Программа для разграничения прав доступа

Планета. Доступ

ОПИСАНИЕ ПРОГРАММЫ

Версия: 1.1

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Наименование программы

Наименование: Программный комплекс «Планета.Доступ» - «внешнее» средство защиты информации прикладного программного обеспечения информационных систем.

Условное наименование: Программный комплекс «Планета.Доступ»

Краткое наименование: ПК "Планета.Доступ".

1.2 Назначение программы

ПК "Планета.Доступ" предназначен для обеспечения выполнения требований регуляторов к безопасности персональных данных (ПДн) и защите информации (ЗИ), применимых к ППО.

ПК "Планета.Доступ" предназначен для создания ИС со следующей классификацией:

- по информационной безопасности (ИБ) – до К2 включительно;
- по уровню защищенности ИСПДн – до УЗ-2 включительно;
- по требованиям по защите информации от несанкционированного доступа к информации (НСД) – до 1Г включительно.

ПК "Планета.Доступ" предназначен к использованию в ИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну.

ПК "Планета.Доступ" должен иметь оценку соответствия, проводимой путем сертификации как средства защиты информации и обеспечивать выполнение требований по ИБ и защите ПДн, без сертификации ППО, реализующего бизнес-функции ИС.

В состав ПК "Планета.Доступ" входят следующие программные комплексы:

- управление субъектами доступа и объектами доступа;
- обеспечение доступа субъектов доступа к объектам доступа;
- личные кабинеты администраторов;
- идентификация и аутентификация субъектов доступа;
- авторизация субъектов доступа;
- регистрация и обработка событий безопасности;
- обеспечение целостности ППО.

ПК "Планета.Доступ" поддерживает на уровне приложений и баз (хранилищ) данных функционирование в кластерной конфигурации и обеспечивает горизонтальное масштабирование в случае увеличения нагрузки.

1.3 Функции программы

ПК "Планета.Доступ" состоит из семи программных комплексов, объединенных в единую информационную систему.

1.3.1 Функции программного комплекса «Управление субъектами доступа и объектами доступа»

Программный комплекс «Управление субъектами доступа и объектами доступа» обеспечивает выполнение следующих функций:

- Регистрация сведений об организационной структуре для множества организаций (поддержка multi-org).
- Возможность определять иерархию организаций и организационно-штатных единиц в организации.
- Управление (заведение, активация, блокирование/разблокирование и логическое удаление) учетными записями внутренних пользователей.
- Проверка на уникальность логина.
- Управление хранением неактивных логинов.
- Блокирование пользователя на период или бессрочно.
- Привязка учетной записи внутреннего пользователя к одной и более организации (орг-штатной единице).
- Возможность определить роль внутреннего пользователя в организации (орг-штатной единице) – руководитель, сотрудник с правом подписи, сотрудник (из справочника типов ролей).
- Регистрация учетных записей внутренних пользователей на основании электронных документов (ЭД) – заявок, регистрируемых уполномоченными пользователями через web-сервис, предоставляемый ПК "Планета.Доступ" (вызывается по гиперссылке из прикладного приложения).
- Формирование одноразового пароля для новой учетной записи внутреннего пользователя.
- Регистрация сведений о сертификате ключа электронной подписи (СКП ЭП) пользователя (для входа с использованием СКП ЭП).
- Ведение перечня информационных систем (подсистем), для которых определяются объекты доступа.
- Определение объектов доступа (функций, процессов, объектов данных, экземпляров объектов данных) для ИС (ПС) – формирование «матрицы доступа».
- Регистрация запроса на доступ к личному кабинету внешних пользователей через web-сервис, предоставляемый ПК "Планета.Доступ" (вызывается по гиперссылке в окне ввода логина-пароля или через функцию «регистрация»).
- Запрос внешнего пользователя на доступ к личному кабинету может содержать атрибуты для определения правил доступа внешних пользователей к объектам доступа.

– Обеспечение регистрации учетной записи внешнего пользователя в автоматическом режиме после подтверждения запроса или администратором доступа.

– Обеспечение синхронизации сведений об учетных записях внутренних пользователей с внешними информационными ресурсами, обеспечивающими идентификацию и аутентификацию:

AD (LDAP)

– Ведение и сохранение информации о периоде действия, периоде бездействия (блокирования) для всех регистрируемых данных.

– Защищенное хранение персональных данных пользователей (в том числе открытых ключей СКП ЭП).

1.3.2 Функции программного комплекса «Обеспечение доступа субъектов доступа к объектам доступа»

Программный комплекс «Обеспечение доступа субъектов доступа к объектам доступа» обеспечивает выполнение следующих функций:

– Регистрация набора полномочий на доступ к функциям, процессам и объектам в виде роли доступа.

– Определение ролей доступа для внутренних пользователей (с возможностью автоматического присвоения роли на основании роли пользователя в организации).

– Регистрация (изменение) ролей доступа для внутренних пользователей на основании ЭД – заявок, регистрируемых уполномоченными пользователями через web-сервис, предоставляемый ПК "Планета.Доступ" (вызывается по гиперссылке из прикладного приложения) – автоматизировано при согласовании заявки.

– Определение заместителей для внутренних пользователей с указанием срока замещения.

– Определение правил ограничения доступа к экземплярам объектов данных для личного кабинета.

– Определение правил доступа внешних пользователей к объектам доступа (личным кабинетам).

– Определение политик доступа к объектам данных и экземплярам объектов данных ИС на основании контекста пользователя (ролей доступа и/или сведений из учетной записи пользователя).

– Применение политик доступа в ППО защищаемых ИС.

– Определение правил настройки пароля пользователя:

  - минимальной сложности пароля с требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

  - минимального количества измененных символов при создании новых паролей;

- максимального и минимального времени действия пароля;
- правил блокировки при неуспешном (многократном) вводе пароля;
- запрет на использование пользователями определенного числа последних использованных паролей при создании новых паролей.

– Автоматическое блокирование учетной записи пользователя на основании правил блокировки при неуспешном вводе пароля.

– Регистрация запроса на сброс пароля пользователя через web-сервис, предоставляемый ПК "Планета.Доступ" (вызывается по гиперссылке в окне ввода логина-пароля).

– Автоматическое формирование одноразового пароля в случае сброса пароля внутреннего пользователя и отправка по зарегистрированному для учетной записи каналу (электронная почта, СМС).

– Передача данных об учетных данных пользователей (без паролей) и их полномочиях в защищаемое ППО (web-сервис, планировщик задач).

– Определение продолжительности сессии пользователя для ИС при неактивности пользователя, с принудительным отключением от защищаемой ИС.

– Возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий) для ИС, основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли.

– Проверка прав доступа при информационном взаимодействии (передаче информации) - в зависимости от полномочий инициатора потока и (или) адресата потока настраиваются правила фильтрации (что разрешено) передаваемой информации.

1.3.3 Функции программного комплекса «Личных кабинетов администраторов»

Программный комплекс «Личных кабинетов администраторов» обеспечивает выполнение следующих функций:

– Личный кабинет «Администратора ИБ» предназначен для изменения настроек (метаданных) ПК "Планета.Доступ", обеспечивающих защиту информации в защищаемом ППО, и назначения администраторов доступа.

– Личный кабинет «Администратора ИБ» с функциями, относящимися к:

- ведению правил парольной защиты;
- ведению организаций;
- ведению перечня ИС;
- ведению объектов доступа;

- ведению прав доступа (ролей и правил ограничения доступа к экземплярам объектов данных для личного кабинета);
- ведению учетных данных администраторов доступа (имеют права только для работы с ПК "Планета.Доступ");
- назначению администраторов доступа для организации.

– Личный кабинет «Администратора доступа» предназначен для управления пользователями и полномочиями пользователей администрируемых организаций.

– Личный кабинет «Администратора доступа» с функциями, относящимися к:

- ведению (созданию, изменению, блокированию, удалению) организаций и орг-штатной структуры организации, определенной при назначении и всех подведомственных организаций;
- ведению учетных данных пользователей организации, определенной при назначении и всех подведомственных организаций;
- обработка заявок на изменение прав доступа
- присвоение администрируемым пользователям прав доступа.

– Регистрация сведений об организационной структуре для множества организаций (поддержка multi-org).

1.3.4 Функции программного комплекса «Идентификация и аутентификация субъектов доступа»

Программный комплекс «Идентификация и аутентификация субъектов доступа» обеспечивает выполнение следующих функций:

– Web-сервис с окном выбора способа аутентификации и вводом логина-пароля.

– Показ пользователю информации (например, в виде сообщения в модальном окне) о дате и времени предыдущего входа в ИС от имени этого пользователя.

– Защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий:

- отображение вводимого пароля знаками «*» или аналогичными;
- количество вводимых пользователем символов пароля не совпадает с количеством отображаемых знаков (если такие требования предъявлены).

– Обеспечение идентификации и аутентификации пользователей с использованием внешнего каталога пользователей (LDAP).

– Передача контекста (идентификационных данных пользователя) на время сессии для указания этих данных при изменении объектов или запуске процессов.

– Реализация функций SSO (однократная аутентификация

пользователей при входе в несколько ИС)

- Принудительное отключение пользователя от всех ИС при завершении сессии в SSO или изменении прав доступа пользователя.

1.3.5 Функции программного комплекса «Авторизация субъектов доступа»

Программный комплекс «Авторизация субъектов доступа» обеспечивает выполнение следующих функций:

- Реализация доступа пользователей к функциям и информационным ресурсам на основании ролевой модели, с ограничением множества защищаемых объектов, доступных пользователю по матрице доступа.
- Выполнение правил доступа к защищаемым информационным объектам, экземплярам объектов, записям реестров и справочников, в том числе с учетом значений атрибутов соответствующего информационного объекта (проксирование, применение автоматически создаваемых политик безопасности или иной способ).
- Предоставление агента (сервиса) для выполнения авторизации доступа к функциям в ППО

1.3.6 Функции программного комплекса «Регистрация и обработка событий безопасности»

Программный комплекс «Регистрация и обработка событий безопасности» обеспечивает выполнение следующих функций:

- Регистрация входа (выхода) субъектов доступа в каждую защищаемую ИС (с составом сведений по требованиям к классу защищенности 1Г).
- Регистрация фактов доступа пользователей ИС к защищаемым информационным ресурсам в соответствии с назначенными полномочиями (матрицей доступа).
- Регистрация фактов выполнения процессов, запускаемых пользователем ИС, в том числе в отложенном режиме.
- Регистрация фактов выполнения системных процессов в ИС.
- Формирование журналов регистрации событий безопасности.
- Автоматическое блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены к событиям нарушения безопасности информации.
- Архивирование с очисткой журналов событий безопасности.

1.3.7 Функции программного комплекса «Обеспечение целостности ППО»

Программный комплекс «Обеспечение целостности ППО» обеспечивает выполнение следующих функций:

- Обеспечение целостности программных средств СЗИ НСД (как модулей ПК "Планета.Доступ", так и модулей-агентов (библиотек приложений, объектов (политик безопасности) БД) в защищаемых ИС.
- Логирование проверок целостности.
- Оповещение Администратора ИБ об обнаружении нарушения целостности.

1.4 Компонент пользовательских интерфейсов

Компонент пользовательских интерфейсов предоставляет пользователю ПК "Планета.Доступ" следующие типовые интерфейсы (веб-формы), обеспечивающие:

- Управление пространствами для пользователя с соответствующими правами
- Управление клиентами
- Управление областями действия
- Управление провайдерами
- Управление ролями
- Управление пользователями
- Управление группами
- Управление авторизациями
- Управление объектами системы

1.5 Сведения о технических и программных средствах, обеспечивающих выполнение программы

1.5.1 Минимальный состав технических средств

ПК "Планета.Доступ" функционирует на технических средствах со следующими минимальными характеристиками:

- Процессор: Intel Core i5 (с частотой не менее 3.2 ГГц).
- Оперативная память: 32 Гб, 64 Гб.
- Объем дискового пространства: 200 Гб.
- Сеть: Ethernet (IEEE 802.3), 100-BaseTX.

1.5.2 Минимальный состав программных средств

ПК "Планета.Доступ" функционирует под управлением одной из следующих ОС:

- ОС семейства Microsoft Windows x64:

Возможно использование настольных ОС Windows: 7, 8.1, 10 или Windows Server 2008 R2, 2012 R2, 2016, 2018, 2019.

- Дистрибутивы GNU/Linux:
  - AstraLinux 1.7;

- Ubuntu 18.04+;
- AltLinux 10.

Веб-интерфейс функционирует под управлением не менее одного для каждой из ОС клиентских рабочих мест web-браузеров:

- Google Chrome версии 32 и выше;
- Mozilla Firefox версии 32 и выше;
- Safari версии 9 и выше;
- Microsoft Edge;
- Спутник.

Платформа взаимодействует с базами данных с системамойуправления БД (СУБД): PostgreSQL[1] v10 и выше.

1.5.3 Категории пользователей программы

Пользователями ПК "Планета.Доступ" являются администраторы информационной безопасности.

1.5.4 Используемые технологии

ПК "Планета.Доступ" построен на принципах трехуровневой архитектуры.

Состав технологических компонентов ПК "Планета.Доступ", используемых на каждом из уровней, приведен на Рисунке 1.

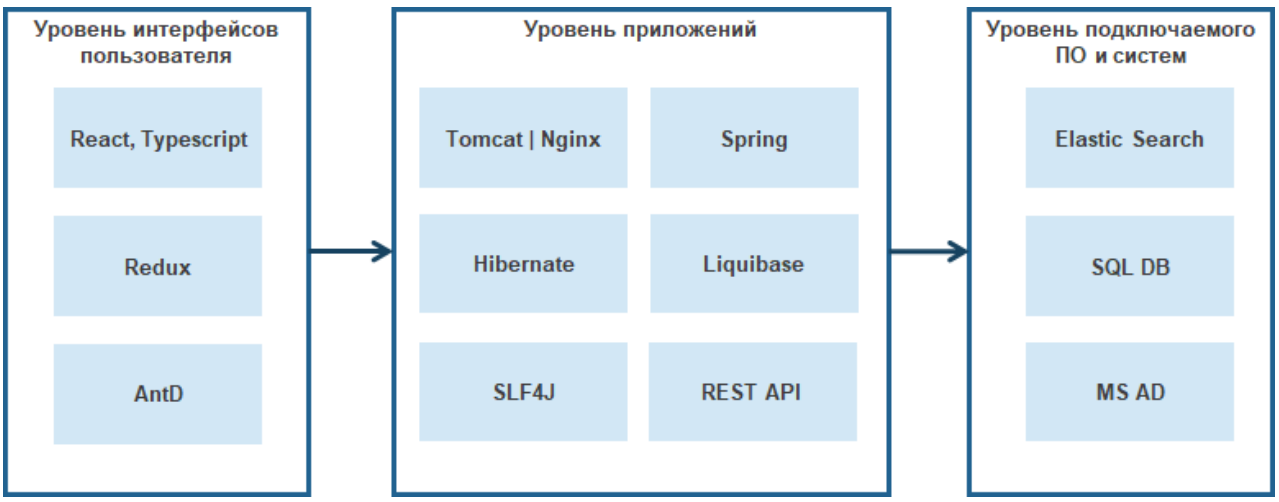

Рисунок 1. Состав технологических компонентов ПК "Планета.Доступ"

Разработка ПК "Планета.Доступ" выполнена на языке программирования Java.

Основным каркасом (framework) разработки использован каркас Spring Framework.

Сборка разрабатываемого приложения осуществлена на основе инструментов с открытым кодом: Apache Maven, Jenkins.

[1] Рекомендуем использовать сертифицированную и внесенную в реестр российских программ версию Postgres Pro https://reestr.digital.gov.ru/request/174839/

2. СТРУКТУРА ПРОГРАММЫ

2.1. Сведения о структуре программы

Планета.Доступ состоит из:

1. API, которые помогают в управлении основными сущностями приложения (realm-api, client-api, role-api и тд).
2. Redis для хранения данных сессий и кешей.
3. Postgresql – БД для хранения основных данных приложения.
4. Kafka – опционально, для уведомлений внешних приложений об основных событиях сущностей.

На примере платформы Планета, в которую входит Планета.Доступ на схеме указаны основные внешние (по отношению к Доступу) компоненты в Planeta-Cloud:

1. Api-Gateway в качестве клиента (в терминах OAuth2), в котором происходит проверка и хранение актуальных JWT с привязкой к сессии в браузере пользователя.
2. Discovery-service - нахождение и регистрация бизнес-сервисов в облаке.
3. Config-service – предоставление конфигураций для бизнес-сервисов.
4. Random-service – любой бизнес-сервис облака.

Так как Планета.Доступ использует протокол OAuth2(OIDC), для возможности использования программы необходимы:

1. Клиенты (Client) – приложения, которые будут использовать Планета.Доступ для аутентификации.
2. Сервисы ресурсов (Resource server) – приложения, которые должны предоставлять данные или выполнять обработку данных и защищать эти данные.
3. Аутентификационный сервис (Auth server) – приложение, которое выполняет аутентификацию, выполняет данную роль Планета.Доступ.

Общая структурная схема ПК "Планета.Доступ" представлена на Рисунке 2.

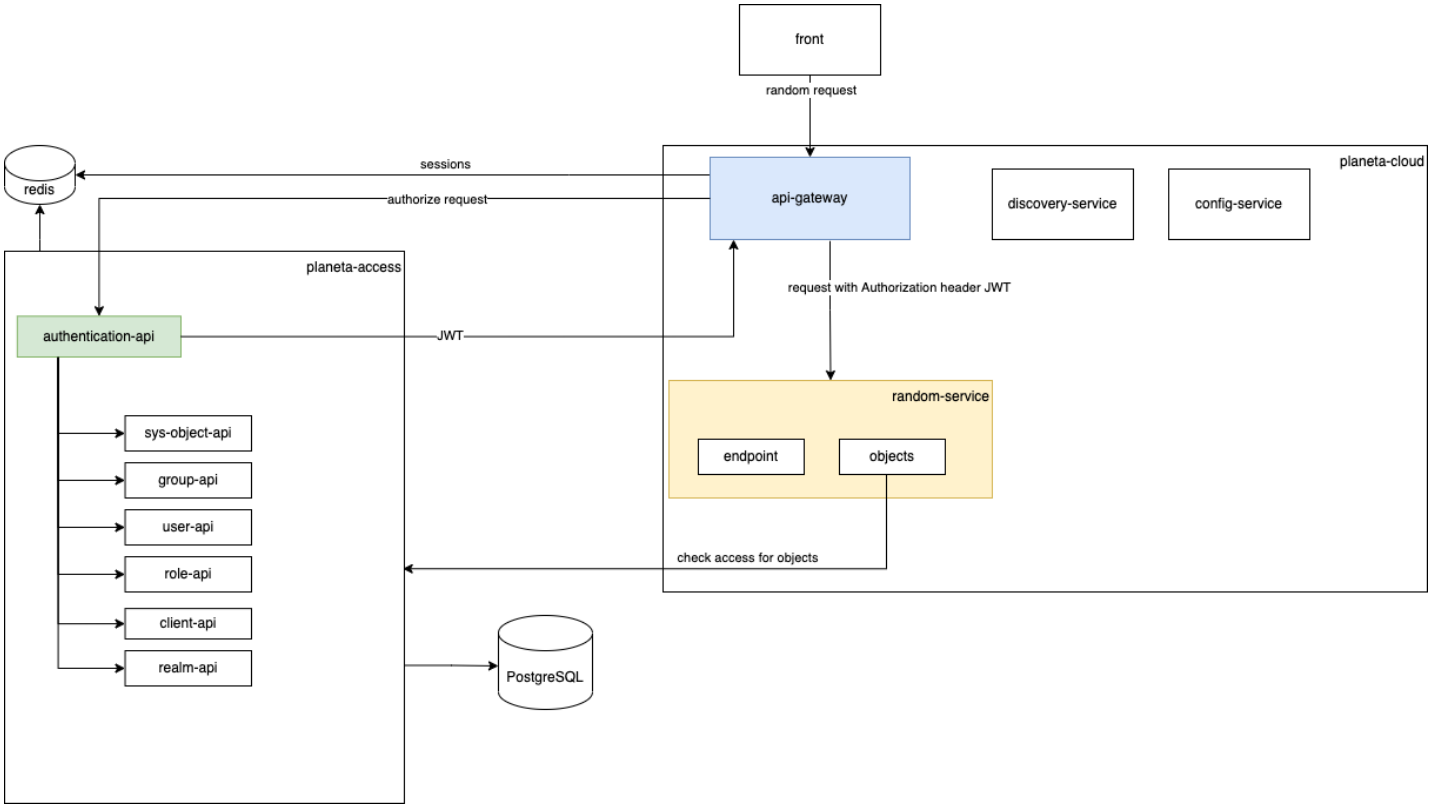

Рисунок 2. Общая структурная схема ПК "Планета.Доступ"

Операторы взаимодействует с компонентами ПК "Планета.Доступ" через экранные формы. Специалисты службы поддержки получают информацию о текущем состоянии каждого компонента через средства мониторинга.

2.2. Сведения о составных частях программы

2.2.1. Функциональный блок planeta-cloud

В задачи данного функционального блока входит получение и перенаправление запроса в соответствующий микросервис с токеном авторизации. В случае обращения к объектам – проверка прав доступа, с выполнением запроса к Планета.Доступ для получения необходимой информации

2.2.2. Функциональный блок planeta-access

Задачами данного функционального блока является аутентификация и авторизация пользователя и приложений на основании протокола OAuth 2.0.

2.2.3. Redis

Redis является хранилищем данных, сессий и токенов аутентификации.

2.2.4. PostgreSQL

Postgres является хранилищем основных данных Планета.Доступ.

2.3. Сведения о связях между составными частями программы

Компоненты ПК "Планета.Доступ" связаны между собой посредством программных интерфейсов и сетевых протоколов взаимодействия: HTTP/HTTPS, SMTP, TCP, UDP, JDBC и API.

2.4. Сведения о связях программы с другими программами

Платформа может взаимодействовать с внешними источниками, приёмникамии хранилищами данных, к которым относятся:

- внешние прикладные автоматизированные системы;
- сервера электронной почты, обеспечивающие отправку оповещений.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Описание
БД	База данных – подключаемое программное обеспечение
ИС	Информационные системы
ИТ	Информационные технологии
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
РФ	Российская Федерация
СУБД	Система управления базами данных