ПЕРЕДОВЫЕ ТЕХНОЛОГИИ
ДЛЯ СОВРЕМЕННОЙ КИБЕРБЕЗОПАСНОСТИ

КОМПАНИЯ ИНДИД

КОМПАНИЯ
ИНДИД

НАША КОМПАНИЯ

14+

ЛЕТ ОПЫТА

Проектирование, разработка, тестирование и внедрение комплексных решений

200+

АКТИВНЫХ ЗАКАЗЧИКОВ

90+

РЕГИОНАЛЬНЫХ ПАРТНЕРОВ

80+

СОТРУДНИКОВ

Распределенная команда: 4 региона, 3 страны

3

ПРОДУКТА

Полностью самостоятельная разработка

КОМАНДА ЭКСПЕРТОВ

Для представления коллектива мы выбрали специалистов технической поддержки — именно они первыми приходят на помощь нашим заказчикам.

АНТОН ШЛЫКОВ

Руководитель службы технической поддержки

НИКОЛАЙ ИЛЬИН

Эксперт по аутентификации пользователей

МИХАИЛ ЯКОВЛЕВ

Эксперт по управлению цифровыми сертификатами

МАКСИМ КУЗЬМОВ

Эксперт по управлению привилегированными учетными записями

ОБРАЗОВАНИЕ

Большинство сотрудников компании Индид имеют профильное высшее образование и владеют иностранными языками, многие ежегодно повышают квалификацию. Четверо имеют степень кандидата наук.

ОПЫТ

Ключевые сотрудники и руководители обладают более чем 15-летним опытом в сфере разработки программного обеспечения для информационной безопасности. Они регулярно выступают на профильных конференциях и представляют компанию на отраслевых выставках.

СОВРЕМЕННЫЙ ПОДХОД

Команды разработки и тестирования используют современные технологии и методы, поэтому мы легко подстраиваем наши решения под индивидуальные запросы заказчиков.

ОТРАСЛЕВЫЕ РЕШЕНИЯ

ФИНАНСЫ

Специализированные решения для управления цифровыми сертификатами и доступом пользователей позволяют добиться высочайших показателей кибербезопасности и непрерывности бизнеса в соответствии с требованиями регуляторов.

ЭНЕРГЕТИКА

Централизованное управление цифровыми сертификатами и контроль действий разных групп пользователей — приоритетная задача для сектора с распределенной инфраструктурой и большим разнообразием информационных систем.

ПРОМЫШЛЕННОСТЬ

Современные производители широко используют цифровые технологии, поэтому им жизненно необходимы средства для защиты от несанкционированного доступа к управлению технологическими процессами.

ТЕЛЕКОММУНИКАЦИИ

Специфика сектора — размытый периметр безопасности, удаленная работа сотрудников, использование мобильных устройств и облачных сервисов — требует особого внимания к защите и дополнительному онтролю.

ТРАНСПОРТ

По мере развития компаний отрасли и автоматизации их рабочих процессов растет потребность в надежной и эффективной аутентификации сотрудников при доступе к разнообразным бизнес-приложениям.

РИТЕЙЛ

Централизованные решения с функциями самообслуживания позволяют легко решать задачи управления цифровыми сертификатами и ключевыми носителями в масштабах федеральной розничной сети.

ОТЗЫВЫ КЛИЕНТОВ

АЛЕКСАНДР ЛАВРОВ

Начальник службы безопасности
СТС Медиа

СТС

Внедрение многофакторной аутентификации сотрудников и контроль действий администраторов, подрядчиков и тех, кто работает в удаленном формате, – это этапы комплексной работы над повышением уровня информационной безопасности компании. Сейчас мы закрыли парольную брешь линейных сотрудников и пользователей, имеющих привилегированные права, то есть многократно снизили количество потенциальных несанкционированных точек входа в нашу систему извне и тем самым защитили расширяющиеся границы периметра информационной безопасности.

АНАТОЛИЙ СКОРОДУМОВ

Начальник управления по обеспечению информационной безопасности Банк «Санкт-Петербург»

БАНК САНКТ-ПЕТЕРБУРГ

Нам удалось убедить бизнес в экономической целесообразности внедрения системы биометрической аутентификации прежде всего из-за неотделимости аутентификаторов (пальцев) от пользователя. Передать аутентификатор физически нельзя, и подделать его при современном уровне сканеров отпечатков пальцев достаточно сложно. Ушли все риски, связанные с проблемами использования парольного доступа и компрометацией: с подбором пароля, с передачей пароля коллегам по работе, с записью паролей в блокнотах, на листочках календаря, на стикерах, приклеиваемых к монитору.

ВЛАДИМИР СОЛОНИН

Директор по информационной безопасности
СДМ-Банк

СДМБАНК

Внедрение было комплексным. Внедрялось сразу несколько систем, отвечающих за создание новых пользователей при заведении в кадровую систему, а также за автоматизированную смену паролей, управление сертификатами пользователей, ограничение доступа в случае отпуска или ухода из офиса. Важный критерий выбора вендора – российское происхождение. Простота внедрения, опыт успешных внедрений в банках, качественная поддержка и открытость к пожеланиям заказчика – тоже важные факторы. Мы несем ответственность перед клиентами за то, чтобы системы защиты работали, а новые внедряемые системы не усложняли существующие процессы.

INDEED ACCESS MANAGER

Защита доступа к информационным системам

ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ И УПРАВЛЕНИЕ ДОСТУПОМ

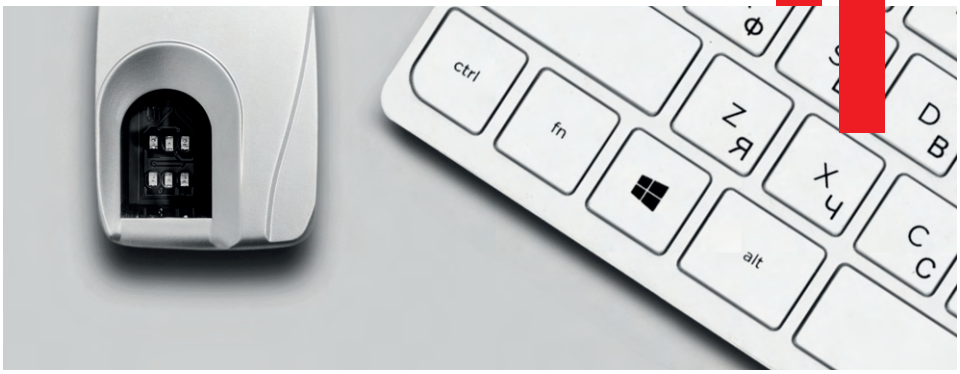
1. Единая система аутентификации для всех корпоративных ресурсов, информационных систем и бизнес-сервисов
2. Реализация механизма единого входа Single Sign-On
3. Общий журнал событий доступа с персонификацией каждого подключения
4. Различные сценарии и комбинации аутентификации сотрудников
5. Политики управления доступом: на уровне пользователя, приложения, протокола или группы

УСИЛЕННАЯ И МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

1. Поддержка различных технологий аутентификации: биометрия, аппаратные аутентификаторы, одноразовые пароли
2. Различные комбинации аутентификаторов в зависимости от сценария и способа аутентификации
3. Управление аутентификаторами: назначение, отзыв, блокировка
4. Сервисы самообслуживания пользователей для управления собственными аутентификаторами
5. Хранение и автоматическая смена паролей для исключения их несанкционированного использования в обход системы усиленной аутентификации

МЕХАНИЗМЫ ИНТЕГРАЦИИ

1. Поддержка любых корпоративных веб-приложений с помощью технологии Single Sign-On
2. Поддержка целевых ресурсов: IIS, Microsoft Windows, Microsoft RDS
3. Поддержка протоколов аутентификации: AD/LDAP, RADIUS, SAML, ADFS, OpenID Connect
4. Интеграция с системами класса Identity Management
5. API для интеграции с иными системами
6. Интеграция с SIEM через syslog



С ПОМОЩЬЮ INDEED AM ВЫ СМОЖЕТЕ:

ПОСТРОИТЬ СИСТЕМУ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ

- Управление доступом пользователей на базе политик
- Журналирование всех попыток входа в приложения
- Сокращение издержек использования паролей
- Web SSO, Enterprise SSO

ПЕРЕЙТИ НА БИОМЕТРИЧЕСКУЮ АУТЕНТИФИКАЦИЮ

- Различные технологии: 3D/2D-лицо, отпечаток пальца, ладонь
- Биометрическая идентификация пользователей
- Комбинирование биометрии с традиционными методами аутентификации

ЗАЩИТИТЬ УДАЛЕННЫЙ ДОСТУП

- Двухфакторная аутентификация для доступа в локальную сеть (VDI), для удаленных рабочих столов (RDP) и веб-приложений
- Аутентификация, адаптированная под удаленный режим работы: OTP, SMS, Email, push-уведомления

ОБЪЕДИНИТЬ ЛОГИЧЕСКИЙ И ФИЗИЧЕСКИЙ ДОСТУП

- Вход в ПК и приложения по пропуску СКУД
- Поддержка различных RFID-карт: Mifare, EM Marin, HID Prox, HID iClass
- Интеграция со СКУД

Больше решений – на сайте

Важными критериями для нас были: наличие полноценной технической поддержки для оперативного решения вопросов, возникающих в ходе внедрения и эксплуатации системы, а также простота и удобство использования системы, поскольку пользователи обладают различным уровнем знаний в области информационных технологий.

ИВАН ЧЕРНОКНИЖНИКОВ

Руководитель IT-отдела компании «Газпром сера»

INDEED PRIVILEGED ACCESS MANAGER

Защита привилегированного доступа

ЗАЩИТА ПРИВИЛЕГИРОВАННОГО ДОСТУПА

1. Единые политики управления привилегированным доступом
2. Поддержка протоколов удаленной работы: SSH, RDP, HTTP(s), различные проприетарные протоколы
3. Двухфакторная аутентификация пользователей для усиленной защиты привилегированных учетных записей: пароль + TOTP (программный генератор), смарт-карта (PKI)
4. Независимость от особенностей рабочих станций пользователей, целевых серверов и приложений
5. Запрет на изменение правил доступа самим привилегированным пользователем
6. Автоматический импорт перечня ресурсов из Active Directory

КОНТРОЛЬ ПРИВИЛЕГИРОВАННЫХ СЕССИЙ

1. Мониторинг в режиме реального времени и механизм разрыва активной сессии
2. Различные механизмы фиксации действий: видео- и текстовая запись сессий, клавиатурный ввод, вводимые команды, передача файлов
3. Журналирование событий с указанием того, кто, куда и под какой учетной записью выполнял вход и как долго длилась сессия
4. Отправка уведомлений по протоколу SMTP
5. Отправка журналов в SIEM по протоколу syslog

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ УЧЕТНЫМИ ЗАПИСЯМИ

1. Предоставление административного доступа без раскрытия пароля привилегированной учетной записи
2. Поддержка работы с учетными записями: Active Directory, Linux/Unix, Windows, СУБД (MS SQL, MySQL, PostgreSQL, Oracle DB)
3. Механизмы управления учетными записями: поиск и автоматическое предоставление целевым ресурсам, ведение истории паролей, автоматическая смена паролей и SSH-ключей
4. Сквозная аутентификация на целевых серверах и в целевых приложениях

С ПОМОЩЬЮ INDEED PAM ВЫ СМОЖЕТЕ:

ЗАЩИТИТЬ ПРИВИЛЕГИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ

– Защищенное хранилище учетных записей
– Исключение несанкционированного использования паролей
– Сохранение истории паролей
– Обнаружение незарегистрированных привилегированных учетных записей

ВЫПОЛНИТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

– Идентификация и аутентификация сотрудников
– Управление доступом и аудит
– ФСТЭК, ГОСТ, PCI DSS, ISO

ОРГАНИЗОВАТЬ АУДИТ РАБОТЫ АДМИНИСТРАТОРОВ

– Различные механизмы фиксации действий и событий доступа
– Повышение эффективности расследования инцидентов и сбоев
– Исключение необоснованных обвинений в отношении сотрудников

КОНТРОЛИРОВАТЬ ДОСТУП ПОДРЯДЧИКОВ

– Списки разрешенных и запрещенных команд
– Подключение после обязательного подтверждения администратором PAM
– Выдача доступа на время или только в рабочие часы

Больше решений – на сайте

PAM имеет в своей структуре компоненты для контроля действий сотрудников – администраторов системы. Теперь мы можем в любой момент самостоятельно расследовать любой инцидент, произошедший в информационной системе компании. Эффект роста самодисциплины распространился не только на тех, кому предоставлена возможность административного управления системой.

НИКОЛАЙ ЧУПРИН

Руководитель отдела информационных систем группы компаний «ЕПК»

INDEED CERTIFICATE MANAGER

Цифровая подпись, управление сертификатами

ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ И УПРАВЛЕНИЕ

1. Централизованные политики выпуска сертификатов
2. Автоматизация типовых операций по управлению цифровыми сертификатами
3. Использование клиентского агента для назначения задач управления цифровыми сертификатами и их носителями на рабочих станциях пользователей (обновление и отзыв сертификатов, смена PIN-кода и т. д.)
4. Постановка под контроль цифровых сертификатов сторонних УЦ
5. Сервис самообслуживания пользователей

АУДИТ ИНФРАСТРУКТУРЫ PKI

1. Журналирование операций с сертификатами и ключевыми носителями
2. Панели мониторинга, отображения сводной информации и состояния системы
3. Отправка уведомлений по протоколу SMTP
4. Отправка журналов в SIEM по протоколу syslog
5. Генерация журналов учета средств криптографической защиты информации (СКЗИ)

ТЕХНОЛОГИЧЕСКАЯ ИНТЕГРАЦИЯ

1. Поддержка ключевых носителей сертификатов: Rutoken, eToken, ESMART, JaCarta, AvestKey, ID Prime и других
2. Поддержка удостоверяющих центров: КриптоПро УЦ, InfoTeCS CA, Windows CA и других
3. Поддержка технологий виртуальных/сетевых носителей: Indeed AirCard, TPM, Windows Hello for Business, Реестр
4. Поддержка принтеров смарт-карт
5. API для интеграции с иными системами
6. Интеграция с SIEM через syslog

С ПОМОЩЬЮ INDEED CM ВЫ СМОЖЕТЕ:

СОКРАТИТЬ ЗАТРАТЫ НА СОПРОВОЖДЕНИЕ PKI

- Поддержка любых ключевых носителей
- Автоматизация задач управления пользовательскими сертификатами
- Своевременное обновление сертификатов
- Сервис самообслуживания пользователей
- Дашборд администратора

ВНЕДРИТЬ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ И ЭЛЕКТРОННУЮ ПОДПИСЬ

- Любые виды подписи: НЭП, КЭП, УКЭП
- Поддержка виртуальных смарт-карт и WHfB
- Одновременная работа с разными УЦ (Microsoft, КриптоПро)

ОРГАНИЗОВАТЬ ВЫПУСК КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

- Интеграция с КриптоПро УЦ и DSS
- Публикация сертификатов в ЕСИА
- Проверка данных пользователя в ПФ, ФНС

ВЕСТИ УЧЕТ СКЗИ СОГЛАСНО ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

- Ведение журнала СКЗИ
- Автоматические внесение записей в журнал
- Выгрузка журнала для отчетности
- Учет любых типов СКЗИ

Больше решений – на сайте

Мы стали использовать смарт-карты для аутентификации и дополнительным бонусом получили сертификат, который будем применять для электронной подписи в электронной почте и в офисных документах, а совместив чип с сертификатом и пропуск — интегрировали систему со СКУД. Организовали работу процессов, связанных с жизненным циклом пропусков, порядком их выдачи и замены.

ВЛАДИМИР СОЛОНИН

Директор по информационной безопасности СДМ-Банка

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

ВТБ

Проведена замена конкурирующего решения по управлению цифровыми сертификатами и ключевыми носителями. Организован мониторинг подключаемых устройств на рабочих местах пользователей. Заказчик использует смарт-карты различных производителей, поэтому для реализации проекта была проведена доработка программного комплекса.

Продукты: рутокен Keybox (Indeed CM)

Охват пользователей: более 70 тыс.

МАГНИТ

В результате внедрения автоматизирован процесс и усилен контроль за использованием сертификатов электронной подписи ЕГАИС. Заказчик активно применяет инструменты выпуска и обновления сертификатов для аутентификации в ОС и полностью контролирует инфраструктуру виртуальных смарт-карт, включая выпуск и управление.

Продукты: Indeed CM

Охват пользователей: более 100 тыс.

Домодедово
Московский аэропорт

Решены задачи по обеспечению прозрачного доступа пользователей в целевые приложения и созданию централизованной системы двухфакторной аутентификации сотрудников на рабочих местах – терминалах общего доступа, расположенных на территории аэропорта. Внедрена двухфакторная аутентификация с использованием биометрических сканеров рисунка вен ладони и RFID-карты.

Продукты: Indeed AM, Indeed AM ESSO

Охват пользователей: более 16 тыс.

БАНК САНКТ-ПЕТЕРБУРГ

Решены задачи по созданию централизованной системы беспарольной биометрической аутентификации сотрудников по отпечатку пальца. Оптимизированы процессы защиты от несанкционированного доступа в приложения, жизненно важные для бизнеса. Внедрены платформы для управления цифровыми сертификатами и ключевыми носителями, а также для защиты привилегированного доступа.

Продукты: Indeed AM, Indeed AM ESSO, Indeed PAM, Indeed CM

Охват пользователей: более 5 тыс.

ГАЗПРОМ НЕФТЬ

Внедрена система защиты подключений по протоколу удаленного доступа с использованием многофакторной аутентификации сотрудников. Одновременно применяются несколько методов аутентификации для различных групп пользователей. Автоматизированы и защищены процессы получения пользователями уведомлений с разными видами одноразовых паролей.

Продукты: Indeed AM, Indeed AM ESSO, Indeed PAM, Indeed CM

Охват пользователей более 28 тыс.

Альфа-Банк

В результате внедрения программного комплекса создана централизованная система беспарольной аутентификации мобильных (удаленных) сотрудников. Реализованы механизмы двухфакторной аутентификации при подключении по протоколу VPN. В качестве второго фактора аутентификации используется одноразовый пароль, который генерируется на смартфоне сотрудника.

Продукты: Indeed AM, Indeed AM ESSO

Охват пользователей: более 2,5 тыс.

СТС

Решена задача по обеспечению единой точки входа для пользователей разных доменов с ресурсами, опубликованными через RDS на разных площадках с использованием многофакторной аутентификации. Также внедрена платформа контроля действий привилегированных пользователей – администраторов систем и подрядчиков компании.

Продукты: Indeed AM, Indeed PAM

Охват пользователей: более 1 тыс.

O'KEY

Внедрена система защиты и управления доступом к привилегированным учетным записям. Для реализации задач контроля используется механизм, позволяющий персонифицировать подключения. Для расследования инцидентов активно применяется полнотекстовый поиск по сессиям, мониторинг действий пользователя и вводимых им команд.

Продукты: Indeed PAM

Охват пользователей: более 1 тыс.

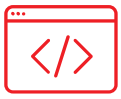
НАШИ ПРЕИМУЩЕСТВА

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

- ISO 27001.2013 (менеджмент информационной безопасности)
- PCI DSS V.3.2.1 от 05.2018 (защита данных держателей карт)
- Приказ ФСТЭК № 17 от 11.02.2013 (защита ГИС)
- Приказ ФСТЭК № 21 от 18.02.2013 (защита ПДн)
- Приказ ФСТЭК № 31 от 14.03.2014 (защита АСУ ТП)
- Приказ ФСТЭК № 239 от 25.12.2017 (защита ОКИИ)
- ГОСТ 57580.1-2017 (защита финансовых операций)
- Приказ ФАПСИ №152 (порядок использования СКЗИ)

ПОДДЕРЖКА КЛИЕНТА НА ВСЕХ ЭТАПАХ ВНЕДРЕНИЯ

Наша команда может провести для заказчика вебинар о работе продуктов или их пилотное внедрение. Специалисты технической поддержки принимают участие во внедрении продукта в рамках полного цикла – от пилотного проекта до окончания использования. Благодаря этому заказчик может оценить работу программного обеспечения в своей информационной системе.



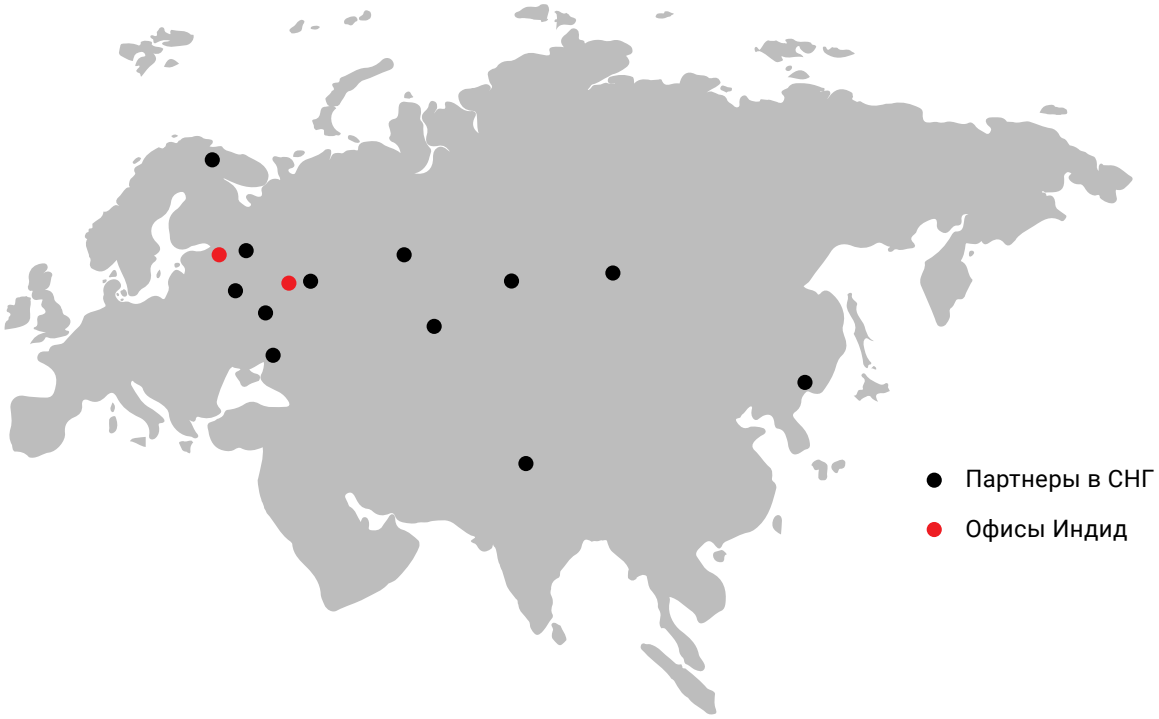
ИНДИВИДУАЛЬНАЯ ДОРАБОТКА ПРОГРАМНОГО ОБЕСПЕЧЕНИЯ

Все компании имеют свою специфику и используют разное программное обеспечение. Не существует универсального решения, подходящего всем. Наши заказчики довольны результатами внедрения и интеграцией с используемым ПО, потому что мы дорабатываем продукты с учетом индивидуальных требований.

ИМПОРТОЗАМЕЩЕНИЕ

Индид — российская компания. Наши продукты прошли государственную сертификацию. Они соответствуют стандартам российского законодательства и требованиям к ПО для использования вместо зарубежных аналогов. Наши решения легко интегрируются с разработками других российских компаний.

НАШИ ПАРТНЕРЫ



МОСКВА

Angara Technologies, Axoft, INLINE Technologies, Softline, SoftwareOne, Информзащита, Инфосистемы Джет, Рубитех, Системный софт

САНКТ-ПЕТЕРБУРГ

Газинформсервис, Диджитал Дизайн, Пятый элемент

РОССИЯ

Астерит, ICL, Марвел-Дистрибуция, Телеком Интеграция, УЦСБ, OCS

СНГ

Axoft, AkNur Security, LVO, Mobile Service

КОМПАНИЯ
ИНДИД

indeed-company.ru

8 800 333-09-06

sales@indeed-company.ru

Скачайте электронную
версию буклета