NOVENTIQ
Global expertise, local outcomes

Microsoft 365:

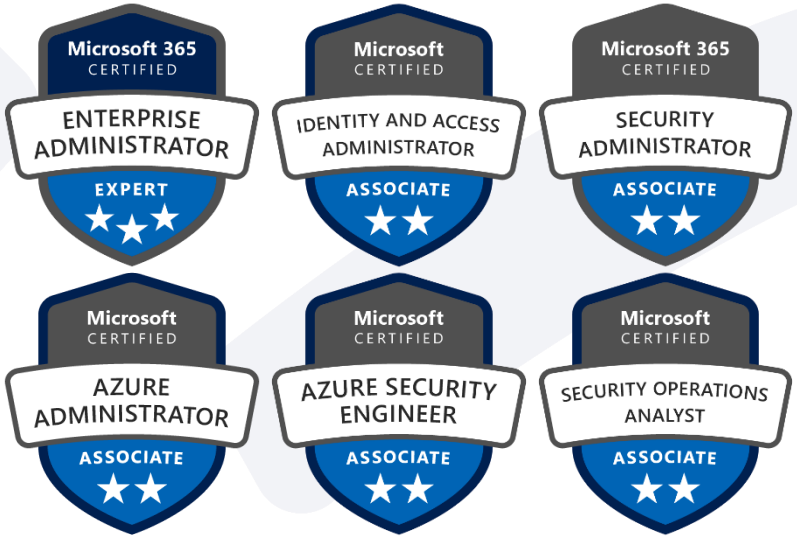
Современный подход к безопасности офисной инфраструктуры в финансовой индустрии

AIFC

Сергей Жуйков
Архитектор решений Microsoft
Sergey.Zhuykov@noventiq.com

22.11.2023

Спикер



Сергей Жуйков

Sergey.Zhuykov@noventiq.com

Astana International Finance Center

Уникальный центр финансового мира Центральной Азии

Международный финансовый центр «Астана» (МФЦА) является драйвером финансовых инноваций в экономике Казахстана и за его пределами, обеспечивающим надёжную инфраструктуру и юрисдикцию, уникальные продукты и услуги для ведения бизнеса и привлечения локальных и зарубежных инвестиций. МФЦА воплотил в себе передовые практики ведущих финансовых центров мира, таких как Нью-Йорк, Лондон, Гонконг, Сингапур и Дубай.

Видение

Стать драйвером и ключевым хабом для инвестиций и финансовых инноваций в экономике Казахстана с целью её дальнейшего роста

Миссия

Способствовать устойчивому экономическому развитию Казахстана за счёт предоставления уникальной инфраструктуры для инвестирования и ведения бизнеса, надёжной юрисдикции, независимого суда и арбитражных услуг, а также поддержки инноваций и развития потенциала в сфере финансовых продуктов и услуг

Финансовый центр тюркского мира

Городу Астана был присвоен статус Финансового центра тюркского мира на 2024 год. Ряд инфраструктурных проектов структурированы в МФЦА.

Astana International Exchange

Биржа нового формата

Astana International Exchange (AIX) образована в 2017 году в рамках развития Международного финансового центра «Астана». Миссия AIX заключается в развитии надёжных и ликвидных рынков капитала в Центральной Азии и за её пределами путём предоставления инновационных продуктов и услуг для бизнеса и инвесторов.

Регуляторные условия, понятные иностранному инвестору

- Правовой режим, основанный на принципах английского права
- Нормативная база учитывает международные стандарты
- Независимые суды с международными судьями и арбитрами

Развитая инфраструктура мирового класса

Высокотехнологичная торговая платформа

- Сертификаты соответствия стандартам информационной и кибер-безопасности ISO 27001, ISO 27017, ISO 27018, ISO 27032

Noventiq — ведущий партнер Microsoft

Microsoft — крупнейший в мире поставщик стратегических технологий для цифровой трансформации предприятий. Для Noventiq, Microsoft является основой большинства наших решений.

Microsoft Partner

700+
Сертифицированных Microsoft профессионалов

Gold Microsoft Partner
Microsoft

Azure Expert MSP

Member of Microsoft Intelligent Security Association
Microsoft

Проверенный временем и успешный

25+
Лет сотрудничества

1 из 10
глобальных партнёров Microsoft по всему миру

Лучшие практики лицензирования
LSP статус в 34 странах
CSP с момента запуска (T1 and T2)
SPLA реселлер в течение 8 лет

В ряде стран мы являемся единственным поставщиком **Azure Expert Managed Service Provider**

Microsoft Partner of the Year 2020, 2021


Bulgaria


Cambodia x2


Malaysia


Vietnam x2

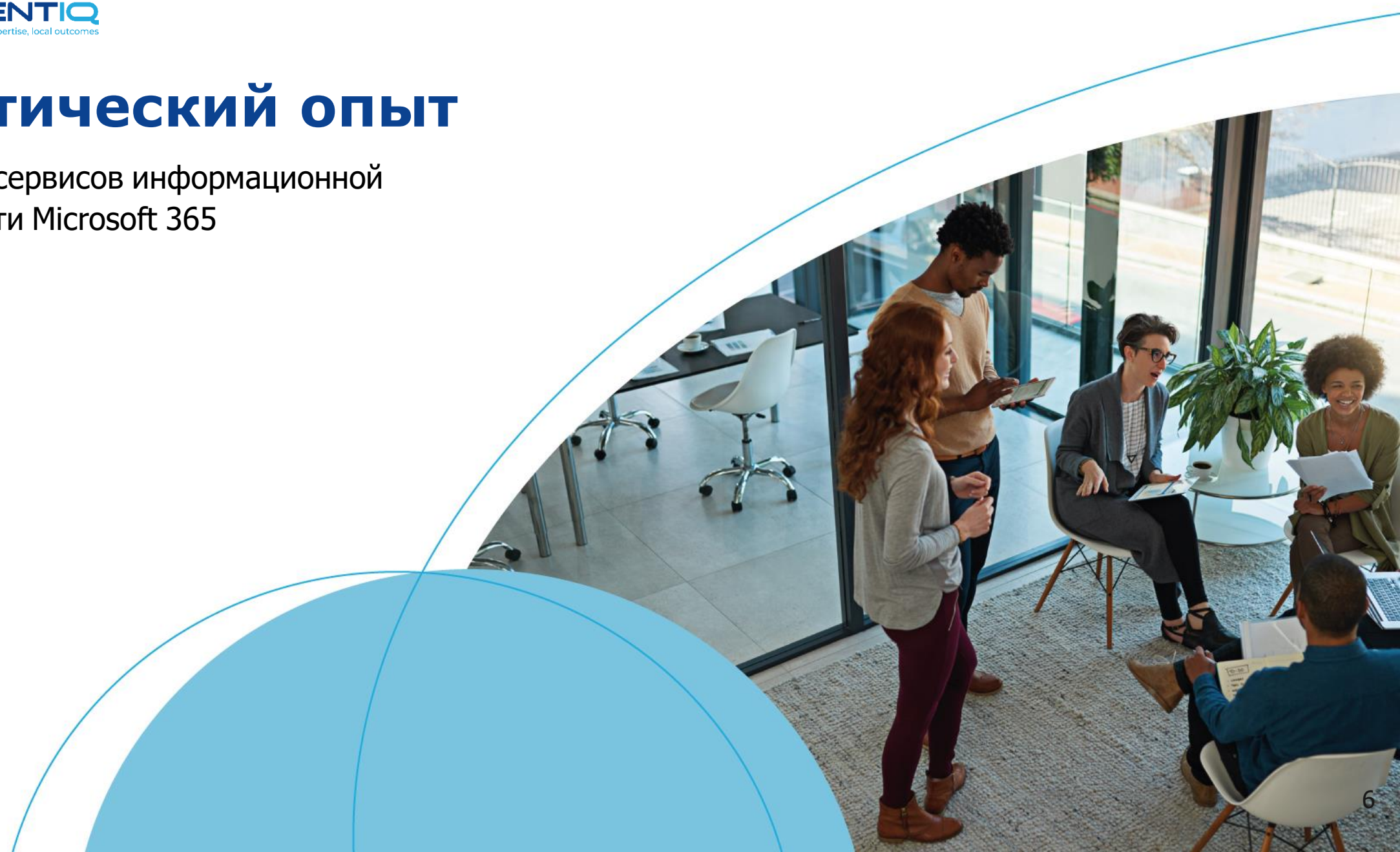
Microsoft Advanced Specializations:

- Windows Server and SQL Server Migration to Microsoft Azure
- Adoption and Change Management
- Kubernetes on Microsoft Azure
- Linux and Open-Source Database Migration to Azure
- Microsoft Windows Virtual Desktop
- Cloud Security
- Identity and Access Management
- Information Protection and Governance
- Threat Protection
- Azure Virtual Desktop Advance Specialization

- Security Partner of the Year 2021 Малайзия
- Modern Work Partner of The Year 2021 Малайзия
- Security Partner of the Year 2021 Камбоджа
- Security Partner of The Year 2021 Myanmar
- Security Excellence Award Филиппины
- Modern Work Partner of The Year 2021 Камбоджа
- Победитель 2021 Microsoft India's Cloud Champions programme

Практический опыт

Внедрения сервисов информационной безопасности Microsoft 365



Защита учётных записей

AIFC

Задача

Необходимость защищать учётные данные сотрудников и автоматизировать соответствие регламентам и политикам. Необходимость обеспечения гранулярного доступа к чувствительной информации компании.

Решение – Microsoft Entra ID

Entra ID предоставляет расширенные возможности аутентификации, многоуровневые меры безопасности и гибкие настройки условного доступа, которые позволяют точно контролировать доступ.

Результат

Внедрена MFA.
Настроены гибкие политики безопасности, позволяющие гранулярно регулировать доступ с учётом контекста и местоположения.

Выводы

Управление гибридной инфраструктурой имеет большую сложность и требует больших ресурсов.
Настройки условного доступа дают необходимую гибкость, но требуют расширенных компетенций.

NOVENTIQ

Global expertise, local outcomes

Защита данных

Задача

Рост объёмов чувствительной информации и требования к безопасности, а также соответствию стандартам ISO, создали необходимость в унификации подходов к защите информации.

Решение – Microsoft Information Protection

Решение позволило перенести политики защиты данных, соответствующие требованиям ISO, на цифровые документы, а также обеспечило обучение пользователей с помощью встроенных подсказок.

Результат

Классификация и защита чувствительных данных компании, а также инструменты предотвращения утечек данных. Повышение осведомлённости о мерах безопасности. Соответствие требованиям ISO.

Выводы

Маркировка данных на основе тегов на рабочих станциях была заменена на маркировку на основе контента. Инструменты DLP закрывают весь периметр, включая рабочие станции, облачные сервисы и CASB.

Управление мобильными устройствами

Задача

Необходимость управлять корпоративными мобильными устройствами и корпоративными данными на BYOD-устройствах. Необходимость автоматизировать соответствие регламентам и политикам.

Решение – Microsoft Intune MDM/MAM

Intune предоставляет инструментарий для централизованного управления устройствами, соответствия политикам и регламентам, применения политик безопасности и обеспечения защиты данных.

Результат

Внедрены сценарии MDM и MAM.
Настроена проверка соответствия устройств.
Настроено управление данными на корпоративных и BYOD-устройствах.

Выводы

Приведение всех устройств в соответствие политикам оказалось вызовом из-за разнообразия операционных систем и конфигураций.
Пересечение политик с другими сервисами Microsoft.

NOVENTIQ

Global expertise, local outcomes

Защита от угроз

Задача

Угроза внешних атак, необходимость защиты точек, контактирующих с сетью Интернет.
Необходимость автоматизации расследований и реагирования, возможность превентивных действий.

Решение – Microsoft Defender EDR

Решение для обнаружения и предотвращения атак на конечных точках и серверах. Оно обеспечивает единое управление, непрерывный мониторинг безопасности, проактивное обнаружение угроз и сценарии MDR.

Результат

EDR внедрён для рабочих станций и серверов.
Снижение количества атак и времени реагирования на инциденты. Централизация управления инцидентами.
Наглядность и расширенная аналитика инцидентов.

Выводы

Основным вызовом стала интеграция Defender for Endpoint Plan 2 в существующую инфраструктуру ИБ.
Также потребовалось обучение персонала для эффективного использования всех возможностей EDR.

Безопасный доступ

AIFC

Задача

Обеспечение безопасного доступа к локальным веб-сервисам, включая MFA и политики условного доступа. Публикация веб-сервисов без необходимости открывать внешний доступ в DMZ или внутреннюю сеть.

Решение – Entra ID Application Proxy

Обеспечивает безопасный и удобный доступ к веб-сервисам в локальной среде, разделяя традиционный reverse proxy на портал подключения и соединитель, а также предоставляет пре-аутентификацию.

Результат

Обеспечен безопасный доступ к внутренним веб-сервисам с использованием MFA и условного доступа из любой точки мира. Веб-сервисы не имеют публичных точек внешнего доступа.

Выводы

Entra ID App Proxy имеет ограничения по максимальной нагрузке и может снижать скорость подключения.
В качестве альтернативного решения рассматривается Entra ID Security Service Edge решение.

NOVENTIQ

Global expertise, local outcomes

Целевой фишинг

AIFC

Задача

Блокировка таргетированных фишинговых атак. Существующие системы не могли эффективно обнаруживать и предотвращать такие атаки.

Решение – Microsoft Defender for Office 365

Обеспечивает многоуровневую фильтрацию почты и проверку файлов, хранящихся в облаке Microsoft с использованием моделей AI и «песочниц». Проверка ссылок происходит при каждом «клике» по ним.

Результат

В кратчайшие сроки обеспечена высокая степень фильтрации спама и фишинга. Встроенный симулятор фишинговых атак и обучающий контент повысили осведомлённость сотрудников.

Выводы

Обучение моделей AI потребовало около 1 месяца для снижения уровня ложных срабатываний до приемлемых значений. Обнаружение некоторых атак, например, Quishing, требует создания собственных правил.

NOVENTIQ

Global expertise, local outcomes

ISO/IEC 21017:2015 Cloud security

AIFC

Задача

Прохождение сертификации ISO/IEC 27017.
Часть процессов находятся в зоне ответственности облачного провайдера сервисов.

Решение – Purview Compliance Manager

Microsoft 365 уже обладает соответствующими сертификатами, а также предлагает интегрированные инструменты для контроля соответствия требованиям.

Результат

Сокращение времени и усилий, необходимых для подготовки к сертификации. Снижение операционных расходов, так как большое количество инструментов и ресурсов уже доступны в Microsoft 365.

NOVENTIQ

Global expertise, local outcomes

NOVENTIQ
Global expertise, local outcomes

Вопросы?

NOVENTIQ
Global expertise, local outcomes

Спасибо!

Sergey.Zhuykov@Noventiq.com

+7 705 311 62 12