Европейский телекоммуникационный рынок

Проблема гарантированного сохранения данных

СЕГОДНЯ РАЗЛИЧНЫЕ ЗАКОНЫ И НОРМАТИВЫ, ОПРЕДЕЛЯЮЩИЕ ПРАВИЛА ХРАНЕНИЯ ДАННЫХ, ЗАСТАВЛЯЮТ ПРЕДПРИЯТИЯ ПЕРЕСМАТРИВАТЬ СВОЙ ПОДХОД К УПРАВЛЕНИЮ ЖИЗНЕННЫМ ЦИКЛОМ ДАННЫХ, ПОЭТОМУ ГАРАНТИРОВАННОЕ СОХРАНЕНИЕ ПРЕВРАТИЛОСЬ В ОДНУ ИЗ ГЛАВНЫХ ПРОБЛЕМ, С КОТОРЫМИ СТАЛКИВАЮТСЯ КОМПАНИИ.

Тревор Вильямс,
Hitachi Data Systems

Вопросы соответствия (compliance) полностью изменили отношение к хранению данных — если раньше это был чисто технический вопрос, то сегодня его обсуждает совет директоров компании, что означает более высокий приоритет и выделение бюджета, который раньше невозможно было получить для решений хранения данных.

Новая директива ЕС приведет к генерации огромных объемов дополнительных данных и ее выполнение потребует многомиллионных инвестиций. Это создает новую возможность для предложения решений, которые обеспечат соблюдение законодательства, вступающего в силу в сентябре 2007 г.

Обзор

После трагических событий 11 сентября правительства разных стран мира предприняли беспрецедентные меры по усилению системы безопасности для борьбы с глобальными террористическими группировками и организованной преступностью. Примером может послужить возрастающее число законодательных актов, требующих от провайдеров услуг, прежде всего из телекоммуникационного сектора, предоставления государственным ведомствам информации, которая способна помочь в выявлении противозаконной деятельности и может быть использована в качестве улики во время судебного разбирательства. В результате резко повысилась важность телекоммуникационных систем и теперь, также как в финансовом секторе, телекоммуникационные операторы должны обеспечить точное выполнение требований законодательства, от которого во многом зависит также конкурентоспособность компании и стоимость ее акций.

Новое законодательство затрагивает провайдеров следующих типов сервисов:

— доступа к Интернет;
— услуг стационарных сетей связи;
— услуг мобильных сетей связи;
— операторов виртуальных сетей;
— VoIP с обменом трафиком с телефонными сетями общего пользования.

В данной статье рассматриваются проблемы выполнения требований законодательства с точки зрения операторов мобильной связи. Она не затрагивает специфики Интернет-провайдеров.

Законодательство

Предпринимая меры по борьбе с международной организованной преступностью, Европейский союз (ЕС) в то же время заботится о правах и свободах своих граждан, перемещающихся по странам ЕС и не занимающихся незаконной деятельностью, поэтому законодательство учитывает вопросы защиты частной жизни. Выпущенная ЕС директива 2002/58/ЕС определяет правила обработки данных о трафике и

местонахождении, а также данных, по которым можно идентифицировать отправителя и получателя в телекоммуникационных системах, например, в системах сотовой связи, и относится ко всем операторам сотовой связи стран ЕС. Страны — участники ЕС также должны обеспечить хранение этих данных в течение срока от шести месяцев до двух лет со времени сеанса связи.

Подобное законодательство действует и в некоторых других странах, например агентство национальной безопасности (АНБ) США организовало централизованный сбор данных о звонках, а в ЮАР операторы сотовой связи обязаны хранить записи о звонках не менее трех лет.

Станы ЕС должны обеспечить выполнение этой директивы к 15 сентября 2007 г., что потребует от операторов сотовой связи этих стран значительных усилий.

Какие данные нужно будет сохранять?

При каждом звонке по мобильному телефону создается отдельная запись call data record (CDR), которая затем может использоваться для биллинга, сегментации рынка, выявления случаев мошенничества и других приложений. Данные, которые нужно сохранять в соответствии с директивой — это вся информация CDR за исключение голосовых данных. Также нужно сохранять данные обо всех неудачных звонках.

Данные CDR, которые нужно сохранить в соответствии с директивой, включают следующую информацию:

— номер телефона, с которого был сделан звонок, в который может быть включена информация об адресе зарегистрированного абонента;

— номер телефона, на который был звонок, в который может быть включена информация об адресе зарегистрированного абонента;

— географические координаты обоих телефонов в течение всего сеанса связи;

— дата звонка;

— время, когда был сделан звонок;

— базовая станция, начавшая обслуживание звонка;

— длительность звонка;

— переадресация звонка (если она использовалась);

— серийные номера обоих мобильных телефонов (IMEI & IMSI details.)

Сбор и обработка данных CDR — это стандартная функция устройств телекоммуникационных сетей. Эти и другие данные, пересылаемые по сети, должны быть надежно защищены от случайного или умышленного уничтожения, потери и модификации, неавторизованной или незаконной обработки, доступа или разглашения. Они могут быть уничтожены либо сделаны анонимными по истечении срока хранения, за исключением тех данных, к которым был осуществлен доступ на законных основаниях и которые сохранены для расследования. Кроме того, собранные в соответствии с директивой ЕС данные запрещается использовать в коммерческих целях. Если государственные или местные органы правопорядка запросили эти данные, то оператор обязан предоставить их немедленно.

Проблемы телекоммуникационного сектора

Перед телекоммуникационными компаниями, работающих в странах ЕС, стоят трудные проблемы, решение которых потребует существенных расходов. Например, из-за глобального характера мобильной связи требуется обеспечить выполнение законодательства разных стран. Например, операторы из стран, не входящих в ЕС, должны выполнить требования по сбору информации, действующие в ЕС. Это означает, что данные о звонке с мобильного телефона в России и Украине абоненту, зарегистрированному в ЕС, должны быть сохранены оператором, обслуживающем этого абонента.

Вторая серьезная проблема — объем данных CDR, который оператор мобильной связи должен обрабатывать ежедневно. За один рабочий день может накопиться до миллиарда CDR, которые нужно сохранить. Для обеспечения управления и целостности этих данных потребуются значительные инвестиции в ИТ-системы и обслуживающий их персонал. Однако не все операторы мобильной связи могут столкнуться с такими строгими требованиями сбора и отслеживания данных, что для одних операторов создаст дополнительные преимущества, а у других ухудшит конкурентоспособность.

Gartner приводит оценки Deutsche Telecom, которая считает, что для поддержки инициативы ей придется потратить 150 млн евро. С учетом того, что эти базы запрещается использовать в коммерческих целях, главной задачей становиться сведение к минимуму затрат на удовлетворение минимальных требований.

Возможности для хранения данных

Потенциальные потребности в хранении данных могут быть огромны. По подсчетам Gartner, до 50 тыс. терабайт дополнительных данных будут собраны только в ЕС, и все эти данные необходимо сохранить. Потребности в хранении данных CDR можно рассчитать, умножив размер одной записи на число звонков, которые система обрабатывает каждый день.

Например, 10 млн CDR в день, умноженные на 500 байт (ориентировочный размер одной CDR), дают 5 Гбайт дополнительных данных, которые генерируются каждый день.

Для поддержки этих операций нужна большая система хранения, способная хорошо масштабироваться без потери производительности в течение всего жизненного цикла. С учетом агрессивной модели затрат, база данных о звонках, которую нужно создать в соответствии с требованиями законодательства, должна обеспечить сжатие данных по крайней мере в 10 раз для того, чтобы сократить стоимость хранения и обеспечить платформу для неограниченного роста. Из-за высоких расходов на построение этой базы данных некоторые операторы мобильной связи могут передать сбор данных на аутсорсинг, но такой вариант имеет существенные ограничения - данные должны быть всегда "под рукой" чтобы их можно было немедленно предъявить по требованию государственных ведомств, как того требует законодательство, а защита конфиденциальности информации осложняется из-за расширения круга лиц, имеющих к ней доступ. Кроме того, при использовании аутсорсинга вся ответственность за выполнение законодательства остается на операторе мобильной связи, который должен найти компромисс между интересами бизнеса и соблюдением национальных законов о защите информации и конфиденциальности.

Система сбора данных должна обладать следующими характеристиками:

— доступность — развернута на надежной ИТ-платформе;

— высокая производительность — способность обрабатывать большой объем записей CDR;

— масштабируемость — эволюция по мере изменения информационной системы;

— гибкость — способность легко вносить любые необходимые изменения в формат CDR;

— открытость — наличие интерфейсов со всеми системами предбиллинга и биллинга.

Кроме того, решение должно соответствовать требованиям законодательства к системе архивирования. Решения для

архивирования имеют атрибуты хранения и защиты данных в соответствии с такими законами, как Sarbanes Oxley и SEC 17a-3. Архивное хранение должно обеспечить следующие базовые функции:

— сохранение (Retention) — сохранение документа в течение установленного законодательством периода времени. В некоторых случаях закон требует продления периода хранения, однако данный период никогда не может быть сокращен;

— уничтожение данных (Data Destruction) — уничтожение записей по истечению периода хранения определенным способом. В системах хранения могут использоваться механизмы, гарантирующие невозможность восстановления удаленных документов;

— аутентификация (Authenticity) — в процессе следствия или судебного разбирательства от оператора связи могут быть запрошены доказательства того, что представленные им документы не были изменены;

— контроль доступа и аудит (Access Controls and Auditing) — четко определяет, кто имеет право доступа к оригиналам записей. Для специальных записей могут действовать особые правила доступа и аудиторские параметры для подтверждения соблюдения сохранности.

— обнаружение (Discovery) — в ходе расследования от операторов связи могут быть затребованы записи CDR за определенный период времени (которые должны быть немедленно представлены) и невыполнение таких запросов влечет судебные преследования, поэтому необходимо применять ИТ-стратегии, обеспечивающие быстрый доступ к документу. Имеется два способа реализации таких решений — на уровне программного обеспечения и систем хранения.

Такие коммерческие программные решения, как предлагаемая Hitachi Data Systems платформа HCAP, — это полнофункциональные архивные системы, способные извлечь данные CDR из шлюза предбиллинга и записать их в архив. Законодательство требует, чтобы из записи CDR были удалены ненужные поля и, возможно, добавлены метаданные. Извлечение данных может быть реализовано с помощью прямого доступа к устройству архивирования (например, запрос к базе данных SQL или извлечение плоских файлов), либо через интерфейс бизнес-приложений, который обеспечивает доступ к нужным полям CDR.

Информация о звонке извлекается из сетевого коммутатора в шлюз предбиллинга. Данные CDR могут перенаправляться на любое число бизнес-приложений, выполняющих обработку данных или осуществляющих их генерацию. Из данных CDR, собранных системой предбиллинга, отбрасываются поля, которые не нужны для выполнения требований хранения, после чего CDR записываются в архив в виде плоского файла или в формате SQL.

После того, как данные загружены в архив, их хранение производится в соответствии с директивой в течение определенного периода, затем они уничтожаются, из них удаляется вся личная информация, либо они по-прежнему хранятся для использования в будущих расследованиях. Для выполнения требований законодательства ЕС решение, которое использует оператор связи, должно обладать следующими атрибутами:

— масштабируемость — требуется обеспечить высокую производительность хранения растущих объемов данных и миллиардов объектов;

— надежность хранения — нужно гарантировать защиту информации, которая сгенерирована и сохранена сегодня, от потери данных, деградации носителей и угроз. Также требуется обеспечить возможность управления и извлечения информации в многовендорной среде;

— доступная цена — необходимо использовать новые технологии, снижающие стоимость хранения данных;

— удобный доступ к данным — возможность предоставить нужную информацию разным категориям пользователей.

Возможности рынка

Данная ситуация, затрагивающие множество операторов связи, работающих в ЕС, создает новые возможности для расширения клиентской базы Hitachi Data Systems. Обсуждение нового законодательства с отвечающими за хранение данных менеджерами даст лучшее понимание потенциальных проблем и предлагаемых HDS-решений, которые сокращают затраты на приобретение и эксплуатацию решения.

Возможность получения источника дополнительной прибыли означает, что на этот рынок выйдут новые игроки, в том числе производители СХД и баз данных. В ЕС сейчас работает более 70 операторов мобильной связи и все они должны обеспечить соблюдение нового законодательства к сентябрю 2007 г., поэтому им потребуется развернуть соответствующее решение.

Выводы

Хотя операторы связи постоянно развиваются, по мере изменения ситуации на рынке ряд задач их бизнеса остается неизменным, например, выставление счетов клиентам, контроль их прибыльности и лояльности, привлечение новых клиентов и, что самое главное, выполнение разнообразных требований законодательства. Средний оператор связи ежегодно тратит от 10 до 12 млн евро только на поддержание инфраструктуры хранения CDR в соответствии с требованиями законодательства. Однако операторы стран, не входящих в ЕС (например, России), могут использовать базу данных записей CDR не только для хранения данных, но и для маркетинга, продаж, планирования развития сетей и финансовых приложений, что позволит им в отличие от европейских коллег получить прибыль от инвестиций в эту инфраструктуру.

Выполнение требований законодательства стало существенным компонентом бюджета на ИТ и расширяет юридическую ответственность руководителей ИТ-подразделений, поэтому ему уделяется больше внимания, чем большинству остальных проектов, напрямую связанных с бизнесом. Технологии помогают решить эти задачи, но они будут бесполезны, если оператор не обеспечит внедрение соответствующих процедур и правил, и в результате ему придется платить штрафы. Новая директива ЕС — это еще один закон, который должен выполняться на уровне центра обработки данных, а за ним последует закон о санкциях за нарушение авторских прав (бесплатной загрузки контента, защищенного авторским правом). Все эти законы необходимо учитывать при планировании новых проектов ИТ.

Для выполнения директивы ЕС операторам связи потребуется система с низкими начальными расходами, поскольку она не дает прибыли. Помимо этого часть расходов будет нести потребитель — оператор или повысит тарифы, или выполнение данного закона будет оплачивать государство из налоговых поступлений.

Основные сведения о директиве ЕС о сохранении данных

Директива требует от операторов мобильной связи и Интернет-провайдеров сохранять данные о сеансах связи и предоставлять их по требованию.

• Эта директива является основой законодательства ЕС, определяющей защи-

ту частной жизни при использовании электронных средств связи.

• Под эту категорию данных не попадает содержание разговора/электронного письма, что позволяет трактовать их сохранение как чисто техническое требование для операторов, работающих по законам ЕС.

• Директива требует от операторов телефонной связи и Интернет-провайдеров хранить такие данные, как номера телефонов и адреса электронной почты.

• Сейчас в 15 странах ЕС нет обязательных правил сохранения данных, например, в Великобритании сохранение данных не является обязательным для операторов.

• В тех десяти странах, где сохранение данных является обязательным, отсутствуют инструкции по осуществлению такого хранения, а его период составляет от трех месяцев до трех лет.

• Пересмотренные правила предусматривают хранение данных в течение 6 месяцев Интернет-провайдерами и 6 — 24 месяца операторами телефонной связи.

• Директива ЕС позволяет правительствам отдельных стран увеличивать срок хранения — например, в Ирландии операторы должны сохранять данные в течение трех лет.

• В Польше сейчас рассматривается закон о сохранении данных в течение 15 лет, что позволит стране выйти за верхний предел продолжительности хранения, установленный в ЕС.

• Чиновники ЕС предпочитают не называть точной суммы затрат, а говорят лишь, что выполнение директивы будет стоить от десятков миллионов до сотен миллионов евро.

• Если соединение было установлено, но на другом конце провода не сняли трубку, то такие звонки тоже должны фиксироваться, но при условии, что оператор собирает информацию о них.

• Правоохранительные органы могут запрашивать эти данные только для борьбы с терроризмом и другими опасными преступлениями (например, наркоторговлей или нелегальной иммиграцией).

АНБ СОБРАЛО ОГРОМНУЮ БАЗУ ДАННЫХ О ЗВОНКАХ АМЕРИКАНЦЕВ

Leslie Cauley, USA TODAY

Как сообщают осведомленные источники, Агентство Национальной Безопасности тайно собрало данные о звонках, которые сделали миллионы американцев, используя данные, полученные от AT&T, Verizon и BellSouth. В базу данных АНБ попали данные о миллионах звонках, которые сделали со своих домашних и служебных телефонов обычные американцы, подавляющее большинство которых непричастны ни к какой преступной деятельности.

Как сообщают источники USA Today, три телекоммуникационные компании подписали соответствующее соглашение с АНБ, которое запустило программу выявления террористов и слежки за ними в 2001 г. Белый Дом преуменьшает масштабы программы АНБ и в прошлом году Буш разрешил АНБ без ордера прослушивать международные звонки и перехватывать переписку по электронной почте лиц, подозреваемых в терроризме в случае, если один из собеседников или корреспондентов находится в США. Для наполнения базы данных агентство также использует информацию, получаемую по ордеру.

Уникальная роль операторов связи

После того, как недавно AT&T поглотила SBC, на рынке телекоммуникаций США сейчас самыми крупными операторами являются три компании — Verizon, BellSouth и AT&T. Всего услугами местной и мобильной связи этих трех компаний пользуются более 200 млн абонентов.

Эти три оператора эксплуатируют охватывающие многие штаты сети и используют новейшие технологии связи. Они предоставляют различные виды услуг связи, в том числе местную и междугороднюю, беспроводную и широкополосную, включая передачу видео. Без помощи этих операторов, обслуживающих миллионы домашних и служебных телефонов, невозможно организовать отслеживание телефонных разговоров американцев.

Среди операторов связи только Qwest отказался сотрудничать с АБН из-за опасений, что против оператора может быть возбуждено дело по обвинению в предоставлении правительству информации о своих клиентах без ордера.

Из-за отказа Qwest от участия в программе база данных оказалась неполной. Базирующийся в Денвере Qwest предоставляет услуги местной связи 14 млн человек в 14 штатах Запада и Северо-Запада США. Однако AT&T и Verizon также предоставляют услуги междугородней и мобильной связи в этих регионах, что позволило АНБ частично компенсировать отказ Qwest.

За прошедшие годы приемы, которые использует АНБ для доступа к информации, совершенствовались вместе с технологиями. Агентство широко применяет технологию "data mining" — просеивание информации в поисках закономерностей. Это один из многих инструментов аналитиков и математиков NSA для взлома шифров и отслеживания международных каналов связи.

Необходимость использования базы данных звонков внутри страны, которое собрало АНБ, остается спорным вопросом, как и возможность использования этой базы для других задач.

Программа АНБ по отслеживанию звонков внутри страны спорна и с юридической точки зрения. Раньше AT&T и региональные телефонные компании требовали ордера суда даже для рассмотрения запроса правоохранительных органов о предоставлении данных о звонках своих клиентов. Это объясняется историческими традициями старой Bell Telephone System, наследниками которой являются эти телефонные компании. Она строго защищала интересы своих клиентов и предоставляла информацию только по решению суда.

Неприкосновенность частной жизни была зафиксирована в законодательстве: в параграфе 222 Закона о связи, первая редакция которого вступила в действие в 1934 г., телефонным компаниям запрещалось предоставлять такую информацию о звонках своих абонентов, как кому они звонили, как часто и даже как переадресовывался их звонок собеседнику, а также информацию о входящих звонках и звонках по мобильному телефону. Федеральная комиссия по связи (FCC), контролирующую работу всего телекоммуникационного рынка США, может наложить штраф до 130 тыс. долл. за один день нарушения это параграфа, а общая сумма штрафов может составить 1,325 млрд долл. Однако у FCC нет четкого определения, что понимается под нарушением этого параграфа — нарушение может затрагивать телефонные звонки одного абонента или миллиона абонентов.

Для проведения программы АНБ по отслеживанию международных звонков Буш подписал специальное разрешение агентству действовать без ордера. Президент и его представители настаивают, что это разрешение дает полное право агентству перехватывать разговоры, однако с этим утверждением несогласны ряд групп по защите гражданских прав, в том числе American Civil Liberties Union.

Особая позиция Qwest

Из крупных операторов связи в программе отказался участвовать только Qwest. Руководство Qwest было обеспокоено тем, что оператор должен был передавать данные без решения суда или разрешения FISA. Его опасения усилились из-за того, что Qwest не мог выяснить, кто будет иметь доступ к информации о его клиентах и как она будет использоваться.

Qwest тревожили финансовые последствия участия в программе, поскольку за незаконное разглашение информации о звонках абонентов оператор должен заплатить значительный штраф. Поскольку АНБ требовало от Qwest передать ей миллионы записей, то это грозило оператору огромными убытками. Без согласия на сотрудничество Qwest агентство не могло собрать полную базу данных. Если Qwest не будет сотрудничать с агенством, он может не получить контракты, имеющие гриф секретности (как и все крупные операторы, Qwest выполняет ряд контрактов с грифом секретности и надеется на их подписание в будущем). До сих пор вопрос о легальности запроса АНБ к Qwest остается открытым.