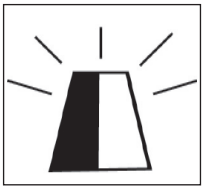

С. В. Запечников

МЕТОДЫ И МЕХАНИЗМЫ КОНТРОЛЯ ДОСТУПА К ШИФРОВАННЫМ ДАННЫМ, ХРАНИМЫМ В ОБЛАЧНЫХ СРЕДАХ[1]

Введение

Проблема контроля доступа к информационным ресурсам при хранении и обработке их в автоматизированных системах относится к числу фундаментальных проблем информационной безопасности. На нынешнем этапе развития компьютерной техники один из важных аспектов этой проблемы связан с контролем доступа к информационным ресурсам, хранимым, обрабатываемым и передаваемым в облачных средах.

Объективные причины, определяющие отличия в постановке этой проблемы для облачных сред по сравнению с ранее известными решениями для распределенных компьютерных систем другой архитектуры, таковы:

- в облачных архитектурах разделяются роли владельца данных, пользователя данными и провайдера сервиса хранения данных;
- облачные сервисы далеко не всегда могут пользоваться доверием владельцев данных, а нередко и пользователей сервисов;
- количество пользователей облачного сервиса может быть очень большим, и в этих условиях необходимо избегать неэффективного использования дискового пространства хранилища.

Эти причины приводят к необходимости хранить в зашифрованном виде любые данные, передаваемые в облачную среду, если только они не являются общедоступными и свободно распространяемыми. В связи с этим задача контроля доступа к данным, хранимым в облачных средах, ставится только применительно к шифрованным данным.

Основные требования к методам контроля доступа к данным в облачных средах состоят в следующем:

- масштабируемость в очень широких пределах, соразмерная широкой масштабируемости сервисов самой облачной среды;
- достаточный уровень производительности средств контроля доступа для использования сравнительно низкопроизводительных (в том числе мобильных, портативных) устройств;
- достаточный уровень разграничения полномочий пользователей, возможность «тонкой» настройки правил разграничения доступа;

[1] Данная работа выполнена при поддержке «ИнфоТеКС Академия» — Программы поддержки научных исследований, проводимой ОАО «ИнфоТеКС».

- учет множественности ролей пользователей, многообразия характера информации, хранимой в облачных средах, и степени ограничений доступа к ней;
- наличие механизмов отзыва полномочий пользователей в случае их выбытия из системы и (или) компрометации ключевой информации.

В связи с возникновением новых требований традиционные методы контроля доступа, основанные на дискреционной, мандатной, ролевой моделях доступа или их сочетаниях, не могут эффективно применяться в облачных средах.

1. Задачи обеспечения информационной безопасности в облачных средах

По определению NIST [1, 2], облачные вычисления (cloud computing) — это модель, предоставляющая повсеместный, массовый доступ по запросу через сеть к совместно используемому через сеть пулу конфигурируемых компьютерных ресурсов (сетей, серверов, накопителей данных, прикладных программ, сервисов), которые могут быть быстро предоставлены (когда в них возникает необходимость) и освобождены (когда необходимости в них нет) с минимальными затратами на управление или взаимодействие с провайдером облачного сервиса.

Задачи, возникающие в связи с необходимостью обеспечения информационной безопасности в облачных средах, определяются множеством факторов. Основные из них — степень доверия потребителей к провайдеру облачного сервиса, наличие или отсутствие среди обрабатываемой информации конфиденциальной, предположения об угрозах и нарушителях [3].

В самом общем виде задачи обеспечения безопасности информации, передаваемой потребителем вовне, в облачную среду для хранения и обработки, связаны с обеспечением следующих основных аспектов информационной безопасности [4]:
- конфиденциальность, или, точнее будет сказать, тайна частной жизни (privacy) — предотвращение НСД к некоторым видам информационных ресурсов;
- целостность — обеспечение сохранности данных и кода и отсутствия в них модификаций (integrity);
- верифицируемость — проверка корректности результатов выполнения операций с данными (verifiability): сервер облачной среды должен быть способен доказать действительность и правильность результатов выполненных им операций.

Контроль доступа в облачных средах нацелен, прежде всего, на обеспечение первого из перечисленных аспектов. Разграничивать доступ к шифрованным данным проще всего было бы, реализуя соответствующие схемы управления ключами шифрования. Однако в этом случае неизбежным становится хранение в облачной среде множества экземпляров одних и тех же данных, зашифрованных на разных ключах. Учитывая то обстоятельство, что круг пользователей облачных сервисов может быть весьма обширным (тысячи и даже миллионы пользователей), такой подход приведет к крайне неэффективному использованию ресурсов памяти. В связи с этим актуальным становится поиск иных, чем традиционные, моделей контроля доступа и способов их реализации при помощи криптографических схем.

2. Математические и методические основы схем контроля доступа к шифрованным данным

Основой абсолютного большинства известных механизмов контроля доступа к шифрованным данным является новая *атрибутная модель контроля доступа* [5]. В атрибутной модели доступ предоставляется не на основе прав пользователя, ассоциированных с ним после аутентификации, а на основе сопоставления атрибутов всех компонентов тракта доступа субъекта к объекту. Политика контроля доступа специфицирует, какие заявления относительно наличия атрибутов должны быть удовлетворены для того, чтобы к тому или иному объекту контроля доступа был предоставлен доступ. Атрибутом теоретически может быть информация любого типа. Могут задаваться атрибуты пользователей, атрибуты ресурсов, атрибуты внешней среды и т. д. Важно, чтобы

атрибут был неотчуждаем от того субъекта или объекта, которому он присвоен или принадлежит. В отношении субъектов доступа неотчуждаемость атрибутов достигается либо физически, либо путем применения технических, организационных, юридических и иных мер защиты. В отношении информационных ресурсов она достигается преимущественно криптографическими методами. Атрибуты могут сравниваться как со статическими величинами, так и друг с другом, превращаясь в контроль доступа на основе отношений (relation-based access control).

Для получения доступа пользователь должен представить механизму контроля доступа доказательства соответствия атрибутов правилам политики контроля доступа. В простейшем случае механизм контроля доступа может «поверить на слово» пользователю (скажем, в случае, когда проверяемым атрибутом является «возраст старше 18 лет»), в другом случае атрибутами могут служить шаблоны биометрических данных пользователя: для их проверки используется биометрический считыватель. Способ и полнота проверки этих атрибутов, однако, лежат вне «плоскости» собственно механизма принятия решения о доступе. Любому пользователю, который сможет доказать соответствие этому заявлению, предоставляется доступ. Пользователи могут быть анонимными, если строгие идентификация и аутентификация не требуются, но, тем не менее, анонимным пользователям также должны быть предоставлены средства доказательства их соответствия заявляемым атрибутам. Стандартом описания атрибутных политик контроля доступа является язык XACML [6]. Текущая версия стандарта XACML 3.0 вышла в январе 2013 г.

В результате анализа алгоритмических схем, используемых для решения задачи контроля доступа, выделен общий математический и методический аппарат, на котором по преимуществу базируются эти схемы. Наиболее существенными элементами этого аппарата являются:

- теория специального вида отображений между алгебраическими группами — спариваний (pairings), обладающих свойствами линейности по каждой из переменных и потому называемых билинейными спариваниями (bilinear pairings);
- теория линейных схем разделения секрета (linear secret sharing schemes), являющихся обобщением широко известных пороговых схем разделения секрета;
- теория функционального шифрования: частными видами функциональных шифров являются широко используемые в схемах контроля доступа идентификационные (identity-based) и атрибутные (attribute-based) схемы шифрования.

3. Классификация криптографических схем контроля доступа к шифрованным данным, хранимым в облачных средах

Криптографические схемы, реализующие функции контроля доступа к шифрованным данным, условно можно подразделить на несколько классов по признаку большей или меньшей приближенности основного механизма контроля доступа к субъекту либо к объекту доступа:

- *Схемы «спутанного» шифрования данных* [7] — механизм, наиболее близкий к субъекту доступа, представляющий собой не что иное, как специальный код, преобразующий контролируемый массив файлов таким образом, что становится возможен как контроль целостности всего массива, так и разграничение доступа к каждому файлу в отдельности.
- *Схемы контроля доступа на основе идентификационных и бессертификатных криптосистем* [8] и соответствующих схем управления ключами — механизм, наиболее близкий к субъекту доступа. При этом к контролируемым данным, как правило, применяется одна из схем шифрования: симметричная, реже — схема открытого шифрования. Однако схемы шифрования могут отличаться от традиционных: с целью оптимизации управления ключами помимо традиционных криптосистем с инфраструктурой открытых ключей используются идентификационные и их развитие — бессертификатные криптосистемы. Механизмы контроля доступа основаны соответственно на

идентификационных либо бессертификатных схемах шифрования. Эффект разграничения доступа достигается почти исключительно путем соответствующего манипулирования ключами.

- *Схемы контроля доступа на основе перешифрования данных по доверенности* ([9–12] и др.) — механизм, приближенный по своей идеологии к схемам управления ключами, однако в целях снижения сложности управления ключами вводится «промежуточное звено» в виде центра доверия, который в соответствии с запросами пользователей и по разрешениям владельцев данных подготавливает массивы данных для обеспечения возможности доступа к ним уполномоченных пользователей путем перешифрования на ключах, распределяемых этим пользователям.

- *Атрибутные схемы шифрования* ([13–15] и др.) — это механизм контроля доступа, который носит «посреднический» характер и «привязывает» правила политики доступа либо к объектам контроля доступа, то есть к единицам хранения шифрованных данных: файлам, базам данных, директориям, либо к криптографическим ключам, с помощью которых этот доступ осуществляется.

На атрибутных схемах шифрования основан еще один класс схем контроля доступа — схемы, способные функционировать при наличии в облачной среде *множества* центров доверия, присваивающих атрибуты пользователям, — *атрибутирующих центров* [16–20]. Отличительной особенностью такого рода схем является возможность назначения нескольких независимых атрибутирующих центров и, таким образом, интеграции нескольких самостоятельных подсистем контроля доступа с автономными центрами доверия в единую среду с согласованной политикой контроля доступа. В настоящее время их следует рассматривать как самые совершенные и максимально удобные для практической реализации.

4. Сравнительная оценка методов и механизмов контроля доступа

Представляет интерес сравнение проанализированных методов и механизмов по их качествам и свойствам, существенным с точки зрения потребителя (владельца данных, пользователя, провайдера облачного сервиса) и разработчика средств и систем защиты информации.

По гибкости задания прав доступа наибольшие возможности предоставляют способы контроля доступа, основанные на атрибутных схемах шифрования с привязкой политики доступа к шифртексту или к ключу. И в том, и в другом случае правила доступа могут быть сформулированы в виде сколь угодно сложного предиката, состоящего из элементарных высказываний, принимающих при проверке значение «истина» или «ложь» и соединенных логическими операциями AND и OR. В ряде схем возможно формулировать выражения по «пороговому» принципу: выражение становится истинным, если не менее заданного количества входящих в него логических переменных принимают значение «истина». Привязка политики доступа к шифртекстам или к ключам не имеет существенного значения с точки зрения выразительных возможностей для формулирования правил доступа — решение о реализации той или иной схемы должно приниматься, в основном, из соображений удобства.

По количеству объектов контроля доступа ни одна из схем не имеет каких-либо принципиальных ограничений. Пределом по этому показателю может являться лишь сложность практической реализации системы, быстродействие механизмов контроля доступа и объем накопителей для хранения данных.

Наибольшими *функциональными возможностями* обладает способ на основе «спутанного» хранения файлов, так как соединяет в себе механизм контроля доступа с механизмом контроля сохранности файлов. Поскольку реальным объектом контроля доступа являются ключи шифрования контента, можно предположить, что схема «спутанного» хранения файлов в принципе может быть интегрирована с атрибутными схемами шифрования, но для этого требуется дополнительная доработка обоих решений.

Для точного сравнения *быстродействия* различных криптосхем с сопоставимой функциональностью требуется проведение дополнительного исследования, сопровождаемого их

макетной реализацией, поскольку этот показатель зависит от большого числа факторов, не всегда очевидных или поддающихся непосредственной оценке при документальном изучении криптосхем. В ряде случаев авторы схем контроля доступа проводят сравнительный анализ предлагаемых ими решений с ранее известными. Однако чаще ведущим мотивом при конструировании криптосхем является создание схем с новой, дополнительной или расширенной функциональностью или схем, обладающих стойкостью к более широкому классу атак. При этом производительность схемы может не только не повыситься, но даже ухудшиться. Таким образом, можно сделать предварительный вывод о том, что в рассматриваемой области еще не накоплена «критическая масса» стабильных и апробированных криптографических конструкций (как, например, в сфере блочных шифров), что позволяло бы сравнивать однородные конструкции по четкому набору критериев и делать однозначные выводы о том, какая из них предпочтительнее.

Сравнение схем контроля доступа по *криптографической стойкости* показывает, что все предлагаемые в настоящее время схемы разрабатываются в модели «доказательной безопасности» (provable security), в соответствии с которой делается предположение о вычислительной сложности одной из типовых задач, применяемых в криптографии. Поскольку в основу рассматриваемых конструкций преимущественно положен математической аппарат билинейных спариваний, то в качестве вычислительно сложной задачи чаще всего выступает тот или иной вариант билинейной проблемы Диффи — Хеллмана. Конструирование схемы при доказательном подходе предполагает получение строгого формального доказательства того, что нарушение криптостойкости схемы каким бы то ни было способом (в пределах введенной модели противника) сводится к решению соответствующей вычислительно сложной задачи. В этих условиях трудоемкость нарушения безопасности схемы определяется трудоемкостью решения задачи противником. Эта трудоемкость задается, как правило, порядком (числом элементов) тех алгебраических структур, в терминах которых формулируется задача, то есть в конечном итоге заданием некоторого (условного) параметра безопасности. Таким образом, криптостойкость каждой схемы может регулироваться индивидуально и изменяться в широких пределах.

По критерию *удобства и эффективности реализации основных математических операций* практически все рассматриваемые криптосхемы находятся в равных условиях, так как в явном виде либо опосредованно используют математический аппарат билинейных спариваний Тэйта и Вейля, вычисление которых осуществляется по алгоритму Миллера. Несмотря на сложность реализуемого математического аппарата, в настоящее время имеется множество конкурирующих между собой реализаций и готовых библиотек разработчика. К числу наиболее известных следует отнести PBC — Pairing-Based Cryptography library [21] и комплекс инструментальных средств для создания прототипов криптографических механизмов Charm [22].

Выразительные возможности и гранулярность задания правил политики доступа для различных схем варьируются в широком диапазоне: от самой простой (и даже примитивной) модели «один пользователь — один файл» в схеме «спутанного» хранения файлов до сколь угодно сложных логических выражений с произвольным количеством атрибутов контроля доступа в способах, основанных на атрибутных схемах шифрования. Но наибольшие выразительные возможности присущи схемам контроля доступа с множеством центров доверия (атрибутирующих центров).

Таким образом, окончательный выбор алгоритмического обеспечения для реализации механизмов контроля доступа к шифрованным данным, хранимым в облачных средах, должен осуществляться с учетом всего комплекса перечисленных факторов.

5. Практические рекомендации по реализации и применению механизмов контроля доступа

1. Размещение на хранение в облачной среде информации ограниченного распространения, требующей контроля доступа к массивам данных, должно осуществляться с учетом оценки

рисков несанкционированного доступа к данным, утраты их целостности и доступности. В связи с выходом данных за границы контролируемой владельцем данных среды эти риски могут быть повышенными по сравнению с традиционными способами хранения данных. Источниками угроз при этом могут выступать не только провайдеры и пользователи облачного сервиса, но и третьи лица. В то же время в ряде случаев обращение к такому способу хранения может быть неизбежным: например, в случае, когда владелец данных не обладает достаточными собственными ресурсами долговременного хранения данных.

2. Во всех случаях хранения в облачной среде информации, требующей контроля доступа, основной рекомендацией является постоянное хранение данных в зашифрованном виде. Данные рекомендуется загружать в облачное хранилище и выгружать из облачного хранилища только в зашифрованном виде, а все операции по обработке данных выполнять после их расшифрования на стороне пользователя. Рациональным способом хранения шифрованных данных является применение гибридной схемы: для защиты пользовательских данных рационально применять симметричные схемы шифрования с любым алгоритмом, удовлетворяющим требованиям достаточной криптостойкости (например, ГОСТ 28147-89, AES) и режимом шифрования, удовлетворяющим условиям применения (например, режимы CBC, CTR или ориентированный на дисковое хранение режим XTS), для защиты ключей симметричных криптосхем — схемы открытого шифрования, удовлетворяющие требованиям достаточной криптостойкости (например, схемы RSA или Эль-Гамаля). При этом реальными объектами контроля доступа становятся не столько сами массивы данных, доступ к которым теперь опосредован через ключи шифрования контента, сколько ключи симметричных схем шифрования.

3. Для реализации механизмов контроля доступа к ключам шифрования контента рационально использовать одну из готовых криптосхем, описанных в научной литературе. Такие криптосхемы, как было показано в работе, могут быть подразделены на несколько типов и упорядочены по критерию большей или меньшей приближенности к объектам либо субъектам контроля доступа. При этом подавляющее большинство схем контроля доступа к шифрованным данным, хранимым в облачных средах, предполагает реализацию атрибутной модели контроля доступа.

4. Способы контроля доступа, в которых *механизм контроля доступа приближен к субъектам контроля доступа*, в значительной степени основаны на традиционных, хорошо апробированных криптографических алгоритмах, протоколах и моделях построения инфраструктуры управления ключами. Их применение может быть рекомендовано при наличии у владельцев данных (пользователей) достаточно развитой и хорошо апробированной инфраструктуры управления ключами, а также при низкой степени доверия владельцев данных (пользователей) к нетрадиционным технологиям, отсутствии достаточно квалифицированного персонала разработчиков и эксплуатационников, что не позволяет внедрить и поддерживать решение, основанное на существенно новой алгоритмической базе.

5. Применение способов, в которых *механизм контроля доступа приближен к объектам* контроля доступа, в частности способа «спутанного» хранения файлов, целесообразно в том случае, когда провайдер облачного сервиса несет материальную ответственность за сохранность и достоверность передаваемых ему на хранение данных. Сам механизм хранения данных, представляющий собой в этом случае не что иное, как специфический способ кодирования массивов данных, делает крайне невыгодным для провайдера облачного сервиса удаление или модификацию хотя бы одного (любого) фрагмента хранимых данных.

6. Способы, в которых *механизм контроля доступа занимает промежуточное положение между объектами и субъектами контроля доступа*, то есть по сути создается посреднический механизм регулирования доступа, представляют собой наиболее разработанный тип механизмов контроля доступа к шифрованным данным, хранимым в облачных средах.

Большинство из них основано на атрибутных схемах шифрования, второй по распространенности способ — это перешифрование данных по доверенности. Их применение может быть рекомендовано в большинстве практических ситуаций, а выбор той или иной конкретной криптосхемы будет диктоваться, скорее всего, критериями удобства реализации и применения, а также быстродействия. Сколько-нибудь существенные различия в их криптостойкости вряд ли можно выявить.

7. Наибольшую практическую ценность имеют *криптосхемы с функциями контроля доступа в облачной среде с несколькими атрибутирующими центрами*. Однако эти схемы отличаются от всех схем иных типов, в том числе и от схем с одним центром доверия на базе атрибутных схем шифрования, и, таким образом, несовместимы с ними. В связи с этим основная рекомендация по реализации схем такого рода состоит в следующем. Если систему облачного хранения данных с функциями контроля доступа, первоначально реализуемую с одним центром доверия — однодоменную, в будущем предполагается расширить до многодоменной, то все алгоритмы, составляющие схему контроля доступа, с самого начала следует реализовывать такими, какими они должны быть в одной из выбранных многодоменных схем. При этом если текущие потребности создания системы требуют наличия только одного центра доверия (атрибутирующего центра), то в многодоменной схеме временно реализуется только один центр доверия, а остальные добавляются позднее по мере необходимости, то есть изначально реализованная система, скорее всего, будет обладать избыточным набором функций и сниженной производительностью. Однако такая «жертва» позволит в будущем безболезненно развивать и масштабировать систему контроля доступа.

8. Реализация большинства схем контроля доступа к шифрованным данным, хранимым в облачных средах, требует, в свою очередь, эффективной реализации ряда криптографических примитивов, а именно вычисления билинейных спариваний Тэйта и Вейля по алгоритму Миллера, а также алгоритмов разделения и восстановления секрета, составляющих линейную схему разделения секрета. Эти операции являются типовыми, повторяясь в алгоритмах и протоколах практически всех схем контроля доступа. Их высокопроизводительная реализация критически важна для обеспечения достаточного быстродействия схем контроля доступа.

6. Справочно-информационная система

Основным практическим результатом исследования является созданная электронная справочно-информационная система в форме комплекса взаимосвязанных гипертекстовых файлов формата HTML. Основное содержание системы посвящено расширенному описанию и характеристике методов и механизмов контроля доступа, включая математическое описание составляющих их алгоритмов и криптографических протоколов.

Для функционирования системы необходима программная платформа на базе свободно распространяемого ПО в составе: веб-сервера Apache, интерпретатора языка PHP, СУБД MySQL, системы управления контентом («движка») MediaWiki в версии BitNami, утилиты для администрирования базы данных phpMyAdmin. Интерфейс системы подобен хорошо известному большинству пользователей интерфейсу «Википедии» (рис. 1).

В справочно-информационной системе присутствует глоссарий терминов и определений (с указанием синонимов и эквивалентных англоязычных понятий). Справочно-информационная система включает в себя как составную часть систематизированную библиографическую базу публикаций по рассматриваемой предметной области. Каждая запись о публикации содержит краткие данные, позволяющие читателю оценить необходимость обращения к первоисточнику сверх имеющейся справочно-информационной системы. Каждая запись в базе данных содержит список ключевых слов из глоссария, характеризующий более конкретно тематику публикации. Обеспечивается возможность поиска в базе данных: по именам авторов, фрагменту названия и

ключевым словам публикации. Библиографическая база данных выполнена штатными средствами системы управления контентом MediaWiki и оформлена в табличном виде.

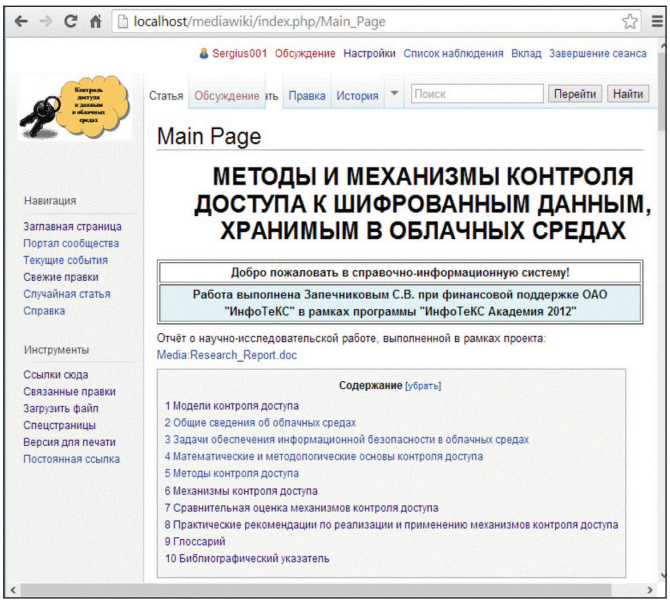

Рис. 1. Главная страница справочно-информационной системы

Заключение

Основные результаты исследования состоят в следующем.

1. Проведенный анализ научной и технической литературы позволил выделить:

а) наиболее значимые теоретические и методологические подходы к решению проблемы контроля доступа к шифрованным данным, хранимым в недоверенных средах (на примере хранения данных в облачной среде);

б) основные составляющие математического аппарата, используемого для решения задач контроля доступа в рамках нескольких выявленных методологических подходов;

в) наиболее интересное в методическом и практическом отношении алгоритмическое обеспечение схем контроля доступа к шифрованным данным.

Методы и механизмы контроля доступа к шифрованным данным систематизированы и описаны в форме, которая представляется удобной для дальнейшего использования в учебных и справочных целях.

2. Анализ и систематизация моделей, методов и механизмов контроля доступа к шифрованным данным позволили классифицировать алгоритмические схемы контроля доступа, провести их сравнительную оценку по потребительским характеристикам и характеристикам, существенным с точки зрения разработчика, и выработать практические рекомендации по реализации и применению механизмов контроля доступа.

3. Полученные в результате исследования материалы позволили создать справочно-информационную систему «Методы и механизмы контроля доступа к шифрованным данным, хранимым в облачных средах» в виде комплекса взаимосвязанных гипертекстовых файлов формата HTML, которая может служить учебно-методическим и справочным руководством для разработчиков средств и систем защиты информации с функциями контроля доступа к шифрованным данным в облачных средах. Справочно-информационная система обладает возможностями дальнейшего содержательного наполнения и тематического расширения.

Дальнейшее развитие проекта возможно как в направлении проведения поисково-аналитических работ по другим (смежным) актуальным направлениям прикладной криптографии,

так и в направлении проектно-конструкторских работ по реализации и совершенствованию механизмов контроля доступа в средствах и системах защиты информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Badger L., Grance T., Patt-Corner R., Voas J.* Cloud computing synopsis and recommendations. Recommendations of the USA National Institute of Standards and Technology. Special Publication 800–146. May, 2012. – 81 p. URL: http://csrc.nist.gov/publications/PubsSPs.html (дата обращения: 25.06.2013).
2. *Mell P., Grance T.* The NIST definition of cloud computing. Recommendations of the USA National Institute of Standards and Technology. Special Publication 800–145. Sept., 2011. – 8 p. URL: http://csrc.nist.gov/publications/PubsSPs.html (дата обращения: 25.06.2013).
3. *Jansen W., Grance T.* Guidelines on security and privacy in public cloud computing. NIST Special Publication 800–144. Dec., 2011. – 70 p. URL: http://csrc.nist.gov/publications/PubsSPs.html (дата обращения: 25.06.2013).
4. *Dara S.* Cryptography challenges for computational privacy in public clouds. – 5 p. URL: http://eprint.iacr.org/2013/272 (дата обращения: 25.06.2013).
5. *Hu V., Ferraiolo D., Kuhn R., etc.* Guide to Attribute Based Access Control (ABAC) definition and considerations (draft). NIST Special Publication 800–162. Apr., 2013. – 54 p. URL: http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf (дата обращения: 02.07.2013).
6. *Keleta Y., Eloff J. H. P., Venter H. S.* Proposing a secure XACML architecture ensuring privacy and trust. – 10 p. URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf (дата обращения: 25.06.2013).
7. *Ateniese G., Dagdelen O., Damgard I., Venturi D.* Entangled cloud storage. – 25 p. URL: http://eprint.iacr.org/2012/511 (дата обращения: 27.06.2013).
8. *Benaloh J., Chase M., Horvitz E., Lauter K.* Patient controlled encryption: Ensuring privacy of electronic medical records. – 12 p. URL: http://research.microsoft.com/en-us/um/people/horvitz/ccsw_2009_benaloh_chase_horvitz_lauter.pdf (дата обращения: 26.06.2013).
9. *Dong Ch., Russello G., Dulay N.* Shared and searchable encrypted data for untrusted servers // Proc. of DAS'2008. Springer-Verlag, LNCS 5094, 2008. P. 127–143. URL: http://pure.strath.ac.uk/portal/files/6710100/fulltext.pdf (дата обращения: 26.06.2013).
10. *Zhang Y., Chon J.-L.* Efficient access control of sensitive data service in outsourcing scenarios. – 6 p. URL: http://eprint.iacr.org/2010/242 (дата обращения: 26.06.2013).
11. *Chen Y.-R., Chu Ch.-K., Tzeng W.-G., Zhou J.* CloudHKA: A cryptographic approach for hierarchical access control in cloud computing. – 20 p. URL: http://eprint.iacr.org/2013/208 (дата обращения: 26.06.2013).
12. *Liang K., Pang L., Wong D., Susilo W.* A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. – 21 p. URL: http://eprint.iacr.org/2013/236 (дата обращения: 26.06.2013).
13. *Goyal V., Pahdey O., Sahai A., Waters B.* Attribute-based encryption for fine-grained access control of encrypted data. – 28 p. URL: http://eprint.iacr.org/2006/309 (дата обращения: 27.06.2013).
14. *Bethencourt J., Sahai A., Waters B.* Ciphertext-policy attribute-based encryption. 2007. – 15 p. URL: http://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe.pdf (дата обращения: 27.06.2013).
15. *Hur J., Noh D.* Attribute-based access control with efficient revocation in data outsourcing systems // IEEE Trans. on parallel and distributed systems. July, 2011. Vol. 22. № 7. P. 1214–1220. URL: http://www.computer.org/csdl/trans/td/2011/07/ttd2011071214.pdf (дата обращения: 27.06.2013).
16. *Lin H., Cao Zh., Liang X., Shao J.* Secure threshold multi-authority attribute-based encryption without a central authority. – 17 p. URL: http://tdt.sjtu.edu.cn/~xhliang/papers/Indocrypt'08.pdf (дата обращения: 28.06.2013).
17. *Lewko A., Waters B.* Decentralizing attribute-based encryption. – 31 p. URL: http://eprint.iacr.org/2010/351 (дата обращения: 28.06.2013).
18. *Ruj S., Nayak A., Stojmenovic I.* DACC: Distributed access control in clouds. – 8 p. URL: http://www.site.uottawa.ca/~ivan/DACC.pdf (дата обращения: 28.06.2013).
19. *Yang K., Jia X., Ren K.* DAC-MACS: Effective data access control for multi-authority cloud storage systems. – 12 p. URL: http://eprint.iacr.org/2012/419 (дата обращения: 28.06.2013).
20. *Boyen X.* Attribute-based functional encryption on lattices (ext. abstract). – 24 p. URL: http://eprint.iacr.org/2012/716 (дата обращения: 27.06.2013).
21. *Lynn B.* On the implementation of pairing-based cryptosystems. Ph.D. theses. USA, Stanford University, 2007. – 111 p. URL: http://crypto.stanford.edu/pbc/thesis.html (дата обращения: 26.06.2013).
22. *Akinyele J. A., Green M., Rubin A.* Charm: a framework for rapidly prototyping cryptosystems. – 19 p. URL: http://eprint.iacr.org/2011/617 (дата обращения: 26.06.2013).