ПРОГРАММНЫЙ ПРОДУКТ
«PROFESSIONAL IDENTITY SECURITY MANAGER»
«PRISMA»

Руководство администратора

АННОТАЦИЯ

Данное Руководство содержит описание изделия «Professional Identity Security Manager» (далее – Prisma, изделие) и предназначено для Администраторов Prisma.

Руководство включает:

- описание назначения, функциональных особенностей и решаемых Prisma задач;
- описание процесса установки и настройки Prisma;
- описание действий Администраторов при обслуживании Prisma

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Область применения

Данное Руководство предназначено для внутренних пользователей.

1.2. Краткое описание возможностей

Prisma представляет собой средство защиты информации, предназначенное для решения следующих задач:

- реализация технологии единой точки доступа (Single Sign On, SSO) к информационным системам;
- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- регистрация событий безопасности (РСБ);
- обеспечение целостности Prisma и информации (ОЦЛ).

Prisma должен обеспечивать

реализацию следующих мер защиты информации в соответствии с требованиями документов «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (введены в действие приказом ФСТЭК России № 17 от 11.02.2013), «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введены в действие приказом ФСТЭК России № 21 от 18.02.2013) и «Меры защиты информации в государственных информационных системах» (утверждены директором ФСТЭК России 11.02.2014:

- Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):
  - идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1),

- идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2),
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3),
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4),
- защита обратной связи при вводе аутентификационной информации (ИАФ.5),
- идентификация и аутентификация пользователей, не являющихся работниками оператора (ИАФ.6);

- Управление доступом субъектов доступа к объектам доступа (УПД):
  - управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);
  - реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2);
  - разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);
  - назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5), а именно создание первой учётной записи Prisma;
  - ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6);
  - ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы (УПД.9);

- блокирование сеанса доступа субъекта в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10);

- Регистрация событий безопасности (РСБ):
  - сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3):
    - регистрация событий входа, попыток входа, выхода субъектов доступа в систему,
    - регистрация запуска (завершения) программ и процессов, связанных с обработкой защищаемой информации, реализованных в Prisma.
  - реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (РСБ.4);
  - мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5);
  - защита информации о событиях безопасности (РСБ.7)
- Обеспечение целостности информационной системы и информации (ОЦЛ):
  - контроль целостности программного обеспечения (ОЦЛ.1);
  - ограничение прав пользователей по вводу информации в информационную систему (ОЦЛ.6).

1.3. Состав персонала, обеспечивающего функционирование Prisma

Функционирование Prisma обеспечивается внутренними пользователями.

Численность персонала и возможность совмещения функций зависит от количества пользователей Prisma. Внутренние пользователи могут выполнять и другие (не связанные с эксплуатацией Prisma) функции.

2. УСЛОВИЯ РАБОТЫ СИСТЕМЫ

2.1. Требования к аппаратному и программному обеспечению

Требования к аппаратному и программному обеспечению приведены в таблице ниже.

Требования к аппаратному и программному обеспечению

Компонент	**Требования к программной части**
1	**3**
Prisma	1) Поддерживаемые операционные системы: - Astra Linux Special Edition 1.6 - Astra Linux Special Edition 1.7 - Astra Linux Common Edition 2.12 - Альт 8 СП Сервер - РЕД ОС 7.3 2) JAVA 8 (JDK) 3) Сервер приложений WildFly 24.0.1.Final 4) СУБД Postgres Pro 11.9 **Примечание:** допустимо использование более новых версий указанного программного обеспечения

[1] Без учета пространства занимаемого логами сервера приложений, операционной системой и ее данными и пользовательскими данными в СУБД

2.2. Требования и условия организационного характера

Перед эксплуатацией Prisma необходимо внимательно ознакомиться с комплектом программной эксплуатационной документации, а также необходимыми организационными мерами, рекомендуемыми разработчиком в эксплуатационной документации.

При эксплуатации Prisma должно быть обеспечено выполнение следующих условий:

– должен быть регламентирован запрет использования Prisma для обработки информации, содержащей сведения, составляющие государственную тайну;

- в ходе эксплуатации Prisma необходимо контролировать процесс синхронизации времени ОС, установленной на сервере;
- в подключаемой информационной системе должны быть определены роли, группы пользователей, пользователи области видимости и роли Клиентов, к которым необходимо применять разграничение прав;
- должен быть ограничен доступ к лог-файлам сервера приложений (доступ должен быть предоставлен только администратору, имеющему доступ к серверу-приложений);
- использование изделия в информационных системах 1 класса защищенности разрешается при реализации оператором требований по усилению мер защиты информации согласно методическому документу «Меры защиты информации в государственных информационных системах» (утверждены ФСТЭК России 11.02.2014);
- должна быть реализована защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны, путем блокирования несанкционированного физического доступа (подключения) к ним;
- при использовании изделия в информационных системах 1, 2, 3 классов защищенности при организации доступа в информационно-телекоммуникационные сети международного информационного обмена необходимо использовать сертифицированный межсетевой экран;
- при использовании изделия в информационных системах 1, 2, 3 классов защищенности должны использоваться сертифицированные ФСТЭК России версии ОС и СУБД с установленными на них актуальными обновлениями;
- должно быть обеспечено наличие администратора, обеспечивающего правильную эксплуатацию изделия, в том числе:
  - предотвращение несанкционированного доступа к идентификаторам и токенам привилегированных пользователей,

- обеспечение физической сохранности оборудования, на котором установлен Prisma, и исключение возможности доступа к нему посторонних лиц,
- обеспечивающего ограничение доступа к лог-файлам сервера приложений и хранение их не менее трех месяцев, если иное не предусмотрено законом Российской Федерации;

– необходимо проводить контроль целостности Prisma по мере необходимости, но не реже одного раза в квартал;

– обеспечить периодическое создание резервных копий конфигурации изделия в соответствии с требованиями процедуры восстановления;

– должна быть обеспечена ежедневная проверка программной среды ПЭВМ, использующейся в качестве административной консоли, на наличие вредоносного ПО;

– необходимо проводить ежемесячный поиск актуальных уязвимостей и сведений об уязвимостях изделия и среды функционирования, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности.

2.3. Требования и условия технического характера

Для работы Prisma необходимо выполнение следующих технических требований:

– перед установкой Prisma должен быть развернут SMTP-сервер и создан почтовый ящик, с которого будут отправляться оповещений Prisma;

– в ходе эксплуатации Prisma необходимо контролировать процесс синхронизации времени ОС, установленной на сервере;

– должен быть настроен конфигурационный файл для настройки автоматической очистки лог-файла сервера приложений по процессу логирования;

– при организации сетевого взаимодействия между субъектами доступа, подключенной информационной системой и Prisma должно выполняться условие сохранения оригинального IP-адреса устройства субъекта доступа, а также адрес Клиента;
– для субъекта доступа, сеанс которого был закрыт, должны быть заблокированы любые действия по доступу к объектам доступа Клиента и пользовательским интерфейсам, кроме необходимых для аутентификации, при этом на странице аутентификации не должны отображаться аутентификационные данные пользователя, сеанс которого был закрыт.

2.4. Требования и условия технологического характера

Для работы Prisma каких-либо особых требований и условий технологического характера не предъявляется.

3. УСТАНОВКА СИСТЕМЫ

Настройка Prisma включает выполнение следующих действий:

- подготовительные действия;
- установка и настройка сервисов;
- установка приложения Prisma.

3.1. Подготовительные действия

Веб-сервер, сервер БД и приложение ПО Prisma устанавливаются в рамках одного сервера.

Функционирование Prisma требует наличия следующих средств:

- Виртуальная или физическая машин с развернутой ОС из списка доступных
- Пакеты Java JDK 8;
- Сервер приложений WildFly 24.0.1;
- PostgreSQL PRO 11 с заведенными учетной записью пользователя и базой данных;
- Дистрибутив Prisma.

Для подготовки ОС к установке Prisma следует выполнить следующие настройки:

- Настроить ip-адрес
- Настроить сервер SSH
- Настроить службы точного времени NTP
- Создать пользователей

3.2. Установка приложения ПО Prisma

3.2.1. Установка приложения ПО Prisma

Инициализация Prisma происходит в процессе установки, во время которой указываются:

- логин и пароль администратора Prisma;
- параметры подключения к базе данных (адрес сервера базы данных, имя базы данных, имя пользователя базы данных, пароль пользователя базы данных).

Перед началом установки Prisma, необходимо убедиться, что развернуты:

- Пакеты Java JDK 8;
- Сервер приложений WildFly 24.0.1.Final;
- PostgreSQL PRO 11 с заведенными учетной записью пользователя и базой данных.

Установка Prisma состоит из следующих шагов:

- Установка приложения ПО Prisma;
- Настройка контроля целостности
- Запуск и проверка работы сервиса.

1) ***Важно!*** *При* выполнении команд через терминал, *необходимо использовать запуск от привилегированного пользователя с правами sudo.* Для установки приложения необходимо скопировать содержимое архива из дистрибутива Prisma в корень каталога WildFly, при этом необходимо согласиться на все слияния папок и замену файлов. (prisma-overlay-11.0.2.Tar.gz). В результате будет папка со всеми файлами, необходимыми для Prisma.

Рис.4.1. Пример ввода команды для извлечения файлов Prisma.

Следующим шагом необходимо перейти в каталог '/ <адрес дистрибутива, в котором расположен корневой дистрибутив сервера

приложений WildFly> / <Наименование дистрибутива сервера приложений Wildfly> /' и с правами sudo выполнить команду:

./iamc_setup.sh

В результате выполнения команды будет выполнена инициализации и регистрации Prisma, добавления jdbc драйвера, DataSource. Так же будут настроены standalone, так и standalone-ha версии модуля.

Рис.4.2. Пример вводимой команды.

Примечание. В случае повторного запуска скрипта или обновления существующей установки, возможны появления сообщений о дубликатах ресурсов. В результате действия в терминале появится сообщение, изображенное на рисунке ниже (рис.4.3)

Рис.4.3. Пример правильного ответа.

Переменные окружения, определенные в запускаемом скрипте, будут формировать настройки системы. Для этого необходимо отредактировать файл /дистрибутив, в котором расположен корневой дистрибутив WildFly/Наименование дистрибутива сервера приложений Wildfly/bin/standalone-ha.sh (либо standalone.sh, в зависимости от необходимого режима) заменив значения переменных на актуальные, отредактировав следующие строки:

- DB_ADDR='*адрес* PostgreSQL сервера (если порт PostgeSQL сервера отличается от стандартного (*5432*), его следует указать через двоеточие*)*'
- DB_DATABASE='*имя БД*'
- DB_USER='*логин* учетной записи в *БД*'
- DB_PASSWORD='*пароль* учетной записи для *БД*'
- #DB_SCHEMA='*наименование схемы*' (заполняется в случае, если в СУБД используется схема)

- #JDBC_PARAMS='*настройки* JDBC *драйвера*' (заполняется в случае, если используются специфичные настройки JDBC драйвера)
- crcmon_enable= Если true, включает модуль контроля целостности (При этом, в случае обнаружения изменений в файлах приложения, запуск сервиса будет остановлен!)
- crcmon_path= Путь к утилите контроля целостности crcmon
- crcmon_log= Путь к файлу логов crcmon. В логе фиксируется статус прохождения контроля целостности при последнем запуске.
- PROXY_ADDRESS_FORWARDING='*true/false*' (требует объявления при работе с обратным прокси, таким как nginx, это позволяет Prisma определять IP-адрес клиента из HTTP-заголовка)
- HAL_ORIGIN - определяет доменное имя при использовании обратного прокси, с протоколом, но без символа «/» в конце (к примеру HAL_ORIGIN=«https://dev-iamc-module.testcompany.ru«)
- BIND_ADDR= '*IP*-адрес интерфейса, на котором должен работать *Prisma'*
- SERVER_OPTS='-Djboss.bind.address=$BIND_ADDR -bmanagement $BIND_ADDR --server-config=standalone.xml' (При необходимости разнести Prisma и HAL консоль WildFly по разным интерфейсам, следует явно указать IP-адрес. Параметр
- jboss.bind.address определяет адрес для Prisma, bmanagement – для HAL консоли)

Дополнительно при работе в режиме standalone-ha указываются параметры:

- jgroups.bind_addr - определяет IP-адрес для сервиса обмена сообщениями JGroup и по умолчанию равен $BIND_ADDR
- jboss.tx.node.id - данный параметр позволяет уникально идентифицировать хост при работе с общей БД, должен быть уникален и по умолчанию инициализируется результатом выполнения команды *'hostname'*

Рис.4.4. Пример заполнения файла standalone.sh

3.2.2. Настройка контроля целостности

Контроль целостности приложения осуществляется утилитой crcmon, использующий штатные средства ОС для проверки контрольных сумм подконтрольных файлов.

Проверяемые каталоги необходимо указать в конфигурационном файле /opt/iamc/crcmon/dirs_0, требуется указать каталог с установленным Prisma:

/opt/iamc

Исключаемые файлы и каталоги указываются в конфигурационном файле /opt/iamc/crcmon/exclude_0 и включает в себя следующие файлы и каталоги:

/opt/iamc/crcmon/opt/iamc/standalone/log/opt/iamc/standalone/tmp/opt/iamc/standalone/configuration/logging.properties/opt/iamc/standalone/configuration/standalone_xml_history/opt/iamc/docs

Для включения модуля контроля целостности, необходимо в файле standalone-ha.sh (либо в standalone.sh, при использовании конфигурации без кластера) установить параметр crcmon_enable=true. При первом запуске приложения Prisma (с ключом crcmon_enable=true) , контрольные суммы будут созданы автоматически.

В дальнейшем, при внесении изменений в конфигурационные файлы, необходимо использовать специальные команды crcmon, для пересчета контрольных сумм, иначе запуск приложения будет остановлен.

Команды crcmon:

– Для обновления базы контроля целостности (если файлы были изменены) необходимости выполнить команду: su - iamc -c

«/opt/iamc/crcmon/crcmon -u»где, команда su - iamc -c, запускает скрипт от пользователя iamc.

– Для ручной проверки целостности файлов выполнить команду: su - iamc -c «/opt/iamc/crcmon/crcmon -c»

Результат выполнения контроля целостности будет записан в файл логов /opt/iamc/standalone/log/crcmon_out.log

3.2.3. **Запуск и проверка** работы сервиса

Запуск серверов осуществляется командой:

/ <дистрибутив, в котором расположен корневой дистрибутив WildFly> / <Наименование дистрибутива сервера приложений Wildfly > / bin / standalone-ha.sh.

Данную команду необходимо выполнить на всех нодах кластера Prisma.

```
root@fstek-iamc-2:~# /opt/iamc/bin/standalone-ha.sh
```

Либо, использовать - standalone.sh, в случае, если используется конфигурация без кластера.

```
root@fstek-iamc-2:~# /opt/iamc/bin/standalone.sh
```

Рис.4.5. Пример вводимой команды на OS AstraLinux SE 1.6

В результате всех действий будет запущенный Prisma. Пример сообщение полученного в результате правильной отработки команды изображен ниже (рис.4.6).

```
10:09:07,325 INFO  [org.jboss.as] (Controller Boot Thread) WFLYSRV0060: Http management interface listening on http://127.0.0.1:999
9/management
10:09:07,332 INFO  [org.jboss.as] (Controller Boot Thread) WFLYSRV0051: Admin console listening on http://127.0.0.1:9990
```

Рис.4.6. Пример правильного ответа на вводимую команду на OS AstraLinux SE 1.6

При необходимости запускать Prisma как сервис systemd, необходимо отредактировать содержимое файла сервиса systemd/iamc.service из дистрибутива, актуализировав в нем пути к Prisma, имя пользователя для старта Prisma, скорректировать скрипт запуска, указать:

Если планируется использовать конфигурацию без кластера, оставить значение по умолчанию (ExecStart=/opt/iamc/bin/standalone.sh).

Скопировать файл systemd/iamc.service в каталог /etc/systemd/system.

Обновить конфигурацию systemd:

```
# systemctl daemon-reload
```

Для добавления сервиса в автозагрузку выполнить команду:

```
# systemctl enable iamc.service
```

Если в файле сервиса был указан запуск от определенного пользователя (например, iamc), то необходимо этого пользователя сделать владельцем каталога с помощью команды:

```
# chown -R iamc: /opt/iamc
```

Команды необходимо выполнить на всех нодах кластера Prisma.

Для запуска сервиса использовать команду:

```
# systemctl start iamc
```

Дальше Prisma будет управляться как любой сервис system и чтение логов будет осуществляться командой journalct.

Проверить сервис можно с помощью команды ps:

```
# ps -aux | grep iamc
```

Пример выполнения команды:

3.3. Проверка работоспособности

Проверка правильности запуска и работоспособности Prisma выполняется путем проведения операции запуска консоли администратора Prisma и подтверждается отсутствием информации об ошибках в лог-файлах Prisma, а также статусами сервисов, отображаемых в интерфейсе Prisma.

Для проверки работоспособности необходимо запустить сервис (если не запущен) командой:

```
sudo systemctl start iamc
```

Открыть веб-консоль Prisma на странице: http(-s)://Адрес сервера приложений/

(по умолчанию адрес http://127.0.0.1/auth) (рис.4.7).

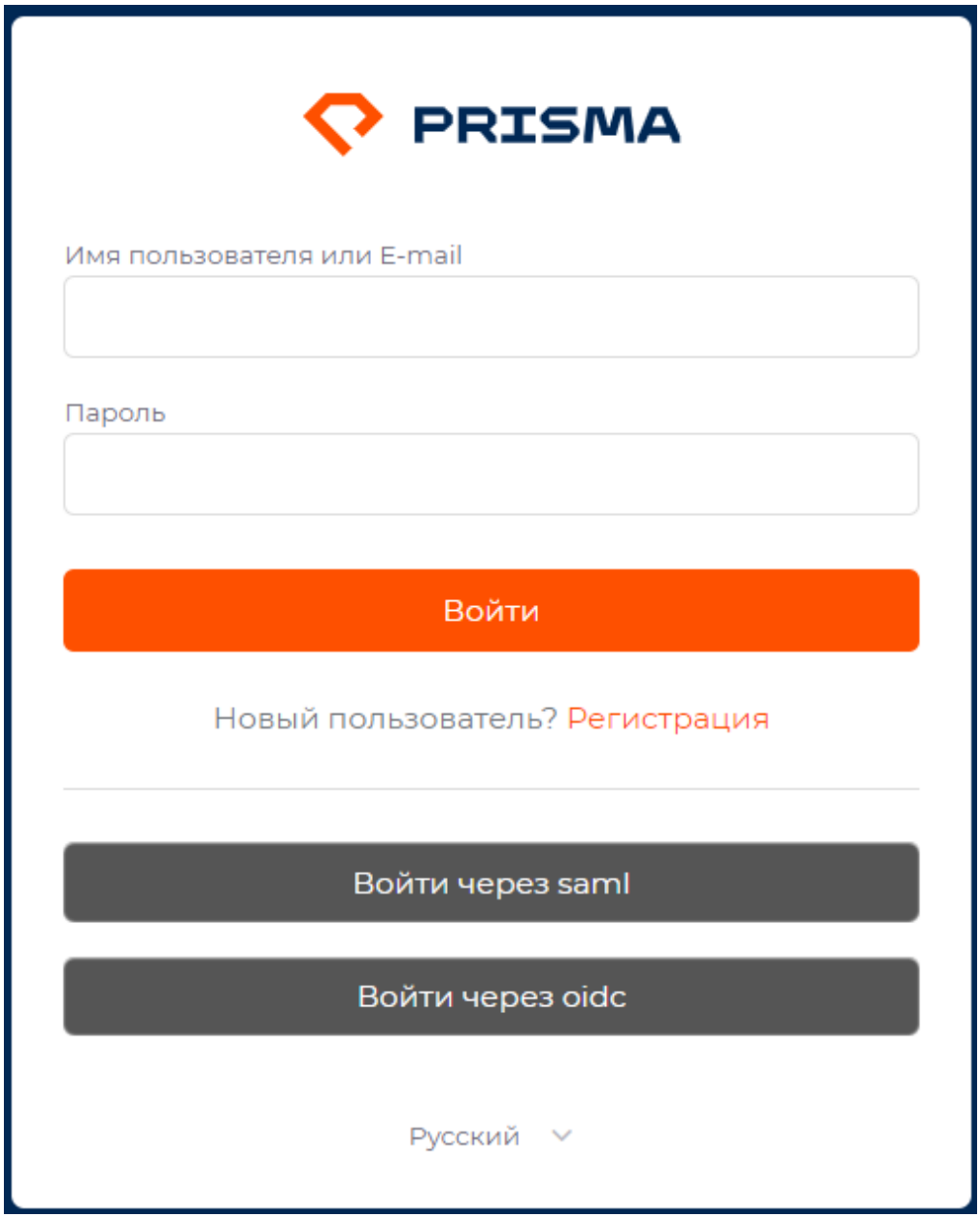


Рис.4.7. Пример начальной страницы консоли Prisma.

Если отобразилась страница аутентификации пользователя, то с текущего момента есть уверенность, что Prisma запущен и функционирует.

После ввода данных администратора сервера приложений WildFly откроется консоль Prisma (по умолчанию страница конфигурации Prisma) (рис.4.8).

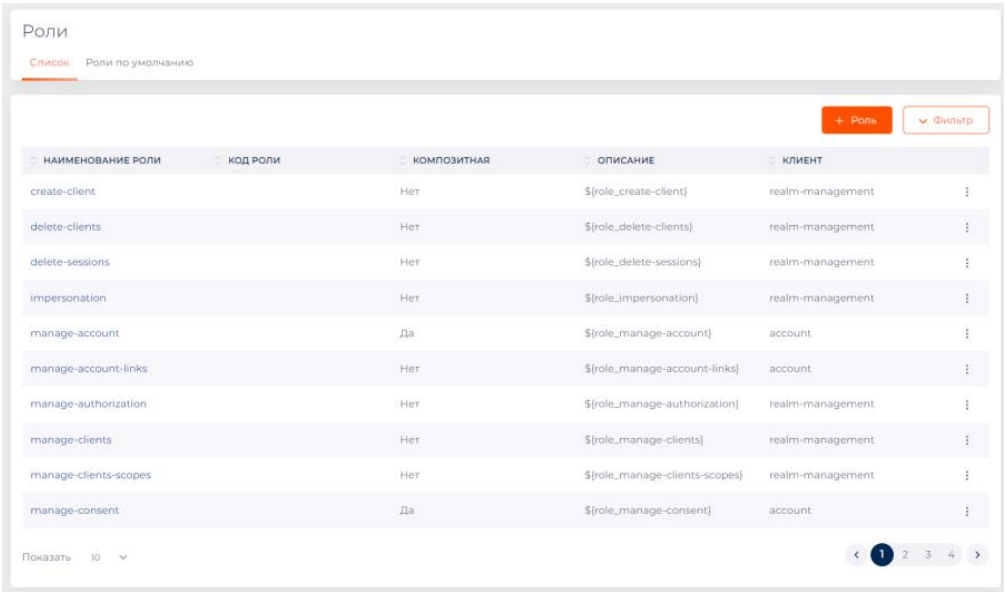


Рис.4.8. Пример страницы конфигурации Prisma.

Дальнейшими шагами необходимо настроить Prisma.

4. НАСТРОЙКА СИСТЕМЫ

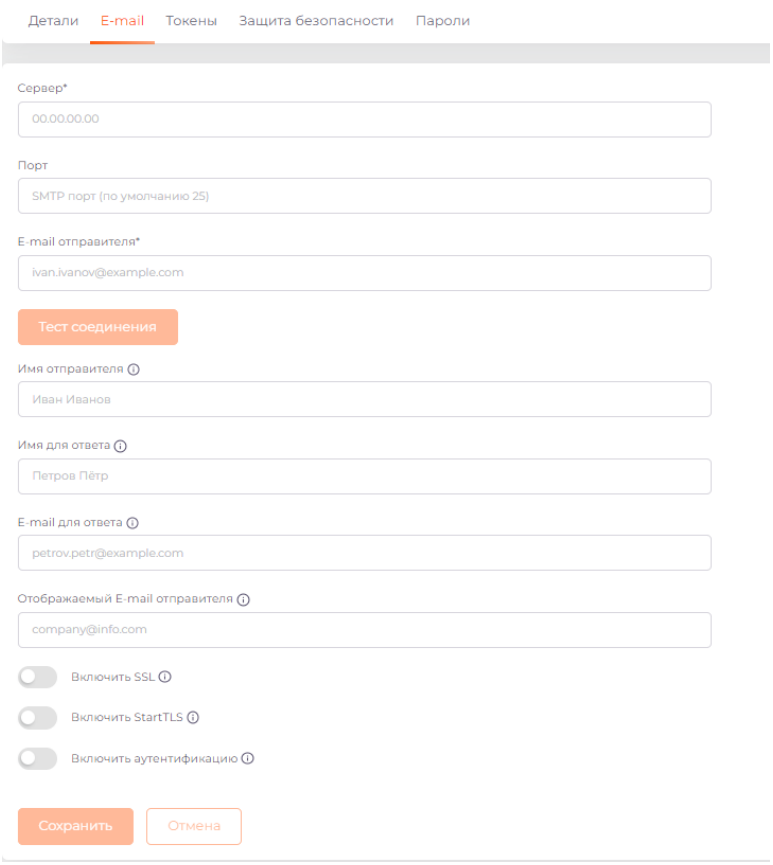
4.1. Настройка ПО Prisma после установки и проверки работоспособности

При установке Prisma некоторые параметры задаются по умолчанию (см. раздел «Настройки по умолчанию»). Кроме этого, необходимо настроить конфигурации Клиентов и Областей ИС согласно инструкциям, приведенным в руководстве пользователя, а также выполнить следующие настройки:

- Внести данные SMTP-сервера для отправки уведомлений на e-mail;
- Указать электронный адрес (рекомендовано рабочий) в данные учетной записи первого пользователя;
- Включить использование МФА для пользователей.

4.2. Настройка SMTP-сервера Prisma

Для настройки SMTP-сервера необходимо после совершения первого входа открыть Область ИС master, раздел Настройки, вкладку настройки E-mail и указать параметры подключения к smtp-серверу


Детали
E-mail
Токены
Защита безопасности
Пароли
Сервер*
00.00.00.00
Порт
SMTP порт (по умолчанию 25)
E-mail отправителя*
ivan.ivanov@example.com
Тест соединения
Имя отправителя
Иван Иванов
Имя для ответа
Петров Пётр
E-mail для ответа
petrov.petr@example.com
Отображаемый E-mail отправителя
company@info.com
Включить SSL
Включить StartTLS
Включить аутентификацию
Сохранить
Отмена

3.4.1. Указание электронного адреса учетной записи первого пользователя

Для того чтобы указать электронный адрес пользователя необходимо выполнить следующие шаги: перейти в раздел управления пользователями (см. рисунок) и открыть учетную запись, под которой был совершен вход.

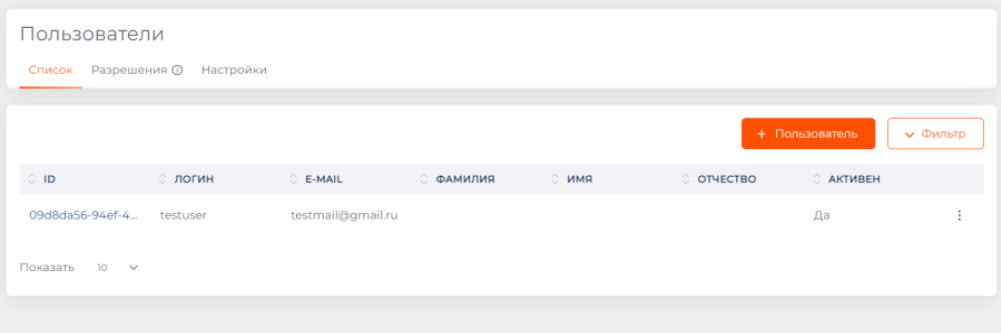


Рис. Раздел управления пользователями.

В открывшемся окне, в поле «E-mail» необходимо указать электронный адрес, на который будут приходить уведомления (см. Рисунок). и сохранить.

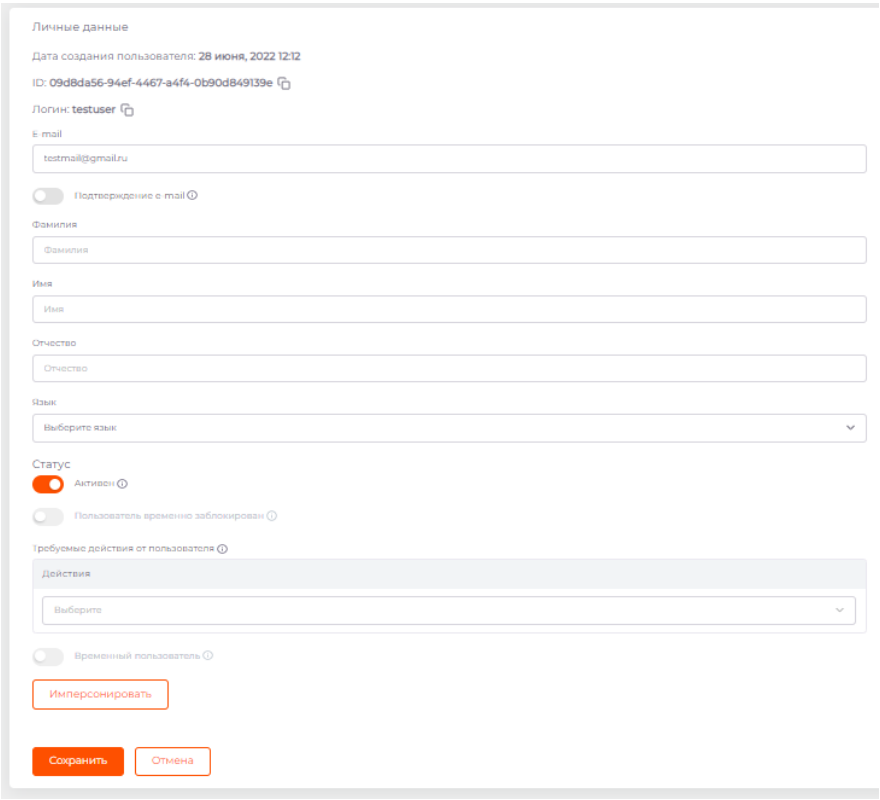


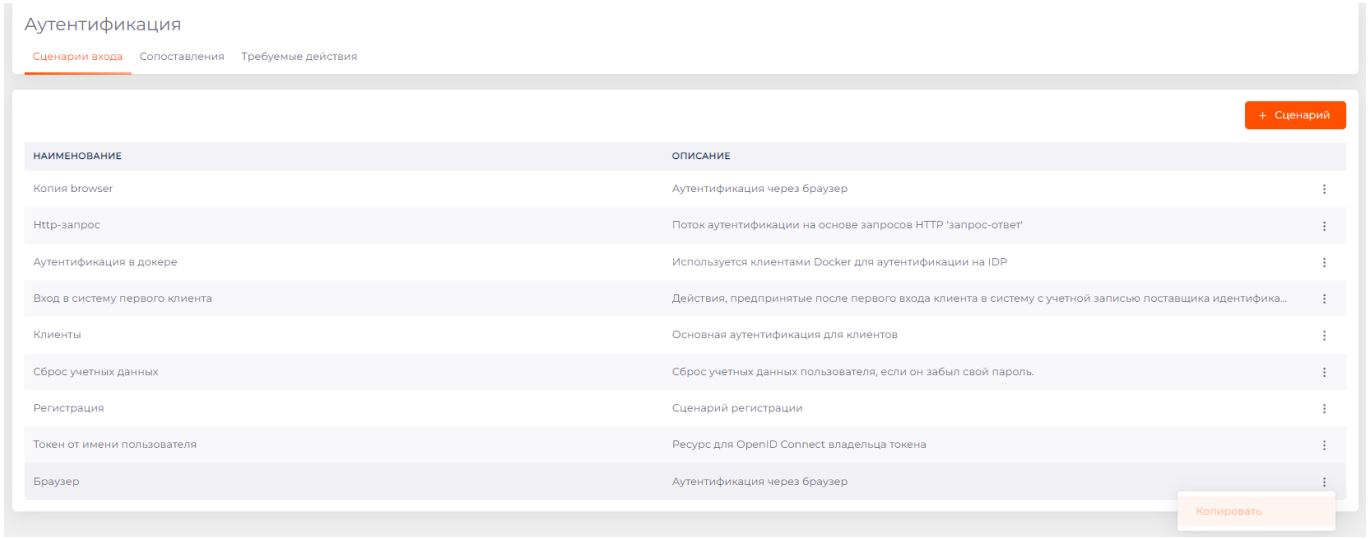
Рис. Форма настройки определенной учетной записи.

3.4.2. Включение использования МФА для пользователей

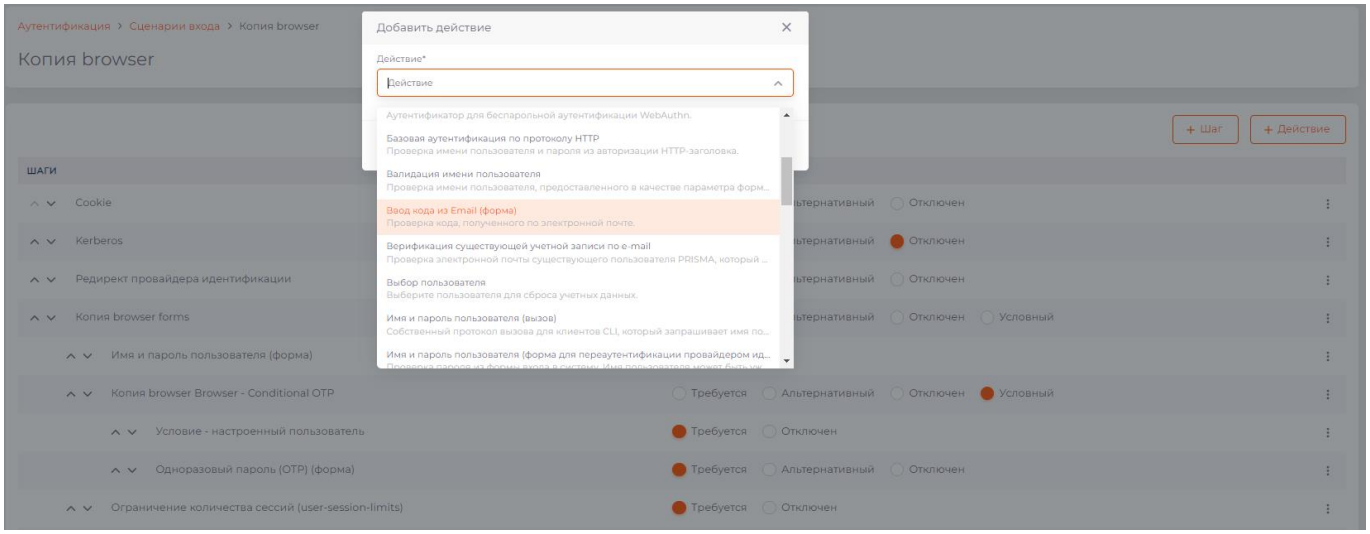
Для включения использования МФА для внутренних пользователей необходимо настроить сценарий прохождения аутентификации.

– **Предупреждение!** Не стоит указывать сценарий с МФА, если не настроен почтовый сервер и не указан e-mail у первого пользователя (администратора), так как без них не будет возможности получить код для входа в Prisma.

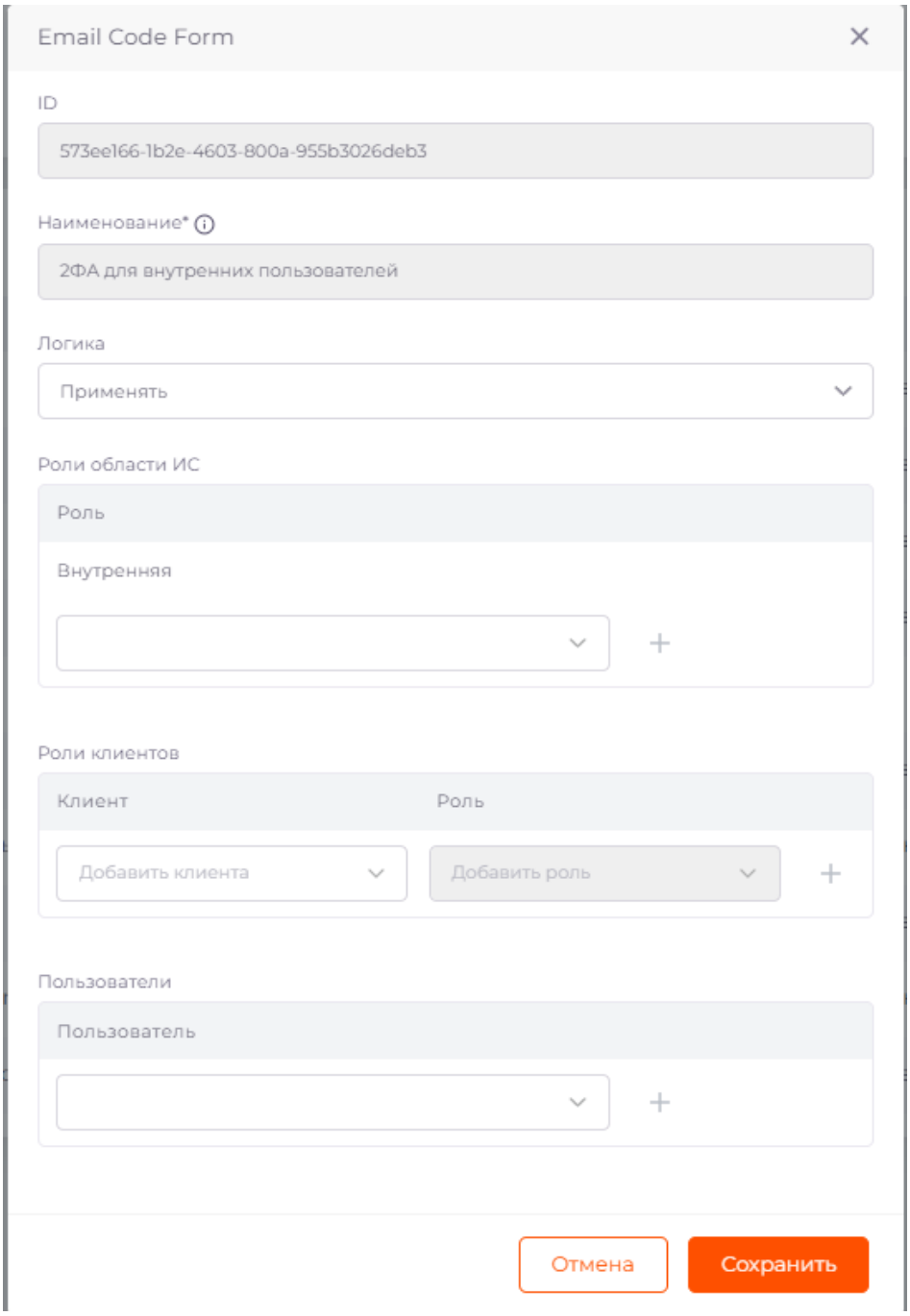
Для настройки сценария аутентификации с использованием 2ФА необходимо в разделе «Аутентификация» открыть сценарий, заданный в качестве сценария браузера, скопировать его.



и добавить в новый сценарий браузера Действие «Ввод кода из Email (форма)»:

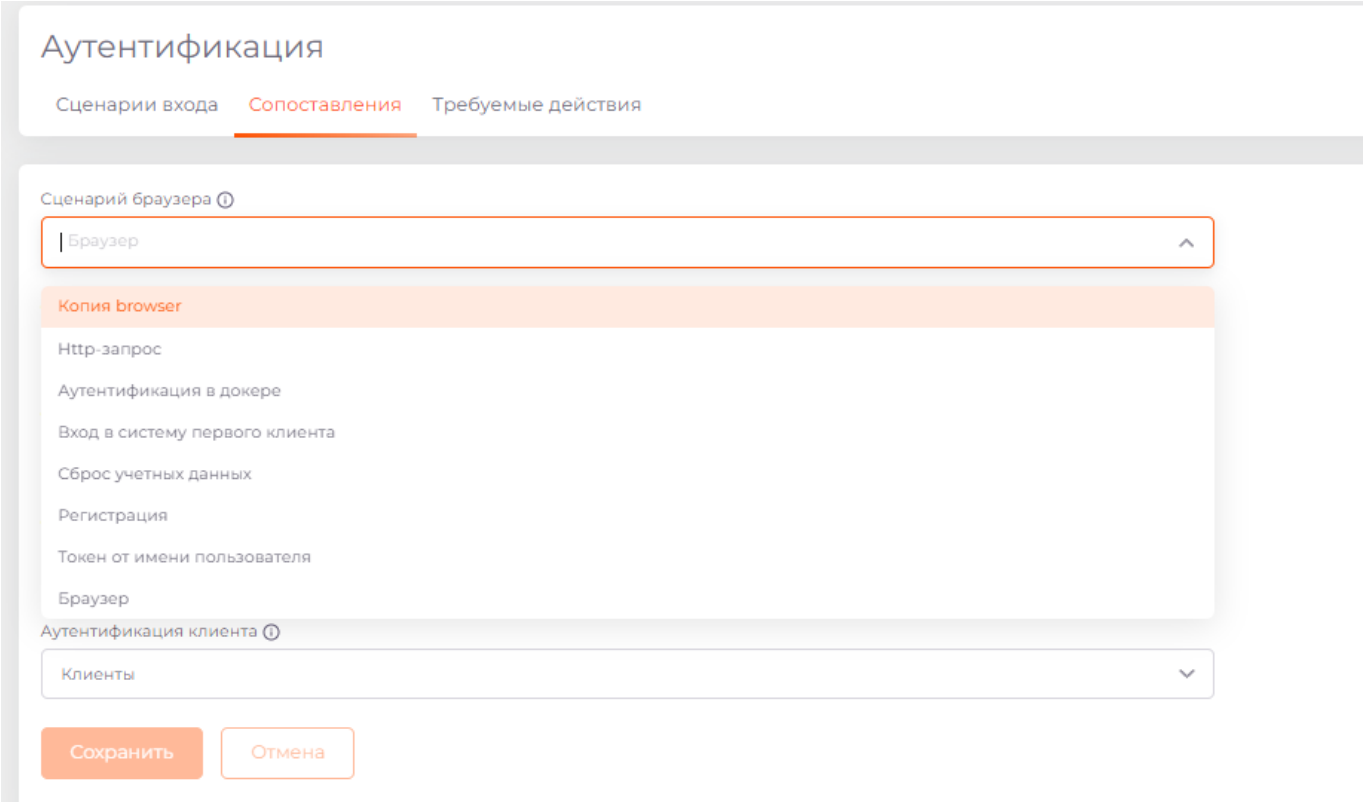


Действие необходимо сконфигурировать, указав логику «Применять» и роль «Внутренняя», как указано на рисунке.



После конфигурирования действие следует включить

и указать новый сценарий в качестве сценария браузера



При следующем входе в консоль администрирования любого пользователя с ролью **Внутренняя**, после ввода логина и пароля ему на электронную почту будет направлено письмо с кодом второго фактора аутентификации.

3.4.3. Настройки по умолчанию

При создании Prisma и Областей ИС, для поддержания первого класса защиты, следующие значения установлены по умолчанию:

№	Параметр	Требование ФСТЭК	Значение
1	**2**	**4**	**5**
1	Управление политиками паролей	− задание пароля длиной не менее восьми символов; − задание максимального времени действия пароля, но не более 60 дней; − запрет на использование двух последних использованных паролей при создании новых паролей	По умолчанию не заданы
2	Блокировка пользователей при превышении допустимых попыток входа	Блокировка до момента разблокировки уполномоченным пользователем	По умолчанию включено
3	Настройка количества дней до блокировки УЗ пользователя	Не более 45 ней	45
4	Ограничение попыток входа	3-4 попытки	3
5	Ограничение параллельных сеансов для всех пользователей, которым не присвоена роль «внутренняя»	2	По умолчанию настроено
6	Настройка срока бездействия пользователя до закрытия сеанса	5 минут	5 минут
7	Настройки регистрации событий	− События входа и попыток входа субъектов доступа в подключенную информационную систему и PRISMA. − Запуск (завершение) процессов, связанных с обработкой защищаемой информации, реализованных в PRISMA. При этом регистрации подлежат: события безопасности, которые происходят в результате управления субъектами и объектами доступа PRISMA, конфигурацией PRISMA (внутренние события), а также события безопасности, которые происходят в следствие отправки запросов подключенной ИС в PRISMA, связанных с	По умолчанию регистрация выключена

№	Параметр	Требование ФСТЭК	Значение
1	**2**	**4**	**5**
		получением разрешения на выполнение действия, управлением объектами и субъектами доступа ИС (внешние события)	
8	Настройка времени очистки истории событий безопасности	Хранение не менее трех месяцев (90 дней)	0

.

ПЕРЕЧЕНЬ ТЕРМИНОВ

В данном документе используются следующие основные термины и их определения:

1) **Администратор Prisma** – лицо, ответственное за функционирование Prisma, в установленном штатном режиме работы, согласно правилам разграничения доступа.

2) **Администратор Клиента** – лицо, ответственное за функционирование Клиента, в установленном штатном режиме работы, согласно правилам разграничения доступа.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
БДУ	Банк данных угроз
ЕСПД	Единая система программной документации
ИБ	Информационная безопасность
ИС	Информационная система
PRISMA	Professional Identity Security Manager
ОС	Операционная система
ОЦЛ	Обеспечение целостности информационной системы и информации
ПО	Программное обеспечение
РСБ	Регистрация событий безопасности
СЗИ	Средство защиты информации
СУБД	Система управления базами данных
ТУ	Технические условия
УПД	Управление доступом субъектов доступа к объектам доступа
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
SSO	Single sign-on
UID	User identifier
URL	Uniform Resource Locator