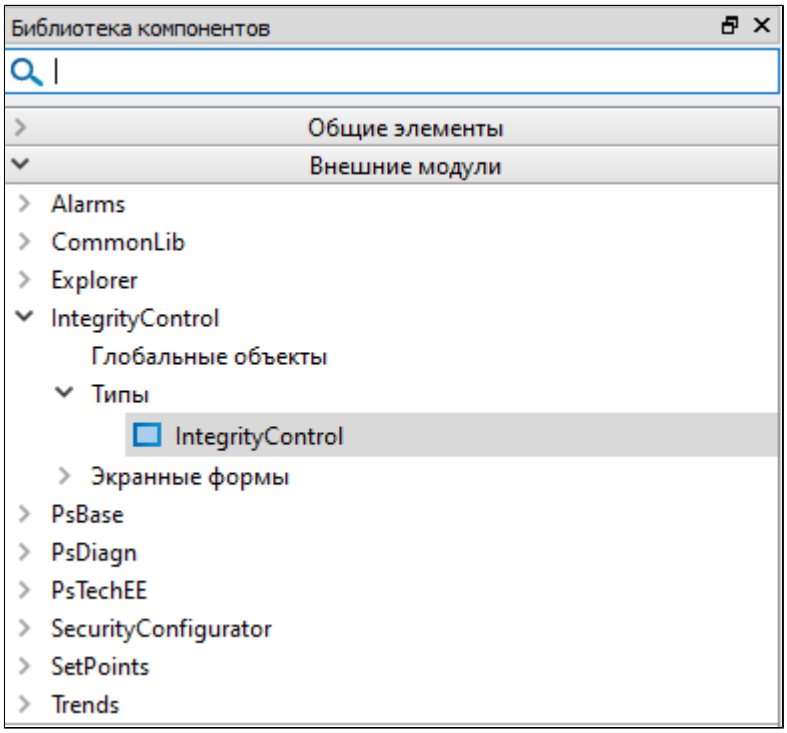


4. Откройте свой проект в дизайнере Astra.HMI.

5. Перейдите в меню Проект и выберите команду "Обновить ссылки на внешние юниты".



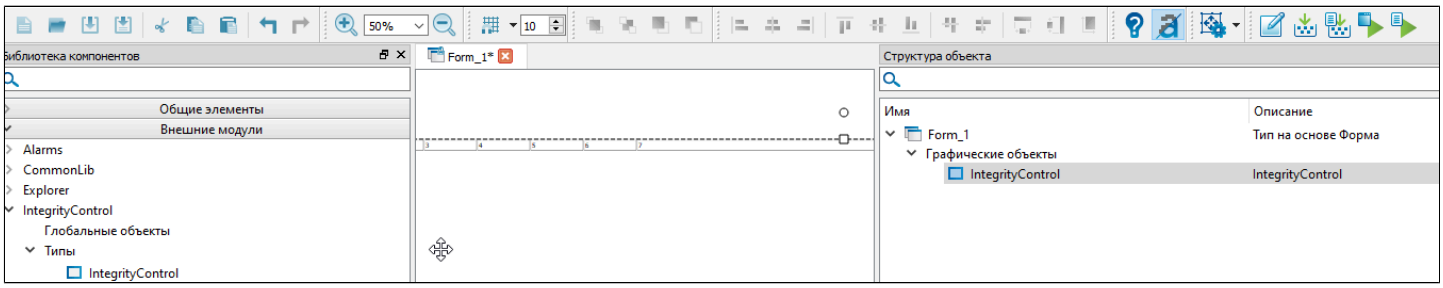
Так вы обновите список внешних модулей своего проекта и новый модуль **IntegrityControl** появится в библиотеке компонентов.



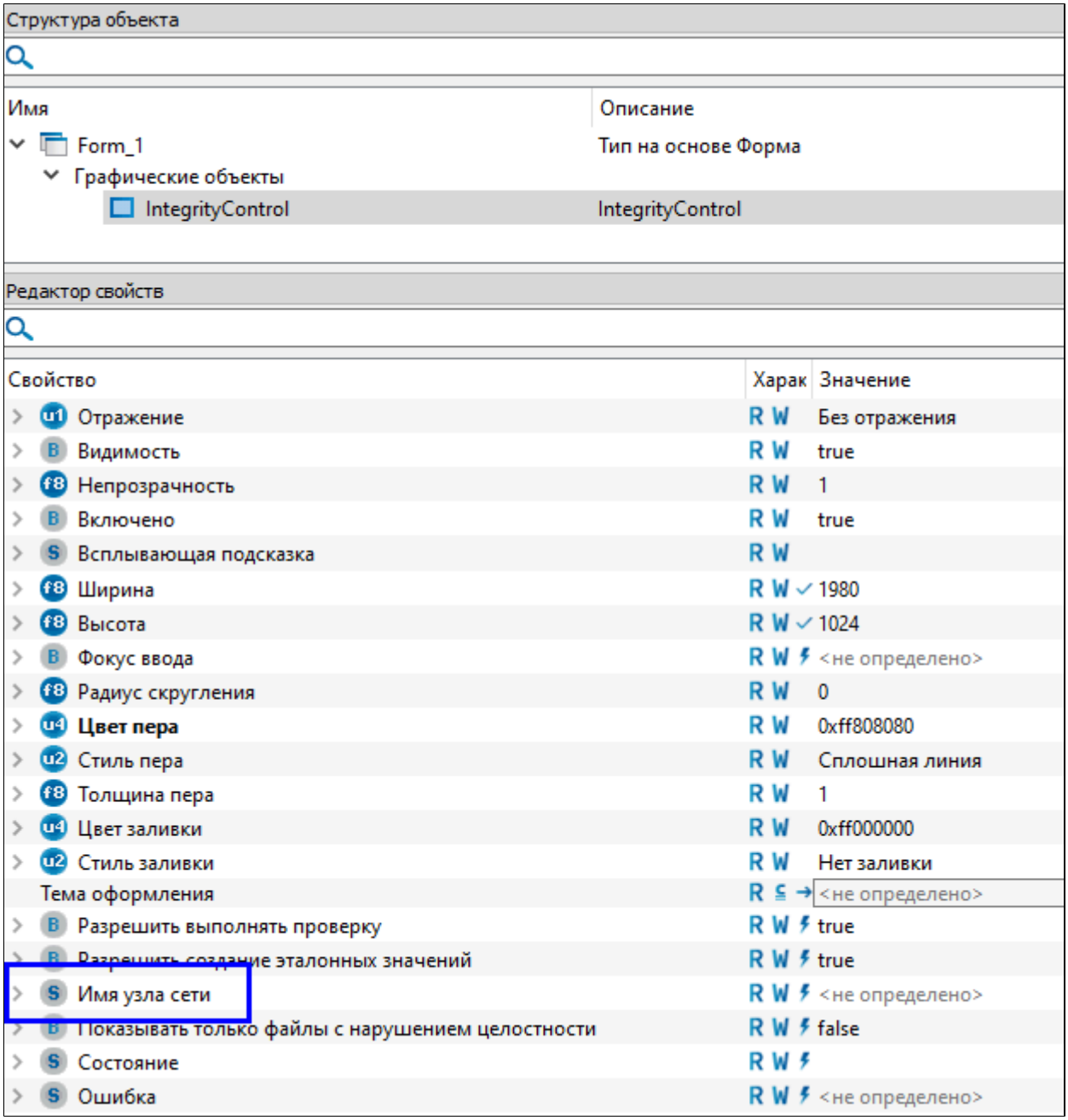
1.3.1.3. Встраивание в проект

Чтобы встроить Astra.HMI.IntegrityControl в проект и начать работу с приложением:

1. Подключите Astra.HMI.IntegrityControl к проекту как внешний модуль.
2. Добавьте экземпляр типа IntegrityControl в проект.

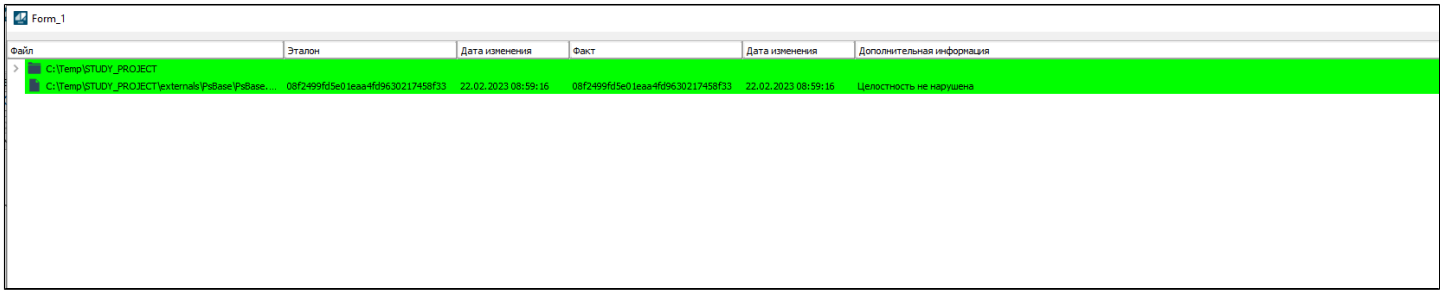


3. Укажите для экземпляра типа IntegrityControl в свойстве **NodeName** (Имя узла сети) узел сети Astra.Net, на котором выполняется контроль целостности.



Если узел локальный, его имя указывать не обязательно.

В интерфейсе встроенного экземпляра типа IntegrityControl вы увидите только дерево контролируемых файлов с указанного вами узла и результаты проверок по каждому файлу и папке. Если в Astra.Security включен периодический контроль целостности, вы также увидите как меняется окраска измененных файлов и папок.



Чтобы добавить дополнительные кнопки, панель со статистикой и т.д., используйте API, которое предоставляет экземпляр типа IntegrityControl.

1.3.1.3.1. API

- Свойства
- Команды

1.3.1.3.1.1. Свойства

Свойство	Описание
NodeName	Имя узла Astra.Net, которое указано для узла в файле конфигурации Astra.Net
AllowCheck	Разрешить выполнить проверку
AllowCreateEtalon	Разрешить создавать эталонные значения
ShowOnlyChanged	Включить фильтрацию элементов дерева и отображать только файлы с нарушением целостности
Status	Описание текущей операции
Error	Описание ошибки, которая произошла при выполнении последней операции

1.3.1.3.1.1.1. NodeName

Имя узла Astra.Net, которое указано для узла в файле конфигурации Astra.Net. Можно не указывать значение, если узел локальный.

string NodeName

1.3.1.3.1.1.2. AllowCheck

Разрешает выполнять проверку целостности.

bool AllowCheck

Значение

Значение	Описание
false	Выполнение проверки целостности запрещено
true	Выполнение проверки целостности разрешено

1.3.1.3.1.1.3. AllowCreateEtalon

Разрешает создавать эталонные значения.

bool AllowCreateEtalon

Значение

Значение	Описание
false	Создание эталонных значений запрещено
true	Создание эталонных значений разрешено

1.3.1.3.1.1.4. ShowOnlyChanged

Включает фильтрацию элементов дерева и отображения только файлов с нарушением целостности.

bool ShowOnlyChanged

Значение

Значение	Описание
false	Фильтрация отключена
true	Фильтрация включена

1.3.1.3.1.1.5. Status

Отображает описание текущей операции.

string Status

1.3.1.3.1.1.6. Error

Отображает описание ошибки, которая произошла при выполнении последней операции.

string Error

1.3.1.3.1.2. Команды

Команда	Описание
Check	Запускает проверку контролируемых файлов
CreateEtalon	Создает эталон на узле

1.3.1.3.1.2.1. Check

Запускает проверку контролируемых файлов на узле, указанном в свойстве NodeName.

void Check()

Примеры

```
//Запустить проверку целостности контролируемых файлов на выбранном узле
IntegrityControl.Check();
```

1.3.1.3.1.2.2. CreateEtalon

Создает эталон на узле, указанном в свойстве NodeName.

void CreateEtalon()

Примеры

```
//Создать эталон контролируемых файлов на выбранном узле
IntegrityControl.CreateEtalon();
```

1.4. Системы резервного копирования

Потерять данные можно из-за вирусов и хакерских атак, вследствие ошибок пользователей и администраторов, поломок оборудования, форс-мажорных обстоятельств (краж, пожаров, стихийных бедствий).

На сегодняшний день разработано множество способов, программ и устройств, предназначенных для защиты данных от потери, но в основе их лежит общий принцип – создание копий данных.

Необходимо делать регулярно резервные копии ("бэкапы") критически важных данных.

Система резервного копирования — совокупность программного и аппаратного обеспечения, выполняющее задачу создания копии данных на носителе, предназначенном для восстановления информации в оригинальном месте их расположения в случае их повреждения или разрушения.

Основные функции

› периодическое автоматическое копирование системных и пользовательских данных на резервные носители или в облако;
› оперативного восстановления данных.

Резервировать можно как конкретные файлы и папки, так и образы систем и серверов, содержимое баз данных и приложений.

Архитектура

Централизованная система резервного копирования имеет многоуровневую архитектуру, в которую входят:

- сервер управления резервным копированием, способный также совмещать функции сервера копирования данных;
- один или несколько серверов копирования данных, к которым подключены устройства резервного копирования;
- компьютеры-клиенты с установленными на них программами-агентами резервного копирования;
- консоль администратора системы резервного копирования.

Администратор системы ведет список компьютеров-клиентов резервного копирования, устройств записи и носителей хранения резервных данных, а также составляет расписание резервного копирования. Вся эта информация содержится в специальной базе, которая хранится на сервере управления резервным копированием.

В соответствии с расписанием или по команде оператора сервер управления дает команду программе-агенту, установленной на компьютере-клиенте, начать резервное копирование данных в соответствии с выбранной политикой. Программа-агент собирает и передает данные, подлежащие резервированию, на сервер копирования, указанный ей сервером управления.

Сервер копирования сохраняет полученные данные на подключенное к нему устройство хранения данных. Информация о процессе (какие файлы копировались, на какие носители осуществлялось копирование и т. п.) сохраняется в базе сервера управления. Эта информация позволяет найти местоположение сохраненных данных при необходимости их восстановления на компьютере-клиенте.

Чтобы система резервного копирования сохраняла непротиворечивые данные компьютера-клиента, они не должны подвергаться изменениям в процессе их сбора и копирования программой-агентом. Для этого приложения компьютера-клиента должны завершить все транзакции, сохранить содержимое кэш-памяти на диск и приостановить свою работу. Этот процесс инициируется по команде программы-агента, которая передается приложениям компьютера-клиента.

Поскольку система резервного копирования предназначена для восстановления данных после сбоя или аварии, созданные резервные копии необходимо проверять на предмет целостности и работоспособности.

Системы резервного копирования

Название	Реестр российского ПО	Сертификат ФСТЭК	Кроссплатформенность
Кибер Бэкап (Acronis)	Да	Да	Да
RuBackup	Да	Нет	Да
Handy Backup	Да	Нет	Да

Для применения в ПТК AstraRegul рекомендуется к использованию Кибер Бэкап.

1.4.1. Методы резервного копирования

Полное резервирование (Full backup) — создание резервного архива всех системных файлов, обычно включающего состояние системы, реестр и другую информацию, необходимую для полного восстановления рабочих станций. То есть резервируются не только файлы, но и вся информация, необходимая для работы системы.

При полном резервном копировании заданный набор файлов полностью записывается на носитель. Этот метод самый надёжный. Восстановление информации при полном копировании осуществляется наиболее быстро, так как для этого достаточно только одного записанного образа.

Инкрементальное резервирование (Incremental backup) — создание резервного архива из всех файлов, которые были модифицированы после предыдущего полного или добавочного резервирования.

Инкрементальный метод представляет собой поэтапный способ записи информации. Первая запись на ленту является полной копией. При последующих записях переписываются только те файлы, которые были изменены со времени предыдущей записи. По истечении заданного времени цикл повторяется снова. Данный метод копирования является самым быстрым.

Восстановление информации при инкрементальном копировании – самое длительное: информацию необходимо сначала восстановить с полной копии, а затем последовательно со всех последующих. Тем не менее, это самый популярный метод резервного копирования у системных администраторов, поскольку восстановление информации процедура достаточно редкая в нормально работающей системе.

Дифференциальное резервирование (Differential backup) — создание резервного архива из всех файлов, которые были изменены после предыдущего полного резервирования.

По времени резервного копирования этот метод занимает больше времени, чем при инкрементальном копировании. Однако для восстановления данных достаточно всего двух копий – последней полной и последней дифференциальной копии.

Выборочное резервирование (Selective backup) — создание резервного архива только из отобранных файлов.

Независимо от применяемого метода резервного копирования записываемая или восстанавливаемая информация может быть пропущена через фильтры для отбора лишь нужных файлов.

1.4.2. Требования к системам резервного копирования

Требования для внедрения системы резервного копирования должны содержать следующую информацию:

- Подробное описание клиентской инфраструктуры для резервного копирования: вид (файловые системы, приложения, базы данных), тип (физическая / виртуальная / облачная), объем данных, версия ПО.
- Значения время восстановления (RTO) и точка восстановления (RPO) для каждого объекта защиты (файл/диск/приложение/база данных/операционная система).
- План резервного копирования и восстановления.
- Функциональные требования к системе резервного копирования
- Требования к хранению резервных копий: количество РК и период хранения, способ хранения (диски, ленты, в облаке), уровень надежности (шифрование, защита от изменений, политика доступа).
- Аппаратные и системные требования.
- Описание сетевой архитектуры и каналов передачи данных.
- Требования к отказоустойчивости сервера резервного копирования и хранилища резервных копий.
- Требования к предоставляемой технической документации по управлению системой (руководства / мануалы) и условиям предоставления технической поддержки/сопровождению.

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

1. Безагентное резервное копирование виртуальных машин (без установки отдельного агента на каждую виртуальную машину).
2. Репликация на уровне виртуальных машин или дисков.
3. Создание моментальных снимков (Snapshot).
4. Поддержка различных каналов и протоколов передачи данных: подключение и передача данных в сетях SAN и NAS, копирование по протоколу NDMP, Off-host backup.
5. Хранение резервных копий:
   - локальные или сетевые устройства хранения;
   - дисковое или облачное/объектное хранилище;
   - объединение нескольких устройств хранения в один пул;
   - управление сроком жизни резервных копий;
   - репликация и многоуровневое хранение резервных копий;
   - дедупликация данных;
   - шифрование резервных копий;
   - проверка целостности бэкапа/тестирование на возможность восстановления (песочница);
   - поддержка функций неизменяемых хранилищ.

6. Гранулярное/выборочное восстановление приложений и баз данных.
7. Полное, дифференциальное, инкрементное и синтетическое резервное копирование.
8. Блочное и файловое резервное копирование.
9. Многопоточное резервное копирование.
10. Поддержка технологии Changed Block Tracking (CBT) и Microsoft Volume Shadow Copy Service (VSS).
11. Восстановление на «голое» железо или на оборудование, отличное от исходного (Bare metal recovery).
12. Автоматическое отслеживание и распределение нагрузки между несколькими заданиями по резервному копированию.
13. Возможность составления гибкого расписания для проведения резервного копирования.
14. Настройка приоритетов заданий резервного копирования.

15. Возобновление выполнения задания резервного копирования данных в случаи сбоя.
16. Администрирование по ролям для распределения прав доступа к системе.
17. Функции мониторинга, оповещения и создания отчетов.
18. Аварийное восстановление системы резервного копирования: создание диска аварийного восстановления с конфигурацией системы или отказоустойчивого кластера.
19. Централизованное управление резервным копированием в территориально распределенной инфраструктуре (архитектура системы).
20. Встроенные антивирусные средства.
21. Работа с RAID-массивами
22. Работа в автоматическом режиме.
23. Процедуры резервного копирования/восстановления данных должны инициализироваться как с агента резервного копирования, так и с сервера.
24. Возможность проведения резервного копирования данных файловых серверов и серверов приложений без прерывания работы приложений и пользователей.
25. Высокая скорость проведения резервного копирования и восстановления данных.
26. Полная автоматизация операций с носителями резервных копий.
27. Удобный графический интерфейс.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

1. Модульная структура, обеспечивающая постепенное наращивание функциональных возможностей.
2. Поддержка различных операционных систем, баз данных и приложений.
3. Поддержка широкого спектра архивационных устройств.

1.4.3. Кибер Бэкап

Кибер Бэкап прост в управлении, быстро развертывается и не требует специального обучения.

.

Сайт производителя: https://cyberprotect.ru/

Включен в реестр российского ПО.

Решение для резервного копирования:

- локальное;
- облачное;
- гибридное.

Функции

- Резервное копирование данных с серверов, мобильных устройств, облачных платформ и виртуальных машин.
- Восстановление отдельных файлов, приложений и баз данных.
- Резервные копии на платформе облачного хранилища.
- Консоль централизованного управления по сети.
- Быстрое инкрементное и дифференциальное резервное копирование.
- Дедупликация данных.

Получен сертификат ФСТЭК для применения ПО на объектах критически важной инфраструктуры.

Шифрование

Чтобы хранить свои архивные резервные копии, не опасаясь кражи данных, используйте шифрование.

Типы шифрования:

- 128-бит AES.
- 192-бит AES.
- 256-бит AES.