

Правила личной сетевой защиты

Windows IT Pro/RE

№2 ФЕВРАЛЬ 2019 | WWW.WINDOWSITPRO.RU | ИНФО ДЛЯ ИТ-ПРО

Мобильная
версия



Google play



Базы данных в новом свете

Обеспечиваем соответствие требованиям
регламента по защите данных

Шифрование и управление ключами
в SQL Server

Управление ключами шифрования
для Microsoft SQL Server 2008–2016

ISSN 1563-101X



19002



9 771563 101008

Издание для специалистов, интересующихся технологиями компании Microsoft.

Главный редактор: Д. Ю. Торопов (toropovd@osp.ru)
Ответственный редактор: Е. Петровичева
Корректор: Л. Терemenko
Верстка и дизайн: О. Шуранова
Номер также готовили: Е. Овсянников
Т. Евдокимова, А. Китаев, А. Федотов,
Н. Басалова, Ю. Власов, Д. Шепкин, А. Адзиев

Адрес для писем: 123056, Москва, а/я 82
Телефоны: (495) 725-4780/83, (499) 703-1854
Факс: (495) 725-4783
E-mail: windowsitpro@osp.ru

Учредитель: ООО «Издательство
«Открытые системы»

© 1999-2019 Издательство «Открытые системы»
© 1999-2019 Penton Media, Inc.

Журнал зарегистрирован в Роскомнадзоре.

Свидетельство о регистрации средства
массовой информации ПИ № ФС 77-63737
от 16 ноября 2015 г.

Дата выхода в свет — 5.02.2019 г.

Цена свободная. Выходит 12 раз в год.



**ОТКРЫТЫЕ
СИСТЕМЫ**
Open Systems Publications

Адрес редакции и издателя:

ООО «Издательство «Открытые системы»
127254, Москва, пр-д Добролюбова, д. 3,
стр. 3, комн. 13.

Президент М. Е. Борисов

Генеральный директор Г. А. Герасина

Директор ИТ-направления П. В. Христов

Коммерческий директор Т. Н. Филина

Подписные индексы:

Объединенный каталог «Пресса России» — 38185,
«Каталог российской прессы» — 99483,
ФГУП «Почта России» — П2337
Отпечатано в ООО «МИНИН»
г. Нижний Новгород, ул. Красноезвездная,
д. 7а

Тираж: 6900 экз. — печатная версия,
3280 экз. — PDF-версия

Редакция не несет ответственности за содержание
рекламных материалов. Все права защищены. Полное
или частичное воспроизведение или размножение
каким бы то ни было способом материалов, опублико-
ванных в настоящем издании, допускается только
с письменного разрешения ООО «Издательство
«Открытые системы».

Windows®, Windows Vista® и Windows Server® —
зарегистрированные торговые марки корпорации
Microsoft. Название Windows IT Pro используется Penton
Media, Inc. в соответствии с соглашением с владельцем
торговой марки. Название Windows IT Pro/RE использу-
ется ООО «Издательство «Открытые системы» по лицен-
зионному соглашению с Penton Media, Inc. Windows IT
Pro/RE — независимое от корпорации Microsoft изда-
ние. Корпорация Microsoft не несет ответственности
за редакционную политику и содержание журнала.
Редакция оставляет за собой право не вступать
в переписку.

Отобранные для публикации письма редактируются
в соответствии с терминологическими нормами,
принятыми в издательстве.

Названия продуктов и компаний, упомянутых в
журнале, могут быть товарными знаками их владельцев.



Penton Media, Inc.

ТЕМА НОМЕРА

2 Обеспечиваем соответствие требованиям регламента по защите данных

ТИМ ФОРД

5 Шифрование и управление ключами в SQL Server. Часть 2

ПАТРИК ТАУНСЕНД

10 Управление ключами шифрования для Microsoft SQL Server 2008–2016

WINDOWS ИЗНУТРИ

14 На пути к совместимости

СЕРГЕЙ ВАСИН

ВВОДНЫЙ КУРС

22 Правила личной сетевой защиты

ВЛАДИМИР БЕЗМАЛЫЙ

28 Windows 10 превращается...

ВЛАДИМИР БЕЗМАЛЫЙ

ПЛАНИРОВАНИЕ

31 Совершенствуем управление данными

ДЭЙВ РАССЕЛЛ

ЛАБОРАТОРИЯ

35 Резервное копирование и восстановление корпоративных данных

ДЖОН КОННОР

38 Обзор методов аналитики на современном предприятии

SQL SERVER

46 Использование DBCC CLONEDATABASE для настройки производительности запросов

ТИМ ФОРД

ИЛЛЮСТРАЦИЯ НА ОБЛОЖКЕ GRAPHICCOMPRESSOR (ADOBE STOCK)



Обеспечиваем соответствие требованиям регламента по защите данных

Тим Форд

Главная из проблем, которые одинаково заботят администраторов баз данных, директоров по защите данных и управляющих ИТ,— безопасность данных клиентов в контексте общего регламента по защите персональных данных (GDPR), а также способность реляционной базы данных, или базы NoSQL, обеспечить соответствие новым требованиям.

В GDPR содержатся требования к методам управления и обработки персонально идентифицируемых сведений. Также требуется, чтобы контролеры (лица, отвечающие за размещение, хранение, управление данными, с помощью которых можно идентифицировать человека) и обработчи-

ки, использующие эти самые данные для вычислений или анализа, были подотчетны лицам, чьи персональные данные они контролируют или обрабатывают. Помимо прочего, GDPR требует, чтобы контролеры и обработчики выполняли пожелания пользователей «забыть» их данные, своевременно предоставляли им их персональные сведения и прекращали обработку данных по требованию. Свод правил GDPR содержит и другие требования, но эти три обсуждаются наиболее активно.

Кроме того, вызывает немало вопросов способность систем управления базами данных обеспечить соответствие требованиям GDPR. Особую проблему могут представлять базы данных типа NoSQL.



Что же представляют собой базы данных, отличные от SQL, и что отличает их от таких реляционных

онному: они пожертвовали некоторыми свойствами транзакций, такими как неделимость, целост-

мени, и пара «ключ-значение» может выглядеть так: «Первому игроку приготовиться» и «Тревора Форда».

Что же представляют собой базы данных, отличные от SQL, и что отличает их от таких реляционных баз данных, как Microsoft SQL Server или Oracle? Чтобы ответить на эти вопросы, нужно вернуться в 60-е годы XX века

баз данных, как Microsoft SQL Server или Oracle? Чтобы ответить на эти вопросы, нужно вернуться в 60-е годы XX века.

Краткая история баз данных, отличных от SQL

Базы данных NoSQL первоначально назывались non SQL или «нереляционные», но сегодня обозначаются термином not only SQL («не только SQL»).

В современных NoSQL способы хранения и извлечения данных иные, нежели в таблицах и соединениях между таблицами традиционных реляционных моделей.

Базы данных NoSQL существуют уже более 50 лет, но они не получали широкого распространения до появления сетевых технологий, известных как Web 2.0, в 1990-х, а также социальных сетей и розничных гигантов, таких как Facebook, Google и Amazon. Эти и другие компании стремились преодолеть некоторые недостатки традиционных систем управления реляционными базами данных, относящиеся в основном к быстродействию. Базы данных NoSQL изначально ориентированы на производительность, но в ущерб некоторым достоинствам систем управления реляционными базами данных.

Первоначально разработчики баз данных NoSQL старались обойти реляционные ограничения, однако впоследствии избрали более центристский подход к управлению данными, близкий к реляци-

онности, изолированность и устойчивость (от англоязычных терминов Atomicity, Consistency, Isolation, Durability), обозначаемыми как ACID, ради доступности и быстродействия. Поэтому вполне вероятно, что проблемы, решаемые в реляционных базах данных, например гарантия фиксации всех операций чтения данных и всех транзакций, переданных в базу данных, могут возникать в NoSQL.

Однако важно отметить, что не все базы данных NoSQL одинаковы. Существует три отдельных категории.

1. Базы данных типа «ключ-значение»

Базы данных типа «ключ-значение» (Key-Value) используют дополнительный, ассоциативный, массив (то есть «карту» или «словарь») для обозначения отношений различных ключей вместо типовых таблиц и объединений в реляционной базе данных. В базах данных типа «ключ-значение» данные представлены как коллекция пар «ключ-значение», при этом каждая возможная ключевая пара встречается в коллекции не более одного раза.

Фундаментальная проблема с использованием чистой пары «ключ-значение» заключается в том, что используются естественные ключи, то есть сохраняется действительное значение ключевой пары. Примером может служить предприятие по прокату фильмов: только один человек может арендовать фильм в определенный момент вре-

Альтернатива естественным ключам — хеш-таблица, в которой используется алгоритм для естественных значений ключей. Возникают затруднения, если алгоритм создает дублированный хеш для различных пар «ключ-значение», но в таких случаях применяются обходные маневры. При этом возникает серьезная проблема с парами «ключ-значение», использующими естественные ключи, подобно тому, как это бывает в реляционной базе данных с естественными ключами: они персонально идентифицируемы. В приведенном выше примере легко идентифицировать человека по имени — Тревор Форд. Если Тревор Форд попросит забыть свои данные, то удовлетворить требованиям GDPR будет трудно. При этом разрушается пара «ключ-значение», на которой основан метод идентификации записи в базе данных типа «ключ-значение». Хеш придется вычислять повторно, если компания использует хеш-таблицу как альтернативу естественным ключам при поступлении запроса. В результате увеличиваются накладные расходы и могут возникнуть дополнительные проблемы.

Приведу несколько примеров баз данных NoSQL типа «ключ-значение»:

- Apache Ignite;
- Couchbase;
- Riak;
- Redis;
- MUMPS;
- база данных Oracle NoSQL;

2. Документо-ориентированные базы данных

Базовый элемент хранилища документов — документ. Хотя во всех продуктах данной категории применяются различные подходы, неизменно предполагается, что данные в документах хранятся в некотором стандартном формате, таком как JSON или XML. Каждый документ имеет уникальный ключ, идентифицирующий конкретный документ, и в каждом документе хранятся значения, связанные с записью (в реляционных терминах). Базы данных, хранящие документы, по-прежнему используют хранилище «ключ-значение», но предоставляют API-интерфейс или некоторый вид языка запросов для получения данных. Однако, в отличие от реляционных баз данных, документы могут иметь различную структуру. В этом проявляется отход от строгой схемы структуры реляционной таблицы. Различные поставщики баз данных для хранения документов по-разному подходят к организации документов: через коллекции документов, расстановку тегов, иерархии или иные способы отмечать метаданные. С хранилищами документов возникают те же проблемы, что и с базами данных типа «ключ-значение», когда речь идет о предусмотренном GDPR праве быть забытым и даже требовании безопасного экспорта данных пользователя. Выживание персонально идентифицированных данных из огромного множества документов может оказаться делом нелегким. Некоторые примеры баз данных документов:

- CouchDB;
- CosmosDB;
- MongoDB;
- IBM Domino.

3. Базы данных, построенные на графах

По мере развития науки о данных и приобретения специалистами соответствующего опыта огромную популярность получили базы данных, построенные на графах. Они

предназначены для данных, отношения между которыми соответствуют графу, состоящих из элементов с заданным числом связей между

запросом, можно использовать несколько запросов. Запросы NoSQL часто выполняются быстрее, чем запросы реляционных баз данных,

Приходится учитывать множество факторов, но ненормализованная природа баз данных NoSQL и использование мягкого удаления может затруднить выполнение требований GDPR по сравнению с реляционными базами данных

ними. Базы данных, построенные на графах, имеют преимущество перед реляционными базами данных в том, что моделирование сложных иерархических структур в них выполнять гораздо удобнее, чем в реляционных аналогах. Во многих базах данных, построенных на графах, внутренние компоненты созданы по реляционной модели, и их язык запросов отличен, так как реляционные запросы не могут справиться с иерархическими сложностями при построении графов. В результате проблемы, возникающие вокруг GDPR, обычно близки к тем, с которыми приходится сталкиваться пользователям реляционных баз данных. Некоторые примеры таких баз данных:

- Apache Giraph;
- MarkLogic;
- OrientDB;
- ArangoDB.

Работа с реляционными данными

Большинство баз данных NoSQL не могут выполнять объединения; схема баз данных обычно проектируется с учетом этого обстоятельства. В частности, используются перечисленные ниже приемы.

Несколько обращений. Вместо того чтобы извлекать все данные одним

поэтому расходы на дополнительные запросы могут оказаться приемлемыми.

Вложения и ненормализованные данные.

Часто используемый метод: сохранение большего объема данных, причем ненормализованных. Сохранив как суррогатный ключ (например, идентификатор пользователя), так и имя, фамилию и т. д., можно будет создать одно обращение к данным. За быстрое действие приходится расплачиваться повышенными требованиями к ресурсам памяти. Метод может привести к размножению персонально идентифицируемых данных, а это увеличивает вероятность нарушений GDPR и затрудняет достижение соответствия правовым нормам.

Таким образом, приходится учитывать множество факторов, но ненормализованная природа баз данных NoSQL и использование мягкого удаления может затруднить выполнение требований GDPR по сравнению с реляционными базами данных.



Тим Форд (timothyford@gmail.com) — независимый консультант, автор и специалист по данным. С 2000 года работает администратором баз данных в области здравоохранения