Forbes

Новая эра: как бизнесу развиваться в цифровой реальности

Издание: Forbes

Спикер: Вячеслав Максимов, технический директор АО НИП «Информзащита»

Авторы: Ирина Телицына, Дмитрий Филонов

Как пандемия повлияла на цифровизацию бизнеса и что будет дальше

Даже для опытных предпринимателей, чьи компании прошли через несколько внешних и внутренних кризисов, нынешняя ситуация в экономике не имеет аналогов. Пандемия и связанные с нею ограничения вызвали рекордное сокращение потребительского спроса — в I квартале 2020 года, по оценке McKinsey, он впервые с 40-х годов прошлого века упал на 40–50%. Быстрые изменения бизнес-среды под влиянием глобальных трендов — как технологических, так и социально-демографических — еще до пандемии побуждали компании к трансформации. Текущая ситуация стала катализатором этих изменений.

Кристина Тихонова, президент Microsoft в России, отмечает, что сегодняшняя ситуация беспрецедентна для бизнеса любого масштаба и отрасли. Путь цифровой трансформации, который раньше мог растянуться на несколько лет, многие прошли за пару месяцев. «Это очень важный этап для многих организаций: по мере того, как мир привыкает к жизни в новых условиях, бизнес адаптируется, становится все более цифровым и гибким, отвечая на «новые правила игры». Технологии стали ключевым инструментом в «перезагрузке» предприятий, способствуя развитию инноваций даже в традиционных областях. Мы стремимся не только предоставить необходимые технологические инструменты для обеспечения непрерывности бизнеса, но и оказать нашим заказчикам необходимую поддержку, предоставить необходимые технологические инструменты для обеспечения непрерывности бизнеса и предложить сценарии по наиболее эффективной цифровизации. В этом нам помогает обширная экосистема наших партнеров по всему миру — компаний, создающих на основе наших технологий собственные бизнес-решения, и тех, кто помогает развертывать и внедрять наши продукты», — говорит Кристина Тихонова. Экспертиза, накопленная в этой экосистеме, может помочь бизнесу оставаться конкурентоспособным и в текущих обстоятельствах: оптимизировать логистику, настроить удаленную работу сотрудников, обеспечить безопасность и многое другое. С новыми вызовами, по мнению президента Microsoft, пришли и новые возможности, а уроки, вынесенные из этих преобразований, как и приобретенные навыки, будут способствовать успеху бизнеса в гораздо более долгосрочной перспективе.

Тренд:

По мере цифровизации все большего количества отраслей и сфер жизни растут и риски в сфере кибербезопасности — по данным PwC, несколько последних лет киберугрозы, по мнению опрашиваемых руководителей компаний, входят в топ-3 рисков для непрерывности бизнеса. Рынок сервисов кибербезопасности растет теми же темпами, что и рынок цифровых решений для бизнеса. Эксперты Accenture осенью 2019 года прогнозировали, что к 2021 году объем мирового рынка информационной безопасности увеличится на 66% и составит $202 млрд. При этом совокупный мировой ущерб от кибератак может вырасти к 2021 году на 39%, до $2,1 млрд.

Новые вызовы и ответ на них:

«Еще в начале года никто не ожидал такого массового перехода на удаленную работу», — говорит Вячеслав Максимов, технический директор компании «Информзащита», системного интегратора со специализацией на информационной безопасности. Как рассказывает Максимов, многие бизнесы, оказавшись в условиях удаленной работы, столкнулись с необходимостью организации надежного и безопасного удаленного доступа к внутренней инфраструктуре. И многие оказались не полностью готовы. С технической стороны, ключевыми проблемами стали недостаточная пропускная способность интернет-каналов и сетевого оборудования, малая мощность терминальных серверов, размытие периметра.

Компьютеры пользователей раньше находились внутри доверенной сети компании, а теперь — в малозащищенных домашних сетях. Чем это грозит? Возрастают риски утечки конфиденциальных данных, компрометации данных и информационных систем. «Подавляющее большинство компаний справились с возникшими проблемами и обеспечили

возможность удаленной работы, масштабировав уже применяемые решения. Но в сложившихся условиях скорость была гораздо важнее надежности и безопасности. Постоянное решение требует переоценки рисков, внедрения дополнительных систем и средств защиты. А на это нужно время, которого просто не было», — говорит Максимов.

Александр Беленький, директор департамента по работе со средними и малыми организациями и партнерами Microsoft в России, приводит данные исследования компании Wrike: 41% удаленных работников получают доступ к конфиденциальной рабочей информации, используя незащищенные персональные устройства. Решить проблему защиты данных при удаленной работе позволяют продукты, которые обеспечивают управление системой обеспечения безопасности и доступа пользовательских устройств в сети, такие как, к примеру, Microsoft Enterprise Mobility + Security.

По мнению эксперта, целенаправленные атаки, основанные на принципах социального инжиниринга (фишинг), по-прежнему остаются одним из самых больших рисков для организаций. «Из-за текущей ситуации в мире наши почтовые ящики, телефоны, телевизоры и новости полны сообщениями о COVID-19, и злоумышленники этим пользуются. Они знают, что многие сотрудники переходят по ссылкам не глядя. Поэтому сейчас наблюдается рост успешных атак с применением фишинга и социальной инженерии. Злоумышленники добавляют ключевые слова, связанные с COVID-19, в уже существующие кампании, включая вымогательские программы, фишинг и другие механизмы распространения вредоносных программ».

Как показало недавнее исследование Microsoft и TAdviser, с целенаправленными кибератаками столкнулись 39% компаний сектора СМБ. «Встроенное в Microsoft Office 365 решение Advanced Threat Protection имеет прогрессивные методы отслеживания борьбы и с фишинговыми атаками. К примеру, оно может отмечать подозрительные паттерны с помощью алгоритмов машинного обучения, а также позволяет системным администраторам производить симуляцию атак, чтобы учитывать варианты реагирования сотрудников на подобные сообщения, — отмечает Александр Беленький. — Очень важно проводить обучающие тренинги по информационной безопасности для повышения цифровой грамотности сотрудников, тем самым снижая риски утечки из-за человеческого фактора». Новая реальность:

По словам Максимова из «Информзащиты», создание безопасного доступа при удаленной работе станет одним из трендов. Раньше для многих организаций удаленная работа была скорее исключением: человек мог работать из командировки или иногда из дома. Но из-за вынужденного полномасштабного режима удаленной работы компании оценили плюсы такого формата и стали задумываться о возможности работы хотя бы части сотрудников удаленно при обеспечении безопасности данных.

Александр Ермаков, управляющий партнер Awara IT, отмечает, что использование все большего количества цифровых решений в разных отраслях тоже обостряет вопрос кибербезопасности: «Одно дело, когда компания эпизодически использует какое-либо решение, и совсем другое дело, когда это решение становится неотъемлемой частью критического бизнес-процесса. Именно сейчас и проявились в полной мере все недостатки безопасности многих систем, что отнюдь не сказалось положительно на доверии к ним рынка. Именно поэтому для компании Microsoft на первый план выходит безопасность бизнес-приложений — корпорация очень много инвестирует сейчас именно в кибербезопасность».

Вячеслав Максимов из «Информзащиты» добавляет, что за последние годы у руководителей компаний существенно вырос уровень осведомленности в области информационной безопасности, уровень понимания необходимости системного обеспечения защитных мер. Существенно вырос и спрос на специалистов по информационной безопасности: они стали острым дефицитом на рынке труда. Это обуславливает еще один тренд — рост востребованности профессиональных сервисов по информационной безопасности, передачи на аутсорсинг функций, требующих глубоких компетенций в предметной области.

По словам Александра Беленького, из-за невероятной скорости произошедших изменений многие компании просто не успели принять необходимые меры защиты. На помощь приходят готовые решения — к примеру, Microsoft и «Информзащита» предлагают виртуальный облачный Security Operation Center (SOC) на базе Microsoft Azure Sentinel, который включает в себя не только инновационную технологическую платформу, но и сервисы по мониторингу и реагированию на инциденты от экспертов. У облачного SOC есть несколько плюсов: он не требует покупки дополнительной аппаратной инфраструктуры, ее внедрения и развертывания. Организации, которые занимаются предоставлением услуг по информационной безопасности, настраивают его под политики безопасности заказчика. Помимо этого, у организации отпадает необходимость искать и нанимать дополнительных экспертов по защите данных.

«Интеллектуальные возможности, встроенные в решения Microsoft Security, обучены на основе 8 трлн сигналов об ежедневных угрозах, а также на знаниях 3500 экспертов по безопасности. Специально разработанные алгоритмы и модели машинного обучения ежедневно изучают миллиарды запросов. Благодаря этому решения Microsoft Security помогают выявлять угрозы и реагировать на них на 50% быстрее, чем это было возможно всего 12 месяцев назад. Сегодня решения Microsoft Security способны автоматизировать 97% рутинных задач, которые отнимали у специалистов по безопасности ценное время еще два года назад», — отмечает Александр Беленький.

Станут ли компании меньше тратить на информационную безопасность из-за кризиса? По словам Вячеслава Максимова, сокращение бюджетов и отказ от каких-то дорогостоящих решений возможен. Но он приводит в пример кризис 2014 года: подразделения по информационной безопасности это затронуло в меньшей степени. «Во время кризисов возрастают риски, а такие подразделения как раз с рисками борются», — говорит Максимов.

Материал приводится в сокращенном виде.

Полная версия: https://www.forbes.ru/partnerskie-materialy-photogallery/402273-novaya-era-kak-biznesu-razvivatsya-v-cifrovoy-realnosti