СОЛАР

SOLAR INRIGHTS ORIGIN

WHITE PAPER

Версия 1.0

Дата выпуска версии 17.02.2025

МОСКВА, 2025

Содержание

1. Введение

В условиях стремительно меняющегося мира информационные технологии становятся неотъемлемой частью бизнеса. Управление доступом к ресурсам компании представляет собой важный аспект обеспечения безопасности информационных систем, охватывающий подходы, практики и технологии для управления учетными данными и правами пользователей.

2. Цели и задачи документа

Цель документа – рассмотреть проблемы управления доступом, с которыми сталкиваются организации и помочь компаниям, которые имеют ограниченный бюджет и стремятся к оптимизации процессов управления доступом, оценить возможности системы Solar inRights Origin и принять решение для перехода к более эффективной модели управления доступом на основании лучших практик информационной безопасности.

3. Проблематика управления доступом

Проблематика управления доступом включает в себя несколько ключевых аспектов, которые необходимо учитывать:

Неструктурированные процессы

Во многих компаниях процессы управления доступом неуправляемые и разрозненные. Часто права доступа назначаются вручную, что приводит к недостаточной прозрачности и сложности в отслеживании. Частичная автоматизация на основании самописных программных инструментов закрывает лишь малую часть задач и не отвечает требованиям безопасности. Поэтому неструктурированные и ситуативные подходы к управлению доступом делают организации уязвимыми к внутренним и внешним угрозам.

Человеческий Фактор

Ручное управление доступом часто приводит к высокому уровню человеческих ошибок. Ошибки при назначении прав доступа могут вызывать серьезные инциденты информационной безопасности, такие как утечка конфиденциальной информации, несанкционированный доступ к данным, кражи интеллектуальной собственности, финансовые и репутационные потери.

Ограниченная информация об уязвимостях и риски ИБ

Отсутствие информации о потенциальных уязвимостях и рисках доступа к системам создает дополнительные вызовы. Без инструментов для всестороннего анализа и мониторинга предоставленных полномочий сложно оценить, какие пользователи имеют доступ к критическим системам и ресурсам и какого уровня и, как следствие, служба ИБ не сможет принять необходимых и своевременных решений для устранения угроз, возникающих на уровне управления доступом.

Часто требования к пристальному рассмотрению вопросов доступа становятся актуальными лишь в индивидуальных ситуациях во время спонтанных аудитов, что приводит к нерегулярным пересмотрам полномочий учетных записей, созданных для внешних и внутренних сотрудников, а также технических учетных записей. Это не обеспечивает достаточного контроля доступа к ресурсам и создает риски для безопасности.

Нехватка инструментов для управления доступом

Имеющиеся в организации инструменты управления доступом часто не соответствуют современным требованиям и ее нуждам. Применяемые устаревшие методы и решения не обеспечивают необходимого уровня автоматизации. Это приводит к дополнительной нагрузке на ИТ-специалистов, вынужденных тратить значительное время на рутинные операции.

Соответствие регуляторным требованиям

Соблюдение законодательства становится приоритетом для многих организаций. В частности, финансовые учреждения обязаны соответствовать требованиям Банка России по безопасности (ГОСТ 57580, СТО БР) в том числе в части управления доступом. Неспособность выполнить эти требования может привести к штрафам и репутационным потерям. Более того, необходимость внедрения систем управления доступом может стать рекомендацией аудиторов в рамках проверок.

Высокий порог входа и большие затраты для внедрения существующих технологий

Многие организации отказываются от внедрения существующих на рынке решений в сфере управления доступом из-за высокой стоимости и длительности проектов (от 1,5 до 3 лет). Затягивание процесса может быть критичным для организаций, которым необходимо оперативно наладить процессы управления доступом для закрытия внутренних и внешних требований. Сложные IdM/IGA-системы требуют значительных затрат, высоких компетенций и ресурсов для обучения сотрудников, что может оказаться неподъемной задачей для компаний с ограниченным бюджетом.

Существующие системы часто требует высокой зависимости от компетенций и ресурсов конкретных вендоров т.к. сложность развертывания, настройки и поддержки системы создает дополнительные трудности для организаций.

Вся эта проблематика указывает на потребность в более простых и инновационных подходах к управлению доступом. Решение Solar inRights Origin предлагает разумную альтернативу, которая направлена на устранение этих проблем и дает возможность быстро, эффективно и гибко управлять доступом к ключевым системам организации.

4. О системе Solar inRights Origin

Solar inRights Origin (коротко inRights/система) — это комплексное и полнофункциональное коробочное решение, предназначенное для автоматизации процессов управления доступом. Оно позволяет получать кадровые данные из системы 1С и управлять доступом к системам Microsoft Active Directory (MS AD) и Microsoft Exchange.

Ключевыми преимуществами решения являются: наличие подробной документации, описывающей все настроенные процессы, методология внедрения, требований к управляемым системам, а также возможность использования заранее настроенной конфигурации. Все это является надежной опорой для ваших сотрудников, позволяя им легко подготовиться к внедрению, разобраться в нюансах работы системы и быстро приступить к ее использованию. В случае если ваша организация не знает с чего начать, наше решение станет идеальным вариантом, позволяющим оперативно настроить и внедрить процессы управления доступом на основании лучших практик и многолетней собранной экспертизы. Такой подход приводит к тому, что процесс внедрения занимает всего лишь несколько месяцев.

Кроме того, система построена на гибкой платформе, что открывает возможности для дальнейшего развития и расширения её функциональности. При желании, ваше работающее решение можно адаптировать с учетом изменяющихся бизнес-требований, внедряя дополнительные возможности помимо коробочных функций.

4.1. Решаемые задачи

Подготовка организационной среды для внедрения изменений

Внедрение необходимых организационных изменения, подготовка информационных систем, оптимизация процессов и обучение персонала для последующего бесшовного и оперативного внедрения технологической платформы по управлению доступом. Это важный шаг для того, чтобы донести цели и преимущества внедрения системы до всех заинтересованных сторон, обеспечить комфортную среду по развертыванию и настройке системы и сосредоточиться на достижении бизнес-целей.

Увеличение эффективности бизнес-процессов и оптимизация затрат

Автоматизация процессов управления доступом, предлагаемых Solar inRights Origin, позволяет значительно сократить время, необходимое для выполнения рутинных задач. До 80% сокращается нагрузка на ИТ подразделение за счет автоматизации предоставления и изменения прав доступа на основании кадровых событий. Не более 10 минут требуется для получения доступа новых сотрудников к основным системам. На 50 % экономится время сотрудников за счет сервисов самообслуживания. Это с одной стороны улучшает рабочие процессы и повышает общую производительность работников компании и с другой стороны сокращает операционные расходы, связанные с управлением доступом. Использование системы высвобождает ИТ-специалистов для выполнения более стратегических задач, таких как работа над проектами, повышающими конкурентоспособность компании.

Снижение рисков безопасности

Исполнение разработанных политик в части доступа, автоматизация контроля и мониторинга прав обеспечивают защиту от утечек информации и других инцидентов безопасности, минимизируя потенциальные убытки и репутационные риски для бизнеса

Повышение уровня сервиса для сотрудников

Поддержка функций самообслуживания в системе Solar inRights Origin позволяет сотрудникам оперативно управлять своими правами доступа, снижая зависимость от ИТ-подразделения. Это повышает удовлетворенность пользователей и позволяет быстрее реагировать на изменения в рабочих процессах.

Гибкость и адаптация к изменениям бизнеса

В быстро меняющемся бизнес-окружении важно иметь возможность гибко адаптировать процессы к новым требованиям. Решение Solar inRights Origin интегрированное с ключевыми системами организации поможет быстрой адаптации под изменения в структуре бизнеса, такие как увеличение числа сотрудников или взаимодействие в рабочих задачах с новыми внешними контрагентами. Такие изменения могут потребовать создание новых команд, пересмотр функций подразделений, интеграцию в процессы внешних партнеров и, как следствие, оперативное предоставление изменение доступа, контроль уровня полномочий, назначение кураторов для контрагентов и своевременный отзыв прав по завершению договоров.

Принятие обоснованных решений на основе точных данных

Система предоставляет аналитические инструменты и отчеты, которые помогают руководителям подразделений проводить плановые пересмотры доступа, принимать оптимальные оперативные решения относительно доступа персонала компании и предоставленных полномочий. Это касается и работы с отклонениями и нарушениями доступа для оперативного выявления потенциальных проблем, и получения консолидированной отчетности с целью отслеживания динамики изменений, оптимизации процессов и управления рисками.

4.2. Принцип работы

Solar inRights Origin получает данные о сотрудниках и структуре организации из системы кадрового учёта 1С ЗУП. Затем программа использует эти сведения для запуска процессов, связанных с изменениями в кадровой информации: приём на работу, перевод на другую должность или увольнение.

Решение также интегрировано с управляемой системой MS AD и взаимодействует с ней в двух направлениях: собирает актуальные данные о пользователях и их правах и автоматически управляет доступом пользователей в соответствии с настроенными процессами.

Процессы в системе Solar inRights Origin могут быть полностью автоматическими, например, создание учетной записи при приеме на работу и блокировка при увольнении, или требовать участия сотрудников, например, согласование заявки на дополнительные права доступа. В рамках автоматизированных процессов система отправляет оповещения по электронной почте ответственным лицам о различных событиях.

Сотрудники взаимодействуют с системой через веб-приложение. Они могут использовать систему в соответствии со своими ролями и установленными разрешениями для управления доступом:

просматривать свои и чужие права, подавать заявки и проверять их статус, согласовывать заявки, получать отчёты, менять пароль, блокировать доступ и выполнять другие функции.

Рисунок 1. Схема работы Solar inRights Origin

4.3. Архитектура системы

Программный комплекс (ПК) Solar inRights Origin разработан на Java, работает на импортонезависимых операционных системах и построен с использованием клиент-серверной архитектуры и состоит из следующих компонентов:

- **Сервер приложений** – синхронизирует данные между inRights и подключенными системами, управляет выполнением фоновых задач, отправляет уведомления о событиях в исполняемых бизнес-процессах, предоставляет веб-интерфейс для использования и настройки системы;
- **Сервер коннекторов** – на сервере коннекторов развернуты коннекторы для взаимодействия с подключенными системами;
- **Реляционная СУБД** (PostgreSQL) – является хранилищем учетных данных, а также настроек системы;
- **Сервер конфигураций** – хранилище объектов конфигураций для интерфейса пользователя (далее WEB UI).

ПК Solar inRights взаимодействует:

- с подключенными системами: как с источником кадровых данных (система 1С ЗУП), так и с управляемыми системами (MS AD/Exchange);
- с SMTP-шлюзом для отправки уведомлений.

Схема архитектуры ПК Solar inRights Origin приведена на рисунке:

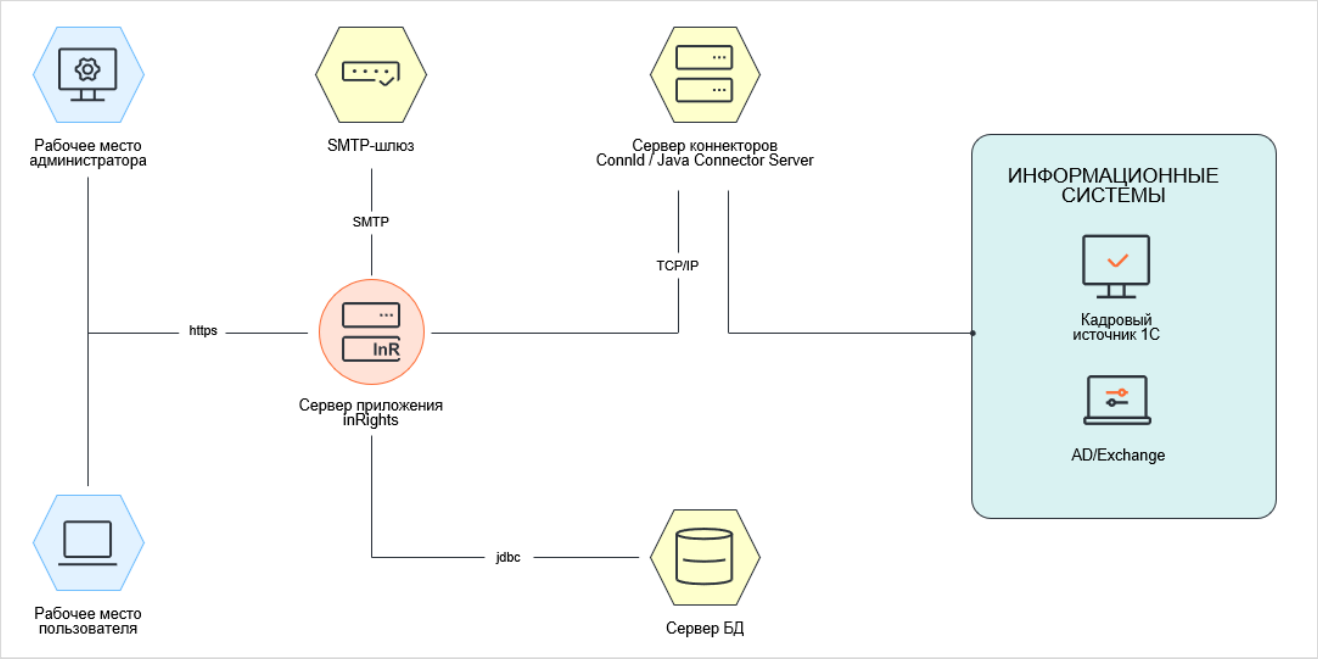

Рисунок 2. Архитектура ПК Solar inRights Origin

ПК Solar inRights Origin связывается с источником кадровых данных и управляемой информационной системой с помощью коннекторов – специальных модулей, которые являются каналами передачи данных. В общем случае коннектор – это независимый модуль, предоставляющий интерфейс определенного вида для доступа к функциям внешней системы.

Коннекторы разворачиваются на сервере коннекторов. Сервер коннекторов – это сервис, управляющий объектами управляемой системы (аккаунтами, полномочиями и т.п.) по запросам от ПК Solar inRights Origin.

Настройка взаимодействия Solar inRights Origin с внешними информационными системами заказчика требует определенной подготовки этих систем к взаимодействию, описанному в «Требованиях для интеграции с inRights Origin». Данный документ входит в комплект поставки решения. Подготовка систем не является сложным процессом и занимает относительно немного времени. Часть требований должна быть реализована вручную, в то время как другая часть может быть выполнена автоматически посредством установки расширений, например, для системы 1С.

4.4. Объекты системы

Все данные и метаданные, с которыми работает inRights, являются объектами разных типов. Часть объектов выполняют служебные функции (например, описание маршрута согласования), другие являются проекциями объектов, получаемых из внешних информационных систем, или представляют собой данные, с которыми работает inRights (пользователи, подразделения, роли и др.). Объекты хранятся в базе данных, их можно экспортировать и импортировать в виде XML-документов.

Основными объектами в inRights являются:

- Конфигурация системы – совокупность параметров работы системы;
- Ресурс (информационная система) – профиль информационной системы;

- Шаблон объекта – описание правил жизненного цикла объекта;
- Ресурсный объект – образ объекта, полученного из внешней системы через коннектор;
- Пользователь (сотрудник) – профиль пользователя с информацией о сотруднике, его аккаунтах в информационных системах (ИС) компании и его ролях;
- Роль – набор прав доступа, который назначается пользователю, в результате чего пользователь получает полномочия на выполнение некоторых действий;
- Подразделение – структурная единица организации, может объединять внутри себя другие структурные единицы;
- Должность – сущность (штатная позиция), которая связана с подразделением;
- Место работы (трудоустройство) – сущность, которая хранит кадровую информацию о месте работы сотрудника, включая дату приема/увольнения и другие параметры. Одно трудоустройство может быть связано только с одним пользователем в Системе.

Одна из важных функций inRights – автоматическая синхронизация атрибутов между внутренними объектами системы и данными во внешних системах. Объекты, между которыми происходит автоматическая синхронизация: Пользователь, Роль, Подразделение, Должность и Место работы.

InRights получает данные из кадрового источника и управляемых систем по заданному расписанию. Настройки взаимодействия (параметры подключения, схемы данных, правила обработки этих данных, правила синхронизации) с конкретной системой задаются в inRights в XML-описании этой системы (ресурса).

В соответствии с заданными настройками, inRights преобразует полученные данные в специальную структуру – Ресурсный объект, что позволяет работать с объектами различных ИС в едином формате. В Ресурсном объекте хранятся атрибуты ресурса – общие унифицирующие и специальные, определяемые для каждого ресурса отдельно.

При передаче данных применяются специальные правила, которые настраиваются при описании ресурса. Эти правила задают соответствие между данными в inRights и данными в других системах. Если данные передаются из внешней системы в атрибуты объекта inRights, то используются правила переноса данных из Ресурсного объекта в атрибуты объекта inRights - входящие маппинги (inbound mapping). При обратной передаче используются правила переноса из объекта inRights в объект внешней системы - исходящие маппинги (outbound mapping).

Обработка данных объекта в самом inRights выполняется в соответствии с правилами, заданными в шаблоне объектов. Для различных видов объектов можно задать разные шаблоны, где описаны алгоритмы и правила обработки атрибутов объекта, которые будут применяться ко всем объектам одного вида.

Общий процесс взаимодействия inRights и ИС включает этапы:

1. Загрузка данных из систем-источников и преобразование полученной информации в формат Shadow.

2. Перенос данных из Shadow в атрибуты объекта inRights в соответствии с правилами inbound mapping.
3. Обработка данных объекта inRights в соответствии с правилами, заданными в шаблоне объектов.
4. Установление связей между объектами inRights и объектами управляемой системы. Например, установление связи конкретного объекта User с конкретной учётной записью в управляемой системе.
5. Перенос данных в соответствии с правилами outbound mapping и их преобразование в Shadow .
6. Загрузка данных из inRights в управляемую систему и реконсиляция данных (установка соответствия полномочий пользователей в inRights и управляемых системах).
7. Загрузка данных из управляемых систем и преобразование полученной информации в формат Shadow.
8. Перенос данных из Shadow в атрибуты объекта inRights в соответствии с правилами inbound mapping.

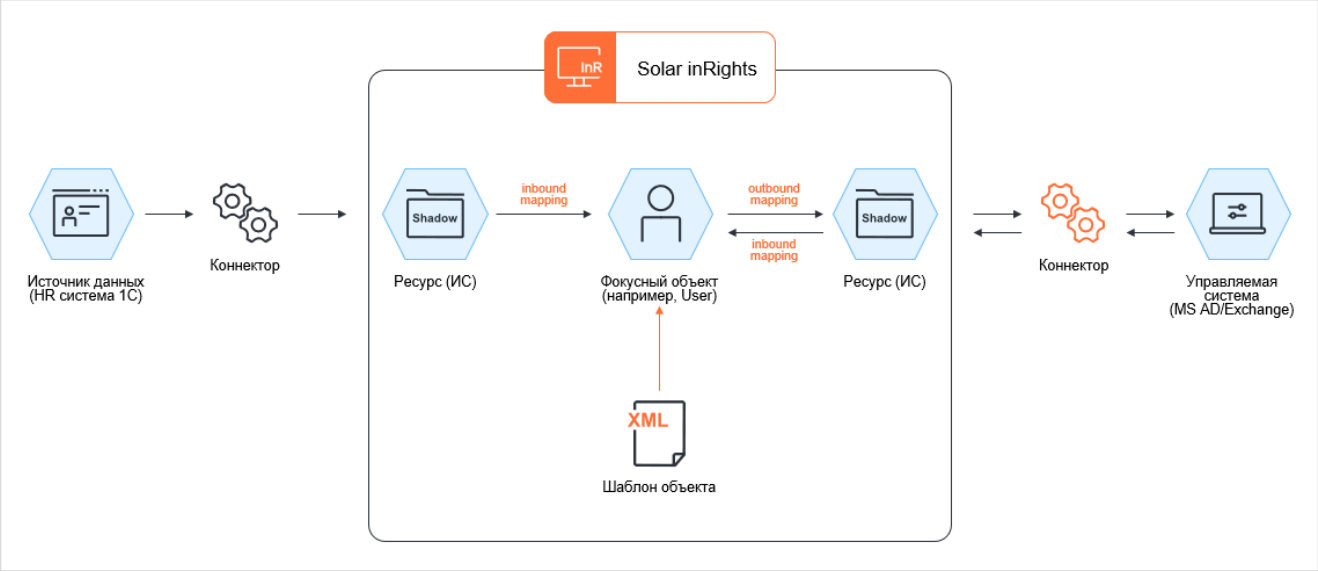

Рисунок 3. Схема процесса взаимодействия Solar inRights Origin с информационными системами

4.5. Требования для интеграции с системой Solar inRights Origin

Требования к аппаратному обеспечению

Для установки ПК предъявляются следующие требования к аппаратному обеспечению:

Роль	ОС	CPU, шт	RAM, GB	HDD, GB
Сервер приложений БД PostgreSQL Сервер коннекторов Коннектор к AD	Astra Linux 1.7 Ubuntu 20.04.2	4	24	50

Коннекторы к 1С				

Требования к кадровому источнику

Для обеспечения интеграции кадрового источника с Solar inRights Origin необходимо учитывать несколько критически важных требований:

- Система 1С должна быть не ниже версии 3.1 и включать ведение штатного расписания. Для указания Руководителей подразделений должна быть включена константа «Используется сервис кабинет сотрудника», которая позволяет редактировать Руководителя в карточке подразделения и сохранить связку подразделений и руководителей в регистр «Позиции руководителей (кадровых) подразделений».
- Для всех подразделений должен быть указан Руководитель.
- При увольнении или переводе руководителя подразделения должна указываться не вакантная должность, замещающая руководителя подразделения.
- Должно быть включено хранение истории изменений "При записи" для Организаций, Подразделений, Физических лиц и Штатного расписания.
- На конфигурацию 1С должно быть установлено функциональное расширение из комплекта поставки от Исполнителя, для публикации Web-сервисов интеграции с inRights Origin, либо расширение, реализующее аналогичные функции.
- Для успешной интеграции системы управления доступом с кадровым источником необходимо предусмотреть наличие REST API, поддерживающего обмен данными в формате JSON. Это условие позволяет обеспечить высокую степень совместимости и гибкости системы, значительно упрощая процесс интеграции. Следует отметить, что, по сравнению с интеграцией через протокол SOAP, REST API с JSON обеспечивает более легкий и эффективный обмен данными.

Требования к MS AD

Для успешной интеграции MS Active Directory (AD) с Solar inRights Origin должны быть учтены несколько ключевых требований, подробно описанных в документации к поставке решения:

- Должна быть создана доменная учетная запись idmadmin с правами на управление пользователями и группами, а также возможности сброса паролей.
- Необходимо настроить сетевые доступы для взаимодействия с контроллером домена и MS Exchange.
- Учетные записи должны быть корректно распределены по контейнерам, следуя заданной структуре OU, чтобы обеспечить правильность и удобство управления.
- Важно заполнить необходимые атрибуты для связывания учетных записей работников и контрагентов с их ФИО и кураторами.
- Группы безопасности должны быть логично организованы и находиться в соответствующем OU, чтобы их можно было использовать в inRights.

4.6. Автоматизация процессов

В системе Solar inRights Origin предусмотрены **следующие автоматические процессы управления доступом** на основании данных их кадрового источника:

- Приём на работу штатного сотрудника;
- Повторный прием на работу;
- Изменение данных о пользователе автоматическое;
- Перевод по должности;
- Отпуск;
- Декретный отпуск;
- Увольнение сотрудника с трудоустройства;
- Увольнение сотрудника из компании;
- Работа с организационно штатной структурой автоматически.

Решение позволяет автоматизировать **следующие ручные кадровые процессы** управления доступом:

- Прием на работу внештатного сотрудника;
- Изменение данных о пользователе вручную;
- Добавление трудоустройства вручную;
- Изменение трудоустройства;
- Работа с организационно штатной структурой вручную;

Система поддерживает **автоматизацию следующих процессов** по управлению доступом:

- Предоставление прав доступа;
- Согласование заявки;
- Смена пароля через inRights;
- Продление/сокращение сроков действия прав доступа;
- Отзыв прав доступа;
- Работа с нарушениями политик.

4.7. Функции системы

Solar inRights Origin в рамках своего назначения предоставляет следующие функции:

Управление данными о пользователях и их правах доступа:

- создание карточки пользователя и пользовательских УЗ в inRights;
- изменение информации о пользователе;
- блокировка/разблокировка пользовательских УЗ в inRights;
- создание/изменение пользовательских УЗ в Управляемых ИС;
- блокировка/разблокировка пользовательских УЗ в Управляемых ИС;
- связывание пользовательских УЗ с карточкой пользователя в inRights;

– назначение/изменение ролей;
– осуществление пересмотра набора назначенных пользователю ролей;

Управление назначениями ролей:

– ведение политик назначения ролей;
– продление/ограничение срока действия роли;
– управление функциональными ролями inRights;

Управление заявками:

– создание заявок различных типов;
– формирование маршрута согласования заявок;
– вычисление согласующих;
– делегирование полномочий на согласование заявок;

Предоставление возможности ручного ввода данных:

– регистрация и изменение данных внешних пользователей;
– ввод и изменение данных об организационных единицах;
– ввод и изменение данных о ролях и Управляемых ИС;
– предоставление сервиса самообслуживания пользователей.

4.8. Работа с системой

Система Solar inRights является универсальным решением для администрирования доступа, проведения аудита и контроля, а также для подачи и согласования заявок на предоставление полномочий, сброса или смены пароля и получения справочной информации об объектах доступа и статусе процессов.

Работа с системой Solar inRights Origin осуществляется через веб-интерфейс. Интерфейс разделен на навигационное меню и основную область, что облегчает работу с различными блоками системы. Через навигационное меню пользователи системы могут переходить к разным блокам для работы с различными объектами системы: пользователями, ролями, организационной структурой, каталогами ролей и другими.

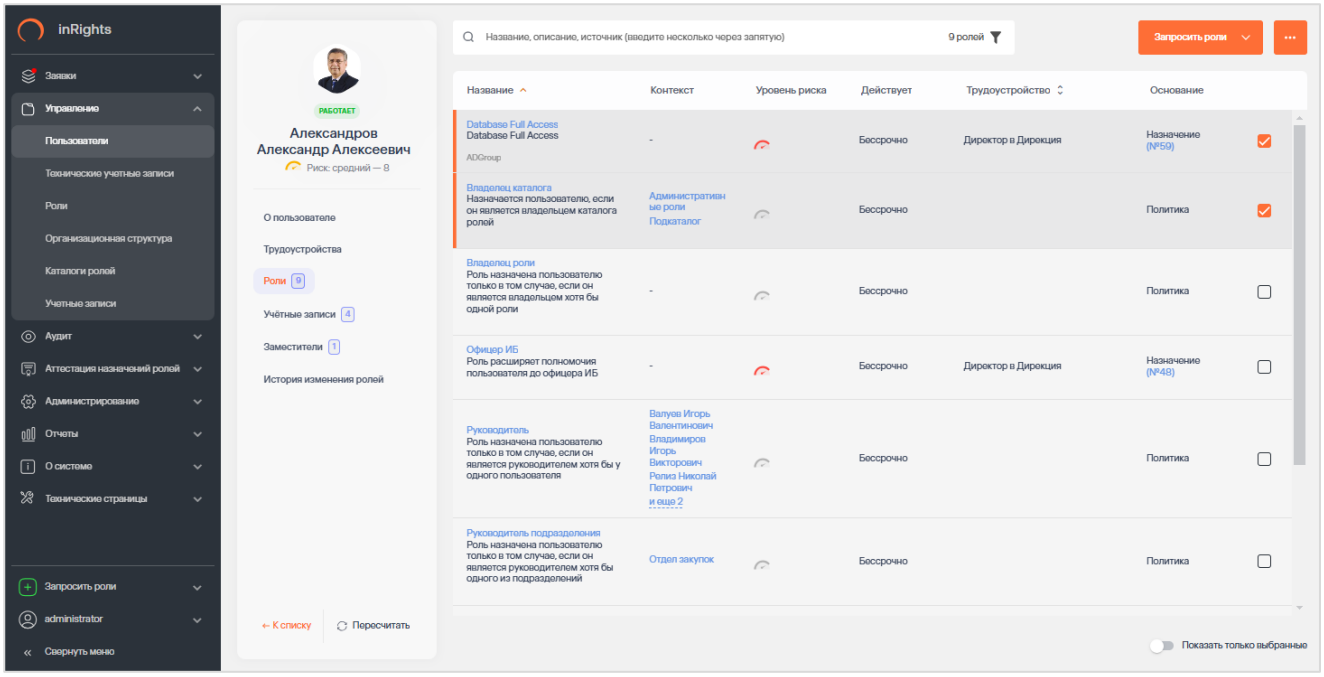

Рисунок 4. Работа с системой

Система предоставляет инструменты для создания, изменения и удаления учетных записей пользователей, включая сотрудников и контрагентов. Все действия фиксируются, что обеспечивает прозрачность процессов.

Решение поддерживает функцию самообслуживания, пользователи могут подавать заявки на изменения в правах доступа, проводить согласование заявок, а также получать актуальную информацию о ходе исполнения каждой заявки и историческую информацию об основаниях предоставления полномочий.

Solar inRights Origin предлагает механизмы для мониторинга прав доступа и отслеживания отклонений и нарушений, а также возможность проводить регулярные аудиты, обеспечивая соблюдение нормативных требований.

Стандартные отчеты системы помогают в получении консолидированной информации об учетных записях и ролях пользователей, об истории изменения ролей и оформленных заявках за определенный период времени. Оформление подписок на получение регулярных отчетов помогает контролирующим сотрудникам отслеживать динамику изменений и принимать обоснованные решения для защиты данных.

В системе применяется объектная модель, которая позволяет удобно работать с различными элементами: пользователями, учетными записями, ролями и каталогами. Каждая карточка объекта содержит подробную информацию о нем, включая атрибуты, характеристики и связи с другими объектами. Благодаря функции «Drill down» можно легко переходить от одного объекта к другому анализировать и исследовать данные на различных уровнях детализации для получения всей необходимой информации.

5. Лицензирование и ценообразование

1. Основная поставка:

- Программное обеспечение Solar inRights
- Лицензии на использование ПО Solar inRights для управления УЗ до 2 000 сотрудников (бессрочные)
- Лицензии на использование ПО Solar inRights для управления УЗ до 1 000 сотрудников (годовые)
- Преднастроенная конфигурация продукта
- Годовая подписка на Центр поддержки продукта Solar inRights Origin, который включает:
  - Базу знаний
  - Нейроконсультанта
  - Обновления программного продукта Solar inRights
  - Обновления коннекторов к ИС и конфигурации (-й)
  - Гарантийную поддержку – в первый год – бесплатно.

2. Дополнительные услуги

- Консультационное сопровождение внедрения
- Техническая поддержка (первый год 14 мес., последующие – 12 мес.)
- Расширение лицензии на 1000 пользователей
- Продление годовой подписки к Центру поддержки продукта Solar inRights Origin

6. Соответствие требованиям

Система Solar inRights Origin:

- Соответствует параметрам ГОСТ Р 71753-2024 «Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования». Приказ Росстандарта от 30 октября 2024 г. N 1558-ст;
- Внесена в Единый реестр отечественного ПО (запись 7759) и сертифицирована ФСТЭК России на соответствие требованиям по 4-му уровню доверия (сертификат №4633 от 27.12.2022);
- Соответствует требованиям 152-ФЗ, руководящих документов ФСТЭК и ФСБ, отраслевых стандартов СТО БР ИББС-1.0-2014, ГОСТ 57580.1, PCI DSS, ISO 27001.
- Полностью отечественная разработка и санкционно-независимое решение, поскольку способно функционировать в полностью импортозамещенной и сертифицированной ФСТЭК среде, включая ОС и СУБД.

7. Преимущества использования Solar inRights Origin

Быстрое внедрение

Solar inRights Origin может быть введена в эксплуатацию в течение 3-6 месяцев, что существенно быстрее, чем традиционные системы IdM/IGA.

Подход с низким порогом входа

Система требует минимальных затрат на прохождение обучения, ознакомление с документацией и может быть развернута одним инженером по инструкции, что делает её доступной для компаний с ограниченными ресурсами и бюджетом.

Снижение нагрузки на ИТ-подразделение

Автоматизация процессов управления доступом, упрощение подготовки данных для аудита, переход от лоскутной автоматизации и ручных процессов к единому централизованному решению, а также минимизация ошибок человеческого фактора.

Минимизация рисков ИБ

Полная картина прав доступа сотрудников к информационным системам, контроль соблюдения регламентов предоставления доступа и снижение числа инцидентов, связанных с избыточными полномочиями.

Сертификация и соответствие требованиям

ПК Solar inRights Origin сертифицирован ФСТЭК России и включен в реестр отечественного ПО, что подтверждает его надежность и соответствие законодательным требованиям.

Обучение и поддержка

Пользователи получают доступ к базе знаний с обучающими материалами и нейроконсультатну (чат-боту с функцией искусственного интеллекта), что способствует самостоятельному освоению системы, оперативному получению ответов на возникающие вопросы и дальнейшему развитию решения.

Интуитивно понятный интерфейс

Современный и дружелюбный интерфейс создан на основе передовых технологий и делает работу с системой комфортной и понятной для всех пользователей. Лёгкость использования и комфорт в работе обеспечиваются благодаря визуальным графическим инструментам для управления объектами, процессами и правилами.

Solar inRights Origin представляет собой решение для организаций, стремящихся автоматизировать процессы управления доступом, повысить безопасность и сократить затраты, тем самым способствуя созданию эффективной и безопасной бизнес-среды.

8. О компании ГК «СОЛАР»

Группа компаний «Солар» – ведущий поставщик решений кибербезопасности в России, архитектор комплексной кибербезопасности. Ключевые направления деятельности – аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солар» – 1 000 крупнейших компаний России. Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC – Solar JSOC, экосистему управляемых сервисов ИБ – Solar MSS.

Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, систему управления неструктурированными данными Solar DAG, анализатор кода Solar appScreener и другие. ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир».

Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности. Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Штат компании – более 2 000 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

9. Контактная информация

Телефоны:

+7 (499) 755-07-70 — продажи и общие вопросы

+7 (499) 755-02-20 — техническая поддержка

E-mail:

solar@rt-solar.ru — продажи и вопросы по сервису

support@rt-solar.ru — техническая поддержка

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Нижний Новгород, Казанское шоссе, 25, корпус 2
- Самара, Молодогвардейская ул., 204
- Ростов-на-Дону, Доломановский пер., 70Д
- Хабаровск, ул. Серышева, 56