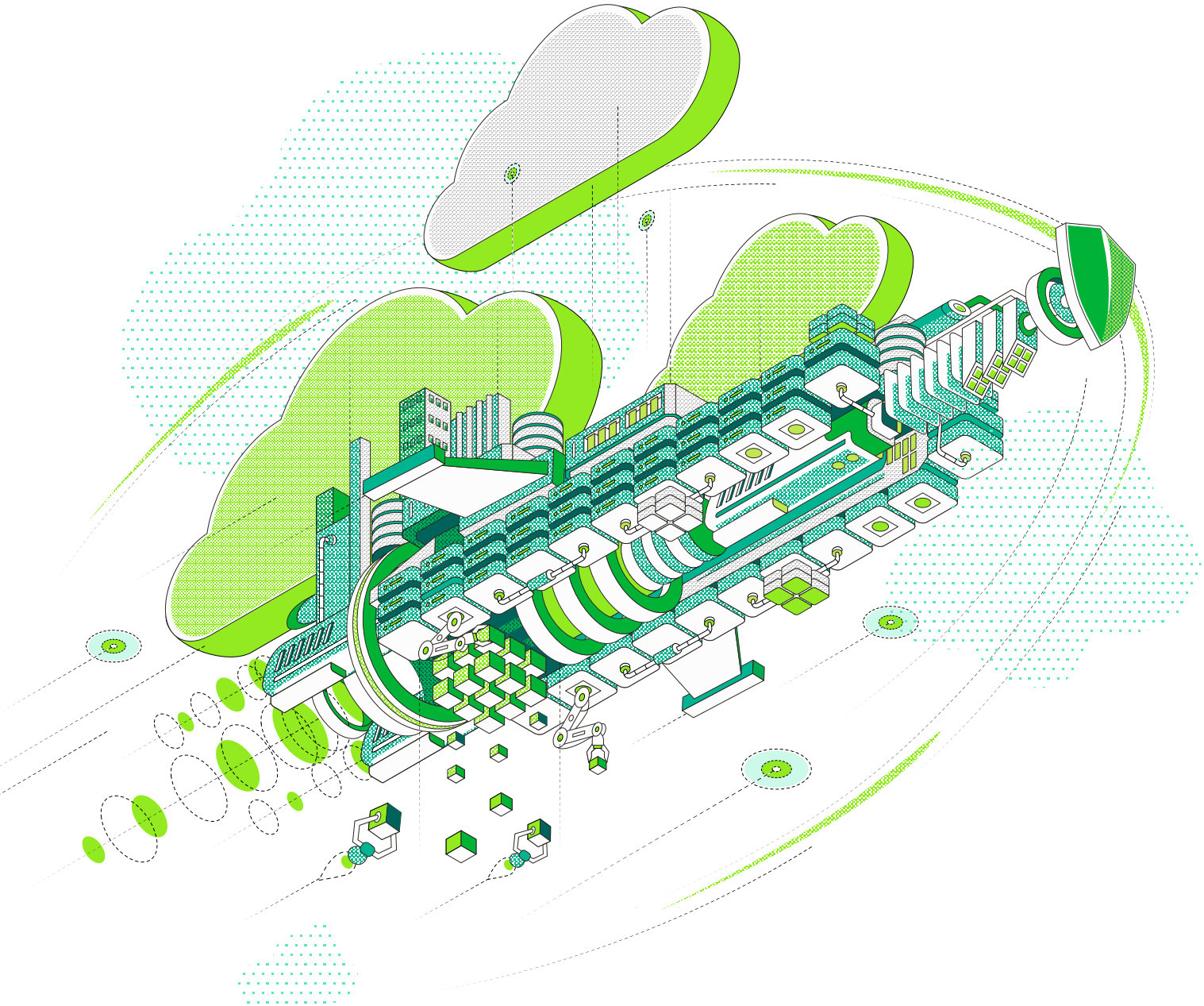
КРАТКИЙ ОБЗОР

2022 г.

Основные тенденции в сфере защиты данных

Восточная Европа и Россия



Изменения в ИТ-отрасли происходят все быстрее. Как компаниям удается реализовать современную защиту данных? С октября по декабрь 2021 года независимая исследовательская компания провела опрос более 3000 ИТ-руководителей и ИТ-специалистов, посвященный факторам и стратегиям развития защиты ИТ-инфраструктуры и данных в 2022 году. Почти все респонденты работают в организациях, насчитывающих более 1000 сотрудников. Они представляют 28 различных стран, в том числе 327 респондентов — страны Восточной Европы и Россию.

По словам респондентов, бюджет их организаций на зашиту данных, включая резервное копирование, обеспечение непрерывности бизнеса и послеаварийное восстановление, в 2022 году вырастет в мире в среднем на **5,9%** в глобальном масштабе. В Восточной Европе и России этот рост составит **6,7%**. Из-за пандемии сложилась уникальная ситуация, когда в сфере локальных ИТ-инфраструктур возник застой, и в результате появились проблемы в цепочках поставок, а облачные сервисы по той же причине развивались ускоренными темпами. Логично, что в 2022 году ожидаются значительные инвестиции в зашиту данных в разнообразных производственных средах, которыми сегодня пользуются компании.

Исследование тенденций в сфере зашиты данных проводилось уже третий год подряд. В этот раз целью опроса было определить количественные показатели изменений с точки зрения, с одной стороны, проблем с зашитой данных, а с другой — целей и стратегий в этой сфере. Кроме того, мы стремились получить представление об обшей ситуации на рынке зашиты данных, послеаварийного восстановлении, кибербезопасности и зашиты от программ-вымогателей, а также контейнеров.

Приоритетными типами инфраструктур остаются гибридные и мультиоблачные

За три года, что проводится это исследование, были собраны данные от более чем **8000** респондентов. На основе этих данных можно заключить, что новая реальность современной ИТ-отрасли — это соотношение локальных и облачных серверов примерно 50/50. В дата-центрах постоянно используются как физические, так и виртуальные платформы. В облаке используется взвешенный подход, сочетаюший гипермасштабируемые инфраструктуры и сервисы поставщиков управляемых услуг.

19%

организаций поменяли решения для резервного копирования в первую очередь по экономическим причинам, а 27% стремились повысить надежность и сократить показатели RPO/RTO

67%

организаций используют облачные сервисы в рамках стратегии защиты данных

76%

организаций за последний год подверглись по крайней мере одной атаке программ-вымогателей

Рис. 1.1

Как вы оцениваете долю серверов каждого вида, используемых вашей организацией в настоящий момент, и какова, по вашим прогнозам, будет эта доля через два года?

В 2022 году в Восточной Европе и России 25% составляют физические серверы, 24% — виртуальные, а 49% — облачные. Эти тенденции позволяют сделать два основных вывода:

- Дата-центры никуда не исчезли и не исчезнут. Даже компании, отдающие приоритет облаку, по многим причинам используют не только облачные, но и локальные системы
- Стратегия зашиты данных должна охватывать физические, виртуальные и различные облачные системы

Несоответствие возможностей ИТ-отделов ожиданиям бизнеса усугубляется

Разрыв между ожиданиями современного бизнеса и уровнем сервиса, который могут обеспечить ИТ-отделы, продолжает расти. Мы отмечаем это на протяжении пяти лет. В Восточной Европе и России:

- **85%** ИТ-руководителей считают, что в их компании существует **проблема ограниченной доступности данных**: ИТ-отдел не может выполнить требования SLA ко времени восстановления работы.
- **83%** ИТ-руководителей считают, что в их компании существует проблема недостаточной зашиты данных, то есть они не могут обеспечить достаточно частое резервное копирование, чтобы гарантировать минимально допустимые потери данных.

Причина этих проблем, вероятнее всего, заключается в том, что увеличилось количество критически важных систем. Однако существует очевидная корреляция между основными движушими факторами изменений: улучшением показателей RTO (доступность) и RPO (зашита), а также повышением надежности (рис. 1.3 в отчете) — и названными выше проблемами. Проблемы, о которых говорят ИТ-руководители, и движушие факторы, которыми руководствуются специалисты, отвечаюшие за ИТ-инфраструктуру и стремяшиеся снизить потери данных и время простоя, особенно важны, если учесть, что **40%** серверов в мире по крайней мере раз в год оказываются в ситуации вынужденного простоя.

40%

серверов как минимум один раз оказывались в ситуации вынужденного простоя

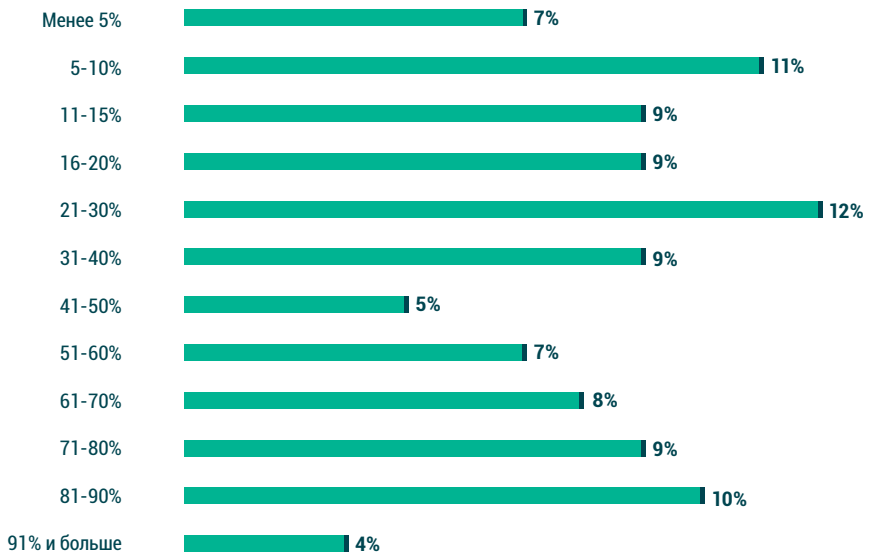
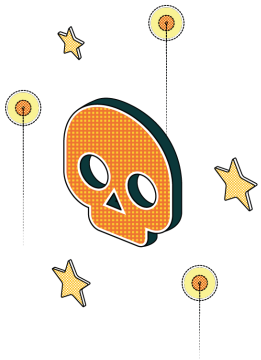


Рис. 1.2

Какой процент ваших серверов хотя бы один раз столкнулся с неожиданным простоем (включая случаи незапланированного перезапуска) за последний год?

Разница между приоритетными и обычными данными не так уж велика



Конечно, некоторые системы имеют большее значение, чем другие, но требования к их восстановлению отличаются не очень сильно.

Потери данных. В мире допустимый период потерь составляет не более часа для 56% приоритетных и 49% обычных данных. Организации в Восточной Европе и России говорят, что допустимый период потерь составляет не более часа для 62% приоритетных и 52% обычных данных. Это значит:

- разница между приоритетными и обычными данными не так уж велика — важны все данные;
- резервного копирования недостаточно, потому что его нельзя выполнять каждый час. Помимо резервных копий необходимо использовать аппаратные снимки и (или) репликацию.

Эти данные особенно интересны, если посмотреть на трехлетнюю тенденцию, которая выявляется с помошью соответствуюших отчетов о тенденциях в сфере зашиты данных. Ниже — средняя частота создания точек восстановления (в минутах) для предотвращения потерь приоритетных и обычных данных:

	2019 год	2020 год	2021 год
Частота создания точек восстановления для приоритетных данных	205 минут	198 минут	121 минута
Частота создания точек восстановления для обычных данных	663 минуты	423 минуты	171 минута

53%

организаций столкнулись со сбоями в работе из-за атак программ-вымогателей. Уже второй год подряд кибератаки становятся причиной большинства простоев

Вполне естественно, организации будут и дальше постепенно улучшать зашиту приоритетных данных: частота составляла **205** минут в 2019 году, а к 2022-му сократилась до **121** минуты. Показательно, что за те же два года организации значительно увеличили частоту создания точек восстановления для остальных данных: с **663** минут (то есть примерно каждые 8 часов или по ночам) до **171** минут (каждые три часа, то есть точки восстановления создаются неоднократно в течение дня). Это уже очень близко к зашите приоритетных данных и подтверждает гипотезу, что все данные важны, а также обшее стремление сочетать резервное копирование (обычно выполняется ночью) с аппаратными снимками и репликацией.

Вынужденные простои. Как и в случае с потерями данных, время допустимого вынужденного простоя отличается для приоритетных и обычных приложений лишь на **10%** и составляет не более одного часа: еше одно подтверждение, что важны все данные, а традиционного резервного копирования раз в сутки уже недостаточно.

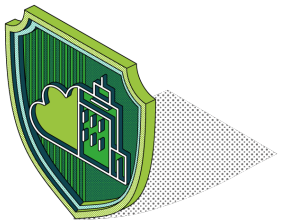
36%

данных оказалось невозможно восстановить после атаки программ-вымогателей

Что это означает в 2022 году?

За последние два года была осуществлена масштабная модернизация ИТ-инфраструктур, особенно там, где можно использовать облачные сервисы. Это связано с осуществлением программ цифровой трансформации, а также ускоренным внедрением облака во время пандемии. **Быстрая модернизация производственных сред заставила многие организации осознать, что они не модернизировали свою защиту теми же темпами, хотя их зависимость от данных и неудовлетворенность текущим положением дел как никогда высоки. Это определяет три основных тенденции 2022 года:**

- инвестиции в защиту данных будут увеличиваться, чтобы защитить современные производственные системы, которые часто размещены в облаке;
- основные движущие факторы изменений будут в основном связаны с качественным улучшением надежности, частоты создания точек восстановления и гибких возможностей восстановления, что позволит сократить показатели RPO и RTO. Кроме того, важную роль будут играть повышение экономичности и оптимизация использования ресурсов, а также защита IaaS/SaaS/контейнеров и использование облака для резервного копирования и послеаварийного восстановления;
- улучшение защиты данных в значительной степени обусловлено признанием того, что кибератакам, в первую очередь атакам программ-вымогателей, рано или поздно подвергнется большинство организаций, а надежное восстановление — важная часть стратегии защиты от киберугроз. Таким образом, все понимают, что программы-вымогатели — это серьезная угроза, а автоматизированное восстановление из резервных копий — критически важный компонент любого плана обеспечения непрерывности бизнеса, послеаварийного восстановления и защиты от киберугроз.



42%

ИТ-руководителей в мире считают, что главная характеристика любого решения для резервного копирования данных в крупных компаниях – широта спектра защищаемых систем

Точка зрения Veeam

Платформа Veeam для резервного копирования данных и управления ими

Сейчас компаниям особенно важна уверенность, что их данные защищены и всегда доступны, где бы они ни находились — в локальной инфраструктуре, на удаленных устройствах или в облаке. Veeam предлагает единую платформу для защиты облачных, виртуальных и физических систем, а также SaaS и Kubernetes. Наши заказчики уверены, что их приложения и данные надежно защищены от программ-вымогателей, аварий и злоумышленников, а также всегда доступны благодаря самой простой, гибкой надежной и эффективной платформе в отрасли.

Veeam помогает заказчикам ускорить цифровую трансформацию, защититься от киберугроз и гарантировать отказоустойчивость бизнес-процессов, обеспечивая защиту и доступность данных. Сократите расходы и упростите работу с помощью Veeam — №1 для резервного копирования и восстановления данных.

Подробнее: **https://www.veeam.com/ru**.

Читайте полный текст глобального отчета

Вопросы, касающиеся данных и результатов исследования, можно задать по электронной почте StrategicResearch@veeam.com