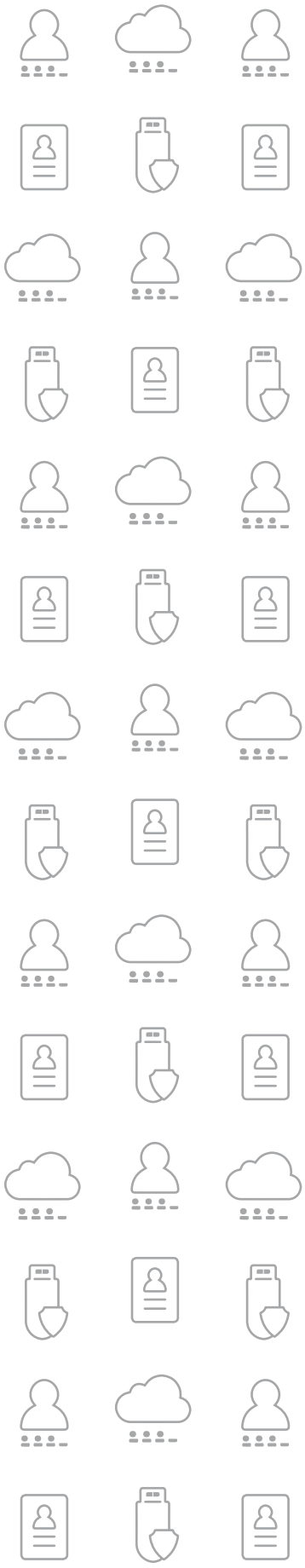
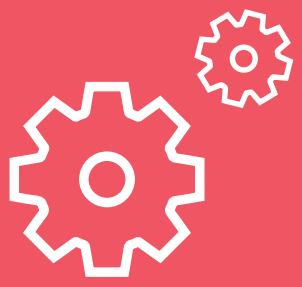


Avanpost IDM

Централизованное управление правами доступа

Avanpost

Более
50
внедрений



О системе

Avanpost IDM – самая современная российская система централизованного управления учетными записями и правами доступа в различных информационных системах компании.

Система позволяет автоматизировать процессы управления жизненным циклом идентификационных данных, повысить уровень информационной безопасности и оптимизировать затраты на администрирование ИТ-инфраструктуры.

Для кого:

Средние и крупные компании и холдинги

Кредитно-финансовые организации

Государственные учреждения, министерства и ведомства

Федеральная налоговая служба РФ

Самый крупный проект

150 000 пользователей

Avanpost IDM обеспечивает:

1. Управление жизненным циклом учетных записей пользователей в соответствии с кадровыми событиями
2. Автоматическое управление правами доступа пользователей на основе ролевой модели
3. Управление заявками на изменение прав доступа пользователей к информационным ресурсам
4. Централизованное управление паролями пользователей
5. Аудит прав доступа пользователей в управляемых системах

Возможности системы Avanpost IDM

- Создание, блокирование и удаление учетных записей на основе кадровой информации и событий (прием, перевод, отпуск, увольнение)
- Назначение, изменение и отзыв прав в соответствии с ролевой моделью
- Автоматическое назначение ролей пользователям на основе кадровых данных
- Ручное назначение ролей через консоль администратора IDM
- Обновление свойств учетных записей при изменении кадровой информации
- Управление парольными политиками для каждого ресурса в отдельности
- Сброс паролей учетных записей пользователей через консоль администратора IDM
- Поиск изменений по учетным записям и правам в целевых системах, выполненных в обход IDM
- Автоматическое и ручное (через консоль администратора IDM) устранение выявленных расхождений по учетным записям и правам
- Создание отчетов по историческим данным с возможностью выгрузки в pdf и xls
- Гибкая настройка бизнес-процессов управления заявками на доступ с помощью конструктора, настраиваемых справочников и вычисляющих функций
- Личный кабинет пользователя с возможностью создания заявки на доступ, изменения личных данных и сброса паролей для своих учетных записей
- Личный кабинет руководителя с возможностью просмотра и изменения кадровых данных и прав доступа его сотрудников
- Кадровая консоль для создания дополнительных подразделений и должностей, а также учетной карточки внештатного пользователя с возможностью расширения типов кадровых данных (телефон, номер кабинета и др.)
- Управление заявками на доступ разных типов (для себя, для сотрудников, «как у сотрудника», на время, отзыв прав, блокировка и разблокировка учетных записей, изменение личных данных и др.)
- Почтовые рассылки, настраиваемые на события в IDM (создание и блокирование учетных записей, назначение и отзыв прав, изменение свойств учетных записей, генерация и сброс паролей, аудит целевых систем, согласование и обработка заявок и др.)

Управление заявками

Avanpost IDM имеет развитый сервис самообслуживания, предназначенный для автоматизации приема, согласования и исполнения запросов пользователей, связанных с изменением прав доступа, состояния и атрибутов учетных записей.

Инструмент позволяет просматривать текущий набор своих учетных записей и прав доступа, а также прав доступа подчиненных, изменять пароли своих учетных записей через веб-интерфейс и создавать заявки.

Стандартный набор заявок включает следующие виды:

на предоставление / отзыв доступа

на блокировку / разблокировку учетной записи

на изменение личных данных

Такой комплект позволяет автоматизировать основные процессы управления доступом по запросам пользователей. Кроме этого, возможно создание индивидуальных форм заявок на этапе внедрения.

Работу сервиса обеспечивает мощный движок управления бизнес-процессами. С помощью графического редактора он позволяет разработать отдельный бизнес-процесс для каждого вида заявки, состоящий из неограниченного количества блоков, которые включают взаимодействие с пользователями (согласование, визирование, исполнение, уведомления), взаимодействие с сервисами, управляющие конструкции и служебные блоки.

Движок позволяет организовать как последовательную, так и параллельную обработку заявки группами пользователей, реализовать интеграцию бизнес-процессов со смежными системами, контролировать и запускать активности по расписанию и запускать бизнес-процесс по любому событию, полученному или сгенерированному в IDM.

Построение ролевой модели

Avanpost Role Manager – уникальный инструмент Avanpost IDM, позволяющий существенно упростить создание ролевой модели на предприятии любого масштаба.

Если ранее «ручное» создание ролевой модели занимало несколько месяцев, то автоматизированный механизм аналитического построения ролей сделает это за несколько часов.

Avanpost Role Manager сравнивает существующие наборы прав пользователей по принципу похожести и нахождения сотрудников на одинаковых должностях, даже если они будут отличаться в названии.

По результатам сравнения он предлагает предварительную ролевую модель с возможностью ручного редактирования до необходимого результата. Полученный финальный вариант можно автоматически загрузить в Avanpost IDM и запустить систему в промышленную эксплуатацию.

Одной из интересных функциональных особенностей модуля Avanpost Role Manager является возможность выявить различия в правах между сотрудниками с одинаковыми должностными обязанностями и просигнализировать об этом администратору безопасности для последующей оценки правомерности дополнительного доступа.

Зачем нужен IDM?

1. Автоматизация рутинной ручной работы по созданию большого количества учетных записей и предоставлению прав доступа в информационных системах
2. Организация автоматизированных процессов согласования и исполнения запросов, связанных с изменением прав доступа
3. Одновременное предоставление или изменение прав доступа большому количеству сотрудников
4. Контроль за предоставлением и изменением прав доступа сотрудников и проведение расследований инцидентов информационной безопасности
5. Своевременное блокирование доступа уволенных сотрудников, что позволяет решить проблему так называемых «мертвых душ»

Почему Avanpost IDM?

- Единственное российское решение, имеющее подтверждённые масштабные внедрения и проверенное временем
- Полностью российское решение (входит в Единый реестр отечественного ПО), русскоязычный интерфейс
- Инструмент автоматического создания ролевой модели в комплекте
- Соответствие требованиям законодательных актов, в частности 152-ФЗ «О персональных данных», руководящих документов ФСТЭК и ФСБ, в частности Приказ ФСТЭК от 18 февраля 2013 г. № 21, отраслевых стандартов, в частности СТО БР ИББС-1.0-2014 и PCI DSS
- Масштабируемость и возможность кастомизации
- Гибкая политика лицензирования
- Невысокие начальные затраты на внедрение и низкая стоимость владения
- Наличие большого количества готовых коннекторов к информационным системам, представленным на российском рынке
- Возможность разработки коннекторов по требованиям заказчиков
- Низкие требования к вычислительным мощностям
- Регулярный выпуск релизов с учетом текущих потребностей заказчиков
- Открытые документированные API и развитые возможности интеграции
- «Бесшовная» интеграция с другими решениями линейки Avanpost (PKI, SSO)

Бизнес-кейсы

РоссельхозБанк

30 000
пользователей

бумажный
документооборот

6
месяцев

Задача: обеспечить быстрый и прозрачный процесс изменения прав доступа работников операционных офисов.

Решение: в рамках проекта был разработан и согласован обобщенный процесс запроса прав доступа, включающий несколько видов заявок: на предоставление доступа, на отзыв доступа, на блокировку и разблокировку учетных записей с возможностью запроса на временной период. Для каждого из видов заявок был создан маршрут согласования и исполнения, включающий согласование руководителями, определяющимися на основании данных кадровой системы и ответственными, гибко вычисляемыми в контексте запрошенных прав и ресурса, а также автоматическое или ручное исполнение запроса в зависимости от типа подключения системы.

В результате внедрения Avanpost IDM заказчик получил единую, понятную пользователю форму запроса прав доступа. Были автоматизированы действия администраторов, процессы согласования заявок и проверки SOD-конфликтов в момент подачи заявки. Это позволило полностью отказаться от бумажного документооборота.

Среднее время согласования и исполнения запроса пользователя сократилось до 3 часов, количество отклоняемых согласующими заявок упало с 30% до 5%, 80% запросов на изменение прав доступа или состояния учетной записи стали исполняться автоматически.

lamoda

5 500 пользователей

массовый подбор

6 месяцев

Задача: обеспечить оперативное создание учетных записей и предоставление прав доступа работникам, массово принимаемым на рядовые позиции и проходящим стажировку.

Решение: в Avanpost IDM был реализован интерфейс кадровой консоли, с помощью которой осуществляется учет стажеров, не учтенных в кадровой системе компании. В случае положительных результатов стажировки, сотрудник принимается на работу и проводится в кадровой системе, при этом Avanpost IDM не создает новую учетную запись, а объединяет карточки сотрудника из кадровой системы компании и кадровой консоли. При отрицательном результате стажировки, если работник так и не был заведен в кадровую систему, IDM проводит блокировку его учетной записи в течении двух недель с момента создания карточки сотрудника.

Кроме того, в результате внедрения Avanpost IDM был автоматизирован процесс авторизации пользователей в информационных системах. Заказчик получил возможность создания учетных записей новому сотруднику или автоматической блокировки уволенного сотрудника в течение 3-х часов после внесения изменений в кадровой системе.

ДИТ

80 000 пользователей

100 информ. систем

импорто-замещение

2 этапа в течение года

Задача: обеспечить управление правами доступа в децентрализованных организационной и ИТ-инфраструктурах.

Решение: в рамках системы управления доступом к информационным ресурсам (СУДИР) каждый орган исполнительной власти получил интерфейс, с помощью которого администраторы могут управлять доступом сотрудников в информационные системы, принадлежащие данному органу, а также запрашивать доступк системам других органов и управлять состоянием аккаунтов сотрудников. Владельцы систем, в свою очередь, могут согласовывать заявки на доступ госслужащих и сотрудников подведомственных организаций в свои информационные системы. А удобство пользователей обеспечено едиными логином и паролем для входа в информационные системы.

Внедрение позволило сократить издержки на администрирование пользовательских аккаунтов и делегировать функции управления учетными записями сотрудников в информационных системах Правительства Москвы на уровень органов исполнительной власти, сохранив контроль владельцев систем за доступом к их ресурсам.

Компоненты системы

Коннекторы к доверенным источникам — интеграционные модули, позволяющие загружать и обновлять данные о пользователях из источников различных типов, таких как кадровые системы, файловые ресурсы, доменные службы и т.д.

Сервис синхронизации — служба, обеспечивающая синхронизацию, обновление, объединение данных и выявление изменений в доверенных источниках. Служба поддерживает актуальное состояние метакаталога и порождает события при выявлении изменений в процессе синхронизации.

Метакаталог — база данных, хранящая информацию о текущем состоянии организационной структуры, пользователях и связанных с ними атрибутах, а также историческую информацию и события.

Редактор каталога — веб-приложение, обеспечивающее возможность корректировки информации из внешних источников и ручное ведение каталога (создание и редактирование оргструктуры, данных пользователей).

Модуль управления доступом — корневой компонент IDM-системы, реализующий логику управления доступом на основе ролевой модели.

Модуль управления бизнес-процессами — управляет исполнением бизнес-процессов, обеспечивающих обработку запросов пользователей и запросов, порожденных кадровыми событиями.

Модуль исполнения политик — механизм, отвечающий за применение политик, связанных с ролевой моделью (SOD, Access control), кадровыми событиями, изменением паролей и т.д.

Механизм проверки соответствия — механизм выявления и контроля несанкционированных действий в управляемых системах. Сравнивает актуальное состояние учетных записей и прав в системе с моделью IDM, устраняет расхождения и порождает инциденты безопасности.

Портал самообслуживания — веб-приложение, основной интерфейс IDM, предназначенный для пользователей предприятия. Позволяет оформлять заявки на изменение прав доступа, управлять своими учетными записями в системах, управлять доступом подчиненных сотрудников, а также обеспечивает интерфейс для выполнения задач участниками бизнес-процессов.

Консоль администратора — веб-интерфейс, обеспечивающий настройку основных механизмов и справочников IDM, контроль за состоянием компонентов и очередей задач.

Консоль администратора безопасности — веб-интерфейс, предназначенный для обработки инцидентов, просмотра отчетов по данным IDM.

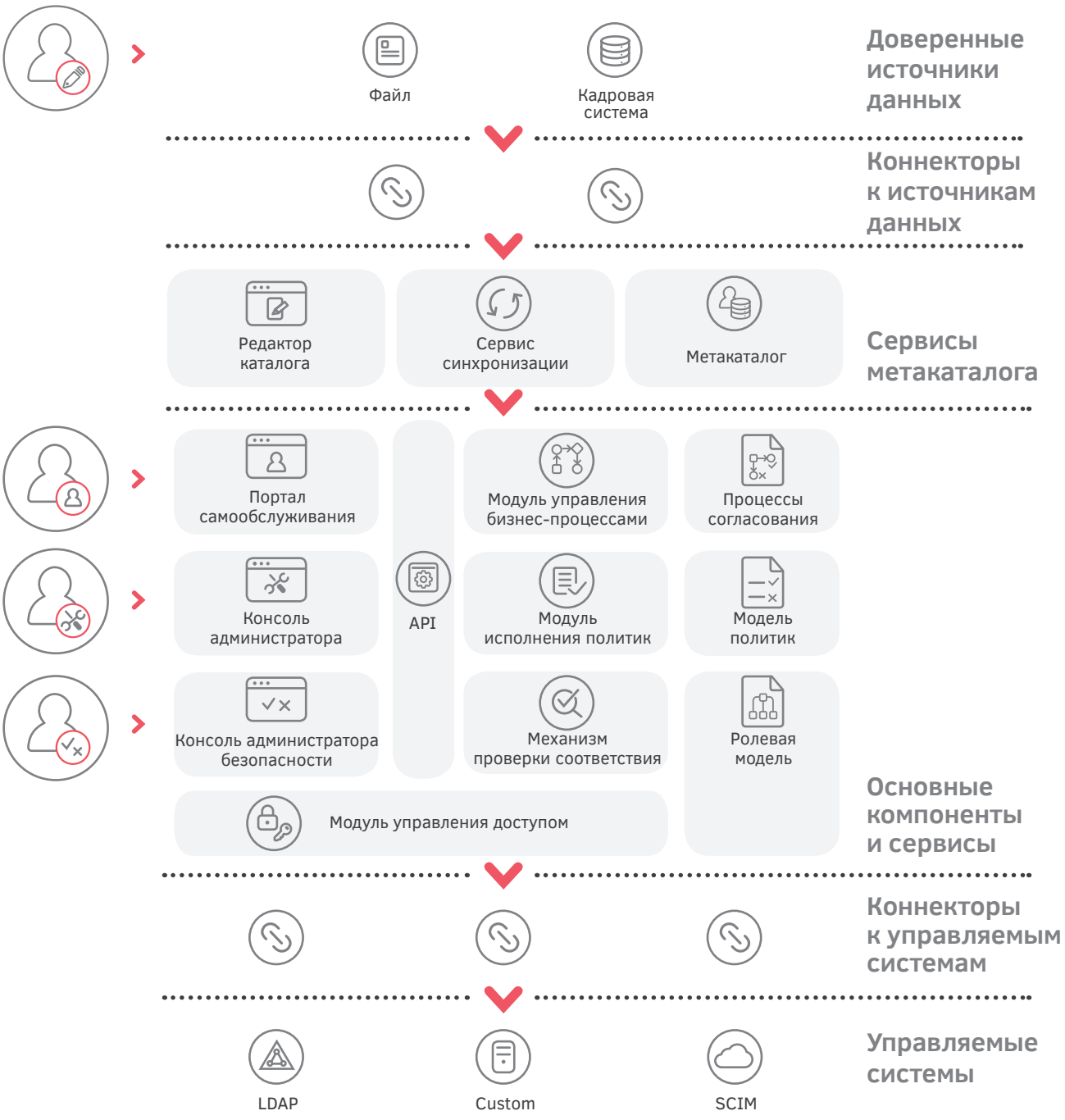
API — веб-сервисы и разделяемые библиотеки. Обеспечивают взаимодействие компонентов между собой, интеграцию со смежными системами и возможность разработки кастомных сервисов, реализующих специфичные требования.

Коннекторы к управляемым системам — интеграционные модули, реализующие функции управления доступом в конкретных системах. Абстрагируют ядро IDM от деталей реализации управляемых систем, приводят модель безопасности системы к модели IDM.

Архитектура Avanpost IDM

Avanpost IDM построен с использованием современных принципов модульной архитектуры.

Основные компоненты выполнены как отдельные веб-приложения и службы, взаимодействующие между собой через сервисную шину и REST API. Такая архитектура обеспечивает горизонтальную масштабируемость и отказоустойчивость решения, позволяет изолировать критичные компоненты в отдельном контуре, а также предоставляет обширные возможности интеграции и необходимый уровень гибкости.



Факты об эффективности Avanpost IDM

Сокращение среднего времени согласования
и исполнения заявки на изменение доступа
с 5-ти дней до 2-х часов

Снижение нагрузки
на группу администраторов почтовой системы
на 40%

Предоставление нового права
или заполнение атрибута учетной записи в системе
в течении 1 часа

Создание учетных записей
и предоставление базовых прав пользователю
в течении нескольких минут
с момента проведения приказа
о приеме на работу в кадровой системе

Управление ролевой моделью, включающей
более 3000 бизнес-ролей
и более 5 000 000 атомарных прав
и полномочий в отдельных информационных системах

Достаточно **2-х виртуальных серверов**
для управления инфраструктурой, включающей
30 000 пользователей, 4 ИТ-ресурса, 2 500 ролей,
600 заявок в день

Возможности интеграции

Интеграция Avanpost IDM с информационными ресурсами организации осуществляется посредством модулей, отвечающих за взаимодействие IDM с внешними системами — коннекторов, которые позволяют связать IDM с любыми прикладными элементами корпоративной информационной системы.

Интеграционная инфраструктура Avanpost IDM удовлетворяет следующим требованиям:

1. Наличие готовых интеграционных модулей к популярным информационным системам
2. Возможность интеграции в SOA-инфраструктуру предприятия, имеющуюся интеграционную инфраструктуру уровня предприятия
3. Присутствие универсальных интеграционных решений, подходящих для реализации взаимодействия с большинством собственных решений заказчика
4. Существование документации и библиотек для самостоятельной разработки интеграционных модулей
5. Наличие точек интеграции для построения сквозных бизнес-процессов с внешними системами

Коннекторы к доверенным источникам

Кадровые системы: 1С ЗУП, SAP HR, Oracle HR, Босс Кадровик, Диасофт, Галактика и др.

Прочие: LDAP, Excel, SCV, XML и др.

Коннекторы к целевым системам

ОС: Windows, Linux

СУБД: Oracle, My SQL, PostgreSQL, Informix, InterBase

Платформы и прикладное ПО: Exchange, Lotus, SharePoint, SAP, 1C, Directum

Веб-сервисы: SCIM, SOAP, REST

Avanpost IDM позволяет организовать управление учетными записями и правами доступа к виртуальным ресурсам — информационным системам, для которых по решению заказчика не будет создано прямого физического подключения к IDM (системы, находящиеся в защищенном сегменте, к которому нет доступа извне; системы, которые планируется в ближайшее время вывести из эксплуатации и т.п.).

О Компании Аванпост

Аванпост — ведущий российский разработчик систем идентификации и управления доступом.

Компания работает на рынке информационной безопасности с 2007 года и к настоящему моменту является технологическим лидером в сегменте Identity Management.

Наши решения:

Avanpost IDM
система централизованного управления доступом к корпоративным ресурсам

Avanpost PKI
система управления всеми элементами PKI-инфраструктуры из единого центра

Avanpost SSO
система управления аутентификацией пользователей в корпоративных ресурсах

Avanpost Web SSO
система управления аутентификацией пользователей в web-ресурсах

Нам доверяют:

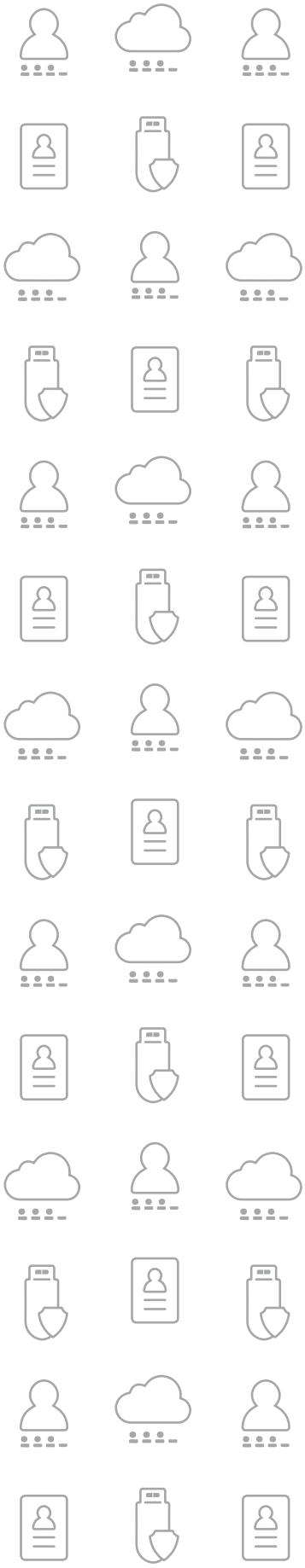
РОСНАНО
Ростех
РОСНЕФТЬ
ДИТ
РоссельхозБанк
Федеральная налоговая служба
КАЛАШНИКОВ КОНЦЕРН
МОСВОДОКАНАЛ
Шереметьево Карго
АРМЗ
МОСКОВСКИЙ ИНДУСТРИАЛЬНЫЙ БАНК
РОСГОССТРАХ БАНК
Северсталь
МТС
Мультикарта
ВЭБ БАНК РАЗВИТИЯ
Федеральная грузовая компания
lamoda
РТИ
ТРАСТ
МСП БАНК

10 лет
опыта в ИБ

Более
100 партнеров
в России и странах СНГ

Более
2 000 000
пользователей

Более
70 успешных
проектов



109129, Россия, Москва,
ул. 8-я Текстильщиков, д. 11, стр. 2

+7 (495) 641-80-80
info@avanpost.ru
www.avanpost.ru