6. ГОСТ Р 43.0.3-2009 Информационное обеспечение техники и операторской деятельности. Ноон-технология в технической деятельности. Общие положения. Дата введения 01.01.2011 г.

Мухина А.Е.

Безопасность данных в Master Data Management системах

Аннотация: Описаны потери, при отсутствии системы по управлению мастер-данными. Проанализированы основные аспекты безопасности данных, которые необходимо учитывать при имплементации MDM-систем.

Ключевые слова: информационная безопасность, Master Data Management (MDM)

Данные являются ценнейшим ресурсом во всех сферах бизнеса. Качественные данные помогают не только увеличить прибыль, но также позволяют преуспевать во всех видах управленческих решений, которые опираются на получаемые из систем данные. На текущий момент сложно представить крупный холдинг компаний, который не сталкивался бы с проблемой разрозненности данных от системы к системе. К примеру, справочник контрагентов может использоваться одновременно как в CRM-системе, так и в бухгалтерских системах при проведении проводок, в маркетинговой системе при проведении рассылок, и в дополнение ко всему – в системах, отвечающих за предоставление ключей на коробочные лицензии той или иной программы. Что же возникает, если справочник не интегрирован от системы к системе и не нормализирован, не очищен от дублей, заполнен некачественными непроверенными данными? Бизнес может нести убытки различных категорий.

Репутационные – из-за того, что один и тот же клиент заведен дважды как в CRM-системе, так и в маркетинговой, но пользователь решил отменить подписку на рассылку промо-материалов. В итоге, в одной системе отписка успешно прошла, но во второй системе, он по-прежнему числится активным подписчиком и ему продолжают поступать письма. Критическим моментом является потеря чувствительных данных клиентов, таких как ИНН, банковские счета и т.д.

Инвестиционные – зачастую инвесторы компаний запрашивают отчетность по прибыли компании в различных разрезах. В случае, если в CRM-системе не проверяется качество данных, то очень легко получить задублированные выкладки по различным контрагентам, что влияет на качество отчетности. Инвесторы очень придирчивы к качеству предоставляемых им данных, и их вполне может отпугнуть хаос во внутренней отчетности компании.

Маркетинговые – в случае, если при продажах используются данные одного и того же контрагента, но де-факто это дубли, то при аллоцировании прибыли, и подведению маркетинговых итогов, например, расчету корпоративной скидки для контрагента, можно не учесть часть выручки, что приведет к неверным расчетам, к формированию неверной маркетинговой стратегии, которая применяется при работе с ключевыми клиентами.

Финансовые – компания, которая вынуждена вручную поддерживать качество данных в зоопарке своих систем, тратит огромные средства на штат сотрудников – IT-специалистов, на отделы, которые проверяли бы и очищали дубли и данные в каждой из подключенных в контур систем. Каждая система, в которой справочники не интегрированы между собой, требует решения одной и той же проблемы в каждой системе индивидуально.

Решения, названные Master Data Management systems (MDM), позволяют компаниям преодолевать проблемы разрозненных хранилищ, данных от системы к системе, создавать надежные профили справочников, и в конечном итоге, как в случае с клиентами – обеспечивать дифференцированное обслуживание [1]. MDM-системы позволяют устранять дублирования, управлять данными из единого центрального репозитория, гарантируя, что любая запись, созданная или обновленная в каждой из ваших систем, отражена, нормализирована и верифицирована в центральном репозитории (рисунок 1).

Как лучше организовать безопасность данных при внедрении и функционировании MDM-решения, ведь она затрагивает все мастер-данные внутри компании? Перед внедрением требуется тщательно проработать стратегию, которая фокусируется на защите данных, которые не только хранятся в различных базах, но и на подвижных данных, переходящих от системы к системе [2]:

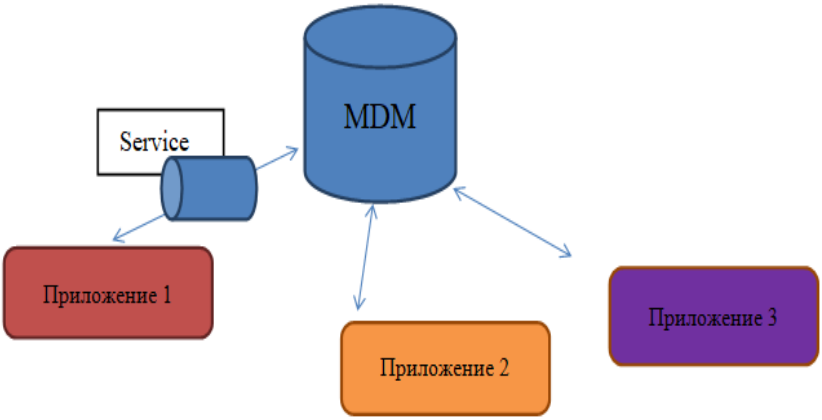

Рисунок 1 – Возможная архитектура MDM-решения

1) Имплементировать защиту приложения внутри MDM-системы.

Аутентификация пользователей – процесс проверки личности юзера. Пользователь в контуре MDM может быть не только человек, которому требуется получить доступ к системе, но и другие приложения, которые потребляют информацию из MDM. Очень важно, чтобы MDM-решение включало хорошо продуманный внутренний протокол управлением аутентификацией, с настроенной выдачей аппаратных токенов. Во многих случаях MDM-система должна интегрировать существующие в компании доменные системы, такие как Microsoft Active Directory [3].

Авторизация пользователей – процесс определения, имеет ли пользователь достаточные привилегии для доступа к запрошенным данным в MDM-системе. Использование этой технологии позволяет предоставлять пользователям доступ только к той части приложения, с которыми он имеет право работать. К примеру, большинству пользователей должен быть запрещен доступ к проведению процедуры дедубликации записей, и соответствующие права должны быть только для учетной записи Дата Стюарта – пользователя, отвечающего за качество данных в системе.

Логирование и временные отметки – каждая система предусматривает журнал логов, чтобы можно было отследить, кто запрашивал, редактировал записи внутри приложения.

2) Имплементировать централизованную защиту данных.

Управление рисками, связанными с конфиденциальными данными – требуется дополнительная аналитика, чтобы идентифицировать все чувствительные данные в конечных системах, центральном MDM-хранилище, а также каналы их распространения между системами. Для контроля доступа к таким данным, требуется применять шифрование, маскирование, токенизацию и контроль доступа, чтобы гарантировать, что только те, у кого есть специальный доступ, могут просматривать конфиденциальные данные [4].

3) Обеспечить бесшовную имплементацию MDM-решения в контур существующей системы информационной безопасности.

Очень важно сотрудничать с группой коллег, которые занимаются вопросами информационной безопасности в компании. Важно подключить в контур MDM уже унаследованные средства контроля и безопасности, которые помогут в идентификации кибератак. При имплементации любого модуля в MDM-решение, требуется проверять поставщиков услуг на наличие сертификатов, соответствия отраслевым стандартам для защиты данных.

Литература:

1. *Федосин С.А., Федюшкин Н.А., Савинов И.А.* Обзор семантического подхода к моделированию и управлению мастер-данными. Модель зрелости в управлении мастер-данными//Аллея науки. – 2019. – № 1 (28). – С. 138-146.

2. *Loshin D.* Master Data Management. – Burlington: Morgan Kaufmann Publishers, 2008. – 274 p.

3. Обзор доменных служб Active Directory [Электронный ресурс]. – URL: https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата обращения: 27.09.2020).

4. How Master Data Management Supports Data Security [Электронный ресурс]. – URL: https://blog.stibosystems.com/how-master-data-management-supports-data-security (дата обращения: 27.09.2020).