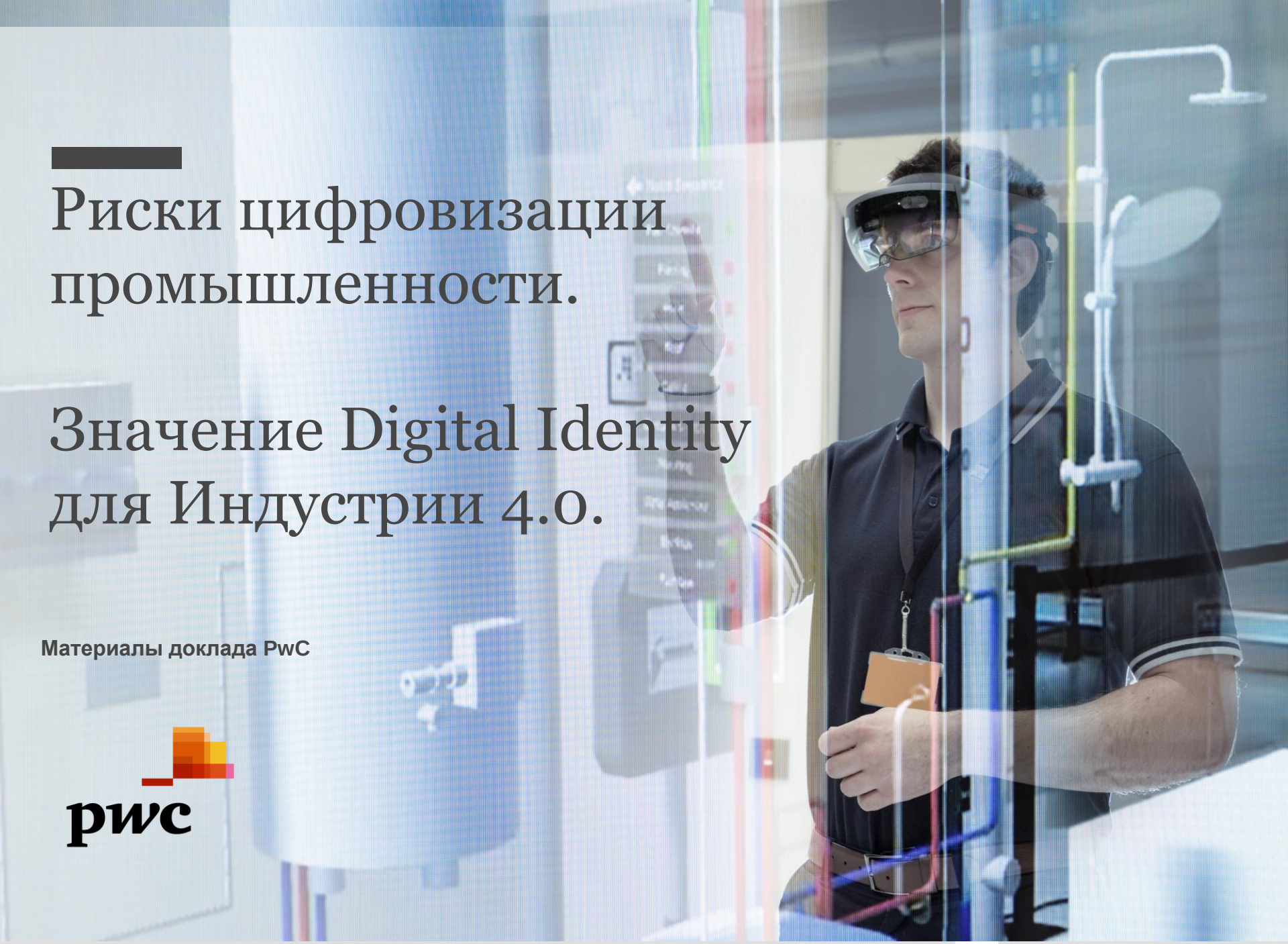
Риски цифровизации промышленности.

Значение Digital Identity для Индустрии 4.0.

Материалы доклада PwC



На пути к цифровому доверию

В будущем на рынке преуспеют те цифровые компании, которые сегодня занимают передовые позиции в обеспечении безопасности, сохранности, надежности информации, а также защите персональных данных и соблюдении информационной этики.

Это путь, который стоит пройти.

4,3 млрд.

кибератак в 2018 году совершено на критическую информационную инфраструктуру РФ*

17 тыс.

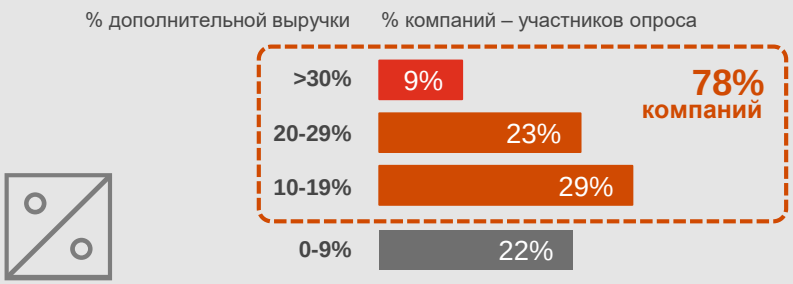
наиболее опасных

Наиболее серьезные начались с получения **доступа** и нахождении в инфраструктуре в течении длительного времени **необнаруженными.**

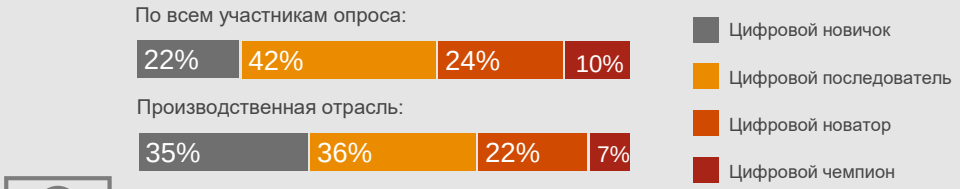
* По данным Интерфакс – брифинг Николая Мурашова, зам.директора Национального координационного центра по компьютерным инцидентам в декабре 2018 и июне 2019 года

Цифровые продукты в условиях современного бизнеса

Дополнительная выручка от применения цифровых технологий в ближайшие 5 лет, %



Распределение уровня цифровой зрелости:



Амбиции

«All-In»

Цифровые решения как основа ключевых процессов компании

Бюджет: **до 2.4% выручки**

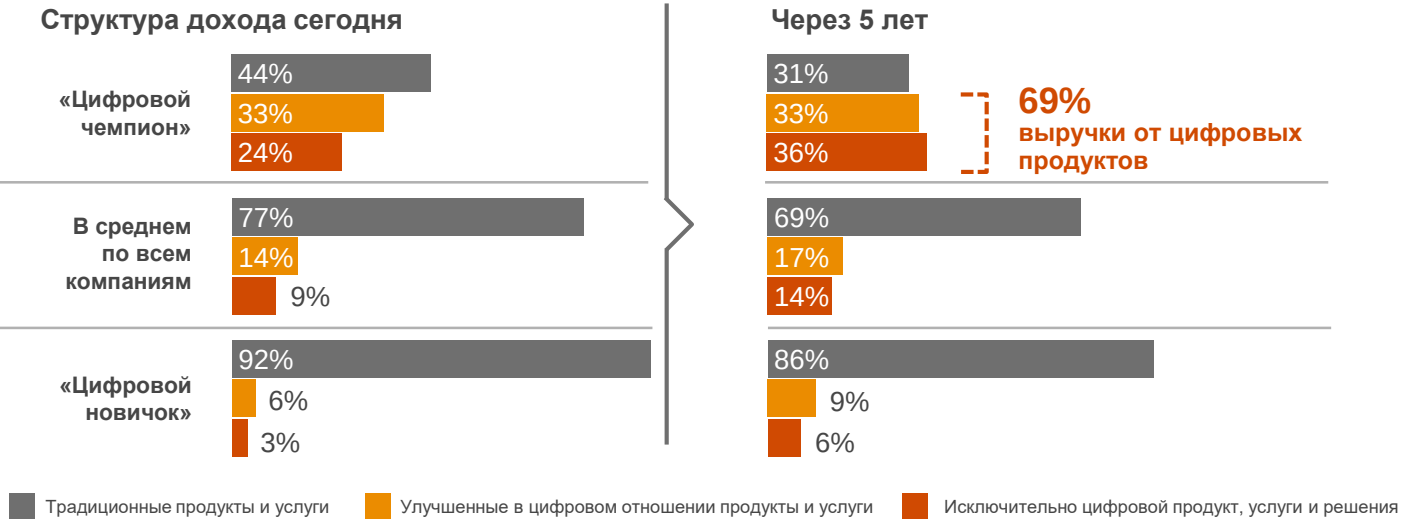
Операционный эффект: **до 20% OPEX**

«Try&See»

Цифровые решения как дополнения к не ключевым процессам

Бюджет: **<0.1%** выручки

Операционный эффект: **<1.5%** OPEX



Примечание. На основе опроса 1155 компаний.
Источники: Глобальное исследование цифровых операций в 2018 и 2019 г. подразделения PwC Strategy&

Цифровизация заключается в том как люди, бизнес-процессы, умные «вещи», технологии и партнеры взаимодействуют - как генерируют, обрабатывают и передают данные

$1,2 – 3,7 трлн*

прироста, глобальный ВВП получит к 2025 г.
за счет перехода на Индустрию 4.0

*Источник: Глобальное исследование McKinsey, 2018

Современная модель цифрового доверия больше не имеет периметров и строится на основе цифровой идентичности

Цифровая идентичность – это цифровой «паспорт» человека (сотрудника, клиента, партнера), бизнес-процесса, компании, сервиса, сенсора или умной «вещи», который однозначно позволяет удостоверить владельца.

Цифровизация требует выхода бизнеса за рамки периметра организации, для этого ставят цифровую идентичность в центр модели цифрового доверия – основав доверие к цифровому процессу, появляется возможность использовать его преимущества и дальше развивать его.

Цифровая идентичность и цифровое доверие позволяют построить фундамент для упрощения и ускорения диверсификации промышленности

Простая, быстрая и безопасная интеграция, запуск продуктов и инициатив.

Доверие цифровым и текущим технологиям и сервисам.

Улучшенный бизнес

Компания «IKEA» запустила успешную инициативу по применению AR в моделировании планировки квартиры или офиса.

Компания «Exxon», ввиду глобального распределенного бизнеса в Северной Америке определила возможность использовать более дешевое сырье для своей собственной переработки и последующей продажи (это стало возможным благодаря данным по добыче, транспортировке и переработке). Лишь это действие позволило достичь $880 млн дополнительной прибыли за полгода после запуска инициативы, лишь за счет лучшей локализации своих ресурсов.

Новый тип бизнеса

Компания «Total» взяла контроль над 23% компании «Eren RE» которая владеет портфолио солнечных, ветряных и гидро электростанций, расширяясь до 3 ГВт в течении пяти лет.

Компания «Chevron» активно диверсифицирует бизнес – ветряные и солнечные электростанции, биотопливо, химические продукты и пищевые добавки, судоходная и трубопроводная компании, смазочные масла и топливные инжекторы.

Компания «Daimler» поглотила и перезапустила самый популярный, самый успешный и один из первых сервисов по каршэрингу (car2go), работая совместно с сервисом «BMW», объединенная компания захватила и развивает 25% этого рынка во всём мире.

Как реализацию маркетинговой и социальной инициативы, компания «MOL» управляет сервисом шаринга велосипедов.

Новый необычный бизнес

Контроль, сбор и анализ релевантных данных, маркетинг.

Целевые продажи, программы лояльности.

Активный успешный ритейл бизнес

Решения цифровой идентичности можно активно применять в процессе добычи

Разведка, Бурение, Добыча

Проблемы	Решения	Польза
Цикличность цен на ресурсы требует оптимизации расходов для снижения себестоимости.	Автоматизация операций – снижение операционных расходов (персонал, устройства, ИТ, транспорт).	Снижение операционных расходов в добыче ведёт к снижению себестоимости ресурсов.
Внедрение систем управления транспортом требует снижение рисков утечек данных, а также необходимость в полноценной и качественной обработке этих данных.	Возможность идентификации транспортных единиц, централизация управления и дальнейшее использование данных.	Снижение рисков утечек данных по транспорту, контроль управляющего доступа, оптимизация эффективности транспорта.
Внедрение электронных сенсоров и/или умных устройств (IoT) требует снижения рисков утечек и подлога (цифровое доверие), а также более эффективного управления.	Поддержка «жизненного цикла» сенсоров и IoT – защита доступа и оптимизация стоимости.	Снижение рисков аварий и утечек данных, оптимизация (снижение) расходов связанных с сенсорами и IoT устройствами.
Контроль доступа сотрудников: ▪ базовый контроль доступа – данные собираются на вход/выход из помещения, либо с датчиков присутствия ▪ контроль доступа к критичным данным, представляющих серьезный коммерческий интерес отсутствует ▪ контроль доступа к инфраструктуре – аварийные, химические сенсоры, дроны	Возможность централизации идентичных данных на физическом и ИТ уровнях - для дальнейшего поведенческого анализа, полноценного контроля доступа	Повышение эффективности сотрудников. Улучшение процесса контроля доступа, предотвращение угроз, аварий и воровства вызванных сотрудниками.
	Контроль доступа к конфиденциальным данным, критичным ресурсам и инфраструктуре	Защита конфиденциальных данных о разведке, бурении и добычи от конкурентов. Защита машин и сенсоров от подлога и аварий.

Пример – жизненный цикл «умных» вещей IoT

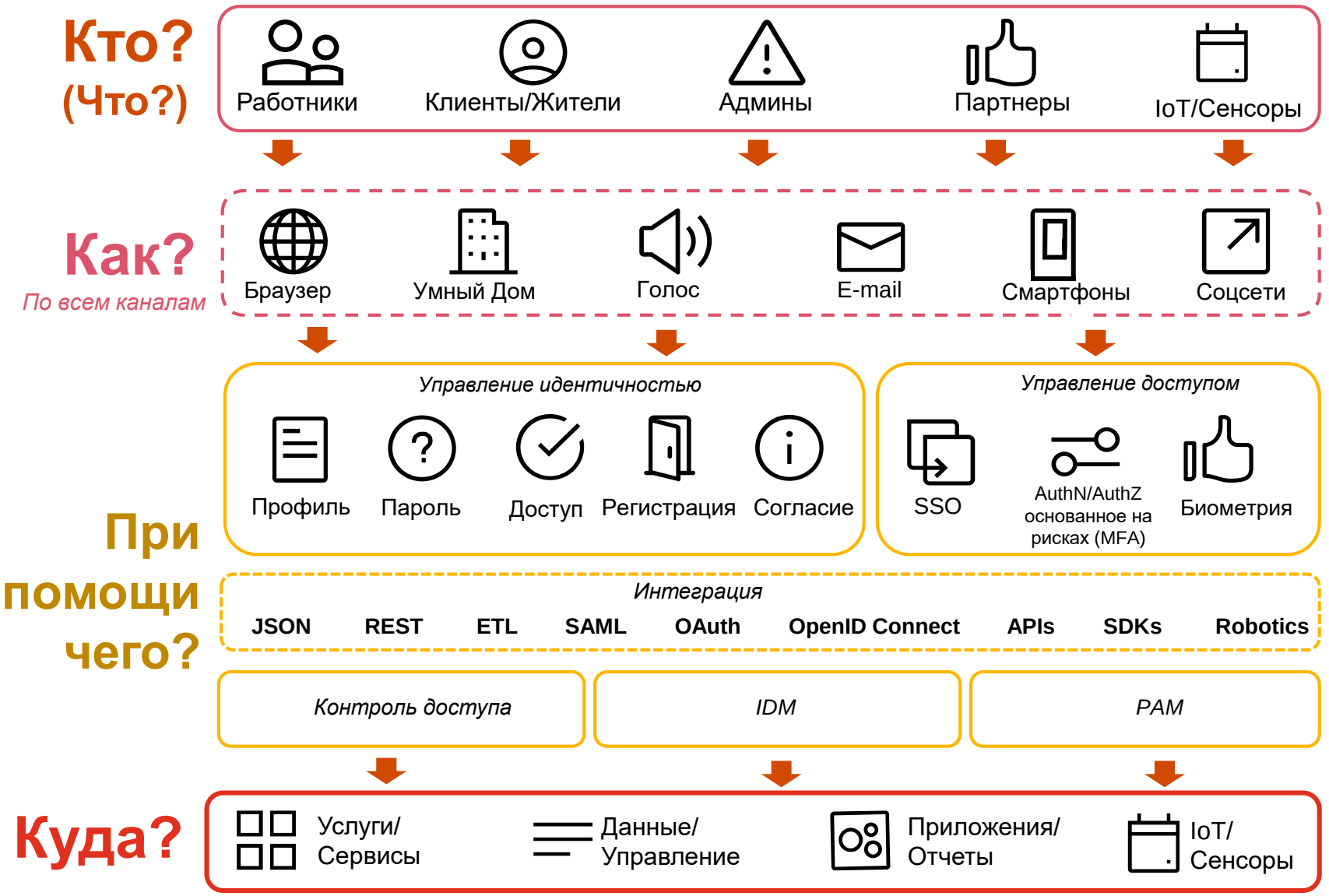
IoT Бизнес-процесс	Техническая реализация
Создание и хранение идентичности «умного» устройства	*Каталог, IDM.*
Аутентификация «умного» устройства в сервис	*Шлюз, контроль доступа, каталог.*
Авторизация «умного» устройства на доступ к API	*Контроль доступа, каталог.*
Регистрация пользователя IoT устройства	*IDM, каталог.*
Моделирования опыта IoT пользователя	*Контроль доступа, каталог.*
Отзыв ассоциации «пользователь-устройство»	*IDM, контроль доступа, каталог.*
Защита IoT устройства	*Шлюз, контроль доступа, каталог.*
Защита критичных данных IoT	*Контроль доступа, каталог, брокер.*

Решения цифровой идентичности можно активно применять в процессе производства и переработки

Транспортировка и хранение, производство и переработка

Проблемы	Решения	Польза
Более эффективное взаимодействие с поставщиками и дистрибьютерами.	Простое безопасное подключение поставщиков и дистрибьютеров к системам и данным.	Снижение простоев в поставках и хранении активов. Повышение опыта поставщиков и покупателей.
Данные по транспортировке, активам и запасам требуют защиты, ввиду их критичности, но они должны использоваться для оптимизации цепочки поставок.	Улучшение контроля доступа к данным, не снижая скорости сбора и централизации данных для дальнейшего использования.	Повышение эффективности цепочки поставок, благодаря сбору полной картины данных по транспортировке и хранению.
Внедрение систем управления транспортом требует снижение рисков утечек данных, а также необходимость в полноценной обработке этих данных, ввиду их объема.	Поддержка «жизненного цикла» сенсоров и IoT – защита доступа и оптимизация стоимости.	Снижение риска утечек и неавторизованного доступа к информации связанной с транспортировкой и хранением.
Нет понимания насколько эффективны сотрудники в различных функциях. Более того, нет понимания кто, когда и куда имел доступ и имеет доступ.	Централизация и создание взаимосвязей по идентичностям – сотрудники, площадки, отделы, этажи, устройства, системы и т.п.	Повышение эффективности сотрудников. Оптимизация операционных моделей – снижение издержек.
Внедрение электронных сенсоров и/или умных устройств (IoT) требует снижения рисков утечек и подлога (цифровое доверие), а также более эффективного управления.	Поддержка «жизненного цикла» сенсоров и IoT – защита доступа и оптимизация стоимости.	Снижение рисков аварий и утечек данных, оптимизация расходов связанных с использованием сенсоров и IoT устройств.

Пример – реализация фреймворка доступа к системам



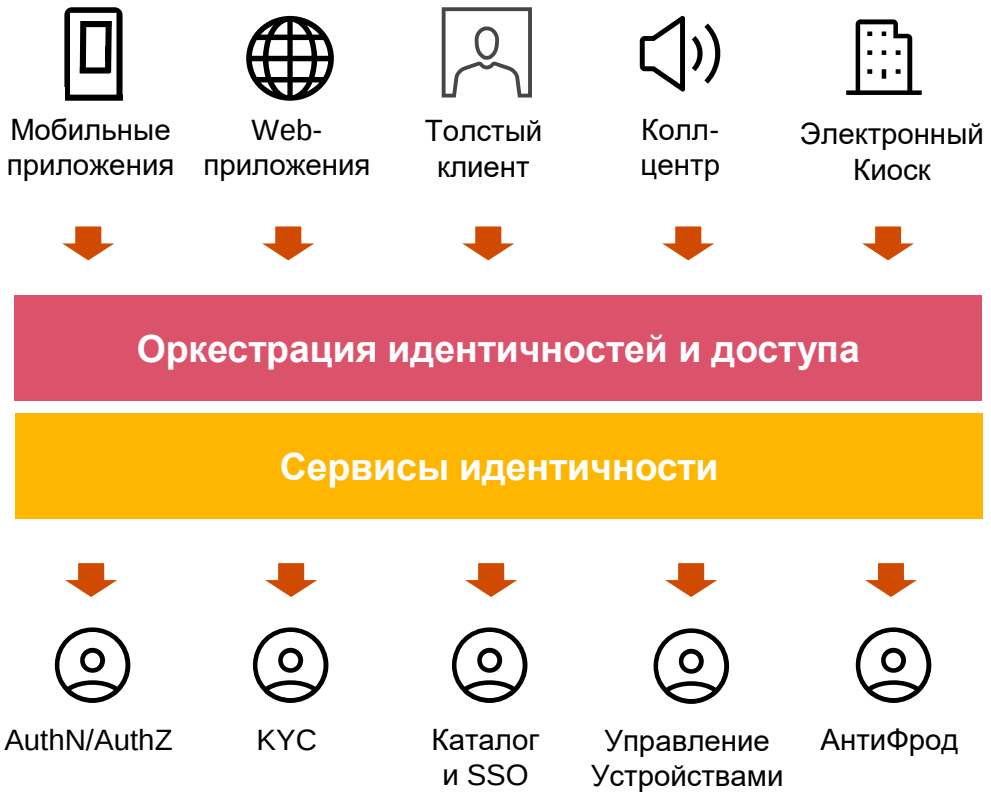
Решения цифровой идентичности можно активно применять в процессе розничных продаж

Розничные продажи

Проблемы	Решения	Польза
Трудности в управлении сетью розничных продаж и мелкооптовых продаж напрямую.	Повышение эффективности программ лояльности и малых оптовых продаж: ▪ Сбор и анализ данных по доступу к покупке – место, количество, частота и т.п. ▪ Реализация мобильного приложения лояльности. ▪ Реализация омни-канальности.	Увеличение эффективности сети продаж Предсказуемые данные по продажам для балансировки цепочки поставок Точно знать клиентов по всем каналам, управлять спросом клиентов: • категория клиента (частный/бизнес) • объём • ценообразование Контроль и управление сетью продаж: • KPI для точке продаж/конкретного сотрудника • управление мотивацией
Клиенты не лояльны, управляемы принципом наименьшей цены, либо предпочитают конкурентов.		
Продажи нестабильны, для реализации стратегии по повышению розничных продаж не хватает данных.		
Для оптовых и мелкооптовых продаж уже используются CRM, но количество клиентов нестабильно. Нет данных для управления и повышения спроса.	Поддержка CRM систем дополнительными данными.	
	Упрощенная регистрация в системы продаж и лояльности	Увеличение количества клиентов за счет упрощения процесса регистрации.
Подключение нового клиентского сервиса или приложения, также как и интеграция с внешними сервисами (Яндекс, банки и т.п.) обычно требует серьезных вложений времени, финансов и ресурсов.	Упрощение подключения новых приложений и интеграции со сторонними сервисами (напр. Яндекс.Навигатор)	Снижение стоимости разработки и поддержки ИТ-систем и приложений. Снижение времени и стоимости интеграции со сторонними системами.

Пример – улучшение «опыта» пользователя

Примеры бизнес-процессов
Биометрия и поведенческий анализ
Создание и управление учетной записью/«KYC»
Усиленная и многофакторная аутентификация
Целостность транзакций через «подпись»
Моделирование рисков доступа
Предотвращение мошенничеств на базе ИИ
Полноценное использование смартфона
Аутентификация колл-центров
Беспарольная аутентификация
Централизация данных пользователей
Федерация и SSO



Пример опыта

Глобальная производственная компания

Поглощение международной компании

Компания-производитель оборудования в Нидерландах была поглощена крупным производителем из США. Обе компании активно использовали свои собственные решения, процессы и операционные команды в управлении доступом сотрудников, партнеров и контрагентов.

Результаты проекта:

- Существенно снижена стоимость владения и управления сервисами доступа
- Запущен единый цикл управления идентичностями – процессы, технологии, операционная модель
- Усилена безопасность благодаря внедрению двухфакторной аутентификации

PwC помогло объединить и оптимизировать модель доступа компании в США и Нидерландах, запустив программу объединения систем цифровой идентичности.

Минимизировав риски и влияние на текущие процессы, мы запустили ряд инициатив по объединению систем, начав с операционных процессов.

В рамках новой модели, мы применили современные методы цифровой идентичности, оптимизировав получившуюся модель по отношению к результатам как одной, так и второй организации.

Это лишь малая часть решений, которые мы с успехом применяем по всему миру...

Павел Николаев

Лидер направления
Digital Identity PwC Russia

700+
профессионалов в области Digital Identity (IAM)

1 500 000 000+
учетных записей, управляемых в наших решениях

400+
внедренных решений Digital Identity по всему миру

Внедрения для **78+**
компаний из списка **Fortune 500**

Практика IAM существует в PwC более 15 лет, в течение последних 5 лет, мы и наши проекты выигрывали многочисленные вендорские награды.

«PwC» назван мировым лидером в консалтинге в области кибербезопасности в Европе в 2019 году - **Forester**

pavel.nikolaev@pwc.com
+7(966)062-3167

Спасибо
за внимание!

pwc.com