Обсуждаются «облачные» технологии и их применение для решения задач информационной безопасности. Показано, что их использование приводит к новым постановкам задач и способствует повышению стеганостойкости алгоритмов, улучшению нижних оценок стойкости стеганосистем.

УДК 681.3:519.72:003.2655

В.К. ЗАДИРАКА, А.М. КУДИН, И.В. ШВИДЧЕНКО

СТЕГАНОГРАФИЯ В ОБЛАЧНЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Введение. По данным отчета Cisco Global Cloud Index (2011–2016) [1] в 2013 году трафик, обрабатываемый центрами обработки данных (ЦОД), построенными по облачным технологиям впервые превысил трафик, обрабатываемый ЦОД, построенными по традиционным технологиям, а по прогнозу на 2017 год доля «облачных» систем в общем трафике превысит 2/3. Облачные технологии – одна из реализаций теоретической концепции распределенных информационно-вычислительных технологий и фактически является развитием нескольких технологий: виртуализации, Грид-вычислений, тарифицируемых вычислительных ресурсов (utility computing), сервис-ориентированных архитектур (SOA), различных технологий, составляющих понятие web 2.0.

Далее будут обсуждаться «облачные» технологии и их применение для решения задач информационной безопасности. В частности, будет показано, что использование данных технологий приводит к новым постановкам задач, может способствовать повышению стеганостойкости соответствующих алгорит-мов и т. д.

1. Системы облачных вычислений и их безопасность. Говоря неформально, «облачные» вычисления – это технология распределенной обработки данных, при использовании которой совместно используемые компьютерные ресурсы[1], программное обеспечение

[1] Идея предоставления вычислительных ресурсов как платных услуг была высказана еще в 1960-х годах.

и данные предоставляются пользователям по запросу как удаленные услуги (например, через Интернет). Вычисления в облаке – это базирующийся на совокупности разных технологий способ удаленного предоставления клиенту ресурсов как услуг, при котором средства поддержки этих услуг скрыты от него, а сами ресурсы оплачиваются клиентом по мере их использования. Переход к данной модели вычислений выглядит как перенос компьютеров и систем хранения из предприятия в отдельную общую группу или облако. Конечный пользователь выставляет определенные требования к ресурсам, а облако собирает из своих внутренних компонентов нужные мощности и предоставляет их пользователю.

По сравнению с традиционными ИТ-инфраструктурами облачные вычисления позволяют управлять более крупными инфраструктурами, обслуживать различные группы пользователей. Они уменьшают сложность ИТ-инфраструктуры за счет эффективного объединения ресурсов.

Уточним терминологию «облачных» систем. В настоящее время существуют два основных определения: функциональное [2] и технологическое [3]. Функциональное определяет облачные системы с точки зрения возможностей обработки информации, предоставляемые ими, по этому определению к облачным системам относятся такие системы, в которых:

– используются эластичные (или такие, которые предоставляются в любом нужном объеме) вычислительные мощности, единое пространство динамически распределяемых вычислительных ресурсов любого типа (без ограничений на географическое расположение ресурсов), возможность удаленного доступа к ресурсам системы с требуемой скоростью без ограничения географического расположения пользователя (что определяет использование высокоскоростных мобильных сетей), ведется точный учет потребления вычислительных ресурсов[2] пользователями;

– существует несколько моделей предоставления услуг: «программное обеспечение (прикладное программное обеспечение, в том числе – системы управления базами данных и «рабочий стол») как сервис» (SaaS, DbaaS, DaaS), «платформа (операционная система и т. д.) как сервис» (PaaS), «инфраструктура (физические вычислительные ресурсы и виртуальные машины, управляющие ними) как сервис» (IaaS);

– определяется четыре модели использования ресурсов системы: частное облако (ресурсы принадлежат клиенту или используются им в «лизинге»), общественное облако (ресурсы принадлежат некоторому сообществу, характерный пример – социальные сети), публичное облако (ресурсы принадлежат провайдеру облачных услуг), гибридное облако.

[2] В дальнейшем свойство учета потребления предоставляемых потребителям вычислительных (или информационных) ресурсов назовем «тарифицируемые» вычислительные услуги.

В основе технологического определения облачных вычислений лежит совместное применение двух технологий: тарифицируемых вычислительных услуг, которые берут начало в Грид-технологии [3] и виртуализации, которая позволяет эффективно решать задачу миграции программного обеспечения между гетерогенными элементами распределенной системы. Сегодня в мире существует большое количество поставщиков услуг вычислений в облаке. Это такие компании как Google, Amazon, Salesforce.com, IBM, Microsoft, SAP и Oracle. Примерами IaaS облачных систем являются: Google compute engine, Amazon AWS, Windows Azure (Microsoft), SmartCloud Enterprise (IBM), Vmware cloud, Tucha (Украина); PaaS облачных систем являются: Amazon.com, Windows Azure (Microsoft), App Engine (Google), SmartCloud Application Service (IBM), Force.com, Heroku (Salesforce), TuchaHome (Україна); примерами SaaS (DaaS, DbaaS) облачных систем являются GoogleApps, CloudStorage (Google), SmartCloud for social business, IBM SPSS (IBM), Drawloop (Salesforce), iCloude (Apple), Tuchabox (Украина).

Преимущества облачных вычислений: снижаются требования к вычислительной мощности ПК; удаленный доступ к данным в облаке; обеспечение высокой скорости обработки данных; экономия на приобретении, поддержке, модернизации ПО и оборудования; имеются возможности простого расширения для обслуживания большого количества пользователей; пользователь оплачивает услугу только тогда, когда она ему необходима.

Недостатки облачных вычислений: пользователь не является владельцем и не имеет доступа к внутренней облачной инфраструктуре; удаленные облачные сервисы не находятся в круге влияния пользователя: пользователь получает тот уровень безопасности в облаке, который может предоставить провайдер; для получения качественных услуг пользователю необходимо иметь надежные, быстрые и мобильные коммуникации с провайдером «облака».

Основные проблемы безопасности облачной инфраструктуры следующие [4–6]:

- защита периметра и разграничение сети;
- динамичность виртуальных машин;
- уязвимости и атаки внутри виртуальной среды;
- защищенность данных и приложений;
- доступ системных администраторов к серверам и приложениям;
- защита бездействующих виртуальных машин;
- влияние традиционной безопасности на производительность;
- управление обновлениями.

2. Проектирование комплексных систем защиты информации в распределенных и облачных системах. Известно, что основной чертой теоретических и практических методик проектирования и реализации комплексных систем защиты информации (КСЗИ) для информационно-коммуникационных систем (ИКС) является использование для построения систем защиты таких же принципов, какие используются для построения самих ИКС. Сформулируем утверждения, которые иллюстрируют ограниченность использования существующих

методик построения КСЗИ по отношению к облачным системам и следуют из относительности самого определения безопасности информации в ИКС как состояния системы, при котором вся информация обрабатывается только по заранее введенным правилам. Во-первых: формулировка теоремы безопасности в виде определения состояния безопасности системы и формальных (формализованных) условий-ограничений, при которых это состояние может быть достигнуто, зависит от технологий, использующихся в ИКС. Во-вторых, существующие модели и методы формального анализа уровня безопасности информации адекватны при условии известных множеств объектов/субъектов защиты, и, следовательно – определенных моделей уязвимости, угроз и нарушителя.

С учетом этого, алгоритм проектирования КСЗИ для облачных систем предлагается строить таким образом:

– определить цели функционирования облачной системы и формальную модель ее функционирования;

– определить модель уязвимости и пути ее динамического построения;

– определить для любого события в системе степени злонамеренности относительно целей функционирования системы;

– определить факт наличия и алгоритм проведения атак с помощью адаптивных (интеллектуальных) систем анализа вторжений;

– определить политику безопасности для системы и правила ее изменения;

– определить механизмы и средства реализации политики безопасности, способной к адаптивному поведению;

– определить в рамках данного подхода методы обеспечения гарантий.

Построение общего алгоритма не решает проблемы проектирования КСЗИ для заданной облачной системы. Действительно, проблемы существования и построения эффективных алгоритмов формальных моделей облачных систем, анализа уровня их безопасности, построение адаптивных политик их безопасности и т. п. еще недостаточно исследованы. Рассмотрение данных проблем выходит за рамки статьи. Для дальнейшего изложения отметим одну из особенностей проектирования КСЗИ для облачных систем – адаптивность механизмов защиты во времени и относительно изменяющейся архитектуры системы. В соответствии этим принципам будем рассматривать и стеганографические системы защиты.

3. Стеганография в облачных системах – модели и реализация. Рассмотрим известные подходы к оценке стойкости стеганосистем с точки зрения возможности их применения в облачных системах. Стеганографическую систему будем представлять как совокупность множеств $\Gamma = (C, M, K, F, S, Q)$, где Q – множество наблюдаемых сообщений, состоящих из пустых контейнеров C и стеганограмм S, которое является некоторой избыточной характеристикой информационной системы, изменение которой не сказывается на функциональности системы (заметим, что выбор «избыточности» существенно зависит от модели нарушителя, а метод ее извлечения – от архитектуры системы); M – множество скрываемых сообщений; K – множество ключей стеганографической системы; $F : C \times M \times K \to Q$ – множество операторов модификации

или выбора избыточной информации для формирования скрытого сообщения (в частном случае это множество вероятностных алгоритмов, реализующих скрытие информации).

Комплексный анализ подходов к оценке стойкости стеганографических систем [7, 8] позволяет выделить два типа подходов относительно формулировки задачи стеганоанализа.

Первый подход [9 – 11] сводит задачу стеганоанализа к задаче разбиения множества наблюдаемых аналитиком сообщений Q на два непересекающихся подмножества S и C. При этом в зависимости от метода и критерия, применяемого для разбиения, можно строить стеганосистемы стойкие как в теоретико-информационном [9], так и в теоретико-сложностном смысле [10, 11]. Если на множествах S и C заданы соответствующие распределения вероятностей P_S и P_C [9], то в качестве критерия различия множеств применяется теорема Неймана – Пирсона и относительная энтропия

$$D(P_C \parallel P_S) = \sum_{q \in Q} P_C(q) \log \frac{P_C(q)}{P_S(q)}.$$

Совершенно стойкая стеганосистема соответствует равенству $D(P_C \parallel P_S) = 0,$ которое выполняется тогда и только тогда, когда распределения контейнеров и стего совпадают. Условием применения данного подхода, как правило, указывается необходимость знания априорного распределения контейнера, из которого следует стационарность источника контейнера. Это условие трудно обеспечить на практике для традиционных вычислительных систем. В облачных системах типа SaaS, напротив, легко указать источник таких контейнеров. Самым простым примером является сервис получения случайных чисел с равномерным распределением.

В качестве другого подхода к разделению множеств S и C применяются методы теории сложности [10, 11], а в качестве показателя стойкости – величина «выигрыша противника» [10].

Другой тип формулирования задачи стеганоанализа и введения показателей стойкости основан на невозможности определения **причины** различия множеств S и C (в частном случае – эти различия вызваны случайными факторами или применением стеганографической системы).

Исторически первый подход такого типа основан на использовании для этих целей взаимной информации $I(M;(S,C)) = H(M) - H(M \mid (S,C))$ [12]. В качестве известных недостатков такого подхода отмечается:

– для произвольной совершенно стойкой стеганосистемы доказывается лишь факт ее существования, но не учитывается возможность и сложность решения задачи ее построения;

– для произвольной совершенно стойкой стеганосистемы не рассматривается вычислительная сложность алгоритма встраивания сообщений.

Другой подход, основанный на использовании чебышевского радиуса информации, развивается авторами в работах [7, 8]. Этот подход, в отличие от других, позволяет строить стеганосистемы, стойкие в теоретико-информационном

смысле по отношению к выбранному критерию распознавания скрытого сообщения. Это свойство очень полезно для использования в облачных системах, поскольку позволяет строить стеганосистемы с **адаптивно** изменяющимся показателем стойкости.

Как показано в [8], при формировании контейнеров стеганосистем в облачных системах необходимо комплексно использовать все виды избыточности систем: функциональную (возможность решения задач более чем одним методом), информационную (наличие избыточной информации, например, в базах данных, информационных хранилищах и т. п.), представления данных (избыточность кодирования). При этом возможно использовать избыточность как в основной системе предоставления услуг, так и в инфраструктуре, созданной для обеспечения функционирования основной системы.

Приведем практический пример комплексного использования различных подходов для построения стеганосистемы в облачных системах. Выделим два уровня использования избыточности – микроуровень (в рамках одной SaaS) и макроуровень (случайный выбор из нескольких SaaS, используемых как контейнеры). В рамках одной SaaS целесообразно использовать подходы первого типа, например подход, приведенный в [9]. Это объясняется тем, что в качестве функциональности SaaS можно выбрать генерацию случайных последовательностей или сервис сохранения данных от видеорегистраторов в моменты остановки записи или поломки видеорегистратора (т. е. когда данные являются белым шумом). Для сведения «на нет» недостатков подходов первого типа на макроуровне выбирается подходы второго типа [7, 12], как раз ориентированные на выбор случайного подмножества используемых контейнеров из всего доступного множества контейнеров.

Выводы. Новые свойства облачных информационно-коммуникационных технологий, такие как эластичность и тарифицируемость вычислительных услуг, приводят к новым постановкам задач в области защиты информации, в частности – в проектировании, оценки стойкости и реализации стеганографических систем. Рассмотренные в статье постановки задач и методы решения некоторых из них показывают необходимость пересмотра многих традиционных подходов, принятых в теории защиты информации и стеганографии.

В.К. Задірака, А.М. Кудін, І.В. Швідченко

СТЕГАНОГРАФІЯ В ХМАРНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Обговорюються «хмарні» технології та їх застосування для розв'язання задач інформаційної безпеки. Показано, що їх використання призводить до нових постановок задач і сприяє підвищенню стеганостійкості алгоритмів, поліпшенню нижніх оцінок стійкості стеганосистем.

V.K. Zadiraka, A.M. Kudin, I.V. Shvidchenko

STEGANOGRAPHY IN CLOUD INFORMATION AND COMMUNICATION SYSTEMS

"Cloud" technologies and their application to solving information security problems are discussed. It is shown that their use leads to the new problem statements and promotes the increase of steganographic robustness of algorithms and the improvement of lower bounds of steganographic systems.

1. *Cisco* Global Cloud Index. – http://www.cisco.com.
2. *Peter Mell* and *Timothy Grance* The NIST definition of cloud computing // National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2011.
3. *Петренко А.І.* Хмарні і Грід-обчислення для Е-науки // Праці міжнародної конференції «Кластерні обчислення». – 2012. – С. 294–295.
4. *Степаненко В.* Облачная обработка данных – миф или реальность? // Сети и бизнес. – 2010. – № 6. – http://www.sib.com.ua/arhiv_2010/2010_6/ statia_6_6_2010/statia_6_6_2010.htm.
5. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.
6. *Кондрашин М.* Безопасность облачных вычислений // PC Magazine. – 2010. – № 1. – С. 65–67. – http://www.pcmag.ru/solutions/detail.php?ID=38248.
7. *Кудин А.М.* Математическая модель стеганографической системы на базе общей теории оптимальных алгоритмов // Математичне та комп'ютерне моделювання. – 2010. – № 4. – С. 136– 143.
8. *Задирака В.К., Кудин А.М.* Облачные вычисления в криптографии и стеганографии // Кибернетика и системный анализ. – 2013. – № 4. – С. 113 – 119.
9. *Cachin C.* An information-theoretic model for steganography // Information and Computation. – 2004. – N 192. – P. 41 – 56.
10. *Hopper N.J., Langford J., Von Ahn L.* Provably Secure // Advances in Cryptology: CRYPTO 2002, Springer LNCS 2442. – 2002. – P. 77 – 92.
11. *Rainer Böhme* An Epistemological Approach to Steganography // Proceedings of Information Hiding 2009, LNCS 5806, Springer Verlag. – 2009. – P. 15 – 30.
12. *Zollner J., Federrath H., Klimant H., Pfitzmann, A., Piotraschke, R., Westfeld, A., Wicke G., Wolf G.* Modeling the security of steganographic systems // Information Hiding, LNCS 1525, Springer Verlag. – 1998. – P. 344 – 354.

Получено 11.03.2014

Об авторах:

Задирака Валерий Константинович,
доктор физико-математических наук, профессор,
член-корреспондент НАН Украины
Института кибернетики имени В.М. Глушкова НАН Украины,
zvk140@ukr.net.

Кудин Антон Михайлович,
кандидат технических наук, старший научный сотрудник
Физико-технического института, НТУУ «КПИ»,
playshner@mail.ru

Швидченко Инна Витальевна,
кандидат физико-математических наук, научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины.
zvk140@ukr.net.