

IDM. Управление учетными данными

презентация продукта



О КОМПАНИИ

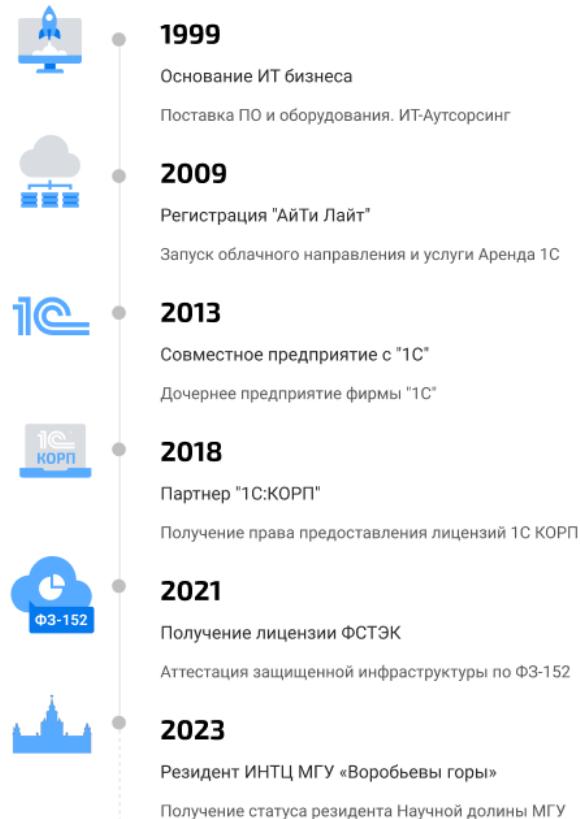
ООО «АйТи Лайт» основана в 1999 году как аутсорсинговая ИТ-компания. С 2009 года в числе первых в России начали работать как облачный провайдер услуг.

Дочернее предприятие «1С» с 2013 года. В настоящее время - стабильно развивающаяся ИТ-компания с филиальной сетью в нескольких городах России и стран СНГ.

Отказоустойчивая инфраструктура построена на базе двух геораспределенных Дата-центров класса TierIII, связанных двумя каналами и проложенными по выделенным оптическим кабелям разными маршрутами. Более 20 операторов связи, ключевой узел MSK-IX, волокна до ММТС-9 и ММТС-10.

Основные направления деятельности:

- проекты внедрения и сопровождения 1С, заказная разработка
- создание, аренда, поддержка ИТ-инфраструктур предприятий
- аренда выделенных и виртуальных серверов, частного облака, IaaS, SaaS
- аренда и хостинг 1С, включая лицензии ERP, КОРП
- корпоративная почта в облаке, резервное копирование как сервис
- круглосуточная ИТ поддержка, аутсорсинг 1-3 линий поддержки.



Identity Management - это

Identity Management (IDM) – комплекс подходов, практик, технологий и специальных программных средств для управления учётными данными пользователей с целью повышения безопасности и производительности информационных систем при одновременном снижении затрат, оптимизации времени простоя и сокращения количества повторяющихся задач.

Система «**IDM.Управление учётными данными**» на платформе "1С:Предприятие 8" – это инструмент, позволяющий реализовать данный класс задач на программном уровне.

Это система для автоматизации процессов централизованного управления учётными записями и правами пользователей, которая решает следующие основные задачи:



централизованное управление правами в информационных системах предприятия



автоматизация процессов по созданию учётных записей и предоставлению прав доступа в различные системы; процессов согласования и исполнения заявок



учет и контроль прав и доступов всех пользователей предприятия

Проблематика и предпосылки к внедрению

Сотрудники пользуются ИС и приложениями различного класса: почта, базы 1С, CRM, документооборот, корп. портал, АБС, service desk, СКУД, телефония и прочими.

Управление пользователями и их правами в системах **не централизовано и не автоматизировано**.

Ручное управление - **трудозатратно и неоперативно**; является источником ошибок, издержек и рисков информационной безопасности.

Поскучная автоматизация покрывает не все процессы, не отвечает требованиям бизнеса и ИБ.

Возникают **издержки на ФОТ, ошибки** в выдаче доступов.

Между ИБ и ИТ нет согласованности, самостоятельности служб.

Большие риски информационной безопасности.

Типичные вопросы, требующие решения

Пользователи (потребители услуги):

- Почему так долго? Срочно нужен доступ!
- Как запросить доступ к ИТ-системе?
- Как запросить доступ к ИТ-системе для моего сотрудника?
- Кто должен согласовать доступ?
- Почему не прошло согласование?
- Когда доступ будет предоставлен?

ИТ-служба (исполнитель услуги):

- Кто может запросить изменение доступа?
- Кто утверждает доступ в эту систему? На основании чего?
- Как гарантировать время выполнения запросов?
- Предоставление прав к ИТ-системам требует всё больше и больше времени. Как обосновать очередное увеличение штата?
- Никто заранее не информирует о новых сотрудниках, перемещениях, увольнениях.

ИБ-служба (контролер услуги):

- Кто отвечает за доступ к этой системе?
- Кто предоставил доступ к этой системе этому пользователю? Когда, на основании чего?
- Как избавиться от лишних активных учётных записей?
- Сколько у нас устаревших неиспользуемых, но активных учётных записей?
- Действительно ли этим пользователям нужны такие широкие права?
- Отзыв прав доступа занимает слишком много времени.

Ущерб бизнесу

Отсутствие автоматизации управления правами доступа ведет к следующим проблемам:

Пользователи:

- **медленное исполнение заявок** на изменение прав, предоставления доступа – простой сотрудников и бизнес-процессов
- **вовремя не отзываются права** у бывших сотрудников, не блокируются УЗ
- **беспорядок в учёте** - данные неактуальны, не синхронизированы. Отсутствие единой, актуальной базы учета пользователей и УЗ ведет к недостоверности информации, ошибкам, появлению уязвимостей.

ИТ-служба:

- **большой поток заявок**, связанных с правами и доступами – ручная работа
- **беспорядок в управлении** - непонятно, кому какие права нужны, с кем должно быть согласовано; невозможность быстро определить, куда имеет доступ конкретный сотрудник. Невозможность отследить, на основании чего и когда выданы права
- **отсутствие сквозного процесса** влечет множество ошибок.

ИБ-служба:

- **нет инструмента** для прямого исполнения функции ИБ, отсутствие самостоятельности службы
- **сложно предотвращать** и расследовать инциденты - нет мониторинга, контроля и учета
- **риски**: уволенные сотрудники имеют доступ к системам и данным; сотрудники имеют избыточные права; утечки конфиденциальных и корпоративных данных из-за несанкционированного доступа.

Угрозы безопасности



Незаблокированные учетные записи
ушедших сотрудников – “дыра” в безопасности компании. При увольнении сотрудников заявки на блокировку долго исполняются, УЗ остаются активными – это риски кражи, утечки, потери данных, нарушения работы систем.



Отсутствие или невыполнение регламентов безопасности
в части прав доступа. Помимо рисков ИБ это невыполнение требований регуляторов и, как следствие, штрафы/лишение лицензий – финансовые убытки и риски для бизнеса.

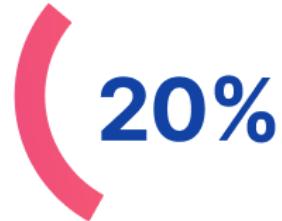


Накопление излишних прав
при кадровых переводах, выдаче временных доступов. Угрозы ИБ: неправомерное использование доступа; получение доступа и т.д.



Отсутствие механизма контроля прав
служба ИБ не имеет инструмента для предотвращения инцидентов, а также их оперативного расследования. Отсутствует контроль и мониторинг над выданными доступами и правами.

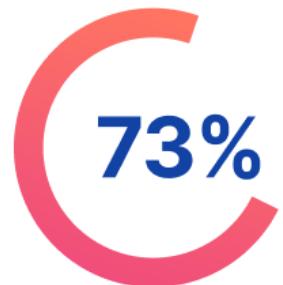
Актуальность проблемы



более 20% инцидентов
кибербезопасности связаны
с нарушениями доступа



в 50% компаний у
уволившихся сотрудников
сохраняются доступы к
внутренним системам



компаний регистрируют у
себя случаи нарушений прав
доступа



случаев - нарушение доступа
приводят к утечке
конфиденциальной
информации компаний

Целевая аудитория продукта

Независимо от отрасли, целевая аудитория внедрения системы IDM:

1. Крупные компании

Большое количество сотрудников часто сопровождается беспорядком в управлении их правами, а ручное управление приводит к высоким накладным расходам.

2. Компании с большим количеством ИС

Вне зависимости от количества сотрудников, большое количество информационных систем, баз 1С также вызывает проблемы в оперативном управлении и влечет соответствующие риски.

3. Малые-средние компании, от 200 сотрудников

Проблема учета и оперативного управления правами пользователей в ИС стоит даже в средних и малых компаниях. Зачастую последствия ручного управления для их бизнеса оказываются еще критичнее.

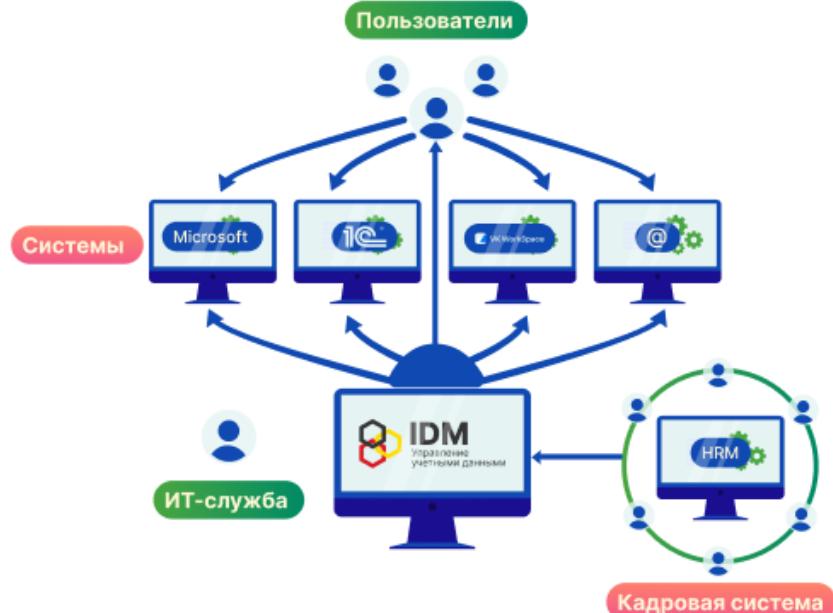


Как работает IDM

Работая под управлением "1С:Предприятие", система IDM.Управление учетными данными:

1. **получает данные** по сотрудникам предприятия из кадровой системы - например, 1С:ЗУП
2. **интегрируется** с имеющимися на предприятии информационными системами и приложениями
3. **изменяет права доступа** и настройки учетных записей в целевых системах на основании кадровых событий и ролевой модели на предприятии
4. **формирует пул задач** на согласование и изменение прав. Оповещает пользователей по email, sms
5. **предоставляет инструмент контроля**, мониторинга и предотвращения инцидентов для службы ИБ.

Система автоматически мониторит данные по правам и учетным записям в системах предприятия, фиксирует любые несоответствия в выданных правах, позволяет расследовать причины расхождений и принять решение об изменениях.



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

| Интеграция | Автоматизация процессов | Централизованное управление | Учет и контроль |
|---|---|---|---|
| <p>1. Коннекторы:</p> <ul style="list-style-type: none"> • Active Directory, Open LDAP • 1С приложения • Битрикс-24, 1С-Битрикс • MS Exchange, Яндекс 360, VK WorkSpace • IP ATC 3CX • Универсальный HTTP-коннектор <p>2. Взаимодействие через веб-сервисы, API, PowerShell.</p> <p>3. Работа коннекторов 1С через 1С:Шина.</p> <p>4. Синхронизация с кадровыми и целевыми системами в автоматическом режиме.</p> <p>5. «Автономные приложения» - управление правами доступа к целевой системе, для которой отсутствует прямое физическое подключение.</p> <p>6. Универсальный шаблон коннектора для самостоятельной настройки к другим ИС.</p> | <p>1. Бизнес-процессы: управление УЗ пользователей, правами, организационной структурой, ролевой моделью предоставления прав и другие.</p> <p>2. Автоматическое создание, блокировка, удаление УЗ на основе кадровой информации и событий. Обработка нескольких одновременных кадровых событий.</p> <p>3. Настройка реакции на кадровые события по смене рабочего статуса пользователя (прием, увольнение, отпуск), переводу в орг. структуре.</p> <p>4. Последовательное, параллельное согласование. Настройка бизнес-процессов согласования заявок. Согласование заявок по e-mail.</p> <p>5. Автоматическое создание и сопоставление в IDM подразделений по кадровой базе.</p> <p>6. Оповещения по событиям через e-mail/ SMS, например, «Создание учетной записи», «Предоставление права» и т.д.</p> <p>7. Управление парольными политиками. Заявки на изменение/сброс пароля.</p> | <p>1. Ролевая модель доступа: автоматическое назначение прав доступа пользователям на основании формальных признаков («место работы», «подразделение» и др.). Функционал настройки ролевой модели.</p> <p>2. Пересмотр прав пользователей по ролевой модели. Пересмотр ролевой модели в IDM.</p> <p>3. Управление привилегированными правами и УЗ.</p> <p>4. Управление заявками на доступ разных типов, отзыв прав, блокировка и разблокировка учетных записей.</p> <p>5. Заявки на временный доступ, доступ внештатных сотрудников.</p> <p>6. Разграничение видимости прав для различных групп пользователей.</p> <p>7. Рабочий стол руководителя с возможностью просмотра и изменения прав доступа сотрудников.</p> <p>8. Рабочий стол пользователя с возможностью создания заявки на доступ и просмотра своих прав.</p> <p>9. Сканер общих папок и доступа к ним.</p> | <p>1. Выполнение аудита учетных записей и прав доступа пользователей в целевых системах с автоматической либо ручной обработкой обнаруженных расхождений в IDM.</p> <p>2. Обновление свойств учетных записей при изменении кадровой информации.</p> <p>3. Система отчетности, история обработки всех заявок, история изменения доступов пользователей.</p> <p>4. Реализована штатная возможность создания новых отчетов без программирования.</p> <p>5. Управление SOD-рисками, установка несовместимых прав.</p> |

Процесс Управления доступом по ITIL

Управление доступом (Access Management) - процесс, отвечающий за допуск пользователей к использованию услуг, данных или других активов.

Управление доступом помогает обеспечить конфиденциальность, целостность и доступность активов за счет того, что только авторизованные пользователи имеют возможность получить доступ.

Назначение процесса:

- обеспечить право пользователей на доступ к сервисам
- деятельность процесса реализует на операционном уровне требования политик безопасности и доступности.

Задачи процесса:

Соблюдение политик

Управление доступом к услугам на основе политик и мер, определенных Управлением ИБ.

Эффективное выполнение

Эффективное выполнение запросов на предоставление, изменение или ограничение прав доступа к услугам.

Надзор за доступом

Надзор за доступом и обеспечение правомерности доступа к услугам.

Типовые услуги и процессы

1. Процессы управления

| | |
|------------------------|--|
| Предоставление доступа | Предоставление доступа пользователю к ИС с необходимым набором прав. Ручное предоставление доступа, автоматическое предоставление доступа по событию. |
| Отключение доступа | Автоматическое и ручное отключение доступа пользователя к ИС. Блокирование учетной записи. |
| Изменение доступа | Изменение прав доступа пользователя в ИС в рамках существующих ролей и наборов прав. |
| Создание обращений | Создание заявки на доступ, просмотр своих прав во всех ИС. |
| Управление обращениями | Управление заявками на доступ разных типов: блокировка-разблокировка, отозвать-предоставить право, делегирование, прием-увольнение внешнего сотрудника, смена ФИО. Процессы согласования выдачи прав. |

2. Процессы мониторинга

| | |
|---------------------------|---|
| Мониторинг прав доступа | Выявление нетиповых доступов. Аудит учетных записей и прав доступа пользователей в целевых системах с автоматической либо ручной обработкой обнаруженных расхождений. |
| Предоставление отчетности | Система отчетности, история обработки всех заявок, история изменения доступов пользователей. |

3. Процессы расследования

| | |
|--------------------------------------|---|
| Расследование, диагностика, аудит ИБ | Расследование инцидентов, связанных с: неправомерным получением доступа, кражей/утечкой данных, нарушением работоспособности систем. Обнаружение и устранение причин и последствий инцидента. Инструменты системы: логирование, аудит УЗ, отчетность, настройка прав доступа, настройка процессов согласований предоставления прав. |
|--------------------------------------|---|

Примеры сценариев работы IDM

| Сценарий | Автоматизация в IDM |
|--|---|
| Прием сотрудника на работу | IDM создала учетные записи, выдала права в соответствующих системах, отправила сотруднику sms / email с доступом. |
| Сотрудник сменил должность | IDM создала заявки на изменение прав. Заявки пошли по маршруту согласования руководителям. |
| Отпуск, больничный, командировка | Механизм делегирования и наследования прав. Замещающий сотрудник получает необходимые права и доступы. |
| Сотрудник запросил доступ / права. Заявку согласовали | Выдача доступа, прав по заявке. Отзыв по истечению срока действия. |
| Обработка расхождений | Отчет, показывающий найденные расхождения. Автоматическое устранение несоответствия в правах либо после согласования по маршруту. |
| Сотрудник получил права в обход IDM | Система оповестила / исправила. |
| Потеря корпоративных данных, спорные ситуации, требующие расследования ИБ. | Журнал регистрации действий, показывающий, когда и какой пользователь получил те или иные права в соответствующей системе. |
| Увольнение сотрудника | IDM заблокировала и отозвала все права. |

Внедрение продукта

В ходе проекта внедрения разворачивается **тестовый контур**, производится загрузка данных из учетных систем, оценка актуальности и качества данных по сотрудникам, **сопоставление** учетных записей и пользователей.

Обнаруженные в кадровых системах **коллизии устраняются**. Вырабатывается единая стратегия по нормализации данных во всех системах предприятия.

В ходе тестирования проверяются **основные процессы**: прием на работу сотрудника в кадровой системе, кадровый перевод, увольнение, смена ФИО, временное предоставление-отзыв прав сотрудника, предоставление прав внешним сотрудникам, процесс согласования изменения права, отражение в отчетах всех изменений по правам.

Производится **анализ существующих целевых систем**, с которыми будет взаимодействовать IDM; анализ инструментов по загрузке данных в IDM. При необходимости разрабатываются дополнительные коннекторы к внешним ИС.



Разработка ролевой модели

Разработка и внедрение ролевой модели в рамках задачи внедрения IDM – это определение и регламентирование **набора типовых полномочий** для групп пользователей с последующим применением модели в рамках инструментария ИС.

Цель – формализация и автоматизация; упрощение и ускорение выдачи прав.

1. Определение функциональных ролей, групп пользователей; набора прав в каждой из целевых ИС.
2. Разработка правил, процедур, процессов. Создание типовых прав для групп пользователей.
3. Масштабирование, внедрение единых бизнес-ролей в ИС для должностей и подразделений по штатной структуре.

Роль – совокупность прав и доступов для выполнения сотрудником своих функциональных обязанностей.

Ролевая модель - совокупность ролей сотрудников компании, позволяющая эффективно выполнять свою роль каждому сотруднику.



Варианты внедрения

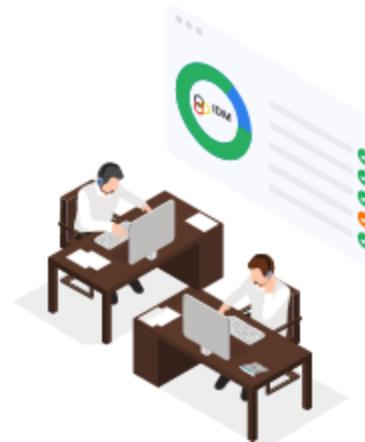
Внедрение продукта возможно реализовать с любой степенью вовлеченности заказчика:

| | | |
|---|---|--|
| 1 | Внедрение “под ключ”: минимальное вовлечение заказчика | <p>Все работы выполняются исполнителем: написание ТЗ, тестовая выгрузка, анализ и нормализация данных, НСИ и т.д. Ресурсы заказчика привлекаются в минимально-необходимом объеме.</p> |
| 2 | Самостоятельное внедрение: максимальное вовлечение заказчика | <p>Подходит при наличии у заказчика соответствующих ресурсов. Заказчик совместно с исполнителем проходит все этапы внедрения на тестовой среде. В рабочем контуре системы заказчик выполняет работы самостоятельно с консультациями исполнителя.</p> <p>Исполнитель предоставляет методики и рекомендации, оказывает полную консультационную и техническую поддержку (возможность работы “по часам”).</p> |

Сопровождение продукта

В рамках сопровождения продукта оказываются следующие услуги:

1. Консультации, поддержка пользователей
2. Обновления продукта и поддержка их развертывания
3. Развитие функциональности продукта
4. Обучение. Типовые курсы для пользователей и администраторов
5. Добавление новых пользователей, расширение пакета лицензий.



Интерфейс сотрудника

Процессы создания и управления обращениями.

Максимально привычный и интуитивно понятный интерфейс 1С.

1С [КОПИЯ] IDM.Управление учетными данными, ред. 2.0 (1С.Предприятие)

Поле поиска: Пойск Ctrl+Shift+F

Справка: ? Администратор: Администратор

Меню: Главное, Система, Предприятие, Ролевая модель, Учетные данные, Администрирование

Мои права (активирован):

- Логин: S.Bodrov
- Приложение: Active Directory (основной домен)
- Логин: S.Bodrov@test.int
- Приложение: MS Exchange
- Логин: Администратор
- Приложение: IDM: Управление учетными данными
- Логин: Сергей Бодров
- Приложение: Управление торговлей 11
- Логин: Сергей Бодров(Системный администратор)
- Приложение: Зарплата и управление персоналом 3
- Логин: Сергей Бодров(Системный администратор)
- Приложение: Бухгалтерия 3

Мои задачи (0):

Мои заявки:

Новая заявка:

Админ. системы:

Права доступа (активирован):

- Право: CN=Администраторы схемы
- Право: CN=Администраторы предприятия
- Право: CN=Администраторы домена
- Право: CN=Пользователи домена
- Право: IDM: Управление учетными данными
- Право: Открытие внешних отчетов и обработок
- Право: Администраторы
- Право: Бухгалтерия 3
- Право: Администраторы
- Право: Зарплата и управление персоналом 3
- Право: Открытие внешних отчетов и обработок
- Право: Обмен с "1С.IDM"
- Право: Администраторы
- Право: Управление торговлей 11
- Право: Открытие внешних отчетов и обработок
- Право: Администраторы

Учетные записи:

- Добавить
- Сменить имя
- Разблокировать
- Блокировать

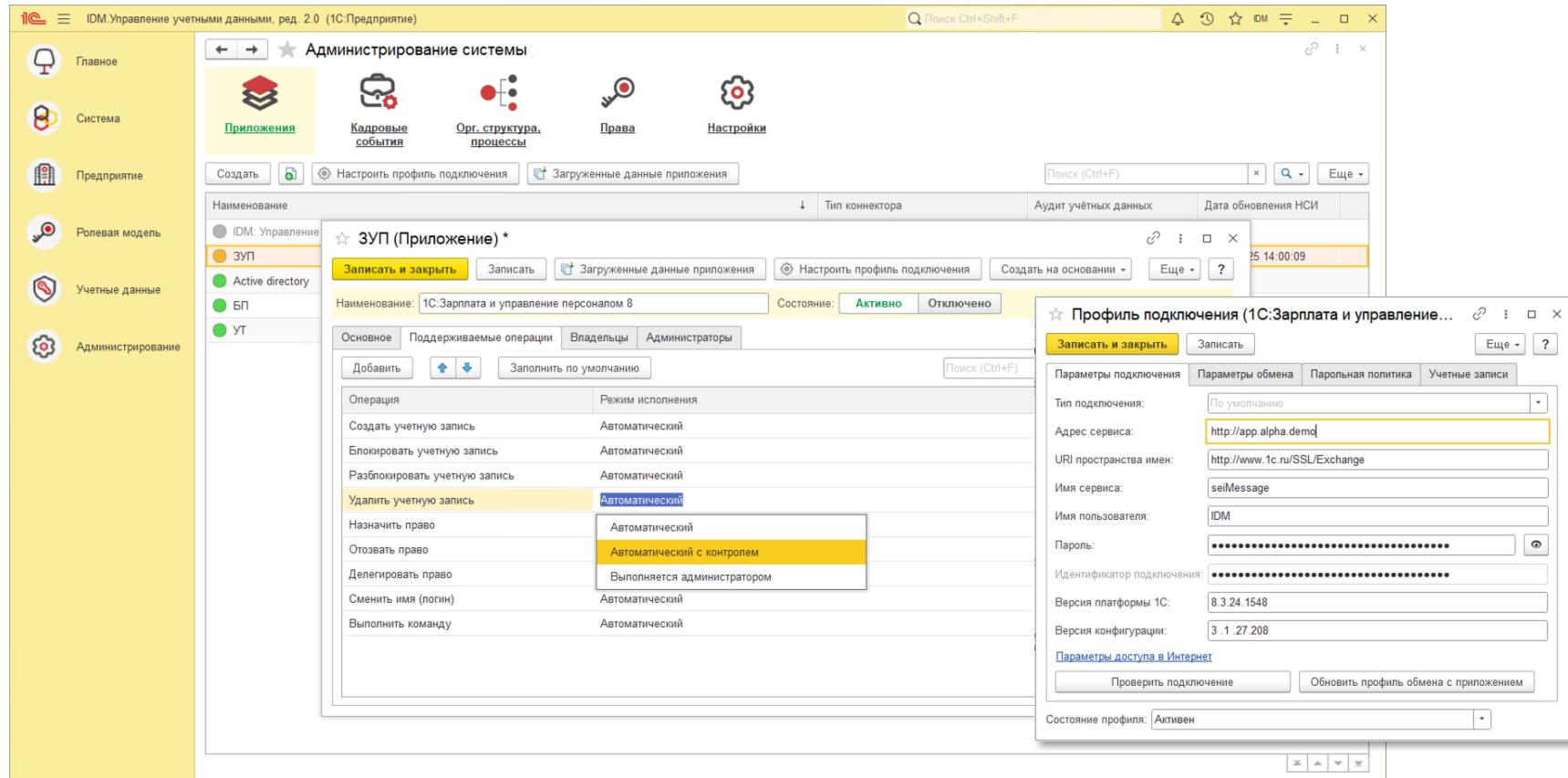
Внешние сотрудники:

- Приём сотрудника
- Увольнение сотрудника

Панель навигации: Начальная страница

Администрирование

Настройки администрирования. Управляемые ИС, статусы, подключение новых систем.



1C IDM Управление учетными данными, ред. 2.0 (1С:Предприятие)

Поиск Ctrl+Shift+F IDM

Администрирование системы

Приложения Кадровые события Орг. структура, процессы Права Настройки

Создать Настроить профиль подключения Загруженные данные приложения

Наименование Тип коннектора Аудит учётных данных Дата обновления НСИ

ЗУП (Приложение) * Тип коннектора: Аудит учётных данных НСИ Дата обновления: 25.14:00:09

Записать и закрыть Записать Загруженные данные приложения Настроить профиль подключения Создать на основании Еще ?

Наименование: 1С:Зарплата и управление персоналом 8 Состояние: Активно Отключено

Основное Поддерживаемые операции Владельцы Администраторы

Добавить ↑ ↓ Заполнить по умолчанию Поиск (Ctrl+F)

Операция Режим исполнения

Создать учетную запись Автоматический

Блокировать учетную запись Автоматический

Разблокировать учетную запись Автоматический

Удалить учетную запись Автоматический

Назначить право Автоматический

Отозвать право Автоматический с контролем

Делегировать право Выполняется администратором

Сменить имя (логин) Автоматический

Выполнить команду Автоматический

Параметры подключения Параметры обмена Парольная политика Учетные записи

Тип подключения: По умолчанию Адрес сервиса: http://app.alpha.demo/

URI пространства имен: http://www.1c.ru/SSL/Exchange Имя сервиса: seiMessage

Имя пользователя: IDM Пароль: *****

Идентификатор подключения: ***** Версия платформы 1С: 8.3.24.1548

Версия конфигурации: 3.1.27.208 Параметры доступа в Интернет

Проверить подключение Обновить профиль обмена с приложением

Состояние профиля: Активен

Коннекторы к целевым системам и приложениям

Кроме коннекторов, идущих в поставке, а также в новых релизах системы – доступна работа с Автономными приложениями (управление правами в целевых системах, программная интеграция с которыми отсутствует).

Возможность самостоятельной настройки коннектора к другим ИС (шаблон коннектора).

Администрирование системы

Приложения **Кадровые события** **Орг. структура, процессы** **Права**

Настройки

Приложение (создание) *

Записать и закрыть **Записать** **Загруженные данные приложения** **Настроить профиль подключения** **Создать на основании** **Еще** **?**

Наименование: **СКУД** Состояние: **Активно** **Отключено**

Основное **Поддерживаемые операции** **Владельцы** **Администраторы**

Тип коннектора:

Правило формирования имен учетных записей:

Приложение зависимости учетной записи:

Приложение корпоративной почты

Если настройка активна, то при оповещениях сотрудникам использоваться учётная запись этого приложения.

Автономное приложение

Выбрать из списка

Active directory
MS Exchange server
Универсальный HTTP
1C
Open LDAP
Почта VK WorkSpace
Автономное приложение
ATC ЗСХ
Битрикс
Яндекс360

| Наименование | Тип коннектора | Последнее обновление |
|-------------------------------|-----------------------|----------------------|
| IDM: Управление учетными д... | 1C | 09.01.2025 17:03 |
| ЗУП | 1C | |
| Active Directory | Active directory | 09.01.2025 17:03 |
| MS Exchange | MS Exchange server | |
| Open LDAP | Open LDAP | |
| Битрикс 24 | Битрикс | |
| ВК корпоративная почта | Почта VK WorkSpace | 09.03.2025 23:17 |
| Корп-сайт на WordPress | Универсальный HTTP | |
| Управление торговлей 10.3 | 1C | |
| Устанавливаемые ПО (ручно... | Автономное приложение | |
| УТ 11 | 1C | |
| Яндекс 360 | Яндекс360 | 21.03.2025 15:46 |
| Зарплата и управление перс... | 1C | |

Загрузка первичных данных

Загрузка данных приложения происходит единожды после успешного подключения профиля приложения. В последующем - регулярными регламентными заданиями. Дальнейшее сопоставление учетных записей, должностей и подразделений.

Данные приложения ЗУП

Учетные записи Группы доступа Профили доступа Группы пользователей Организации Подразделения Должности Метаданные Первичная загрузка

Поиск (Ctrl+F) Ещё

| Логин | Сотрудник | Дата создания | Состояние |
|--|-----------|---------------------|-----------|
| АВ.Орлов | Орлов АВ | 23.11.2025 18:08:19 | Включена |
| Аристотель.Минчев | | | Включена |
| Борис.Федоров | | | Включена |
| Буллатов И.В. (Генеральный директор) | | | Включена |
| Громова Н.П. (Нач. отд. по работе с персоналом) | | | Включена |
| Г.С.Абрамов | | | Включена |
| Дмитрий.Боровой | | | Включена |
| Елена.Москальк | | | Включена |
| Елена.Симутина | | | Включена |
| Жанна.Работкина | | | Включена |
| Иван.Иванов | | | Включена |
| Лев.Гольд | | | Включена |
| Мария.Соловникова | | | Включена |
| Михаил.Соколов | | | Включена |
| Назар.Кураев | | | Включена |
| Наталья.Москаленко | | | Включена |
| Орлова Е.Н. (Нач. отд. расчетов по оплате труда) | | | Включена |
| ОтправкаСерверныхОповещений | | | Включена |
| Петр.Иванов | | | Включена |
| Савинская З.Ю. (Системный программист) | | | Включена |
| Светлана.Габровская | | | Включена |
| СлужебныйПользовательДляОбновленияПредставлени | | | Включена |

Загрузка первичных данных

Приложение: ЗУП Профиль подключения: http://app

Управление доступом

1. Загрузить роли доступа
2. Загрузить метаданные
3. Загрузить профили доступа
4. Загрузить учетные записи
5. Загрузить группы доступа
6. Загрузить группы пользователей

Данные приложения Active directory

Учетные записи Группы доступа Подразделения Первичная загрузка

Кадровый учет

1. Загрузить организации
2. Загрузить подразделения
3. Загрузить должности
4. Загрузить сотрудников

Первичная загрузка

Функция первичной загрузки данных в приложение предназначена для **разового** использования при инициализации данных из приложения. После загрузки первичных данных обмен должен происходить фоновой операцией **“Получение справочной и кадровой информации”**, а для обновления списка учётных записей и их прав необходимо включить фоновую операцию **“Аудит учётных данных в приложении”** и опцию аудита в самом приложении.

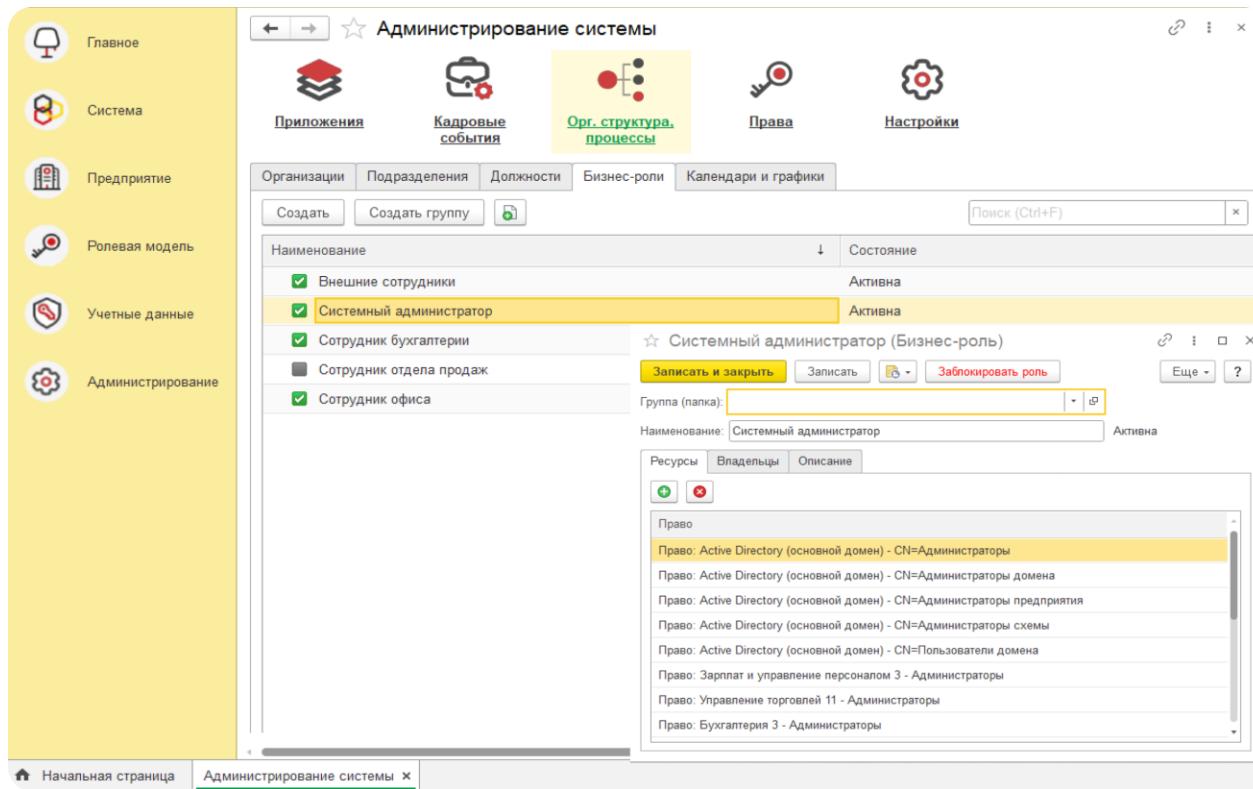
Перед загрузкой кадровых данных необходима **организации, подразделения и должности** с орг. структурой IDM. (Раздел **“Предприятие”** - **“Сервис”**)

5. Загрузить кадровые данные

Оргструктура и бизнес-роли

Настраивается орг. структура, должности, производственный календарь, бизнес-роли для назначения прав.

Бизнес-роль можно использовать в правилах автоматического назначения прав как для кадровых событий (прием на работу, кадровый перевод), так и для обычных заявок.



Администрирование системы

Приложения Кадровые события Орг. структура, процессы Права Настройки

Организации Подразделения Должности Бизнес-роли Календари и графики

Создать Создать группу Помощь Поиск (Ctrl+F)

Наименование Состояние

Внешние сотрудники Активна

Системный администратор Активна

Сотрудник бухгалтерии

Сотрудник отдела продаж

Сотрудник офиса

Системный администратор (Бизнес-роль)

Записать и закрыть Записать Заблокировать роль

Группа (папка):

Наименование: Системный администратор

Ресурсы Владельцы Описание

Право: Active Directory (основной домен) - CN=Администраторы

Право: Active Directory (основной домен) - CN=Администраторы домена

Право: Active Directory (основной домен) - CN=Администраторы предприятия

Право: Active Directory (основной домен) - CN=Администраторы схемы

Право: Active Directory (основной домен) - CN=Пользователи домена

Право: Зарплата и управление персоналом 3 - Администраторы

Право: Управление торговлей 11 - Администраторы

Право: Бухгалтерия 3 - Администраторы

Начальная страница Администрирование системы

Кадровые события

Настройка предназначена для создания правил обработки кадровых событий при импорте из кадровых систем: прием, увольнение, перевод, отпуск. Возможность создания новых правил.

Главное

Система

Предприятие

Ролевая модель

Учетные данные

Администрирование

Приложения

Кадровые события

Администрирование системы

Настройка кадрового события (создание)*

Записать и закрыть Записать

Наименование: Приём на работу главного бухгалтера Вкл Выкл

Вид события: Приём на работу Использовать ролевую модель

Условия Пра

Добавить новое

Поле

Отбор

Подразделение Равно

Должность Равно Главный бухгалтер

Сотрудник Равно

Приложение (Кадровая система) Равно

Организация Равно

Автор: Администратор Приоритет: 0

Настройка ролевой модели. Матрица легальных прав

Позволяет в том числе сформировать матрицу доступа на основе текущих выданных прав "как есть". Может являться основой для разработки/актуализации текущей модели, создания эталона ролевой модели; определения дополнительных, допустимых полномочий.

1C IDM Управление учетными данными, ред. 2.0 (1С:Предприятие)

Настраойка ролевой модели (создание)

Провести и закрыть Записать Провести Отчеты

Дата: 24.12.2025 0:00:00 Номер: Заполнить список:

Изменения прав Дополнительно

Добавить Добавить в документ Заполнить по текущим правам

| N | Операция | Организация | Подразделение |
|----|----------------|-------------|--|
| 3 | Добавить право | Крон-Ц | Отдел автоматизированных систем и сис... |
| 4 | Добавить право | Крон-Ц | Отдел автоматизированных систем и сис... |
| 5 | Добавить право | Крон-Ц | Отдел автоматизированных систем и сис... |
| 6 | Добавить право | Крон-Ц | Отдел по работе с персоналом |
| 7 | Добавить право | Крон-Ц | Отдел по работе с персоналом |
| 8 | Добавить право | Крон-Ц | Отдел по работе с персоналом |
| 9 | Добавить право | Крон-Ц | Отдел по работе с персоналом |
| 10 | Добавить право | Крон-Ц | Отдел поставки оборудования |
| 11 | Добавить право | Крон-Ц | Отдел поставки оборудования |
| 12 | Добавить право | Крон-Ц | Отдел поставки оборудования |
| 13 | Добавить право | Крон-Ц | Отдел поставки оборудования |
| 14 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 15 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 16 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 17 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 18 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 19 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 20 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 21 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 22 | Добавить право | Крон-Ц | Отдел продаж торгового направления |
| 23 | Добавить право | Крон-Ц | Отдел работы с дистрибуторами |

Заполнение по текущим правам

Перенести в документ Заполнить Печать Еще ?

Права Настройки Отбор (0)

Должности по подразделениям Кол. Сотрудники Кол. сотр. орг.

| Подразделение | Кол. Сотрудники | Кол. сотр. орг. |
|--|--------------------------------|-----------------|
| Крон-Ц | | |
| Отдел автоматизированных систем и сист... | | |
| Отдел по работе с персоналом | | |
| Отдел поставки оборудования | | |
| Отдел продаж торгового направления | | |
| Отдел работы с дистрибуторами | | |
| Отдел расчетов по оплате труда | | |
| Отдел установки и эксплуатации оборудов... | | |
| Руководство | | |
| Генеральный директор | 1 Булатов Игорь Виленович | 1 |
| Главный бухгалтер | 1 Боровой Дмитрий Валентинович | 1 |
| Active directory | 1 Боровой Дмитрий Валентинович | 1 |
| Пользователи | 1 Боровой Дмитрий Валентинович | 1 |
| БП | 1 Боровой Дмитрий Валентинович | 1 |

Выбрано прав для ролевой модели: 82

Руководитель отдела...

Руководитель отдела...

Руководитель отдела...

Руководитель отдела...

Руководитель отдела...

Начальник отдела

Сервис самообслуживания

Панель сотрудника позволяет:

- Просматривать актуальные статусы своих прав и учетных записей к системам
- Создавать новые заявки и контролировать их выполнение (приём/увольнение, согласование выдачи прав)

← → Бодров Сергей Иванович

Главное Система Предприятие Ролевая модель Учетные данные Администрирование Инструменты

Мои права Мои задачи (13) Мои заявки Новая заявка Админ. системы

Внимание В работе Мои Завершенные Отмененные Все Операция

Номер Дата ↑ Заявка Право Приложение Сотрудник Событие

| | | | | | | |
|-------------|---------------------|--|--------------------|-------------------|-------------------|------------------|
| 00000000816 | 22.12.2025 12:14:02 | Блокировать учетную запись №816 от 22 дека... | Зарплата и упра... | Зарплата и упр... | Цветочный Лют... | Событие 00000... |
| 00000000815 | 22.12.2025 12:14:02 | Отозвать право №815 от 22 декабря 2025 г. | Старшие расчет... | Зарплата и упр... | Цветочный Лют... | Событие 00000... |
| 00000000814 | 22.12.2025 12:14:01 | Назначить право №814 от 22 декабря 2025 г. | Казначеи | Управление тор... | Цветочный Лют... | Событие 00000... |
| 00000000813 | 22.12.2025 12:14:01 | Разблокировать учетную запись №813 от 22 де... | Управление тор... | Управление тор... | Цветочный Лют... | Событие 00000... |
| 00000000812 | 22.12.2025 11:13:09 | Блокировать учетную запись №812 от 22 дека... | Зарплата и упра... | Зарплата и упр... | Прелесть Натал... | Событие 00000... |
| 00000000811 | 22.12.2025 11:13:09 | Отозвать право №811 от 22 декабря 2025 г. | Старшие расчет... | Зарплата и упр... | Прелесть Натал... | Событие 00000... |
| 00000000810 | 22.12.2025 11:13:09 | Назначить право №810 от 22 декабря 2025 г. | Казначеи | Управление тор... | Прелесть Натал... | Событие 00000... |
| 00000000809 | 22.12.2025 11:13:08 | Разблокировать учетную запись №809 от 22 де... | Управление тор... | Управление тор... | Прелесть Натал... | Событие 00000... |
| 00000000805 | 17.12.2025 14:24:35 | Блокировать учетную запись №805 от 17 дека... | Управление тор... | Управление тор... | Мамалыга Над... | Событие 00000... |
| 00000000804 | 17.12.2025 14:24:34 | Отозвать право №804 от 17 декабря 2025 г. | Казначеи | Управление тор... | Мамалыга Над... | Событие 00000... |
| 00000000803 | 17.12.2025 13:50:50 | Отозвать право №803 от 17 декабря 2025 г. | Казначеи | Управление тор... | Маркиза Марфа... | Событие 00000... |
| 00000000801 | 17.12.2025 13:44:36 | Блокировать учетную запись №801 от 17 дека... | Зарплата и упра... | Зарплата и упр... | Маркиза Марфа... | Событие 00000... |
| 00000000569 | 11.12.2025 14:05:14 | Назначить право №569 от 11 декабря 2025 г. | Кассиры | Управление тор... | Казакова Натал... | |

Аудит и устранение коллизий

Настройка автоматической проверки прав с возможностью устранения выявленных несоответствий и прав, полученных в обход IDM.

★ Active Directory (основной домен) (Приложение)

Записать и закрыть Записать Загруженные данные приложения Настроить профиль подключения Создать на основании

Наименование: Active Directory (основной домен) Состояние: Активно Отключено

Основное Поддерживаемые операции Владельцы Администраторы

Тип коннектора: Active directory

Правило формирования имен учетных записей: Лев([Имя],1) + "." + [Фамилия]
Имена учетных записей формируются латиницей

Правило формирования полных имен учетных записей: [ФИО]

Правило формирования UPN-суффикса: Если [Организация ИдентификаторВПриложении] = "781a"

Приложение зависимости учетной записи:

Приложение корпоративной почты
Если настройка активна, то при оповещениях сотрудников будет использоваться учётная запись этого приложения.

Аудит учетных данных
При включенной настройке будет производиться поиск и устранение расхождений в учетных данных и их правах в IDM и приложении. Аудит не производится.

[Правила установлены](#) [Расписание по умолчанию](#)

Настройка правил устранения коллизий

Сохранить и закрыть Отмена

Правила учетной записи:

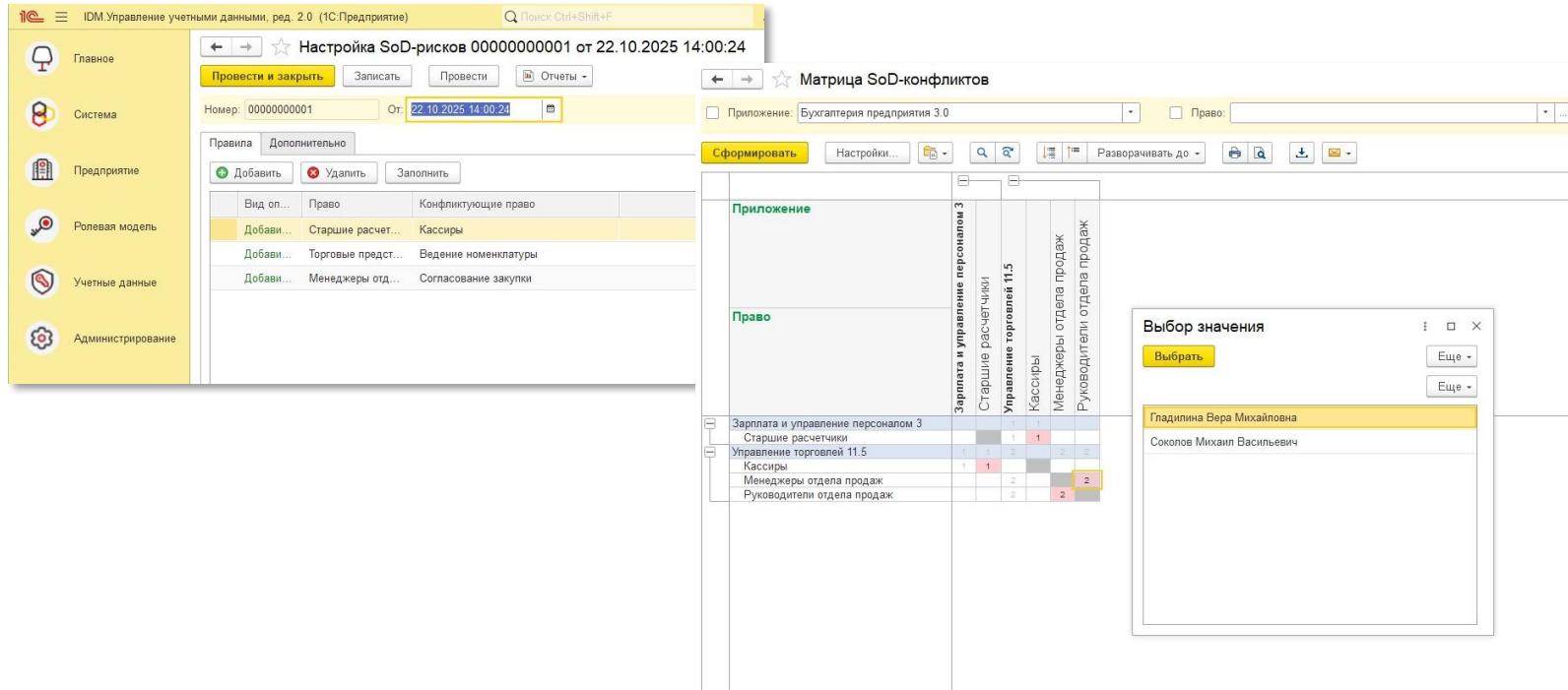
| Статус данных | Режим и способ устранения коллизий |
|------------------------------------|---|
| Новый в IDM | Автоматический Привести в соответствие с приложением |
| Зарегистрирован в IDM и приложении | Автоматический Привести в соответствие с IDM |
| Удален в приложении | Выполняется администратором |

Правила права:

| Статус данных | Режим и способ устранения коллизий |
|------------------------------------|---|
| Новый в IDM | Автоматический Отозвать право |
| Зарегистрирован в IDM и приложении | Автоматический Привести в соответствие с приложением |

Матрица SoD-конфликтов

SoD-конфликты (Separation of Duties, разделение обязанностей) — это риски безопасности в ИС, возникающие, когда одному пользователю предоставляются права для выполнения нескольких критических этапов одной бизнес-операции, что позволяет ему совершить мошенничество или ошибку (например, создать и утвердить платеж).



The screenshot displays the IDM (Управление учетными данными) software interface, specifically the 'Настройка SoD-рисков' (Setup of SoD Risks) screen. The main window title is 'Настройка SoD-рисков 00000000001 от 22.10.2025 14:00:24'. The left sidebar shows navigation links: Главное, Система, Предприятие, Ролевая модель, Учетные данные, and Администрирование. The main content area is titled 'Матрица SoD-конфликтов' (SoD Conflict Matrix). It includes a toolbar with buttons for 'Провести и закрыть' (Run and Close), 'Запись' (Record), 'Провести' (Run), and 'Отчеты' (Reports). The matrix grid is divided into two main sections: 'Приложение' (Application) and 'Право' (Right). The 'Приложение' section lists 'Зарплата и управление персоналом 3' (Salary and personnel management 3), 'Старшие расчетчики' (Senior accountants), 'Управление торговлей 11.5' (Trade management 11.5), 'Кассиры' (Cashiers), 'Менеджеры отдела продаж' (Sales department managers), and 'Руководители отдела продаж' (Sales department directors). The 'Право' section lists 'Зарплата и управление персоналом 3', 'Старшие расчетчики', 'Управление торговлей 11.5', 'Кассиры', 'Менеджеры отдела продаж', and 'Руководители отдела продаж'. A 'Выбор значения' (Select value) dialog box is open on the right, showing a list of users: Гладилина Вера Михайловна and Соколов Михаил Васильевич. The matrix grid itself shows various risk levels (1, 2, 3) across the application and right categories.

Пересмотр прав сотрудников по ролям

Инструмент для автоматического выравнивания доступов в соответствии с утвержденной ролевой моделью.

1C IDM Управление учетными данными, ред. 2.0 (1С:Предприятие)

Пересмотр прав сотрудников по ролевой модели

Заполнить права Вперед >

Права Отбор (1)

Режим: **Экспорт** Сотрудники: **Все сотрудники**

Права по сотрудникам

| Сотрудник | Статус | Операция |
|---|-------------------|----------------------------|
| Булатов Игорь Виленович | Недостающая | Создать учетную запись |
| Пользователи домена - Active Directory (основной домен) | Недостающее | Назначить право |
| УЗ: Бухгалтерия предприятия 3.0 | Недостающая | Создать учетную запись |
| Администраторы - Бухгалтерия предприятия 3.0 | Недостающее | Назначить право |
| УЗ: Управление торговлей 11.5 | Недостающая | Создать учетную запись |
| Руководители отдела продаж - Управление торговлей 11.5 | Недостающее | Назначить право |
| Волков Андрей Иванович | | |
| УЗ: Active Directory (основной домен) | Непредусмотренная | Блокировать учетную запись |
| Пользователи домена - Active Directory (основной домен) | Непредусмотренное | Отозвать право |
| Волков Марат Савельевич | | |
| Участник планирования закупок - Управление торговлей 11.5 | Недостающее | Назначить право |
| Захаркин Савелий Петрович | | |
| Доступ DCOM службы сертификации - Active Directory (основной домен) | Непредусмотренное | Отозвать право |
| Казакова Наталья Александровна | | |
| УЗ: Зарплата и управление персоналом 3 | Непредусмотренная | Блокировать учетную запись |
| Старшие расчетчики - Зарплата и управление персоналом 3 | Непредусмотренное | Отозвать право |
| Карницин Василий Алексеевич | | |
| УЗ: Active Directory (основной домен) | Непредусмотренная | Блокировать учетную запись |
| Пользователи домена - Active Directory (основной домен) | Непредусмотренное | Отозвать право |
| Лопырев Константин Валерьевич | | |
| УЗ: Active Directory (основной домен) | Непредусмотренная | Блокировать учетную запись |
| Пользователи домена - Active Directory (основной домен) | Непредусмотренное | Отозвать право |
| Милова Светлана Афанасьевна | | |

Назначить право: 7 Отозвать право: 7 Блокировать УЗ: 4 Создать УЗ: 5

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Отчеты

Мониторинг прав доступа. Предоставление отчетности.

Матрица доступа, права сотрудников, статусы, история изменения прав и другие.

История изменения прав

Сформировать Настройки Разворачивать до

| Сотрудник | Право | Статус | Приложение | Основание | Вид события |
|----------------------------|-------------------------------------|---------------|------------------------------------|-----------|-------------|
| Период | | | | | |
| Бодров Сергей Иванович | CH=Администраторы | Предоставлено | Active Directory (основной домен) | | |
| | CH=Администраторы схемы | Предоставлено | Active Directory (основной домен) | | |
| | CH=Администраторы предприятия | Предоставлено | Active Directory (основной домен) | | |
| | CH=Администраторы домена | Предоставлено | Active Directory (основной домен) | | |
| | CH=Пользователи домена | Предоставлено | Active Directory (основной домен) | | |
| | Active Directory (основной домен) | Предоставлено | Active Directory (основной домен) | | |
| | MS Exchange | Предоставлено | MS Exchange | | |
| | Открыты внешних отчетов и обработок | Предоставлено | Зарплата и управление персоналом 3 | | |
| | Обмен с "1С IDM" | Предоставлено | Зарплата и управление персоналом 3 | | |
| | Администраторы | Предоставлено | Зарплата и управление персоналом 3 | | |
| | Зарплата и управление персоналом 3 | Предоставлено | Зарплата и управление персоналом 3 | | |
| | Администраторы | Предоставлено | Бухгалтерия 3 | | |
| | Бухгалтерия 3 | Предоставлено | Бухгалтерия 3 | | |
| | Открыты внешних отчетов и обработок | Предоставлено | Управление торговлей 11 | | |
| | Администраторы | Предоставлено | Управление торговлей 11 | | |
| | Управление торговлей 11 | Предоставлено | Управление торговлей 11 | | |
| | Открыты внешних отчетов и обработок | Предоставлено | IDM: Управление учетными данными | | |
| | Администраторы | Предоставлено | IDM: Управление учетными данными | | |
| | CH=Администраторы схемы | Отозвано | Active Directory (основной домен) | | |
| Гриневский Юрий Михайлович | Active Directory (основной домен) | Предоставлено | Active Directory (основной домен) | | |
| | MS Exchange | Предоставлено | MS Exchange | | |
| | Управление торговлей 11 | Предоставлено | Управление торговлей 11 | | |
| | Менеджер отдела продаж | Предоставлено | Управление торговлей 11 | | |
| | CH=Пользователи домена | Предоставлено | Active Directory (основной домен) | | |
| | Управление торговлей 11 | Отозвано | Управление торговлей 11 | | |
| Дронов Игорь Петрович | Active Directory (основной домен) | Предоставлено | Active Directory (основной домен) | | |
| | MS Exchange | Предоставлено | MS Exchange | | |
| | Управление торговлей 11 | Предоставлено | Управление торговлей 11 | | |
| | CH=Пользователи домена | Предоставлено | Active Directory (основной домен) | | |
| | Менеджер отдела продаж | Предоставлено | Управление торговлей 11 | | |
| | Управление торговлей 11 | Предоставлено | Управление торговлей 11 | | |
| | Открыты внешних отчетов и обработок | Предоставлено | Управление торговлей 11 | | |
| | Открыты внешних отчетов и обработок | Отозвано | Управление торговлей 11 | | |
| | Сотрудник организации | Предоставлено | IDM: Управление учетными данными | | |
| Евтухов Илья Иванович | Active Directory (основной домен) | Предоставлено | Active Directory (основной домен) | | |
| | MS Exchange | Предоставлено | MS Exchange | | |
| | CH=Пользователи домена | Предоставлено | Active Directory (основной домен) | | |
| | Руководитель подразделения | Предоставлено | IDM: Управление учетными данными | | |

Отчеты

Права сотрудников
 История изменения прав
 Матрица доступа
 Матрица SoD-конфликтов
 Анализ прав сотрудников по ролевой модели
 Анализ прав сотрудников по объектам метаданных
 Дополнительные отчеты
 Анализ доступа сотрудников к ресурсам
 Ресурсы по источникам

Назначить право №22 от 20 ноября 2020 г.
 Отозвать право №23 от 20 ноября 2020 г.

Создать учетную запись №13 от 20 ноября 2020 г.
 Создать учетную запись №14 от 20 ноября 2020 г.
 Назначить право №15 от 20 ноября 2020 г.

Прием на работу
 Прием на работу
 Прием на работу
 Прием на работу

Анализ прав сотрудников по объектам метаданных

Отчет предназначен для вывода прав сотрудников в разрезе доступа к метаданным в приложениях 1С.

IDM Управление учетными данными, ред. 2.0 (1С:Предприятие)

Анализ прав сотрудников по объектам метаданных

Сотрудник: Приложение: Зарплата и управление персоналом 3

Параметры: Приложение: Зарплата и управление персоналом 3

Приложение

Таблица

Абрамов ГС
Балов Сергей Викторович
Булатов Игорь Викторович
Буров Валентин Викторович
Гарбовская Светлана Чарковна
Гольд Лев Самуилович
Грекова Надежда Петровна
Иванов Иван Петрович
Казакова Наталья Александровна
Куравев Назар Магомедович
Лопырев Константин Валерьевич
Масюк Диана Антоновна
Мейерсон Солья Гарольдина
Минеев Аркадий Борисович
Мосланенко Наталья Леонидовна
Орлов АВ
Орловская Елена Николаевна
Погорелов Иван Николаевич
Работникова Юлия Дмитриевна
Савицкая Зоя Юрьевна
Симончук Елена Оранцевна
Соколовская Мария Пахомовна
Фадеев Борис Михайлович

(не используется) Необработанные результаты согласования кабинет сотрудника(РегистрСведений)
(не используется) Непрочитанная переписка с контролирующими органами(РегистрСведений)
(не используется) Области персональных данных(РегистрСведений)
(не используется) Объекты для удаления из сервиса кабинет сотрудника(РегистрСведений)
(не используется) Обыски с оштрафами заполнения(РегистрСведений)
(не используется) Органы ПФР(Справочник)
(не используется) Основания для досрочной пенсии (СЗВ-К)(Справочник)
(не используется) Основания для досрочной пенсии(Справочник)
(не используется) Основания для исчисления стажа(Справочник)
(не используется) Основания для исчисления стажа(Справочник)
(не используется) Основания для увольнения(Справочник)
(не используется) Особые условия труда ПФР(Справочник)
(не используется) Ответы на запросы выписок из ЕГРЮЛ/ЕГРИП(РегистрСведений)
(не используется) Ответы на запросы ИОН(РегистрСведений)
(не используется) Отправки в ФСС(Справочник)
(не используется) Ошибки заполнения публикуемых объектов кабинет сотрудника(РегистрСведений)
(не используется) Параметры Интернет-поддержки пользователей(РегистрСведений)
(не используется) Переписка с контролирующими органами(Справочник)
(не используется) Правила публикации кабинет сотрудника(РегистрСведений)
(не используется) Публикуемые объекты кабинет сотрудника(РегистрСведений)
(не используется) Регламентированные отчеты(Справочник)
(не используется) Результат обмена с сервисом 1С:Кабинет сотрудника(РегистрСведений)

Активизация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Начальная страница | Анализ прав сотрудников по объектам метаданных |

Права сотрудников

Отчет показывает текущее состояние прав сотрудников.

1C IDM Управление учетными данными, ред. 2.0 (1С:Предприятие)

Права сотрудников

Приложение: Подразделение: Сотрудник:

Сформировать Настройки... Разворачивать до

Σ 0

Права сотрудников

Подразделение
Сотрудник
Приложение
Право

| Статус | Учетная запись | Срок действия | |
|--------------------------------------|----------------|-----------------------|-----------|
| Действует | IDM | Бессрочно | |
| Включена | IDM | Бессрочно | |
| Включена | МаскоДБ | Бессрочно | |
| Действует | МаскоДБ | Бессрочно | |
| Управление торговлей 11.5 | | | |
| Администратор | | | |
| Бухгалтерия предприятия 3.0 | | | |
| Управление торговлей 11.5 | | | |
| Администраторы | Действует | Admin | |
| Администраторы | Действует | Administrator | |
| Администраторы | Действует | Администратор | |
| Открытие внешних отчетов и обработок | Действует | Admin | |
| Открытие внешних отчетов и обработок | Действует | Administrator | |
| Управление торговлей 11.5 | Включена | Admin | |
| Управление торговлей 11.5 | Включена | Administrator | |
| Управление торговлей 11.5 | Включена | Администратор | |
| Белов Сергей Викторович | | | |
| Active Directory (основной домен) | | | |
| Active Directory (основной домен) | Отключена | Sergey Belov | Бессрочно |
| Demo Users | Отозвано | Sergey Belov | Бессрочно |
| Пользователи домена | Отозвано | Sergey Belov | Бессрочно |
| Зарплата и управление персоналом 3 | | | |
| Буров Валентин Викторович | | | |
| Active Directory (основной домен) | | | |
| Active Directory (основной домен) | Отключена | Valentin.Burov | Бессрочно |
| Demo Users | Отозвано | Valentin.Burov | Бессрочно |
| DnsAdmins | Отозвано | Valentin.Burov | Бессрочно |
| Пользователи домена | Отозвано | Valentin.Burov | Бессрочно |
| Зарплата и управление персоналом 3 | | | |
| Отключенные УЗ | | | |
| Управление торговлей 11.5 | | | |
| Бухгалтеры | Отозвано | Бухгалтер (СидоровНП) | Бессрочно |
| Сотрудники | | | |

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Начальная страница | Анализ прав сотрудников по объектам метаданных | Анализ прав сотрудников по ролевой модели | Права сотрудников

Управление привилегированными правами

Возможность работы с привилегированными правами. Отражение в отчете соответствующего признака у сотрудника.

Выполнение требований ГОСТ

ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация."

ГОСТ Р 70262.1-2022 "Защита информации. Идентификация и аутентификация. Уровни доверия идентификации". Стандарт устанавливает единообразную организацию процесса идентификации субъектов и объектов доступа в средствах защиты информации, средствах вычислительной техники и информационных системах. Положения стандарта рекомендуются к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом.

ГОСТ Р 57580.1-2017 "Защита информации финансовых организаций" – требования в части, касающейся базового состава мер по организации и контролю учетных записей, логического доступа.

ГОСТ Р 71753-2024 "Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования"

Обоснование внедрения

Кроме количественных параметров, позволяющих приблизительно посчитать экономические затраты на издержки, связанные с управлением прав - есть вопросы, напрямую влияющие на эффективность связанных бизнес-процессов, а также на информационную безопасность:

- | | |
|---|---|
| 1 | Трудозатраты на работу, связанную с управлением правами и учетными записями: - количество кадровых процессов: найм, увольнение, перемещение - количество запросов на выдачу/изменение прав доступа в ИС - время на выполнение заявок |
| 2 | Наличие единой, актуальной базы учета пользователей и учетных записей |
| 3 | Наличие филиальной структуры, где управление доступом осуществляется разрозненно |
| 4 | Наличие сквозного процесса создания УЗ и согласования предоставления им доступов |
| 5 | Наличие регулярного аудита прав доступа; инструмента контроля, выявления несанкционированных и излишних доступов, коллизий |
| 6 | Как быстро забираются права, блокируются УЗ у уволенных сотрудников? |

Эффективность продукта

| | |
|------------------|---|
| до 5 мин. | сокращение времени предоставления доступа с 1-3 дней до 5 минут |
| 80% | экономия затрат на управление доступом и УЗ |
| 55% | экономия времени бизнес-пользователей на решение задач с доступом и правами |
| 78% | сокращение нагрузки на ИТ-администраторов |
| 15% | сокращение лишних учёток в системах |
| 20% | снижение рисков нарушения ИБ, утечки данных |

Бизнес-пользователям

- + сокращение издержек при управлении доступом
- + права новым сотрудникам предоставляются автоматически и под контролем
- + информация по заявкам в режиме онлайн
- + разработка, внедрение актуальной ролевой модели

ИТ-службе

- + снижение трудозатрат и нагрузки на ИТ
- + заявки на доступ исполняются автоматически
- + самостоятельное формирование заявок
- + оперативный мониторинг и актуальная отчетность

Службе информационной безопасности

- + автоматическая блокировка при увольнении
- + пересмотр прав при смене должности
- + предотвращение утечки данных, избыточного доступа
- + инструмент для контроля, мониторинга и расследования инцидентов.

Конкурентные преимущества

1

Платформа 1С

Продукт реализован на платформе 1С, что обеспечивает включение его в экосистему. Сертификат 1С «Совместимо!».

2

Разработчик – дочерняя компания «1С»

Наличие необходимых ресурсов и компетенций для выполнения проектов любой сложности и масштаба.

3

Функциональная гибкость решения

Интеграция с любыми информационными системами. Большие возможности по адаптации и наращиванию функционала.

4

Низкая зависимость от разработчика

Открытый исходный код. Возможность самостоятельного внедрения, адаптации, доработки продукта.

5

Гибкое ценообразование

Конкурентоспособная цена с индивидуальным подходом к каждому проекту. Бессрочные лицензии – либо годовая подписка.

6

Поддержка и сопровождение

Консалто-часы, обучение, обновление, линия поддержки, возможность внедрения под ключ.

Пример проекта

Заказчик - крупнейший дистрибутор техники Komatsu. Более 1600 сотрудников.



Основные причины начала проекта:

- большое количество кадровых процессов
- долгая выдача доступов и их блокировка
- отсутствие актуальной ролевой модели
- частые изменения в подразделениях
- нет контроля над выданными доступами, отчетности.

Работы и решения:

- интеграция с кадровой системой; настройка подключений и правил обменов с AD, Exchange, 1С
- загрузка, анализ и нормализация НСИ в кадровых и целевых системах; сопоставление учетных записей сотрудников
- настройка реакций на кадровые события, правил предоставления прав
- тестирование системы, ОПЭ, обучение.

Результат:

- ✓ организовано эффективное управление УЗ и правами более 1600 пользователей из единой системы IDM
- ✓ автоматизированы процессы движения сотрудника по жизненному циклу
- ✓ ускорение бизнес-процессов приема и увольнения сотрудников, отпусков, кадровых переводов и др. Оперативное согласование заявок и выдача/отъем прав
- ✓ предоставили инструмент контроля, учета и анализа прав; предотвращения и расследования инцидентов ИБ.

Пример проекта

Задача:

Внедрить систему автоматизации управления учетными записями пользователей на основе матрицы доступа (ролевая система) к основным объектам доступа - целевым системам.

Выполнить требования законодательства по ГОСТ 57580 в части соответствующих мер.

Работы и решения:

- Поэтапная настройка системы с созданием и сопоставлением УЗ сотрудников, настройкой реакций на кадровые события, созданием и настройкой бизнес-ролей
- Интеграция с кадровой системой; настройка подключений и правил обменов с AD, Exchange, 1С
- Предоставление тестовой среды и среды разработки. Проведение опытно-промышленной эксплуатации
- Обучение администраторов.

Результат:

- Организовано эффективное управление УЗ и правами нескольких сотен пользователей из единой системы IDM
- Выполнены требования ГОСТ
- Ускорение бизнес-процессов приема и увольнения сотрудников, отпусков, кадровых переводов и др.
- Повышен уровень информационной безопасности Банка.



АКЦИОНЕРНОЕ ОБЩЕСТВО
АВТОГРАДБАНК

Акционерное общество
«АВТОГРАДБАНК»
430001, г. Набережные Челны,
г. Набережные Челны,
ул. Гагарина, 10
тел. +7 (8552) 33-00-00, факс. +7 (8552) 33-00-01, почтовый ящик 342/284/4466, к/к
420000, г. Набережные Челны, ул. Гагарина, 10
E-mail: avtobank@avtobank.ru, www.avtobank.ru, www.avtobank.ru/ru

Акционерное общество
«АВТОГРАДБАНК»
430001, г. Набережные Челны,
г. Набережные Челны,
ул. Гагарина, 10
тел. +7 (8552) 33-00-00, факс. +7 (8552) 33-00-01, почтовый ящик 342/284/4466, к/к
420000, г. Набережные Челны, ул. Гагарина, 10
E-mail: avtobank@avtobank.ru, www.avtobank.ru, www.avtobank.ru/ru

нк. №620-003 от 04.03.2024 г.

Генеральный директор

ООО «АВТОЛайн»

Чернов И. Ю.

Отказ
о внедрении системы IDM. Управление учётными данными
на базе платформы «С-Предприятие 8»

АО «Автографбанк» - универсальный коммерческий банк, основанный в г. Набережные Челны в 1991 году. Представляется в рядах регионов страны, в крупных городах Москва, Казань, Рязань, Волгоград, Грозный и других населенных пунктах Российской Федерации.

Основное функциональное требование при выборе системы IDM - управление учетных записей пользователей и настройка соответствующих правил доступа к различным объектам доступа. В качестве целевых систем мы рассматривали как стандартные (MS Active Directory, MS Exchange, IC-UUD) так и специальные - автоматизированные банковские системы. Важным критерием было выполнение требований ГОСТ 57580 в части соответствия мер.

Цели проекта:

- помочь усилить информационный безопасности за счет предоставления возможностей контроля и централизованного управления доступом пользователей;
- сimplify задачи по обслуживанию процессов управления учетными записями и правами доступа за счет автоматизации;
- сократить временные затраты на предоставление, изменение и отзыв прав доступа пользователей.

В ходе проекта проведены следующие работы:

- разработка частичного тестового окружения;
- подключение к тестовой системе с созданием и сопоставлением учетных записей сотрудников, настройкой правил на кадровые события, создание и настройкой бизнес-ролей, правил согласования;
- интеграция с кадровой системой: настройка подключений и правил обмена с AD;
- тестирование на производительность;
- предоставление тестовой среды и среды разработки. Разработка ПМК. Проведение опытно-промышленной эксплуатации;
- обучение администраторов системам.

По результатам проекта внедрена и принята в промышленную эксплуатацию Система управления учетными записями и управление правами информации наименование АО «Автографбанк». Проведено внедрение и тестирование цели. В перспективу запланированы работы по последующей модернизации и улучшению системы, подключение дополнительных систем.



Ю.В. Незлин

И другие проекты (NDA). Решение внедрено и эксплуатируется на крупных предприятиях различных отраслей с десятками тысяч пользователей.

Продукт находится в [Едином реестре](#) российских программ для ЭВМ.
Сертификат «Совместимо! Система программ 1С:Предприятие».
Государственная регистрация, Реестр программ для ЭВМ.



Минцифры
России



Будем рады проконсультировать вас по всем возникшим вопросам!
Подробная информация - на сайте <https://www.it-lite.ru/IDM/>

[+7 \(495\) 646-23-16](tel:+74956462316)
sales@it-lite.ru

Москва, Раменский б-р, 1 www.it-lite.ru

