thalesgroup.com

#2020DataThreat

THALES

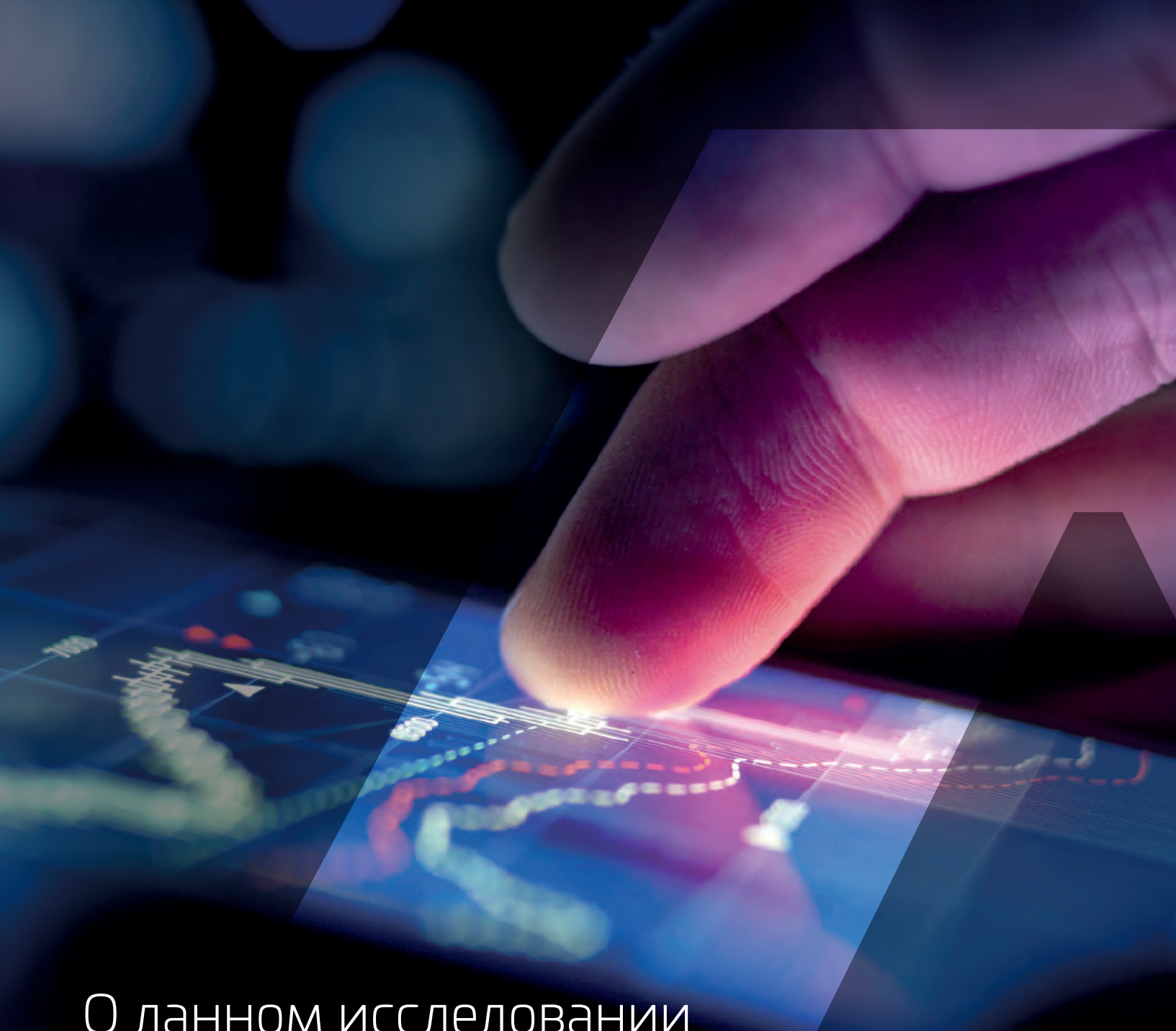
Новые аспекты системы защиты данных

2020 Отчёт Thales об угрозах безопасности данных

Во всём мире

ИССЛЕДОВАНИЯ И АНАЛИТИКА:

IDC | АНАЛИЗ БУДУЩЕГО



О данном исследовании

Настоящий отчет основан на глобальном веб-опросе, выполненном Международным центром данных IDC, по ответам 1723 руководящих работников, ответственных за информационные технологии и безопасность данных или влияющих на них. Респонденты представляли 16 стран: Австралию, Бразилию, Францию, Германию, Индию, Индонезию, Японию, Малайзию, Мексику, Нидерланды, Новую Зеландию, Сингапур, Южную Корею, Швецию, Великобританию и США. Организации являлись представителями целого ряда отраслей, в основном из области здравоохранения, финансовых услуг, розничной торговли, технологий и организационно-распорядительной деятельности органов власти. Должности участников опроса варьировались от руководителей высшего звена, включая генеральных директоров, финансовых директоров, главных специалистов по обработке данных, руководителей подразделений по информационной безопасности, главных научных сотрудников по обработке данных и главных сотрудников по управлению рисками, и до президентов компаний и их заместителей, IT-администраторов, аналитиков безопасности, инженеров по безопасности и системных администраторов. Респонденты представляли широкий спектр компаний и учреждений по размерам и значительности, в большинстве своем насчитывающих от 500 до 10 000 сотрудников.

Опрос проводился в ноябре 2019 года.

Содержание

Наши спонсоры:

Резюме

Компании, организации и учреждения используют широкий спектр технологий, в том числе облачные, мобильные, а также системы контроля оборудования через Интернет (IoT, Интернет вещей), в целях совершенствования своего бизнеса, повышения качества обслуживания клиентов, поиска новых источников доходов и сокращения расходов. Исследования Международного центра данных IDC показывают, что цифровизация (DX) идет полным ходом: 43% компаний, участвующих в данном исследовании, заявили, что они либо агрессивно подрывают рынки, в которых участвуют, либо внедряют цифровые технологии, обеспечивающие повышение гибкости предприятия.

Хотя DX может обеспечить существенное увеличение доходов, одновременно с этим она усложняет защиту данных. Организации все больше зависят от объема данных, хранящихся на периферийных устройствах, и постоянно расширяют его, а это означает, что им необходимо сосредоточиться на аспектах, выходящих за рамки традиционных границ сетевого окружения. В работе с облачными данными мы находимся в стадии перелома, поскольку половина всех данных теперь хранится в облачных средах, и 48% этих данных являются конфиденциальными. Кроме того, большинство организаций полагаются на среды с несколькими облаками. Все это делает сегодняшние среды, использующиеся для хранения и обработки данных, еще более сложными; эта сложность является главным барьером для обеспечения безопасности данных.

Вместе с тем, организации неадекватно реагируют на проблемы, связанные с безопасностью данных. Две трети из них считают, что они обеспечивают высокий уровень безопасности и не внедряют процессы и не инвестируют в технологии, необходимые для надлежащей защиты данных. Более половины допустили определенные нарушения или не прошли проверки безопасности. И когда речь идет о защите данных в облаке, большинство компаний неправильно строят свои отношения с облачными провайдерами в области их ответственности.

43%

компаний, участвующих в данном исследовании, говорят, что они либо агрессивно подрывают существующие рынки путем разработки все новых и новых продуктов, либо внедряют цифровые технологии, обеспечивающие повышение гибкости предприятия.

Что касается инвестиций, обеспечение защиты данных по-прежнему составляет небольшую долю в общем бюджете безопасности. Сорок шесть процентов организаций планируют увеличить расходы по этой статье в течение следующих 12 месяцев, столько же, сколько было в прошлом году. Но эти организации по-прежнему направляют непропорционально большую часть своих расходов на сетевую безопасность, поскольку 34% респондентов сосредоточены на защите данных, а расходы на нее в среднем составляют всего 15% от общего бюджета информационной безопасности.

С точки зрения возникающих угроз, на горизонте уже появилась квантовая вычислительная техника, которая обещает еще больше усложнить вопросы обеспечения безопасности данных. При появлении в сети такой техники требования к криптографии в корне изменятся, и 72% респондентов обнаружат, что квантовая криптография повлияет на их организации в ближайшие пять лет.

Поскольку организации сталкиваются с более сложными проблемами защиты данных и увеличением их количества, им нужны более разумные и более эффективные способы обеспечения безопасности. Компании должны применять многоуровневый подход к защите данных, принимая на себя общие обязанности по обеспечению безопасности облачных вычислений и применяя модели с нулевым доверием, которая проверяет подлинность пользователей и устройств, обращающихся к приложениям и сетям, а также использует более надежное обнаружение данных, их защиту, предотвращение потери данных и решения для шифрования.

34%

респондентов сосредоточены на защите данных, а расходы на нее в среднем составляют всего 15% от общего бюджета информационной безопасности

01
Основные выводы

Расширение масштабов цифровизации усложняет защиту данных

Компании, организации и учреждения фундаментально переосмысливают свою деятельность и используют преимущества цифровых технологий, таких, как облачные, мобильные и IoT, для цифровизации своих операций. Даже «традиционные компании» будут получать больший доход от цифровых продуктов, услуг и используя свою квалификацию. Сорок три процента организаций, принявших участие в нашем исследовании, говорят, что они либо агрессивно подрывают существующие рынки путем выпуска все более совершенной продукции, либо внедряют цифровые технологии, которые обеспечивают большую гибкость предприятия (см. рис. 1). США опережают все страны, представители которых были опрошены на данный момент, при этом 59% опрошенных считают, что они либо ведут агрессивную политику на своих рынках, либо внедряют возможности цифровых технологий; за США следует Великобритания (51%)

Рис. 1 – Положение с цифровизацией
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Ни одна из организаций не застрахована от угроз безопасности данных: 49% респондентов оз безопасности данных: 49% респондентов во всем мире хотя бы однажды во всем мире хотя бы однажды сталкивались с утечкой данных, в то время как в прошлом году - 26%. Кроме этого, 47% организаций сообщают, что имели место нарушения или они не прошли аудит соответствия в прошлом году.

«Ни одна из организаций не застрахована от угроз безопасности данных: 49% респондентов во всем мире хотя бы однажды сталкивались с утечкой данных».

В то время как организации, осуществляющие цифровизацию, находят новые источники обеспечения конкурентного преимущества, они сталкиваются с проблемами безопасности данных, которые кроет в себе DX. Степень цифровизации DX напрямую влияет на уязвимость данных: чем выше степень цифровизации, тем больше вероятность того, что она повлечет за собой утечку данных. В отчете Thales об угрозе безопасности на 2020 год отмечено, что 45% организаций в одной из двух лучших категорий DX столкнулись с утечкой данных в этом году, что значительно выше, чем общий уровень уязвимости. Кроме того, компании, которые тратят больше средств на IT-безопасность, чаще сталкиваются с утечками. Двадцать девять процентов организаций, для которых безопасность составляет более 10% их IT-бюджета, столкнулись с нарушением в прошлом году, и 52% были нарушены в какой-то момент, по сравнению с 19% и 40%, соответственно, для компаний, у которых расходы на обеспечение безопасности составляют 10% или менее (см. рис. 2). Организации со стратегией цифровизации – те организации, которые принимают стратегические, организационные, технологические и финансовые решения, приводящие их к цифровизации в ближайшие несколько лет, – также могут подвергаться большей угрозе безопасности данных. Их более высокий уровень сложности может также означать, что они, скорее всего, будут знать, что они нарушаются. Менее опытные компании могут иметь меньшую подверженность риску или подвергаются нарушениям, не зная этого.

> «Чем выше степень цифровизации организации, тем больше вероятность того, что она столкнется с утечкой данных».

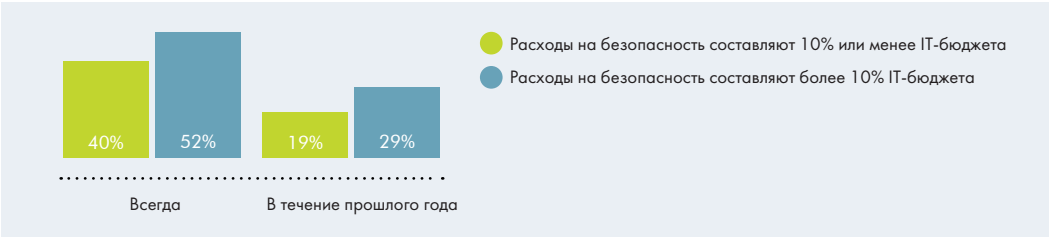


Рис. 2 – Процент инцидентов с нарушением безопасности в зависимости от расходов
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC , ноябрь 2019 г.

Организации размещают конфиденциальные данные, используя широкий спектр технологий

Организации внедряют широкий спектр технологий платформ 3-го уровня, включая облачные, мобильные, социальные, большие данные и IoT. Приложения SaaS получили самое широкое распространение: 95% против 71% в 2018 году (см. рис. 3). Мобильные платежи, социальные сети и облачные среды IaaS и PaaS также ведут к планируемому внедрению новейших технологий. Необходимо обратить внимание, что многие из этих технологий, такие как IoT и мобильная связь, являются новейшими технологиями, которые еще более укрепляют концепцию, согласно которой доступ к данным выходит далеко за рамки традиционного сетевого окружения.

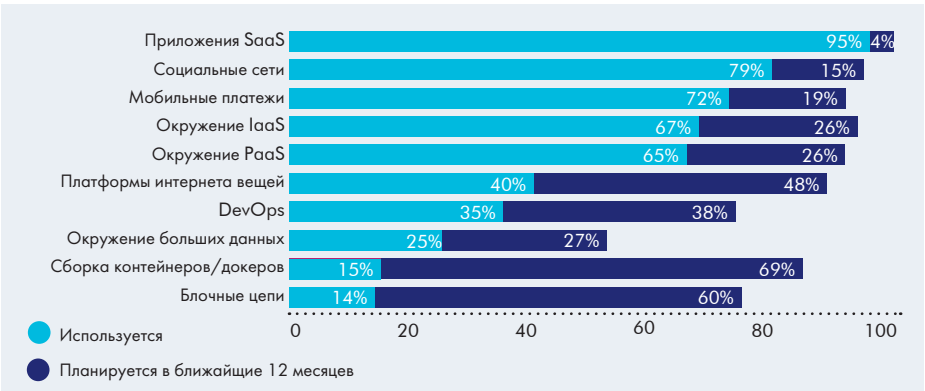
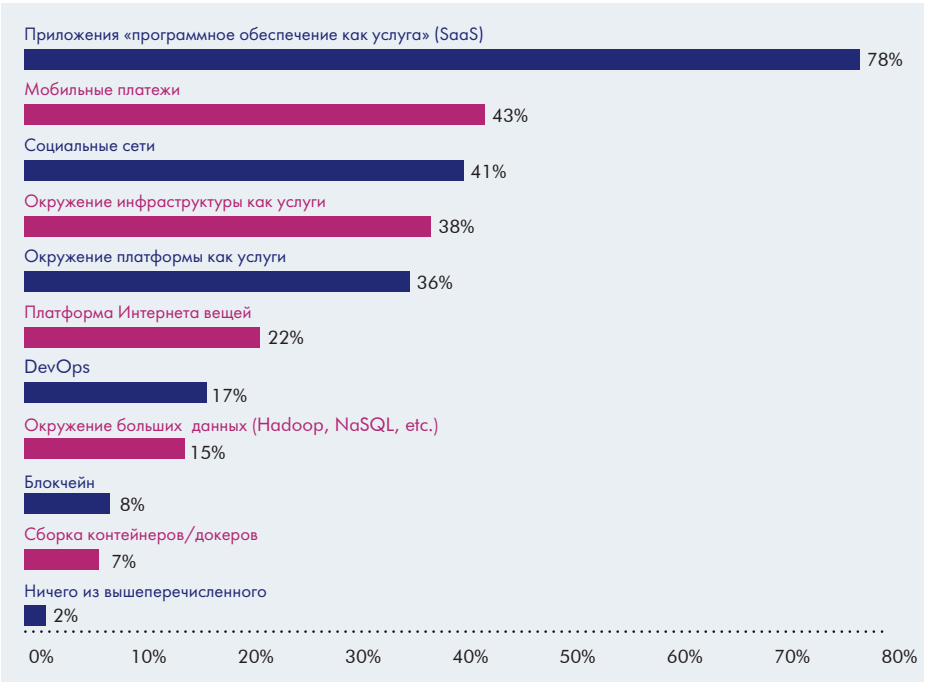


Рис.3 – Уровни внедрения технологий
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Аналогичным образом, многие организации размещают данные в одинаково широком наборе технологий. 78% из них хранят конфиденциальные данные в приложениях SaaS, 38% — в средах IaaS и 36% — в средах PaaS. Девяносто восемь процентов организаций хранят данные, по крайней мере, в одной из технологий, вошедших в опрос (см. рис. 4). Данные по США показывают еще более высокую частоту хранения конфиденциальных данных в облачных средах: 79% в приложениях SaaS, 48% в средах PaaS (по сравнению с 36% в мире) и 46% в средах IaaS (по сравнению с 38% в мире).



> Защита периметра мало что дает для защиты локальных данных, что говорит о необходимости использования подхода с нулевым доверием и защитой данных».

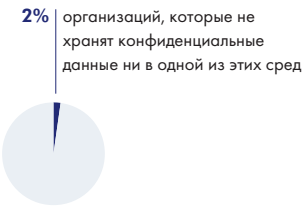


Рис. 4 – Технологические среды, используемые для хранения конфиденциальных/регламентированных данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г

Необходимо подчеркнуть, что число респондентов, заявивших, что они хранят данные в этих средах, увеличилось по сравнению с прошлым годом (при этом более 40% респондентов заявили, что используют такие среды, как большие данные и IoT, для хранения конфиденциальных данных). IDC рассматривает это как своего рода признак зрелости в отрасли. Мы полагаем, что респонденты в прошлом году реагировали на модные словечки и ревностно брали на себя ответственность за принятие соответствующих технологий. Напротив, респонденты в этом году более реалистично оценивают использование этими организациями более перспективных технологий.

По мере того, как компании расширяют использование технологий облачных, мобильных, социальных сетей, больших данных и IoT платформы 3-го уровня, в результате чего конфиденциальные данные потенциально становятся все более уязвимыми. Таким образом, защита периметра мало что дает защите локальных данных, что говорит о необходимости использования подхода с нулевым доверием и защитой данных в целях повышения безопасности. Такой подход с нулевым доверием исключает бинарный подход доверия/отсутствие доверия вчерашней локальной реальности, ориентированной на периметр, и вместо этого требует подхода с минимальными привилегиями, непрерывной проверкой и проверкой, обеспечивающей защиту доступа как к сети, так и к приложению. Аналогичным образом такие технологии, как шифрование и токенизация, гарантируют, что в случае взлома, утечки данных или кражи физических устройств данные также будут надлежащим образом защищены.

Большинство данных хранятся в облаке, что создает дополнительные риски

Девяносто восемь процентов опрошенных организаций хранят некоторые данные в облаке. Действительно, данные, хранящиеся в облаке, достигли точки перелома, и наше исследование показало, что примерно 50% данных находится в облаке. Что еще более важно, по утверждению респондентов, приблизительно 48% этих данных в облаке являются конфиденциальными. Организации в США полагаются на облако для хранения данных в большей степени, чем респонденты во всем мире. По оценкам респондентов из США, 55% данных хранятся в облачных средах, а 54% этих облачных данных являются конфиденциальными (см. рис. 5).

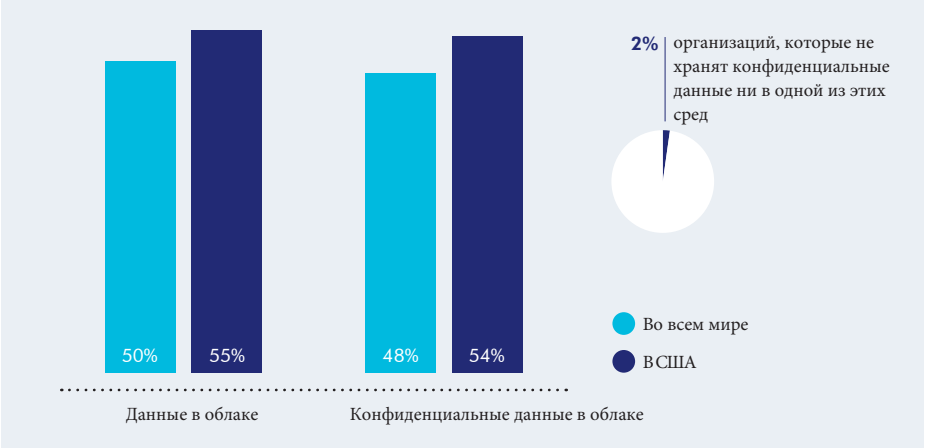


Рис. 5 - Данные, хранящиеся в облачных средах
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Чем больше конфиденциальных данных хранится в облачных средах, тем выше риски для их безопасности. Тем не менее, несмотря на значительное количество конфиденциальных данных, степень шифрования и токенизации данных низка. Действительно, 100% респондентов говорят, что по крайней мере некоторые из конфиденциальных данных в облаке не зашифрованы. Только 57% конфиденциальных данных, хранящихся в облачных средах, защищены шифрованием, и менее половины - 48% - защищены токенизацией. США используют шифрование данных (63%) и токенизацию (54%) для защиты конфиденциальных данных в облаке в большей степени, чем в во всем мире (см. рис. 6).

> «100 % респондентов считают, что по крайней мере некоторые из конфиденциальных данных в облаке не зашифрованы».

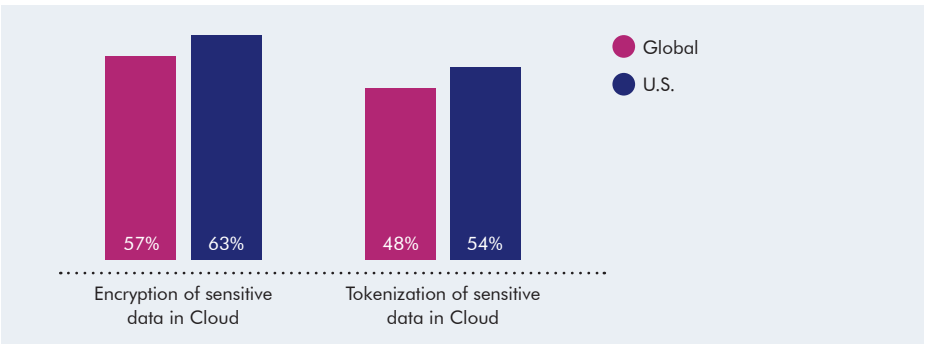


Рис. 6 - Безопасность конфиденциальных облачных данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Сложность является главным барьером для безопасности данных, так как Multicloud становится нормой

Обеспечение безопасности усложняется по мере увеличения количества переносимых в облако данных. Но в основном эта сложность связана с внутренними причинами, поскольку множественные облачные системы среды становятся все более распространенными. Компании используют несколько сред IaaS и PaaS, а также сотни приложений SaaS. Восемьдесят один процент респондентов по всему миру пользуется услугами более одного поставщика IaaS (86% в США), 81% имеют более одного поставщика PaaS (86% в США) и 11% используют более 100 приложений SaaS для управления (14% в США) (см. рис. 7).

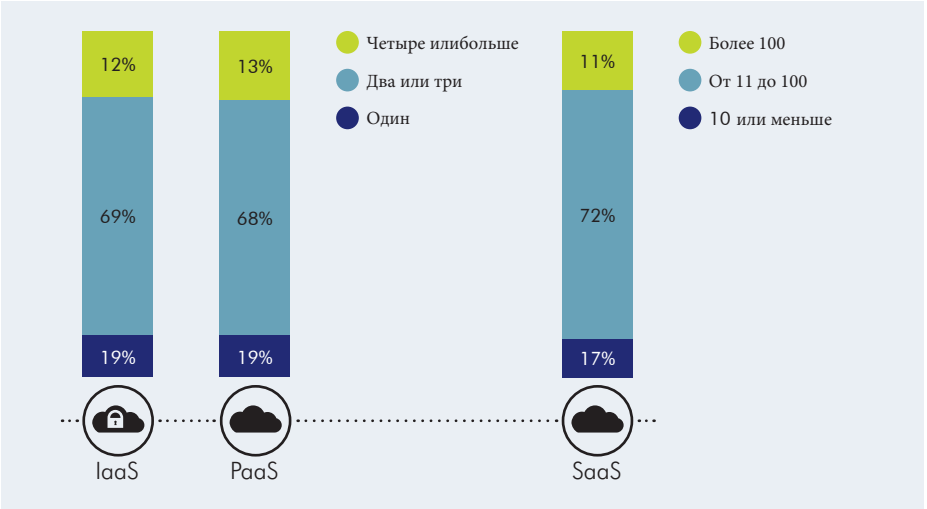


Рис. 7 – Количество поставщиков IaaS/PaaS/SaaS

Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

В результате усложняется жизнь специалистов по безопасности. Респонденты оценивают сложность в качестве главного воспринимаемого барьера для обеспечения безопасности данных, что влечет за собой стремление избежать влияния на производительность и бизнес- процессы (см. рис. 8). Подавляющее большинство организаций понимают важность безопасности данных и считает, что проблемой является «отсутствие ощутимой потребности» (26%) или «отсутствие заинтересованности организации» (25%).

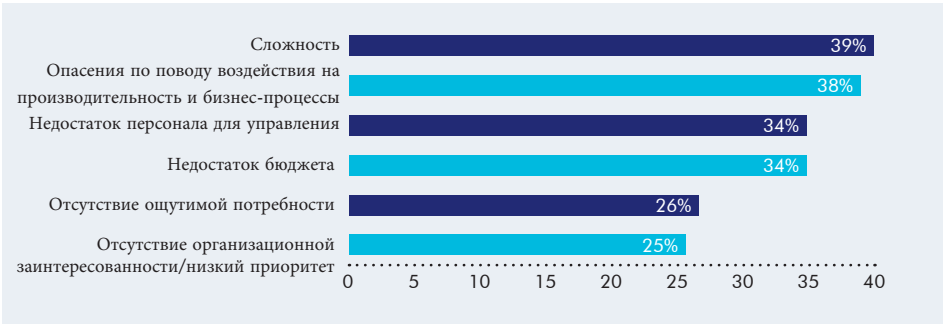


Рис. 8 – Барьеры для реализации безопасности данных

Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

> Респонденты оценивают сложность в качестве основного предполагаемого барьера для обеспечения безопасности данных, за которой следует стремление избежать влияния на производительность и бизнес-процессы».

Предвидятся проблемы безопасности с внедрением квантовых вычислений

Обеспечить безопасность данных станет еще сложнее с появлением квантовых вычислений. Требования криптографии подчеркивают критическую проблему безопасности, вызванную высокой производительностью квантовых вычислений. 72% организаций отдают себе отчет в том, как они повлияют на криптографические операции в последующие пять лет (см. рис. 9). Девяносто два процента респондентов обеспокоены тем, что квантовые вычисления облегчат доступ к конфиденциальным данным, а 35% проявляют высокую и очень высокую степень обеспокоенности. Респонденты из США воспринимают ситуацию аналогичным образом: 72% считают, что это повлияет на криптографические операции в последующие пять лет, 91% обеспокоены тем, что квантовые вычисления могут поставить под угрозу конфиденциальные данные, и 41% проявляют высокую и очень высокую степень обеспокоенности.

> «Девяносто два процента респондентов обеспокоены тем, что квантовые вычисления откроют доступ к конфиденциальным данным, а 35% проявляют высокую и очень высокую степень обеспокоенности».

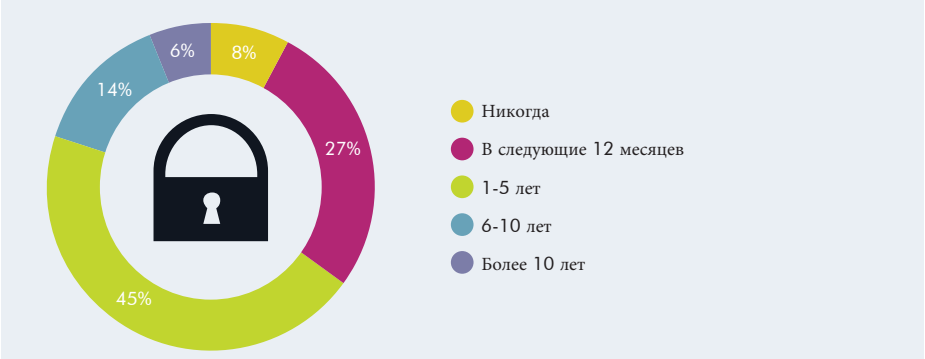


Рис. 9 – Влияние на организации квантовой криптографии
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Основной стратегией устранения угроз из-за квантовых вычислений является изменения архитектуры IT- безопасности (35%) и развертывание ключевой инфраструктуры управления (34%). Но многие организации не знают, как реагировать, даже если угрозы появятся в ближайшие пять лет. Двадцать два процента респондентов планируют использовать системы с критическим диапазоном приемлемости, а 6% не планируют вообще их использовать.

Ощущение безопасности в организациях противоречит реальности

Несмотря на распространяющиеся угрозы безопасности данных, в 2019 году предприятия чувствуют себя менее уязвимыми, чем в 2018 году. Шестьдесят семь процентов организаций чувствовали себя уязвимыми в 2019 году по сравнению с 86% в 2018 году, даже несмотря на то, что риски для безопасности растут. Результаты показывают, что уровень воспринимаемой уязвимости снижался из года в год, и 33% респондентов заявляют, что они «совсем не уязвимы» по сравнению с 14% в 2018 году (см. рис. 10). Организации США занимают аналогичную позицию: 69% считают себя уязвимыми, а 31% вовсе не уязвимыми.

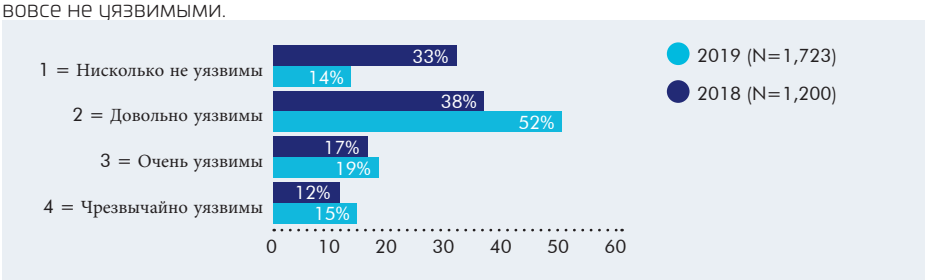


Рис. 10 - Уязвимость данных, 2019 г. по сравнению с 2018 г.
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Такой низкий уровень восприятия уязвимости говорит об отрыве от реальности. Респонденты высказываются о том, что они не получают достаточной поддержки соответствующими методами защиты данных или инвестициями. Организации не очень изменили свое поведение, не используя инструменты, которые сделали бы их менее уязвимыми. Как упоминалось ранее, степень шифрования и токенизации конфиденциальных данных в облаке довольно низка. Кроме того, только 61% респондентов используют шифрование файлов, а 59% - шифрование базы данных. Внедрение шифрования файлов и баз данных увеличилось лишь незначительно в 2019 году по сравнению с 2018 годом с темпами внедрения 56% и 55% соответственно (см. рис. 11). Обратите внимание, что в США наблюдается более широкое использование шифрования файлов (69%) и шифрования базы данных (65%) по сравнению с мнениями респондентов во всем мире.

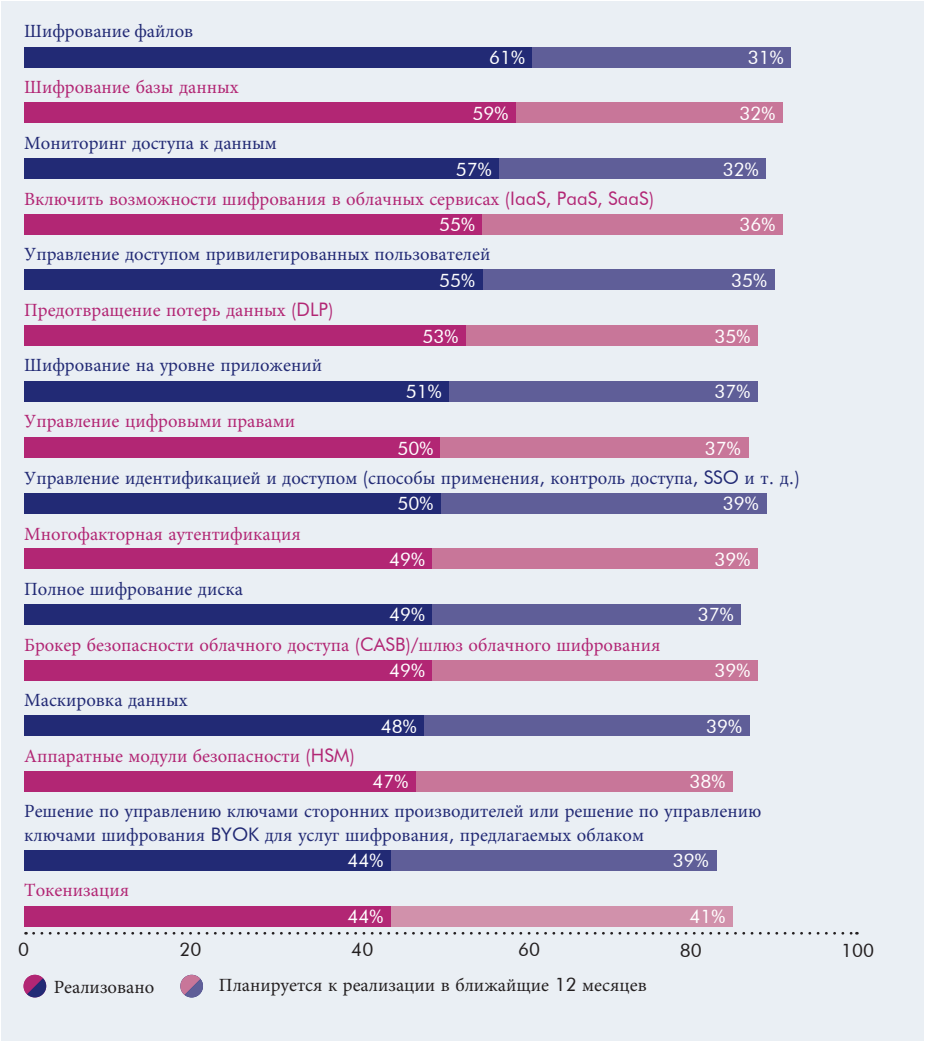


Рис. 11 – Внедрение инструментов шифрования и защиты данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Увеличение расходов на безопасность не соответствует ее приоритетам

Организации планируют потратить больше денег на безопасность данных в следующем году и делать это по ставкам, аналогичным прошлому году. Сорок девять процентов респондентов заявили, что в ближайшие 12 месяцев они будут инвестировать в той или иной степени в безопасность данных. Тем не менее, рост бюджета на безопасность данных немного замедляется, и почти одна из пяти организаций планирует сократить расходы на безопасность данных в 2020 году (см. рис. 12). Компании США отмечают больший рост бюджетов по защите данных, чем респонденты во всем мире: 58% компаний США увеличивают расходы на защиту данных и только 13% сокращают их.

58%

американских компаний увеличивают расходы на безопасность данных и только 13% снижают их.

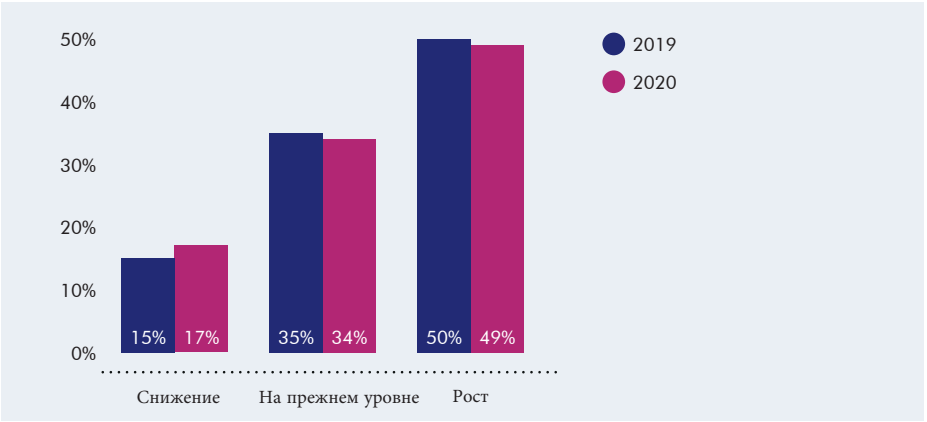


Рис. 12 – Расходы на безопасность данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Предприятия уделяют примерно одинаковое внимание безопасности сети, данных и приложений, причем несколько больше внимания уделяют безопасности сети, чем безопасности приложений или данных (см. рис. 13). И хотя 34% внимания уделяется безопасности данных, расходы на безопасность данных значительно отстают от этого показателя, поскольку только 15,5% бюджетов безопасности расходуются на безопасность данных.

Рис. 13 – Пропорции распределения внимания к разным аспектам безопасности
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Респонденты считают, что, демонстрируя несоответствие между бюджетом безопасности и вниманием департаментов безопасности, злоумышленники представляют собой наибольшую опасность для данных. Пятьдесят семь процентов компаний опасаются киберпреступников, которые крадут данные в целях получения выгоды, а 52% беспокоятся о кибертеррористах, которые наносят ущерб компаниям, выставляя их в непривлекательном виде.

Интересно, что респонденты меньше заботятся о повседневных проблемах, которые на самом деле могут представлять большую угрозу. Это проблемы, связанные с ситуациями, над которыми они имеют контроль, такими, как партнеры с внутренним доступом, привилегированный доступ пользователей, учетные записи поставщиков услуг и учетные записи подрядчиков. Организации должны быть осторожны с предоставлением чрезмерного количества счетов и их сумм, поскольку риск со стороны подрядчиков часто больше связан с небрежностью, чем со злонамеренным поведением (см. рис. 14 и 15).

Рис. 14 – Вредоносные угрозы в отношении данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Рис. 15 – Внутренние угрозы в отношении данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

02

Безопасность облачных данных на переходном этапе

Отчет Thales об угрозах безопасности данных во всем мире в 2020 г.

Размещение данных в облачной среде требует изменений в подходе к сфере безопасности

Более половины данных теперь хранятся в облаке, причем значительная часть этих данных является конфиденциальной. В результате отделы IT-безопасности теперь, как никогда, должны принять на себя ответственность за работу в своей части облачной среды и внедрять передовые методы обеспечения безопасности данных, поскольку поставщик облачных услуг чаще всего не гарантирует безопасность на уровне данных.

Организации обеспокоены многими проблемами безопасности данных при размещении их в облачной среде. Тем не менее, они, по-видимому, больше всего обеспокоены проблемами, с которыми сталкиваются облачные провайдеры, такими, как нарушения безопасности у провайдера и случаи сбоя провайдера безопасности (выделено красным на рис. 16). Несмотря на реальные опасения, вероятность возникновения этих проблем в действительности довольно низка. Организации, по-видимому, меньше озабочены проблемами, над которыми они имеют непосредственный контроль и которые представляют большие потенциальные уязвимости, такими, как управление ключами шифрования (выделено второй и третьей красными полосами на рис. 16).

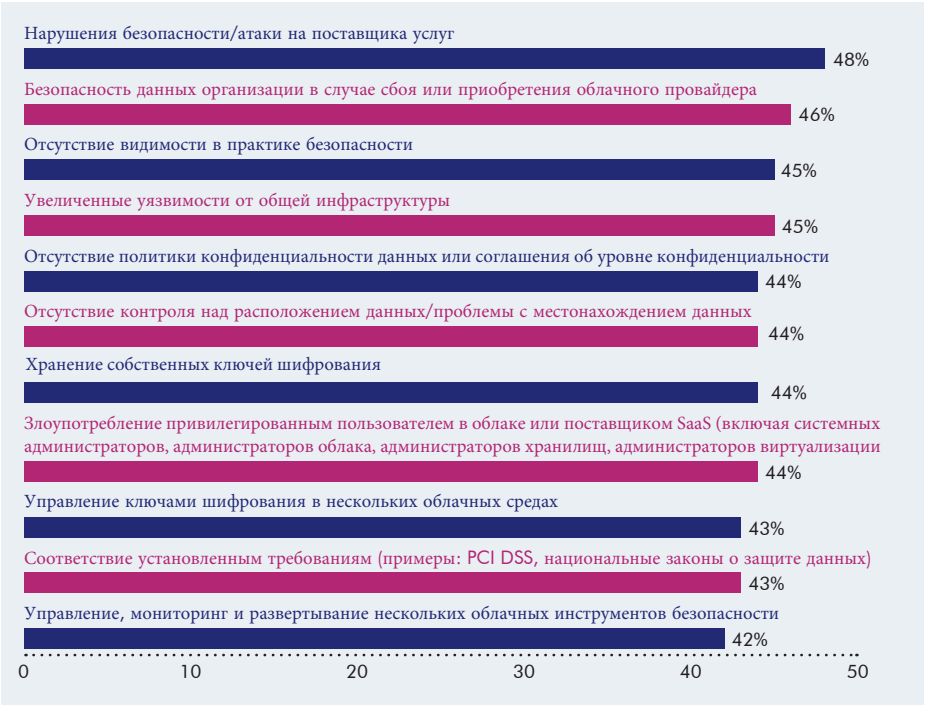


Рис. 16 – Проблемы безопасности в облаке
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

> «Организациям следует сместить акцент на облачную безопасность и сосредоточиться на той части модели совместной ответственности, где сама организация может влиять на безопасность своих собственных данных».

Это несоответствие между угрозами, которые воспринимают респонденты, и теми угрозами, которые в действительности представляют наибольший риск, подразумевает, что респонденты не в полной мере учитывают требования безопасности в облачном окружении. Каждый тип облачной среды требует изменения ответственности за идентичность, данные, приложения, операционные системы, виртуализацию серверов, сеть, инфраструктуру и оборудование. Организации должны сместить акцент в своей облачной безопасности на часть модели общей ответственности, где сама организация может влиять на безопасность своих собственных данных (см. рис. 17).

Рис. 17 – Модель общей ответственности IDC
Источник: IDC, ноябрь 2019 г

Проблемы безопасности также меняются по мере того, как организации внедряют больше данных в приложения SaaS, а также в среды IaaS и PaaS

Согласно нашему исследованию, 93% респондентов по крайней мере в некоторой степени обеспокоены безопасностью данных приложений SaaS. Проблемы безопасности SaaS охватывают широкий спектр рисков: шифрование данных в организации поставщика услуг и возможность управлять шифрованием с помощью локальных ключей шифрования, возглавляющих список (см. рис. 18).

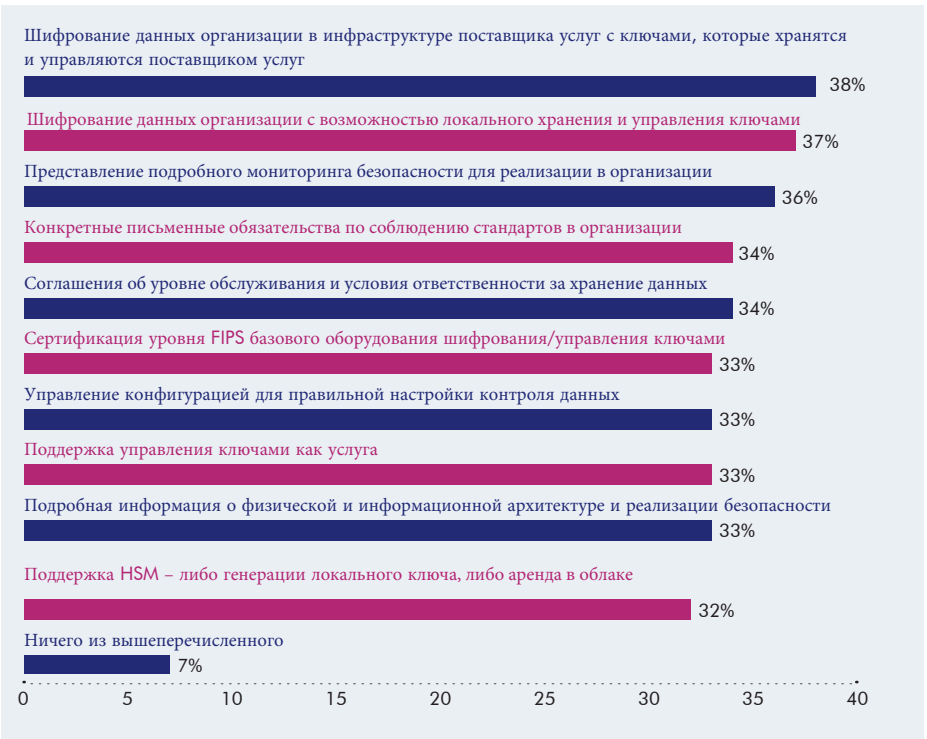
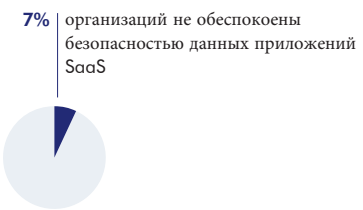
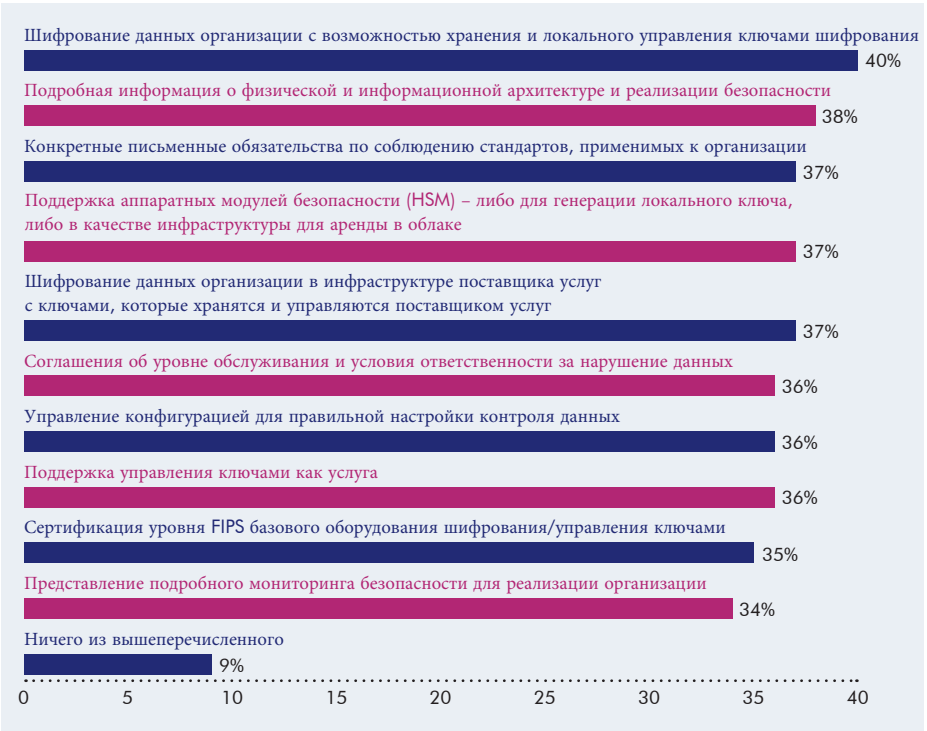


Рис. 18 - Проблемы безопасности SaaS
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

> «Проблемы безопасности SaaS охватывают широкий спектр рисков: шифрование данных в организации поставщика услуг и возможность управлять шифрованием с помощью локальных ключей шифрования, возглавляющих список».



Девяносто один процент респондентов имеют по крайней мере некоторые опасения по поводу безопасности данных в средах IaaS. Проблемы безопасности IaaS также охватывают широкий спектр проблем, связанных с интеграцией локальных ключей и информацией о физической схеме расположения, в качестве главных проблем (см. рис. 19).



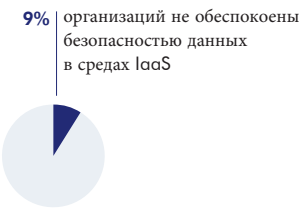
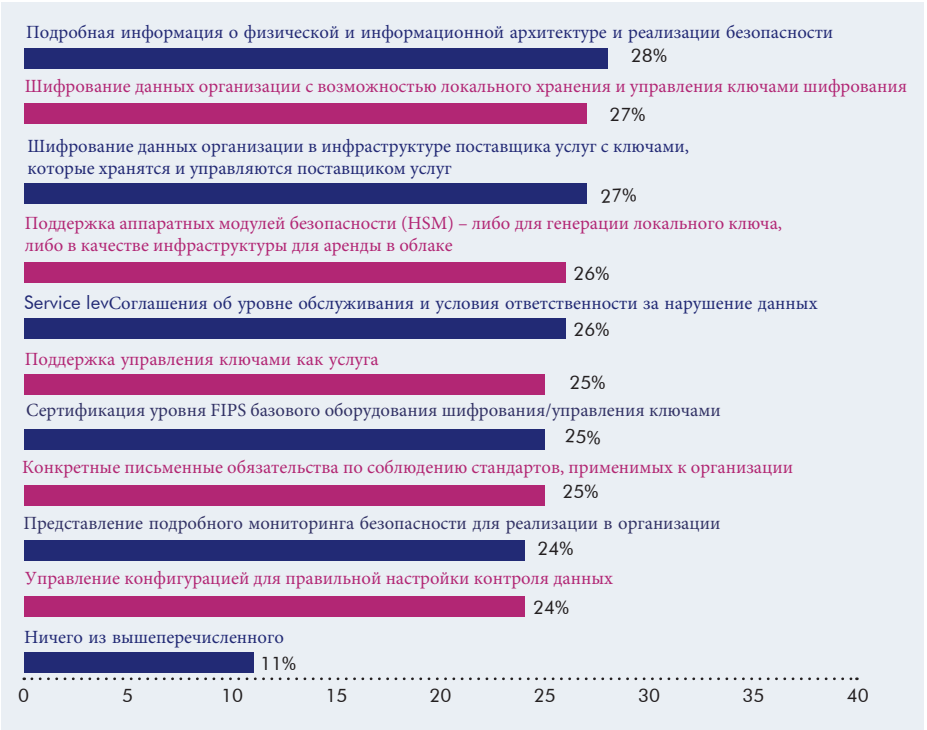


Рис. 19 – Проблемы безопасности IaaS
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г

Восемьдесят девять процентов респондентов имеют по крайней мере некоторую озабоченность по поводу безопасности данных в средах PaaS, где первыми являются информация о физической схеме расположения и шифрование данных (см. рис. 20).

«Респонденты выразили обеспокоенность по поводу шифрования данных организации с возможностью локального хранения и управления ключами шифрования».



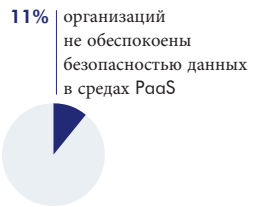


Рис. 20 - Проблемы безопасности PaaS

Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Конечно, каждая из различных облачных сред имеет свои уникальные проблемы; Тем не менее, респонденты выразили некоторые общие мнения по тематике IaaS, SaaS и PaaS (рис. 18-20). В каждом из выделенных красных прямоугольников на предыдущих рисунках, которые указывают на наиболее волнующие вопросы, респонденты выразили обеспокоенность по поводу «шифрования данных организаций с возможностью локального хранения и управления ключами шифрования».

Аналогично: «Шифрование данных организации в инфраструктуре поставщика услуг с помощью ключей, которые хранятся и управляются поставщиком услуг», является постоянной проблемой, значение чего повышается по мере снижения уровня контроля в инфраструктуре (как показано на рис. 17). Наши респонденты выражают обеспокоенность контролем и управлением ключами шифрования.)

03

Проблемы безопасности и методы смягчения последствий с помощью окружения данных

Цифровизация создает новые проблемы для обеспечения безопасности

Наряду с обеспечением новых возможностей реализации новых технологий, цифровизация создает и новые проблемы безопасности. Современные технологии цифровизации, такие, как IoT и мобильные платежи, позволяют организациям привлекать клиентов повсюду, и в то же время это связано с переносом проблем безопасности с локальных на облачные среды. Большие данные, контейнеры и технологии DevOps поддерживают облачные и периферийные вычисления. Облако расширяет применение этих технологий, обнаружение конфиденциальных данных и управление ключами играют еще более важную роль в безопасности данных. Тем не менее, обнаружение данных и управление ключами не воспринимаются как первоочередные задачи, что создает потенциальные пробелы в практике обеспечения безопасности данных.

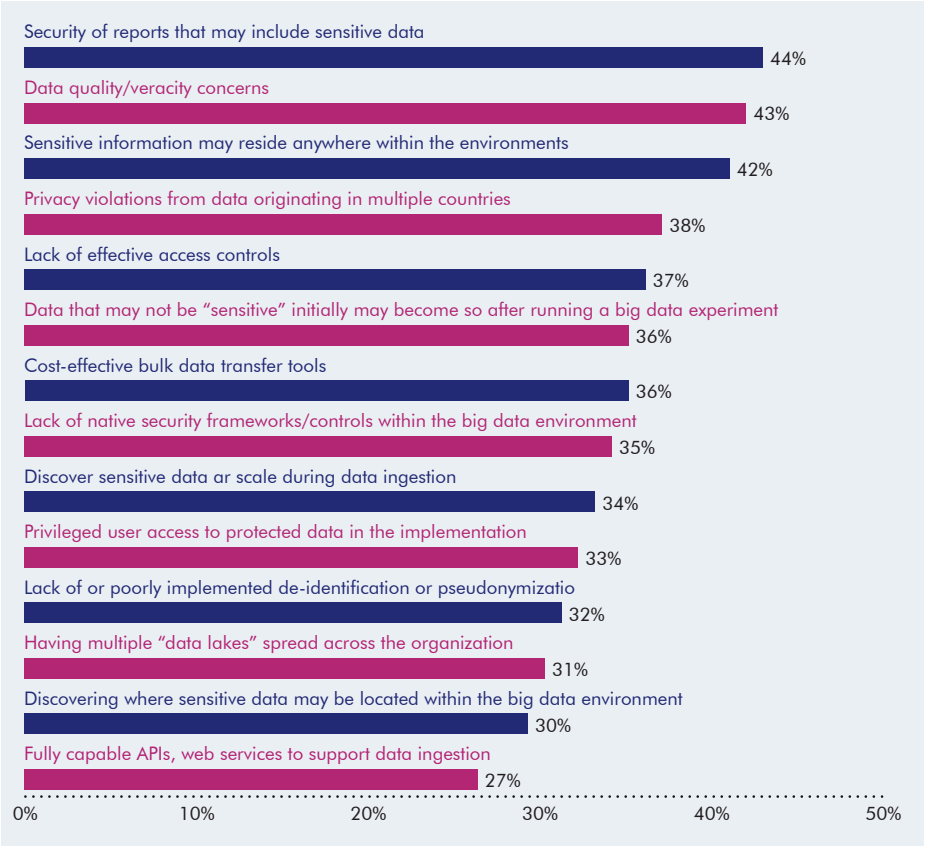
Девяносто девять процентов компаний, участвующих в этом исследовании, ощущают некоторый уровень безопасности, когда направляют больше данных в эти новые развертывания технологий, а 66% чувствуют себя защищенными или крайне защищенными. Респонденты из США чувствовали себя еще более защищенными, чем их коллеги во всем мире, при этом 78% чувствовали себя в полной или экстремальной безопасности (см. рис. 21).

Рис. 21 – Уровень безопасности при развертывании новых технологий
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

«Наряду с обеспечением новых возможностей реализации новых технологий, цифровизация создает и новые проблемы безопасности»

Проблемы безопасности больших данных

Сто процентов респондентов обеспокоены безопасностью данных в средах хранения больших данных. Основные проблемы безопасности больших данных связаны с безопасностью отчетов, качеством данных и распространенностью конфиденциальных данных. Проблемы обнаружения данных не воспринимаются как главные проблемы. Обнаружение конфиденциальных данных в масштабе во время приема данных составило 34%, а обнаружение того, где конфиденциальные данные могут находиться в среде больших данных, составило всего 30% (см. Рис. 22).



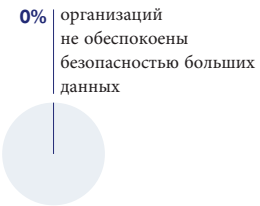


Рис. 22 - Проблемы безопасности больших данных
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Ведущие методы для решения проблем безопасности больших данных включают более строгую аутентификацию и шифрование или токенизацию данных. Несмотря на то, что усиленная аутентификация и шифрование важны для повышения безопасности больших данных в целом, эти меры напрямую не устраняют вышеупомянутые проблемы безопасности отчетов и качества данных. Кроме того, обнаружение и классификация конфиденциальных данных занимает последние места в иерархии решений для защиты больших данных.

Проблемы безопасности Интернета вещей

Основные проблемы безопасности IoT отметили 99% процентов респондентов, имеющих проблемы с безопасностью данных IoT, включают атаки на устройства, нехватку квалифицированного персонала и шифрование/токенизацию. Кроме того, выявление и обнаружение конфиденциальных данных, генерируемых устройствами IoT, было четвертым среди критических проблем - 27% (см. рис. 23). Аутентификация с использованием цифровой идентификации, шифрование данных и защита от вредоносных программ являются адекватными ответами для решения основных проблем безопасности IoT. По мере развертывания устройств IoT управление ключами приобретает все большее значение для эффективной реализации безопасности идентификации и шифрования данных на устройствах IoT.

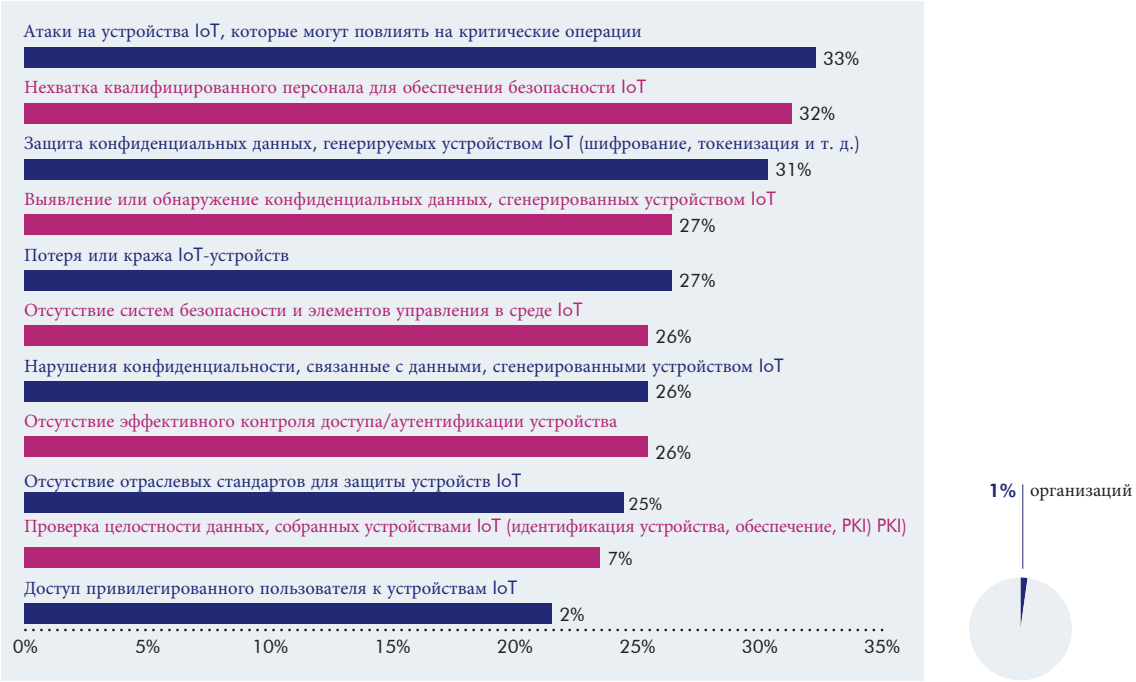
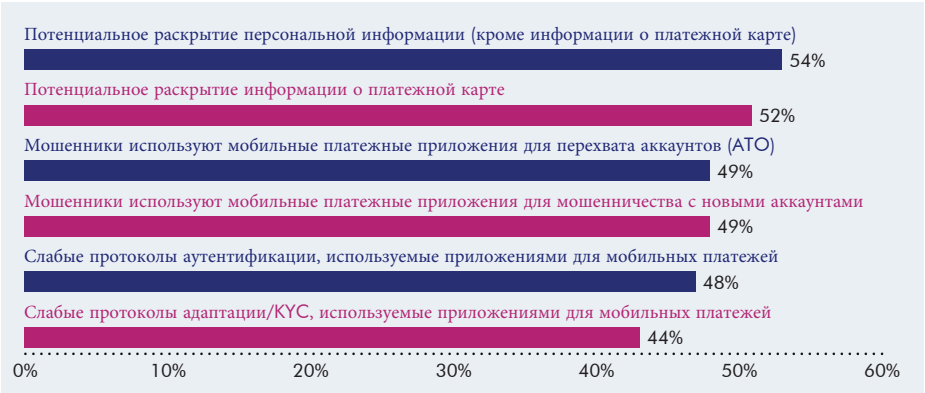


Рис. 23 - Проблемы безопасности Интернета вещей
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

«По мере развёртывания IoT-устройств управление ключами становится все более важным для эффективной реализации защиты идентификационных данных и шифрования на IoT-устройствах».

Проблемы безопасности мобильных платежей

Девяносто девять процентов респондентов имеют по крайней мере некоторые проблемы безопасности данных в области мобильных платежей. Обнаружение информации, позволяющей установить личность (PII), и раскрытие информации о платежной карте являются главными проблемами (см. рис. 24). Рассматривается множество широкомасштабных решений по обеспечению безопасности мобильных платежей. Главными среди них являются шифрование данных учетной записи, управление паролями, безопасные/зашифрованные протоколы беспроводной сети и экраны блокировки.



1% организаций не заботятся о безопасности приложений по мобильным платежам

Рис. 24 - Проблемы безопасности мобильных платежей
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Проблемы безопасности контейнеров

Учитывая относительную недостаточное совершенство технологий безопасности, связанных с контейнерами, организации обеспокоены множеством различных проблем, поскольку они продолжают лучше понимать контейнеры и их безопасность, хотя 96% выражают некоторую озабоченность по поводу безопасности данных. Отсутствие сертификатов соответствия и нарушения конфиденциальности возглавляют список, за которыми следуют безопасность данных, хранящихся в контейнерах, и несанкционированный доступ к контейнерам (см. рис. 25). Шифрование, защита от вредоносных программ и цифровые подписи являются важными решениями, которые организации могут использовать при разработке контейнеров.

> Шифрование, защита от вредоносных программ и цифровые подписи являются важными решениями, которые могут использовать организации при внедрении контейнеров».

4% организаций не обеспокоены безопасностью данных контейнерных сред

Рис. 25 – Проблемы безопасности контейнеров/докеров
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Проблемы безопасности DevOps

Когда речь заходит о DevOps, 98% респондентов обеспокоены безопасностью данных среды DevOps. Организации больше всего обеспокоены неправильной практикой хранения ключей и сертификатов. Эта проблема также говорит о важности управления ключами и использования аппаратных модулей безопасности. Другие главные проблемы безопасности DevOps –воздействие внешних DDoS-угроз и общая безопасность облачной инфраструктуры в среде DevOps (см. рис. 26). Ненадлежащее исправление, профилактические обновления и небезопасное использование API имеют на удивление низкий уровень в этой иерархии, и это может означать, что ответственность за эти проблемы ложится на производство, а не на разработчиков Рассматривается множество различных подходов для устранения проблем безопасности DevOps, обусловленных непрерывными процедурами безопасности производственной среды, шифрованием, токенизацией и постоянным обучением сотрудников, отвечающих за DevOps.

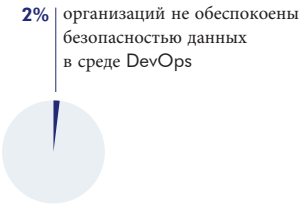
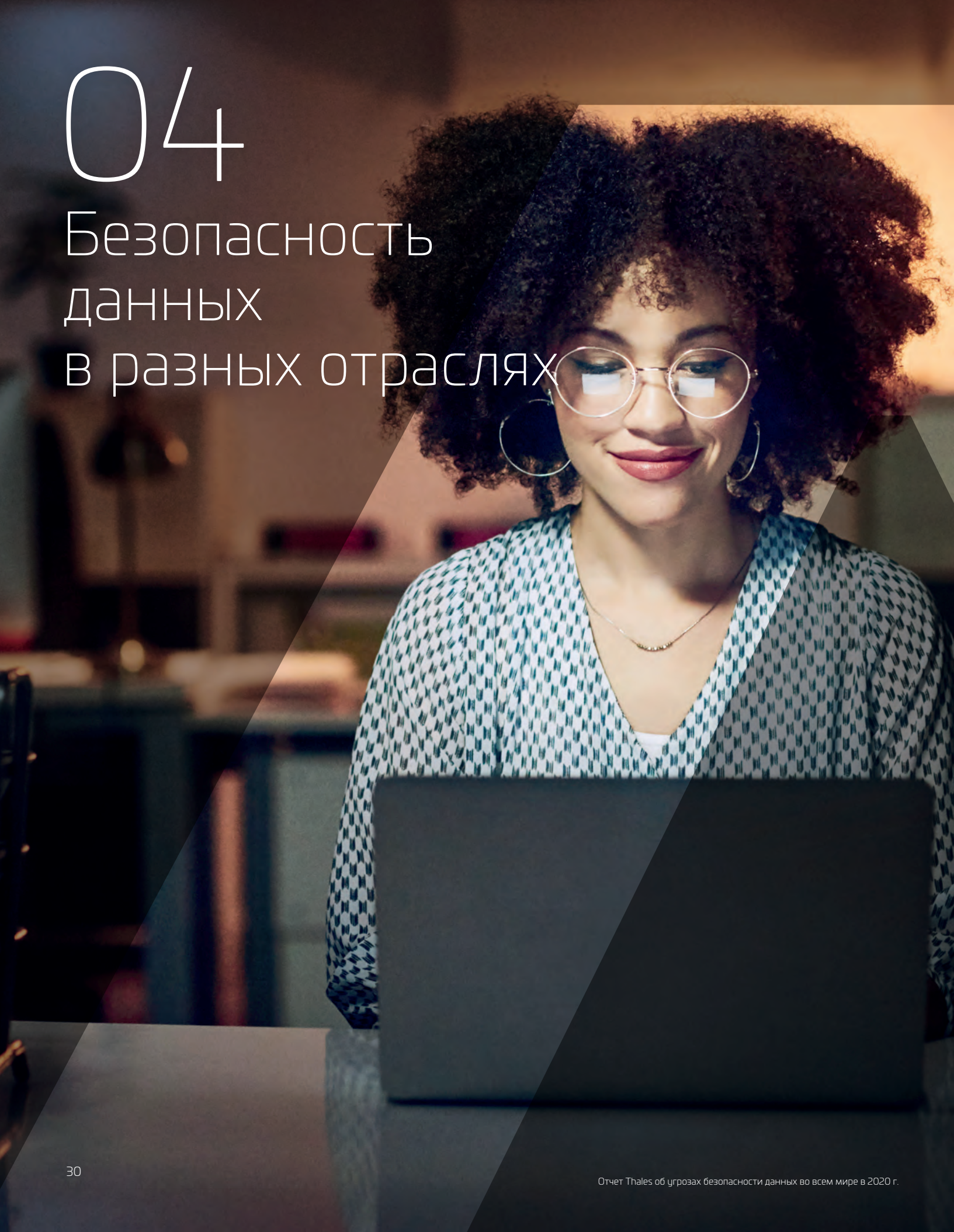


Рис. 26 – Проблемы безопасности DevOps
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

04 Безопасность данных в разных отраслях



Разница в подходе к безопасности данных в зависимости от отрасли

В отчете Thales об угрозе безопасности данных на 2020 год приведены также результаты исследований, в каком аспекте предприятия, компании и организации различных отраслей рассматривают и воспринимают безопасность данных. Секторы государственного управления, финансовых услуг, здравоохранения и розничной торговли в различной степени овладевают цифровизацией и понимают связанные с ней проблемы безопасности.

Организации в каждом из секторов сообщают о несколько разных позициях в их DX-развитии. Интересно, что федеральные государственные организации считают себя наиболее продвинутыми: 49% респондентов из государственного управления сообщают, что их организации либо агрессивно ведут подрыв рынков, в которых участвуют, либо внедряют цифровые технологии, которые обеспечивают большую гибкость предприятия. В секторе здравоохранения за этим внимательно следят 47%, в розничной торговле – 45%, в финансовых услугах – 30% предприятий.

98%

респондентов обеспокоены безопасностью данных своей среды DevOps.

Отрасли с более высокой степенью цифровизации могут подвергаться большей угрозе. Пятьдесят четыре процента респондентов из сектора финансовых услуг в этом году столкнулись с утечками данных или не прошли аудит соответствия; за ними следуют государственное управление (52%), розничная торговля (49%) и здравоохранение (37%).

Отрасли, которые в большей степени перешли на цифровые стандарты, часто имеют более строгие нормативные требования и требования к безопасности данных, что также является движущей силой для DX. В некоторых случаях организации государственного управления вынуждены выполнять определенные цели или обновления системы, для оплаты которых могут потребоваться дополнительные средства. Хотя и государственное управление иногда отстает в расходах на DX, такие законы могут помочь ускорить переходный период. Например, в США организации государственного управления испытывают сильное давление, направленное на закрытие старых центров обработки данных и перенос приложений на облачные и виртуальные серверы.

Задачи для организаций в различных отраслях усложняются тем, что они всё больше своих данных хранят в облачных средах. Девяносто девять процентов организаций, предоставляющих финансовые услуги, хранят данные в облаке. Девяносто восемь процентов предприятий розничной торговли и здравоохранения и 97% государственного управления соответственно хранят данные в облаке (см. рис. 27).

Рис. 27 – Данные в облаке с распределением по отраслям

Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Важно, что большая часть этих облачных данных является конфиденциальной. По оценкам, 51% данных в облаке являются конфиденциальными для сектора финансовых услуг и 50% для здравоохранения Государственное управление и розничная торговля имеют несколько более низкие показатели конфиденциальных данных в облаке – примерно 47% и 44% соответственно (см. рис. 28).

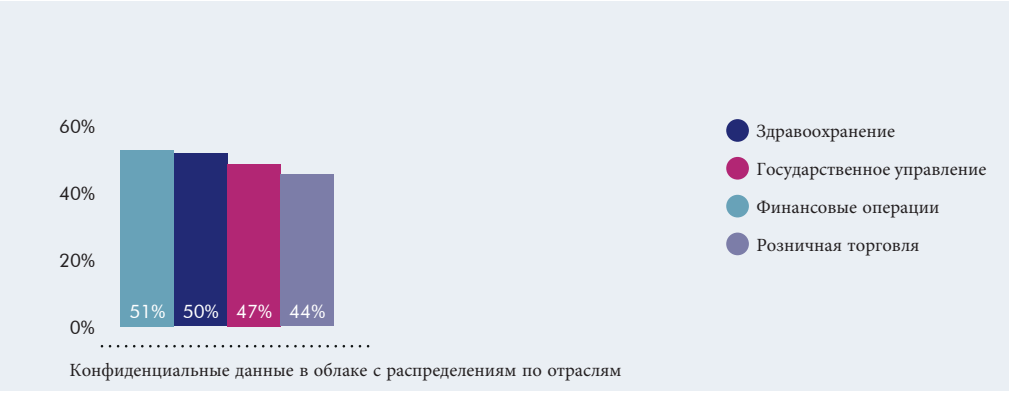


Рис. 28 – Конфиденциальные данные в облаке с распределениям по отраслям
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г

Организации тратят всё больше денег на безопасность данных, при этом расходы предприятий финансовых услуг увеличиваются больше всего на 55%, за ними следуют розничная торговля, государственное управление и здравоохранение (см. рис. 29). Средний процент бюджета безопасности, направляемый на защиту данных, различается в зависимости от отрасли, наибольший имеют финансовые услуги – 16,1%. По безопасности данных здравоохранение занимает второе место (15,9%), за ним следуют государственное управление (15,2%) и розничная торговля (15,0%).

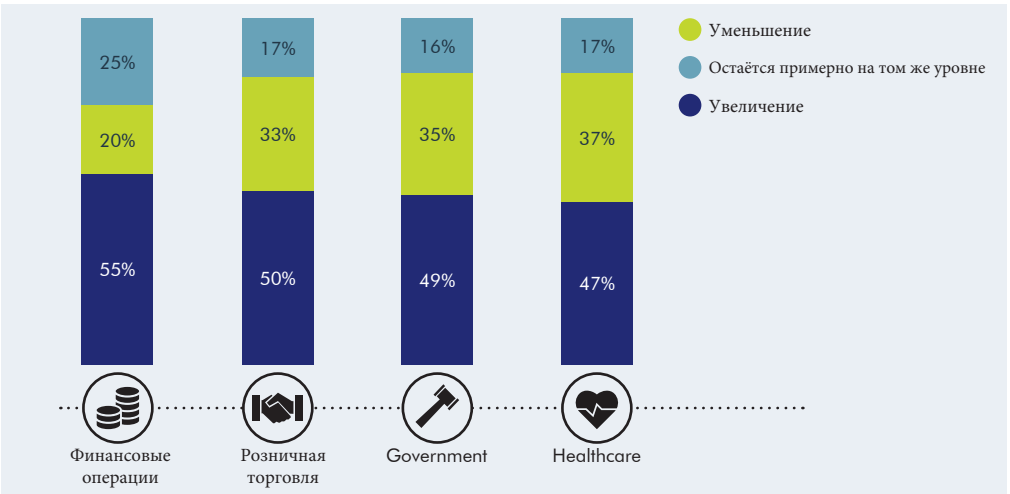


Рис. 29 – Средства, направляемые на обеспечение безопасности данных с распределением по отраслям
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

55%

Организации тратят больше денег на безопасность данных, при этом в отрасли финансовых операций они составляют больше всего (55%)

Разрыв между восприятием безопасности данных и реальностью распространяется на все отрасли.

Что касается сектора государственного управления, необходимо иметь в виду, что некоторые типы безопасности включены в расходы по другим решениям и, следовательно, могут не отслеживаться как чистые расходы на безопасность. Например, мониторинг сети, управление конфигурацией, контроль доступных серверных портов и т. д. важны для надежного обеспечения безопасности той или иной организации. Но многие из них не учитывают это как часть своего бюджета на безопасность. Можно обнаружить также и инвестиции, направленные на повышение безопасности организаций государственного управления, программное обеспечение и связанные с ними сервисы, за которыми следуют менеджмент IoT и мобильное управление.

Компании розничной торговли компании чувствуют себя наиболее защищенными с их новыми технологиями развития, 71% респондентов этого сектора оценивают свои ощущения как безопасные или очень безопасные. То же самое относится и к предприятиям финансовых операций (70%) (см. рис. 30).

Рис. 30 – Новые и экстремально безопасные отрасли индустрии
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

> «Реалии безопасности и шифрования данных не становятся проще. Отрасли также должны быть готовы к тому, что квантовые вычисления могут оказать влияние на безопасность данных в ближайшей перспективе».

Как и в случае глобального опроса, представители различных отраслей недостаточно обеспокоены проблемами, создающими наибольшую опасность. Уровень шифрования и токенизации во всех отраслях остается низким.

В то время как сетевая безопасность долгое время была основным направлением деятельности органов государственного управления, в данный момент разные организации прилагают одинаковые усилия для обеспечения безопасности данных и приложений.
И все же реализация многогранных подходов к безопасности нелегка. Агентства нуждаются в инструментах, помогающих им справляться с более сложными задачами, включая те, которые способны охватить унаследованные от прежних систем локальные потребности, а также современные облачные, ориентированные на современные методики технологии с такими решениями, как шифрование и токенизация. По мере роста пограничных вычислений и искусственного интеллекта эта сложность будет только увеличиваться.
Розничная торговля имеет самую низкую скорость шифрования конфиденциальных данных - 54%, т. е. 46% конфиденциальных данных вообще не защищены никаким шифрованием. Кроме того, только 45% компаний розничной торговли защищают конфиденциальные данные с помощью токенизации.
Организации здравоохранения имеют самый высокий уровень шифрования и токенизации конфиденциальных данных (59% и 49% соответственно), хотя эти уровни также считаются низкими (см. рис. 31).

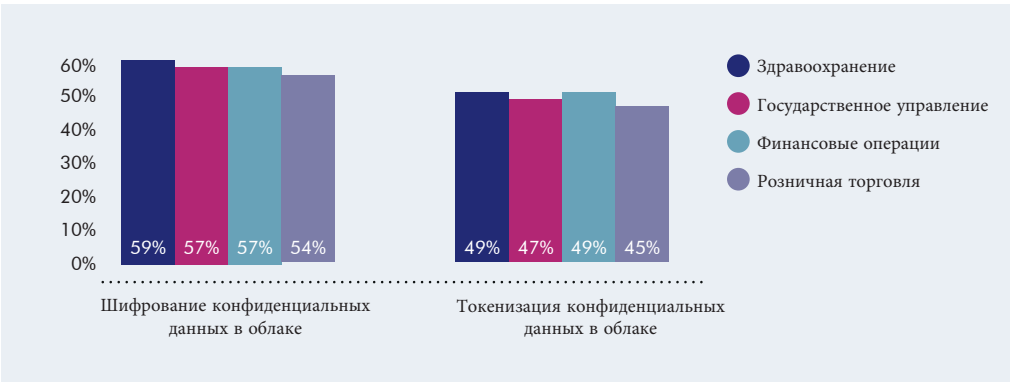


Рис. 31. Безопасность конфиденциальных данных в облаке по отраслям
Источник: Отчет Thales об угрозах безопасности данных в 2020 г., IDC, ноябрь 2019 г.

Реалии безопасности и шифрования данных не становятся проще. Отрасли также должны быть готовы к тому, что квантовые вычисления могут оказать влияние на их безопасность данных в ближайшей перспективе.
В течение ближайших 1-5 лет 77% предприятий финансовых служб ожидают, что на них повлияет квантовая криптография, за ними следует розничная торговля (75%) и здравоохранение и государственное управление (73%).
Отрасли обеспокоены тем, что квантовые вычисления откроют доступ к конфиденциальным данным. Предприятия, осуществляющие финансовые операции, обеспокоены больше всего, при этом 94% из них выражают озабоченность по поводу способности потенциала квантовых вычислений открыть доступ к данным, а 46% - крайнюю обеспокоенность.
Обеспокоены девяносто два процента государственных организаций управления, за ними следуют розничная торговля (90%) и здравоохранение (88%).

05 РУКОВОДСТВО И ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНОГО ЦЕНТРА ДАННЫХ IDC

Необходимость внедрения более разумных подходов к безопасности данных

Инвестиции в современные, гибридные и многооблачные инструменты защиты данных, которые обеспечивают работу модели совместной ответственности, оправдывают себя. Конфиденциальные данные хранятся в облаке. Организациям следует сосредоточиться на решениях, которые могут упростить окружение безопасности данных и снизить сложность в нескольких облаках, устаревших средах и современных технологиях цифровизации. Модель совместной для организаций ответственности напоминает, что они не могут полагаться на поставщиков услуг в отношении мер безопасности данных. Кроме того, компании должны учитывать все элементы безопасности данных, находящиеся под их контролем, такие, как идентификация, шифрование (как при передаче, так и в неактивном состоянии), управление ключами, токенизация и предотвращение утраты данных.

Рассмотрение модели с нулевым доверием для защиты данных. Организации по-прежнему сосредоточены на сетевой безопасности, поскольку они стремятся контролировать доступ к данным. Безопасность данных выходит за рамки традиционного процесса, будь то облачные технологии, виртуальные среды, центры обработки данных или другие технологии DX. Этим средам данных требуется более устойчивая модель с нулевым доверием, которая не исключает защиту данных как чью-либо проблему, но вынуждает организации предоставлять наименее привилегированный доступ к данным. За счет уменьшения размеров объекта атаки и ужесточения доступа к данным с использованием таких подходов, как шифрование данных в неактивном состоянии, конфиденциальные данные защищены не только от внешних субъектов, но и от злонамеренных инсайдеров, что значительно снижает риск внутренней угрозы. Необходимо обратите внимание та то, что 82% респондентов чувствовали себя уязвимыми для внешних угроз; 67% – для внутренних. Оба этих вектора должны быть устранены.

Повышение внимания к решениям для обнаружения данных и централизации управления ключами для усиления безопасности данных. Проблемы безопасности данных развиваются по мере того, как расширяются границы использования сред больших данных, устройств IoT, мобильных платежей, контейнеров и сред DevOps. Больший упор на обнаружение конфиденциальных данных в этих средах, а также в существующих средах усиливает позицию безопасности данных, определяя, где находятся конфиденциальные данные и как получить к ним доступ. Кроме того, шифрование конфиденциальных данных имеет решающее значение, и организации должны активно управлять ключами, чтобы упростить шифрование в других сложных средах. В облачных средах, где включено собственное шифрование, необходимо также использовать собственные API-интерфейсы ключей для обеспечения ответственности и контроля данных.

Влияние квантовых вычислений на криптографию не за горами. Обеспечение безопасности данных не упрощается, поскольку высокая производительность квантовых вычислений увеличивает степень возможного раскрытия данных. Организации должны начать планировать свою инфраструктуру и настройки управления ключами, чтобы противостоять фундаментальным изменениям в криптографии, вызванным квантовыми вычислениями. Инвестируя в новую инфраструктуру, надо проверить, что они обеспечивают гибкость в шифровании и будут поддерживать новые стандарты NIST по мере их появления.

Сосредоточиться на правильных векторах угрозы. Да, отрицательные персонажи игры в этой области ежедневно совершенствуют свои методы. В ответ на эти вызовы должны постоянно совершенствоваться специалисты по безопасности. Будьте осторожны с чрезмерным количеством и объемом расчетов как внутри поставщиков услуг и подрядчиков, так и за их пределами.

Решения по защите данных, особенно шифрование, имеют ключевое значение для сохранения бдительности в реалиях сегодняшних рисков. Даже несмотря на то, что CSO и CISO переносят фокус своего внимания и бюджеты с традиционной сетевой безопасности на данные, приложения и удостоверения, они не должны проявлять излишнюю доверчивость, полагая, что они являются менее уязвимыми. Организации должны разработать меры безопасности данных для защиты современного IT-окружения, когда данные переносятся в облако. Эта современная эволюция основана на шифровании.

Быстрое внедрение облачных вычислений снизило эффективность локальных мер защиты контента. Наши данные живут в облаке; таким образом, многооблачная реальность спровоцировала рост не зависящей от местоположения безопасности SaaS-контента. Для государственных учреждений, в частности, локальные решения для обеспечения безопасности больше не являются жизнеспособным вариантом для защиты облачных современных предприятий и приложений. Результатом этого является значительное усложнение задачи. Хотя выбор решений, подходящих для каждой новой облачной среды, является лучшим подходом, проблема сложности будет решаться с помощью точно такой же сложности продукта. Создание согласованного подхода к защите данных с несколькими нагрузками и несколькими средами, которые защищают данные независимо от того, где они находятся и где они могут находиться, безусловно, является наилучшей практикой. Внедрение такой платформы напоминает случай, когда родители интересуются, где их дети, только после наступления темноты; убедитесь, что вы можете ответить «да» на вопрос: «Вы знаете, где находятся ваши ключи?»

THALES

Arboretum Plaza II, 9442 Capital of Texas
Highway North, Suite 100, 78759 Austin, TX USA

+1 888 744 4976
+1 954 888 6200

>thalesgroup.com <

thalesesecurity.com/DTR

#2020DataThreat

Отчет Thales об угрозах безопасности данных во всем мире в 2020 г.