ОСНОВНЫЕ КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ, ПЕРЕДАВАЕМЫХ В ОБЛАЧНЫЕ СЕРВИСЫ И СЕТИ ХРАНЕНИЯ ДАННЫХ

Минаков С.С.[1]

Аннотация.

Цель работы: *разработка технологии криптографической защиты информации в сторонних облачных сервисах и сетях хранения данных с использованием стандартизированных интерфейсов и протоколов, алгоритмов блочного шифрования.*

Метод: *системный анализ деградации уровня безопасности информации при её обработке с использованием облачных вычислений. Анализ научной литературы в области теоретических и прикладных криптографических исследований, выявление ограничений гомоморфных методов шифрования. Синтез криптосистемы с использованием метода аналогии, алгоритмов хеширования и блочного шифрования.*

Полученный результат: *предложена перспективная криптографическая система «Утро» для обеспечения безопасности информации в облачных сервисах и в сетях хранения данных. Заданы её основные криптографические механизмы: функции, логика и схема шифрования для программной реализации с использованием алгоритмов блочного шифрования. Даны пояснения по практическому применению, предложенных механизмов криптографической защиты, к протоколам передачи данных типа iSCSI, FiberChannel, WebDAV и возможности их использования локально.*

Ключевые слова: *шифрование, облачные вычисления, криптографическая схема, сервис, сетевой протокол, безопасность информации.*

DOI:10.21681/2311-3456-2020-03-66-75

1. Введение

Проблемы обеспечения безопасности информации в облачных технологиях стали активно анализироваться достаточно поздно, когда облака были уже фактически стандартизированы[2] и сложилась иерархия процессов, методов и протоколов обработки и передачи информации[3]. Практика применения облачных вычислений и развёртывания виртуальной инфраструктуры[4] показала, что для защиты информации недостаточно уже имеющихся средств защиты от НСД к информации и криптографических средств, рассчитанных на применение в классических средствах вычислительной техники (далее — СВТ).

Во многом это связано с моделью угроз и нарушителя (далее — МУН): облачная среда увеличивает число уязвимостей и последствий атак [1], более того виртуальна и инфраструктура системы, развёртываемой в облачной среде. Поскольку облачная среда включает все уровни абстракции[5]: эмулируемую инфраструктуру (приложения, операционная система, виртуальные машины и виртуальная сеть), реальную техническую инфраструктуру (приложения, средства управления виртуализацией и гиперконвергенцией, операционные системы, технические средства и сетевое оборудование) – у атакующего есть несколько путей для нарушения безопасности облачного сервиса [2].

Например, уязвимости в облачном Web-приложении, которое не контролирует должным образом, вводимые данные [3, 4] могут вызвать алгоритмическую ошибку с передачей управления другой области памяти, либо обход правил разграничения доступа в системе и раскрытие «чувствительных» данных, хранящихся в центре обработки данных, к которому у web-приложения изначально не было доступа. Более того облачные технологии дают более широкий спектр возможностей для нарушителя в области манипулирования средой функционирования средств защиты информации, в том числе и для криптографических средств. Очевидна угроза обхода средств защиты информации, средств разграничения доступа или нарушение параметров их работы, в том числе вопросы НСД к ключевой информации.

В настоящее время общим решением [5, 6] является организация защиты периметра облачной инфраструктуры и обеспечение криптографической защиты информации, передаваемой по сетями коммутации пакетов стандарта IP/TCP, на базе криптографических

2 ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология» (ISO/IEC 17788:2014, IDT).

3 ГОСТ Р ИСО/МЭК 17826-2015 «Информационные технологии. Интерфейс управления облачными данными (CDMI)» (ISO/IEC 17826:2012, IDT).

4 ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».

5 Проект ГОСТ Р «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений. Общие положения» (www.fstec.ru).

1 Минаков Сергей Сергеевич, старший научный сотрудник, ФГКНУ «Академия криптографии Российской Федерации», г. Москва, Россия. E-mail: ss_minakov@mail.ru

протоколов типа SSL/TLS и IPSec, которая предполагает защиту данных только от третьей стороны в канале связи, доверяя сторонам криптографического протокола после осуществления их взаимной аутентификации.

При использовании сторонних сервисов облачных вычислений во многом утрачивается подконтрольность обрабатываемой и хранимой информации, существенно изменяется МУН [1, 7], что не позволяет наделять сторону облачных сервисов требуемыми гарантиями доверия и считать достаточными рубежи защиты на базе криптографических протоколов.

Таким образом необходимо переходить от криптографического протокола к криптографической схеме, в которой вторая участвующая сторона, реализующая службу облачных вычислений, не обеспечивает конфиденциальности и целостности данных пользователя и не может давать гарантий корректности реализаций механизмов обеспечения защиты информации при реализации облачных вычислений.

Для повышения эффективности защиты информации при использовании облачных вычислений и стандартизированных интерфейсов управления облачными данными CDMI (англ. – Cloud Data Management Interface) предложим основные криптографические механизмы защиты данных, передаваемых в облачные сервисы категории Data Storage as a Service (далее — STaaS / DSaaS) и сети хранения данных типа Storage Area Network (далее — SAN).

Здесь и далее по тексту работы будет предполагаться, что потребитель и пользователь службы облачных вычислений (англ. – cloud service customer, user) взаимодействует с таким облачным сервисом по стандартизированным интерфейсам CDMI, OCCI (англ. – Open Cloud Computing Interface) и протоколам типа WebDAV, CIFS, NFS и т. п. Соответственно пользователь сети хранения данных SAN передает в сеть данные, используя протоколы типа Fiber Channel (Connection) или iSCSI.

2. О применимости методов гомоморфного шифрования

Значительное внимание к применению гомоморфизмов в криптографических алгоритмах и схемах шифрования связано с двумя факторами: повышением эффективности систем обработки информации за счёт развёртывания высокоскоростных каналов связи, виртуализации компьютерной инфраструктуры и внедрения облачных вычислений с одной стороны, и появления математических систем полностью гомоморфного шифрования — с другой стороны [8].

За двадцатилетие произошла эволюция от частично гомоморфных способов к полностью гомоморфным системам шифрования и готовым разработкам [9], на текущем этапе развития такого криптографического метода международным коллективом авторов предложен вариант стандартизации систем гомоморфного шифрования [10].

В России также предложено несколько систем полностью гомоморфного шифрования [11, 12]. Отметим следующую интересную особенность применения гомоморфных способов шифрования — это возможность их использования в качестве одного из инженерно-криптографических[6] механизмов защиты. Например, реализация обработки информации в криптографической системе с аддитивной маской – $E_k^{CTR}(T) \oplus Mask = E_k^{CTR}(T \oplus Mask)$, что позволяет снимать такую маску $Mask$ только после расшифрования данных.

Метод гомоморфного шифрования интересен и при построении облачного сервиса (услуги) SECaaS (англ. – Security as a Service) для возможности реализации частично разделяемого шифрования [13] и «слепой» электронной подписи [14], а также централизованного использования в облачной инфраструктуре аппаратных модулей HSM (англ. – Hardware Secure Module) [15] при условии обеспечения их доверенной загрузки в такой среде [16].

Не менее востребованным может быть использование гомоморфного шифрования при построении облачной услуги SECaaS для ряда задач антивирусной защиты, межсетевого экранирования и обнаружения вторжений (компьютерных атак) в случае использования ими сигнатурных методов обнаружения и контроля.

Широкое внедрение гомоморфных систем шифрования сдерживается их невысокой вычислительной эффективностью [17], проблемой накопления ошибки расшифрования [10, 18] и вопросом обеспечения заданной стойкости гомоморфных шифров.

Необходимо отметить, что оценка криптографической стойкости гомоморфных систем для обеспечения конфиденциальности требует отдельного направления исследований. В частности, стойкость полностью гомоморфной криптографической системы на основе идеальных решеток (решеток со свойствами идеала на некотором кольце чисел) и методике Джентри [19] сводится к NP-полной задаче нахождения кратчайшего вектора. Существенным недостатком криптосистемы Джентри является то, что выполнение вычислений приводит к накоплению ошибки и, после того как она превышает некоторый порог, расшифровать сообщение становится невозможным [18].

Одним из вариантов решения данной проблемы является перешифрование данных после некоторого количества операций с ними, однако такой вариант снижает производительность вычислений и требует регулярного доступа к секретному ключу шифрования [17].

Следует также учитывать, что стойкость полностью гомоморфных криптосистем ограничена сверху [20-22], а во многих случаях они нестойки от определённых криптографических атак. Например, линейные полностью гомоморфные системы, основанные на задаче факторизации чисел [11], принципиально уязвимы к атаке с адаптивно

6 Понятия инженерно-криптографический (ИК) механизм, ИК-система, ИК-требования,ИК-свойства и т. п. используются в тождественном смысле и раскрыты в документе технического регулирования Р 1323565. 1.012.-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», а также в «Требованиях к средствам электронной подписи» и «Требованиях к средствам удостоверяющего центра», утверждённых приказом ФСБ России от 27.12.2011 №796 (опубликован).

подобранным шифрованным текстом [23], предложены атаки [24] по известным открытым текстам к гомоморфной системе Доминго-Феррера (1996 г.) и оставляют актуальным вопрос обеспечения конфиденциальности данных, передаваемых в облачную инфраструктуру, и требуют дальнейших исследований.

3. Построение криптографической схемы защиты данных, передаваемых в облачные хранилища на базе композиции стандартизированных алгоритмов блочного шифрования

Справедливости ради необходимо заметить, что применение алгоритма блочного шифрования с симметричным (секретным) ключом, например, криптоалгоритма по межгосударственному стандарту ГОСТ 34.12-2018 в режиме гаммирования (режим счётчика, CTR-режим), можно рассматривать в качестве реализации частично гомоморфной системы шифрования.

Рассмотрим перспективную криптографическую систему (далее — КС «Утро») на основе схемы шифрования данных, передаваемых в сторонний облачный сервис типа StaaS/DSaaS и сеть хранения данных SAN, в двух вариантах, соответственно, описывающих последовательность и логику информационного обмена, шифрование и имитозащиту с использованием алгоритма блочного шифрования, соответствующего документам технического регулирования (далее — варианты схемы «Утро-1» и «Утро-2»). В Российской Федерации и в странах СНГ такими стандартами являются ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015,ГОСТ Р 34.13-2015 и, соответственно, ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018 и ГОСТ 34.13-2018.

Для простоты будем использовать алгоритмы блочного шифрования и хеш-функции, соответствующие российским криптографическим алгоритмам ГОСТ Р 34.12-2015, 34.13-2015 и ГОСТ Р 34.11-2012. Обозначения криптографических значений и параметров, использованных в описании, соответствуют российским документам технического регулирования (стандартам, рекомендациям).

В работе будем использовать следующие обозначения.

V, V_m, V_0	— множество всех двоичных строк конечной длины, включая пустую строку, множество всех двоичных строк длины m, и множество, единственным элементом которого является пустая строка, соответственно;
$n_1 \| n_2$	— конкатенация строк $n_1, n_2 \in V$, т.е. строка из $V_{\|n_1\|+\|n_2\|}$, в которой подстрока с большими номерами компонент из $V_{\|n_1\|}$ совпадает со строкой n_1, а подстрока с меньшими номерами компонент из $V_{\|n_2\|}$ совпадает со строкой n_2;
$[T]_{i,j}$	— для битовой строки $T=(t_0,\ldots,t_n)$ подстрока $T`=(t_i,\ldots,t_j), 0 \le i \le j \le n$;
K	— исходный ключ длины 256 алгоритма блочного шифрования, определенного в ГОСТ Р 34.12-2015;
$H_{256}(T)$	— значение функции хеширования с длинной хэш-кода 256 бит, определенной ГОСТ Р 34.11-2012, для сообщения T;
N_{max}	— максимально допустимое количество блоков блочного шифра (объём материала), которые могут быть обработаны с использованием выбранного режима работы алгоритмом блочного шифрования без изменения значения ключа;
n	— двоичная длина блока блочного шифра, равная n =128 бит для шифра «Кузнечик» и n =64 бит для шифра «Магма»;

LBN	— максимально допустимое количество логических последовательно нумерованных блоков данных (англ. – Logical Block Numeration/Addressation), технически доступных к операциям ввода-вывода с накопителя информации, сетевого каталога или облачного хранилища в соответствии со спецификацией интерфейса взаимодействия с таким накопителем или хранилищем;
$\{K_{Num}\}, K_i$	— конечное множество ключей (базис ключей), формируемый на основе ключа и LBN для вычисления ключей блочного шифра в различных режимах шифрования и выработки имитовставки, и текущий ключ из такого базиса, соответственно;
$mode$	— указатель, определяющий режим работы алгоритма блочного шифрования и изложенный в ГОСТ Р 34.13-2015 (если иное не оговорено по тексту работы);
$E_k^{mode}(T)$	— функция криптографического преобразования в режиме $mode$ сообщения T с использованием ключа k, здесь и далее по тексту в качестве такой функции используется алгоритм блочного шифрования, определенного в ГОСТ Р 34.12-2015;
$MAC_k(T)$	— результат вычисления кода аутентификации сообщения T с использованием ключа k;
$KDF_{256}(T):\mathrm{V} \to V_{256}$	— функция вычисления производного ключа длины 256 на основе входного значения T;
$k\left(LBN, \{K_{Num}\}\right)$	— функция, вырабатывающая ключ блочного шифра длины 256 бит для двоичного блока данных, кратного длине блочного шифра длины n, на основе логического номера такого блока LBN и конечного базиса ключей $\{K_{Num}\}$;
<o>	— опциональный параметр схемы (может являться строкой нулевой длины);
A, B	— обозначения двух различных сторон, взаимодействующих между собой при криптографической защите данных, передаваемых в облачные сервисы и сети хранения данных;
k_{SAN}, K_{STaaS}	— обозначения ключа шифрования для сети хранения данных SAN и ключа шифрования для облачного хранилища или сетевого каталога – $STaaS$, соответственно;
R	— псевдослучайная последовательность длины t =256 бит;
Id_{obj}	— строка, содержащая уникальный идентификатор объекта облачного сервиса, сетевого каталога или сети хранения данных Obj стороны B, как правило, полный адрес и наименование ресурса Obj или аналогичный тому идентификатор-ссылку на ресурс Id_{obj}, используемые стороной A для однозначной идентификации сервиса хранения и адресации данных стороны B;
0^n	— нулевая последовательность длины n бит;

3.1 Вариант схемы «Утро-1» для защиты данных, передаваемых в облачные и сетевые хранилища

При взаимодействии с облачными сервисами хранения данных класса StaaS/DSaaS или сетевыми каталогами класса NAS (англ. – Network Attached Storage) участвуют две стороны A и B, при этом сторона A – клиент, реализует схему «Утро-1» и передает (получает) зашифрованные данные в (из) облачный (-ого) сервис (-а) хранения данных или сетевой каталог на стороне B – сервере облачного хранилища.

3.1.1. Начальное состояние и логика схемы «Утро-1»

Сторона B осуществляет техническое взаимодействие со стороной A, получает, обеспечивает хранение и выдает (передает) данные по запросу стороны A, и не должна принимать участие в непосредственной реализации криптографических функций и алгоритмов схемы Утро-1 для обеспечения криптографической защиты (шифрования и имитозащиты) данных стороны A.

Параметры протоколов, взаимодействия с облачными сервисами хранения данных класса StaaS/DSaaS или сетевыми каталогами класса NAS, в том числе аутентификационная информация пользователя облачных сервисов хранения, идентификаторы файла и каталога, считаются известными обеим сторонам и согласованными до начала протокола.

Сторона B хранит в облачном хранилище или в сетевом каталоге — $STaaS$ данные стороны A в виде файлов (файл-контейнеров) Obj (англ. – File Extent).

Сторона A зашифровывает и расшифровывает данные файл-контейнера Obj, подлежащие шифрованию, по фрагментно. Длины фрагментов кратны длине блока блочного шифра, равная n =128 бит для шифра «Кузнечик» и n =64 бит для шифра «Магма».

Данные файл-контейнера Obj (его фрагментов) передаются между сторонами A и B только в шифрованном виде.

3.1.2. Схема криптографической защиты данных, передаваемых в облачные сервисы хранения данных, «Утро-1» состоит из следующей последовательности действий:

Шаг 1. Сторона A определяет используемые значения идентификатора Id_{obj}, ключа K. Значение Num для расчёта $LBN = 2^{Num}$, как правило, однозначно определяется параметрами технического протокола взаимодействия между сторонами A и B.

Шаг 2. Сторона A передает стороне B идентификатор Id_{obj} и команду на совершения операции (чтение, запись, создание и др.) к файл-контейнеру Obj.

Шаг 3. При создании в облачном хранилище или сетевом каталоге стороны B файла-контейнера Obj стороной A вычисляется индивидуальный ключ для такого файл-контейнера Obj – ключ K_{STaaS} и базис ключей $\{K_{Num}\}$ (способ их вычисления указан в параграфе 3.3. статьи).

Шаг 4. Стороны A и B обмениваются данными файл-контейнера Obj по фрагментно.

Шаг 5. Сторона A зашифровывает каждый фрагмент файл-контейнера Obj одним выбранным алгоритмом блочного шифрования $E^{CTR}_{K(i,\{K_{Num}\})}(T_{i,Obj})$ в режиме гаммирования на ключе, соответствующем номеру фрагмента i – $k(LBN,\{K_{Num}\})$ с использованием значения синхропосылки (вектора инициализации – iv) равного конкатенации номеров фрагментов – $i||i$, кратной длине значения синхропосылки. Аналогичным образом рассчитывается значение имитозащитной вставки $MAC_k(Obj)$ зашифрованного фрагмента i файла-контейнера Obj.

Шаг 6. Сторона A посылает стороне B – зашифрованный фрагмент файл-контейнера Obj с номером i, значение $MAC_k(Obj)$ зашифрованного фрагмента i файла-контейнера Obj.

Расшифрование фрагмента i файл-контейнера Obj производится стороной A в обратном порядке, только после проверки совпадения вычисленной на соответствующем ключе имитовставки такого фрагмента и имитовставки, ранее записанной вместе с фрагментом i файл-контейнера Obj и присланной стороной B.

3.1.3. Пояснение к варианту схемы «Утро-1»

Для технических протоколов облачного хранения данных типа WebDAV REST API, а также протоколов сетевого файлового доступа к каталогам типа CIFS (англ. – Common Internet File System), NFS (англ. – Network File System) рекомендуется использовать значение LBN не менее $LBN \le 2^{32}$ и, соответственно, для каждого Id_{obj} выработать ключ K_{StaaS} с ключевым базисом $\{K_{32}\}$ с 66 ключами K_i, из которых $(K_0,\ldots,K_{32})$ – ключи шифрования и $(K_{33},\ldots,K_{66})$ – ключи имитозащиты.

3.2. Вариант схемы «Утро-2» для защиты данных, передаваемых в сети хранения данных

При взаимодействии в сети хранения данных класса Storage Area Network участвуют две стороны A и B, при этом:

- сторона A, реализует криптографическую схему У-2 и передает (получает) зашифрованные кадры интерфейса блочного доступа к накопителю информации, физически расположенного у стороны B;
- сторона B реализует физическое и/или логическое управление непосредственным доступом к устройству-накопителю Obj на блочном уровне (англ. – Drive Extent или Disk Extent) в соответствии с заданной технической спецификацией (блочные интерфейсы типа SATA, SAS, SCSI), стандартизированной для применения по сети передачи данных с использованием кадров канальных протоколов и/или пакетов сетевой коммутации.

3.2.1. Начальное состояние и логика схемы «Утро-2»

Параметры протоколов, взаимодействия сети хранения данных класса Storage Area Network, в том числе аутентификационная информация пользователя, идентификаторы точки подключения (условные адрес и имя устройства) – Id_{obj}, считаются известными обеим сторонам и согласованными до начала протокола.

Сторона B реализует сеть хранения данных SAN и предоставляет возможность доступа стороны A к накопителю Obj на блочном уровне с использованием идентификатора Id_{obj}.

Сторона A зашифровывает и расшифровывает данные кадров протокола блочного доступа к устройству Obj, команды протокола блочного доступа при необходимости подлежат только имитозащите. Длины таких кадров устанавливаются кратными длине блока блочного шифра, равная n =128 бит для шифра «Кузнечик» и n =64 бит для шифра «Магма».

Данные блочного доступа к устройству Obj, передаются между сторонами A и B только в шифрованном виде.

3.2.2. Схема криптографической защиты данных, передаваемых в облачные сервисы хранения данных, «Утро-2» состоит из следующей последовательности действий:

Шаг 1. Сторона A определяет используемые значения идентификатора Id_{obj}, ключа K. Значение Num для расчёта $LBN = 2^{Num}$, как правило, однозначно определяется параметрами технической спецификации интерфейса взаимодействия с накопителем и известно сторонами A и B.

Шаг 2. Сторона A передает стороне B идентификатор Id_{obj} и команду на совершения блочной операции (чтение, запись, создание и др.) к устройству Obj.

Шаг 3. При выделении (создании) в сети хранения данных на стороне B устройства Obj с идентификатором Id_{obj} стороной A вычисляется индивидуальный ключ для защиты устройства Obj – ключ k_{SAN}, и базис $\{K_{Num}\}$ (способ вычисления указан в параграфе 3.3. статьи).

Шаг 4. Стороны A и B реализуют блочный доступ к накопителю Obj по сети хранения данных с использованием Id_{obj}, содержимого блока данных и его номера i, подлежащего записи на накопитель Obj, либо результат чтения такого блока данных с номером i.

Шаг 5. Сторона A зашифровывает передаваемый (расшифровывает получаемый) стороне B каждый блок устройства Obj одним выбранным алгоритмом блочного шифрования в режиме гаммирования $E^{CTR}_{K(i,\{K_{Num}\})}(T_{i,Obj})$ на ключе, соответствующем номеру фрагмента i – $k(LBN,\{K_{Num}\})$ с использованием значения синхропосылки (вектора инициализации – iv) равного конкатенации номеров $i||i$, кратной длине значения синхропосылки. Аналогичным образом рассчитывается значение имитозащитной вставки $MAC_k(Obj)$ зашифрованного блока с номером i устройства Obj.

3.2.3. Пояснение к схеме «Утро-1»

Для технических протоколов сетей хранения данных типа FC/FiCon (англ. – Fiber Channel и Fiber Connection, соответственно) и iSCSI (англ. – internet Small Controller System Interface) рекомендуется использовать значение $LBN = 2^{64}$ и, соответственно, для каждого Id_{obj} выработать ключ K_{SAN} с ключевым базисом $\{K_{64}\}$ с 130 ключами K_i, из которых $(K_0,\dots K_{64})$ – ключи шифрования и $(K_{65},\dots K_{130})$ – ключи имитозащиты. Значение Id_{obj} может быть представлено в одной из стандартных систем обозначений: T11 Network Addrress Authority, Extended Uniq Identifier, либо iSCSI Qualified Name с учётом номера LUN (англ. – Logical Unit Number). Не рекомендуется размер кадров блочного доступа к устройству Obj в протоколах iSCSI (объём полезной загрузки кадра до 1400-1500 байт) и FC (объём полезной загрузки кадра до 2112 байт) устанавливать более 1392 байт и 2048 байт, соответственно.

3.3. О криптографических функциях КС «Утро» и их параметрах

В качестве источников псевдослучайных последовательностей R могут использоваться псевдослучайная функция PRF с длиной выхода 256 бит, определенная в рекомендациях по стандартизации Р 50.1.113-2016 или алгоритм выработки псевдослучайной последовательности R длины t =256 бит, определенный в рекомендациях по стандартизации Р 1323565.1.006-2017.

Код аутентификации сообщения $MAC_k(T)$ используется для решения задач имитозащиты передаваемых данных и должен формироваться одним из режимов алгоритма блочного шифрования $E^{mode}_k(T)$, например, ключевой функцией хеширования $OMAC1$ (стандартизована в ISO под названием $CMAC$), вычисляющая имитовставку длины n и определённая в ГОСТ Р 34.13–2015, либо функция хеширования $HMAC$, определенной в Р 50.1.113-2016.

Такое решение потребует увеличения вдвое размерности конечного базиса ключей $\{K_{Num}\}$ для раздельного использования ключей шифрования и ключей имитозащиты блоков данных в связи с существенно различной стойкостью $E^{CTR}_k(T)$ и $E^{CMAC}_k(T)$.

Поэтому наиболее интересным является использование вместо режима гаммирования в КС «Утро» AEAD-режима работы алгоритма блочного шифрования, который обеспечивает т. н. *аутентифицируемое шифрование*: шифрование и имитозащиту блока данных на одном ключе.

Исходя из критериев выбора таких режимов (доказуемая стойкость и вычислительная эффективность), можно предложить отечественные разработки: MGM-режим [25] и GCM'-режим [26], который несколько уступает классическому GCM-режиму работы алгоритма блочного шифрования, но устойчив [26] против атаки Фергюсона [27] на обычный GCM-режим.

DOI:10.21681/2311-3456-2020-03-66-75

Следует отметить, что центральное место в КС «Утро» (варианты «Утро-1» и «Утро-2») занимает этап вычисления производных ключей. Функция выработки производного ключа — KDF (англ. Key derivation function) является существенным компонентом криптографической схемы и должна создавать криптографически стойкие ключи для алгоритма симметричного шифрования на основе источника первоначального ключевого материала, обычно содержащего достаточное количество случайности, но распределённой неравномерно, или о которой нарушитель, производящий атаки, обладает частичной информацией.

В международном стандарте ISO 18033-2 даётся такое определение KDF - функция производного ключа $KDF(x,l)$ получает на вход байтовую строку x и число l. Результатом работы функции является байтовая строка длины l. Строка x может быть произвольной длины, хотя реализации могут ограничивать максимальную длину строки x и значение числа l, выдавая ошибку в случае превышения этих значений.

Основная сложность в использовании KDF связана с исходным ключевым материалом. В случае если исходный ключевой материал K представляет собой равномерный случайный или псевдослучайный ключ типа R, то достаточно просто воспользоваться им в качестве основы псевдослучайной функции, чтобы получить новые ключи. Однако, когда источник ключевого материала не является равномерно случайным, то необходимо извлечь случайность из источника и преобразовать к виду, подходящему для получения на её основе производных ключей.

В качестве функции вычисления производного ключа $KDF_{256}(T):V \to V_{256}$ могут использоваться как сама функция хеширования $H_{256}(T)$, определенная в ГОСТ Р 34.10-2012 с длиной выхода (свертки) 256 бит, так и её производные: алгоритм диверсификации $KDF\_GOSTR3411\_2012\_256$ с заданными параметрами и длиной выхода 256 бит, определенный в Р 50.1.113-2016, или схема функций выработки производных ключей $kdf(S,L,T,P,U,A)$ с заданными параметрами и длиной выхода 256 бит, определенная в Р 1323565.1.022-2018. При этом параметры таких функций могут быть однократно и единообразно заданы в СКЗИ с использованием псевдослучайных последовательностей R требуемой длины.

Вернемся к вычислению ключей k_{SAN}, K_{STaaS} з исходного ключа K, для объекта Obj постоянным символьным идентификатором Id_{obj} ключи K_{STaaS}, k_{SAN} ожно представить в виде функции $KDF_{256}\left(K \oplus H_{256}\left(Id_{obj}\right) \oplus \langle \circ \rangle\right)$ Тогда расчётный базис ключей $\{K_{Num}\}$ от ключей K_{STaaS}, k_{SAN} бъекта Obj ожно получить следующим образом.

Пусть LBN редставимо в виде $LBN = 2^{Num}$ где Num разрядность логической нумерации блоков данных, доступных к чтению-записи на накопителе, сетевом каталоге или облачном хранилище и кратная 2. При этом полагаем, что $10 \le Num \le 256$ Рассмотрим случай без использования $E_k^{MGM}(T)$ и $E_k^{GCM'}(T)$ размерность конечного базиса ключей $\{K_{Num}\}$ устанавливается равной $2*(Num+1)$ при этом первые $Num+1$ ключей такого базиса используются для шифрования $E_k^{CTR}(T)$ вторая часть базиса для вычисления и проверки $E_k^{CMAC}(T)$ кода аутентификации $MAC_k(T) = E_k^{CMAC}(T)$ на такие блоки данных, соответственно.

Тогда ключи в конечном базисе можно задать следующим образом, $K_t = KDF_{256}\left(H_{256}(t) \| k\right)$ (1) для $t = \overline{0, 2*Num+1}$ на весь период действия исходного ключа $k \in \left(k_{SAN}, K_{STaaS}\right)$. Сходным образом можно задать способ вычисления функции $\kappa(LBN, \{K_{Num}\})$ использованием конечного базиса ключей для блока данных накопителя SAN (фрагмента файла хранилища StaaS или каталога NAS) с номером i где $i = \overline{0, LBN - 1}$, $LBN = 2^{Num}$ $i = i_0 * 2^0 + \ldots + i_{Num-1} * 2^{Num-1}$. Для повышения вычислительной эффективности удобно использовать аддитивный способ задания функции $k\left(LBN, \{K_{Num}\}\right)$ для $E_\iota^{CTR}(T)$

$$\kappa(i, \{K_{Num}\}) = i_0 * K_0 \oplus \ldots$$
$$\ldots \oplus i_{(Num \div 2)-1} * K_{Num-2} \oplus \ldots$$
$$\ldots \oplus i_{Num-1} * K_1 \oplus K_{Num}$$

и, соответственно, значение функции $k\left(LBN, \{K_{Num}\}\right)$ для кода аутентификации сообщения $MAC_k(T)$ на такие блоки данных можно представить в виде (2):

$$k\,(i, \{K_{Num}\}) = i_0 * K_{Num+1} \oplus \ldots$$
$$\ldots \oplus i_{(Num \div 2)-1} * K_{2*Num-1} \oplus i_{Num \div 2} * K_{2*Num} \oplus$$
$$\ldots \oplus i_{Num-1} * K_{Num+2} \oplus K_{2*Num+2}$$

В среднем аддитивный способ формирования ключей (2) даёт 4-5 кратное преимущество в скорости вычислений производных ключей перед (1), но как говорилось ранее требует криптографического качества от исходного ключа K и потенциально уязвим к атакам на основе подобранных открытых текстов.

Для снижения уязвимости КС «Утро» к атакам различения на основе подобранного открытого текста и уменьшения развёртываемого ключевого базиса $\{K_{Num}\}$ предлагается использовать алгоритм блочного шифрования в MGM-режиме — $E_k^{MGM}(T)$, описанный в работе [25], а в качестве способа задания функции $k\left(LBN, \{K_{Num}\}\right)$ — функцию, соответствующую (1), где номер блока(фрагмента) i использовать в качестве вектора инициализации iv для $E_k^{MGM}(T)$ аналогично шагу 5 в описании КС «Утро».

3.4. О некоторых ограничениях при использовании КС «Утро»

Укажем, что конфиденциальность защищаемой информации при использовании КС «Утро» будет зависеть от следующих ограничений:

- обеспечение конфиденциальности (секретности) исходного ключа – K – режим работы $mode$ блочного шифра $E_k^{mode}(T)$ в соответствии с ГОСТ Р 34.13-2015 должен соответствовать указаниям Р 1323565.1.005—2017 при объёме материала $N_{max} \geq T$ для обработки на одном ключе, вычисленном функцией $k\left(LBN, \left[K_{Num}\right]\right)$, где T размер единовременно технически считываемого (записываемого) блока данных, кратный длине блока блочного шифра, равной n =128 бит для шифра «Кузнечик» и n =64 бит для шифра «Магма».
- в зависимости от условий эксплуатации и класса средств криптографической защиты информации и для защиты от утечки по побочным каналами необходимо учитывать целесообразность дополнения алгоритмов вычисления и использования конечного базиса ключей $\left\{K_{Num}\right\}$, формируемого на основе ключа K значения LBN механизмами маскированного использования ключевой информации в соответствии с рекомендациями Р 50.1.110-2016 и Р 50.1.112-2016.

4. Выводы

Предлагаемая КС «Утро» позволяет обеспечить криптографическую защиту данных, передаваемых для хранения в облачные сервисы и сети хранения данных. Характерной особенностью такой системы является логика и способ формирования производных ключей, позволяющий их рассчитывать в зависимости от адресации системы хранения данных и тем самым отказаться от необходимости их хранения в энергонезависимой памяти.

Криптосистема «Утро» ориентирована на возможность реализации в виде программного средства в составе операционных систем с использованием штатных криптопровайдеров (например: Microsoft CNG, Linux CryptoAPI), а также в виде отдельного программно-аппаратного решения или аппаратно-программного комплекса. В частности, такой аппаратный комплекс для защиты данных передаваемых по протоколу iSCSI может быть построен на технической базе серийных средств криптографической защиты информации, передаваемой в канал связи, типа IP-шифратор.

Отметим инвариантность применения КС «Утро», что позволяет, сохраняя её общую криптографическую схему, использовать в ней иные алгоритмы блочного шифрования и выработки хэш-функций, а также возможность использования такой схемы шифрования для формирования файлов-контейнеров на локально подключённых накопителях информации или при посекторном шифровании таких накопителей.

Несмотря на задержку вносимую КС «Утро» зашифрованием данных при их передаче и, соответственно, расшифрованием при их приёме из облачного сервиса STaaS/DSaaS, сетевого NAS или сети хранения данных SAN, предложенная криптосхема не предполагает применения полностью гомоморфного шифрования данных в используемом облачном сервисе и не зависит от проблем обеспечения криптографической стойкости подобных решений, реализованных в самом облачном провайдере (поставщике облачных услуг).

Литература

1. Гюнтер Е.С., Нарутта Н.Н., Шахов В.Г. «Облачные» вычисления и проблемы их безопасности. // Омский научный вестник № 2 (120), 2013 г., С. 278-282
2. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам. // Вестник Нижегородского университета им. Н.И. Лобачевского, 2013, № 2 (1), С. 45–51
3. Бессольцев В.Е., Марков П.Н. Уязвимости веб сервисов, используемых в автоматизированных системах управления // I-methods. 2018. Т. 10. № 3. С. 23–35.
4. Оношко Д.Е., Бахтизин В.В. Модель оценки качества web-приложений, основанная на обнаружении уязвимостей к SQL-инъекциям // Доклады БГУИР. 2016. №3 (97). С. 5-11
5. Воробьев В.И., Рыжков С.Р., Фаткиева Р.Р. Защита периметра облачных вычислений. // Программные системы: теория и приложения. 2015. С. 61 – 71.
6. Беккер М.Я., Терентьев А.О., Гатчин Ю.А., Кармановский Н.С. Использование цифровых сертификатов и протоколов SSL/TLS для шифрования данных при облачных вычислениях // Научно-технический вестник информационных технологий, механики и оптики. 2011. №4 (74). С. 125-130
7. Гладкий М.В. Безопасность приложений на платформах облачных вычислений. // Труды БГТУ, 2015. № 6. Физико-математические науки и информатика, С. 204–207.
8. Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Методы полностью гомоморфного шифрования на основе матричных полиномов // Вопросы кибербезопасности. 2015. №1 (9). С. 14-25
9. 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.
10. Martin Albrecht, Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Shai Halevi, Jeffrey Hoffstein, Kim Laine, Kristin Lauter, Satya Lokam, Daniele Micciancio, Dustin Moody, Travis Morrison, Amit Sahai and Vinod Vaikuntanathan. Homomorphic Encryption Standard. // Cryptology ePrint Archive, Report 2019/939, 2019

11. Егорова В.В., Чечулина Д.К. Построение криптосистемы с открытым ключом на основе полностью гомоморфного шифрования // ПДМ. Приложение, 2015, выпуск 8, С. 59–61.
12. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия ЮФУ. Технические науки. 2014. №8 (157). – С. 107-122
13. Душкин А.В., Щербакова Ю.В., Буряк Т.С. Анализ подходов применения схемы шифрования данных cp-abe для облачных технологий // Наукоемкие технологии в космических исследованиях Земли. 2014. №4. С. 64-67.
14. David Chaum. Blind signatures for untraceable payments. // Advances in Cryptology Proceedings of Crypto. №82, 1983: pp. 199–203.
15. Аулов І.Ф. Дослідження механізмів управління особистими ключами користувачів в хмарі // ScienceRise, т. 6, № 2 (23), 2016: С. 51-57.
16. Паращук И. Б., Саенко И. Б., Пантюхин О. И. Доверенные системы для разграничения доступа к информации в облачных инфраструктурах // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. No 6. С. 68–75.
17. Аракелов Г.Г., Грибов А.В., Михалёв А.В. Прикладная гомоморфная криптография: примеры. // Фундамент. и прикл. математика., 21:3 (2016), С. 25–38.
18. Трубей А.И. «Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор)». // Информатика. 2015; (1). С. 90-101.
19. Gentry, C. A Fully homomorphic encryption using ideal lattices / C. Gentry //Symposium on the Theory of Computing (STOC). – Bethesda, USA, 2009. – pp.169-178.
20. Варновский Н.П., Захаров В.А., Шокуров А.В., К вопросу о существовании доказуемо стойких систем облачных вычислений. // Вестник Московского университета, Серия 15, Вычислительная математика и кибернетика, 2016. № 2, – С. 32-46.
21. Малинский А.Е., Оценка криптостойкости полностью гомоморфных систем. Инженерный журнал: наука и инновации, 2013, вып. 11. URL: http://engjournal.ru/catalig/it/security/995.html
22. Трепачева А.В. Криптоанализ шифров, основанных на гомоморфизмах полиномиальных колец // Известия ЮФУ. Технические науки. 2014. №8 (157). – С.96-107
23. Трепачева А.В. Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему // ПДМ. Приложение. 2015. №8. – С. 75-78
24. Трепачева А.В. Улучшенная атака по известным открытым текстам на гомоморфную криптосистему Доминго-Феррера. // Труды ИСП РАН, том 26, вып. 5, 2014 г.- С. 83-98.
25. Liliya Akhmetzyanova, Evgeny Alekseev, Grigory Karpunin and Vladislav Nozdrunov. Security of Multilinear Galois Mode (MGM) // Cryptology ePrint Archive, Report 2019/123, 2019.
26. Зубов А.Ю. Об оценке стойкости AEAD-криптосистемы типа GCM, ПДМ, 2016, номер 2(32). – С. 49–62.
27. Ferguson N. Authentication weaknesses in GCM. Public Comments to NIST. http://csrc.nist.gov/CryptoToolKit/modes/comments, May 2005.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

THE MAIN CRYPTOGRAPHIC MECHANISMS FOR PROTECTION OF DATA, TRANSMITTED TO CLOUD SERVICES AND STORAGE AREA NETWORKS

Minakov S.S.[7]

Abstract.

The purpose: *development of the technology of cryptographic protection of information in third-party cloud services or storage area networks by using standartizated interfaces, protocols and block ciphers algorithms.*

Method: *system analysis of degradation security information level by data recycling with cloud computing. Research and analysis a science papers of cryptology theory and practice, describe limitations of homomorphic encryption. Cryptosystem synthesis is with analogy methods, hash and block ciphers algorithms.*

The result: *new cryptographic system «Utro» (Eng. – Morrow) for real-time protection of confidential data, transmitted to third-party cloud services or storage area networks. The paper is described main cryptographic mechanisms like*

7 Sergey S. Minakov, Senior researcher, Academy of cryptography Russian Federation, Moscow, Russia. E-mail: ss_minakov@mail.ru

function, logic and encryption scheme for program the cryptosystem. It also gives advices of using the proposed methods with data protocols like iSCSI, FiberChannel, WebDAV and possibility a local using.

Keywords. *encryption, cloud storage, computer security, cryptographic system, network protocols.*

References

1. Gyunter E.S., Narutta N.N., Shaxov V.G. «Oblachnye» vychisleniya i problemy ih bezopasnosti. // Omskij nauchnyj vestnik № 2 (120), 2013, pp. 278-282
2. Sabanov A.G. Osobennosti autentifikacii pri dostupe k oblachnym servisam. // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo, 2013, № 2 (1), pp. 45–51
3. Bessol`cev V.E., Markov P.N. Uyazvimosti veb servisov, ispol`zuemyh v avtomatizirovannyh sistemax upravleniya // I-methods. 2018, vol. 10, № 3. pp. 23–35.
4. Onoshko D.E., Baxtizin V.V. Model` ocenki kachestva web-prilozhenij, osnovannaya na obnaruzhenii uyazvimostej k SQL-in``ekciyam // Doklady BGUIR. 2016, №3 (97).
5. Vorob`ev V.I., Ryzhkov S.R., Fatkieva R.R. Zashhita perimetra oblachnyh vychislenij. // Programmnye sistemy: teoriya i prilozheniya, 2015, pp. 61 – 71.
6. Bekker M.Ya., Terent`ev A.O., Gatchin Yu.A., Karmanovskij N.S. Ispol`zovanie cifrovyh sertifikatov i protokolov SSL/TLS dlya shifrovaniya dannyh pri oblachnyh vychisleniyax // Nauchno-texnicheskij vestnik informacionnyh texnologij, mexaniki i optiki, 2011, №4 (74). 125-130
7. Gladkij M.V. Bezopasnost` prilozhenij na platformax oblachnyh vychislenij. // Trudy BGTU, 2015, № 6, Fiziko-matematicheskie nauki i informatika, pp. 204–207.
8. Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V. Metody polnost`yu gomomorfnogo shifrovaniya na osnove matrichnyh polinomov // Voprosy kiberbezopasnosti, 2015. №1 (9), pp. 14-25
9. Astaxova L.V. Zashhita oblachnoj bazy personal`nyh dannyh s ispol`zovaniem gomomorfnogo shifrovaniya / L.V. Astaxova, D.R. Sultanov, N.A. Ashixmin // Vestnik YuUrGU. Seriya «Komp`yuternye texnologii, upravlenie, radioe`lektronika», 2016, vol.16, №3, pp. 52–61.
10. Martin Albrecht, Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Shai Halevi, Jeffrey Hoffstein, Kim Laine, Kristin Lauter, Satya Lokam, Daniele Micciancio, Dustin Moody, Travis Morrison, Amit Sahai and Vinod Vaikuntanathan. Homomorphic Encryption Standard. // Cryptology ePrint Archive, Report 2019/939, 2019.
11. Egorova V.V., Chechulina D.K. Postroenie kriptosistemy s otkrytym klyuchom na osnove polnost`yu gomomorfnogo shifrovaniya // PDM. Prilozhenie, 2015, № 8, pp. 59–61.
12. Burtyka F.B. Simmetrichnoe polnost`yu gomomorfnoe shifrovanie s ispol`zovaniem neprivodimyh matrichnyh polinomov // Izvestiya YuFU. Texnicheskie nauki, 2014, №8 (157), pp. 107-122
13. Dushkin A.V., Shherbakova Yu.V., Buryak T.S. Analiz podxodov primeneniya sxemy shifrovaniya dannyh cp-abe dlya oblachnyh texnologij // Naukoemkie texnologii v kosmicheskix issledovaniyax Zemli, 2014, №4, pp. 64-67.
14. David Chaum. Blind signatures for untraceable payments. // Advances in Cryptology Proceedings of Crypto, №82, 1983: pp. 199–203.
15. Aulov I.F. Doslidzhennya mexanizmiv upravlinnya osobistimi klyuchami koristuvachiv v xmari // ScienceRise, vol. 6, № 2 (23), 2016: pp. 51-57.
16. Parashhuk I. B., Saenko I. B., Pantyuxin O. I. Doverennye sistemy dlya razgranicheniya dostupa k informacii v oblachnyh infrastrukturax // Naukoemkie texnologii v kosmicheskix issledovaniyax Zemli, 2018, vol. 10, № 6, pp. 68–75.
17. Arakelov G.G., Gribov A.V., Mixalyov A.V. Prikladnaya gomomorfnaya kriptografiya: primery. // Fundament. i prikl. matematika., 21:3 (2016), pp. 25–38.
18. Trubej A.I. «Gomomorfnoe shifrovanie: bezopasnost` oblachnyh vychislenij i drugie prilozheniya (obzor)». // Informatika, 2015, (1), pp. 90-101.
19. Gentry, C. A Fully homomorphic encryption using ideal lattices / C. Gentry //Symposium on the Theory of Computing (STOC). – Bethesda, USA, 2009, pp.169-178.
20. Varnovskij N.P., Zaxarov V.A., Shokurov A.V., K voprosu o sushhestvovanii dokazuemo stojkix sistem oblachnyh vychislenij. // Vestnik Moskovskogo universiteta, Seriya 15, Vychislitel`naya matematika i kibernetika, 2016, № 2, pp. 32-46.
21. Malinskij A.E., Ocenka kriptostojkosti polnost`yu gomomorfnyh sistem. // Inzhenernyj zhurnal: nauka i innovacii, 2013, (11), URL: http://engjournal.ru/catalig/it/security/995.html
22. Trepacheva A.V. Kriptoanaliz shifrov, osnovannyh na gomomorfizmax polinomial`nyh kolecz // Izvestiya YuFU. Texnicheskie nauki, 2014, №8 (157), pp. 96-107.
23. Trepacheva A.V. Ataka po shifrtekstam na odnu linejnuyu polnost`yu gomomorfnuyu kriptosistemu // PDM. Prilozhenie, 2015, №8, pp. 75-78.
24. Trepacheva A.V. Uluchshennaya ataka po izvestnym otkrytym tekstam na gomomorfnuyu kriptosistemu Domingo-Ferrera. // Trudy ISP RAN, 2014, vol.26, №5, pp. 83-98.
25. Liliya Akhmetzyanova, Evgeny Alekseev, Grigory Karpunin and Vladislav Nozdrunov. Security of Multilinear Galois Mode (MGM) // Cryptology ePrint Archive, Report 2019/123, 2019.
26. Zubov A.Yu. Ob ocenke stojkosti AEAD-kriptosistemy tipa GCM // PDM, 2016, № 2(32). – pp. 49–62.
27. Ferguson N. Authentication weaknesses in GCM. Public Comments to NIST. http://csrc.nist.gov/CryptoToolKit/modes/comments, May 2005.