Средства безопасности Office 365

Введение

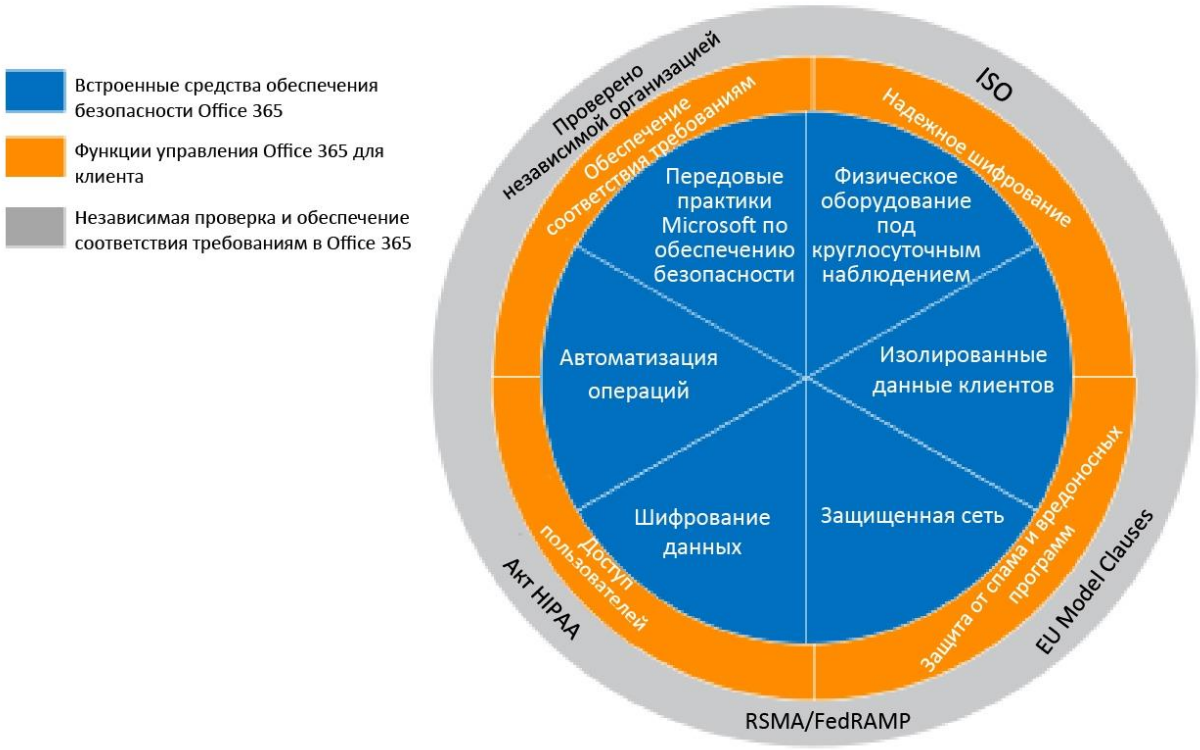
Сегодня практически все организации стремятся к тому, чтобы самостоятельно настраивать и контролировать функции, обеспечивающие безопасность облачных сервисов. Речь идет о компонентах, отвечающих за электронную почту, календарь событий, управление контентом, организацию совместной работы и объединенные коммуникации.

От ИТ-специалистов требуется предоставлять доступ к ИТ-сервисам, документам и данным, которые сегодня размещаются в самых разных местах и доступ к которым осуществляется с огромного количества устройств и платформ. Трудно отрицать очевидные преимущества подобного подхода для пользователей, однако он серьезно осложняет задачу управления безопасностью. Каждое конечное устройство представляет собой потенциальную точку атаки и дополнительный актив, за безопасность которого отвечают специалисты. Каждый день в мире растет количество угроз, с которыми сталкиваются организации. Они должны управлять потенциальными рисками, возникающими в результате случайной потери пользователем устройства или компрометации конфиденциальной информации. Именно поэтому компаниям требуется облачная служба с (а) надежными встроенными средствами безопасности, функции которых (б) можно настраивать в соответствии с потребностями бизнеса. Расширение функций удаленного доступа для поддержки передовых практик обеспечения безопасности — сложная и дорогостоящая задача, если в компании развернуты лишь локальные ИТ-сервисы.

Средства безопасности Office 365™

Microsoft — лидер в вопросах обеспечения безопасности облачных решений. Компания внедряет новые политики и компоненты управления одновременно с локальными центрами обработки данных и наиболее передовыми в этом отношении организациями, а иногда и опережает их. Безопасность Office 365 обеспечивают три компонента. Во-первых, Office 365 защищен встроенными средствами безопасности по умолчанию. Преимуществом Office 365 для пользователей являются встроенные в службу улучшенные функции защиты, разработанные на основе 20-летнего опыта компании в управлении онлайн-данными и подкрепленные значительными вложениями в инфраструктуру безопасности. В Office 365 уже внедрены процессы и технологии проактивного обнаружения и устранения угроз до того, как они превратятся в риски для клиентов. Продолжается развитие и улучшение этих технологий.

Во-вторых, функции управления Office 365 дают клиентам возможность самостоятельно настраивать параметры безопасности. Office 365 пользуется доверием клиентов практически из любой отрасли, в том числе со строгим нормативным регулированием (здравоохранение, финансы, образование, государственные учреждения). Office 365 управляет службами повышения продуктивности для широкого диапазона отраслей в разных странах мира. Благодаря этому клиенты имеют доступ к большому количеству надежных функций защиты данных. В-третьих, Office 365 работает с масштабируемыми процессами обеспечения безопасности, что позволяет проводить независимую проверку и обеспечивать соответствие нормативным требованиям, действующим в отрасли. В этом документе рассмотрены все три аспекта безопасности новой службы Office 365.



Встроенные средства безопасности

Физическое оборудование под круглосуточным наблюдением

Данные Office 365 хранятся в сети центров обработки данных (ЦОД) компании Microsoft, которые размещены в стратегических точках и находятся под управлением службы Microsoft Global Foundation Services. Эти ЦОД гарантируют предоставление услуг и защиту информации от стихийных бедствий или несанкционированного доступа. Персонал имеет доступ в ЦОД в течение 24 часов только для выполнения рабочих задач. Иными словами, доступ к приложениям и службам клиентов открыт узкому кругу лиц. Контроль физического доступа осуществляется посредством многочисленных процедур аутентификации и обеспечения безопасности, например используются бейджи и смарт-карты, биометрический сканер, двухфакторная проверка подлинности, в здании присутствуют сотрудники локальной службы безопасности, ведется постоянное видеонаблюдение. Центры обработки данных оборудованы датчиками движения, системами видеонаблюдения и сигнализации. Безопасность в случае стихийных бедствий обеспечивают сейсмоустойчивые стойки (где это необходимо), а также автоматические системы противопожарной безопасности и пожаротушения.

Изолированные данные клиентов

Одна из причин масштабируемости и низкой стоимости Office 365 состоит в том, что эта служба является многопользовательской (т. е. данные различных клиентов размещены на одних и тех же аппаратных ресурсах). Она предназначена для надежного и безопасного изолированного размещения данных многочисленных клиентов. Хранение и обработка данных каждого клиента осуществляется раздельно с помощью Active Directory® и других средств, специально разработанных для создания, контроля и обеспечения безопасности многопользовательских сред. Active Directory изолирует клиентов, используя зоны безопасности (известные также как «силосные башни»). Такой подход не позволяет одним клиентам получить доступ к данным других клиентов или поставить под угрозу безопасность этой информации.

За дополнительную плату можно приобрести версию Office 365, которая обеспечивает хранение данных на специально выделенном оборудовании.

Автоматизация операций

В ЦОД компании Microsoft доступ персонала к ИТ-системам, где хранятся данные клиентов, строго контролируется посредством управления доступом на основе ролей (RBAC) и процессов блокировки. Управление доступом — это автоматизированный процесс, который следует принципам разделения обязанностей и предоставления наименьших привилегий. Процесс гарантирует, что доступ к ИТ-системам получает только инженер, отвечающий определенным требованиям: его личные данные прошли проверку, отпечатки пальцев совпадают с отпечатками, хранящимися в системе, он прошел обучение по обеспечению безопасности и получил соответствующие допуски. Запрос инженера на выполнение определенных задач попадает в процесс блокировки. Этот процесс определяет продолжительность и уровень доступа независимо от того, нужно ли привлечь другого инженера в качестве наблюдателя для выполнения данной задачи. Подобного рода запросы регистрируются в журнале как запросы на обслуживание, которые можно проверить позднее.

Защищенная сеть

Сети центров обработки данных Office 365 сегментированы и обеспечивают физическое разделение критически важных внутренних серверов и устройств хранения от общедоступных интерфейсов. Средства безопасности пограничных маршрутизаторов выявляют попытки вторжения и признаки уязвимости системы. Подключение клиентов к Office 365 происходит по протоколу SSL, обеспечивающему безопасность Outlook, Outlook Web App, Exchange ActiveSync, POP3 и IMAP. Клиенты осуществляют доступ к веб-службам со своих компьютеров, подключенных к Интернету, а запросы на доступ попадают в ЦОД компании Microsoft. Подключения шифруются с использованием стандартных протоколов безопасности Transport Layer Security (TLS) и Secure Sockets Layer (SSL). Протоколы TLS/SSL гарантируют безопасное подключение клиентов к серверу, конфиденциальность и целостность данных, передаваемых между ПК и ЦОД. Клиенты могут настраивать параметры протокола TLS между Office 365 и внешними серверами как для входящей, так и для исходящей почты. По умолчанию этот параметр включен.

Шифрование данных

Клиентские данные в Office 365 либо находятся в хранилище данных, либо передаются из ЦОД через сеть на устройство клиента. Содержимое электронного сообщения зашифровывается на диске средством BitLocker с помощью алгоритма AES. Под защитой находятся все диски почтовых серверов.

Кроме того, Office 365 осуществляет транспортировку и сохранение сообщений типа S/MIME, а также сообщений, зашифрованных с помощью инструментов шифрования от сторонних разработчиков (например, PGP).

Передовые практики Microsoft по обеспечению безопасности

Обеспечение безопасности в Office 365 — это непрерывный процесс, а не просто последовательность определенных действий. Опытный и хорошо обученный персонал постоянно тестирует, обслуживает и совершенствует средства безопасности. Компания Microsoft стремится поддерживать актуальный уровень программных и аппаратных технологий, использовать надежные процессы разработки, построения, эксплуатации и поддержки. В качестве примера подобных процессов можно привести жизненный цикл разработки безопасных приложений, процессы регулирования трафика, превентивной защиты, обнаружения и устранения брешей в системе безопасности.

Жизненный цикл разработки безопасных приложений

Безопасность в компании Microsoft начинается задолго до того, как на свет появляется конкретное приложение или служба. Жизненный цикл разработки безопасных приложений (Security Development

Lifecycle, SDL) — это комплексный процесс обеспечения безопасности. В ходе его реализации происходит сбор информации о каждом этапе разработки и развертывания программного обеспечения и служб Microsoft, включая Office 365. Этот процесс помогает прогнозировать, выявлять и устранять уязвимости и угрозы во время всего производственного цикла — вплоть до запуска службы — благодаря требованиям, применяемым к разработке, анализу поверхности атаки и моделированию угроз. Компания Microsoft постоянно обновляет SDL, используя последние данные и передовой опыт для того, чтобы с самого первого дня обеспечить высокую надежность новых служб и программного обеспечения Office 365.

Регулирование трафика с целью предотвращения атак типа «отказ в обслуживании»

Служба Exchange Online отслеживает базовые показатели использования и регулирует стандартные всплески трафика таким образом, чтобы это не сказывалось на работе пользователей. Трафик регулируется с того момента, когда он превысил стандартные показатели, и до тех пор, пока использование не нормализуется. Exchange автоматически реагирует на любые скачки трафика, независимо от того, чем они вызваны: поведением пользователя или атаками типа DoS — и исключает влияние этих скачков на работу других пользователей. Кроме этого, Office 365 использует стороннюю коммерческую платформу мониторинга атак типа DoS для контроля и регулировки трафика.

Превентивная защита, обнаружение и устранение брешей в системе безопасности

Превентивная защита — это оборонительная стратегия, направленная на прогнозирование и проактивную защиту от вторжений. Данная стратегия требует постоянного совершенствования встроенных средств безопасности: сканирования портов и устранения обнаруженных проблем, выявления уязвимостей периметра, обновления ОС для установки актуальных версий средств обеспечения безопасности, обнаружения и предотвращения распределенных атак типа «отказ в обслуживании» (Distributed Denial of Service, DDOS), а также многофакторную аутентификацию при предоставлении доступа к службе. Процесс превентивной защиты предполагает пересмотр допусков и действий оператора или администратора и затрагивает как персонал, так и процедуры допуска к выполнению необходимых работ. Обнуляются разрешения служб для администраторов, ошибки в службе устраняются точно в срок при предоставлении допуска и повышении привилегий инженера (это гарантирует, что все необходимые меры будут предприняты в нужное время), сегрегируются почтовая среда сотрудников и среда допусков в рабочую зону. Служащие, не прошедшие проверку основных данных, автоматически лишаются прав доступа с высокими привилегиями. Результаты тщательных проверок основных данных служащих утверждаются в ручном режиме.

Помимо этого, превентивная защита предполагает автоматическое удаление учетных записей пользователя, если сотрудник увольняется из компании, переходит в другую группу или не использует учетную запись до истечения срока ее действия. Там, где это возможно, вмешательство человека заменяется автоматическим процессом, выполняемым специальным инструментом; речь идет о таких рутинных операциях, как развертывание, отладка, сбор данных диагностики и перезапуск служб. В Office 365 продолжается развитие автоматизированных систем, которые позволяют выявлять аномальное и подозрительное поведение и мгновенно реагировать на него с целью устранения риска безопасности. Компания Microsoft постоянно совершенствует высокоэффективные системы автоматического развертывания исправлений, которые решают проблемы, обнаруженные системами мониторинга, без вмешательства человека. Это значительно повышает уровень безопасности и гибкость службы. В Office 365 проводятся тесты на защиту от несанкционированного доступа, цель которых — постоянное улучшение процедур реагирования на инциденты. Результаты этих тестов дают специалистам по безопасности возможность создавать систематизированные, повторяемые и оптимизированные пошаговые процессы реагирования на инциденты и автоматизировать эти процессы.

Элементы управления на стороне клиента

Office 365 сочетает в себе знакомый пользователям пакет приложений Microsoft Office с облачными версиями служб мгновенных сообщений и совместной работы: Microsoft Exchange Online, Microsoft SharePoint® Online и Microsoft Lync® Online. Каждая служба предлагает индивидуализированные функции безопасности, которыми управляет клиент. Элементы управления позволяют обеспечивать соответствие нормативным требованиям, предоставлять сотрудникам организаций доступ к службам и контенту, настраивать защиту от спама и вредоносных программ, а также шифровать данные с помощью ключа.

Использование функций шифрования

Дополнительно к описанным выше надежным функциям шифрования в Office 365 имеются службы управления правами Active Directory Rights Management Services (ADRMS). Они обеспечивают необходимую гибкость при выборе элементов, которые нужно зашифровать. Кроме того, ADRMS можно использовать для шифрования данных, расположенных в хранилище. Включив специализированные службы шифрования Office 365, пользователь получает возможность шифровать электронную переписку с нефедеративными пользователями. Пакет Office Профессиональный плюс содержит улучшенные функции безопасности с гибкой встроенной поддержкой криптографии, интегрированной с криптографическими интерфейсами следующего поколения (CNG) для Windows. Администраторы могут задавать алгоритмы шифрования для шифрования и подписывания документов.

Предоставление доступа пользователям

Данные и службы Office 365 защищаются на следующих уровнях: ЦОД, сетевой, логический, уровень хранения и передачи. Наряду с этим критически важно понимать, какие пользователи получают доступ к данным и какие операции могут выполнять. В качестве базовой платформы идентификации в Office 365 используется Windows Azure Active Directory. Клиенты Office 365, которым необходимы методы строгой аутентификации, получают возможность тщательно контролировать доступ и использование службы ИТ-специалистами и конечными пользователями. Кроме того, Office 365 интегрируется с локальной службой каталогов Active Directory и другими системами хранения и идентификации каталогов, например Active Directory Federation Services (ADFS), или сторонними системами токенов безопасности (STS) для надежной аутентификации с использованием токенов.

Федеративные удостоверения клиентов и обеспечение безопасности с помощью единого входа

Администраторы могут включить в федерацию Active Directory или другие системы каталогов с помощью Windows Azure Active Directory — платформы аутентификации Office 365. После завершения настройки федерации все клиенты Office 365, чьи удостоверения изданы на основе федеративного домена, могут использовать данные входа в корпоративную сеть для работы с Office 365. Федерация обеспечивает безопасную аутентификацию на основе токенов. Администраторы могут создавать дополнительные механизмы аутентификации, например:

- двухфакторную проверку подлинности;
- способ управления доступом со стороны клиента, позволяющий организациям контролировать, как пользователи будут получать доступ к информации с различных устройств или из разных мест, либо с учетом этих двух факторов (например, ограничение доступа с общедоступных компьютеров или через публичные сети Wi-Fi);
- контроль доступа на основе ролей. Эта процедура аналогична процедуре, описанной выше в разделе «Автоматизация операций» для персонала компании Microsoft.

Федерация обмена мгновенными сообщениями (IM) предоставляет пользователям Lync Online возможность отправлять надежно защищенные IM пользователям других организаций, которые используют Lync Online, локальные серверы Lync Server 2010 и даже публичную IM-сеть Skype. Все федеративные коммуникации

между IM-системами шифруются на прокси-серверах доступа. Более того, Lync Online позволяет администраторам сохранять IM-беседы.

Двухфакторная проверка подлинности

Двухфакторная проверка подлинности повышает уровень безопасности в среде со множеством устройств, ориентированной на облачные технологии. Компания Microsoft предлагает решение для двухфакторной проверки подлинности с возможностью аутентификации по телефону, а также поддерживает решения сторонних разработчиков. При двухфакторной проверке подлинности с использованием телефона пользователь получает сообщение с ПИН-кодом и вводит его в качестве второго пароля при входе в службу.

Использование функций соответствия нормативным требованиям

Office 365 предлагает ряд функций соответствия нормативным требованиям: предотвращение утери данных (DLP), обнаружение электронных данных (eDiscovery), а также инструменты проведения аудита и отчетности. Все больше пользователей используют эти возможности, поскольку они просты и не влияют на производительность.

Предотвращение утери данных (DLP)

Вредоносные программы и атаки могут пробить бреши в системе безопасности, однако гораздо большие риски во многих организациях связаны с ошибками пользователей. Exchange Online использует технологию предотвращения утери данных (DLP), с помощью которой осуществляется идентификация, мониторинг и защита конфиденциальных данных. Эта технология позволяет выявлять риски для данных и управлять этими рисками. С помощью технологий DLP можно выявить конфиденциальную информацию в электронном сообщении, например номер социального страхования или кредитной карты, и предупредить пользователя посредством сообщения PolicyTips (Советы по политике) прежде, чем он отправит подобное письмо. В распоряжение администраторов предоставлен широкий спектр функций управления, позволяющих устанавливать ограничения во всей организации. Например, можно просто предупредить пользователя о том, он собирается переслать конфиденциальные данные, можно потребовать пройти авторизацию перед отправкой либо заблокировать отправку. Функции DLP позволяют просматривать сообщения и вложения, а также формировать подробные отчеты о том, какие данные отправляются и кем.

Политики аудита и хранения

Политики аудита Office 365 дают клиентам возможность регистрировать в журнале такие события, как просмотр, изменение и удаление содержимого электронных сообщений, документов, списков заданий, списков проблем, дискуссионных групп и календарей событий. При включении аудита в состав политики управления информацией администраторы могут получать данные аудита и обобщать использование информации. С помощью этих отчетов можно будет определить, как используется информация, управлять соответствием нормативным требованиям и анализировать проблемные области.

Обнаружение электронных данных eDiscovery

Новый, простой в использовании центр eDiscovery Center предназначен для профессиональных пользователей, например для сотрудников, отвечающих за обеспечение соответствия требованиям, или руководителей отдела кадров. Он позволяет самостоятельно решать задачи по поиску электронных данных без привлечения ИТ-специалистов. Центр eDiscovery дает клиентам возможность извлекать содержимое из информации в Exchange Online, SharePoint Online, Lync Online и даже из общих файлов. Office 365 с встроенным центром eDiscovery объединяет функции поиска и сохранения электронных сообщений, документов и содержимого почтовых ящиков сайта. Центр eDiscovery дает клиентам возможность определить, что они хотят найти и сохранить. Функция поиска только нужной информации помогает снизить затраты на выполнение таких операций. Процессы центра eDiscovery осуществляются в фоновом режиме и не требуют привлечения пользователя для сохранения и поиска данных.

Управление утечкой информации

В Office 365 имеются функции обеспечения соответствия, которые клиенты могут использовать при решении проблем, связанных с утечкой информации. Например, если правительственные служащие переслали конфиденциальные данные в Office 365, то смогут сами удалить их. Должностные лица, отвечающие за обеспечение соответствия требованиям и безопасность и имеющие соответствующие привилегии RBAC, могут использовать центр eDiscovery для поиска определенного сообщения или документа и его необратимого удаления. Жесткие диски в случае утечки информации никогда не используются для других целей, не ремонтируются или иным образом перемещаются за пределы зоны физической безопасности центров обработки данных Office 365. Эти диски уничтожаются, в случае если выходят из эксплуатации в инфраструктуре Office 365.

Использование средств защиты от спама и вредоносных программ

Клиенты имеют возможность настраивать средства защиты от спама и вредоносных программ. Кроме того, можно использовать собственные службы защиты от вредоносных программ и направлять потоки данных в Office 365 (и из него) через службы сторонних поставщиков. В Office 365 выполняется антивирусное сканирование входящих, исходящих и внутренних сообщений посредством нескольких механизмов.

Office 365 анализирует полученные сообщения и присваивает им оценку вероятности нежелательной почты (SCL). Сообщения с высокой оценкой SCL удаляются на шлюзе, а сообщения с низкой оценкой SCL доставляются в почтовые ящики пользователей. Сообщения с граничной оценкой SCL помещаются в папки нежелательной почты пользователей, откуда автоматически удаляются через 30 дней. Администраторы могут использовать центр администрирования Office 365 Administration Center для управления настройками защиты от спама и вредоносных программ, в том числе для использования расширенных функций контроля за нежелательной почтой и составления действительных в рамках всей организации списков надежных и заблокированных отправителей. Пользователи имеют возможность управлять собственными списками надежных и заблокированных отправителей через личные папки входящей почты в Microsoft Outlook или Microsoft Outlook Web App.

Для удаления документов с вредоносным ПО используются компоненты управления содержимым и антивирусное сканирование на основе нескольких механизмов. Office 365 использует расширения имен файлов для блокировки файлов определенных типов, которые могут содержать вредоносное ПО, при попытках их передачи в службу или извлечения из нее. В Office 365 применяется интеллектуальный фильтр мгновенных сообщений (IIMF) для защиты службы и сетей клиентов от спама и вредоносных программ в IM-сообщениях. Компания Microsoft разработала фильтр IIMF, опираясь на многолетний опыт эксплуатации безопасных глобальных IM-систем.

Независимая проверка и обеспечение соответствия требованиям

Office 365 превращает обеспечение безопасности в масштабируемый процесс, который можно быстро адаптировать к тенденциям в этой области, а также к специфическим потребностям отдельных отраслей. Компания Microsoft регулярно анализирует процессы управления рисками, разрабатывает и поддерживает структуру управления безопасностью в соответствии с самыми современными стандартами. Жизненный цикл Office 365 предусматривает проведение внутреннего анализа и внешних аудитов с привлечением сторонних организаций. Разработка всестороннего подхода к безопасности облачных приложений является результатом тесных рабочих взаимоотношений с другими командами компании Microsoft.

Эксплуатация глобальной облачной инфраструктуры порождает необходимость соблюдения обязательств в сфере соответствия требованиям, а также проведения аудита с привлечением сторонних организаций. Контролируемые требования содержатся в правительственных документах, промышленных нормах и стандартах, внутренних политиках и передовых отраслевых практиках. В Office 365 ведется постоянный

анализ новых требований, соответствие которым необходимо обеспечивать, с последующим внедрением соответствующих служебных процессов. Как результат, Office 365 прошел ряд независимых сертификаций и получил сертификаты соответствия стандарту ISO 27001 и аудиторским стандартам SSAE16 SOC 1 (Type II). Office 365 может использоваться для передачи данных из Европейского Союза через платформы U.S.-EU Safe Harbor Framework и EU Model Clauses. Компания планирует подписать соглашение о деловом сотрудничестве (HIPAA Business Associate Agreement, BAA) со всеми клиентами, которые получили разрешение на работу от Федерального агентства США в соответствии с актом FISMA и объявили о принимаемых ими мерах по обеспечению безопасности в публичном регистре Альянса по обеспечению облачной безопасности (Cloud Security Alliance). Office 365 предоставляет возможность использовать элементы управления, обеспечивающие соответствие указанным выше стандартам, клиентам, на которых не распространяется действие соответствующих законов или которым не обязательно использовать подобные элементы.

ISO 27001

Служба Office 365 построена на основе стандартов ISO 27001 и стала первой крупной общедоступной облачной службой по повышению производительности бизнеса, которая распространила строгие международные стандарты на физическую среду, логику, процессы и элементы управления.

FISMA

Служба Office 365 получила разрешение на работу FISMA moderate Authority to Operate от многочисленных федеральных агентств. Эксплуатация в соответствии с разрешением FISMA требует прозрачности и регулярной отчетности о соблюдении требований обеспечения безопасности, которая направляется нашим федеральным клиентам в США. Компания Microsoft применяет эти специализированные процессы в своей инфраструктуре для дальнейшего улучшения программы повышения уровня безопасности и обеспечения соответствия требованиям (Online Services Security and Compliance program) в интересах клиентов, которые не подпадают под регулирование на соответствие требованиям FISMA.

HIPAA BAA

Служба Office 365 — первая крупная общедоступная облачная служба по повышению производительности бизнеса, которая предлагает соглашение HIPAA BAA всем своим клиентам. HIPAA — это закон США, который применяется по отношению к медицинским учреждениям и регулирует использование, раскрытие и охрану защищенной информации о состоянии здоровья (PHI), а также требует от этих учреждений подписания соглашения о деловом сотрудничестве со всеми поставщиками, которые имеют доступ к данным PHI.

EU Model Clauses

Служба Office 365 стала первой крупной общедоступной облачной службой по повышению производительности бизнеса, которая подписала стандартные контрактные статьи, разработанные Европейским союзом (известные как EU Model Clauses), со всеми клиентами. Статьи EU Model Clauses связаны с международной передачей данных. Служба Office 365 — одна из немногих, если не единственная, облачная служба, которая получила сертификаты от европейских агентств по защите данных (DPA) в отношении соответствия требованиям EU Model Clauses. Такие сертификаты получены в Баварии, Дании, Франции, Ирландии, Люксембурге, Мальте и Испании.

Альянс по обеспечению облачной безопасности (Cloud Security Alliance)

Служба Office 365 соответствует требованиям по обеспечению соответствия и управлению рисками, установленным альянсом Cloud Security Alliance в матрице Cloud Control Matrix (CCM). Матрица Cloud Control Matrix (CCM) публикуется некоммерческой, управляемой ее членами организацией, состоящей из ведущих специалистов отрасли, которые ставят своей целью оказывать содействие клиентам в принятии правильного

решения при переходе в облако. Матрица содержит детальное описание концепций, принципов безопасности и конфиденциальности, имеющих отношение к 13 областям в соответствии с руководством Cloud Security Alliance. Служба Office 365 опубликовала подробный обзор своих возможностей в отношении соответствия требованиям CCM. В нем описано, каким образом обеспечивается такое соответствие, приведена подробная информация для клиентов, которая вооружает их знаниями, необходимыми для оценки многочисленных предложений, имеющихся сегодня на рынке.

Заключение

Сегодня бизнесу необходимы службы повышения производительности, которые помогут клиентам выполнять больше задач практически из любого места при условии обеспечения высокого уровня защиты от постоянно возрастающего количества угроз. Служба Office 365 в состоянии выполнить два этих требования, предлагая облачную платформу повышения производительности и обеспечивая высокий уровень ее безопасности. Информацию о службе Office 365 в отношении ее безопасности, соблюдения конфиденциальности, обеспечения соответствия требованиям, прозрачности, а также бесперебойности работы можно получить в центре управления безопасностью Office 365. Платформа Office 365 обеспечивает безопасность на всех уровнях: от разработки приложений до физических центров и доступа конечных потребителей. В настоящее время найдется немного организаций, способных сравнительно недорого поддерживать аналогичный уровень локальной безопасности.

Важно отметить, что Office 365 предлагает как (а) встроенные средства обеспечения безопасности, которые упрощают процесс защиты данных, так и (б) гибкость, необходимую администраторам для настройки, интеграции и управления процессами обеспечения безопасности в соответствии с потребностями компании. Выбирая Office 365, вы приобретаете партнера, который действительно понимает потребности бизнеса в обеспечении безопасности и пользуется доверием у множества компаний практически во всех отраслях и уголках земного шара.