УДК 004.056.55 DOI: 10.14529/ctcr160306

ЗАЩИТА ОБЛАЧНОЙ БАЗЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ГОМОМОРФНОГО ШИФРОВАНИЯ

Л.В. Астахова, Д.Р. Султанов, Н.А. Ашихмин

Южно-Уральский государственный университет, г. Челябинск

Обоснована возможность использования гомоморфного шифрования для защиты облачной базы персональных данных при соблюдении действующих нормативных правовых актов по защите персональных данных. Рассмотрены существующие варианты реализации алгоритмов гомоморфного шифрования. Обоснован амбивалентный подход к использованию виртуального сервера для хранения персональных данных и других ценных информационных активов организации на основе гомоморфного шифрования и ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». Проведен анализ экономической эффективности обоснованной модели в организации без использования и с использованием облачных технологий. Обоснованный подход не только соответствует всем требованиям российского законодательства по персональным данным, но и дает возможность получить экономическую выгоду, позволяя масштабировать сервер с меньшими затратами.

Ключевые слова: персональные данные, облачные технологии, гомоморфное шифрование, CryptoDB, базы данных.

Введение

Современная практика требует использования большого количества данных, повышения возможностей их использования, хранения и передачи. Одними из активно развивающихся технологий являются облачные вычисления, технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис [1]. Многие компании уже ощутили потребность в применении распределённых систем, использующих облачные технологии. Но существуют вопросы безопасности при использовании облачных технологий. Физическое расположение облачных сервисов практически невозможно отследить, данные могут располагаться в разных странах и часто дублироваться. Кроме того, компании, предоставляющие облачные сервисы, могут быть под юрисдикцией другого государства и не обеспечивать соблюдение российских законов о защите информации. Из-за этих факторов мы не можем доверять облачным ресурсам и должны использовать шифрование при работе с ними. Криптография является одним из основных методов обеспечения конфиденциальности, аутентичности и контроля целостности информации и используется с древнейших времен.

Тем не менее, защищённое соединение с удаленными ресурсами и даже зашифрованная база данных (БД) на сервере не гарантирует невозможности расшифровки данных, если приватный ключ шифрования будет храниться на облачном сервисе вместе с БД. Передача при каждом запросе целых таблиц на клиента, где происходит расшифровка и обработка запроса, очень накладна и требует много времени и вычислительных мощностей. Это нивелирует основные преимущества использования облачных сервисов [2]. Поэтому возникает необходимость выполнять действия над зашифрованной БД без ее расшифрования.

Данную задачу в 1978 г. впервые поставили изобретатели RSA алгоритма Рональд Ривест, Ади Шамир и Леонард Адлеман в своей статье [3], но они сочли задачу решаемой лишь частично.

Гомоморфное шифрование – именно так называется форма шифрования, позволяющая выполнять математические действия над зашифрованными данными, и получать результат, который соответствует результату операций, выполняемых с открытыми данными. Выделяют частично гомоморфные и полностью гомоморфные криптосистемы.

$$D(E(t_1)) + D(E(t_2)) = t_1 + t_2; \quad (1)$$

$$D(E(t_1)) \cdot D(E(t_2)) = t_1 \cdot t_2, \quad (2)$$

где D – функция расшифрования, E – функция зашифрования, а t_1 и t_2 – открытые тексты.

Внутри частично гомоморфных криптосистем поддерживается либо (1), либо (2) равенство. Внутри полностью гомоморфной криптосистемы поддерживаются сразу оба равенства. Так, например, RSA – частично гомоморфная криптосистема относительно операции умножения.

Спустя 31 год была создана первая криптосистема, удовлетворяющая сразу двум равенствам. В 2009 г. исследователь IBM Крейг Джентри теоретически обосновал в своей работе [4] систему, позволяющую осуществить требуемое шифрование. Схема Джентри является криптосистемой с открытым ключом. В настоящее время разработаны как полностью гомоморфные симметричные криптосистемы [5], так и доработана схема Джентри и предложены другие схемы полностью гомоморфного шифрования [6].

Поскольку было доказано существование гомоморфных криптосистем и разработаны практические варианты реализации некоторых алгоритмов, считаем, что эти алгоритмы могут применяться в практике защиты информации. Однако в отношении облачных баз персональных данных возникает проблема.

Проблема использования гомоморфного шифрования облачных баз персональных данных

В современном обществе все чаще небольшие предприятия предпочитают использовать облачные технологии для хранения своих баз данных, в том числе персональных данных. Но внутри облака, согласно законодательству Российской Федерации, не всегда можно хранить информацию. Мы не можем хранить данные, если:

– облако находится за пределами Российской Федерации [7] (ст. 2 «*5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона*»);

– каналы передачи данных до облака не являются безопасными [8] (гл. 4, ст. 19, п. 2: «Обеспечение безопасности персональных данных достигается, в частности… *2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации*»);

– внутри самого облака не реализованы меры защиты информации, либо используются не сертифицированные средства защиты информации [8] (гл. 4, ст. 19, п. 2).

Шифрование позволяет сохранять конфиденциальность и целостность данных внутри недоверенного облачного ресурса, если данный ресурс не обладает приватным ключом. Использование обычного (симметричного шифрования из ГОСТ) вида шифрования для данных целей требует больших накладных расходов для передачи и расшифрования всей базы данных на стороне клиента. При использовании гомоморфного шифрования накладные расходы будут сопоставимы с использованием открытой базы данных, а также будет сохранена конфиденциальность и целостность информации. Меры по обеспечению доступности информации могут входить в договор предоставления облачной инфраструктуры.

Однако возникает вопрос: как, используя гомоморфное шифрование, выполнить требование использовать сертифицированные СКЗИ при защите персональных данных? Согласно [9] (гл. 2, п. 27), «*при разработке СКЗИ рекомендуется использовать криптографические алгоритмы, утвержденные в качестве национальных стандартов или определенные перечнями, утверждаемыми в порядке, установленном постановлением Правительства Российской Федерации от 23 сентября 2002 года N 691*» (последнее постановление утратило силу в связи с принятием Постановления Правительства РФ от 16.04.2012 N 313 [10]).

Для решения названной проблемы мы предлагаем разработать СКЗИ на основе: 1) гомоморфного шифрования и 2) ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [11]. Назовем данный подход совместного использо-

вания двух криптографических алгоритмов *амбивалентным*. После разработки СКЗИ на основе этого подхода его следует сертифицировать. Рассмотрим подробнее.

Обзор существующих решений

Назовем *защищённой* такую базу данных, которая позволяет не хранить ключ шифрования на сервере. На данный момент существует несколько вариантов реализации таких систем за рубежом и в России: защищённая база CryptDB, защищенная база НГУ и др.

Защищённая база CryptDB

Одной из самых известных защищённых баз данных является разработка Массачусетского технологического института – база CryptDB [12]. Эта база данных реализует концепцию *луковичного шифрования*, то есть шифрование данных последовательно различными алгоритмами, которые расположены в порядке увеличения криптостойкости, то есть внизу лежат наименее стойкие алгоритмы. Каждый уровень шифрования позволяет производить определенные действия над данными, такие как сложение, умножение и сравнение (табл. 1).

Таблица 1

Алгоритмы шифрования, применяемые в CryptDB

№	Название	Описание
0	Исходные данные	Хранит незашифрованные данные
1	Гомоморфное шифрование (DET)	Позволяет выполнять арифметические операции над данными
2	Шифрование, сохраняющее порядок (OPE)	Позволяет выполнять операции сравнения и сортировки над данными
3	Детерминированное шифрование (DET)	Позволяет проверять эквивалентность сообщений
4	Вероятностное шифрование (RND)	Обеспечивает наибольшую стойкость, не позволяет выполнять никаких операций

Рассмотрим пример использования базы данных. Допустим, нам нужно выбрать все поля из таблицы Person с параметром Age < 30. Тогда выполнится следующий алгоритм (рис. 1):

1) пользователь отправляет свой запрос к базе данных, предварительно зашифровав данные до максимального уровня.

2) база данных определяет тип запроса и слой, до которого необходимо расшифровать базу данных, в нашем случае это OPE;

3) база данных запрашивает у пользователя ключи для уровней RND и DET и расшифровывает их;

4) далее она выполняет поиск на уровне OPE и отправляет результат пользователю;

5) пользователь на своей машине расшифровывает уровни OPE и HOM и получает результат запроса.

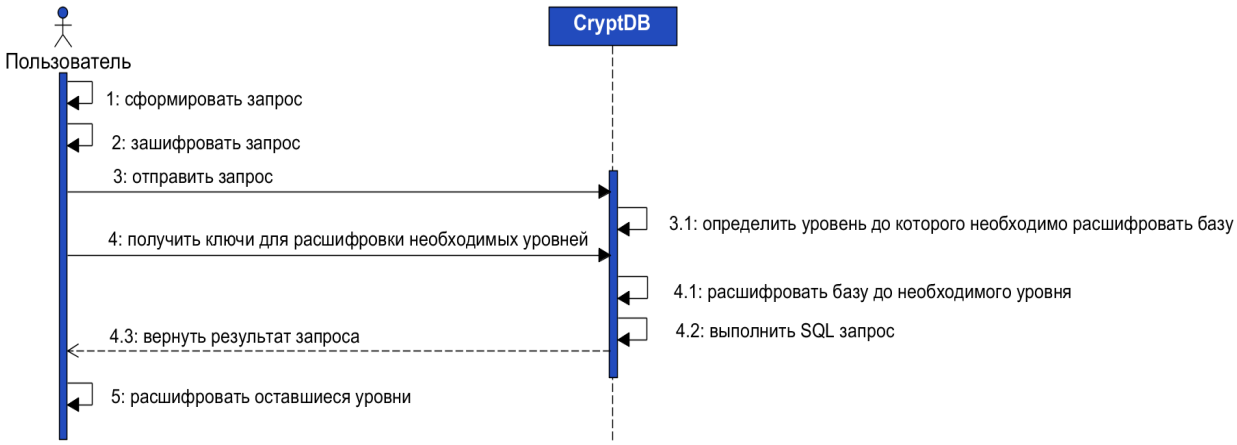

Рис. 1. Алгоритм обработки запросов в CryptDB

В худшем случае при правильно сформулированном запросе база данных защищена, как минимум, одним слоем шифрования и данные никогда не бывают полностью расшифрованы в небезопасной среде, что является основным плюсом этой базы данных. Поэтому, как отмечают эксперты, безопасность данной БД является гарантированной [13]. Авторы заявляют также о высокой скорости работы данной базы, поскольку производительность ухудшается всего на 14,5–26 %, по сравнению с MySQL [11] (рис. 2).

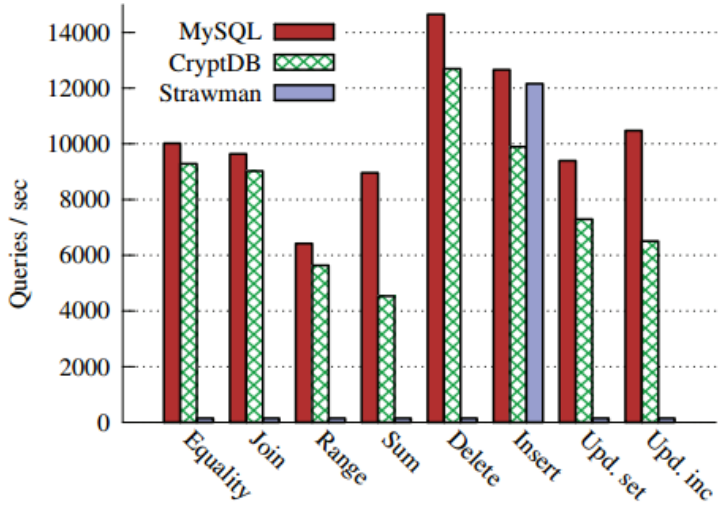

Рис. 2. Сравнение скорости работы СУБД CryptDB с другими СУБД

Кроме того, CryptDB является проектом с открытым исходным кодом и распространяется с лицензией GPL [14].

Но CryptDB имеет и свои существенные минусы:

Во-первых, уязвимым моментом является то, что к базе данных постоянно передаются ключи всех, кроме последнего, уровней шифрования, что в условиях потенциально скомпрометированного облачного сервиса, может привести к их утечке. В этом случае данные будут защищены лишь одним уровнем гомоморфного шифра.

Во-вторых, при правильно подобранных запросах база данных будет защищена наименее стойким гомоморфным методом шифрования. В статье А.В. Трепечевой [15] показывается уязвимость данного метода шифрования при известных открытых текстах, позволяющая в некоторых случаях установить ключ шифрования.

В-третьих, в CryptDB используются зарубежные алгоритмы шифрования. Для сертифицированных СКЗИ в российском законодательстве отсутствуют требования использования только российских алгоритмов шифрования, но, несмотря на это, на практике не встречаются сертифицированные средства криптографической защиты информации, которые используют зарубежные алгоритмы шифрования. В рамках CryptDB данная особенность исправляется только заменой функций шифрования внутри средства, что влечет за собой их разработку и тестирование.

Защищённая база данных НГУ

Существует еще одна защищенная база данных, создаваемая в Новосибирском государственном университете [15]. Она так же, как и CryptDB, построена на принципе луковичного шифрования. Отличие состоит в том, что она позволяет сразу указывать, какие операции необходимо выполнять над данными, и шифрует тем алгоритмом, который позволяет их обеспечить. Например, если мы выполняем поиск по столбцу NAME, то его необходимо шифровать с сохранением порядка, а если столбец LOCATION не участвует в поиске, то его можно шифровать самыми стойкими алгоритмами. Таким образом, защищенная база данных изначально хранит все зашифрованные сообщения в форме, позволяющей выполнять требуемые операции и, в отличие от модели CryptDB, не требует дешифрования данных на стороне сервера.

Данная криптосистема обладает рядом преимуществ перед зарубежной CryptDB: не требуется дешифрования данных на стороне клиента; применены алгоритмы шифрования, разработан-

ные университетом. Но главным недостатком остается отсутствие готовой реализации, несмотря на полностью описанные подходы и принципы построения базы данных [15].

В Новосибирском государственном университете теоретически описаны принципы защищенного калькулятора и разработаны два алгоритма шифрования: алгоритм вероятностного блочного шифрования и алгоритм сохраняющего порядок шифрования.

Обоснование применения CryptDB вместе с ГОСТ Р 34.12–2015

Согласно законодательству по персональным данным [8] (гл. 4, ст. 19, п. 2), «*обеспечение безопасности персональных данных достигается, в частности… 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации*». Разрешается использовать для их защиты только сертифицированные шифровальные программы российского производства, созданные на основе ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [11]. Любое сертифицированное СКЗИ, разработанное в России, должно использовать национальный стандарт как основной алгоритм шифрования. В связи с этим используем частично гомоморфную криптосистему CryptDB вместе с российским ГОСТ Р 34.12–2015.

СУБД CryptDB выполнена в роли надстройки, способной работать с СУБД MySQL 5.1 и PostgreSQL 9, не требуя модификации кода СУБД. Для того чтобы данную надстройку можно было применять в организациях Российской Федерации как средство криптографической защиты информации (СКЗИ), необходимо его сертифицировать. Так как алгоритм из ГОСТ Р 34.12–2015 не является гомоморфным, нет возможности использовать его в структуре луковичного шифрования CryptDB без передачи приватного ключа.

Но возможность использования стандарта остается. Если в базе данных все поля, по которым не осуществляется поиск внутри облака, шифровать с использованием российского стандарта и гомоморфного алгоритма, а остальные поля шифровать только с использованием гомоморфного шифрования, то данная амбивалентная система защиты будет криптостойкой и соответствовать всем требованиям законодательства Российской Федерации.

В этом случае одна из таблиц базы данных (на примере базы персональных данных пациентов больницы, хранящейся в облаке) будет выглядеть следующим образом (рис. 3).

Пациент (а)	**8AEAE339798 (б)**	**20c300e08ba85 (в)**
Имя	Имя	fe8c2372f7f3265802d
Фамилия	Фамилия	802dbbec46e10ce
Отчество **ГОСТ**	35F95C81 9E9B6BD6	415b628784d8e6d5d7f
Полис ОМС **ГОСТ**	464A7FAB 6898B5F3	9cf62d4fb6d619ede6d3
Диагноз **ГОСТ**	01260D36 BAF083FD	7eebc1856b2d4eb2bea
Лечащий врач **ГОСТ**	21EF93CC 43F5C626	26169814a90424413ff
Группа крови **ГОСТ**	55D3CE79 7D603A2D	c300e08ba85fc4baaf45

Рис. 3. Пример структуры таблицы базы данных (а), запись из таблицы с использованием шифрования на основе ГОСТ Р 34.12–2015 (б), запись из таблицы с использованием шифрования на основе ГОСТ Р 34.12–2015 и CryptDB (в)

На рис. 3 показан пример структуры одной таблицы, где указаны все существующие в таблице поля (а); изображена одна запись из таблицы, к которой применен алгоритм шифрования из стандарта РФ (б), при этом поля «имени» и «фамилии» не затронуты, а зашифрованные поля невозможно разделить; изображена одна запись из таблицы, к которой уже был применен алгоритм из российского стандарта и алгоритм шифрования из CryptDB (в). Как видно, структура таблицы изменилась, название таблицы также шифруется.

Все поля, отмеченные «ГОСТ», зашифрованы вместе с использованием ГОСТ Р 34.12–2015. Остальные поля зашифрованы как с использованием ГОСТ, так и с использованием гомоморфного алгоритма.

Так как имя, фамилия и отчество человека не определяют его, можно утверждать, что в случае дешифрования гомоморфного алгоритма злоумышленник получит только обезличенные персональные данные, и лишь в случае дешифровки двух алгоритмов он сможет получить открытые данные.

При применении данного подхода – совместного использования ГОСТ Р 34.12–2015 и СУБД CryptDB – становится возможным создание нового средства криптографической защиты информации и последующей его сертификации. Амбивалентный подход позволяет использовать мощности облачных технологий и соблюдать при этом законодательство Российской Федерации в области защиты персональных данных.

Обоснование экономической выгоды использования модели гомоморфного шифрования

Несмотря на то, что амбивалентный подход удовлетворяет требованиям законодательства Российской Федерации, его использование экономически не обосновано в случаях, когда организация хранит все данные на своем выделенном сервере.

Рассчитаем стоимость использования собственного сервера.

Так как необходимо получить достоверный сравнительный анализ, будем использовать доступное техническое оборудование и программное обеспечение для расчета стоимости. Рассмотрим файловый сервер организации, располагающей 50 автоматизированными рабочими местами.

Работу по размещению, настройке и соединению сервера с рабочими станциями, а также работу специалиста, ответственного за непрерывную работу сервера, учитывать не будем. В таком случае стоимость организации файлового сервера будет складываться из технического оборудования и программных средств. Для иллюстрации возьмем цены, актуальные на апрель 2016 г. (табл. 2).

Для организации файлового сервера, который доступен всем сотрудникам, потребуется приобрести техническое оборудование: сервер; периферийные устройства для настройки сервера и управления им; коммутаторы; соединительные линии.

Кроме того, есть необходимость соблюдать требования ФЗ-152 (гл. 4, ст. 19, п. 2) [8], для чего необходимо установить на сервер программное обеспечение, выполняющее минимальные требуемые функции. К нему относятся: операционная система; программа защиты от несанкционированного доступа; программа межсетевого экранирования; программное антивирусное средство (табл. 3).

Таблица 2

Расчет стоимости серверного технического оснащения

Наименование технического средства	Стоимость, руб.	Количество, шт.
Сервер		
Сервер SL1000/TminiG3	66 437	1
Периферийные устройства		
Монитор Samsung S20D300NH	6460	1
Мышь Intro MU109 черный	299	1
Клавиатура Oxion OKB006BK	340	1
Коммутаторы		
Роутер TP-LINK TL-WR841N(RU)	1490	1
Соединительные линии		
Коммутационный шнур СКС «SNR» 1.5 м	73	1
Витая пара BaseLevel 1 м	375	25

Общая стоимость технического оборудования составляет 75 474 руб.

Таблица 3

Расчет стоимости серверного программного обеспечения

Наименование программного обеспечения	Стоимость, руб.	Количество, шт.
Операционная система		
Microsoft Windows Server Standard 2012 R2	41 349	1
Средство защиты от несанкционированного доступа		
Secret Net 7	7700	1
Межсетевой экран		
TrustAccess	15 675	1
Антивирусное средство защиты		
Dr.Web Server Security Suite	6500	1

Общая стоимость программного обеспечения составляет 71 224 руб.

Кроме того, каждый год необходимо продлевать права на использования программных средств. Например: Secret Net 7 – 7425 руб.; TrustAccess – 10 780 руб.; Dr.Web Server Security Suite – 4550 руб.

В конечном итоге для организации, которой необходим файловый сервер, покупка технического оснащения и программных средств обойдётся в **146 698** руб. и каждый год необходимо затрачивать **22 755** руб. на продление прав использования программных средств защиты информации.

Рассчитаем стоимость использования виртуального сервера.

Использование виртуального сервера от компании Ростелеком с характеристиками, достаточными для выполнения функций файлового сервера (OS Windows Server, 250 Гбайт дискового пространства, 1 процессор, база данных MySQL 1 Гбайт, резервное копирование на 7 дней 50 Гбайт) обойдется в **25 250** руб. в год, при среднем количестве рабочих дней, равном 250.

Использование виртуального сервера от компании 1cloud с характеристиками, достаточными для выполнения функций файлового сервера (OS Windows Server 2012 R2 x64 (Ru), 250 Гбайт дискового пространства, 1 процессор, 2 Гбайт оперативной памяти, резервное копирование на 7 дней) обойдется в **22 832** руб. в год при среднем количестве рабочих дней, равном 250.

Затраты на приобретение серверного оборудования и покупку необходимых программ сопоставимы с 6 годами использования виртуального сервера.

Таким образом, если рассматривать среднесрочный, пятилетний период, то использование облачного хранилища, вместо покупки сервера, позволит сэкономить до 54 % бюджета, что подтверждает экономическую эффективность предложенного подхода.

Выводы

Обоснованный в статье подход использования виртуального сервера для хранения персональных данных и других ценных информационных активов организации на основе гомоморфного шифрования имеет большие перспективы в практике защиты персональных данных. Он не только соответствует всем требованиям российского законодательства, но и позволяет получить экономическую выгоду, позволяя масштабировать сервер с меньшими затратами. Для применения на практике необходимо разработать и сертифицировать базу данных, строящуюся на предложенных принципах.

Учитывая темпы развития облачных технологий, их гибкость и экономичность, данный подход является актуальным как для маленьких, так и для больших организаций, обрабатывающих персональные данные. Новизна данного подхода заключается в синтезе гомоморфного и симметричного алгоритмов шифрования, предложенных принципах разработки СУБД, удовлетворяющей требованиям российского законодательства.

Литература

1. The Business Perspective of Cloud Computing: Actors, Roles and Value Networks / S. Leimeister, M. Böhm, C. Riedl, H. Krcmar // Proceedings of 18th European Conference on Information Systems (ECIS'10), Pretoria, South Africa, June 7–9 2010. – Pretoria, 2010. – P. 245–256.

2. Executing SQL over Encrypted Data in the Database-Service-Provider Model / H. Hacigümüş, B. Iyer, C. Li, S. Mehrotra // Proceedings of the 2002 ACM SIGMOD international conference on Management of data. – ACM, 2002. – P. 216–227. DOI: 10.1145/564691.564717

3. Rivest, R.L. On data banks and privacy homomorphisms / R.L. Rivest, L. Adleman, M.L. Dertouzos. // Foundations of secure computation. – 1978. – Vol. 32, no. 4. – P. 169–178.

4. Gentry, C. A fully homomorphic encryption scheme / C. Gentry. – Stanford University, Ph.D. thesis, 2009.

5. Макаревич, О.Б. Полностью гомоморфное шифрование с использованием матричных уравнений, не имеющих корней / О.Б. Макаревич, Ф.Б. Буртыка // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 219–224.

6. Полностью гомоморфное шифрование (обзор) / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Вопросы защиты информации. – 2015. – № 3. – С. 3–26.

7. Федеральный закон от 21.07.2014 N 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». – https://www.consultant.ru/document/cons_doc_LAW_165838 (дата обращения: 20.05.2016).

8. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015). – http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 20.05.2016).

9. Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66 г. Москва «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». – http://www.consultant.ru/document/Cons_doc_LAW_52098 (дата обращения: 20.05.2016).

10. Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». – http://www.consultant.ru/document/cons_doc_LAW_128739 (дата обращения: 20.05.2016).

11. ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». – М.: Стандартинформ, 2015. – 25 с. – http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 20.05.2016).

12. CryptDB: Protecting Confidentiality with Encrypted Query Processing / R.A. Popa, C.M.S. Redfield, N. Zeldovich, H. Balakrishnan // Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP). – Cascais, Portugal, October 2011. – P. 85–100.

13. Трепечева, А.В. Дерандомизационная криптостойкость гомоморфного шифрования / А.В. Трепечева // Труды Института системного программирования РАН. – 2015 – Т. 27, вып. 6. – С. 381–394. DOI: 10.15514/ispras-2015-27(6)-24

14. Трепечева, А.В. Криптоанализ полностью гомоморфных текстов / А.В. Трепечева // 18-я Международная телекоммуникационная конференция молодых ученых и студентов «Молодежь и наука»: тр. конф., Москва, 1 октября – 20 декабря 2014 г. – М., 2014. – С. 245–256.

15. Егорова, В.В. Схема адаптивного шифрования для эффективного хранения зашифрованных данных в защищенной базе данных / В.В. Егорова // Материалы 52-й Международной научной студенческой конференции «Студент и научно-технический прогресс». Информационные технологии: материалы конф., Новосибирск, 11–18 апреля 2014 г. – Новосибирск, 2014. – С. 48.

Астахова Людмила Викторовна, д-р пед. наук, профессор, профессор кафедры безопасности информационных систем, Южно-Уральский государственный университет, г. Челябинск; lvastachova@mail.ru.

Султанов Денис Радикович, студент кафедры безопасности информационных систем, Южно-Уральский государственный университет, г. Челябинск; sultanov-57@mail.ru.

Ашихмин Никита Андреевич, студент кафедры системного программирования, Южно-Уральский государственный университет, г. Челябинск; veoring@gmail.com.

Поступила в редакцию 22 мая 2016 г.

DOI: 10.14529/ctcr160306

PROTECTION OF CLOUD DATABASE CONTAINING PERSONAL INFORMATION USING HOMOMORPHIC ENCRYPTION

***L.V. Astakhova**, lvastachova@mail.ru,*
***D.R. Sultanov**, sultanov-57@mail.ru,*
***N.A. Ashikhmin**, veoring@gmail.com*
South Ural State University, Chelyabinsk, Russian Federation

In this article, we prove the possibility of using homomorphic encryption for protection of cloud database containing personal information in compliance with the existing normative legal acts on the protection of personal data. We reviewed existing implementations of homomorphic encryption algorithms. We substantiated ambivalent approach to the use of virtual server to store personal data and other valuable information assets of organization based on homomorphic encryption and GOST R 34.12.2015 "Information technology. Cryptographic protection of information. Block ciphers". We performed analysis of economic efficiency of approved model in the organization with and without use of cloud technologies. Our approach not only meets all the requirements of the Russian legislation, but also enables to obtain economic benefit by allowing to scale server at lower cost.

Keywords: personal information, cloud technologies, homomorphic encryption, CryptoDB, databases.

References

1. Leimeister S., Böhm M., Riedl C., Krcmar H. The Business Perspective of Cloud Computing: Actors, Roles and Value Networks. *Proc. of 18th European Conference on Information Systems (ECIS'10), Pretoria, South Africa*, June 7–9 2010. Pretoria, 2010, pp. 245–256.

2. Hacigümüş H., Iyer B., Li C., Mehrotra S. Executing SQL over Encrypted Data in the Database-Service-Provider Model. *Proc. of the 2002 ACM SIGMOD International Conference on Management of Data, ACM*, 2002, pp. 216-227. DOI: 10.1145/564691.564717

3. Rivest R.L., Adleman L., Dertouzos M.L. On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation*, 1978, vol. 32, no. 4, pp. 169–178.

4. Gentry C. A Fully Homomorphic Encryption Scheme. Stanford University, *Ph.D. Thesis*. 2009.

5. Makarevich O.B., Burtyka F.B. [Fully Homomorphic Enciphering Using Rootless Matrix Equations]. *Information Counteraction to the Terrorism Threats*, 2014, no. 23 (23), pp. 219–224 (in Russ.)

6. Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V. [Fully Homomorphic Encryption (Review)]. *Scientific Editions of FSUE "VIMI"*, 2015, no. 3 (110), pp. 3–26. (in Russ.)

7. *Federal'nyy zakon ot 21.07.2014 N 242-FZ (red. ot 31.12.2014)* [On Amendments to Certain Legislative Acts of the Russian Federation in Terms of Clarification of the Order of Processing of Personal Data in the Information – telecommunication networks] Available at: https://www.consultant.ru/document/cons_doc_LAW_165838 (accessed 20 May 2016).

8. *Federal'nyy zakon ot 27.07.2006 N 152-FZ (red. ot 21.07.2014)* [On Personal Data] Available at: http://www.consultant.ru/document/cons_doc_LAW_61801 (accessed 20 May 2016).

9. *Prikaz Federal'noj sluzhby bezopasnosti Rossijskoj Fede-racii ot 9 fevralya 2005 g. N 66 g. Moskva* [On Approval of the Development, Production , Realization and Operation of Encryption (cryptographic) Means of Information Protection (Regulations PKZ-2005)] Available at: http://www.consultant.ru/document/Cons_doc_LAW_52098 (accessed 20 May 2016).

10. *Postanovlenie Pravitel'stva RF ot 16.04.2012 N 313* [On Approval of Provision on Licensing Activities on the Development, Production, Distribution of Encryption (Cryptographic) Means, Information Systems and Telecommunication Systems Protected with Encryption (Cryptographic) Means, Performance of Works, Rendering Services in the Field of Information Encryption Services, Maintenance of Encryption (Cryptographic) Means , Information Systems and Telecommunication Systems Protected with Encryption (Cryptographic) Means (except if the Maintenance of Encryption (Cryptographic) Means, Information Aystems and Telecommunication Systems Protected with Encryption (Cryptographic) Means, is Carried out to Satisfy the Needs of the Legal Entity or Individual Entrepreneur)] Available at: http://www.consultant.ru/document/cons_doc_LAW_128739 (accessed 20 May 2016).

11. *GOST R 34.12–2015* [Information Technology. Cryptographic Protection of Information. Block Ciphers]. Moscow, Standartinform, 2015. 25 p. Available at: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (accessed 20 May 2016).

12. Popa R.A., Redfield C.M.S., Zeldovich N., Balakrishnan H. CryptDB: Protecting Confidentiality with Encrypted Query Processing. *Proc. of the 23rd ACM Symposium on Operating Systems Principles (SOSP) – Cascais, Portugal*, October 2011, pp. 85–100.

13. Trepacheva A.V. [Derandomization Security of Homomorphic Encryption]. *Proceedings of ISP RAS*, 2015, vol. 27, no. 6, pp. 381–394. (in Russ.) DOI: 10.15514/ispras-2015-27(6)-24

14. Trepacheva A.V. [Cryptanalysis Fully Homomorphic Texts]. *18-ya Mezhdunarodnaya telekommunikacionnaya konferenciya molodyh uche-nyh i studentov "Molodezh' i nauka": Trudy konferencii 1 oktyabrya – 20 dekabrya 2014g* [18th International Telecommunications Conference of Young Scientists and Students "Youth and Science": Conference Proceedings October 1 – December 20, 2014], Moscow, 2014. pp 245–256. (in Russ.)

15. Egorova V.V. [Scheme of Adaptive Enciphering for Effective Storage of the Ciphered Data in the Protected Database]. *Materialy 52-y Mezhdunarodnoy nauchnoy studencheskoy konferentsii "Student i nauchno-tekhnicheskiy progress". Informatsionnye tekhnologii: materialy konf., Novosibirsk, 11–18 aprelya 2014 g.* [Proceedings of the 52nd International Scientific Student Conferences "Student and Technological Progress". Information Technology: Proceedings of the Conference 11–18 April 2014]. Novosibirsk, 2014, p. 48. (in Russ.)

Received 22 May 2016

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Астахова, Л.В. Защита облачной базы персональных данных с использованием гомоморфного шифрования / Л.В. Астахова, Д.Р. Султанов, Н.А. Ашихмин // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 3. – С. 52–61. DOI: 10.14529/ctcr160306

FOR CITATION

Astakhova L.V., Sultanov D.R., Ashikhmin N.A. Protection of Cloud Database Containing Personal Information Using Homomorphic Encryption. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2016, vol. 16, no. 3, pp. 52–61. (in Russ.) DOI: 10.14529/ctcr160306