Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК [004.056.5]:004.65

Хлистовская
Мария Игоревна

ПРОДВИЖЕНИЕ ОБЛАЧНЫХ СЕРВИСОВ ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЯ НА ПРИНЦИПАХ GDPR

АВТОРЕФЕРАТ

на соискание степени магистра

по специальности 1-40 80 07 «Электронная экономика»

(профилизация «Электронный маркетинг»)

_____

Научный руководитель
Пархименко Владимир Анатольевич
кандидат экономических наук, доцент

_____

Минск 2021

КРАТКОЕ ВВЕДЕНИЕ

Жизнь человека в информационном мире неизбежно делает его более прозрачным для государства и общества, поэтому желание сохранить "информационную приватность" становится все более ощутимым. Именно развитие информационно-телекоммуникационных технологий, внедрение их во все сферы жизни общества и государства, перевод многочисленных картотек в цифровую форму побудили людей задуматься о защите этой весьма чувствительной информации. Новые технологии, с одной стороны, существенно упростили сбор, обработку, хранение, передачу данных, а с другой - создали очевидные угрозы их незаконного оборота, что ведет к нарушениям прав личности.

Рост цифровой трансформации организаций, обусловленный быстрым внедрением таких технологий, как облачные вычисления и аналитика данных, резко повысил важность внимание к этой области. Эта тенденция влияет как на традиционные отрасли экономики, так и на SaaS и электронную коммерцию.

Данные по праву считаются источником жизненной силы современной глобальной экономики, в то время как передача защищенных данных между странами становится все более сложной. Все больше и больше стран создают барьеры, которые делают этот процесс трудоемким и дорогостоящим из-за недавно принятых правил хранения данных.

По мере того, как информационная эпоха прогрессирует, важность географического положения для конфиденциальности данных становится все более важной. В то время как международные правила конфиденциальности, такие как GDPR, или основные законы, такие как CCPA, становятся главными, существует бесчисленное множество мелких региональных законов, которые часто получают меньше внимания. Эти законы часто являются краеугольным камнем в планах глобального расширения многонациональных компаний и резидентности данных.

Резидентность данных— это локализация регулируемых данных, таких как личная информация, в определенном регионе или стране. Это может быть как хранение данных, так и их обработка, где эти данные обрабатываются в соответствии с законодательством этого конкретного региона.

Несмотря на значительные преимущества для компаний, потребителей и национальных экономик, которые возникают в результате цифровой трансформации, а также способность организаций легко обмениваться данными через границы, десятки стран воздвигли барьеры для трансграничных потоков данных. Среди них — требования к резидентности данных, которые ограничивают данные в пределах границ страны, или концепция, также известная как «локализация данных».

Локализация данных может быть явно обязательной по закону или быть результатом других ограничительных политик, которые делают невозможным передачу данных. Они требуют от компаний хранить копию данных локально, обрабатывать данные локально и требовать согласия отдельных лиц или

правительства на передачу данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью работы является разработка комплексного подхода к продвижению облачного сервиса по хранению и обработке данных, основанного на принципах GDPR.

Задачи исследования:

1. Осуществить анализ сущности услуг облачных сервисов по хранению и обработки данных.

2. Провести анализ опыта обработки и хранения данных пользователя и защите персональной информации с учетом GDPR-регулирования

3. Разработать комплекс практических рекомендаций по продвижению услуг облачных сервисов хранения и обработки данных на принципах GDPR.

Предметом исследования является стратегия продвижения и защита данных в соответствии с принципами общего регламента по защите данных GDPR. Объектом исследования - компании предоставляющие услуги по хранению данных пользователя.

Новизна полученных результатов состоит в том, что облачные провайдеры должны соответствовать требованиям безопасности, чтобы хранить и обрабатывать данные пользователя. Таким образом, был проведен анализ компании, предоставляющей услуги по хранению данных пользователя и разработан комплекс практических рекомендаций по продвижению услуг облачных сервисов хранения и обработки данных на принципах GDPR.

Положения, выносимые на защиту:

1. Комплексная система по хранению и обработке данных, базирующаяся в отличие от существующих аналогов на принципах GDPR и включающая такие элементы, как: перечень регулируемых данных, стек соответствия данных, требования к шифрованию данных и др.

2. Политика продвижения облачных сервисов, включающая в себя план использования инструментов партнерского маркетинга и вебинарного маркетинга.

3. Концепция новой услуги Data Residency as a Service и методы по ее обеспечению, в том числе целостности, доступности и конфиденциальности персональных данных пользователя, с внедрением данной услуги в компанию InCountry.

Полный объем диссертации составляет 72 страницы.

Количество иллюстраций –12.

Количество таблиц – 3.

Количество приложений – 2.

Количество библиографических источников – 39.

Магистерская диссертация выполнена самостоятельно, проверена в системе «Атиплагиат». Процент оригинальности соответствует норме не менее 50%, установленной кафедрой экономики. Цитирования обозначены ссылками на публикации, указанные в «Библиографическом списке».

Опубликованность результатов исследования. Опубликованы две статьи: одна в сборнике Международной научно-практической конференции «ПЕРСПЕКТИВЫ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ» (31.03.2021), вторая - сборнике Международной научно-практической конференции «ПЕРСПЕКТИВЫ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ» (31.03.2021).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Структура и объем диссертации. Данная работа состоит из трех глав, каждая из которой является логическим продолжением предыдущей.

В первой главе «Теоретические и методологические основы облачных сервисов и их применение» рассмотрены модели и характеристики предоставления услуг на рынке облачных сервисов, где должны учитываться требования по безопасности и конфиденциальности данных.

Во второй главе проведен анализ опыта хранения данных пользователя и защите персональной информации и обнаружено, что не все компании могут хранить данные пользователя в зашифрованном виде, а также находится в стране присутствия и обеспечить хранение и обработку данных в пределах страны.

В третьей главе разработан комплекс практических рекомендаций по продвижению услуг облачных сервисов в и защите персональной информации которая предоставляет уникальное решение по услуге Data Residency as a Service для компаний, позволяя им хранить и обрабатывать регулируемые данные соответствующим образом для каждой юрисдикции в зашифрованном виде.

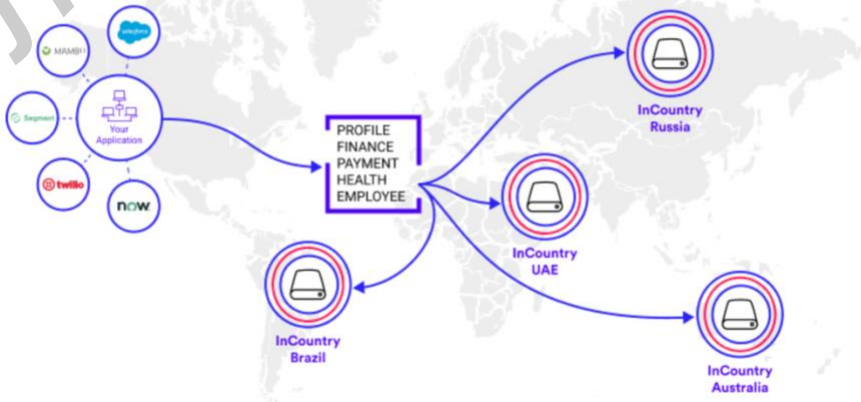


Рисунок 1- Локализация данных использования сервиса с партнерской интеграцией

Предлагается использовать сочетание глобальных облачных провайдеров и авторизированных центров обработки данных высшего уровня для предоставления двух реплицированных объектов в каждой стране.

Платформа работает на двух отдельных точках присутствия в каждой стране. Эти две точки присутствия важны в случае, если один из них отключается или временно недоступен для непредвиденных событий.

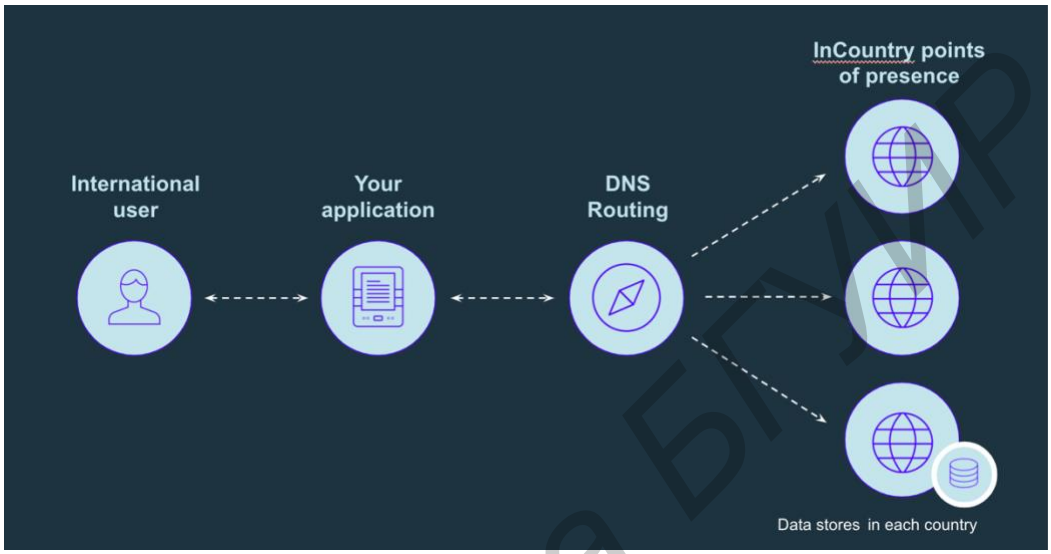


Рисунок 2 –Хранение данных сервиса

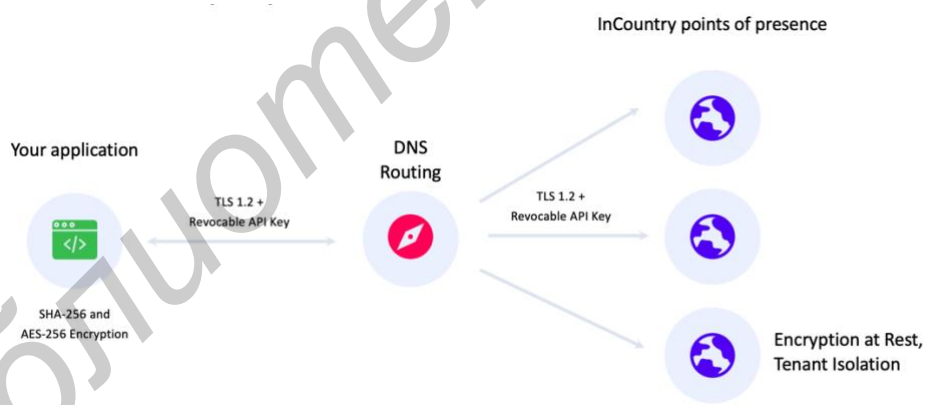


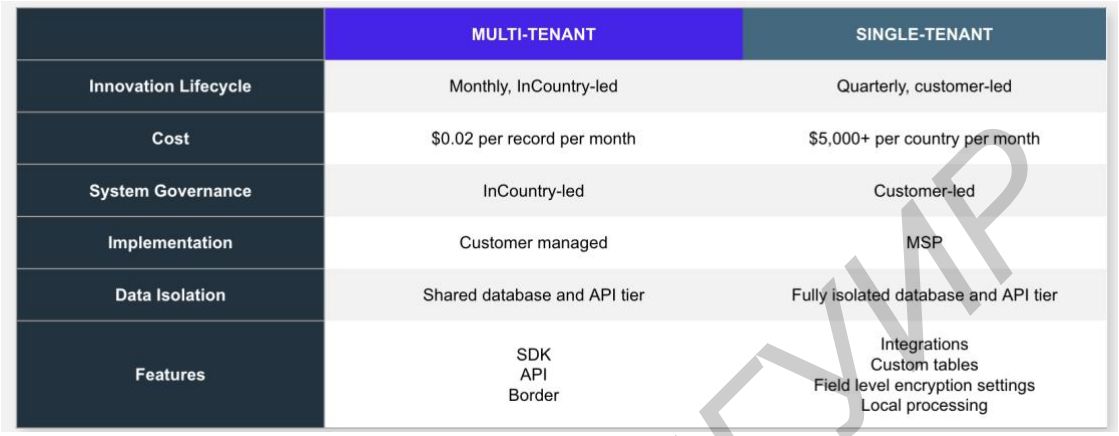
Рисунок 3 – Обеспечение конфиденциальности и безопасности данных в сервисе

Как только зашифрованные данные отправляются в страну и хранятся, для хранения используется шифрование AES-256 бит.

Этот уровень шифрования гарантирует, что данные всегда будут в безопасности.

Для дополнительной безопасности сетевая связь укреплена TLS 1.2 и отзывным API ключом. Кроме того, арендаторы полностью изолированы, так что только API-ключ разработчика может получить доступ к их данным и вся информация хранится на удаленных серверах с шифрованием в состоянии покоя.

Благодаря двойному подходу шифрования (SHA-256, AES-256) предоставляется зашифрованная база данных, которая полностью доступна для поиска. Данные клиентов шифруются непосредственно в вашем приложении с помощью SDK. SDK использует хэш SHA-256 для шифрования индексированных полей и симметричное шифрование AES-256 для шифрования всей записи.



	MULTI-TENANT	SINGLE-TENANT
Innovation Lifecycle	Monthly, InCountry-led	Quarterly, customer-led
Cost	$0.02 per record per month	$5,000+ per country per month
System Governance	InCountry-led	Customer-led
Implementation	Customer managed	MSP
Data Isolation	Shared database and API tier	Fully isolated database and API tier
Features	SDK API Border	Integrations Custom tables Field level encryption settings Local processing

Рисунок 4 — Ориентировочный расчет стоимости в зависимости от модели развертывания

В диссертации предлагается следующий подход к ценовой политике. Клиенту будут доступны 2 варианта: первая зависит от количества записей который хранит клиент (0.02$ за запись в базе данных) при условии, что это модель развертывания multi-tenant. В случае, если single tenant, то для одного клиента 5000$ в месяц за одну страну присутствия.

ЗАКЛЮЧЕНИЕ

С учётом проведённого анализа услуг облачных сервисов по хранению и обработки данных, опыта обработки и хранения данных пользователя и защите персональной информации с учетом GDPR-регулирования можно сделать вывод, что в условиях глобализации и перехода в облако компаниям необходимо следить за безопасностью и конфиденциальностью данных в облаке.

К основным методам относится:

1. Управление активами.
2. Контроль доступа.
3. Криптографическая безопасность.
4. Физическая и экологическая безопасность; Концепция реализации облачных технологий основана на том, что пользователи не знают точного местонахождения центров обработки данных и не осуществляют контроля за физическим доступом к этим данным. Наиболее известные провайдеры облачных сервисов располагают центрами обработки данных,

расположенными по всему миру. Однако приложения и данные могут храниться в странах, где поставщики услуг должны подчиняться требованиям безопасности и правовым нормам страны пребывания, что нередко затрудняет деятельность пользователя, незнакомого с законодательством страны, где обрабатываются его данные. InCountry в свою же очередь данной проблемы не имеет, так как использует только сертифицированные ЦОД в соответствии с нормативными требованиями.

5. Безопасный жизненный цикл разработки программного обеспечения.

6. Реагирование и расследование инцидентов; всякий раз, когда зафиксировано нарушение безопасности, «контрольный сервер», служащий в качестве реплицирующего устройства может переходить на режим «онлайн». В некоторых случаях резервная копия сервиса может быть легко сгенерирована и помещена на облако, не затрагивая нормальный ход бизнеса.

7. Восстановление данных. InCountry обеспечивает безопасность данных в случае естественных и техногенных катастроф. Как правило, это достигается репликацией данных на нескольких узлах.

8. Соответствие нормативам. InCountry подвергается проверкам внешних аудиторов. Если этого не делается, кредит доверия со стороны клиентов снижается.

Для решения указанных проблем в диссертации в разделе 3.1 разработана комплексная система по хранению и обработке данных, базирующаяся в отличие от существующих аналогов на принципах GDPR и включающая такие элементы других регуляторных органов стран, которым может потребоваться локализация данных.

Кроме того, в диссертации в разделе 3.2 разработана политика продвижения облачных сервисов в частности предложено в рамках партнерского маркетинга интеграция с платформами Intertrust, Mambu, Salesforce, Segment, Okta, Twilio и Servicenow в которых нуждаются клиенты, а также разработан план вебинарного маркетинга для демонстрации своих товаров и услуг для потенциальных клиентов отраженных в Приложении Б.

Также в диссертационном исследовании в разделе 3.3 автором разработана концепция новой услуги - Data Residency as a Service и методы по ее обеспечению, в том числе по обеспечению целостности, доступности и конфиденциальности данных.

Все эти предложенные в диссертации решения имеют единую базу - они строго и однозначно основываются на принципах GDPR.

GDPR - один из самых действенных законодательных актов, которые имеет серьезные требования для поставщиков облачных услуг и бизнеса, взаимодействующего с клиентами. Закон является не только проблемой соблюдения нормативных требований, но и оказывает влияние на все секторы производственно-сбытовой цепочки организации, влияет на работу процессоров и контроллеров данных. Поставщики облачных услуг должны полностью пересмотреть свои процессы, пересмотреть способы хранения и обработки личных данных, чтобы обеспечить полное соответствие, что

повысит ценность, и определить новые способы улучшения обслуживания клиентов с полной безопасностью данных. Чтобы реализовать все положения GDPR, поставщики облачных услуг должны провести тщательный анализ всех процедур безопасности организации и стандартов защиты данных, а также пересмотреть роли и обязанности. Следует инициировать повторную проверку состояния данных организации, относящихся к личным и конфиденциальным личным данным. Необходимо запланировать различные требования GDPR, внедрить организационные и технологические подходы для решения проблем и усилить политику и процедуры для уменьшения наихудших результатов. процедуры защиты данных должны быть разработаны по умолчанию, а стандарты поставщиков облачных услуг должны быть улучшены, чтобы соответствовать требованиям закона.

Внутренний аудит может показаться утомительным процессом, но он намного менее болезнен и затратен, чем выяснение того, что компания или один из ее облачных сервисов нарушили GDPR и в конечном итоге сталкиваются с расследованием со стороны регуляторов данных и потенциально крупными штрафами.

Такой аудит также может привести к выявлению недостатков в существующей ИТ-инфраструктуре и процессах компании и позволит принять меры по оптимизации, чтобы обеспечить наиболее эффективную работу как бизнеса, так и ИТ-операций

Для многих компаний GDPR - сложный проект. Правовые, технические и организационные проблемы, связанные с GDPR, пока решены лишь частично. В частности, в случае крупных проектов миграции в среде облачных вычислений, в среде IoT или в сценариях больших данных повседневный бизнес оставляет мало времени для беспокойства о реализации GDPR. Однако, помимо многочисленных проблем внедрения, GDPR также предлагает возможность преуспеть за счет переопределения и внедрения новых стратегий защиты данных и ИТ-безопасности, особенно в контексте облачных вычислений.

Один из простых способов продемонстрировать соответствие требованиям безопасности и «Конфиденциальности» - это получить сертификаты ISO 27001, ISO 27701 или ISO 27018. Если нет, они могут продемонстрировать это с помощью выполненной оценки воздействия на защиту данных (DPIA) и / или оценки безопасности. Таким образом, InCountry является привлекательной для клиентов и партнеров так как соответствует стандартам ISO 27001, ISO 27017, ISO 27701.

Получить оценки экономической эффективности предлагаемых в диссертации решений в общем виде не представляется возможным так как стоимость сервиса для клиентов рассчитывается индивидуально в зависимости от модели развертывания и используемых функций, однако и разработанная комплексная система по хранению и обработке данных, и политика продвижения, и концепция новой услуги - все это позволит компании, работающей на рынке облачных сервисов, в данной диссертации компании InCountry, существенно увеличить конкурентоспособность своих

ИТ-решений, усилить позиции на рынке и обеспечить долгосрочную финансовую устойчивость.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1 - А] Хлистовская М.И., Законы о резиденстве данных /Хлистовская М.И// Международной научно-практической конференции «ПЕРСПЕКТИВЫ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ» от 31.03.2021

[2 - А]Хлистовская М.И., Хранение данных в облаке /Хлистовская М.И// Международной научно-практической конференции «ПЕРСПЕКТИВЫ РАЗВИТИЯ НАУКИ И ОБРАЗОВАНИЯ» от 31.03.2021