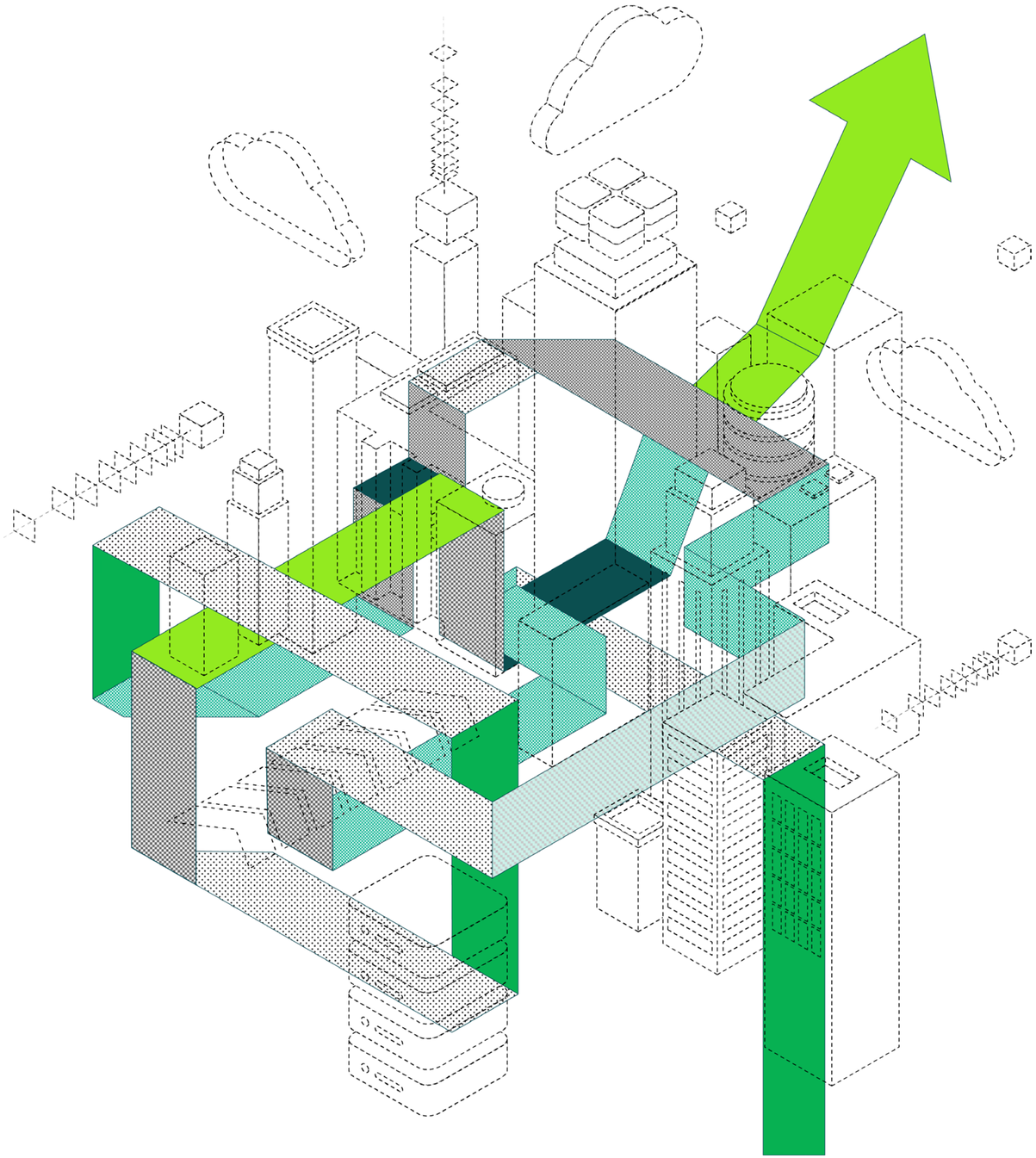
2020

Тенденции в области защиты данных



VEEAM

Почему важно управлять данными в облаке

В **январе 2020 года** независимая исследовательская компания подвела итоги опроса **1550** крупных компаний из 18 стран, **каждая из которых включает в себя более 1000 пользователей**. Задачей исследования было выяснить проблемы и цели компаний в области зашиты данных, независимо от поставщиков средств зашиты, услугами которых они пользуются или планируют пользоваться. Исследование проведено по заказу компании Veeam под руководством двух специалистов по зашите данных, чей совместный опыт в этой отрасли насчитывает более 60 лет. В этом отчете представлены результаты и выводы исследования с комментариями Veeam.

Дэйв Рассел

Вице-президент Veeam по корпоративной стратегии (VP of Enterprise Strategy), бывший вице-президент (VP) направления «Магический квадрант решений для резервного копирования» компании Gartner, заслуженный аналитик (Distinguished Analyst) и ведущий автор статей по этой тематике.

@BackupDave

Джейсон Баффингтон

Вице-президент Veeam по стратегии развития решений (VP of Solutions Strategy), бывший главный аналитик (Principal Analyst) в области защиты данных в Enterprise Strategy Group (ESG).

@JBuff

Оглавление

1.1

Цифровая трансформация и модернизация ИТ-инфраструктуры

Технологии непрерывно развиваются, изменяя и трансформируя принципы ведения бизнеса. В связи с цифровой трансформацией компаниям необходимо постоянно следить за новинками в ИТ-отрасли и уточнять свои цели, стратегию использования решений и способы устранения проблем.

Этот отчет составлен по результатам недавнего опроса более **1550** независимых крупных компаний во всем мире. Целью опроса было выяснить, как современные компании защищают данные и управляют ими и как они планируют справляться со сложными ИТ-задачами, включая растущие потребности и сбои в обслуживании, и достигать более амбициозных целей в сфере модернизации ИТ и цифровой трансформации.

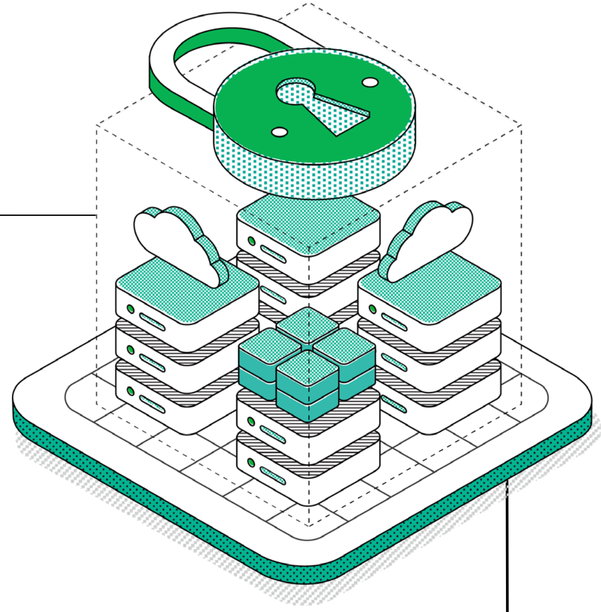
Многие организации уже используют гибридные среды, включающие в себя физические серверы **(38%)**, виртуальные машины **(30%)** и облачные ВМ **(32%)**, и в ближайшие 2 года доля локальных инфраструктурных систем, перемещенных на облачные платформы (например, AWS и Azure), увеличится примерно на **10%**. Такой быстрый переход говорит о том, что цифровая трансформация побуждает компании делать выбор в пользу облачных технологий.

Проблемы, стоящие перед компаниями, остаются неизменными: это в первую очередь доступность данных и облачных платформ, удовлетворенность клиентов и репутация брендов. Однако исследование показывает, что модернизация систем защиты данных с использованием простых и гибких решений позволяет значительно повысить уровень безопасности и удобства использования данных, а также высвободить ресурсы и сосредоточиться на модернизации ИТ-инфраструктуры и управлении.

При чтении отчета рекомендуем вам сфокусироваться на собственных ИТ-задачах и проблемах, чтобы оценить, насколько ситуация в вашей организации соотносится с положением дел в **1550** компаниях, принявших участие в опросе по поводу современных подходов к защите данных.

2.0 Важность защиты данных для бизнеса

Большинство компаний не может представить свою работу без цифровых данных. Неудивительно, что ИТ-отделы уделяют много внимания защите информации, причем не только резервному копированию и восстановлению, но и внедрению новых возможностей. Тем не менее многие компании до сих пор используют устаревшие системы защиты данных, не вполне понимая, как это влияет на развитие бизнеса.



В среднем простой длится **117 минут**

2.1

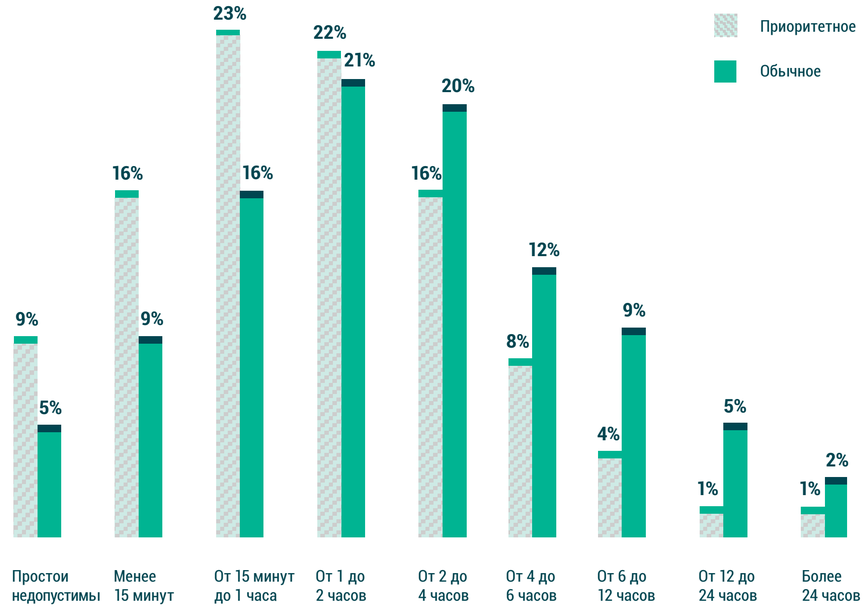
Критически важное значение данных

В случае сбоя требуется время для восстановления доступа к данным, а время, как известно, деньги. Исследование показало, что **95%** организаций сталкиваются с непредвиденными простоями, при этом как минимум **10%** их серверов выходит из строя по крайней мере раз в год. Поскольку в среднем сбой длится около 2 часов, а средняя продолжительность наиболее длительных вынужденных простоев составляет более 4 часов, некоторые организации воспринимают их как норму.

Учитывая эти показатели, можно посчитать экономические последствия вынужденных простоев. Отсутствие доступа к «критически важному» приложению в течение часа может обойтись в **67 651 долл. США**. Недоступность «обычного» приложения в течение часа может стоить бизнесу **61 642 долл. США**. С учетом того, что, по оценкам компаний, 51% данных имеют высокий приоритет, а 49% — стандартный, можно подсчитать, что в среднем один час простоя обходится в **64 647 долл. США**. Такое соотношение долей обычных и высокоприоритетных данных и финансовых потерь от сбоев показывает, что «все данные важны», а вынужденные простоив современных средах в принципе недопустимы.

Согласно этой статистике компании вынуждены работать с простоями, которые длятся слишком долго и обходятся слишком дорого. Они нуждаются в современном подходе, который позволит создавать больше точек восстановления и сократить простои. Исходя из того, что стоимость часа простоя одного приложения может составлять больше **67 000 долл. США**, любой сбой негативно сказывается на финансовых и репутационных показателях компании.

Какое время простоя считается в вашей компании приемлемым для приоритетных и обычных приложений?



2.1

Критически важное значение данных

Комментарий Veeam о том, почему управление данными в облаке необходимо. Современные решения для защиты данных должны обеспечивать частое и интеллектуальное резервное копирование. Компания Veeam провела собственный опрос **500** зарегистрированных клиентов с таким же демографическим и географическим распределением, что и у **1550** независимых участников международного исследования. Клиенты Veeam заявили, что с помощью решений компании им удалось снизить время восстановления критически важных приложений на **86%**. Они также отметили, что общие ежегодные расходы на защиту данных в среднем сократились на **49%** по сравнению с показателями международного исследования.

Потеря доверия заказчиков – **самое серьезное** последствие простоев

2.2

Влияние вынужденных простоев: нефинансовая сторона

Поскольку отсутствие доступа к данным негативно сказывается на бизнес-процессах, простои выражаются для компаний в различных видах финансовых убытков. Помимо этого, у простоев и потерь данных есть и нефинансовые последствия.

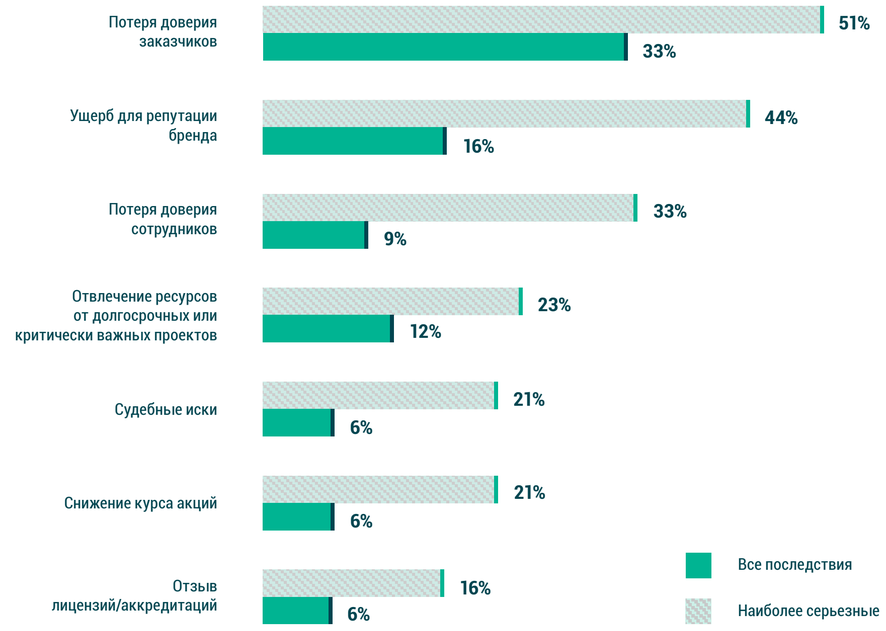
Самое распространенное и важное — утрата доверия клиентов. Аварийные сбои снижают уровень обслуживания, поэтому, по мнению респондентов, в **51%** простои отрицательно сказались на взаимоотношениях с клиентами. На второе место по значимости опрошенные поставили ущерб для целостности бренда, который стал результатом **44%** сбоев.

Негативное отношение клиента, вызванное непредвиденными обстоятельствами, не всегда кажется оправданным, но, с точки зрения клиента, подобный опыт — это повод задуматься о том, стоит ли пользоваться услугами этой компании в дальнейшем. К тому же простои затрагивают не только клиентов, но и сотрудников.

На третье место участники поставили утрату доверия к компании со стороны сотрудников, к которой приводят **33%** простоев. Не только у клиентов, но и у сотрудников есть требования к бизнесу. Они хотят, чтобы организации, в которых они работают, приносили прибыль, поддерживали устойчивое развитие и предоставляли карьерные возможности. Если ИТ-инфраструктура постоянно дает сбои, то и сотрудники не могут качественно выполнять свою работу и в конечном итоге переходят в другие компании.

Помимо этого, простои отвлекают ресурсы от других долгосрочных и важных проектов **(23%)**, становятся причиной судебных исков **(21%)**, приводят к снижению курса акций **(21%)** и отзыву лицензий **(16%)**.

Какие последствия может иметь для вашей организации вынужденный простой приложений? Какие последствия вы считаете наиболее серьезными?



2.2

Влияние вынужденных простоев: нефинансовая сторона

Комментарий Veeam о том, почему управление данными в облаке необходимо. Неавтоматизированная защита данных отнимает много времени, приводит к более длительным простоям и снижает эффективность работы ИТ-отдела. Комплексное ПО для резервного копирования, например Veeam Availability Suite, может повысить общую эффективность ИТ-отдела на **30%** и сократить снижение производительности сотрудников из-за потерь данных на **82%**[1]. Это повышает гарантию непрерывности бизнеса в целом на **78%**[2].

2.3

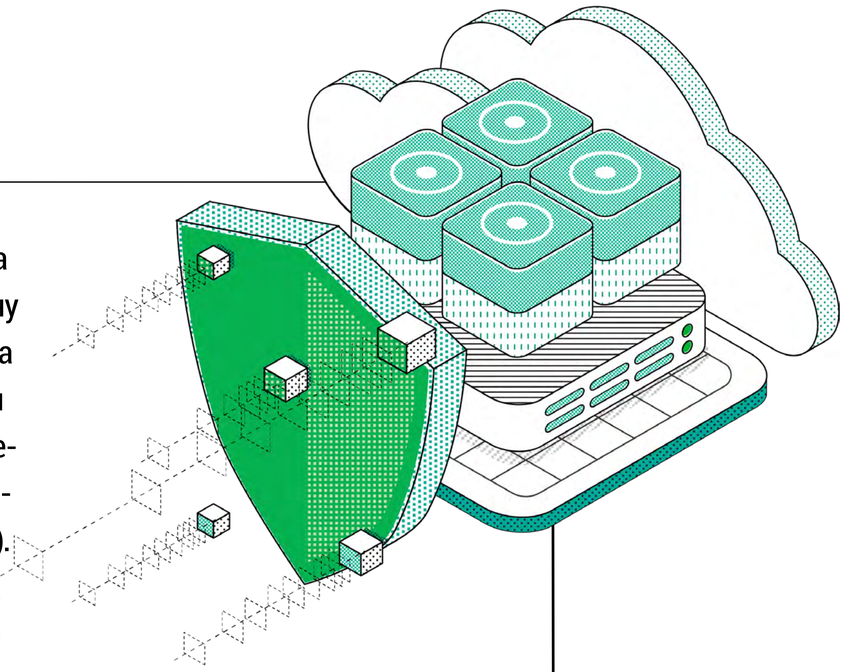
Выводы

Данные крайне важны для бизнеса. Факт очевидный, но бесспорный. Еще одно бесспорное утверждение: данные компаний находятся под угрозой. Почти каждая компания сталкивается с простоями из-за проблем, возникающих в работе **каждой десятой виртуальной машины**. Подобные сбои длятся несколько часов и приводят к потере сотен тысяч долларов. При этом финансовые потери — только видимая часть айсберга: потери и уязвимости данных негативно влияют на репутацию брендов и взаимоотношения с клиентами и сотрудниками, что в свою очередь приводит к упущенным сделкам.

Очень важно, чтобы безопасность данных была приоритетом компании. Проводить цифровую трансформацию следует прежде всего с целью модернизации системы защиты данных. Лучшие передовые технологии помогут обеспечить доступность и безопасность данных и выполнять их восстановление при первой необходимости. Устаревшие системы — это риск для бизнеса, который обходится очень дорого. Влияние на бизнес любых простоев, возникших из-за человеческого фактора, природных катаклизмов или кибератак, можно снизить с помощью надежной системы защиты данных.

3.0 Изменение ситуации в сфере защиты данных

В современном мире, когда многие организации требуют от ИТ-отдела не просто поддержания операционной деятельности, а движения в сторону цифровой трансформации и модернизации ИТ-инфраструктуры, защита данных стала одним из основных приоритетов. Данные и приложения больше не привязаны к одному серверу. Теперь они распределяются по нескольким центрам обработки и облачным сервисам через файлообменные системы, общие хранилища и даже SaaS-платформы (ПО как услуга). Устаревшие инструменты резервного копирования локальных хранилищ файлов и приложений не справляются с задачами в гибридной и мультиоблачной среде, требуют временных затрат и денежных вложений и подвергают данные риску.



3.1

Проблемы, связанные с цифровой трансформацией

Участники опроса признают роль цифровой трансформации в ускорении развития их бизнеса. Модернизация бизнес-процессов и операций позволяет добиться значительного повышения качества обслуживания, сократить расходы и разгрузить сотрудников. Более **80%** организаций планируют или уже проводят цифровую трансформацию, однако многие из них сталкиваются с проблемами на пути к желаемым результатам.

В основном их беспокоит недостаток квалифицированных ИТ-специалистов **(44%)** и зависимость от старых систем **(40%)**. Эти препятствия также приводят к значительному дефициту времени и средств. Другими словами, устаревшие платформы и выполняемые вручную процессы серьезно замедляют модернизацию.

Что мешает (помешало) вашей компании реализовать проекты цифровой трансформации?

Устаревшие системы затрудняют цифровую трансформацию

3.1

Проблемы, связанные с цифровой трансформацией

Комментарий Veeam о том, почему управление данными в облаке необходимо. Многие компании считают облачные вычисления основной движущей силой цифровой трансформации, а **78%** респондентов утверждают, что именно цифровая трансформация является основной причиной внедрения облачной инфраструктуры и сервисов. Но отсутствие времени, ресурсов и средств может стать серьезным препятствием на пути реализации этой стратегии. Модернизация системы защиты данных на основе решений Veeam протекает на **30%** более эффективно, а потери времени в ходе резервного копирования и восстановления снижаются на **82%**[1]. Это позволяет направить временные и финансовые ресурсы и специалистов на то, что действительно важно, — на трансформацию ИТ-инфраструктуры.

3.2

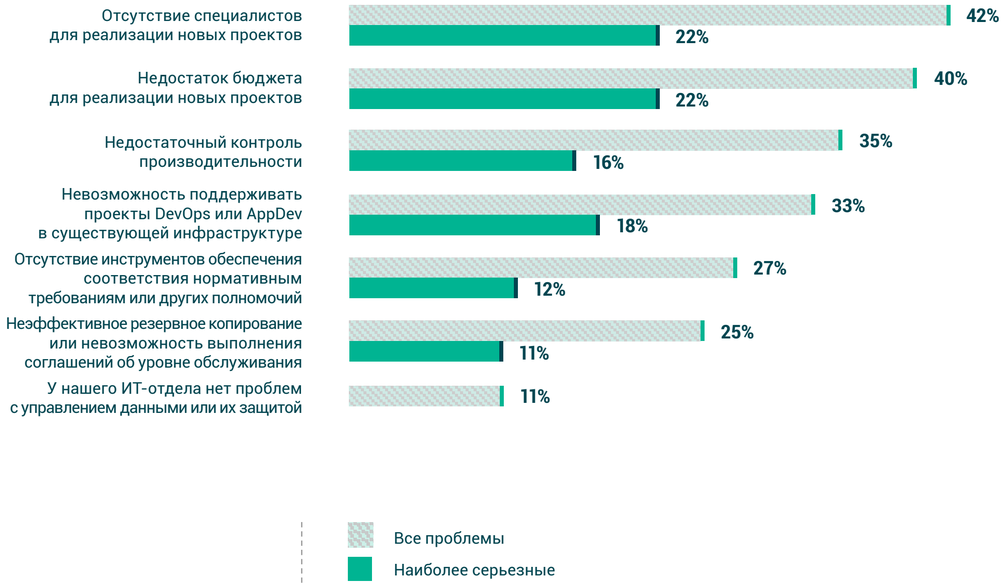
Проблемы, связанные с защитой данных

8 из **9** компаний заявляют, что у них возникают сложности с управлением данными и их защитой, в первую очередь из-за недостатка ресурсов. Основная проблема — нехватка квалифицированных кадров, способных реализовать новые проекты **(42%)**. На втором месте — недостаток средств **(40%)**. Подобные заявления говорят о том, что компании стремятся улучшить управление и защиту данных. Они хотят задействовать больше специалистов и нуждаются в дополнительных средствах на внедрение новых возможностей.

Далее в порядке убывания называются различные технические задачи, в том числе мониторинг операционных показателей, поддержка DevOps (сред разработки и эксплуатации) или AppDev (систем разработки приложений), обеспечение соответствия нормативным требованиям и неэффективность резервного копирования. Недостаток времени, средств и специалистов зачастую не позволяет выполнять некоторые важные для бизнеса задачи, например разработку приложений, управление и обеспечение безопасности.

Более чем в **40%** организаций нет сотрудников, которые могли бы реализовывать новые проекты по защите данных

С какими из следующих трудностей в области управления данными или их защиты сталкивается ИТ-отдел вашей компании? Какие из них более всего влияют на вашу работу?



3.2

Проблемы, связанные с защитой данных

Комментарий Veeam о том, почему управление данными в облаке необходимо. Программное обеспечение должно быть простым, гибким и надежным. Если для добавления нового устройства NAS (сетевого хранилища) или облачного хранилища необходимо изменить процедуру защиты данных и потратить время на переобучение ИТ-специалистов, это означает, что вы выбрали неверный подход. Управление данными в облаке с помощью Veeam позволяет высвободить ресурсы и бюджет для инновационного развития и повысить эффективность работы специалистов по резервному копированию и восстановлению данных более чем на **55%**[1].

Главная угроза для современного бизнеса – программы-вымогатели.

3.3

Проблемы в 2020 году

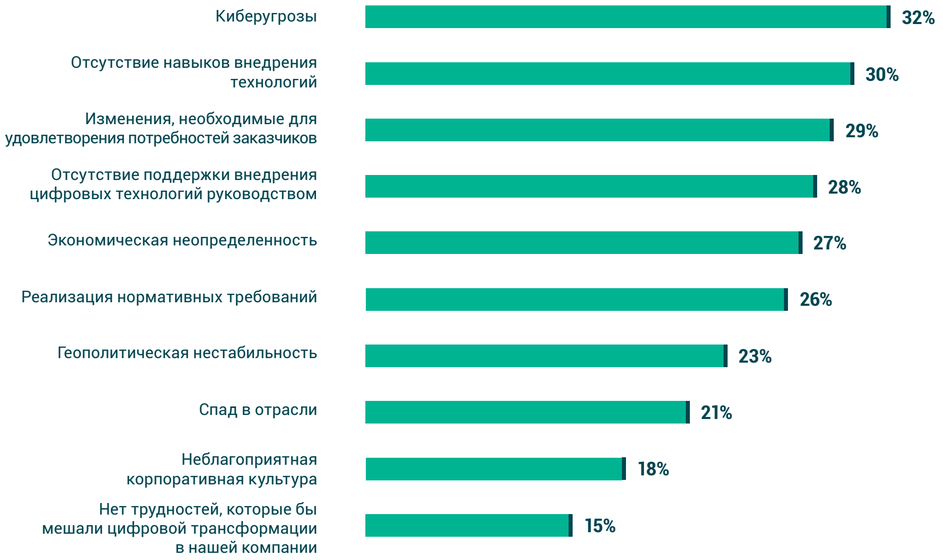
Чего ожидают компании в 2020 году? Точнее говоря, какие изменения, по их мнению, произойдут в ИТ-сфере и как реализовать цифровую трансформацию, чтобы решить связанные с ними задачи?

Крупные компании считают, что самой распространенной проблемой 2020 года станут киберугрозы **(32%)**, в том числе программы-вымогатели, шпионское и вредоносное ПО. Развитие технологий может пойти несколькими путями. Чем больше технологический прогресс упрощает работу пользователей, тем изощреннее становятся инструменты злоумышленников. Компании знают об этом и прогнозируют появление в 2020 году кибератак, к противостоянию которым необходимо подготовиться.

Еще один повод для беспокойства — отсутствие навыков внедрения технологий (**30%**). С учетом киберугроз это очень высокий показатель. Опытные специалисты и умение внедрять технологии — ключевые составляющие цифровой трансформации, которые необходимы для защиты от атак злоумышленников. Количество компаний, которых беспокоят проблемы киберугроз и внедрения технологий, примерно одинаково.

Еще одна трудная задача — выполнение меняющихся требований заказчиков **(29%)**. Предсказание потребностей заказчиков напоминает прогнозирование развития технологий: в обеих сферах происходят активные изменения. В 2020 году на первый план выйдут новые потребности, и предприятия должны быть готовы удовлетворить эти потребности в кратчайшие сроки или хотя бы максимально быстро под них подстроиться.

Как вы думаете, с какими из этих трудностей и задач столкнется ваш бизнес в течение следующего года?



3.3

Проблемы в 2020 году

Комментарий Veeam о том, почему управление данными в облаке необходимо. Значительно выросло число компаний, для которых программы-вымогатели стали не мифической угрозой, а перспективой ближайшего будущего. Veeam предлагает понятные и реалистичные стратегии обучения сотрудников, передачи резервных копий между несколькими объектами и использования облачных платформ для максимальной защиты резервных копий. С помощью Veeam Cloud Data Management Platform **95%** компаний сократили выплаты авторам программ-вымогателей в среднем до **5000 долл. США**, а **76%** организаций полностью избежали таких расходов[3].

Аварийное восстановление по модели «как услуга» (DRaaS) помогает быстрее внедрять облачные технологии

3.4

Основные возможности современной системы защиты данных

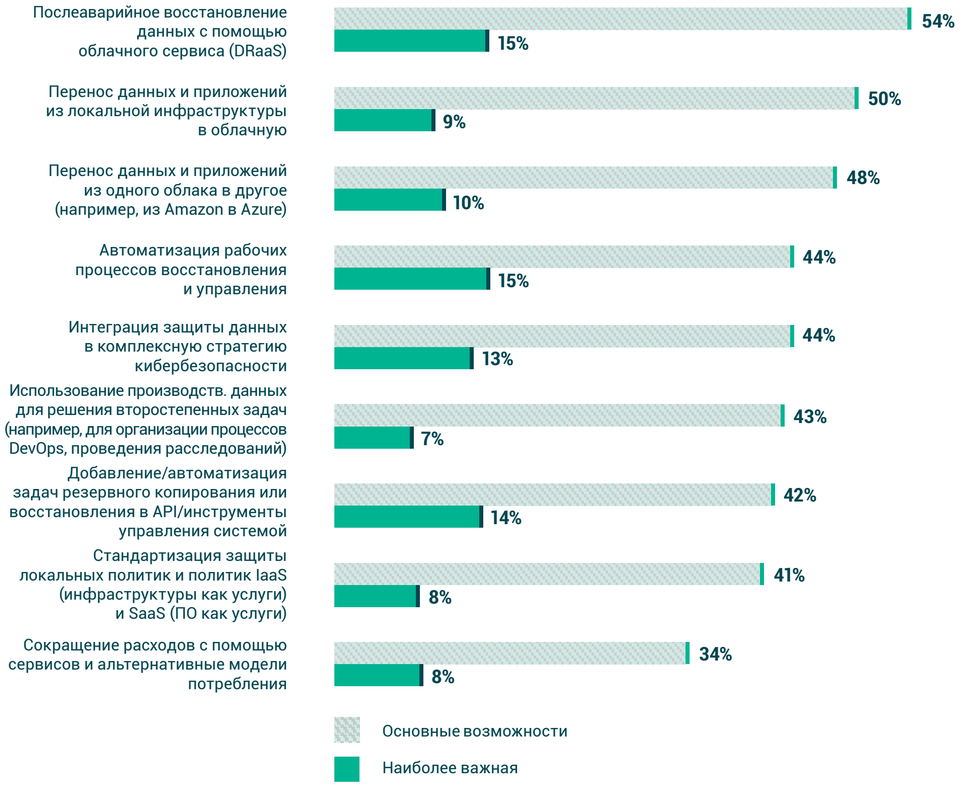
Крупным компаниям известно, что для соответствия новым отраслевым стандартам необходимо продолжать модернизацию ИТ-инфраструктуры и цифровую трансформацию. По данным этого отчета, основные аспекты современной стратегии защиты данных основаны на использовании различных возможностей облачных сервисов.

На первом месте (**54%** опрошенных) стоит послеаварийное восстановление с использованием облачных сервисов, на втором — возможность переноса данных и приложений из локальной инфраструктуры в облачную (50%), замыкает тройку перенос данных и приложений из одной облачной инфраструктуры в другую (**48%**).

Другими словами, половина компаний признают, что облако играет важнейшую роль в современных стратегиях защиты данных и в будущем его значимость будет только расти. Хотя некоторые компании до сих пор используют устаревшие решения, большинство рассматривают в качестве основного пути цифровой трансформации переход на облачные технологии. Тем не менее продвинутые планы защиты данных должны не просто включать использование облака, но быть гибкими и поддерживать локальные инструменты и несколько облачных служб.

Кроме того, современная система защиты данных должна поддерживать автоматизированное восстановление и управление **(44%)**, интеграцию защиты данных в комплексную стратегию кибербезопасности **(44%)** и использование производственных данных для решения второстепенных задач **(43%)**.

Какие из следующих возможностей вы считаете определяющими для «современного», или «инновационного», решения по управлению данными или защите данных, подходящего вашей компании? Какая, на ваш взгляд, является основной?



3.4

Основные возможности современной системы защиты данных

Комментарий Veeam о том, почему управление данными в облаке необходимо. Готова ли ваша компания к переносу данных в облако и внедрению системы управления рабочими процессами? **52%** организаций утверждают, что «перенос приложений или данных в облако» является основным препятствием для реализации ИТ-проектов, что усложняет модернизацию защиты данных. Модели лицензирования — по-прежнему основной фактор, ограничивающий мобильность данных. Такие решения, как Универсальная лицензия Veeam (Veeam Universal License), позволяют выполнять масштабирование на любой платформе без необходимости докупать лицензии или аппаратное обеспечение.

3.5

Современные требования к технологиям защиты данных

В современном мире данные играют определяющую роль во всех аспектах цифрового бизнеса. Вместе с тем вырос спрос на решения, которые предлагают дополнительные возможности, помимо доступности данных. Зашита данных должна выйти на новый уровень интеллектуальности, чтобы прогнозировать и удовлетворять требования клиентов.

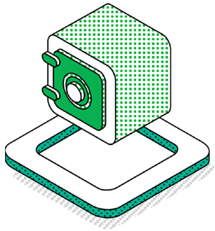
ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ ДОЛЖНЫ БЫТЬ:

ПРОСТЫМИ

Быстрое развертывание и мгновенная окупаемость инвестиций.

ГИБКИМИ

Доступ к данным откуда угодно в любое время.



НАДЕЖНЫМИ

Уверенность в надежной защите, даже с учетом развития инфраструктуры.

3.6

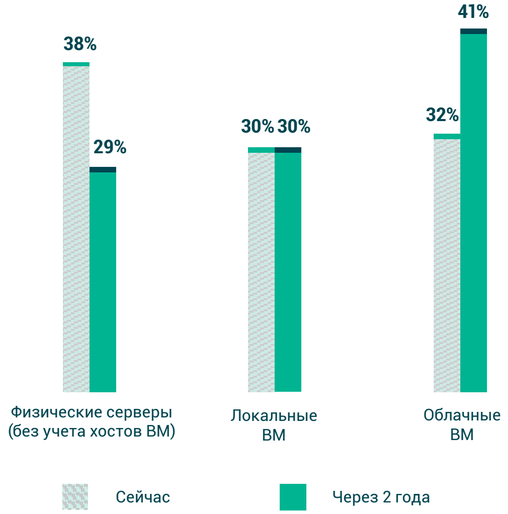
Переход на облачные технологии

Сейчас все больше компаний переносят свои рабочие нагрузки, приложения и данные в облако. Эта тенденция продолжается с начала внедрения виртуализации в середине 2000-х годов. Переходя с физических платформ на виртуальные, компании вышли на новый уровень гибкости и оптимизации операций. Многие организации добились тех же результатов, внедрив облачные сервисы.

По результатам опроса, общее число организаций, планирующих перейти с физических инфраструктур на облачные, составит **9%**. Однако фактически наиболее консервативные компании, скорее всего, перейдут с физических сред на виртуальные, а их более прогрессивные конкуренты — с виртуальных на облачные. Основный вывод исследования заключается в том, что организации в ближайшем будущем планируют использовать гибридные среды, снизить количество физических систем и добавить облачные сервисы. Это усугубит проблемы с защитой данных, так как отказ от устаревших продуктов для резервного копирования и защиты современных платформ и решений подразумевает переход из защищенных центров обработки данных в незащищенные облачные среды.

К 2022 году более **40%** всех серверов будут размещены в облаке

Какой процент серверов вашей компании на сегодняшний день относится к следующим трем категориям? Каким, по вашему мнению, станет это соотношение через два года?



3.6

Переход на облачные технологии

Комментарий Veeam о том, почему управление данными в облаке необходимо. Переход на облачные технологии неизбежен, но вряд ли все компании будут использовать **только** их. Лучше не полагаться полностью на защиту данных только физических или только виртуальных систем и иметь возможность перемещения файлов резервных копий в разные среды. Управление гибридными данными — непростая задача, но клиенты, использующие Veeam Cloud Data Management для защиты данных, добиваются сокращения расходов на **49%**.

К 2022 году использовать облачные услуги в качестве основного способа резервного копирования планируют 77% компаний.

3.7

Доля облачных технологий в современных системах резервного копирования

В любом анализе модернизации ИТ-инфраструктуры необходимо учитывать рост количества внедряемых облачных сервисов. Чтобы понять, какие шаги компании-респонденты планируют для обновления систем защиты данных, им предложили описать существующую среду резервного копирования и предполагаемое состояние среды в 2022 году.

На сегодняшний день организации используют облачные сервисы — хранилища и (или) BaaS (резервное копирование как услугу) — для выполнения примерно половины операций резервного копирования. При этом доля резервного копирования, выполняемого поставщиком услуг BaaS, составляет **24%**, а самостоятельного резервного копирования с использованием облачных сервисов — **25%**. На вопрос о том, каким будет основное решение для резервного копирования в 2022 году, участники исследования ответили, что планируют использовать облачные сервисы, управляемые BaaS, для **43%** резервных копий и выполнять самостоятельное резервное копирование в облако для **34%** данных. Это значит, что к 2022 году организации планируют использовать облачные услуги для более чем ¾ всего объема резервного копирования **(77%)**.

Какой процент производственных данных защищается в вашей компании каждым из следующих способов резервного копирования?

Какой из способов резервного копирования данных станет основным в вашей компании через два года?

3.7

Доля облачных технологий в современных системах резервного копирования

Комментарий Veeam о том, почему управление данными в облаке необходимо. Для большинства компаний переход на облачные технологии откроет доступ к новым сервисам, которые помогут повысить производительность и эффективность, а также ускорить рабочие процессы и сократить расходы. Начав модернизацию инфраструктуры в 2020 году, компании планируют продолжить цифровую трансформацию и увеличить использование облачных технологий до **28%**. Долю самостоятельного резервного копирования с использованием локальных инструментов планируется сократить к 2022 году с **33%** до **18%**.

Расширение возможностей, сокращение расходов и упрощение остаются основными причинами перехода на новые решения для защиты данных

3.8

Причины замены систем резервного копирования в 2020 году: повышение надежности, экономичности и эффективности

Есть такое выражение: «Не надо менять то, что работает». Подобный подход приводит к тому, что компании продолжают использовать устаревшие решения предыдущих поколений. Что может заставить организации заменить основные решения для резервного копирования?

В качестве самой распространенной причины замены существующих решений для резервного копирования **(39%)** называется стремление повысить его надежность. На втором месте — желание улучшить экономические показатели: сократить расходы на программное или аппаратное обеспечение **(38%)**, повысить окупаемость инвестиций и снизить совокупную стоимость владения **(33%)**.

Третья причина — повышение эффективности, включая улучшение показателей RTO и RPO в рамках соглашений об уровне обслуживания **(30%)** и упрощение системы **(30%)**. Помимо этих трех основных трендов, десятку основных причин изменений замыкают использование облачных технологий и поддержка разных форм-факторов и моделей потребления.

Что из нижеперечисленного может стать причиной замены основного решения или сервиса для резервного копирования в вашей компании?

3.8

Причины замены систем резервного копирования в 2020 году: повышение надежности, экономичности и эффективности

Комментарий Veeam о том, почему управление данными в облаке необходимо. В 2020 году компании, стремящиеся обеспечить непрерывную работу бизнеса и сохранить ресурсы, продолжат инвестировать в современные решения для резервного копирования. Это поможет им преодолеть трудности, связанные с цифровой трансформацией, и быстрее воплотить проекты в жизнь. При использовании только решений Veeam вероятность достижения целевых показателей RPO/RTO повышается на **55%**, а количество случаев потери данных сокращается на **33%**. Они также сокращают расходы на резервное копирование и восстановление данных на **50%** по сравнению с аналогичными решениями предыдущих поколений[1].

3.9

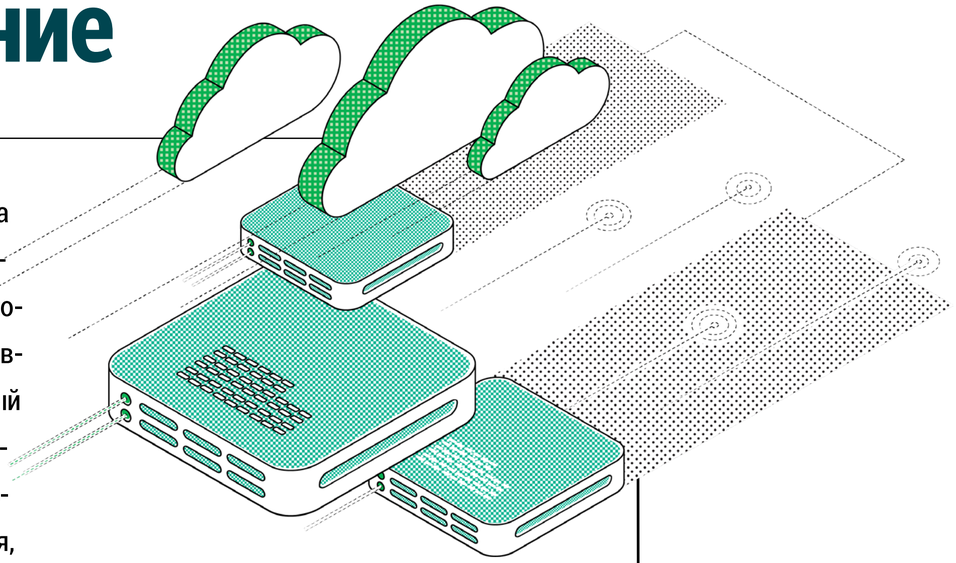
Выводы

Изменения зачастую связаны с определенными проблемами, но бизнес не может не меняться по мере развития ИТ-отрасли. Трудности возникают на любом пути, но в конечном итоге изменения — это всегда путь к прогрессу. По мере адаптации к меняющимся требованиям пользователей компании должны перестраивать ИТ-стратегии для производства и безопасности, получая дополнительные преимущества в ходе этого процесса.

Внедрение единой платформы с поддержкой автоматизации и облачных вычислений помогает компаниям решать текущие задачи и создавать задел на будущее. В современном технократическом мире цифровая трансформация необходима, поскольку компании не могут ограничить изменения системой резервного копирования.

4.0 Управление данными в облаке с помощью Veeam — больше, чем резервное копирование

Руководители компаний осознают важность интеллектуального подхода к бизнесу для достижения успеха. Для этого необходимо создать надежную основу для защиты данных и управления ими. Реализуя эти возможности, руководители бизнеса и ИТ-отделов получают более четкое представление о том, что происходит в организации, и смогут обеспечить быстрый и надежный доступ к данным. Управление данными в облаке не ограничивается резервным копированием. Это следующий шаг цифровой трансформации, способствующий модернизации системы резервного копирования, ускорению внедрения гибридного облака, обеспечению управления данными и их безопасности.

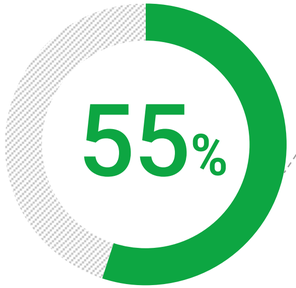


4.1

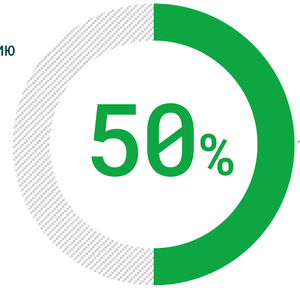
Модернизация резервного копирования

Модернизация резервного копирования позволяет высвободить сотрудников, работающих с устаревшими системами защиты данных, и задействовать их в ключевых инновационных проектах развития бизнеса. Благодаря управлению данными в облаке с помощью Veeam компании могут сократить расходы на резервное копирование и защиту данных на **50%** и повысить эффективность резервного копирования и восстановления данных на **55%**.

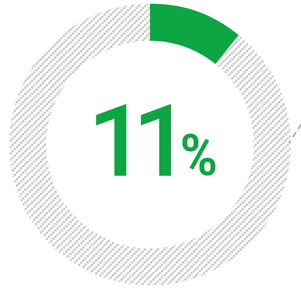
Крупные компании, использующие в качестве основы современную платформу резервного копирования, создают задел для развития своей ИТ-среды и обеспечивают надежную защиту в ходе внедрения облачных и иных типов платформ. Такие организации могут применять интеллектуальную автоматизацию для успешного резервного копирования и восстановления, а также повторно использовать данные для разработки приложений, тестирования приложений, анализа данных и составления отчетов.



более эффективная работа специалистов по резервному копированию и восстановлению[1]



снижение стоимости резервного копирования и защиты данных[1]



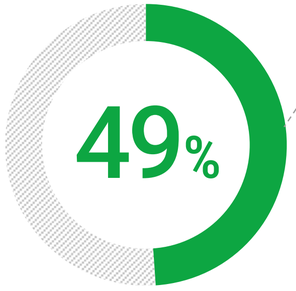
повышение производительности труда разработчиков[1]

4.2

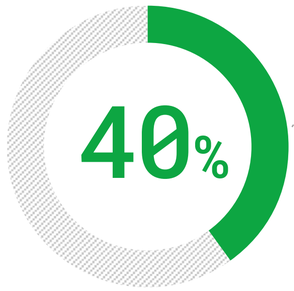
Ускоренное внедрение гибридного облака

Самая сложная задача при переходе на облачные технологии — это перенос данных в облако, так как системы защиты данных и управления основаны на устаревших локальных решениях. Однако проекты ИТ-модернизации и цифровой трансформации ускоряют внедрение облачных сервисов за счет использования комплексных инструментов и обеспечивают сокращение расходов на **49%** благодаря применению гибридных облачных систем защиты. Используя возможности Veeam Cloud Data Management Platform, организации ускоряют обнаружение проблем и принятие мер на **72%**, а также сокращают время планирования и управления ресурсами на **40%**.

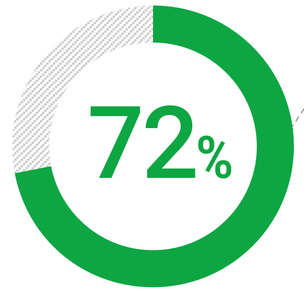
В устаревших системах данные хранятся в соответствующих форматах, а гибридная облачная система делает их мобильными и позволяет передавать из локальной инфраструктуры в облако и из одного облака в другое без ограничений.



снижение расходов на защиту данных в гибридном облаке



сокращение времени на планирование и управление ресурсами[4]



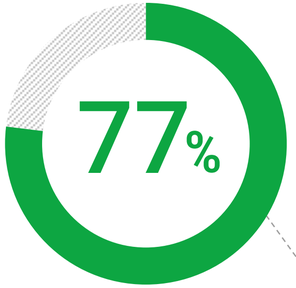
более быстрое выявление и устранение проблем[1]

4.3

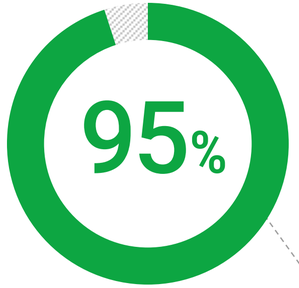
Безопасность данных и управление ими

Количество нормативных требований в области данных и расходы на обеспечение соответствия меняются каждый год, но выполнение этих требований обязательно для бизнеса. Многие компании по-прежнему полагаются на процессы, выполняемые вручную, используют устаревшие или узкоспециализированные облачные системы для защиты и проверки данных, которые невозможно контролировать в комплексе. Такие изолированные системы привлекают киберпреступников.

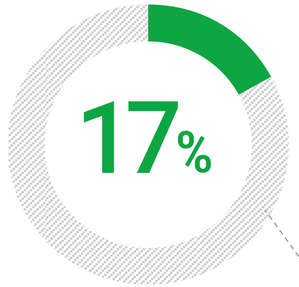
Компании, использующие управление данными в облаке с помощью Veeam, сократили ущерб от кибератак: **95%** из них несут минимальные финансовые потери в результате атак программ-вымогателей. **77%** клиентов Veeam сократили риски потери данных, а **17%** снизили количество ошибок аудита и проблем с выполнением нормативных требований.



значительное снижение риска потери данных[2]



минимальные финансовые потери из-за атак программ-вымогателей[5]



снижение количества ошибок аудита и проблем с соблюдением требований[4]

4.4

Выводы

Решения предыдущих поколений защищают ваши данные, но они настолько устарели, что требуют больше затрат, времени и ресурсов, чем вы можете себе представить. Управление данными в облаке — современная защита данных, которая не ограничивается резервным копированием. Она помогает компаниям выйти на новый уровень. Управление данными в облаке позволяет экономить средства, которые можно потратить на дальнейшее развитие. Оно помогает снять с сотрудников часть задач и направить их усилия на новые многообещающие проекты. Управление данными в облаке поддерживает автоматизацию, позволяя оставить проблемы в прошлом и сосредоточиться на будущем. Оно не привязано к локальным физическим средам. Вместо этого используются облачные ресурсы, которые доступны в любой момент для любых задач.

5.0

Заключение

Данные стали неотъемлемой частью любого цифрового бизнеса, и требования к данным должны быть основой для развития решений. Традиционные решения устаревают и не позволяют решать текущие задачи. Современные системы защиты данных должны стать интеллектуальными, чтобы прогнозировать и удовлетворять потребностеи клиентов. Надежное резервное копирование, мгновенное восстановление и повторное использование данных требуют более совершенных методов управления, использования интеллектуальных возможностей для автономного резервного копирования, переноса данных в соответствии с потребностями бизнеса и защиты от несанкционированных действий.

Veeam стал лидером в сфере резервного копирования и восстановления данных в том числе благодаря своим инновационным решениям и тому, что компания развивает свои передовые методы, предлагая комплексное решение для управления данными. Оно объединяет возможности защиты и переноса данных, обеспечения безопасности и соответствия нормативным требованиям и позволяет защитить данные практически в любой инфраструктуре, которую вы выберете для своего бизнеса.

Внедряя продукты Veeam, заказчики получают доступ к одному из самых современных решений на рынке. Это позволяет им высвободить ресурсы за счет отказа от устаревших инструментов и сосредоточиться на инновационных проектах. Если не обеспечить гибкость данных, их нельзя будет использовать для быстрого внедрения облачных сервисов. Это в свою очередь ограничивает скорость цифровой трансформации. Решения Veeam для гибридного облака позволяют свободно использовать данные в любых облачных средах, независимо от аппаратного и программного обеспечения и без приобретения дополнительных лицензий.

Кроме того, обеспечение защиты данных, ИТ-безопасности и соответствия нормативным требованиям может потребовать участия большого числа сотрудников. Решения Veeam помогают быстро автоматизировать эти задачи и высвободить финансовые и человеческие ресурсы, необходимые для развития бизнеса. Это позволяет обеспечить надежную защиту данных и их использование в гибридной среде, что в свою очередь ускоряет развитие бизнеса и цифровую трансформацию и обеспечивает доступность и целостность важных данных.

[1] Исследование IDC о влиянии Veeam Cloud Data Management Platform на экономические показатели (The Economic Impact of Veeam Cloud Data Management Platform), апрель 2020 г.

[2] Исследование IDC «Способы устранения простоев» (Race to Zero Survey), октябрь 2018 г.

[3] Опрос клиентов Veeam о программах-вымогателях (Veeam Ransomware Customer Study), август 2018 г.

[4] Исследование IDC об использовании решений Veeam для обеспечения доступности и сохранности данных в мультиоблачных средах (Using Veeam to Ensure Data Availability and Retention in Multi-Cloud Environments), август 2019 г.

[5] Опрос клиентов Veeam о программах-вымогателях (Veeam Ransomware Customer Study), август 2018 г.

veeam.com/ru