



Бизнес-план развертывания стратегии "Никому не доверяй"

Практическое руководство по реализации стратегии
"Никому не доверяй" в организации



Оглавление

- 03 [Введение](#)
- 04 [Модель "Никому не доверяй" как условие для безопасного перехода на цифровые технологии](#)
- 05 [Прагматичный подход к стратегии "Никому не доверяй"](#)
- 06 [Три этапа внедрения модели "Никому не доверяй"](#)
 - 07 [Планирование перехода на модель "Никому не доверяй"](#)
 - 10 [Реализация стратегии "Никому не доверяй" в организации](#)
 - 11 [Отслеживание успехов](#)
- 15 ["Никому не доверяй" как залог выживания](#)
- 16 [Что дальше?](#)

Переход на цифровые технологии как фактор "новой нормальности"

Организации переходят на цифровые технологии для эффективного управления постоянными изменениями в деловой среде:

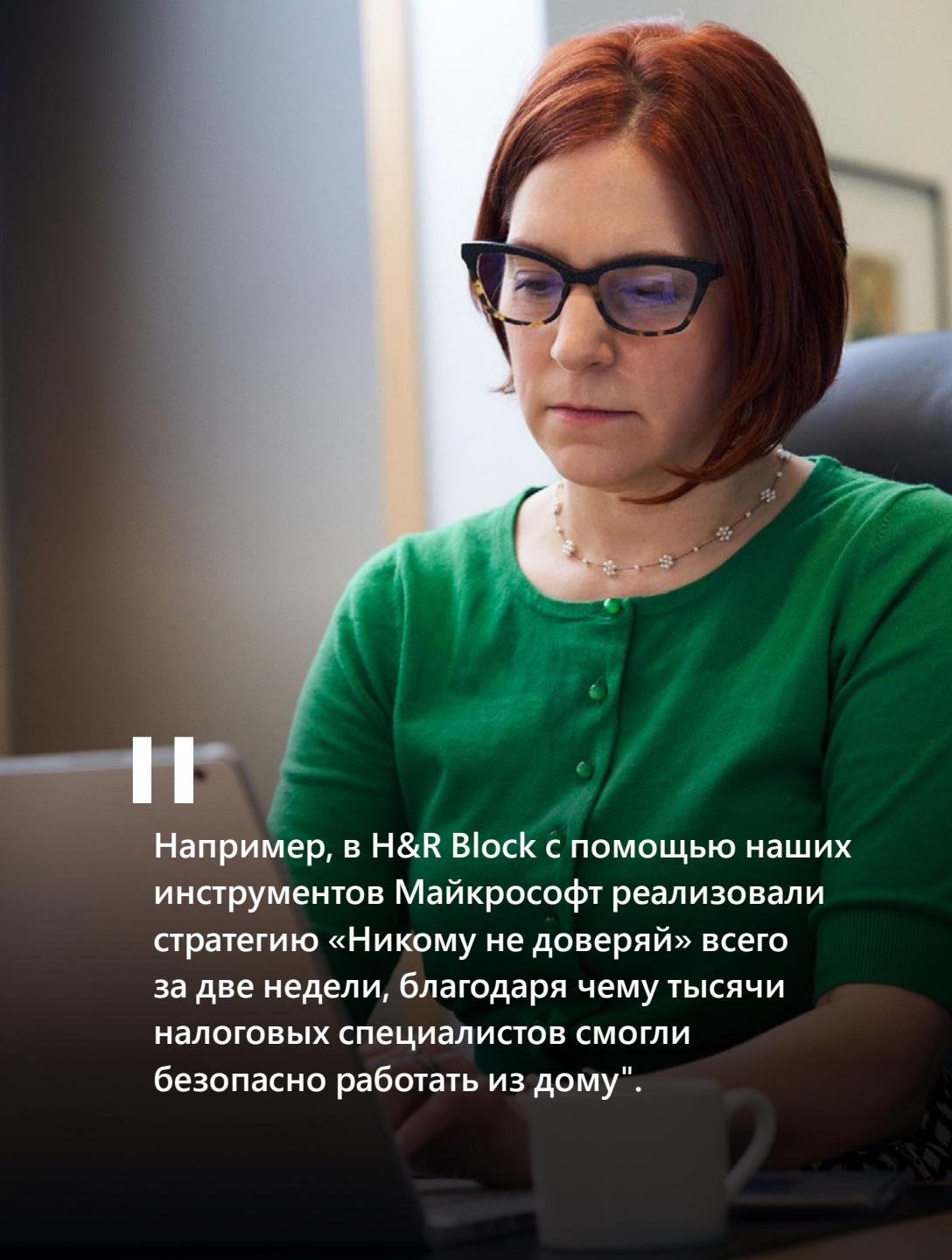
- Эволюция бизнес-моделей и партнерских отношений
- Технологические тренды
- Нормативно-правовые, геополитические и культурные сдвиги

Переход на удаленную работу из-за COVID-19 ускорил эту трансформацию, и теперь безопасность часто превращается из источника расходов в стратегический фактор роста.



Пандемия COVID продемонстрировала всем новые вызовы и необходимость в будущем очень быстро адаптироваться к изменениям. С внедрением модели «Никому не доверяй» становится неважно, откуда именно — из собственного гаража, облака или центра обработки данных — вы работаете".

— Руководитель по решениям для управления удостоверениями и доступом в компании, оказывающей финансовые услуги



Модель "Никому не доверяй" как условие для безопасного перехода на цифровые технологии

Переход на цифровые технологии заставляет по-новому взглянуть на традиционные модели безопасности.

Прежние технологии в сфере безопасности не гарантировали гибкость бизнес-процессов, удобство для пользователей и надлежащую защиту быстро эволюционирующей цифровой инфраструктуры. Многие организации реализуют модель "Никому не доверяй", чтобы справиться с этими изменениями и приспособиться к новым условиям, требующим возможностей для дистанционной работы с любыми пользователями в любое удобное время.

Например, в H&R Block с помощью наших инструментов Майкрософт реализовали стратегию «Никому не доверяй» всего за две недели, благодаря чему тысячи налоговых специалистов смогли безопасно работать из дому".

Эти полезные данные и рекомендации были получены по результатам общения с клиентами и на основе нашего собственного опыта внедрения модели "Никому не доверяй" в Майкрософт.

Прагматичный подход к внедрению модели "Никому не доверяй": думать масштабно, начинать с малого, действовать быстро



Разработка многолетнего бизнес-плана, включающего такие пункты:

Расстановка приоритетов для быстрых результатов
и последовательная реализация каждой инициативы.

Использование существующих технологий,
которые уже развернуты или лицензированы.

Определение взаимосвязей между инициативами,
четких результатов, преимуществ и ответственности.

Развертывание модели "Никому не доверяй"

Мы создали систему практических рекомендаций, которые позволяют реализовать модель "Никому не доверяй". Для каждого этапа мы предлагаем инструкции, советы, ресурсы и инструменты, которые помогут вам внедрить ее у себя.



01 Планирование

Создание бизнес-модели, ориентированной на результат и максимально точно отвечающей рискам и стратегическим целям организации.

02 Реализация

Разработка многолетней стратегии по внедрению модели "Никому не доверяй" и выбор приоритетных начальных мер в зависимости от потребностей компании.

03 Оценка успехов

Контроль за ходом развертывания модели "Никому не доверяй" для оценки конкретных улучшений, связанных с реализацией ее принципов.

План реализации модели "Никому не доверяй": выгоды и преимущества

Рекомендуемые приоритеты:

→ **Выработайте концепцию.** Внедрении модели "Никому не доверяй" включает разные аспекты и может занять не один год. Четкое **определение** целей, результатов и архитектур помогает организациям добиться большего успеха, чем в рамках "реактивного" подхода.

→ **Заручитесь поддержкой руководства.** Успешное внедрение модели "Никому не доверяй" ориентировано на коммерческий результат и требует поддержки со стороны руководства для постановки амбициозных целей, выделения средств и синхронизации усилий.

Примечание. Преимущества и особенности реализации часто сильно зависят от ваших ролей и обязанностей.

→ **Расширьте возможности конечных пользователей.** Модель "Никому не доверяй" позволяет специалистам по технологиям взаимодействовать непосредственно с конечными пользователями, чтобы сделать безопасность фактором удобства и продуктивной работы.



Выработка концепции и поддержка руководства

Чтобы заручиться поддержкой руководства, следует сначала поинтересоваться бизнес-приоритетами, внимательно выслушать ответы, а затем выработать принципы, ориентированные на коммерческий результат.

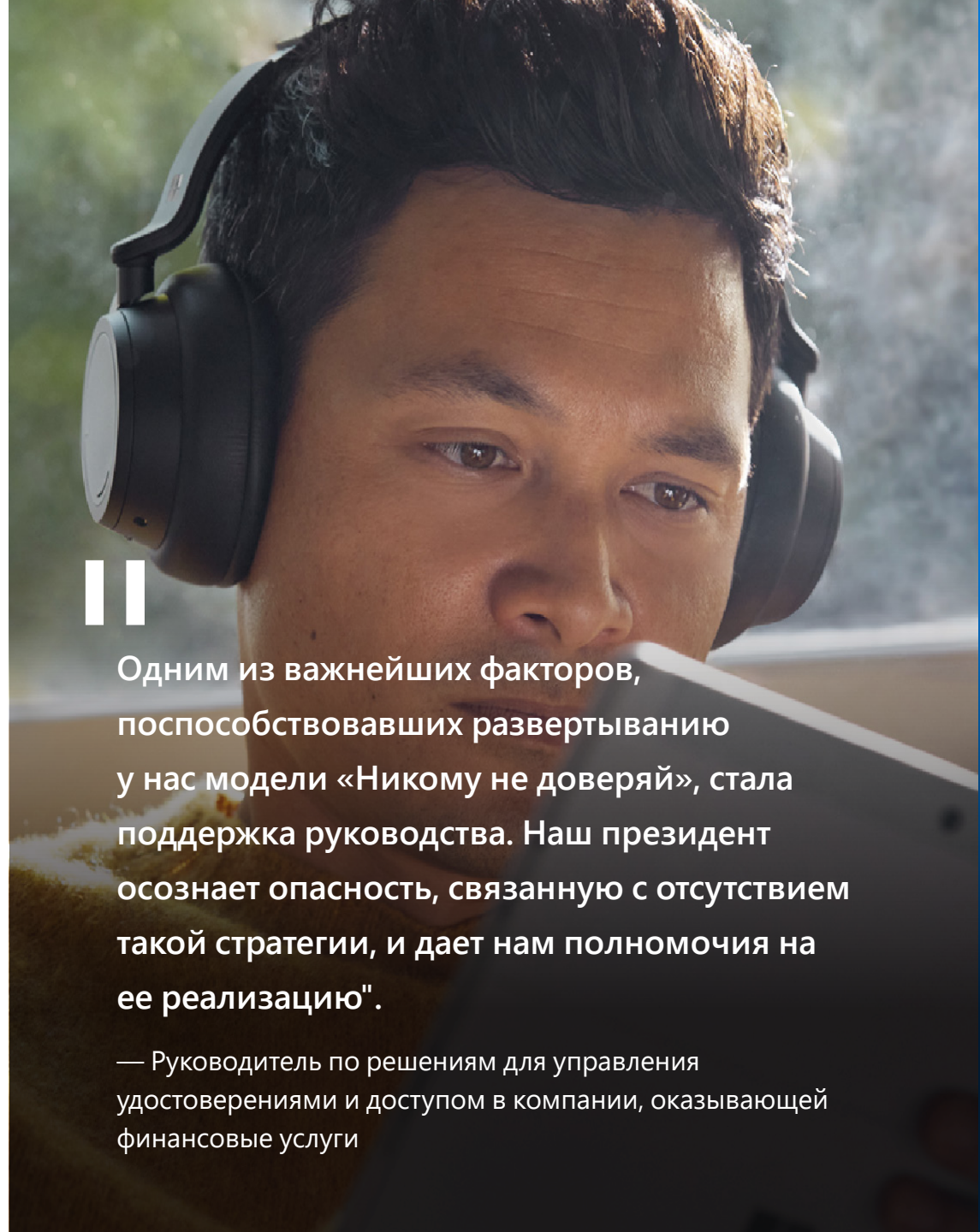
Хотя эта концепция всегда зависит от конкретных приоритетов и культуры компании, мы обнаружили ряд моментов, общих для разных организаций.

- **Гибкость бизнес-процессов**, позволяющая быстро выявлять и использовать новые возможности, а также контролировать риски, переходить на удаленную работу и облачные технологии.
- **Управление сложностями**, возникающими в связи с постоянной эволюцией партнерских отношений, конкурентной среды и быстрым развитием технологий.
- **Измеримость** для отслеживания результатов с точки зрения бизнеса и рисков.



Одним из важнейших факторов, поспособствовавших развертыванию у нас модели «Никому не доверяй», стала поддержка руководства. Наш президент осознает опасность, связанную с отсутствием такой стратегии, и дает нам полномочия на ее реализацию".

— Руководитель по решениям для управления удостоверениями и доступом в компании, оказывающей финансовые услуги



Создание надежной бизнес-модели для стратегии "Никому не доверяй"

Надежная бизнес-модель позволяет заручиться поддержкой руководства и синхронизировать усилия в разных подразделениях компании. Хотя модель безопасности "Никому не доверяй" несет в себе множество преимуществ, организации, как правило, сталкиваются с наибольшей выгодой в четырех основных аспектах.

- Возможность работать в любое время, где бы вы ни находились.
- Надежный и быстрый переход на облачные технологии.
- Экономия за счет упрощенного набора защитных технологий.



Акцент на конечных преимуществах для бизнеса, таких как:

- **Профилактическое устранение рисков** и их контроль.
- **Управление рисками партнеров** с ненадежными стратегиями безопасности.
- **Гибкость с точки зрения безопасности и соответствия требованиям** для адаптации к динамичным изменениям в ролях и организациях.

ПЛАНИРОВАНИЕ › РЕАЛИЗАЦИЯ › ОЦЕНКА УСПЕХОВ

Реализация стратегии "Никому не доверяй": выгоды и преимущества

Разбиение программы на понятные и связанные между собой инициативы. В Майкрософт выяснили, что технические стратегии и архитектуры можно естественным образом сгруппировать по следующим признакам (инициативам) с точки зрения безопасности:

- Безопасность средств продуктивной работы
- Современные процессы обеспечения безопасности
- Операционные технологии и Интернет вещей, *если это применимо для конкретной организации*
- Центры обработки данных, службы и API

Эти рекомендации основаны на опыте Майкрософт и других клиентов, успешно реализовавших стратегию у себя.



Расстановка приоритетов и планирование инициатив

- **Согласуйте каждую инициативу с бизнес-целями** и оцените потенциальный положительный эффект для компании, трудности и вызовы.
- **Составьте краткосрочный план.** Начните с быстрых результатов и найдите заинтересованных лиц среди руководства.
- **Разработайте долгосрочную дорожную карту.**



Оценка успехов: выгоды и преимущества

Определите вехи и цели в аспекте продуктивности для своей организации, измерьте их, зафиксируйте успехи и новый опыт.

- **Новые возможности для бизнеса:** проанализируйте сложности с точки зрения пользователей, а также сроки одобрения инициатив внутренними службами безопасности.
- **Эффективность системы безопасности:** оцените уменьшение числа или серьезности инцидентов безопасности после перевода организации на стратегию "Никому не доверяй".
- **Простота системы безопасности:** уменьшите число поставщиков решений, которые вашим командам приходится интегрировать, и сократите расходы на выполняемые вручную задачи (таких как сброс паролей по запросу пользователей).



Оценка выгод с точки зрения НОВЫХ ВОЗМОЖНОСТЕЙ для бизнеса

Модель "Никому не доверяй" должна повысить удобство для пользователей и разработчиков в следующих аспектах:

- Количество прерываний рабочего процесса для проверки безопасности (например, количество запросов пользователю на многофакторную проверку подлинности в течение дня).
- Ключевые этапы в процессе развертывания (например, доля сотрудников, входящих в приложения через систему единого входа).
- Ключевые этапы в аспекте отслеживания (например, менее активное использование приложения из-за неудобств при входе).
- Среднее время загрузки управляемых устройств в секундах.
- Среднее время проверки безопасности приложений в днях.

Не забывайте о каналах обратной связи для пользователей: интересуйтесь их мнением относительно простоты использования, процедуры сброса паролей и т. п.



Оценка эффективности системы безопасности

Оцените состояние безопасности вашей системы и последствия для нее от инцидентов безопасности:

- Количество инцидентов безопасности (по степени серьезности).
- Ключевые этапы в процессе развертывания (например, доля сотрудников, активно использующих многофакторную проверку подлинности).
- Ключевые этапы в аспекте отслеживания (например, доля управляемых устройств и приложений).
- Состояние безопасности: отслеживание улучшений в [Оценке безопасности \(Майкрософт\)](#).

Работа в контексте: по мере улучшения контроля в рамках модели "Никому не доверяй" вы можете обнаружить инциденты, на которые ранее не обратили внимания.



Оценка простоты системы безопасности

Модель "Никому не доверяй" часто помогает упростить требования к безопасности.

- Количество защитных инструментов, выполняющих аналогичные или полностью идентичные функции.
- Количество защитных инструментов, требующих адаптации для интеграции.
- Доля времени ИТ-специалистов, потраченного на выполнение рутинных задач, таких как сброс паролей.
- Количество выполняемых вручную шагов в рутинных рабочих процессах (таких как анализ стандартных оповещений и инцидентов, подготовка пользователей вручную, формирование отчетов по соответствию требованиям).
- Доля ложных срабатываний, анализируемых службами безопасности.
- Доля времени, потраченного на обслуживание технических решений вместо реагирования на реальные инциденты.



Модель "Никому не доверяй" как залог выживания при переходе на цифровые технологии

Чтобы начать, не нужно сразу отказываться от существующих технологий и заменять их новыми.

Для начала согласуйте вложения в модель "Никому не доверяй" с текущими потребностями своей компании и сделайте акцент на быстрых результатах. Каждый такой результат последовательно помогает снизить риски и улучшить состояние безопасности вашей цифровой инфраструктуры.

Начать никогда не поздно, а любое улучшение имеет значение.



С тех пор как мы внедрили модель «Никому не доверяй» на основе технологий Microsoft 365, наши сотрудники могут выполнять свои обязанности в любой точке мира. При этом мы жестко контролируем ключевые аспекты нашей системы безопасности".

— Игорь Цыганский (Igor Tsyganskiy), технический директор, Bridgewater Associates

Что дальше?

Благодарим вас за то, что ознакомились с нашим практическим руководством по внедрению модели "Никому не доверяй". Если вы еще этого не сделали, рассмотрите [концепцию зрелости модели "Никому не доверяй" от корпорации Майкрософт](#) (щелкните, чтобы скачать ее), где описаны базовые принципы этой стратегии, а также нашей модели оценки зрелости, в которой детализируются высокоуровневые требования по шести базовым аспектам.

Мы также подготовили полезные учебные материалы, технические руководства и другие ресурсы на нашем внешнем сайте, посвященном [модели "Никому не доверяй" от Майкрософт](#).

