VERITAS

Болезни роста

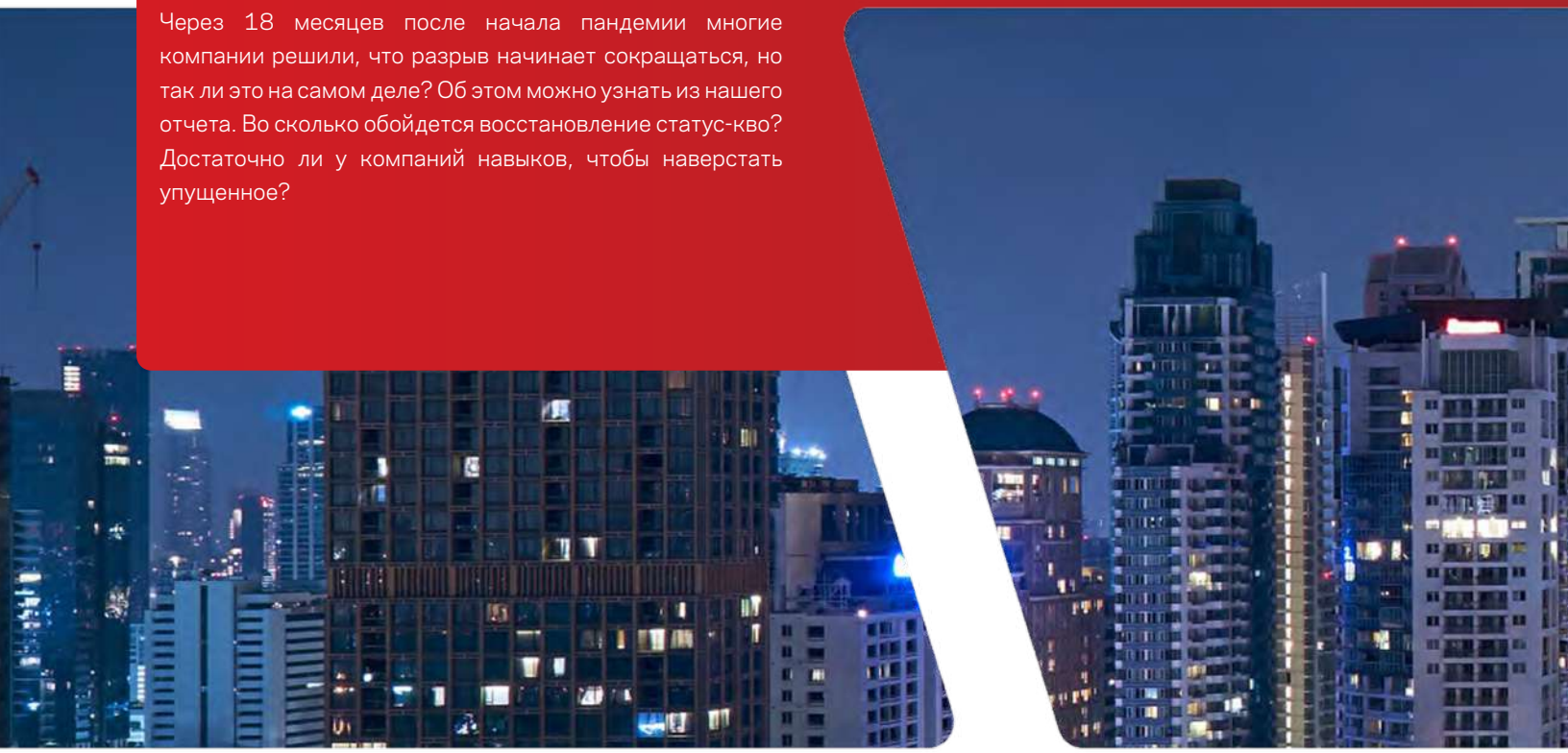
Ускорение цифровой трансформации на волне пандемии COVID-19 повышает риски, связанные с шифровальщиками

Введение

Чтобы защита от угроз была по-настоящему надежной, инфраструктура безопасности должна развиваться в том же темпе, что и другие компоненты информационной среды. Каждое новое приложение, система или рабочая нагрузка, появляющиеся в технологическом стеке организации, должны сопровождаться адекватными инструментами защиты. Однако зачастую потребность (или желание) внедрять инновации ускоренными темпами нарушает этот баланс, и образующийся разрыв делает критические системы и данные уязвимыми для кибератак.

Пандемия COVID-19 послужила катализатором появления таких разрывов во множестве организаций. Компании были вынуждены быстро вводить в эксплуатацию системы и технологии, необходимые в новой реальности: удаленные рабочие места, бесконтактное взаимодействие, предоставление клиентам всех услуг онлайн. Однако при этом приходилось жертвовать вопросами безопасности, что создало эффект «грома и молнии»: сначала мы увидели вспышку инноваций, и лишь затем последовала череда инцидентов.

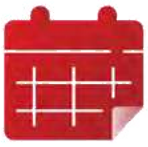
Через 18 месяцев после начала пандемии многие компании решили, что разрыв начинает сокращаться, но так ли это на самом деле? Об этом можно узнать из нашего отчета. Во сколько обойдется восстановление статус-кво? Достаточно ли у компаний навыков, чтобы наверстать упущенное?



Основные выводы

НАСКОЛЬКО ВЕЛИКО ОТСТАВАНИЕ?

Облачные технологии (**56%**) и безопасность (**51%**) чаще всего назывались среди проблемных областей, которые делают организации уязвимыми.



В среднем для устранения уже имеющихся уязвимостей организациям потребуется около **двух лет**.

Средние затраты организаций на решение стратегических проблем с технологиями составят в ближайший год **2,47 миллиона** долларов США.

В среднем компании оценивают численность дополнительного IT-персонала, который им придется нанять для устранения технологического разрыва, в **27 человек**.

В ЧЕМ ПРИЧИНА ОТСТАВАНИЯ?

Организациям не удается поддерживать высокий темп
Только 61% опрошенных организаций уверены, что технологическое отставание программ безопасности, вызванное ускоренной цифровой трансформацией за последние 18 месяцев, полностью устранено.

Технологии приходилось внедрять незапланированно
80% компаний отклонились от первоначальных планов развития облачной инфраструктуры после начала пандемии.

Нет точного понимания, какие технологии были внедрены
Только 58% опрошенных руководителей смогли назвать точное количество облачных сервисов, которые, как они считают, используются в их организациях.

Нет точного понимания, что необходимо защищать
В среднем 35% информации в организациях относится к «темным данным», 50% — к устаревшим, избыточным или незначительным, и только 16% составляют критически важные данные.

НАСКОЛЬКО УЯЗВИМЫМИ СТАЛИ ОРГАНИЗАЦИИ?

88% **организаций были вынуждены приостанавливать работу за последние 12 месяцев**

2,57

В среднем за последние 12 месяцев каждая организация 2,57 раз подвергалась атакам шифровальщиков, которые приводили к незапланированному простою. 14% организаций испытали такие атаки пять и более раз.

в 5 раз

В среднем организации с хотя бы одной стратегической проблемой подвергались атакам шифровальщиков и были вынуждены приостанавливать работу в пять раз чаще, чем организации без таких проблем.

64%

компаний стали уделять больше внимания обновлению и модернизации программного обеспечения из соображений безопасности, связанных с COVID-19.

Насколько велик разрыв, связанный с ускорением инноваций?

На протяжении последних полутора лет компаниям приходится иметь дело с последствиями событий, которые никто не мог предугадать. И в этой ситуации они пытаются действовать наилучшим возможным образом. Сама возможность выживания для многих компаний в значительной степени зависит от способности их IT-команд быстро реагировать на меняющиеся условия и внедрять новые инструменты, в частности для удаленной работы.

К сожалению, столь высокие темпы цифровой трансформации привели к тому, что инфраструктура этих организаций оказалась без должной защиты. Например, многие новые приложения, зачастую расположенные в облаке, стали уязвимы для киберугроз, связанных с безопасностью данных, например для вирусов-шифровальщиков. Такую болезнь роста можно назвать «технологическим разрывом» или «отрывом» общего уровня развития информационных систем от развития средств защиты. Любой из этих терминов в нашем отчете обозначает цифровой риск, который уже существует в организации и будет существовать до тех пор, пока инструменты безопасности не станут снова адекватны технологиям, используемым в бизнесе.

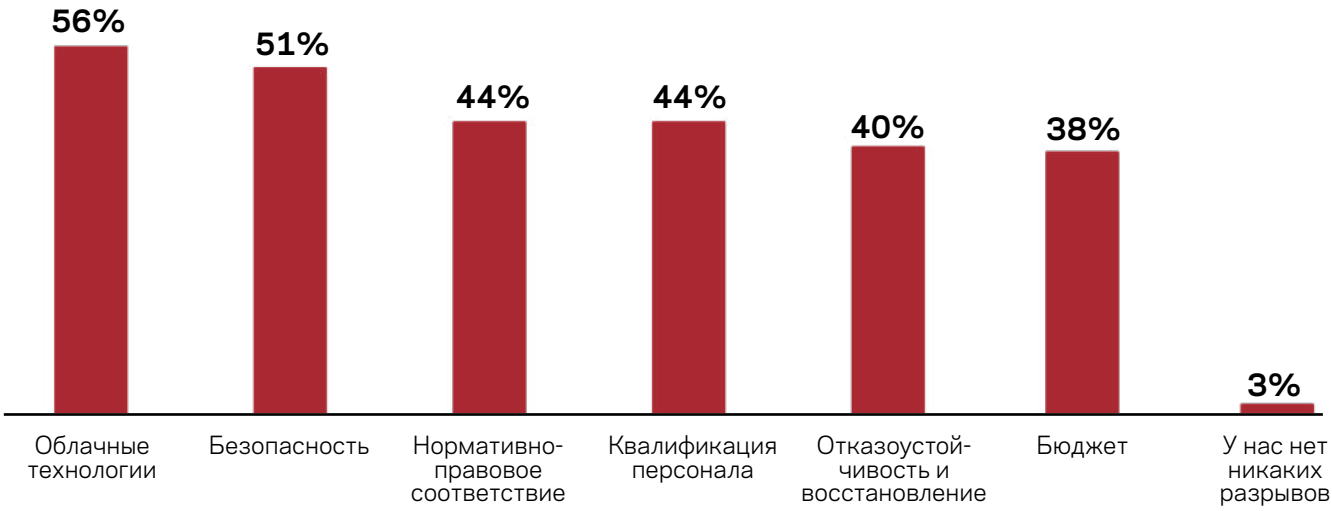
Причины возникновения этого кризиса совершенно понятны, и главное внимание сейчас следует уделять поиску эффективных решений для выхода из него. Так насколько же серьезна эта проблема на сегодняшний день?

Постоянный характер проблемы подчеркивается тем фактом, что 97% лиц, принимающих решения в сфере IT, признали наличие незакрытых уязвимостей, ставших последствием срочных инициатив периода пандемии, как минимум в одной ключевой области.

Чаще всего среди таких областей назывались облачные технологии (56%) и безопасность (51%). Они наглядно демонстрируют, как ускоренное развитие бизнес-систем привело к отставанию в вопросах безопасности, которое теперь должно быть ликвидировано как можно скорее, чтобы защитить организацию от таких серьезных угроз, как вирусы-шифровальщики.

ВОПРОС

По вашему мнению, в каких областях ускорение цифровой трансформации, подстегнутое пандемией COVID-19, привело к появлению технологических разрывов? [2050 респондентов, некоторые ответы пропущены]



Хотя облачные технологии и безопасность — не единственные сферы, в которых необходимо ликвидировать технологическое отставание, в них этот вопрос стоит наиболее остро. Почти половина опрошенных (47%) отметили, что проблемы, вызванные экстренным внедрением облачных технологий, входят в тройку основных вопросов, которым будет уделено первоочередное внимание. Более того, 20% указали, что это единственный действительно серьезный вызов, с которым им придется иметь дело. С безопасностью ситуация выглядит похожим образом: для 41% эта сфера входит в тройку основных, а почти для каждого пятого (16%) является единственной нерешенной проблемой.

Тем не менее, для эффективного решения всех перечисленных проблем организации должны распределять свои усилия оптимальным образом, и возможно поэтому данный процесс идет довольно медленно. В среднем участники опроса ожидают, что устранение всех технологических разрывов в их организации займет около двух лет.

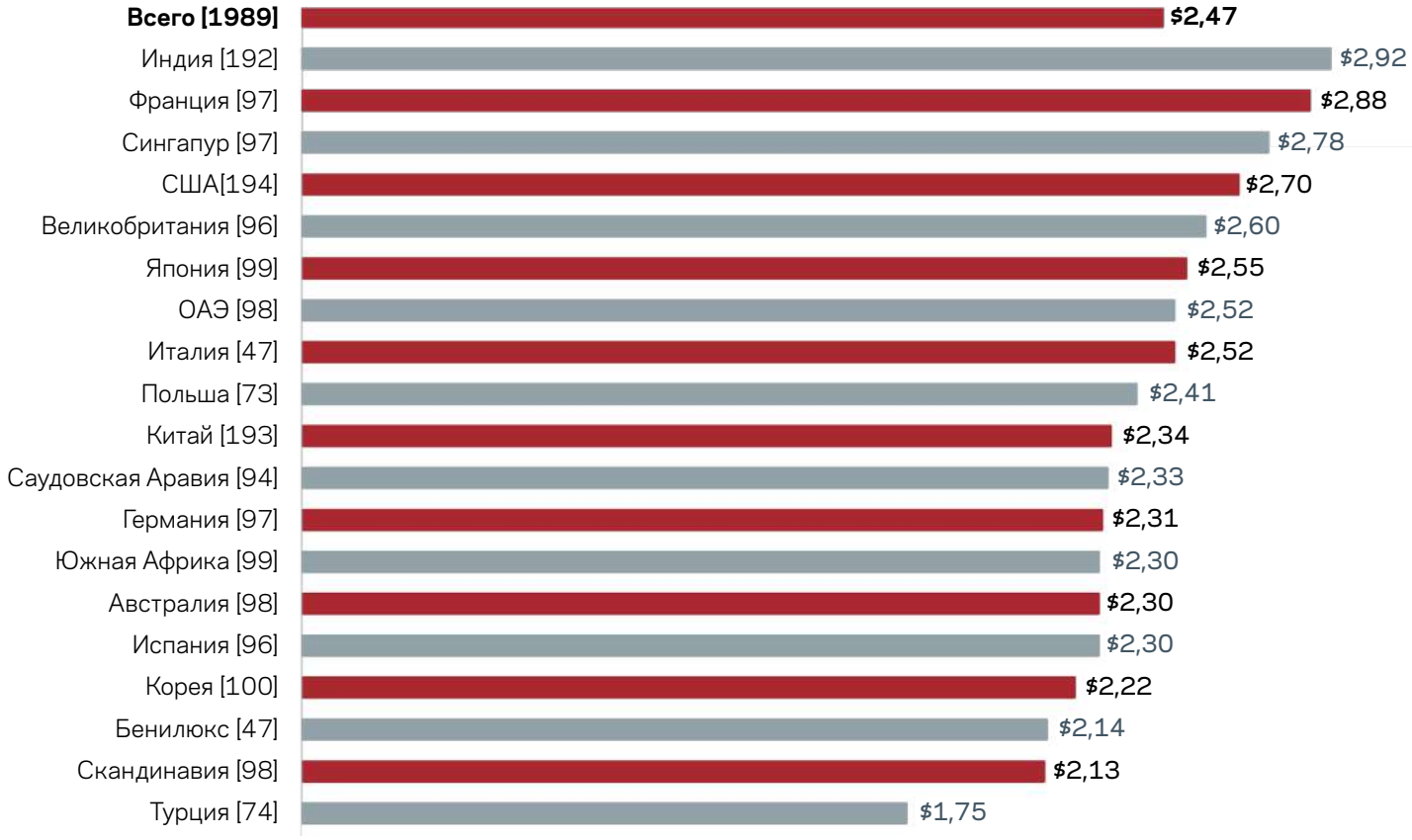
Серьезное беспокойство вызывает тот факт, что по ожиданиям 42% опрошенных восстановление статус-кво займет более двух лет.

К сожалению, время сейчас играет не на стороне организаций. Чем дольше они занимаются решением проблем, тем дольше останутся уязвимыми для целого спектра опасных кибератак. Как это часто бывает при поиске решений, важной частью уравнения являются бюджетные ограничения.

Организациям, которые намерены ускорить закрытие инфраструктурных уязвимостей и защититься от кибератак, придется в следующие 12 месяцев потратить в среднем 2,47 млн долларов США. Учитывая, что общий бюджет, выделяемый компаниями на информационные технологии в 2020 году, составляет в среднем 54,80 млн долларов, найти в нем дополнительные 5% может оказаться непросто.

ВОПРОС

Средний бюджет (в млн долл. США), который организациям необходимо потратить в ближайшие 12 месяцев на устранение технологических разрывов. В опросе принимали участие компании, в которых ускоренная цифровая трансформация привела к отставанию в технологической сфере. Результаты сгруппированы по странам, число участников указано [в скобках].



В дополнение к этим практическим соображениям, касающимся длительности процесса и объема расходов, есть еще один немаловажный фактор — людские ресурсы. До пандемии мы хорошо представляли себе, насколько технические навыки IT-персонала отстают от реальных потребностей. Поэтому, когда произошла всемирная катастрофа, мы понимали, что IT-команды работают под постоянным давлением, и были готовы многое простить им.

Однако по большей части IT-департаменты выдержали удар и, как минимум, смогли обеспечить работоспособность своих систем. Однако сейчас очевидно, что выиграна только половина сражения. Вместо того чтобы заслуженно взять тайм-аут и перевести дух, люди вынуждены с удвоенной энергией заниматься устранением уязвимостей в технологических экосистемах своих компаний.

Это означает, что проблема нехватки навыков никуда не исчезла, а менеджменту становится очевидно, что для решения проблем с технологическим разрывом необходимо действовать очень быстро. По подсчетам самих организаций, им придется не только потратить дополнительные 2,47 млн долларов на ликвидацию уязвимостей, но и нанять в штат в среднем 27 новых IT-специалистов.

«Организациям придется не только потратить дополнительные 2,47 млн долларов на ликвидацию уязвимостей, но и нанять в штат в среднем 27 новых IT-специалистов».

Принимая во внимание кадровый голод, возникший еще до начала пандемии, это выглядит не слишком реалистично. Таким образом, не составляет труда понять, почему устранение технологических разрывов займет в компаниях около двух лет.

Несомненно одно: все усилия и инвестиции не пропадут даром, если они помогут предотвратить атаки вирусов-шифровальщиков и подобные им угрозы или хотя бы ограничить их последствия.

В чем причина технологического разрыва?

В условиях пандемии вопросы безопасности стали играть еще более значительную роль. Пока организации «тушат пожары» в других областях бизнеса, киберпреступники принялись атаковать с удвоенной энергией. И, в свете недавних кибератак на критическую инфраструктуру и цепочки поставок, мы не можем сказать, что в ближайшем будущем хакеры планируют отступить.

Тем не менее, только шесть из десяти опрошенных организаций (61%) считают, что технологическое отставание в вопросах безопасности, вызванное ускоренной цифровой трансформацией за последние полтора года, полностью устранено, а 39% уверены в обратном.

Модернизация системы безопасности без сомнения является серьезным вызовом для организаций, однако им неизбежно придется принять его, чтобы защитить свои ресурсы от киберпреступников.

Без сомнений, одной из основных причин технологического отставания в сфере безопасности является быстрое и внезапное внедрение новых технологий в качестве реакции компаний на пандемию. Основным полем для инноваций стали облачные технологии: 80% компаний признали, что им пришлось существенно скорректировать или расширить первоначальные планы развития облачной инфраструктуры после начала пандемии.

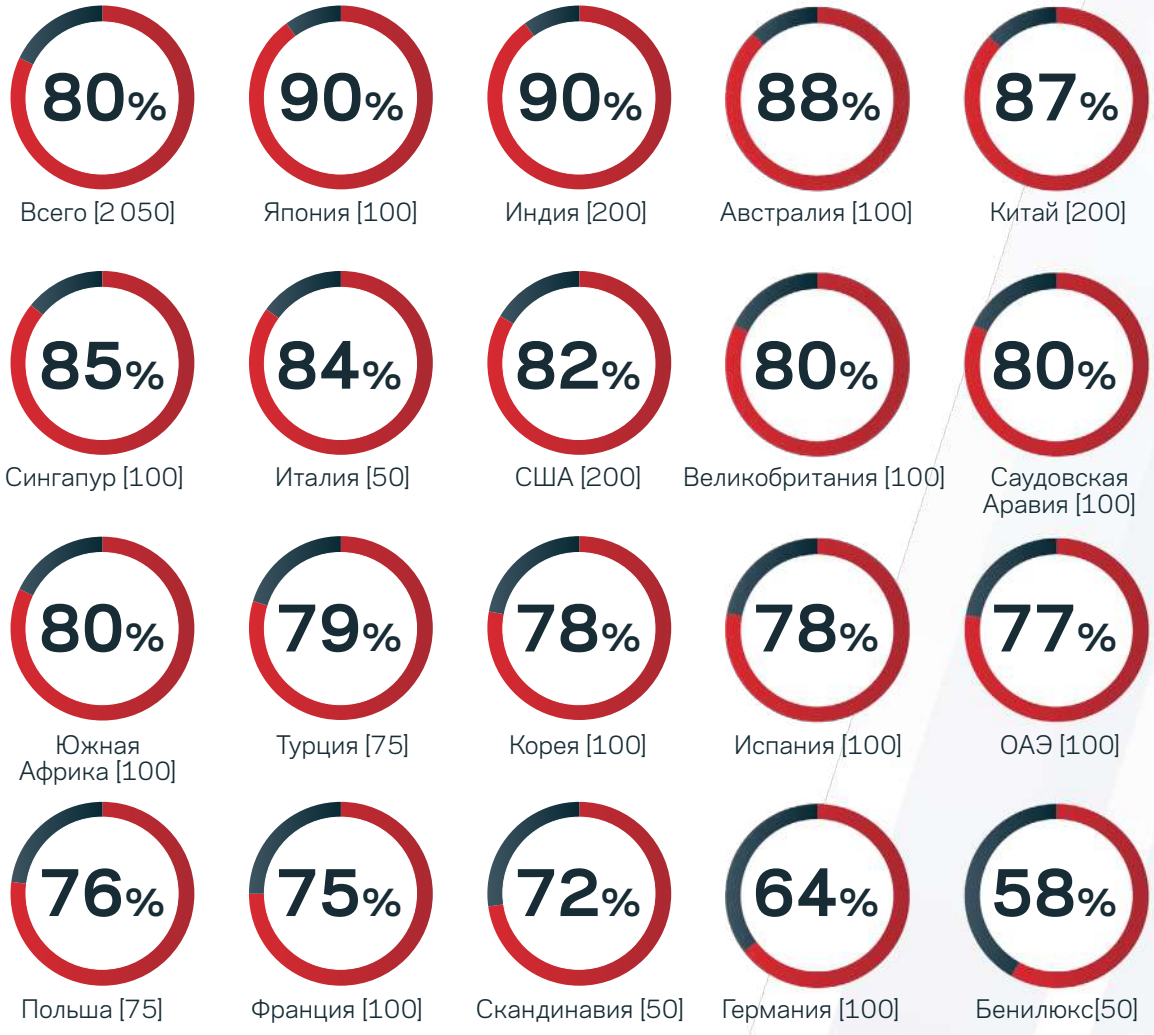
Преимущества облачных технологий хорошо известны. И сегодня эти преимущества — в особенности те из них, что касаются гибкости и совместной работы — многократно усилены пандемией.

Тем не менее, внедрение новых технологий в таких объемах и такими темпами практически неминуемо сопровождается трудностями. В данном случае основной проблемой стала недостаточная прозрачность инфраструктуры.

Только 58% лиц, принимающих решения, могут назвать точное количество облачных сервисов, которые, как они считают, используются в их организациях. Этот факт как ничто другое иллюстрирует масштаб проблемы, с которой приходится иметь дело, чтобы обеспечить эффективное управление облачной инфраструктурой и ее безопасность. В конце концов, ответственность за защиту того, что мы даже не видим, ложится на IT-директоров. Именно они должны решить проблему, пока она не привела к серьезным последствиям.

ВОПРОС

Процент респондентов, которым пришлось существенно скорректировать или расширить первоначальные планы развития облачной инфраструктуры после начала пандемии. Результаты сгруппированы по странам, число участников указано [в скобках].



К сожалению, отсутствием прозрачности дело не ограничивается. Следует также учесть объемы данных, накопленных организациями, а они поистине огромны. Не слишком помогает даже тот факт, что средний бюджет, выделенный на инициативы по снижению рисков, например обеспечение безопасности, защиту данных и отказоустойчивость, увеличился в 2020 году на 6,72% (по сравнению с предшествующим годом).

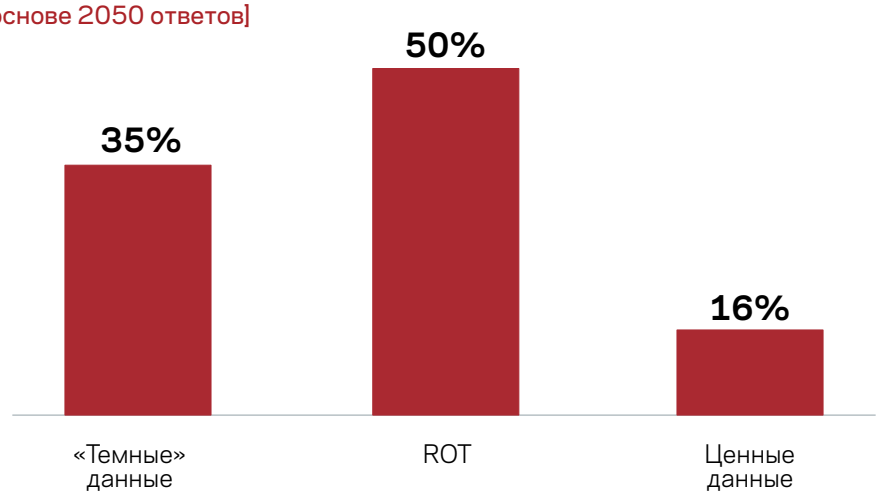
Фактически IT-менеджеры не имеют представления о более чем трети данных в их компаниях. В среднем только 65% данных в организациях каким-либо образом классифицированы или помечены. Оставшиеся 35% — это «темные данные», о которых IT ничего не знают. В частности им неизвестна реальная ценность таких данных, и существует ли она вообще.

50%

данных являются избыточными, устаревшими или незначительными (ROT), и только 16% содержат ценную для бизнеса информацию

ВОПРОС

Средний процент темных, избыточных, устаревших, незначительных (ROT) и ценных для бизнеса данных в организациях [на основе 2050 ответов]



Следующие несколько месяцев станут периодом консолидации. Организации были вынуждены реагировать на беспрецедентные глобальные события, и для многих из них такой реакцией стало быстрое внедрение новых технологий. Однако темпы внедрения этих технологий сделали организации уязвимыми. Компании недостаточно хорошо знают особенности внедренных технологий — особенно это касается облачных сервисов — и недостаточно четко понимают, что именно следует защищать, а также кто конкретно должен этим заниматься.

Результатом является существенное отставание в сфере безопасности, которое необходимо ликвидировать как можно скорее. Атаки шифровальщиков и другие угрозы представляют серьезную и актуальную проблему для организаций, поскольку киберпреступники не упускают ни малейшей возможности воспользоваться ситуацией.

Всего одна успешная атака способна свести на нет все усилия, предпринятые IT-специалистами за последние полтора года, поэтому максимально быстрое и эффективное закрытие уязвимостей критически важно для достижения более масштабных целей по мере того, как последствия пандемии постепенно устраняются.

Насколько уязвимыми стали организации?

За время пандемии компании во всем мире продемонстрировали завидную гибкость и жизнеспособность. Разумеется, не обошлось и без сложностей. Вне зависимости от того, вызваны ли они внутренними или внешними факторами, если результатом является незапланированное прерывание работы, ущерб может быть огромным.

Сбои в работе могут возникать по множеству причин, в числе которых атаки шифровальщиков, природные бедствия и человеческий фактор. Предотвратить все инциденты, которые могли бы послужить причиной сбоя, невозможно. Но это также означает, что мы должны уделить особое внимание быстрому, эффективному и безопасному восстановлению работоспособности в случае, если инцидент все же произошел.

Исследования показывают, что за последний год большинство организаций уже получили определенный опыт возвращения к нормальной работе после инцидентов. За этот период почти девять из десяти опрошенных (88%) сталкивались с незапланированными сбоями IT-систем.

Больше всего в этой ситуации беспокоит тот факт, что основной причиной этих сбоев были вирусы-шифровальщики. Согласно результатам опроса, компании в среднем испытали 2,57 атаки шифровальщиков за последний год, а для 14% такие атаки становились причиной временного прекращения работы пять и более раз.

Это наглядно демонстрирует, насколько распространенным и агрессивным является данный вектор атаки, и насколько важно как можно скорее ликвидировать технологическое отставание. В среднем организации с хотя бы одной стратегической проблемой в сфере безопасности подвергались атакам шифровальщиков и были вынуждены приостанавливать работу в пять раз чаще, чем организации без таких проблем. Это достаточно серьезная мотивация, чтобы приложить не меньше усилий для решения стратегических проблем, чем уже прикладывается для восстановления данных.

Обнадеживает, что компании, похоже, достаточно хорошо осознают шаткость ситуации, в которой они оказались. Почти две трети компаний (64%) стали уделять больше внимания обновлению и модернизации программного обеспечения из соображений безопасности, связанных с COVID-19.

Однако для множества компаний это лишь начало пути, и очевидно, что им нужно действовать быстро, чтобы решить проблемы с безопасностью до того, как очередной инцидент приведет к непоправимым последствиям.

Чем больше технологический разрыв, тем выше вероятность того, что серьезный инцидент, например успешная атака шифровальщиков, послужит причиной не только нарушения работы, но и других негативных последствий.

Сейчас организации уязвимы, но пришло время воспользоваться наработками в области аварийного восстановления и отказоустойчивости, полученными за время пандемии, чтобы решить проблему стратегически.

«Почти две трети компаний (64%) стали уделять больше внимания обновлению и модернизации программного обеспечения из соображений безопасности, связанных с COVID-19».

ВОПРОС

Процент респондентов, которые стали уделять больше внимания обновлению и модернизации программного обеспечения из соображений безопасности, связанных с COVID-19. Результаты сгруппированы по странам, число участников указано [в скобках].

Выводы

Пользуясь пандемией, киберпреступники хватаются за любую возможность, чтобы извлечь выгоду из затруднительной ситуации, в которой оказались компании. Они продолжают совершать атаки, а компании вынуждены восстанавливать данные.

IT-департаментам следует удвоить свои усилия по сокращению технологического отставания в сфере безопасности. Неспособность сделать это существенно повышает риск серьезных негативных последствий.

Тем не менее, некоторые шаги в этом направлении уже предпринимаются: согласно отчету Veritas Ransomware Resiliency Report за 2020 год, 64% компаний были уверены, что отстают в вопросах безопасности от общего развития IT.

Данный отчет показывает, что в 2021 году ситуация улучшилась: на данный момент 39% организаций уверены, что ускоренная цифровая трансформация, произошедшая в последние 18 месяцев, создала технологический разрыв в сфере безопасности. И хотя это означает, что всего 61% организаций — по их собственному мнению — полностью справились с последствиями незапланированных инициатив, ситуация развивается в правильном направлении.

К сожалению, фронт работ еще очень велик. Согласно ответам руководителей в сфере IT, для полного устранения уязвимостей может потребоваться еще около двух лет. Ускорение этого процесса возможно при условии дополнительных инвестиций в размере почти 2,5 млн долларов США и найма 27 новых сотрудников в штат IT в течение следующего года.

Очевидно, это будет нелегкая битва, однако учитывая проблемы с прозрачностью, возникшие в результате ускоренного внедрения облачных технологий, и трудности с эффективным управлением данными, это вполне ожидаемо.

Для компаний, не располагающих дополнительными финансовыми и кадровыми ресурсами, хорошим первым шагом станет внедрение эффективных технологий управления данными, которые, посредством автоматизации, улучшат ситуацию с прозрачностью и безопасностью. Такие технологии не только покажут, в какой плоскости лежат имеющиеся проблемы, но и позволят решить их, не полагаясь на волшебное расширение штата.

Решение этих проблем является критически важной задачей, особенно в свете борьбы с шифровальщиками. Компании, которые не будут действовать максимально быстро, без сомнений пополнят обширный список пострадавших от этого популярного вектора атаки.

Технологические разрывы, вызванные пандемией, обязательно должны быть устранены, поскольку несут в себе неприемлемо высокие риски в эпоху экономической нестабильности.

По мере того как организации пытаются в полной мере осознать последствия ускоренной цифровой трансформации, становится ясно, что практики управления данными отстают от общих темпов развития. Учитывая постоянный рост угроз, связанных с шифровальщиками, и классические опасения, касающиеся потенциальной утечки данных, адаптация к «новой нормальности» потребует повышенного внимания в областях, связанных с высоким риском. Мы в компании Veritas хорошо знакомы с этими проблемами и готовы помочь нашим клиентам решить их. Платформа Enterprise Data Services обладает интегрированным набором функций, обеспечивающим непревзойденное качество управления данными и высочайший уровень контроля, необходимый IT-департаментам и специалистам в области нормативно-правового соответствия в любой отрасли и любой стране.

Узнайте больше на veritas.com.

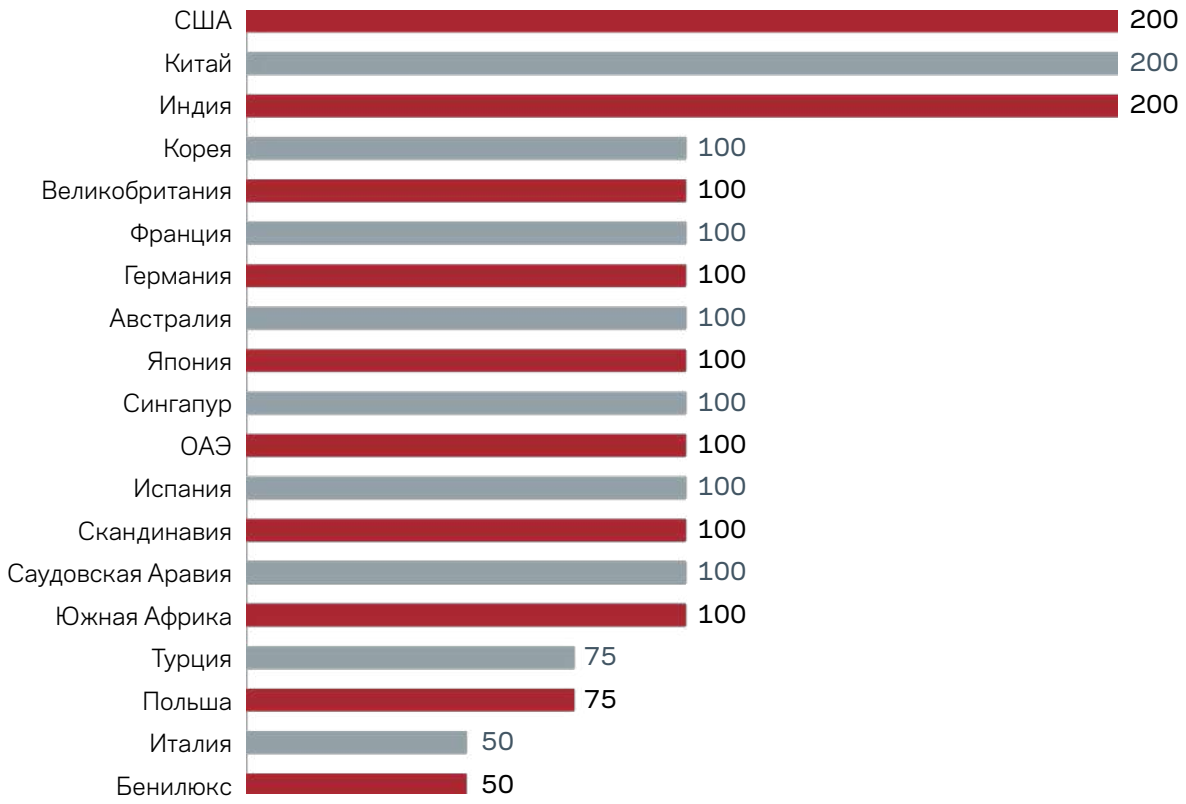
Объем и методология исследования

Этот документ основан на результатах количественного исследования, проведенного независимой исследовательской организацией Vanson Bourne по заказу Veritas Technologies. В опросе, который проходил с июля по август 2021 года в США, странах Европы, Ближнего Востока, Африки и Азиатско-Тихоокеанского региона, приняли участие 2050 лиц, принимающих решения в сфере IT. В опросе приняли участие респонденты из частных и общественных организаций с годовой выручкой не менее 100 млн долларов США. Во всех организациях за предыдущие 18 месяцев произошел запуск каких-либо инициатив по цифровой трансформации, вызванных пандемией COVID-19. К числу таких инициатив относятся внедрение новых инструментов, изменение инфраструктуры, переход к более интенсивному использованию или внедрение новых облачных технологий либо корректировка всей цифровой стратегии организации.

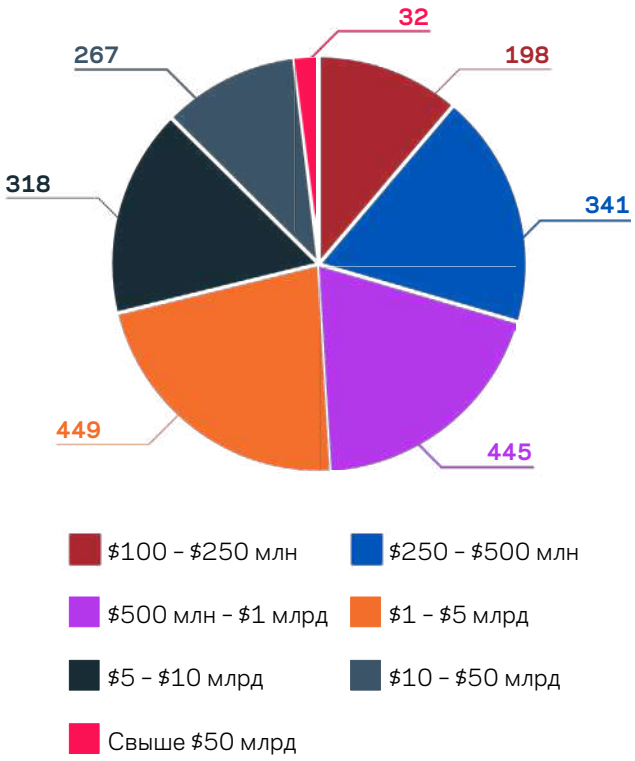
Опрос проводился онлайн после многоуровневого скрининга, позволяющего гарантировать отсев неподходящих кандидатов.

Если не указано иное, результаты основываются на общей выборке, которая включает в себя участников со следующим распределением по странам, годовой выручке и секторам экономики:

СТРАНЫ



ОБЪЕМ ВЫРУЧКИ



ОТРАСЛИ

О компании Veritas

Veritas Technologies является мировым лидером на рынке корпоративных средств резервного копирования и восстановления. Более 80 тысяч заказчиков — включая 87 процентов компаний из списка Fortune 500 — пользуются нашими решениями, чтобы снизить сложность ИТ-инфраструктуры и упростить управление данными. Платформа Veritas Enterprise Data Services Platform автоматизирует защиту данных на предприятиях, обеспечивает круглосуточную доступность критически важных приложений и помогает организациям соблюдать нормативные требования. Она имеет репутацию подходящей под любые требования и исключительно надежной в любых масштабах, поддерживает более 800 источников данных, более 100 операционных систем, более 1400 систем хранения и более 60 облачных платформ.

Узнайте больше на www.veritas.com.

Подпишитесь на нас в Twitter: @veritastechllc.

О компании Vanson Bourne

Vanson Bourne — независимая исследовательская организация, специализирующаяся на технологическом секторе. Исследования компании пользуются заслуженной репутацией надежных и заслуживающих доверия благодаря строгим исследовательским принципам и способности узнавать мнение технических и коммерческих руководителей высшего звена во всех отраслях экономики и на всех основных рынках.

Более подробную информацию можно найти на сайте www.vansonbourne.com.