Информзащита
Системный интегратор

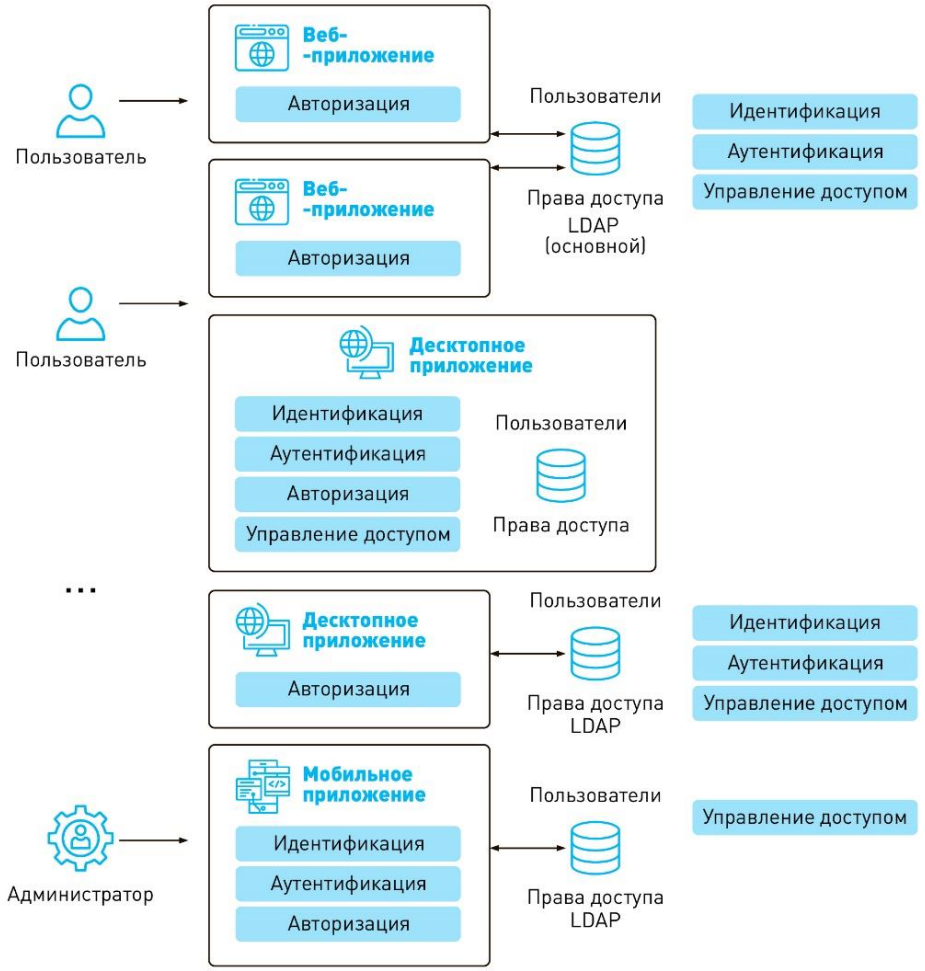
X-IDBox

Платформа идентификации, аутентификации, авторизации и управления доступом

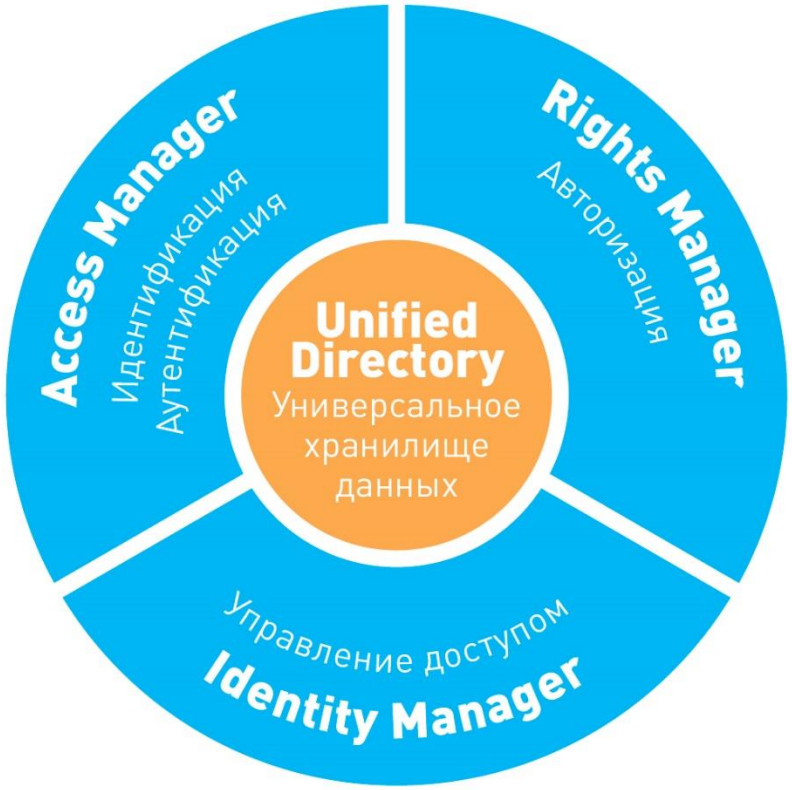
www.infosec.ru

Проблемы управления доступом

- Отсутствие прозрачного и гибкого процесса управления доступом, что **приводит к дополнительным затратам** при расширении инфраструктуры организации.
- Потребность в поиске дополнительных решений по управлению доступом при расширении количества ИС, что **влечет за собой дополнительные избыточные затраты**.
- Необходимость (пере)сертификации при доработках специализированного ПО, что **требует наличия квалифицированных специалистов в области ИБ**.
- Потребность в обновлении зарубежных решений по управлению доступом, что **гарантированно приведет в дальнейшем к рискам информационной безопасности**.
- Отсутствие единого процесса управления доступом к ИС для ИТ- и ИБ-администраторов, что **приводит к несвоевременному реагированию на инциденты безопасности.**

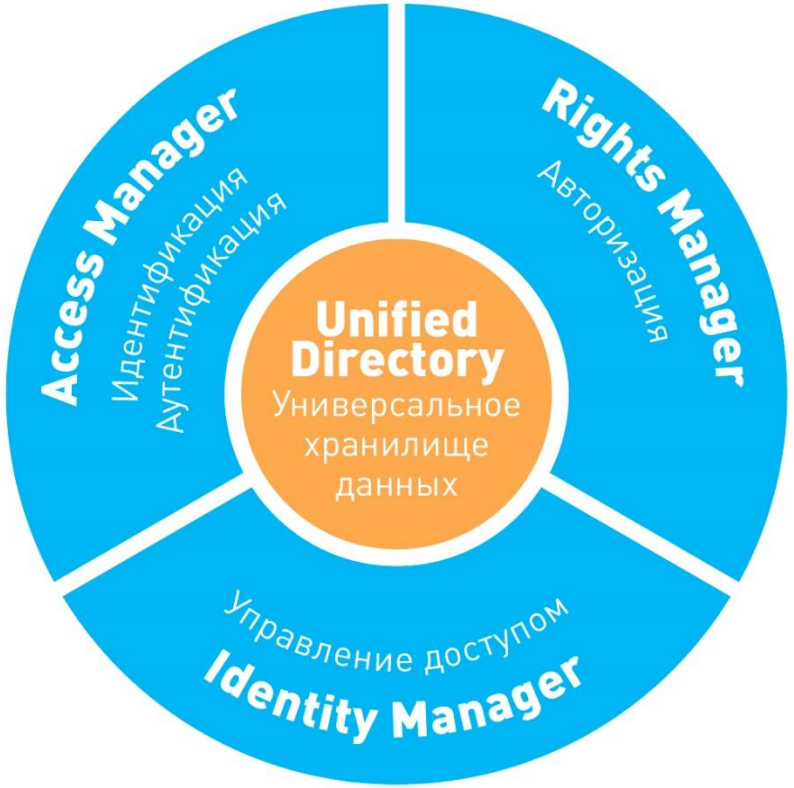


X-IDBox - платформа аутентификации и управления доступом



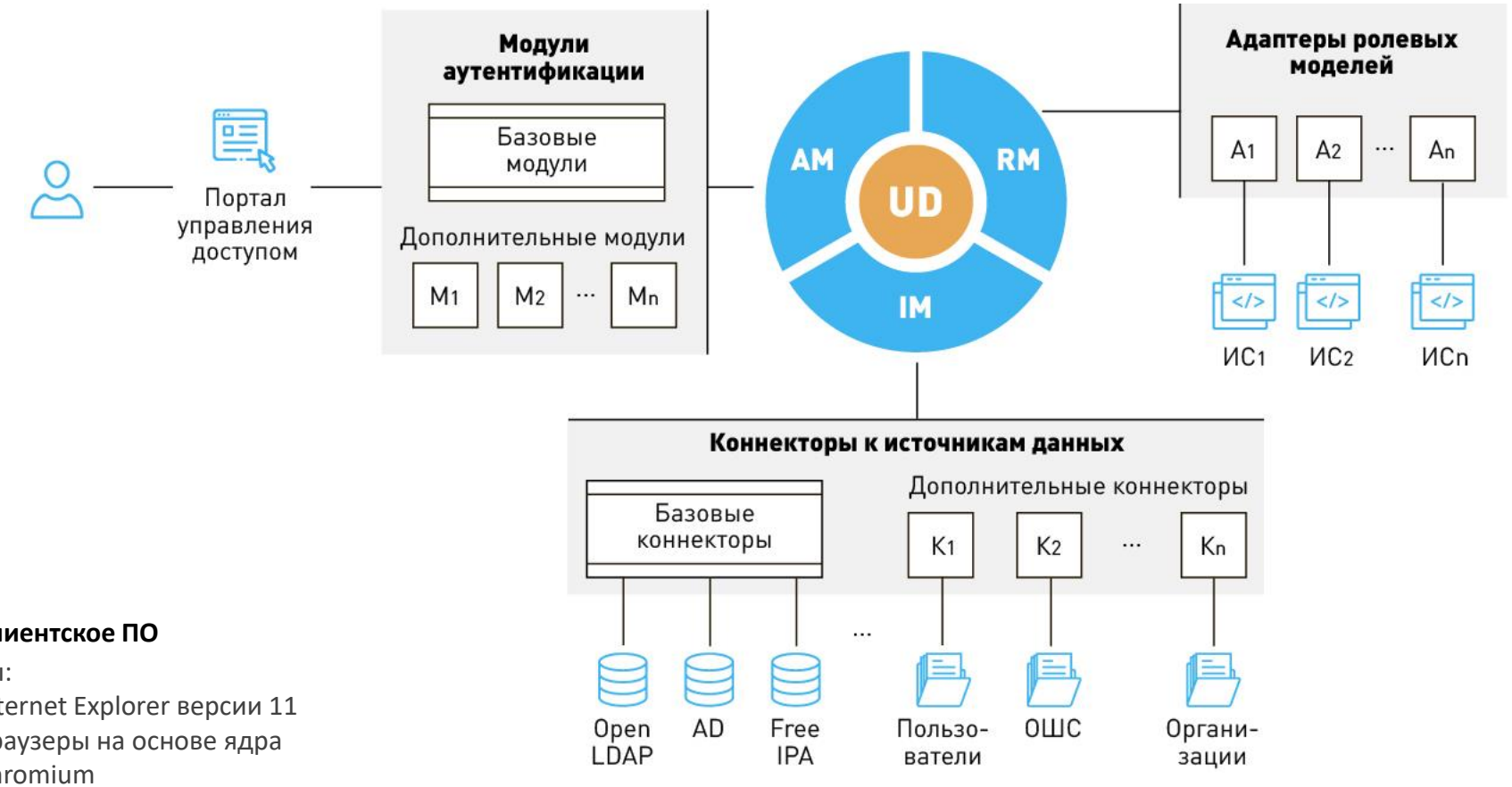
- Является решением **для защиты доступа ко множеству целевых систем**, реализующим функции идентификации, аутентификации, авторизации и управления доступом
- Позволяет настраивать и **расширять набор способов аутентификации**
- **Обеспечивает организацию доступа к** корпоративным информационным системам в режиме **Single Sign On**
- Реализует **модели управления полномочиями RBAC, ABAC, MAC**
- Позволяет гибко **настраивать механизм согласования заявок** по управлению доступом
- Обеспечивает **единое хранение данных пользователей и ОШС организации** для управления доступом, избавляет от необходимости хранения персональных данных пользователей в других системах организации
- Обеспечивает поддержку работы с **разными источниками данных** о пользователях, организациях, ОШС
- Предоставляет **настраиваемый интерфейс пользователя** для управления доступом
- Позволяет **сократить время и затраты на эксплуатацию**, так как все взаимодействия регламентированы в рамках единого процесса подключения к целевым системам

Безопасность и сертификация



- Обеспечивает осуществление всех **действий по управлению доступом** с помощью **заявок**:
  - настраиваемые маршруты согласования
  - уведомления пользователям о действиях над заявками
- Обеспечивает **юридическую значимость** всех действий по управлению доступом
- Обеспечивает возможность **регистрации событий безопасности** для интеграции с SIEM
- Обеспечивает **хранение информации** для **расследования инцидентов безопасности**
- Обеспечивает возможность **управления настройками паролей**
- Обеспечивает возможность **управления настройками безопасности**
- Обеспечивает реализацию **первого класса (К1) защищенности** информационной системы
- Обеспечивает соответствие **оценочному уровню доверия 2 (ОУД2)**

Общая архитектура решения



Клиентское ПО

- Браузеры:
  - Internet Explorer версии 11
  - Браузеры на основе ядра Chromium
- СКЗИ «КриптоПро CSP»

Технологии

- Nginx
- Open Java
- Postgres Pro
- Redis
- СКЗИ «КриптоПро»

Портал управления доступом

Возможности

✓ **Управление УЗ и профилями пользователей**

- регистрация пользователей
- блокирование и активация УЗ и профилей пользователей
- изменение данных пользователей
- группировка пользователей

✓ **Управление доступом пользователей**

- создание и изменение групп пользователей
- должностной доступ
- возможность разделения зон ответственности на основании метаданных пользователей, организаций, ОШС

✓ **Управление правилами доступа в ИС**

- настройка маршрутов согласования заявок
- изменение метаданных ролей и защищаемых ресурсов

✓ **Управление ИС**

- подключение новых ИС
- загрузка ролевых моделей
- управление ролями ИС
- управление способами аутентификации

✓ **Управление настройками безопасности**

- настройка парольных политик
- настройка списка разрешенных УЦ
- настройка сроков действия кодов и ссылок

Базовая ролевая модель

❑ **Пользователь** – обеспечение возможности работы в системе, назначается автоматически зарегистрированным пользователям

❑ **Регистратор** – выполнение регистрационных действий, управление УЗ и профилями пользователей и их доступом

❑ **Оператор** – управление ИС и доступом к ним

❑ **Администратор ИБ** – контроль выполнения требований безопасности, расследование инцидентов

❑ **Системный администратор** – управление настройками системы

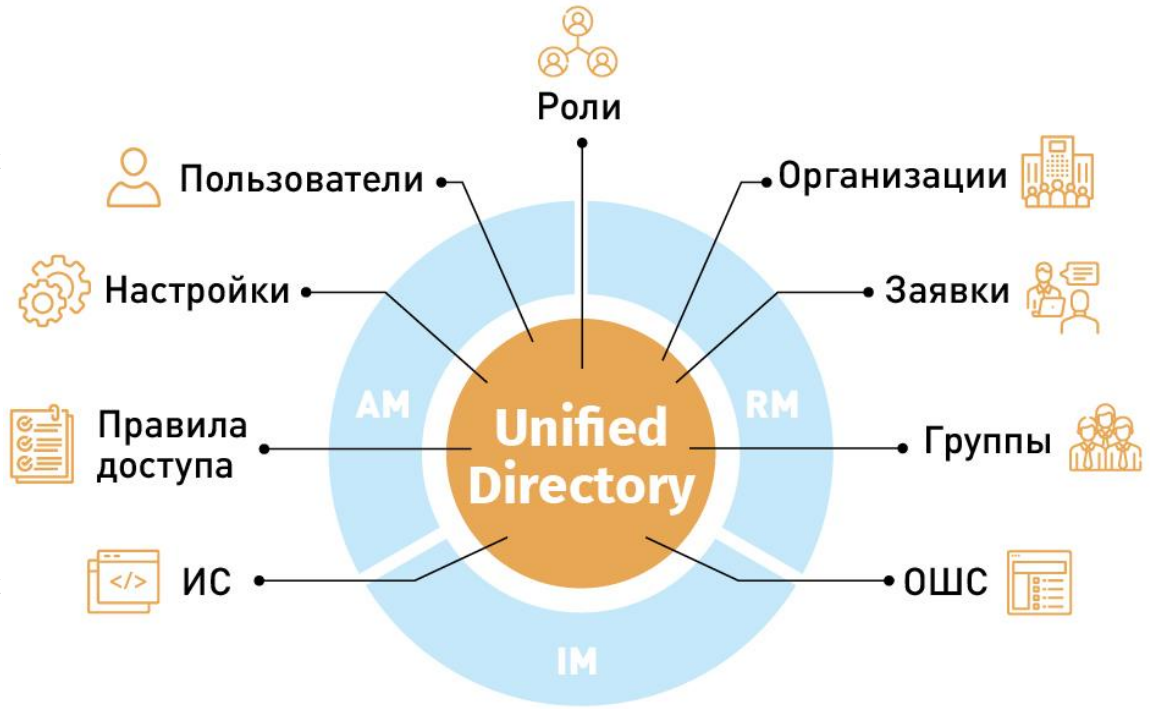
Unified Directory

Пользователи
- Личные данные
- Контактные данные
- Произвольный набор дополнительных атрибутов
- Должности и подразделения
- Профили в организациях
- Сессии пользователей
- Состояния профилей и УЗ
- Роли в ИС

Организации
- Типы организаций (ЮЛ, ИП/КФХ, филиалы)
- Основные атрибуты организаций
- Произвольный набор дополнительных атрибутов

ОШС
- Подразделения
- Должности
- Уровни подразделений

Настройки
- Списка допустимых УЦ
- Маршрутов согласования заявок



Группы
- Группы на основании ОШС
- Группы по атрибутам пользователей
- Включение конкретных пользователей в группы

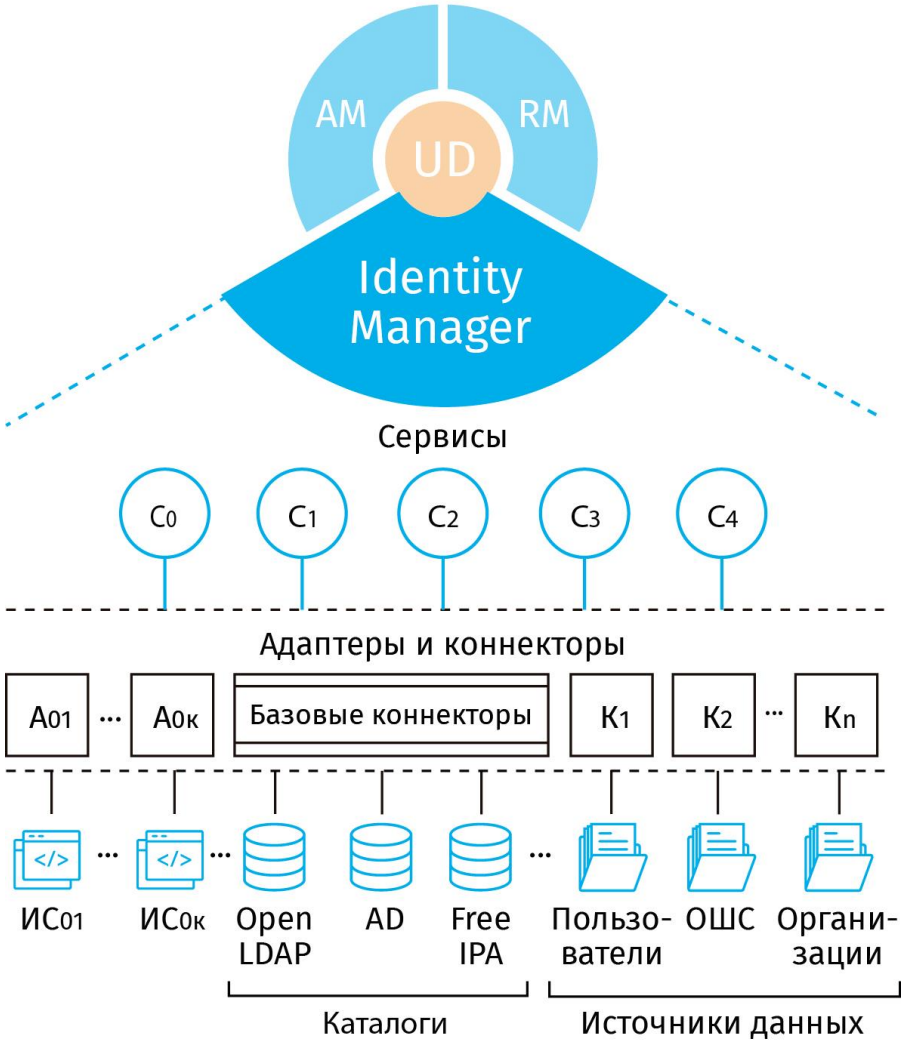
Заявки
- Тип заявки
- Маршрут согласования
- Статус выполнения
- Результат выполнения
- Уведомления об изменении статусов

ИС
- Метаинформация
- Атрибуты
- Доступные способы аутентификации
- Состояние

Роли
- Метаинформация
- Атрибуты
- Состояние
- Условия применимости

Правила доступа
- Типы защищаемых ресурсов
- Защищаемые ресурсы
- Атрибуты защищаемых ресурсов
- Политики доступа
- Условия политик доступа

Identity Manager



Возможности

- ✓ **Централизованное управление** каталогом пользователей
- ✓ **Контроль изменений** во **внешних каталогах** пользователей
- ✓ Поддержка **унифицированного процесса получения доступа** пользователей к целевым системам
- ✓ **Управление пользователями**, предоставление данных о пользователях:
  - Изменение данных
  - Блокирование и активация УЗ и профилей
  - Управление правами доступа
  - Управление группами пользователей

Режимы синхронизации

- ✓ **Unified Directory**: первичный импорт данных из внешних источников
- ✓ **Внешние каталоги**: односторонняя синхронизация данных с Unified Directory
- ✓ **Unified Directory**: односторонняя синхронизация данных с внешними каталогами
- ✓ **Unified Directory, внешние каталоги**: двусторонняя синхронизация данных с внешним каталогом с учетом приоритетов каталогов

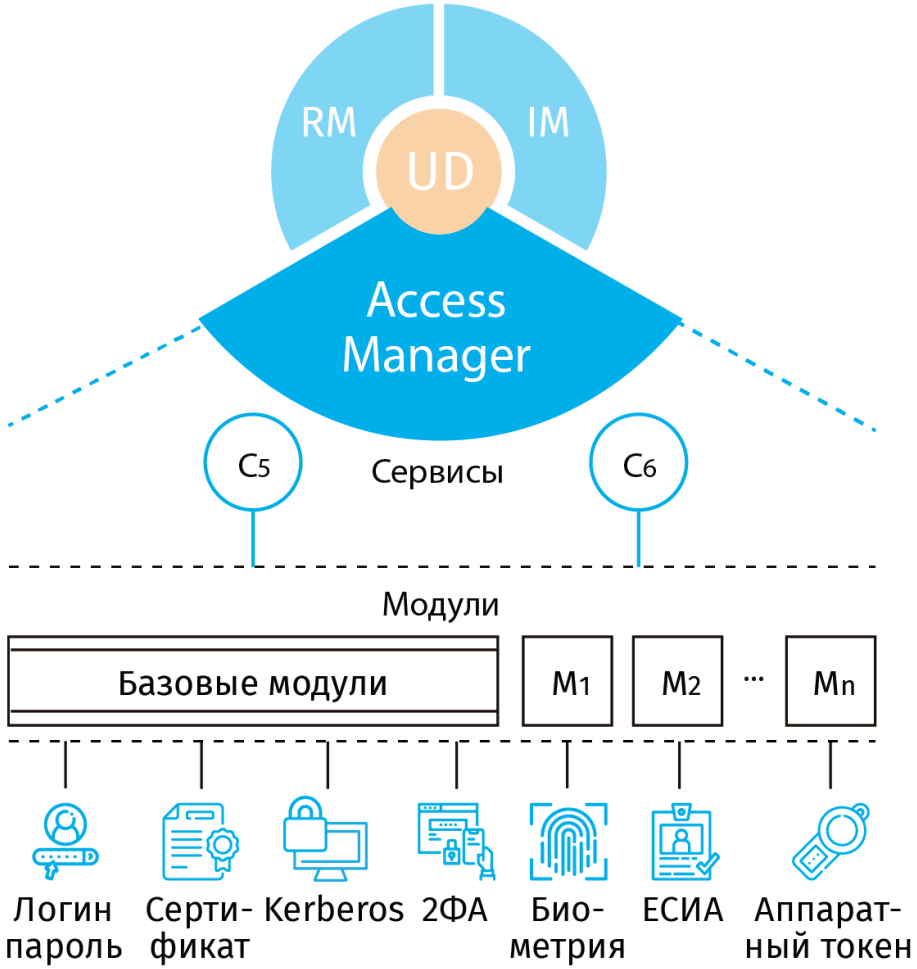
Сервисы

- ❑ **C0** – сервис идентификации
- ❑ **C1** – сервис загрузки организаций
- ❑ **C2** – сервис загрузки ОШС
- ❑ **C3** – сервис регистрации и управления пользователями
- ❑ **C4** – сервис синхронизации данных с каталогами пользователей

Адаптеры и коннекторы

- ❑ **$A0_1$ … $A0_k$** – адаптеры для сервиса идентификации
- ❑ **Базовые коннекторы** для работы с каталогами пользователей: FreeIPA, Active Directory, Open LDAP
- ❑ **Дополнительные коннекторы K_1 … K_n** для работы с данными пользователей, организаций, ОШС из произвольных источников

Access Manager



Возможности

- ✓ Управление **идентификацией** и **аутентификацией** пользователей
- ✓ Поддержка технологии **единого входа** в целевые системы (SSO)
- ✓ Поддержка **двухфакторной аутентификации**
- ✓ Поддержка **модульного механизма** расширения способов идентификации, аутентификации и второго фактора

Настройки

- ✓ Выбор способов аутентификации для каждой ИС
- ✓ Настройка двухфакторной аутентификации
- ✓ Возможность использования внешних идентификаторов пользователя
- ✓ Возможность использования базового интерфейса пользователя
- ✓ Возможность реализации собственного интерфейса пользователя

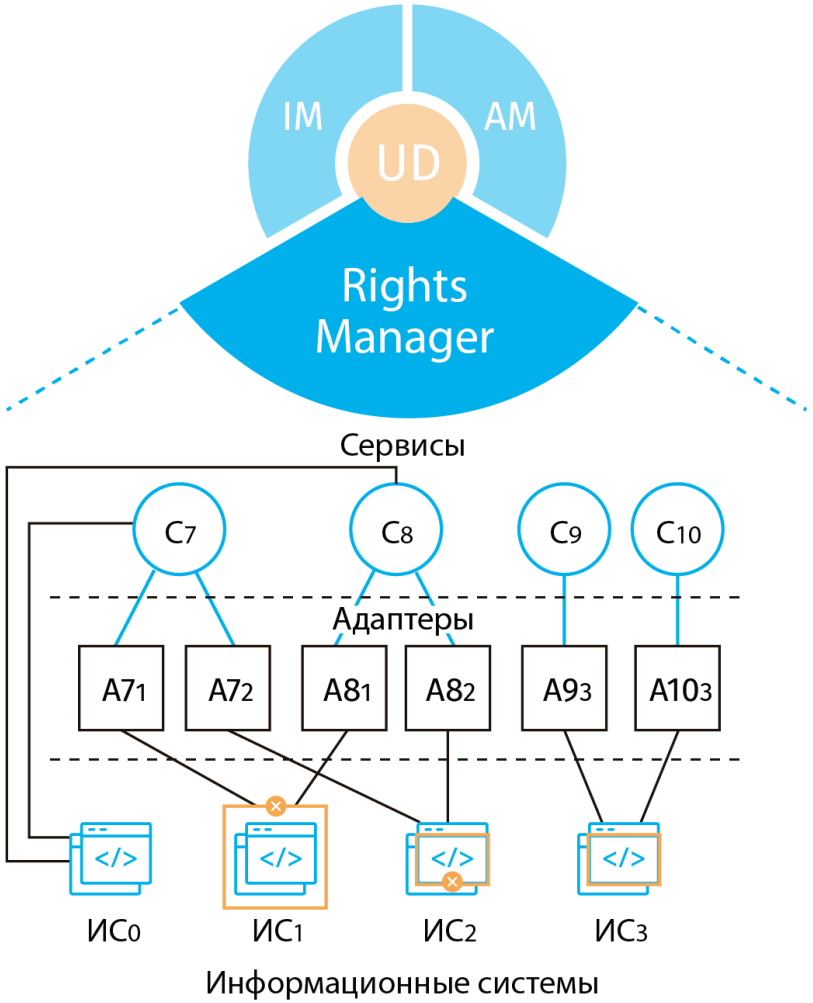
Сервисы

- ❑ **C5** – сервис аутентификации
- ❑ **C6** – сервис OAuth 2.0

Модули

- ❑ **Базовые модули** для идентификации и аутентификации пользователей:
  - ❑ логин/пароль
  - ❑ сертификат
  - ❑ Kerberos
  - ❑ 2ФА
- ❑ **Дополнительные модули M_1 … M_n** для расширения способов идентификации и аутентификации пользователей

Rights Manager



Возможности

- ✓ Хранение и управление **ролевыми моделями** целевых ИС:
  - защищаемыми ресурсами
  - ролями
  - политиками доступа
  - метаданными ролей и защищаемых ресурсов
- ✓ **Разграничение доступа** пользователей к целевым системам
- ✓ Внешний **сервис авторизации**
- ✓ **Уведомление** целевых ИС о **изменении настроек доступа**
- ✓ **Синхронизация назначений**

Методы разграничения доступа

- ✓ **RBAC** – ролевой
- ✓ **ABAC** – атрибутивный
- ✓ **MAC** – мандатный

Сервисы

- ❑ **C7** – сервис авторизации
- ❑ **C8** – сервис загрузки ролевых моделей
- ❑ **C9** – сервис отправки уведомлений
- ❑ **C10** – сервис сверки назначений

Адаптеры

- ❑ **$A7_1$ … $A7_n$** - адаптеры для сервиса авторизации
- ❑ **$A8_1$ … $A8_m$** - адаптеры для сервиса загрузки ролевых моделей
- ❑ **$A9_1$ … $A9_k$** - адаптеры для сервиса сверки и синхронизации назначений с ИС с собственным механизмом авторизации

Информзащита
Системный интегратор

Информационная безопасность 24x7x365

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Пресс-служба

pr@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru