

**Техническое задание**  
**в рамках проведения RFI (Request for information)**  
**на поставку и внедрение системы IdM**  
**для нужд ООО “UMS”**  
**(Общество с ограниченной ответственностью**  
**«Universal Mobile Systems»)**

**Ташкент**

## Содержание

Содержание.....	2
1 Общие сведения.....	3
2 Цели и задачи проекта .....	4
2.1 Цели Проекта .....	4
2.2 Задачи Проекта .....	4
2.3 Границы Проекта.....	4
3 Требования к IdM.....	6
3.1 Общие требования к IdM .....	6
3.2 Общие требования к архитектуре .....	7
3.3 Требования к автоматизируемым бизнес-процессам.....	7
3.4 Требования к управлению заявками.....	9
3.5 Требования к управлению внешними пользователями .....	9
3.6 Требования к взаимодействию со смежными системами .....	9
3.6.1 Требования к взаимодействию с источником кадровых данных.....	9
3.6.2 Требования к взаимодействию с управляемыми ИС .....	10
3.6.3 Требования к взаимодействию с системой обработки заявок.....	15
3.7 Требования к управлению назначениями .....	16
3.8 Требования к пользовательскому интерфейсу .....	16
3.9 Требования к контролю SOD-конфликтов.....	17
3.10 Требования к отчетности .....	18
3.11 Требования к безопасности .....	18
3.12 Требования к доступности и производительности .....	19
3.13 Требования к технической поддержке (3 линии) Исполнителя.....	19
3.13.8 Параметры оказания технической поддержки (3 линии) .....	19
3.13.9 Порядок взаимодействия сторон.....	21
4 Состав и содержание работ по внедрению IdM .....	23
5 Порядок контроля и приемки IdM.....	25
6 Требования к документированию.....	26
7 Общие требования к Исполнителю .....	27
8 Перечень принятых сокращений .....	29
9 Перечень терминов и определений, используемых в ТЗ.....	30

## **1 Общие сведения**

ООО «UMS» - телекоммуникационная компания, оказывающая услуги мобильной связи на всей территории Республики Узбекистан с 1 декабря 2014 года.

ООО «UMS» образован на основании постановления Кабинета Министров Республики Узбекистан №208 «О создании совместного предприятия «Universal Mobile Systems» по оказанию услуг мобильной связи» от 31 июля 2014 года, является одним из ведущих мобильных операторов Республики Узбекистан.

В соответствии с Постановлением Президента Республики Узбекистан №ПП-5187 от 19 июля 2021г. учредителем ООО «UMS» является Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан.

## **2 Цели и задачи проекта**

### **2.1 Цели Проекта**

#### 2.1.1 Цели Проекта:

- реализация Системы IdM (далее – IdM) для управления правами доступа в различных информационных системах (далее – ИС) ООО «UMS» (далее – Компания);
- повышение эффективности управления правами доступа и вовлечение руководителей подразделений в процесс контроля доступов подчиненных работников;
- снижение издержек на управление учетными записями пользователей;
- повышение уровня информационной безопасности за счет улучшения контроля доступов пользователей к информационным системам Компании;
- устранение избыточных ролей и избыточных привилегий в информационных системах;
- реализация инструмента для регулярного проведения аудита прав доступа;
- обеспечение своевременной блокировки учетных записей уволенных работников, внештатных работников, работников подрядчиков и т.п., с которыми завершены договорные отношения.

### **2.2 Задачи Проекта**

#### 2.2.1 Задачи Проекта:

- обследование текущих бизнес-процессов управления учетными записями и доступом пользователей к информационным системам;
- обследование процессов предоставления доступов в рамках кадровых процессов;
- обследование механизмов предоставления прав доступа в управляемых ИС;
- разработка технического решения IdM;
- интеграция IdM с источником кадровых данных;
- интеграция IdM с управляемыми ИС;
- разработка автоматизированных бизнес-процессов управления правами доступа.

### **2.3 Границы Проекта**

2.3.1 Проект включает в себя выполнение работ по внедрению и настройке IdM в Компании.

2.3.2 В границы проведения работ по внедрению IdM должны быть включены следующие ИС:

- Система 1С – источник кадровых данных;
- управляемые ИС:
  - Microsoft Active Directory;
  - Microsoft Exchange;
  - СЭД Bossreferent;
  - 1С Предприятие;
  - Норма – Законодательство;
  - Норма – Строительство;
  - Норма – Бухгалтерия;
  - Foris OSS.
- ITSM-система – система обработки заявок.

2.3.3 Общее количество пользователей IdM должно составить 1800 пользователей, в том числе:

- 1500 штатных сотрудников;
- 300 внештатных работников, работников подрядчиков и т.п.

2.3.4 Работы будут выполняться с помощью удаленного подключения к корпоративной сети Компании.

2.3.5 Срок технической поддержки производителя технического решения IdM должен составлять 1 год.

2.3.6 Срок технической поддержки (3 линии) Исполнителя должен составлять 1 год с возможностью последующего продления.

## **3 Требования к IdM**

### **3.1 Общие требования к IdM**

3.1.1 IdM должна быть построена на основе трехзвенной архитектуры, включающей следующие уровни:

- уровень представления;
- уровень бизнес-логики;
- уровень хранения данных.

3.1.2 Доступ пользователей к IdM должен осуществляться через web-интерфейс.

3.1.3 В IdM все надписи экранных форм, а также уведомления по электронной почте, предназначенные пользователям, должны быть выполнены на русском языке.

3.1.4 В качестве средства связи для информационного обмена между компонентами IdM, а также между АРМ пользователей и IdM должна использоваться локальная вычислительная сеть Компании.

3.1.5 В IdM должна содержаться следующая информация о пользователях:

- информация, полученная из источника кадровых данных;
- перечень учётных записей в управляемых ИС с их атрибутами;
- дополнительные управляемые атрибуты.

3.1.6 IdM должна предоставлять возможность вести и поддерживать сервис-каталог (справочник) информационных ресурсов, полномочий, прав доступа и др. для их публикации в едином интерфейсе пользователя и предоставления сотрудникам возможности запрашивать данные ресурсы.

3.1.7 В IdM должен быть реализован механизм функциональных ролей, позволяющий предоставить доступ только к необходимым функциям IdM.

3.1.8 IdM должна предоставлять функционал обнаружения изменений прав доступа пользователей в управляемых ИС, выполненных в обход IdM.

3.1.9 IdM должна предоставлять возможность настроить различные виды отчетов с учетом разграничения доступа к данным отчетам в рамках функциональных ролей пользователей IdM.

3.1.10 IdM должна предоставлять функционал рассылки уведомлений по всем типам операций, действий и изменений соответствующим лицам по электронной почте.

3.1.11 Для обеспечения восстановления информации после аварий в процессе эксплуатации должна создаваться резервная копия данных и программного обеспечения IdM. Для этого компоненты IdM должны быть включены в контур существующих систем резервного копирования и архивирования Компании.

3.1.12 В IdM должны быть настроены процессы самообслуживания и согласования заявок на доступ в рамках штатного функционала.

3.1.13 СУУЗ должна иметь возможность интеграции с системами корпоративного SSO, и PKI (для управления сертификатами и ключевыми носителями) от производителя ПО (IDM) Системы.

## **3.2 Общие требования к архитектуре**

3.2.1 IdM должна использовать широко известные и распространенные СУБД, ОС и пр. инфраструктурные решения.

3.2.2 IdM должна поддерживать работу в виртуализированной среде, включая размещение компонентов IdM на виртуальных серверах.

3.2.3 IdM должна иметь модульную архитектуру и предоставлять возможность поэтапного запуска в эксплуатацию по мере установки и настройки компонентов, подключения источников данных, подключения управляемых систем, готовности рабочих процессов и т.п.

## **3.3 Требования к автоматизируемым бизнес-процессам**

3.3.1 В IdM должны быть автоматизированы следующие бизнес-процессы:

- предоставление доступов при приеме на работу нового штатного работника;
- изменение данных о пользователе;
- изменение доступов при временном отсутствии работников;
- изменение доступов при переводе работника по должности/между подразделениями;
- прекращение доступа при увольнении работника
- предоставление доступов при повторном приеме на работу/возобновлении сотрудничества;
- блокировка (приостановка) доступов/разблокировка доступов по заявке;
- предоставление/отзыв доступов к управляемым ИС;
- согласование заявок на предоставление/отзыв доступов к информационным системам Компании, подключенным к IdM;
- заведение внешнего пользователя в IdM;
- предоставление доступов внешнему пользователю;
- управление технологическими учетными записями.

3.3.2 IdM должна иметь возможность работы как со штатными, так и с внешними сотрудниками. При этом должна быть обеспечена возможность независимой настройки процессов для разных типов сотрудников.

3.3.3 IdM должна иметь редактор настройки своих бизнес процессов

3.3.4 IdM должна обеспечивать автоматическое создание карточки пользователя при получении информации из источника кадровых данных о приеме на работу работника.

3.3.5 IdM должна обеспечивать автоматическое присвоение определенного минимального набора прав (далее – МНП) доступа в ходе создания карточки пользователя при получении информации из источника кадровых данных о приеме нового работника в соответствии с правилами, принятыми в Компании.

3.3.6 IdM должна позволять настраивать различные МНП в зависимости от подразделения, к которому относится работник в соответствии с правилами, принятыми в Компании.

3.3.7 IdM должна автоматически изменять данные в карточке пользователя и в УЗ в управляемых ИС на основании информации о работниках, полученной из источника кадровых данных.

3.3.8 IdM должна обеспечивать автоматическую обработку переводов работников по должности и/или между подразделениями с последующим изменением прав доступа пользователя в зависимости от типа перевода.

3.3.9 IdM должна обеспечивать автоматическую блокировку доступов пользователя при получении информации из кадрового источника об определенных видах отсутствий работников.

3.3.10 IdM должна обеспечивать возможность сохранения доступов пользователя при получении информации из кадрового источника об определенных видах отсутствий работников.

3.3.11 IdM должна обеспечивать автоматическую разблокировку доступов пользователя при получении информации из кадрового источника о завершении определенных видов отсутствий работников.

3.3.12 IdM должна обеспечивать автоматическую блокировку доступов для пользователей в случае получения из источника кадровых данных информации об увольнении или в случае наступления окончания срока действия договора для работников, работающих по срочным трудовым договорам, контрактам и т.д.

3.3.13 IdM должна автоматически идентифицировать существующего пользователя при получении информации о нем в ходе процесса повторного приема на работу.

3.3.14 IdM должна предоставлять функционал оперативной блокировки/разблокировки доступов пользователя ко всем управляемым ИС вручную через интерфейс IdM.

3.3.15 IdM должна отправлять уведомления определенным пользователям согласно условиям настроенных бизнес-процессов.

3.3.16 IdM должна обеспечивать возможность создания бизнес-процессов по периодическому пересмотру прав доступа.



### **3.4 Требования к управлению заявками**

3.4.1 IdM должна предоставлять возможность пользователям IdM формировать заявки через интерфейс IdM для себя или для другого пользователя IdM при наличии соответствующих прав доступа.

3.4.2 IdM должна предоставлять функционал автоматизированного процесса согласования заявок на доступ к управляемым ИС.

3.4.3 IdM должна обеспечивать возможность настройки и определения процедуры и политики согласования для каждого типа заявки в отдельности.

3.4.4 IdM должна обеспечивать возможность запроса прав доступа и полномочий как на постоянной основе (бессрочно), так и на заданный период времени. По истечении указанного периода доступ должен быть автоматически отозван у пользователя.

### **3.5 Требования к управлению внешними пользователями**

3.5.1 IdM должна предоставлять функционал создания карточки пользователя для внешних пользователей вручную через интерфейс IdM.

3.5.2 IdM должна обеспечивать автоматическое присвоение определенного МНП при создании нового внешнего пользователя в соответствии с правилами, принятыми в Компании.

3.5.3 IdM должна предоставлять функционал обязательного назначения ответственного за внешнего пользователя для внешних пользователей.

3.5.4 IdM должна автоматически изменять данные в карточке пользователя и в УЗ в управляемых ИС внешних пользователей на основании информации, введенной вручную через интерфейс IdM.

### **3.6 Требования к взаимодействию со смежными системами**

#### **3.6.1 Требования к взаимодействию с источником кадровых данных**

3.6.1.1 В качестве источника кадровых данных о работниках и организационной структуре Компании для IdM должна использоваться ИС кадрового учета – 1С.

3.6.1.2 IdM должна осуществлять загрузку информации о работниках, из источника кадровых данных на периодической основе не реже одного раза в сутки и обеспечивать ее дальнейшую обработку в соответствии с кадровыми мероприятиями.

3.6.1.3 IdM должна осуществлять загрузку информации об организационно-штатной структуре из источника кадровых данных и обеспечивать ее актуализацию в соответствии с ее изменениями в источнике кадровых данных.

3.6.1.4 IdM должна поддерживать иерархию (вложенность) объектов организационной структуры Компании (иерархической структуры управлений, подразделений, филиалов).

3.6.1.5 IdM должна обеспечивать автоматическое вычисление руководителя штатного работника, который в дальнейшем будет принимать участие в процессах согласования заявок на доступы в IdM, на основе информации о руководителе, хранящейся на стороне источника кадровых данных.

### **3.6.2 Требования к взаимодействию с управляемыми ИС**

#### **3.6.2.1 Общие требования к взаимодействию с Управляемыми ИС**

3.6.2.1.1 IdM должна предоставлять набор стандартных коннекторов и интерфейсов для подключения информационных систем.

3.6.2.1.2 IdM должна иметь возможность оперировать виртуальными ресурсами

3.6.2.1.3 В составе IdM должны присутствовать следующие стандартные коннекторы:

- Microsoft Active Directory,
- Microsoft Exchange.

3.6.2.1.4 IdM должна обеспечивать запуск синхронизации с управляемыми системами как по расписанию, так и в ручном режиме.

3.6.2.1.5 IdM должна управлять соответствующими объектами в Управляемых ИС, IdM должна обеспечивать поэтапное подключение Управляемых ИС, осуществлять импорт данных и автоматическую синхронизацию изменений объектов в каждой из ИС.

3.6.2.1.6 IdM должна иметь гибкие полностью настраиваемые механизмы поиска существующих учетных записей в Управляемых ИС, задания правил и шаблонов именования и обработки конфликтов имен для каждой Управляемой ИС в отдельности.

3.6.2.1.7 Для управления правами доступа в Управляемых ИС IdM должна обеспечивать возможность создания внутренних объектов IdM для этих ИС и их ролей и управления этими объектами.

3.6.2.1.8 IdM должна обеспечивать процесс управления субъектами доступа (УЗ пользователей) через реализацию следующих процедур:

- создание УЗ;
- изменение УЗ;
- блокировка/разблокировка УЗ;
- продление срока действия УЗ.

3.6.2.1.9 Система должна обеспечивать возможность управления объектами доступа (ролями) через реализацию следующих процедур:

- назначение роли;
- изменение срока действия роли;

– отзыв роли.

3.6.2.1.10 IdM должна формировать логины пользователей в Управляемых ИС в соответствии с требованиями Компании.

3.6.2.1.11 IdM должна формировать пароли для пользовательских УЗ в Управляемых ИС в соответствии с парольными политиками Компании.

3.6.2.1.12 IdM должна предоставлять функционал установки признака «сменить пароль при первом входе» при создании УЗ в Управляемых ИС.

### ***3.6.2.2 Требования к взаимодействию с MS Active Directory***

3.6.2.2.1 IdM должна обеспечивать автоматическое вычисление контейнера (OU) MS AD, в который необходимо поместить УЗ пользователя, при получении соответствующей информации из источника кадровых данных, на основе правил, принятых в Компании.

3.6.2.2.2 IdM должна обеспечивать возможность перемещения по контейнерам учетных записей пользователей MS AD при поступлении из источника кадровых данных информации об изменении данных работника, на основе которых вычисляется контейнер.

3.6.2.2.3 IdM должна обеспечивать заполнение атрибутов создаваемой учетной записи MS AD значениями, вычисленными на основании значений атрибутов работника в источнике кадровых данных в соответствии с правилами, принятыми в Компании.

3.6.2.2.4 IdM должна обеспечивать возможность установки первоначального пароля учетных записей пользователей MS AD с необходимостью смены пароля пользователем при первом входе.

3.6.2.2.5 IdM должна обеспечивать информирование пользователя о его первоначальном пароле посредством электронного письма на почтовый ящик руководителя данного пользователя в соответствии с правилами, принятыми в Компании.

3.6.2.2.6 IdM должна обеспечивать возможность автоматически включать пользователей в группы в MS AD при создании УЗ в MS AD в соответствии с правилами, принятыми в Компании.

3.6.2.2.7 В процессе настройки IdM должна быть обеспечена загрузка в нее информации о существующих учетных записях пользователей MS AD с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### ***3.6.2.3 Требования к взаимодействию с MS Exchange***

3.6.2.3.1 IdM должна обеспечивать создание почтового ящика пользователя в соответствующей базе MS Exchange в зависимости от правил, принятых в Компании, при поступлении информации о приеме нового работника из источника кадровых данных.

3.6.2.3.2 Изменения почтового ящика MS Exchange, производимые IdM, должны осуществляться в соответствующей базе MS Exchange в зависимости от правил, принятых в Компании.

3.6.2.3.3 IdM должна обеспечивать создание почтового ящика необходимого размера в соответствии с правилами, принятыми в Компании.

3.6.2.3.4 IdM должна обеспечивать возможность добавления/исключения пользователя в группу рассылки.

3.6.2.3.5 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих почтовых ящиках MS Exchange с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

#### **3.6.2.4 Требования к взаимодействию с системой СЭД Bossreferent**

3.6.2.5.1 Взаимодействие IdM с ИС СЭД Bossreferent должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.2 IdM должна выполнять следующие операции над следующими объектами СЭД Bossreferent:

**Таблица 1 – Соответствие объектов СЭД Bossreferent и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
1.	Роли	-	-	-	-	+	+	+

3.6.2.5.3 IdM должна выполнять операции над учетными записями СЭД Bossreferent на основании информации из источника кадровых данных.

3.6.2.5.4 IdM должна автоматически выполнять операции над объектами СЭД Bossreferent на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.5 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в СЭД Bossreferent с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

#### **3.6.2.5 Требования к взаимодействию с системой 1С Предприятие**

3.6.2.5.6 Взаимодействие IdM с ИС 1С Предприятие должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.7 IdM должна выполнять следующие операции над следующими объектами 1С Предприятие:

**Таблица 2 – Соответствие объектов 1С Предприятие и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
2.	Роли	-	-	-	-	+	+	+

3.6.2.5.8 IdM должна выполнять операции над учетными записями 1С Предприятие на основании информации из источника кадровых данных.

3.6.2.5.9 IdM должна автоматически выполнять операции над объектами 1С Предприятие на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.10 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в 1С Предприятие с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### **3.6.2.6 Требования к взаимодействию с системой Норма - Законодательство**

3.6.2.5.11 Взаимодействие IdM с ИС Норма – Законодательство должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.12 IdM должна выполнять следующие операции над следующими объектами Норма - Законодательство:

**Таблица 3 – Соответствие объектов Норма – Законодательство и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
2.	Роли	-	-	-	-	+	+	+

3.6.2.5.13 IdM должна выполнять операции над учетными записями Норма – Законодательство на основании информации из источника кадровых данных.

3.6.2.5.14 IdM должна автоматически выполнять операции над объектами Норма - Законодательство на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.15 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в Норма – Законодательство с осуществлением привязки данной

информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### **3.6.2.7 Требования к взаимодействию с системой Норма - Строительство**

3.6.2.5.16 Взаимодействие IdM с ИС Норма – Строительство должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.17 IdM должна выполнять следующие операции над следующими объектами Норма - Строительство:

**Таблица 4 – Соответствие объектов Норма - Строительство и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
2.	Роли	-	-	-	-	+	+	+

3.6.2.5.18 IdM должна выполнять операции над учетными записями Норма - Строительство на основании информации из источника кадровых данных.

3.6.2.5.19 IdM должна автоматически выполнять операции над объектами Норма - Строительство на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.20 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в Норма - Строительство с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### **3.6.2.8 Требования к взаимодействию с системой Норма - Бухгалтерия**

3.6.2.5.21 Взаимодействие IdM с ИС Норма - Бухгалтерия должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.22 IdM должна выполнять следующие операции над следующими объектами Норма - Бухгалтерия:

**Таблица 5 – Соответствие объектов Норма - Бухгалтерия и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
2.	Роли	-	-	-	-	+	+	+

3.6.2.5.23 IdM должна выполнять операции над учетными записями Норма - Бухгалтерия на основании информации из источника кадровых данных.

3.6.2.5.24 IdM должна автоматически выполнять операции над объектами Норма - Бухгалтерия на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.25 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в Норма - Бухгалтерия с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### **3.6.2.9 Требования к взаимодействию с системой Foris OSS**

3.6.2.5.26 Взаимодействие IdM с ИС Foris OSS должно осуществляться с помощью разрабатываемого коннектора IdM.

3.6.2.5.27 IdM должна выполнять следующие операции над следующими объектами Foris OSS:

**Таблица 6 – Соответствие объектов Foris OSS и операций над ними, выполняемыми IdM**

№	Наименование объекта	Операции						
		Создание	Блокировка	Разблокировка	Изменение	Вычитывание	Назначение	Отзыв
1.	Учётные записи	+	+	+	+	+	-	-
2.	Роли	-	-	-	-	+	+	+

3.6.2.5.28 IdM должна выполнять операции над учетными записями Foris OSS на основании информации из источника кадровых данных.

3.6.2.5.29 IdM должна автоматически выполнять операции над объектами Foris OSS на основании информации о согласовании заявки на назначение/отзыв данных объектов.

3.6.2.5.30 В процессе настройки IdM должна быть обеспечена загрузка информации о существующих учётных записях в Foris OSS с осуществлением привязки данной информации к карточкам пользователей IdM, сформированным на основании информации из источника кадровых данных.

### **3.6.3 Требования к взаимодействию с системой обработки заявок**

3.6.3.1 IdM должна быть интегрирована с существующей системой обработки заявок – ITSM-системой.

3.6.3.2 IdM должна обеспечивать создание обращений в ITSM на основании информации о согласованной в IdM заявке на доступ в ИС, не управляемой IdM.

3.6.3.3 IdM должна передавать в ITSM-систему при создании обращения информацию о получателе запрашиваемого доступа, указанного в согласованной в IdM заявке.

3.6.3.4 Обращение должно создаваться на определенную группу исполнителей в ITSM-систему, в зависимости от категории заявки в IdM.

### **3.7 Требования к управлению назначениями**

3.7.1 IdM должна обеспечивать процесс управления объектами доступа (ролями) через реализацию следующих процедур:

- назначение роли;
- изменение срока действия роли;
- отзыв роли.

3.7.2 IdM должна обеспечивать полный контроль текущих прав доступа и полномочий сотрудника в подключенных ИС и являться единым авторизованным источником данной информации.

3.7.3 IdM должна иметь настройки механизма реконсиляции (приведения в соответствие) авторизованных и фактических прав доступа и полномочий, а также механизм уведомлений о всех случаях возникновения избыточных (неавторизованных) прав.

3.7.4 IdM должна предоставлять возможность просмотра в графическом интерфейсе текущих прав доступа, полномочий, ролей и атрибутов сотрудника по всем подключенным информационным системам.

### **3.8 Требования к пользовательскому интерфейсу**

3.8.1 IdM должна иметь в своем составе единый пользовательский интерфейс для всех сотрудников Компании, независимо от их функции в Компании.

3.8.2 Пользовательский интерфейс IdM не должен требовать дополнительной установки программного обеспечения на конечное устройство пользователя (стационарный компьютер, ноутбук, планшет, смартфон).

3.8.3 Пользовательский интерфейс IdM должен отображать информацию на русском языке.

3.8.4 IdM должна иметь гибкие настройки видимости элементов сервис-каталога (информационных ресурсов, прав доступа, полномочий и др.) в пользовательском интерфейсе IdM и доступности их для запроса тем или иным лицом или категорией лиц.

3.8.5 Видимость объектов IdM в пользовательском интерфейсе и доступность определенных действий с ними должны автоматически определяться по совокупности функциональных ролей, присвоенных сотруднику в IdM.

3.8.6 Пользовательский интерфейс IdM должен позволять включение в заявку (запрос) нескольких элементов, выбранных из любой категории сервис-каталога.

3.8.7 В пользовательском интерфейсе IdM в зависимости от внутренней роли (ролей), присвоенных сотруднику, должна отображаться Карточка пользователя, включая:



- Идентификационные данные и сопутствующие атрибуты;
- Учетные записи, присвоенные сотруднику в информационных системах;
- Присвоенные роли, ресурсы, права доступа и полномочия с функцией определения и графического отображения источника прав и полномочий;
- Утвержденные и отклоненные запросы доступа к информационным ресурсам с полной историей и цепочкой согласования запроса;
- Запросы, находящиеся в процессе утверждения с указанием имени и контактов следующего утверждающего.

3.8.8 В пользовательском интерфейсе IdM должна отображаться информация об утвержденных и отклоненных запросах, а также запросах, находящихся в процессе согласования (незавершенных запросах), включая полную историю запроса (с отображением цепочки согласующих и принятом решении на каждом шаге согласования).

### **3.9 Требования к контролю SOD-конфликтов**

3.9.1 IdM должна обеспечивать возможность выявления SoD-конфликтов на уровне ролей в ИС

3.9.2 IdM должна обеспечивать возможность настроить правила сочетаний и зависимости ролей

3.9.3 IdM должна обеспечивать назначение значений рисков для полномочий управляемых ИС для последующей оценки совокупного риска по ролям пользователя для определения действий по реагированию.

### **3.10 Требования к аудиту**

3.10.0 СУУЗ должна выполнять аудит доступов пользователей в управляемых ИС на предмет соответствия настроенным в СУУЗ политикам и назначенным ролям.

3.10.1 При выполнении аудита СУУЗ должна выявлять и регистрировать в журнале событий аудита следующие расхождения:

- избыточные права в управляемой ИС;
- недостающие права в управляемой ИС;
- отсутствует требуемая УЗ в управляемой ИС;
- незарегистрированная УЗ в управляемой ИС;
- не заблокирована УЗ уволенного работника.

3.10.2 СУУЗ должна обеспечивать просмотр и обработку журнала событий аудита. Обработка журнала событий аудита должна включать следующие возможности:

- По выбранным записям в журнале событий аудита устранить соответствующие им расхождения;
- По выбранным записям в журнале событий аудита задавать исключения из процедуры аудита для соответствующих расхождений;
- Автоматически создавать заявки на сертификацию выявленных расхождений;
- Указывать перечень УЗ пользователей в управляемых ИС, которые необходимо исключить из процедуры аудита.

### **3.11 Требования к отчетности**

3.11.1 IdM должна предоставлять функционал формирования отчетов.

3.11.2 IdM должна позволять экспорт отчетов в различных форматах (.pdf, .csv, .html).

3.11.3 IdM должна предоставлять возможность публикации шаблонов отчетов для подписки на них сотрудников, а также возможность определения доступности (видимости) тех или иных отчетов для разных категорий сотрудников. Подписка на отчеты должна самостоятельно осуществляться сотрудником из единого пользовательского интерфейса IdM.

3.11.4 IdM должна предоставлять возможность сформировать следующие отчеты:

- Отчет по истории обработанных заявок;
- Отчет по результирующему набору ролей и доступов по указанному пользователю.

3.11.5 IdM должна предоставлять возможность задания в отчетах отчетного периода и наложения фильтра по системам и пользователям/ролям.

### **3.12 Требования к безопасности**

3.12.1 IdM должна удовлетворять требованиям регламентирующих документов Компании по информационной безопасности.

3.12.2 IdM должна хранить исторические данные для построения отчётов за всю историю согласования. Глубина архива системы должна быть не менее 5 лет.

3.12.3 IdM должна поддерживать возможность экспорта событий IdM во внешние системы.

3.12.4 IdM должна поддерживать возможность интеграции с SIEM-системой.

3.12.5 Идентификация и аутентификация пользователей при входе в пользовательский интерфейс IdM должна осуществляться на основе его логина и пароля домена MS Active Directory (далее – MS AD).

3.12.6 Аутентификация администратора при входе в интерфейс административных приложений должна осуществляться на основе его логина и пароля домена MS AD.

3.12.7 При организации удаленного взаимодействия между АРМ пользователя и IdM, взаимодействия IdM со смежными ИС, а также удаленного управления компонентами IdM должны использоваться сетевые протоколы, обеспечивающие контроль целостности сетевого взаимодействия и аутентификацию участников взаимодействия, такие как SSL/TLS.

3.12.8 На серверы компонентов IdM должны быть установлены средства антивирусной защиты, применяемые в Компании.

### **3.13 Требования к доступности и производительности**

3.13.1 Максимальное время восстановления после сбоя IdM должно составлять 4 часа. При этом недопустимы потери данных, а аварийно прерванные операции должны быть корректно завершены или отменены.

3.13.2 IdM должна позволять одновременную работу 1000 пользователей.

3.13.3 Количество обрабатываемых IdM заявок в день должно составлять не менее 500.

3.13.4 В IdM должен быть обеспечен уровень доступности 24/7 с возможностью плановых отключений в связи с проведением регламентных работ по ее обслуживанию.

### **3.14 Требования к технической поддержке (3 линии) Исполнителя**

3.14.1 Проведение диагностики состояния IdM при получении заявки от Компании о неисправности.

3.14.2 Поиск и локализация неисправностей и ошибок в конфигурациях.

3.14.3 Количество обрабатываемых IdM заявок в день – не менее 500.

3.14.4 Устранение инцидентов, связанных с некорректной работой IdM, несоответствующей эксплуатационной документации и/или появление окна с сообщением об ошибке, ведущее к частичному или полному прекращению предоставления сервисов IdM.

3.14.5 Устранение инцидентов, связанных с событиями, не являющимися частью нормального функционирования IdM, которые привели или могут привести к неработоспособности IdM или к снижению его качества.

3.14.6 При необходимости расширения границ работ между Компанией и Исполнителем подписывается дополнительное соглашение.

3.14.7 Техническая поддержка (3 линия) оказывается Исполнителем в рабочие дни в рабочее время.

#### **3.14.8 Параметры оказания технической поддержки (3 линии)**

3.14.8.1 Определение приоритета обращения типа «Инцидент».

Обращению типа «Инцидент» присваивается один из следующих приоритетов:

- Низкий;
- Средний;
- Высокий;
- Критический.

Приоритетность обращения типа «Инцидент» зависит от следующих параметров: влияние и срочность. Матрица определения приоритета типа «Инцидент» представлена в таблице 7.

*Таблица 7 – Матрица определения приоритета обращений типа «Инцидент»*

		Влияние		
		Высокое	Среднее	Низкое
Срочность	Высокая	Критический	Высокий	Средний
	Низкая	Высокий	Средний	Низкий

Параметр «влияние» характеризует количество сотрудников Компании, затронутых инцидентом, и определяется на основании критериев, приведенных в таблице 8.

*Таблица 8 – Определение влияния Запроса типа «Инцидент»*

Влияние	Описание
<b>Высокое</b>	Более 50 пользователей обратились в течение 1 часа по поводу данного инцидента, либо обратился 1 пользователь и заявил о влиянии инцидента более чем на 50 пользователей.
<b>Среднее</b>	Более 10 пользователей, но менее 50 пользователей обратились в течение 1 часа по поводу данного инцидента, либо обратился 1 пользователь и заявил о влиянии инцидента более чем на 10 пользователей.
<b>Низкое</b>	Инцидент носит единичный характер, обратились от 1 до 10 пользователей

Параметр «срочность» характеризует влияние инцидента на непрерывность бизнеса Компании и определяется на основании критериев, приведенных в таблице 9.

*Таблица 9 – Определение срочности Запроса типа «Инцидент»*

Срочность	Описание
<b>Высокая</b>	Инцидент представляет угрозу для непрерывности бизнеса Компании
<b>Низкая</b>	Инцидент не представляет угрозы для непрерывности бизнеса Компании

### 3.14.8.2 Сроки выполнения заявок на техническую поддержку (3 линию)

Исполнитель отвечает за предоставление технической поддержки (3 линии), а также за организацию контроля и контроль качества услуг специалистов Исполнителя согласно параметрам, которые приведены в таблице 10 настоящего технического задания.

*Таблица 10 – Сроки реакции на обращения типа «Инцидент»*

Приоритеты обращений	Время реакции с момента передачи запроса Исполнителю	Время устранения с момента передачи запроса Исполнителю	Срок решения
Критический	До 1 часа	До 4 часов	До 2 рабочих дней
Высокий	До 2 часов	До 8 часов	До 3 рабочих дней
Средний	До 4 часов	До 2 рабочих дней	До 5 рабочих дней
Низкий	До 8 часов	До 5 рабочих дней	До 10 рабочих дней

Пороговые значения, указанные в таблице, могут быть превышены Исполнителем в следующих случаях:

- требуется восстановление данных из резервной копии/обработка данных IdM при восстановлении/ручная корректировка данных. Величина порогового значения увеличивается на срок восстановления таких данных из резервной копии/обработки данных IdM при восстановлении/ ручной корректировка данных;
- требуется внесение изменений в ПО либо разработка обходного решения. Разработка обходного решения осуществляется в рамках отдельных дополнительных соглашений. Пороговые значения, приведенные в таблице, отсчитываются с момента реализации обходного решения;
- требуется восстановление неисправного оборудования и/или стороннего ПО на стороне Компании. Восстановление неисправного оборудования и/или стороннего ПО осуществляется в рамках отдельных договоров на техническую поддержку производителей Оборудования или Правообладателей ПО и пороговые значения, приведенные в таблице, отсчитываются с момента такого восстановления;
- недоступности сотрудника Компании, необходимого для решения проблемы, или в случае взаимодействия с представителем Компании по интегрируемым системам в процессе диагностики.
- пороговое значение «время устранения» может быть увеличено по согласованию с Компанией в случае, если технически не удастся предоставить временное решение по устранению последствий проблемы.
- сроки, указанные в таблице, относятся к тому часовому поясу, в котором был открыт запрос.

### 3.14.9 Порядок взаимодействия сторон

#### 3.14.9.1 Порядок работы по заявкам.

В случае обнаружения ошибки в работе обслуживаемой IdM и невозможности локализовать проблему своими силами специалист Компании подает запрос, используя выделенный адрес электронной почты.

Если при размещении заявки Компания не обозначила уровень критичности проблемы, Исполнитель регистрирует заявку с приоритетом «НИЗКИЙ». В дальнейшем, в ходе работ по заявке, уровень критичности проблемы может быть изменен (повышен) на основании запроса уполномоченного сотрудника Компании.

При размещении заявки необходимо предоставить следующую информацию:

- приоритет обращения – «КРИТИЧЕСКИЙ», «ВЫСОКИЙ», «СРЕДНИЙ», «НИЗКИЙ»;
- описание проблемы.

В ходе работ специалист Исполнителя может запрашивать у специалиста Компании дополнительную информацию, необходимую для решения проблемы.

При переписке по почте со специалистом Исполнителя Компания должна ставить в копию адрес рассылки. В случае нарушения данного правила Исполнитель не гарантирует своевременную реакцию на письмо.

После завершения работ по заявке специалист Исполнителя отправляет инициатору заявки запрос о её закрытии.

После получения подтверждения о закрытии заявки со стороны Компании работы считаются выполненными, и заявка закрывается специалистом Исполнителя.

При отсутствии со стороны Компании в течение 30 дней подтверждения или обоснованного отказа о закрытии заявки, работы по заявке считаются выполненными в полном объеме, и заявка закрывается специалистом Исполнителя в одностороннем порядке.

#### 3.14.9.2 Порядок разрешения конфликтных ситуаций.

При возникновении проблем в ходе выполнения заявки специалистом Исполнителя, Уполномоченные сотрудники Компании имеют возможность запросить о смене специалиста Исполнителя. Для этого необходимо связаться с любым из Уполномоченных сотрудников Исполнителя, сообщив ему номер инцидента и суть проблемы.

## 4 Состав и содержание работ по внедрению IdM

4.1 Работы по созданию IdM должны проводиться в несколько этапов, структура которых приведена в таблице 11.

**Таблица 11 – Состав и содержание работ по созданию и технической поддержке IdM**

№ п/п	Этап	Результаты работ	Длительность
1.	Этап 1	<ul style="list-style-type: none"> <li>• Собраны требования для функционала IdM Этапа 1.</li> <li>• Разработано Частное техническое задание;</li> <li>• Реализована интеграция с источником кадровых данных – 1С;</li> <li>• Реализована интеграция с ITSM-системой;</li> <li>• Реализована интеграция с управляемыми ИС:                             <ul style="list-style-type: none"> <li>▪ MS AD;</li> <li>▪ MS Exchange</li> <li>▪ СЭД Bossreferent</li> <li>▪ 1С Предприятие</li> <li>▪ Норма - Законодательство</li> <li>▪ Норма - Строительство</li> <li>▪ Норма - Бухгалтерия</li> <li>▪ Foris OSS</li> </ul> </li> <li>• Автоматизированы процессы управления доступом для штатных сотрудников:                             <ul style="list-style-type: none"> <li>▪ Приём на работу;</li> <li>▪ Перевод;</li> <li>▪ Увольнение;</li> <li>▪ Временное отсутствие (длительный отпуск, декрет)</li> </ul> </li> <li>• Разработан комплект документации;</li> <li>• Настроена отправка уведомлений для ручного исполнения заданий.</li> <li>• Настроены процессы:                             <ul style="list-style-type: none"> <li>▪ Управления доступом в управляемых ИС;</li> <li>▪ Запроса и согласования прав доступа;</li> <li>▪ Блокировки/разблокировки УЗ по событиям ИБ;</li> <li>▪ Сброса пароля УЗ в управляемых ИС по запросу пользователей;</li> <li>▪ Построения отчетов (не более 3 отчетов).</li> </ul> </li> <li>• Настроены функциональные роли (не более 5 функциональных ролей).</li> <li>• IdM внедрена и переведена в опытно-промышленную эксплуатацию.</li> </ul>	Д <sup>1</sup> +12 месяцев
2.	Этап 2	<ul style="list-style-type: none"> <li>• Собраны требования для функционала IdM Этапа 2</li> <li>• Разработано Частное техническое задание на развитие IdM</li> <li>• Настроены процессы:                             <ul style="list-style-type: none"> <li>▪ Управления технологическими учетными записями;</li> <li>▪ Управления внешними сотрудниками;</li> <li>▪ Построения отчетов (не более 3 отчетов).</li> </ul> </li> <li>• Реализована ролевая модель в рамках штатного функционала системы (назначение полномочий в рамках должности и позиции).</li> <li>• Актуализирована документация.</li> </ul>	Д <sup>1</sup> <sup>2</sup> +6 месяцев

<sup>1</sup> Д – дата подписания договора

<sup>2</sup> Д<sup>1</sup> – дата завершения Этапа 1

№ п/п	Этап	Результаты работ	Длительность
		<ul style="list-style-type: none"><li>• IdM внедрена и переведена в опытно-промышленную эксплуатацию.</li></ul>	
3.	Техническая поддержка (3 линия)	<ul style="list-style-type: none"><li>• Консультации по телефону и электронной почте по вопросам, связанным с администрированием и настройками;</li><li>• Обеспечение 3-го уровня поддержки (устранение дефектов после анализа инцидента первым и вторым уровнями поддержки Компании, а также поиск обходных решений для разрешения инцидентов, переданных Исполнителю вторым уровнем поддержки Компании в статусе «инцидент»);</li><li>• Установка программных исправлений (корректирующих релизов);</li><li>• Ведение и поддержка в актуальном состоянии эксплуатационной документации – с учетом установленных корректирующих релизов, выявленной информации по проблемам, ошибкам, сбоям, путям выхода из них, а также особенностям работы и настройки IdM.</li></ul>	Д1+12 месяцев



## **5 Порядок контроля и приемки IdM**

5.1 Контроль и приемка работ осуществляются поэтапно на основании Частного технического задания.

5.2 Содержание технической документации согласуется на уровне специалистов Компании и Исполнителя на основе требований Частного технического задания.

5.3 Замечания Компании по технической документации должны быть представлены Исполнителю в письменной форме.

5.4 Для IdM должны быть проведены следующие виды испытаний:

- предварительные испытания IdM в тестовой среде;
- опытная эксплуатация IdM;
- приемочные испытания IdM в промышленной среде.

5.5 Если проведенные испытания будут признаны недостаточными либо будет выявлено нарушение требований регламентирующих документов по составу или содержанию документации, IdM может быть возвращена на доработку и назначен новый срок испытаний. По результатам устранения критичных замечаний каждого вида испытаний принимается решение о допуске IdM к последующему виду испытаний.

5.6 Объектом сдачи в промышленную эксплуатацию является полнофункциональная (обеспечиваются все функции, описанные в данном ТЗ и в Частном техническом задании) IdM, развернутая на площадке Компании.

5.7 Перед началом работы с IdM и его составными частями персонал IdM должен пройти обучение по работе с программными и техническими средствами, применяемыми в IdM.

## **6 Требования к документированию**

6.1 Исполнитель по результатам выполненных работ должен предоставить Компании следующую проектную документацию:

- Пояснительная записка к техническому проекту;
- Программа и методика испытаний;
- Руководство администратора;
- Руководство пользователя;
- Регламент восстановления и штатного обслуживания;
- Рабочий проект.

6.2 Документы разрабатываются Исполнителем на русском языке.

6.3 Документы должны предоставляться Компании в электронном виде, а итоговые согласованные версии документов, предоставляются в печатном сброшюрованном виде в двух экземплярах.

## 7 Общие требования к Исполнителю

7.1 Исполнитель должен обладать компетенцией Expert Partner и иметь возможность, подтвержденную производителем программного обеспечения, самостоятельно реализовывать, комплексные решения, осуществлять проектирование, внедрение и техническую поддержку систем.

7.2 Исполнитель должен предоставить сведения об опыте реализации не менее 3 аналогичных проектов за последние 5 лет с указанием наименования проекта, целей проекта, длительности проекта.

7.3 Исполнитель должен предоставить сведения об опыте проектной команды по внедрению систем Identity Management за последние 3 года с указанием ФИО участника проектной команды, наименования проекта, роли на проекте, длительности проекта.

7.4 В штате Исполнителя должно быть не менее 2 специалистов, имеющих сертификаты по системам Identity Management (подтверждается копией сертификатов).

7.5 Исполнитель должен предоставить сведения о проектной команде в соответствии с ролями, представленными в таблице 12, сведения об опыте проектной команды за последние 3 года с указанием ФИО участника проектной команды, наименования проекта, роли на проекте, длительности проекта.

**Таблица 12 – Перечень ролей специалистов**

Наименование роли	Зона ответственности
Менеджер проекта	Отвечает за общую организацию работ, выделение ресурсов и полученный результат, является основной точкой контакта по вопросам, связанным с ходом проекта, а также: <ul style="list-style-type: none"><li>• Формирование планов;</li><li>• Контроль выполнения планов;</li><li>• Организационная работа (в том числе и с Компанией);</li><li>• Концептуальная архитектура решения;</li><li>• Часть аналитической работы;</li><li>• Оценка длительности и трудоемкости задач в процессе планирования;</li><li>• Распределение работ внутри группы;</li><li>• Организация сбора требований Компании;</li><li>• Соответствие деятельности группы бизнес-процессу разработки;</li><li>• Взаимодействие с представителями Исполнителя;</li><li>• Ведение отчетности;</li><li>• Проведение процедуры эскалации.</li></ul>
Архитектор	<ul style="list-style-type: none"><li>• Архитектура решения, и соответствие ее требованиям Компании;</li><li>• Разработка функциональности (определяет принципиальные моменты, в дальнейшем их детализирует Разработчик);</li><li>• Контроль качества кода, и соответствие его проектным решениям по архитектуре;</li><li>• Участвует в формировании планов и оценке сложности и длительности задач;</li><li>• Участвует в тестировании.</li></ul>

Наименование роли	Зона ответственности
Разработчик	<ul style="list-style-type: none"><li>• Разработка (при участии Архитектора в процессе выработки принципиальных решений);</li><li>• Разработка функциональности;</li><li>• Качество кода;</li><li>• Исправление ошибок в коде;</li><li>• Проведение первичного тестирования кода;</li><li>• Участвует в комплексном тестировании кода.</li></ul>
Аналитик / Технический писатель	<ul style="list-style-type: none"><li>• Разработка методик и регламентов;</li><li>• Контроль правильности использования методики всеми участниками проекта;</li><li>• Контроль полноты и целостности результирующих материалов и отчетов;</li><li>• Контроль результатов подготовки данных;</li><li>• Подготовка отчетной документации;</li><li>• Разработка проектной и эксплуатационной документации.</li></ul>
Тестировщик	<ul style="list-style-type: none"><li>• Тестирование функциональности;</li><li>• Написание тестов;</li><li>• Участвует в разработке ПМИ.</li></ul>

## 8 Перечень принятых сокращений

Сокращение	Определение
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИС	Информационная система
МНП	Минимальный набор прав
ОС	Операционная система
ПМИ	Программа и методика испытаний
ПО	Программное обеспечение
СУБД	Система управления базами данных
СЭД	Система электронного документооборота
ТЗ	Техническое задание
УЗ	Учетная запись
IdM	Identity Manager, Система управления правами доступа

## 9 Перечень терминов и определений, используемых в ТЗ

Термин	Определение
<b>Внешний пользователь</b>	Пользователь IdM, информация о котором не поступает в IdM из источника кадровых данных, а ведется вручную через интерфейс IdM
<b>Заявка</b>	Любой зарегистрированный запрос на обслуживание, в системе учета службы сервисного обслуживания Исполнителя.
<b>Инфраструктурный инцидент</b>	Любое отклонение в работе IdM от состояния, предусмотренного документацией производителя и разработанным проектным решением, требующее исправления и возвращения IdM в штатный режим работы.
<b>Исполнитель</b>	Участник закупки, определенный исполнителем работ конкурентным способом в соответствии с Законом о контрактной системе
<b>Источник кадровых данных</b>	Источник данных IdM, из которого IdM получает кадровую информацию о работниках Компании и организационно-штатной структуре Компании.
<b>Карточка пользователя</b>	Информация о пользователе, полученная из источника кадровых данных или введенная вручную в интерфейсе IdM, а также информация обо всех учетных записях и назначенных правах в управляемых ИС.
<b>Компания</b>	ООО «UMS»
<b>Минимальный набор прав</b>	Набор прав доступа пользователя в управляемых ИС, назначение которых осуществляется автоматически при создании пользователя в IdM.
<b>Право доступа</b>	Совокупность полномочий, назначенных учетной записи пользователя в ИС
<b>Проект</b>	Проект по внедрению системы управления правами доступа
<b>Работник</b>	Физическое лицо, которое находится с Компанией в трудовых отношениях, оформленных в соответствии с трудовым законодательством Российской Федерации
<b>Рабочие дни</b>	Дни недели с понедельника по пятницу (кроме дней, являющихся на территории Российской Федерации официальными нерабочими днями), а также иные дни, официально объявленные рабочими
<b>Рабочее время</b>	С 10 до 18-30 московского времени в рабочие дни
<b>Уполномоченные сотрудники Компании</b>	Сотрудники, определенные Компанией и уполномоченные открывать Запросы/Заявки Исполнителю
<b>Управляемая ИС</b>	Информационная система, процесс управления правами доступа к которой автоматизируется посредством IdM
<b>Учетная запись</b>	Сведения, необходимые для идентификации пользователя при подключении к ИС, информация для аутентификации, авторизации и учета.
<b>Функциональная роль</b>	Совокупность прав доступа пользователя в IdM.