

AK | Ankey IDM

**Централизованное
управления
учетными записями
и полномочиями
в гетерогенной среде**



GIS

ГАЗИНФОРМ
СЕРВИС

Санкт-Петербург

+7 (812) 677-20-53

sales@gaz-is.ru

www.gaz-is.ru

ITSM

Плюсы: Универсальность

Минусы: Минимум
возможностей автоматизации

PAM

Плюсы: Контроль УЗ, Контроль
сессий, Контроль действий

Минусы: Конкурентные сессии,
Контролируется административная
часть УЗ

NAC

Плюсы: Контроль сетевых
доступов

Минусы: Отсутствие управления
УЗ, отсутствие кросс-системного
взаимодействия

SSO

Плюсы: Контроль аутентификации
(кто входит?), Поддержка MFA

Минусы: Частичный контроль
авторизации (что доступно?)

Смежные решения управления доступом

ITSM

Плюсы: Универсальность

Минусы: Минимум

возможностей автоматизации

Автоматизация предоставления
доступов (в т.ч. «ручных»)

PAM

Плюсы: Контроль УЗ, Контроль
сессий, Контроль действий

Минусы: Конкурентные сессии,
Контролируется

административная часть УЗ

Контроль всех УЗ и сессий



NAC

Плюсы: Контроль сетевых
доступов

Минусы: Отсутствие управления
УЗ, отсутствие кросс-системного
взаимодействия

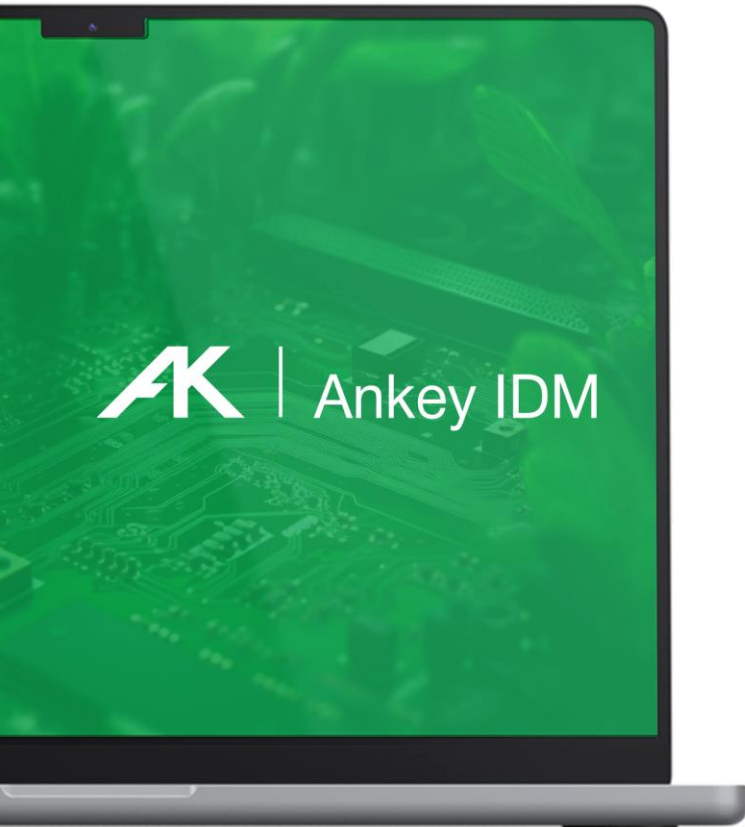
Автоматизация управления
доступом, Кросс-системный
контроль, Единое окно
управления доступом

SSO

Плюсы: Контроль аутентификации
(кто входит?), Поддержка MFA

Минусы: Частичный контроль
авторизации (что доступно?)

Полный контроль авторизации (что
доступно?)



Большинство западных компаний-разработчиков ушли с российского рынка, включая решения для управления учетными записями - **Identity Management (IDM)**, и **Identity Governance & Administration (IGA)**

Программы технической поддержки стали недоступны.



Решение класса **Identity Governance & Administration (IGA)** для управления учетными записями и правами доступа пользователей и администраторов в информационных системах предприятия

Политика импортозамещения решений



Ключевые функции комплекса Ankey IDM



Управление жизненным циклом учётных записей

любых типов на основе адаптивно настраиваемых процессов

Контроль ограничений и разрешений доступов

на основе ролей, полномочий, организационно-штатной структуры, атрибутов и загружаемых метаданных

Автоматизация управления правами доступа

на основе оргштатной структуры предприятия, атрибутах пользователей, подразделений, получаемых из кадровых источников и иных хранилищ

Контроль совмещения кумулятивных полномочий (SoD)

для предотвращения избыточности доступов, или критической совокупности доступа сотрудника

Ключевые функции комплекса Ankey IDM



Поддержка множественных трудоустройств

и сопровождение минимальных прав доступа для автоматизации назначения/отзыва доступов при совместительстве

Графический BPMN-движок

с поддержкой пользовательских скриптов и возможностью работы со сторонними системами и сервисами

Поддержка доменной аутентификации (AD, LDAP)

и возможность использования систем и служб Identity Provider для реализации единой точки входа

Самообслуживание, аудит и сертификация доступов

призваны обеспечить управление и контроль доступов гибким и удобным для пользователей и администраторов систем

Обширные возможности интеграции

со смежными ИТ и ИБ системами: SIEM, ITSM, SSO, PAM, Vault, NAC, SOAR для реализации «купола» безопасности

Покрытие ряда требований регуляторов



- **Стандарт ГОСТ:** Р 57580.1-2017 (ЗИ)
- **ФЗ:** №149, 152, 187 (ЗИ, ИСПДн)
- **Указ Президента РФ:** №166 об обеспечении технологического суверенитета
- **Приказы ФСТЭК:** №17, 21, 31, 239
- **ISO 27001 / ГОСТ 27001:** контроль предоставления полномочий и их пересмотр;
- **В реестре отечественного ПО**
- **Сертификат ФСТЭК №4107**
- **PCI DSS / СТО БР ИББС:** контроль создания, изменений и удаления данных ID; отзыв и пересмотр прав доступа

Покрываемые меры приказов ФСТЭК

| | Приказы | | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|-----|------|
| | №17 | №21 | №31 | №239 |
| АНЗ.5: Парольные политики, разграничение доступа | ✓ | ✓ | | |
| АУД.0: Политика аудита безопасности | | | ✓ | ✓ |
| АУД.10, АУД.11: Проведение аудитов безопасности | | | ✓ | ✓ |
| ИАФ.0, ИАФ.5, ИАФ.6: Идентификация и аутентификация пользователей | | | ✓ | ✓ |
| ИАФ.6: Идентификация внешних пользователей | ✓ | ✓ | | |
| УПД.1, УПД.2, УПД.4, УПД.5: Управление доступом, реализация модели доступа, разделение полномочий, назначение минимальных наборов прав | ✓ | ✓ | ✓ | ✓ |

Покрываемые меры ГОСТ 57580.1-2017

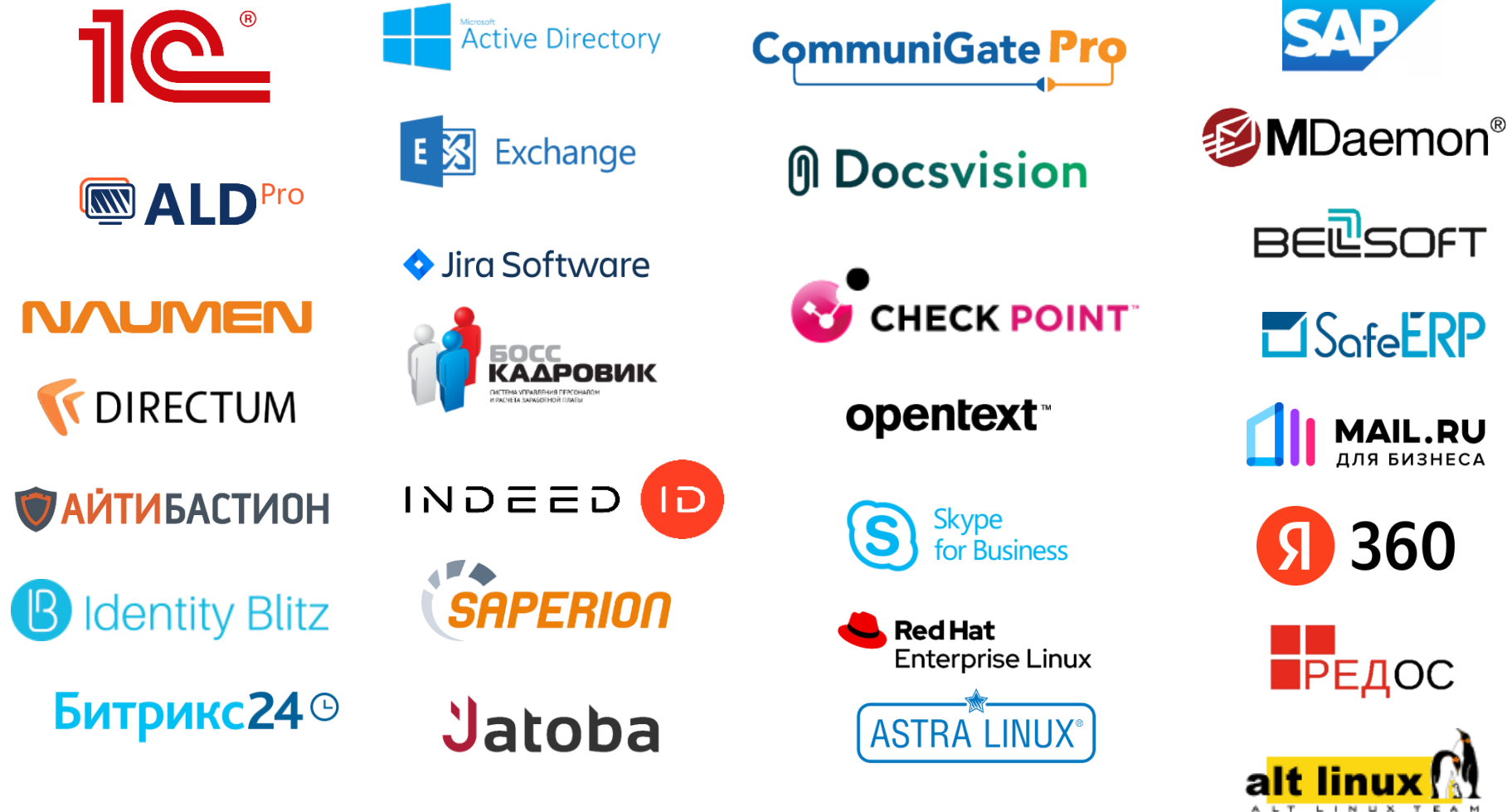
Безопасность финансовых (банковских) операций.
Защита информации финансовых организаций.

Базовый состав мер по организации и контролю использования
учетных записей субъектов логического доступа

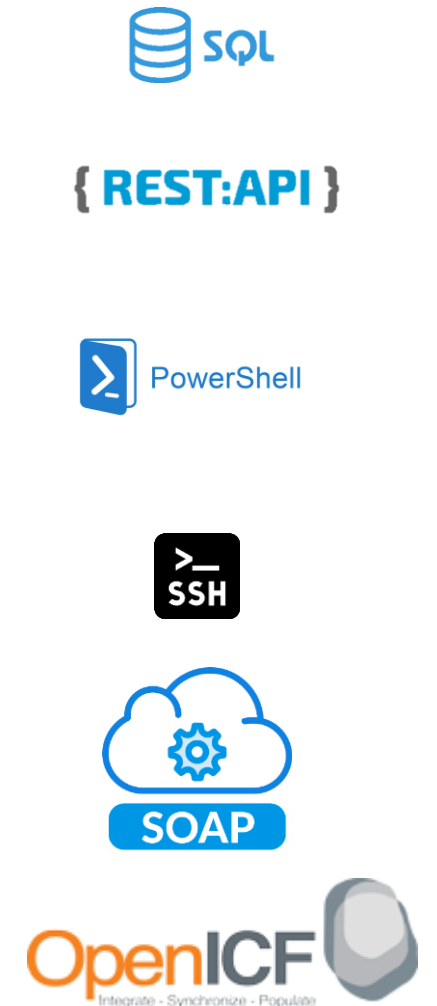
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Уровень защиты информации | | |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---|---|
| | | 3 | 2 | 1 |
| УЗП.1 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями | Т | Т | Т |
| УЗП.2 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа | О | О | Т |
| УЗП.3 | Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации | О | О | Т |

Комплекс Ankey IDM покрывает 27 мер УЗП (ГОСТ 57580.1), в т.ч. обязательных

Поддержка популярного ПО



Универсальные коннекторы



Специально для решений на платформе 1С



Разработан собственный модуль, исходный код для заказчика открыт и доступен

Обеспечена совместимость с любыми решениями на платформе 1С v8, не требует изменений основных конфигураций

Режим «Livesync» обеспечивает снижение нагрузки на системы и существенно увеличивает скорость обновления данных, включая обнаружение изменения полномочий

Реализована интеграция с NAC-решениями

Хранение эталонных сетевых доступов, их назначение и отзыв
в рамках парадигмы «нулевого доверия»



Ankey IDM + Checkpoint GAIA (v 8x)
– работает в продуктивной среде
заказчиков



Ankey IDM + EfrOs DefOps (NAC)
– ожидается в 2024г.*

Любые корпоративные службы каталогов



В Active Directory поддерживаем мультидоменность



Ankey IDM сертифицирован для работы с ALD Pro

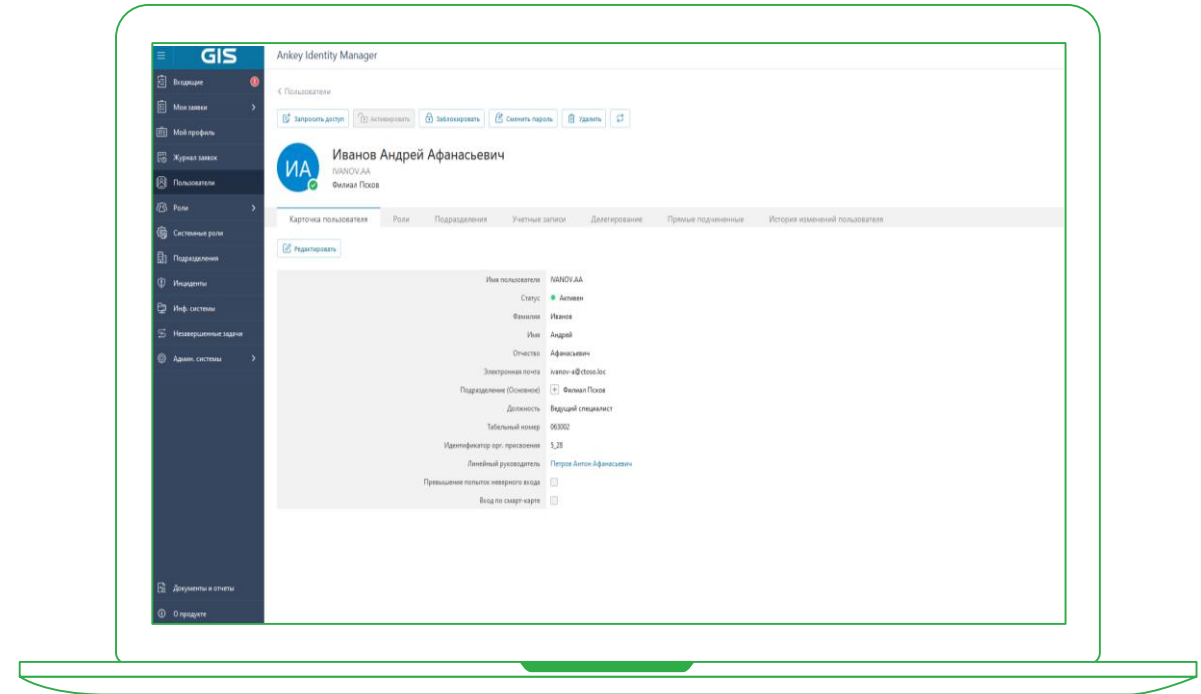
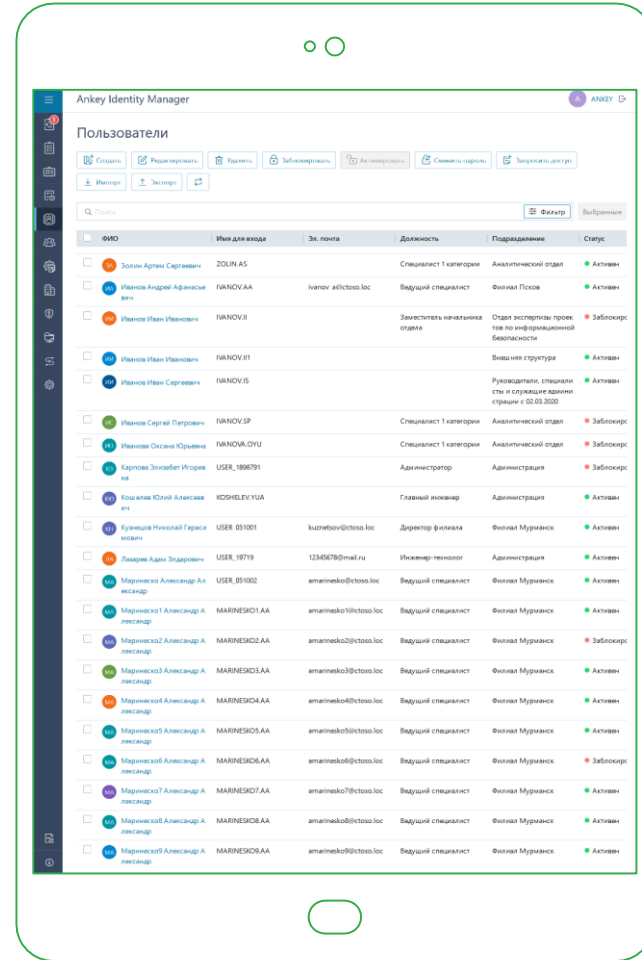
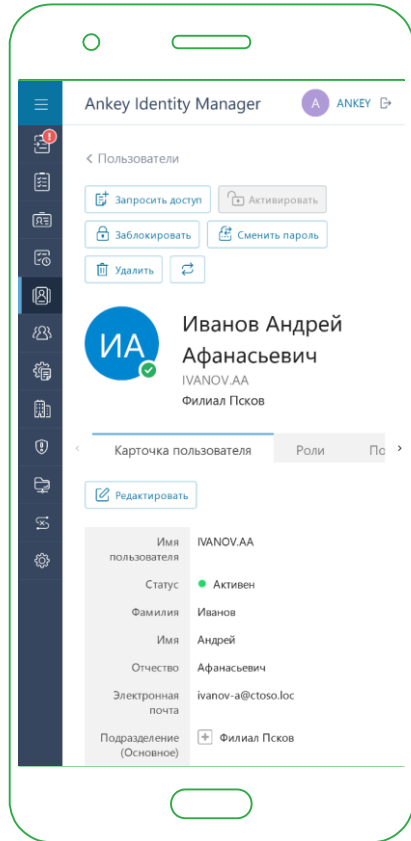
А также поддерживаем решения, реализованные на популярных протоколах:

Samba DC

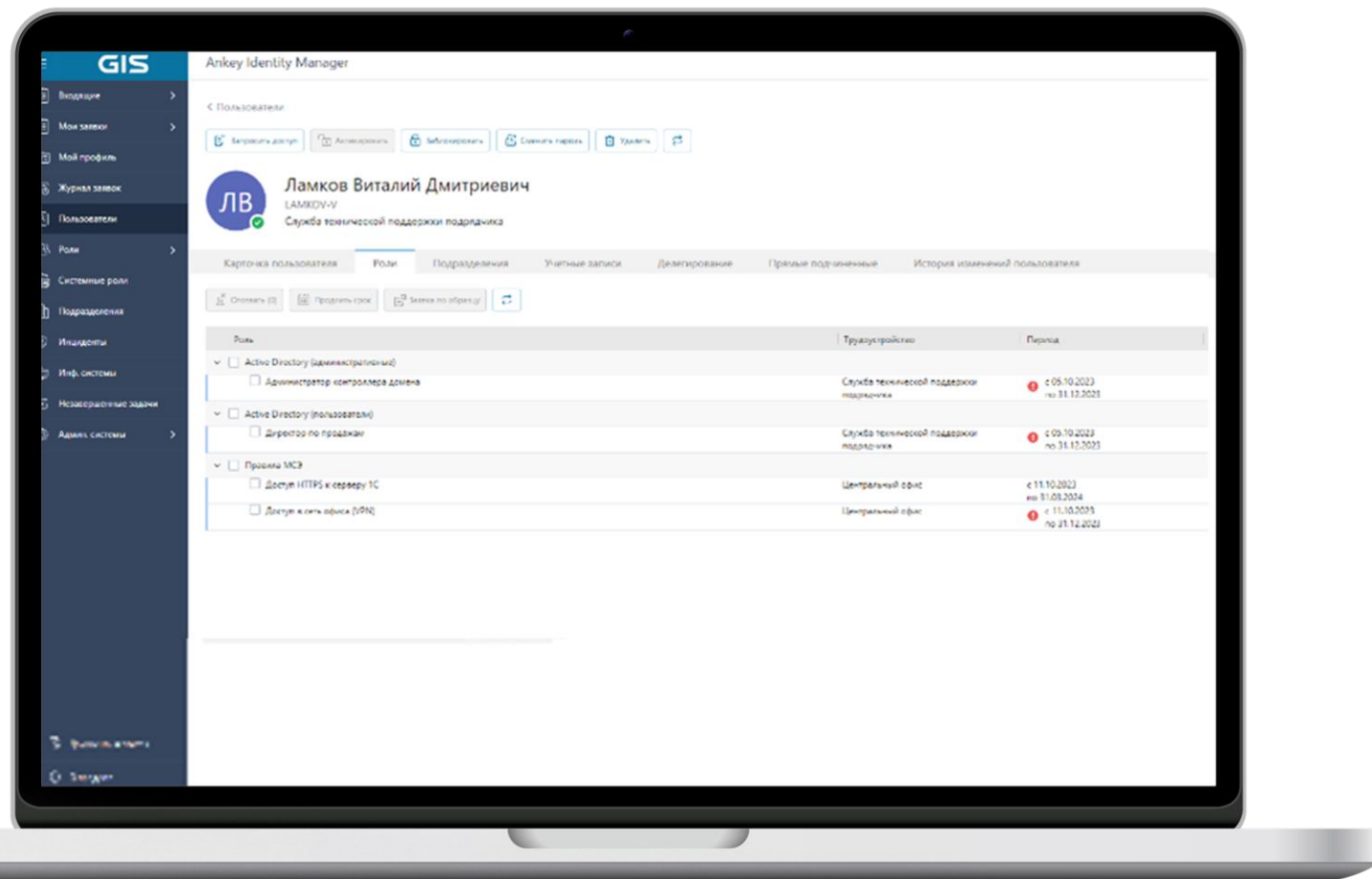
OpenLDAP

FreeIPA

Адаптивный интерфейс системы



Единое управление доступом всех пользователей



Поддержка интеграции:

ITSM – поручение на «ручное» исполнение. Получение на исполнение в IDM.

NAC – назначение сетевых доступов в «одном окне»

SSO – передача сведений о наличии УЗ

PAM – передача сведений о наличии административной УЗ, контроль сессий

Многоуровневые папки и коллекции доступов

The image displays two screenshots of the Ankey Identity Manager web interface, illustrating the multi-level folder and access collection structure.

Top Screenshot:


- Header:** Ankey Identity Manager
- Left Sidebar:**
 - 12
 - Информационные системы
 - Сетевые папки (Запрос доступа к сетевым папкам)
 - SAP (Запрос ролей из подсистем SAP)
 - 1С (Запрос ролей из подсистем 1С)
 - Прочие (Запрос прочих ролей)
 - Бизнес-роли (Запрос бизнес-ролей)
 - Роли (Запрос ролей)
- Main Content:**
 - Информационные системы:** Поиск по ИС в разделе Сетевые папки. Фильтр. Выбранные (3).
 - Доступные роли:** Поиск по ролям. Фильтр. Выбранные (5).
 - Администратор ЗМ: Азаров Степан Никанорович | ООО Газинформсервис. В соответствии с бизнес процессом "Организация закупок и поставок материалов для производства", необходимо провести закупку материалов для производства на основании договора закупки.
 - Администратор ИС

Bottom Screenshot:

- Header:** Ankey Identity Manager
- Left Sidebar:**
 - 12
 - Информационные системы
 - Сетевые папки (Запрос доступа к сетевым папкам)
 - SAP (Запрос ролей из подсистем SAP)
 - 1С (Запрос ролей из подсистем 1С)
 - Прочие (Запрос прочих ролей)
 - Бизнес-роли (Запрос бизнес-ролей)
 - Роли (Запрос ролей)**
- Main Content:**
 - Информационные системы:** Поиск по ИС в разделе Сетевые папки. Фильтр. Выбранные (3).
 - Доступные роли:** Поиск по ролям. Фильтр. Выбранные (5).
 - Запись: Запись. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Чтение: Чтение. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Чтение и запись: Чтение и запись. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Добавление файлов: Добавление файлов. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Перемещение файлов: Перемещение файлов. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Запись: Запись. Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...
 - Чтение: Чтение.

Многоуровневая иерархия систем/филиалов

☰
12
📄
📁

 С.И.

Информационные системы

Фильтр
Выбранные 9

Regions вложенности 2

→ Все папки > Сетевая папка 1 >

_____ | ООС _____

Данный ресурс создается для согласования проектной документации по проекту _____

Сетевая папка 2 вложенности 2

→ Все папки > Прочее > Regions > SPB > ООС _____

Азаров Степан Никанорович | ООС _____

Ресурс создается для согласования документации по проекту Р_____

Сетевая папка 3 вложенности 2

→ Все папки > Прочее > Regions > SPB >

_____ | ООС _____

Ресурс создается для согласования документации по проекту Р_____

Доступные роли

Фильтр
Выбранные 8

Сетевая папка 1 в иерархии 2.Запись

_____ | ООС _____

Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...

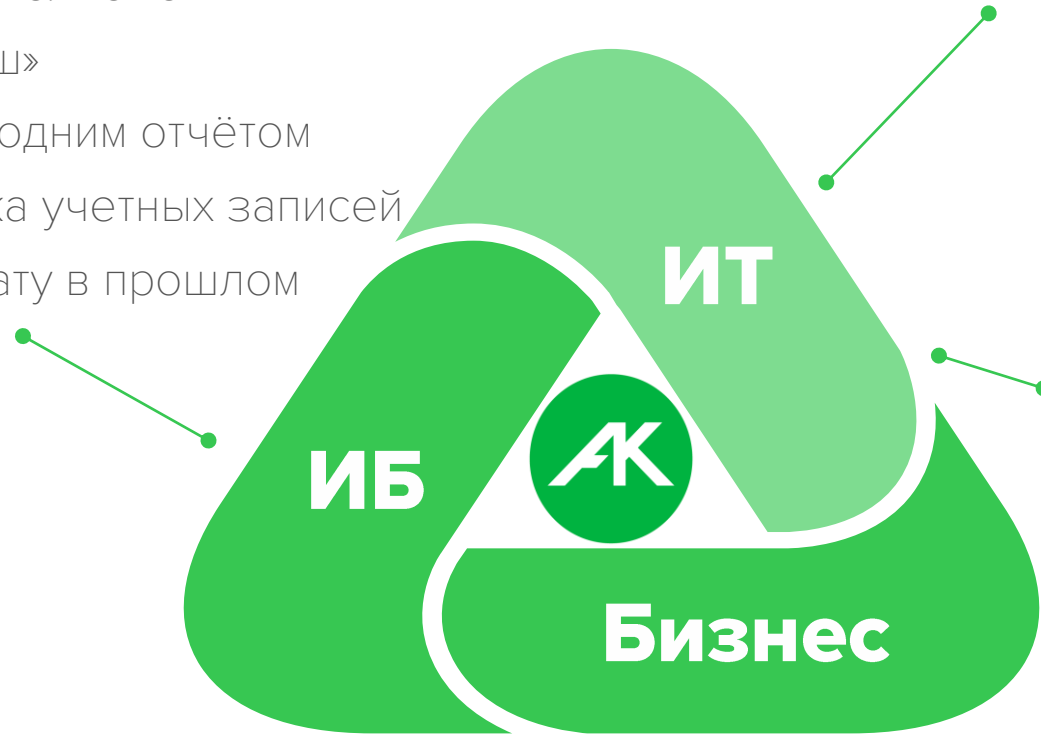
Сетевая папка 1 в иерархии 2.Чтение и запись

_____ | ООС _____

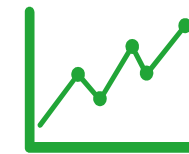
Администратор командировок / Создание задания/заявки на командировку с отправкой на электронное согласование и печать командировочных документов. Ввод и корректировка данных в HR по утвержде...

Соблюдаются интересы и выгоды: ИТ, ИБ, Бизнеса

- Разграничение доступа пользователей
- Оперативное обнаружение изменения полномочий
- Согласование доступа регламентировано
- Контроль кумулятивных полномочий
- Отсутствие «мёртвых душ»
- Аудит всех полномочий одним отчётом
- Оперативная блокировка учетных записей
- Состояние доступа на дату в прошлом



- Автоматизация операций с доступами
- Существенное снижение расходов на аудит полномочий
- Свободные ресурсы для приоритетных ИТ-направлений



- Снижение расходов на управление учетными записями и доступом сотрудников
- Соответствие требованиям регуляторов
- Быстрый ввод сотрудников даже при высокой текучке кадров
- Снижение рисков несанкционированного доступа сотрудников, или инсайдеров

Сопоставимые аппаратные требования

| Число сотрудников | Ядер | ОЗУ | НЖМД* |
|-------------------|------|--------|-------|
| До 1000 | 8 | 16 гб | 500гб |
| 1000 - 5000 | 12 | 32 гб | 1Тб |
| 5 000 - 10 000 | 20 | 64 гб | 2Тб |
| Свыше 10 000 | 40 | 128 гб | 4тб |

Расчёты с учетом 10 подключенных систем и глубиной хранения аудита 1 год


К примеру, для компании в 1000 сотрудников:

Сервер «Yadro Экспресс Филиал» (12 ядер Xeon Gold, 32Гб ОЗУ, 480гб SSD)

Стоимостью **539 220р** (на 01.11.2023г)

**На требования к НЖМД влияют: количество подключаемых систем, их тип, глубина хранимых исторических данных*

Пакеты технической поддержки

| Базовая | Расширенная |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Регистрация заявок круглосуточно | |
| <ul style="list-style-type: none"> • Уведомление об уязвимостях и прочих обстоятельствах препятствующих корректной работе продукта • Консультирование по лицензированию и дальнейшему развитию продукта • Диагностика и устранение проблем базовых функций платформы | <ul style="list-style-type: none"> • Уведомление об уязвимостях и прочих обстоятельствах препятствующих корректной работе продукта • Консультирование по лицензированию и дальнейшему развитию продукта • Диагностика и устранение проблем функционирования и решение конкретных случаев («бизнес-кейсов») • Привлечение к доработке ядра за пределами карты развития продукта (под требование) может оплачиваться отдельно, согласно техническим заданиям. |
| Обновления (минорные патчи, «bug fixing») | Обновления Ankey IDM |
| Реагирование: в течение 24-х часов по рабочим дням 9:00-18:00 | Реагирование: в течение 2-х часов, круглосуточно, 7 дней в неделю  |

Реализованные проекты

Программный комплекс Ankey IDM установлен более чем в 40 компаниях России и СНГ со штатом сотрудников от 720 до 300 000 человек

Показатели на реализованных проектах (на одну инсталляцию):

Максимальное количество подключенных информационных систем: более 1100 систем

Максимальное количество сотрудников под управлением: около 300 000

Максимальное число оформленных заявок в системе за сутки: 58 000 заявок

Максимальный простой системы: 8 часов (проведение регламентных работ)

Сотрудничество

Ознакомьтесь с возможностями

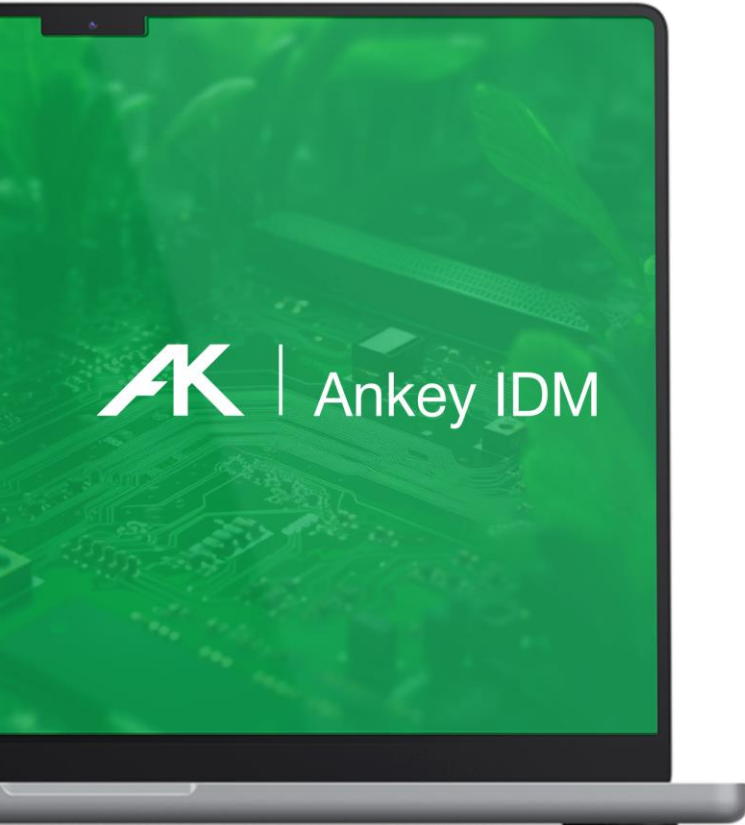
Примите участие в обзорном вебинаре, получите демонстрационную версию с предварительными настройками для базовых систем,

Пилотный проект

Сформулируйте список базовых систем и цели пилотного проекта
Установите и настройте Ankey IDM совместно с нашими специалистами
Подтвердите достижение целей и докажите необходимость использования.

Договор

Согласуйте детали проекта и условия договора на поставку и интеграцию
Проведите совместно опытную эксплуатацию и переведите в продуктив.
Приобретите и активируйте один из пакетов технической поддержки.





СПАСИБО ЗА ВНИМАНИЕ

+7 (812) 677-20-53

sales@gaz-is.ru