Пять самых распространенных ошибок в области защиты данных, которых следует избегать

Узнайте, как укрепить систему безопасности

IBM **Security**

Содержание

Защита данных должна быть приоритетной задачей для компаний, и на это есть причина.

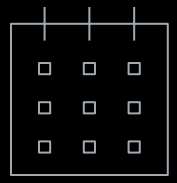
В условиях, когда современный ИТ-ландшафт становится все более децентрализованным и сложным, важно четко понимать, что многие нарушения безопасности можно предотвратить. Компании сталкиваются с разными проблемами в области безопасности, но часто делают одинаковые ошибки в процессе обеспечения безопасности данных. Более того, многие руководители часто считают такие ошибки обычными бизнес-практиками.

Успешному проведению кибератак способствуют как внутренние, так и внешние факторы, включая:

- Ослабление периметра сети
- Расширение контуров атаки вследствие повышения сложности ИТ-сред
- Растущие требования, которые облачные услуги предъявляют к методикам обеспечения безопасности
- Все более изощренный характер киберпреступлений
- Нехватка устойчивых навыков в области кибербезопасности
- Недостаточная осведомленность сотрудников о рисках, связанных с безопасностью данных

8,19 млн долларов США

Средний ущерб от несанкционированного доступа к данным в США в 2019 году[1]



245 дней

Среднее время выявления и устранения последствий утечки данных в США в 2019 году[1]

Насколько эффективна ваша методика обеспечения безопасности данных?

Давайте подробнее рассмотрим пять самых распространенных ошибок в области защиты данных, которые делают организации уязвимыми к потенциальным атакам и которых можно избежать.

Быстрое реагирование на официальные требования

Централизация безопасности

Определение принадлежности

Оценка уязвимостей

Приоритизация операций

Подводный камень 1

Формальный подход к соблюдению требований

Соблюдение требований не является гарантией безопасности. У организаций, которые тратят все силы на проведение аудита и получение сертификатов, может возникнуть обманчивое ощущение безопасности. Многие крупные утечки данных происходили в компаниях, которые отвечали всем нормативным требованиям на бумаге. В следующих примерах показано, каким образом чрезмерное увлечение соблюдением нормативных требований может привести к снижению уровня безопасности:

Неполный охват
Компании часто бросают все усилия на исправление ошибок конфигурации баз данных и устаревших политик управления доступом незадолго до ежегодного аудита. Оценку уязвимостей и рисков следует выполнять на постоянной основе.

Минимальные усилия
Многие компании адаптируют решения для обеспечения безопасности данных только с целью соблюдения требований законодательства или бизнес-партнеров. Принцип "давайте сделаем минимум необходимого и вернемся к работе" может препятствовать эффективному обеспечению безопасности. Эффективная защита данных – это марафон, а не спринт.

Снижение срочности
Компании могут перестать уделять внимание средствам управления после окончательного формирования регулятивных законов, таких как закон Сарбейнса-Оксли (SOX) и Общеевропейский регламент о защите персональных данных (GDPR). Со временем многие руководители начинают меньше заботиться о конфиденциальности, безопасности и защите регламентируемых данных, однако риски и расходы, связанные с нарушением нормативных требований, никуда не деваются.

1,4 в день

Согласно статистике за 2019 год, утечки медицинских данных происходили 1,4 раза в день, несмотря на требования закона HIPAA (Закон США о переносимости и подотчетности в сфере медицинского страхования).[2]

Недостаточное внимание нерегламентируемым данным
Такие ресурсы, как интеллектуальная собственность, могут создавать дополнительные риски для организации в случае их потери или передачи неуполномоченному персоналу. Обращая внимание только на соблюдение требований, организации могут упустить из виду ценные данные, оставив их без надлежащей защиты.

Решение

Исходите из того, что соблюдение требований является только отправной точкой, а не целью

Для обеспечения безопасности данных важно разработать стратегические программы, предлагающие согласованную защиту критически важных бизнес-данных – не стоит ограничиваться просто соблюдением нормативных требований.

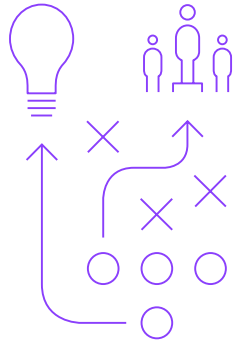
Программы обеспечения безопасности и защиты данных должны включать следующие базовые практики:

- **Поиск и классификация конфиденциальных данных** в локальных и облачных хранилищах данных.
- **Оценка рисков** с помощью контекстного анализа.
- **Защита конфиденциальных данных** с помощью шифрования и гибких политик управления доступом.
- **Мониторинг доступа к данным и схем использования** для оперативного выявления подозрительных действий.
- **Реагирование на угрозы** в режиме реального времени.
- **Упрощение соблюдения требований** и составления отчетности.

Кроме того, следует учитывать правовую ответственность, связанную с соблюдением нормативных требований, возможные потери бизнеса и потенциальный ущерб от этих потерь помимо штрафов за несоблюдение требований.

И наконец, используйте комплексный подход для оценки рисков и ценности данных, которые предстоит защитить.

Рассматривайте соблюдение требований как возможность внедрить инновации и повысить стандарты обеспечения безопасности для поддержки бизнеса.



Подводный камень 2

Отсутствие понимания роли централизованной защиты данных

Без более широкого подхода к соблюдению нормативных требований, охватывающего конфиденциальность и безопасность данных, руководители организаций не смогут в полной мере оценить важность согласованной защиты данных в масштабах предприятия.

В организациях с гибридными мультиоблачными средами, которые постоянно изменяются и расширяются, новые типы источников данных появляются чуть ли не ежедневно, что значительно усложняет управление конфиденциальными данными.

Руководителям компаний, которые развивают свои ИТ-инфраструктуры, не всегда удается точно оценить риски, связанные с изменяющимися контурами атаки. Им не хватает прозрачности и контроля, поскольку конфиденциальные данные циркулируют в разрозненной ИТ-среде, уровень сложности которой постоянно растет. Отказ от внедрения комплексных средств управления конфиденциальностью, безопасностью и защитой данных – особенно в сложных средах – может оказаться очень дорогостоящей ошибкой.

В разрозненных средах решения для обеспечения безопасности могут вызывать дополнительные проблемы. Например, центры оперативного реагирования (SOC) и решения для управления информацией и событиями безопасности (SIEM) могут игнорировать ценную информацию, полученную из решения для обеспечения безопасности данных. Аналогичным образом, недостаточно эффективное взаимодействие между специалистами, процессами и инструментами в сфере обеспечения безопасности может затруднить достижение успеха любой программы безопасности.

Шифрование, управление непрерывностью бизнеса, интеграция безопасности в процесс разработки программного обеспечения (DevSecOps) и обмен аналитическими данными об угрозах могут помочь уменьшить ущерб от несанкционированного доступа к данным.[1]

Решение

Узнайте, где именно находятся конфиденциальные данные, включая локальные и облачные хранилища

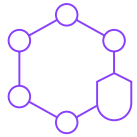
Защита конфиденциальных данных должна обеспечиваться в рамках более широких мер безопасности. Помимо наглядного представления размещения конфиденциальных данных, важно знать, когда и как осуществляется доступ к данным – даже в том случае, если эта информация быстро изменяется. Кроме того, вы можете интегрировать аналитику и политики защиты данных в общую программу безопасности, обеспечив тем самым тесное взаимодействие между технологиями. В этом процессе может помочь решение для обеспечения безопасности данных, охватывающее разнородные среды и платформы.

Когда лучше всего интегрировать защиту данных с другими средствами управления в составе более комплексных методик обеспечения безопасности? Вот несколько признаков того, что ваша организация может быть готова сделать следующий шаг:

Риск потери ценных данных
Ценность персональных, конфиденциальных и собственных данных организации настолько высока, что их потеря может поставить под вопрос жизнеспособность вашего бизнеса.

Нормативное регулирование
В соответствии с законодательными требованиями ваша организация обязана собирать и хранить такие данные, как номера кредитных карт, сведения о платежах и персональная информация.

Защита конфиденциальных данных должна обеспечиваться в рамках более широких мер безопасности.



Недостаточный контроль за безопасностью
В условиях роста организации могут сталкиваться с трудностями при отслеживании и защите всех конечных точек в сети, включая облачные экземпляры. К примеру, есть ли у вас четкое представление о том, где, когда и как хранятся и используются данные в локальных и облачных хранилищах данных?

Неадекватная оценка
Ваша организация переняла фрагментарный подход, в рамках которого отсутствует четкое понимание расходов на меры по обеспечению безопасности. Например, есть ли у вас процессы для точного измерения окупаемости инвестиций (ROI) с точки зрения ресурсов, выделяемых для минимизации рисков безопасности данных?

В любой из этих ситуаций рекомендуется обратить внимание на навыки и решения в области безопасности, необходимые для интеграции защиты данных в существующие методики обеспечения безопасности.

Подводный камень 3

Проблемы при определении ответственных за данные

Несмотря на очевидную важность безопасности данных, во многих компаниях нет ответственных за защиту конфиденциальной информации. Поиск тех, кто фактически несет ответственность часто начинается только на этапе расследования инцидентов аудита или безопасности данных.

Если руководители высшего обратятся к директору по информационным технологиям (CIO), он может ответить: "Мы обеспечиваем работу ключевых систем. Спросите кого-нибудь из ИТ-специалистов". ИТ-специалисты часто отвечают за несколько баз данных с конфиденциальной информацией в условиях ограниченного бюджета на безопасность.

Как правило, подчиненные директора по информационной безопасности (CISO) не несут прямой ответственности за данные, циркулирующие по всей бизнес-среде. Они могут давать советы руководителям бизнес-направлений (LOB), однако во многих компаниях никто не несет непосредственную ответственность за сами данные. Данные являются одним из самых ценных ресурсов любой организации. Тем не менее, защита конфиденциальных данных без назначения ответственных лиц может оказаться сложной задачей.

74%

опрошенных организаций отметили, что нехватка навыков по кибербезопасности повлияла на их работу.[3]

"В 2018 году в штате 67,9% опрошенных компаний был директор по управлению данными (CDO). Однако, его должностные обязанности оставались слишком размытыми".[4]

Отчет NewVantage Big Data and AI Executive Survey 2019, Сводные результаты для руководителей

Ознакомиться с исследованием →

Решение

Наймите директора по управлению данными (CDO) или специалиста по защите данных (DPO), который будет отвечать за состояние и безопасность конфиденциальных и критически важных ресурсов

В сложных ИТ-средах важно отслеживать:

Общие данные, используемые несколькими подразделениями

Данные, расположенные в гибридных мультиоблачных инфраструктурах

Данные на мобильных устройствах

Директор по управлению данными (CDO) или специалист по защите данных (DPO) может взять на себя эти обязанности. Известно, что компаниям, которые базируются в Европе или ведут бизнес с субъектами данных из ЕС, регламент GDPR предписывает назначить DPO. Данное требование отражает тот факт, что ценность конфиденциальных данных (в данном случае персональной информации) распространяется за пределы LOB, в котором эти данные используются. Кроме того, это требование делает акцент на том, что компании должны назначить сотрудников, отвечающих за ресурсы данных. При выборе CDO или DPO рекомендуется учитывать следующие цели и обязанности:

Технические знания и значение для бизнеса
Оценка риска и подготовка практического экономического обоснования инвестиций в средства обеспечения безопасности, которое будет понятно руководителям, не обладающим техническими навыками.

Стратегическая реализация
Прямой технический план внедрения средств контроля для обнаружения, реагирования и безопасности данных.

Руководство программой соблюдения требований
Понимание нормативных требований и умение задействовать средства обеспечения безопасности для их соблюдения.

Мониторинг и оценка
Мониторинг картины угроз и измерение эффективности программы защиты данных.

Гибкость и масштабирование
Он должен знать, когда и как скорректировать стратегию обеспечения безопасности данных. Например, политики управления доступом к данным и их использования может потребоваться распространить на новые среды путем интеграции новых инструментов, обладающих более широкими возможностями.

Разделение труда
Определение ожиданий от провайдеров облачных услуг в отношении соглашений об уровне обслуживания (SLA) и обязанностей, связанных с рисками безопасности данных и устранением уязвимостей.

План реагирования на утечки данных
И наконец, требуется готовность играть ключевую роль в разработке стратегического плана по нейтрализации утечек и реагированию на них.

CDO или DPO должен способствовать развитию сотрудничества в области безопасности данных между коллективами и в масштабе организации, поскольку корпоративные данные можно защитить только совместными усилиями. Такое сотрудничество помогает CDO или DPO контролировать программы и средства защиты конфиденциальных данных.

Подводный камень 4

Недостаточное внимание к известным уязвимостям

Многие громкие случаи утечки корпоративных данных произошли в результате использования известных уязвимостей, которые не были нейтрализованы после выпуска исправлений. Недостаточно оперативное устранение известных уязвимостей подвергает данные вашей организации дополнительным рискам, поскольку киберпреступники активно ищут простые точки входа.

Однако, для многих компаний быстрое применение исправлений является настоящей проблемой вследствие сложностей координирования работы коллективов, отвечающих за ИТ, безопасность и операционную деятельность. Более того, во многих случаях требуется тщательное тестирование исправлений, поскольку они не должны нарушать процессы или открывать дорогу новым уязвимостям.

В облачных средах иногда сложно определить необходимость исправления компонентов приложений или услуг, предоставляемых по договору. Даже в случае обнаружения уязвимости в услуге ее пользователи часто не обладают контролем над процессом устранения уязвимостей на уровне поставщика.

51%

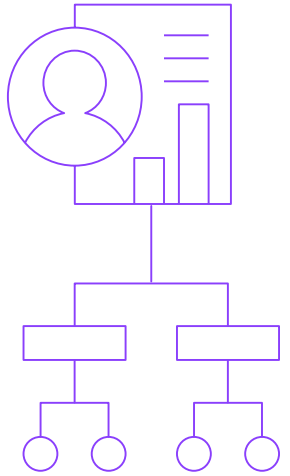
утечек данных, зарегистрированных в 2019 году, были вызваны вредоносными атаками. Вредоносные атаки – это самая распространенная и дорогая причина утечек.[1]

Решение

Организуйте эффективную программу управления уязвимостями на основе подходящей технологии, которая сможет обеспечить ее развитие

Как правило, управление уязвимостями предусматривает работу в следующих направлениях:

- Ведение точного реестра и контрольного состояния ресурсов данных.
- Проведение частых сканирований всей инфраструктуры, включая облачные ресурсы, на предмет уязвимостей.
- Приоритизация действий по устранению уязвимостей с учетом вероятности их использования и потенциального влияния на бизнес.
- Включение требований к управлению уязвимостями и реагированию на них в SLA со сторонними поставщиками услуг.
- Маскировка конфиденциальных и персональных данных всегда, когда это возможно. Для этой цели применяются три методики: шифрование, токенизация и обезличивание.
- Внедрение подходящих средств управления ключами шифрования, включая безопасное хранение и обновление ключей шифрования.



Даже в рамках зрелой программы управления уязвимостями невозможно добиться идеальных результатов. Поскольку злоумышленники могут проникнуть даже в хорошо защищенные среды, вам необходим другой уровень защиты данных. Подходящий комплект методик и средств шифрования данных поможет надежно защитить ваши данные от новых и неизвестных угроз.

Подводный камень 5

Проблемы приоритизации и использования мониторинга действий с данными

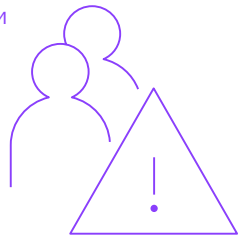
Мониторинг доступа и использования данных является важной частью любой стратегии обеспечения безопасности данных. Руководители компаний должны обладать точной информацией о том, кто, как и когда использует данные. Мониторинг должен помогать определить, должны ли пользователи обладать доступом, является ли уровень доступа правильным и существует ли риск для предприятия.

Идентификационные данные привилегированных пользователей входят в число основных инструментов внутренних угроз.5 План защиты данных должен включать мониторинг учетных записей привилегированных пользователей, чтобы в режиме реального времени выявлять подозрительные или несанкционированные действия. Решение, обладающее возможностью предотвращать возможные вредоносные действия, должно выполнять следующие задачи:

- Блокирование и изоляция подозрительных действий в случае нарушений политик.
- Приостановка или завершение сеансов с аномальным поведением.
- Применение предопределенных потоков операций, соответствующих нормативным требованиям, во всех средах данных.
- Отправка практически применимых предупреждений в системы, отвечающие за ИТ-безопасность и операционную деятельность.

Средний ущерб от утечки данных во всем мире составляет

11,45 млн долларов США.[6]



Мы понимаем, насколько сложно обеспечить анализ информации о защите данных и соблюдении требований, а также своевременное и эффективное устранение потенциальных угроз. В условиях, когда авторизованные пользователи обращаются ко множеству источников данных, включая базы данных, файловые системы, среды мейнфреймов и облачные среды, объем данных для мониторинга и регистрации взаимодействий может показаться ошеломляющим. Главная трудность заключается во внедрении эффективных средств мониторинга, захвата, фильтрации, обработки и реагирования на огромный объем данных об операциях. Без подходящего плана ваша организация может не справиться с осмысленной обработкой информации об операциях – и тогда мониторинг действий с данными потеряет всякий смысл.

Решение

Разработайте комплексную стратегию обнаружения и защиты данных

Приступая к внедрению защиты данных, следует тщательно оценить размер и масштаб системы мониторинга, чтобы надлежащим образом учесть все требования и риски. Зачастую для этого требуется поэтапный подход с разработкой и масштабированием передовых методик на уровне всего предприятия. Более того, важно на начальных этапах этого процесса согласовать краткосрочные и долгосрочные бизнес-цели с заинтересованными лицами бизнеса и специалистами по ИТ.

Кроме того, следует обсудить технологии, необходимые для реализации ключевых инициатив. Например, если компания планирует открыть офисы в новом регионе, используя для этого комбинацию локальных и облачных хранилищ данных, то ваша стратегия защиты данных должна оценивать влияние этого плана на состояние безопасности данных и соответствия требованиям компании. К примеру, на принадлежащие компании данные могут распространяться новые требования безопасности данных и нормативные требования, такие как GDPR, Закон штата Калифорния о защите данных потребителей (CCPA), Общий закон Бразилии о защите данных, Lei Geral de Proteção de Dados (LGPD) и т. д.

Кроме того, рекомендуется расставить приоритеты и сосредоточить внимание на одном или двух источниках с наиболее конфиденциальными данными. Разработав для этих источников четкие и подробные политики защиты данных, вы сможете впоследствии распространить их на всю инфраструктуру.

Средний ущерб от хищения данных был на

95%

выше

в организациях без средств автоматизации защиты в 2019 году.[1]

5,16 млн долларов США **без автоматизации.**[1]

2,65 млн долларов США, **если были развернуты средства автоматизации.1**

Вам нужно автоматизированное решение для мониторинга действий с данными или файлами с расширенными аналитическими возможностями, которые помогут сосредоточиться на ключевых рисках и необычном поведении привилегированных пользователей. Помимо отправки автоматических предупреждений в случае обнаружения аномального поведения, решение мониторинга действий с данными или файлами должно предоставлять возможность быстрого реагирования на аномалии и отклонения от политик управления доступом к данным. Защитные действия должны включать динамическое маскирование или блокировку данных.

Разрабатывая планы мониторинга действий с данными и защиты данных, попытайтесь найти ответы на следующие вопросы:

- Какие два источника содержат наиболее конфиденциальные данные?
- Какие от пяти до десяти источников данных являются наиболее приоритетными после них с учетом объема конфиденциальных данных?
- Подвергаются ли отдельные конечные точки или облачные ресурсы более высоким рискам, связанным с данными?
- Допускается ли свободное перемещение конфиденциальных данных между локальными, гибридными и облачными средами?
- Каким пользователям предоставляется доступ к источнику данных и в каких условиях?
- Каких пользователей с высоким уровнем риска или привилегированных пользователей необходимо отключить или проверять более тщательно?
- Поддерживает ли мое решение для обеспечения безопасности данных мониторинг в режиме реального времени и автоматизированные средства защиты данных?
- Применяется ли мониторинг в режиме реального времени для отслеживания данных в файлах из хранилищ данных, таких как базы данных SQL, экземпляры Hadoop, платформы NoSQL и т. д.
- Охватывает ли мое решение для мониторинга хранилища данных в гибридных мультиоблачных средах и позволяет ли создавать настраиваемые отчеты, которые отправляются нужным людям в нужное время?
- Есть ли у меня средства анализа рисков и мониторинга с фильтрацией, способные эффективно определять приоритеты рисков, уязвимостей и действий по исправлению?

Чем точнее вы сможете описать требования к мониторингу и защите, тем с большей эффективность ваше решение будет применять доступные ресурсы обнаружения и реагирования.

Дальнейшие действия

Каким образом можно избежать этих подводных камней, связанных с безопасностью данных, когда все больше компаний внедряют гибридные мультиоблачные среды? В первую очередь необходимо тщательно проанализировать проблему и подготовить организацию к внедрению проактивного, комплексного подхода к обеспечению безопасности данных, где бы они ни находились.

Организациям со сложными и гибридными ИТ-средами необходим централизованный, комплексный подход к обеспечению безопасности данных. Важно добавить стратегии защиты данных, охватывающие всю инфраструктуру данных и все типы данных.

Дальнейшие действия по защите ценных корпоративных данных:

- Разработка стратегии обеспечения безопасности данных, способствующей достижению краткосрочных и долгосрочных целей в области бизнеса и технологий.
- Внедрение этой стратегии с привлечением подходящих специалистов, процессов и инструментов
- Планирование ресурсов с прицелом на масштабирование программы безопасности и нормативного соответствия по мере внедрения в организации современных технологий

Платформа IBM Security Guardium помогает организациям во внедрении более разумного и адаптивного подхода к защите критически важных данных, где бы они не находились. Узнайте, почему это решение может оказаться оптимальным выбором для вашей организации.

Подробнее: ibm.com/guardium.

Меньше 4 недель

Большинство организаций начинают получать отдачу от Guardium в течение первого месяца.[7]

Почему именно IBM Security?

IBM Security предлагает одно из самых передовых интегрированных портфолио продуктов в сфере корпоративной безопасности. Этот набор решений, использующих признанные во всем мире результаты исследований и разработок подразделения IBM X-Force®, обеспечивает аналитику в области безопасности, помогая организациям повысить комплексную защиту персонала, инфраструктуры, данных и приложений. Предлагает решения для управления идентификацией и доступом, защиты баз данных, разработки приложений, управления рисками, управления конечными устройствами, сетевой безопасности и т. д. Эти решения позволяют организациям эффективно управлять рисками и внедрять интегрированные средства защиты для мобильных, облачных, социальных и других бизнес-архитектур.

В состав IBM входят крупнейшие в мире организации в области аналитики безопасности, разработки и доставки.
IBM отслеживает более

60 миллиардов

событий, связанных с информационной безопасностью, более чем в 130 странах мира.

IBM принадлежит более 3700 патентов в сфере безопасности

IBM Восточная Европа/Азия
123112 Москва
Пресненская наб., 10

Веб-сайт IBM:
ibm.com

Настоящий документ актуален по состоянию на момент публикации и может быть изменен IBM в любое время. Не все предложения могут быть доступны во всех странах, в которых IBM ведет свою деятельность.

Приведенные в настоящей публикации сведения о производительности и примеры данных о заказчиках предназначены исключительно для иллюстрации. Фактические результаты могут отличаться в зависимости от конфигурации и условий работы. Пользователь несет ответственность за оценку и проверку взаимодействия любых других продуктов и программ с продуктами и программами IBM. ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ЛЮБЫЕ ГАРАНТИИ ТОВАРОПРИГОДНОСТИ, СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И ЛЮБЫЕ ГАРАНТИИ ИЛИ УСЛОВИЯ НЕНАРУШЕНИЯ ПРАВ. В отношении продуктов IBM действуют гарантии на основании положений и условий соглашений, в соответствии с которыми эти продукты предоставляются.

Заказчик принимает на себя ответственность за соблюдение законов и законодательных актов. IBM не предоставляет юридических консультаций, не заявляет и не гарантирует, что ее продукты или услуги обеспечивают соблюдение заказчиком законов и законодательных актов.

Заявление о добросовестной политике безопасности: в процесс обеспечения безопасности ИТ-систем входит защита систем и информации путем предотвращения, обнаружения и блокирования несанкционированного доступа к ним изнутри и снаружи организации. Несанкционированный доступ может привести к подмене, уничтожению, краже или неправомерному использованию информации, повреждению систем или их использованию в корыстных целях, в том числе для осуществления атак на других пользователей. Ни одну ИТ-систему или продукт нельзя считать абсолютно безопасными, равно как ни один продукт, услуга или мера безопасности не может обеспечить абсолютную эффективность в предотвращении несанкционированного доступа или неправомерного использования. Системы, продукты и услуги IBM предназначены для работы в комплексе законных мер по обеспечению безопасности, в который для максимальной эффективности обязательно будут входить другие процедуры и, возможно, будут задействованы другие системы, продукты и услуги. IBM НЕ ГАРАНТИРУЕТ, ЧТО СИСТЕМЫ, ПРОДУКТЫ И УСЛУГИ ПОЛНОСТЬЮ ЗАЩИЩЕНЫ ОТ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ ЛЮБОЙ ИЗ СТОРОН ИЛИ ЗАЩИТЯТ ВАШЕ ПРЕДПРИЯТИЕ ОТ ПОДОБНЫХ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ.

1 "Отчет по стоимости утечки данных, 2019 год" *Безопасность IBM.* databreachcalculator.mybluemix.net/executive-summary

2 "Статистика утечек медицинских данных". *HIPAA Journal. www.hipaajournal.com/healthcare-data-breach-statistics*

3 Джон Олтсик (Jon Oltsik). "The Life and Times of Cybersecurity Professionals 2018". *Enterprise Strategy Group and Information Systems Security Association International*, апрель 2019 года. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 Отчет NewVantage "Big Data and AI Executive Survey 2019, Сводные результаты для руководителей". *NewVantage Partners,* 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Сью Поремба (Sue Poremba). "Why Privileged Account Management Is Key to Preventing Insider Threats". *Аналитика безопасности,* 20 июня 2018 года. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 "Cost of Insider Threats: Global Report 2020". *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 "Отчет Ponemon. Мнения клиентов о защите данных с помощью Guardium". *Ponemon Institute,* август 2019 года. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-RURU-00