**программный продукт**

**«Professional Identity Security Manager»**

**«PRISMA»**

**Описание программы**

СОДЕРЖАНИЕ

[1 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ 3](#_Toc117112310)

[2 СТРУКТУРА СИСТЕМЫ 7](#_Toc117112311)

[3 ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ 8](#_Toc117112312)

[4 ТРЕБОВАНИЯ К ПЕРСОНАЛУ 9](#_Toc117112313)

# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Программный продукт (далее – 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).

Функционал аутентификации реализуется через подключение информационных внешних систем (далее - Клиенты) по протоколам Open ID Connect или SAML 2.0 и предоставление токенов Клиентам по запросам.

В процессе взаимодействии по технологии OpenID Connect, Prisma выполняет роль поставщика OpenID. а Клиенты выполняют роль доверяющей стороны, которая использует Prisma для аутентификации пользователей.

Схема взаимодействия:

* Пользователь пытается получить доступ к приложению через браузер
* Клиент перенаправляет пользователя на страницу аутентификации
* Пользователь проходит аутентификацию согласно настроенному в Prisma порядку аутентификации. (аутентификация происходит непосредственно в Prisma)
* В случае успешной аутентификации Prisma возвращает Refresh token и Access token, которые будут храниться в кэше браузера
* После получения токенов Клиент запрашивает разрешения пользователя (список ролей, групп, доменов), непосредственно разрешение или запрет
* После получения ответа Клиент разрешает или запрещает операции
* Токен проверяется при каждом взаимодействии пользователей с Клиентом
* Access token обновляется в указанный период времени.

Предоставляются различные варианты регистрации пользователей – вручную, по протоколам LDAP, Kerberos. Возможна аутентификация пользователей посредством использования других поставщиков идентификации.

Меры защиты информации, реализованные в продукте, 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)](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122995825),
* идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных ([ИАФ.2](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996137)),
* управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов ([ИАФ.3](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996140)),
* 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](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996143)),
* защита обратной связи при вводе аутентификационной информации ([ИАФ.5](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996153)),
* идентификация и аутентификация пользователей, не являющихся работниками оператора ([ИАФ.6](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996156));
* Управление доступом субъектов доступа к объектам доступа (УПД):
* управление (заведение, активация, блокирование и уничтожение) учетных записей пользователей, в том числе внешних пользователей ([УПД.1](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996166)),
* реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа ([УПД.2](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996170)),
* разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы ([УПД.4](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996189)),
* назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы ([УПД.5](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996200)), а именно создание первой учетной записи Prisma,
* ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) ([УПД.6](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996204)),
* ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы ([УПД.9](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996209)),
* блокирование сеанса доступа субъекта в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу ([УПД.10](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996262));
* Регистрация событий безопасности (РСБ):
* сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения ([РСБ.3](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=118139913)):
* регистрация событий входа, попыток входа, выхода субъектов доступа в систему,
* регистрация запуска (завершения) программ и процессов, связанных с обработкой защищаемой информации, реализованных в изделии;
* 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](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996273)),
* мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них ([РСБ.5](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996278)),
* генерирование надежных меток времени и (или) синхронизация системного времени ([РСБ.6](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996284)),
* защита информации о событиях безопасности ([РСБ.7](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=122996293));
* Обеспечение целостности информационной системы и информации (ОЦЛ):
* контроль целостности программного обеспечения ([ОЦЛ.1](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=118139928)),
* ограничение прав пользователей по вводу информации в информационную систему ([ОЦЛ.6](https://wiki.innostage-group.ru/pages/viewpage.action?pageId=118139931)).

# СТРУКТУРА СИСТЕМЫ

Для выполнения задач Prisma предоставляет администраторам Клиентов панель администрирования и REST API для разработчиков Клиентов.

Продукт разворачивается в виде приложения в кластере сервера приложений WildFly. Данные хранятся в БД PostgreSQL.

Общая архитектура Prisma представлена на схеме ниже. ****

**Рисунок 1 Общая архитектура Prisma**

# ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ

Требования к программному комплексу серверов:

* сервер БД:
* ОС Astra Linux \Альт 8 СП \РЕД ОС;
* СУБД PostgreSQL;
* Кластер серверов приложений:
* ОС Astra Linux \Альт 8 СП \РЕД ОС;
* WildFly;
* Prisma.

# ТРЕБОВАНИЯ К ПЕРСОНАЛУ

Пользователь должен обладать квалификацией, обеспечивающей как минимум:

* базовые навыки работы на персональном компьютере с графическим пользовательским интерфейсом (клавиатура, мышь, управление окнами и приложениями, файловая система);
* базовые навыки использования стандартной клиентской программы.

Пользователи администраторской консоли Prisma должны понимать принципы организации и управления доступом, знать базовые принципы протоколов ldap, kerberos, OIDC, SAML 2.0 (в случае необходимости их использования).