УДК 004.056.5

В.В. Богданов, Ю.С. Новоселова

Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз

Рассмотрены характерные особенности систем облачных вычислений. Обоснована актуальность задачи анализа угроз информационной безопасности для систем облачных вычислений, указаны особенности решения данной задачи по сравнению с анализом угроз информационной безопасности традиционных информационных систем. Построена математическая модель систем облачных вычислений. Проведено исследование источников угроз в системах облачных вычислений.

Ключевые слова: системы облачных вычислений, угрозы информационной безопасности, источники угроз.

Технология облачных вычислений является одним из наиболее перспективных направлений развития информационных технологий, в настоящее время рассматриваемых в качестве альтернативы традиционной модели обработки информации. Использование систем облачных вычислений позволяет реализовать возможность удаленной обработки информации, обеспечивает достижение высоких показателей отказоустойчивости и доступности информационной инфраструктуры.

Системы облачных вычислений представляют собой автоматизированные информационные системы, обеспечивающие обработку информации с использованием технологии облачных вычислений и технических средств, предоставляемых пользователям системы облачных вычислений (далее – потребитель) в качестве удаленно доступных информационных сервисов (облачных услуг). В данной статье под провайдером системы облачных вычислений (далее – провайдер) будет пониматься организация, ответственная за поддержание работоспособности и развитие системы облачных вычислений, а также за предоставление облачных услуг потребителям.

По сравнению с традиционными информационными системами, системы облачных вычислений обладают рядом характерных особенностей, которые необходимо учитывать при анализе защищенности данных систем. К ним относятся:

– самообслуживание потребителей – возможность самостоятельного получения доступа к информационным сервисам по необходимости в одностороннем автоматическом режиме без взаимодействия с персоналом провайдера;

– универсальность доступа с использованием информационно-телекоммуникационных сетей – возможность получения доступа к информационным сервисам по каналам информационно-телекоммуникационных сетей с использованием тонких или толстых клиентов;

– высокая консолидация вычислительных ресурсов – объединение вычислительных ресурсов в одной или нескольких точках для обслуживания различных потребителей с возможностью динамического назначения и переназначения физических и виртуальных ресурсов в соответствии с потребностями потребителей;

– динамическая масштабируемость – возможность оперативного автоматического изменения производительности как в сторону уменьшения, так и в сторону увеличения масштабов использования в зависимости от нужд потребителя [1].

Данные особенности определяют основные преимущества использования систем облачных вычислений для потребителей, заключающиеся в оптимизации производственных процессов за счет снижения капитальных и эксплуатационных затрат на собственную информационную инфраструктуру. Вместе с тем данные особенности приводят к возникновению новых актуальных угроз информационной безопасности, связанных, прежде всего, со снижением уровня контролируемости процессов обработки информации и с динамичностью модели предоставления ресурсов. Так, при использовании систем облачных вычислений у потребителя отсутствует возможность применения дополнительных средств ограничения доступа к информации, таких как контроль физического доступа и иных организационных и технических мер. Кроме того, ряд информационных воздействий со стороны недобросовестных потребителей может привести к резкому сокращению количества доступных вычислительных ресурсов или несоответствию между стоимостью потребления информационных сервисов и объемом фактически используемых ресурсов.

Таким образом, имеет место существенное противоречие между возможностью повышения эффективности производственных процессов при использовании систем облачных вычислений, с одной стороны, и наличием ранее не рассматриваемых угроз информационной безопасности, а также отсутствием экспликации требований информационной безопасности к системам облачных вычислений – с другой стороны.

Указанное противоречие обусловливает необходимость детального анализа угроз информационной безопасности, возникающих при использовании систем облачных вычислений. Можно отметить, что актуальность проблемы идентификации угроз информационной безопасности для систем облачных вычислений отмечается во многих исследованиях и аналитических отчетах (см., например, [2, 3]).

Для дальнейшего анализа угроз информационной безопасности определим математическую модель информационной системы пятеркой пространств (I,T,P,S,F), где I – пространство информации, обрабатываемой в информационной системе; T – пространство информационных технологий и технических средств; P – пространство потребителей и персонала провайдера; S – пространство состояний информационной системы; F – пространство переходов из одного состояния в другое, т.е. $F:S\to S$.

Состоянием информационной системы $s\in S$ будем называть набор существенных свойств (атрибутов) системы в отдельный момент времени. В целях анализа информационной безопасности для каждого состояния системы введем три атрибута безопасности информации, обрабатываемой в системе: c_S – конфиденциальность; i_S – целостность; a_S – доступность, такие что $c,i,a\in\{0,1\}$, причем $c=1$ (аналогично $i=1$ и $a=1$), если в данном состоянии обеспечивается конфиденциальность (соответственно целостность и доступность) информации, обрабатываемой в системе. Состояние $s\in S$ системы, в котором $(c_S,i_S,a_S)=(1,1,1)$, будем называть безопасным состоянием, а пространство всех безопасных состояний обозначим

$$S^+=\{s\in S\,|\,(c_S,i_S,a_S)=(1,1,1)\}. \tag{1}$$

Состояние, в котором хотя бы один из атрибутов равен нулю, будем называть небезопасным, пространство небезопасных состояний обозначим

$$S^-=\{s\in S\,|\,\exists k\in\{c_S,i_S,a_S\},k=0\}. \tag{2}$$

Ясно, что

$$S^+\cup S^-=S. \tag{3}$$

Инцидентом безопасности In в информационной системе назовем переход системы от безопасного состояния в небезопасное состояние, т.е.

$$In=f\,|\,f\in F,f:S^+\to S^-. \tag{4}$$

Модель угроз безопасности для информационных систем может быть представлена четверкой пространств (A,O,V,M), где A – пространство источников угроз; O – пространство объектов защиты; V – пространство уязвимостей; M – пространство способов реализации угроз, причем очевидно, что $M\subset F$.

Ясно, что

$$O=\{o\,|\,o\in I\cup T\cup P\}. \tag{5}$$

Уязвимостью $v\in V$ информационной системы будем называть слабость элемента системы $e\in T\cup P$, существование которой в определенном состоянии системы $s\in S$ при наличии источника угрозы $Ag\in A$ может привести к реализации инцидента безопасности, т.е.

$$V=\{v\,|\,v=e\bullet s\,|\,Ag\bullet s\Rightarrow In\}\ [4]. \tag{6}$$

Угрозой безопасности τ назовем комбинацию объекта защиты $o\in O$ и источника угроз $Ag\in A$, приводящую к переходу системы в небезопасное состояние $s^-\in S^-$, т.е.

$$\tau=e\bullet Ag\Rightarrow s^-\ [4]. \tag{7}$$

Заметим, что определенные выше модели являются общими для систем облачных вычислений и традиционных информационных систем. Однако следует отметить, что характерные особенности систем облачных вычислений обусловливают расширение пространств T и F по сравнению с традиционными информационными системами. Данные изменения, в свою очередь, приводят к расширению пространств A, O, V и M и, следовательно, расширению всей модели угроз информационной безопасности для систем облачных вычислений.

Так, с точки зрения технической реализации для систем облачных вычислений характерно использование средств виртуализации, обеспечивающих возможность самообслуживания потребителей и динамической масштабируемости вычислительных ресурсов. Использование средств виртуализации приводит к появлению дополнительных лиц и факторов, воздействующих на системы облачных вычислений и являющихся источниками угроз информационной безопасности, специфическими для технологии облачных вычислений. Так, сбои в работе средств виртуализации могут привести к нарушению изоляции и потере обрабатываемой информации, а уязвимости системы управления виртуальной средой создают возможность для несанкционированного доступа к вычислительным ресурсам или данным со стороны других потребителей системы облачных вычислений.

Универсальность доступа к информационным сервисам по каналам информационно-телекоммуникационных сетей расширяет круг возможных сценариев реализации угроз информационной безопасности со стороны пользователей информационно-телекоммуникационных сетей. В то же время данная особенность систем облачных вычислений подразумевает перенос процессов обработки информации в защищенные и отказоустойчивые центры обработки данных провайдера, что значительно снижает вероятность реализации угроз информационной безопасности посредством физического доступа к компонентам системы облачных вычислений и сокращает потери от реализации угроз, связанных со стихийными бедствиями и природными явлениями.

В связи с используемой в системах облачных вычислений моделью предоставления информационных сервисов персонал провайдера обладает потенциально неограниченным доступом к информации потребителей. В отличие от традиционных информационных систем, персонал провайдера не является представителем потребителя, а значит, находится вне зоны его контроля. С учетом высокой консолидации вычислительных ресурсов в системах облачных вычислений данное обстоятельство значительно расширяет возможности реализации угроз информационной безопасности со стороны персонала провайдера. При этом в зависимости от функциональных задач персонала угрозы могут быть реализованы путем физического доступа к компонентам системы облачных вычислений, а также с использованием системного и прикладного программного обеспечения.

Кроме того, в число возможных источников угроз информационной безопасности в системах облачных вычислений может входить оператор связи [5], предоставляющий услуги подключения между провайдером и потребителями и оказывающий непосредственное влияние на обеспечение доступности информационных сервисов и защиту передаваемых данных.

Обобщенные результаты проведенного анализа источников угроз информационной безопасности для систем облачных вычислений приведены в таблице.

Источники угроз информационной безопасности в системах облачных вычислений

Источник угроз	Описание источника угроз	Особенности источника угроз в системах облачных вычислений
Технические средства обработки информации, программное обеспечение, система электропитания и т.п.	Технические средства и технологии, сбои в работе которых могут привести к реализации угроз информационной безопасности	Влияние данных источников угроз на информационную безопасность систем облачных вычислений аналогично традиционным информационным системам
Средства виртуализации	Уязвимости и ошибки в работе средств виртуализации могут привести к несанкционированному использованию вычислительных ресурсов и доступу к информации потребителей систем облачных вычислений, а также потере данных	Появление данного источника угроз связано с использованием средств виртуализации для обеспечения возможности самообслуживания потребителей, высокой консолидации и динамической масштабируемости ресурсов
Природные явления, стихийные бедствия	Природные явления и стихийные бедствия могут привести к реализации угроз информационной безопасности, связанных с физическим повреждением или уничтожением компонентов системы облачных вычислений	В связи с осуществлением обработки информации в центрах обработки данных провайдера вероятность реализации угроз информационной безопасности, обусловленных наличием данного источника угроз, в системах облачных вычислений снижается

Источник угроз	Описание источника угроз	Особенности источника угроз в системах облачных вычислений
Пользователи информационно-телекоммуникационных сетей	Пользователь информационно-телекоммуникационных сетей может реализовать угрозы информационной безопасности с использованием информационно-телекоммуникационных сетей	В связи с предоставлением доступа к информационным сервисам системы облачных вычислений с использованием информационно-телекоммуникационных сетей возможности реализации угроз информационной безопасности со стороны пользователей информационно-телекоммуникационных сетей расширяются
Оператор связи	Оператор связи может реализовать угрозы доступности информационных сервисов системы облачных вычислений, а также осуществить перехват передаваемых данных	Универсальность доступа с использованием информационно-телекоммуникационных сетей обуславливает зависимость системы облачных вычислений от оператора связи в части обеспечения защищенности и доступности информационных сервисов
Персонал провайдера	Ошибочные действия персонала провайдера, обладающего неограниченным доступом к информации потребителей и компонентам системы облачных вычислений, могут привести к реализации угроз информационной безопасности	Воздействие данных источников угроз на информационную безопасность систем облачных вычислений аналогично традиционным информационным системам
Недобросовестный персонал провайдера	Недобросовестный персонал провайдера, обладая неограниченным доступом к информации потребителей и компонентам системы облачных вычислений, может реализовывать угрозы информационной безопасности, связанные с несанкционированным доступом к информации потребителя	В связи с консолидацией вычислительных ресурсов для обработки информации различных потребителей, а также со снижением контролируемости процессов обработки информации, возможности и масштабы реализации угроз информационной безопасности расширяются
Потребители системы облачных вычислений	Ошибочные действия потребителей системы облачных вычислений, а также несоблюдение требований по защите информации при работе с системой облачных вычислений могут привести к реализации угроз информационной безопасности	Воздействие данных источников угроз на информационную безопасность систем облачных вычислений аналогично традиционным информационным системам
Недобросовестные потребители систем облачных вычислений	Недобросовестные потребители системы облачных вычислений могут реализовывать угрозы информационной безопасности по отношению к информации и вычислительным ресурсам других потребителей системы облачных вычислений	Наличие данного источника угроз информационной безопасности обусловлено динамической масштабируемостью и консолидацией вычислительных ресурсов, а также возможностью самообслуживания потребителей

Таким образом, в данной статье, за счет рассмотрения особенностей систем облачных вычислений, обеспечивающих эффективность использования данных технологий, построения математической модели и анализа особенностей реализации систем облачных вычислений, обоснована необ-

ходимость детального рассмотрения угроз информационной безопасности систем облачных вычислений, указаны его особенности по сравнению с анализом угроз информационной безопасности традиционных информационных систем. Кроме того, проведено исследование типовых источников угроз в системах облачных вычислений, рассмотрены предпосылки необходимости рассмотрения указанных в статье источников. Дальнейшими этапами исследования являются построение модели угроз, а также синтез и экспликация системы требований по обеспечению информационной безопасности для систем облачных вычислений.

Литература

1. Liu F. NIST Cloud Computing Reference Architecture / F. Liu, J. Tong // NIST Special Publication [Электронный ресурс] – Режим доступа: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505, свободный. – Заглавие с экрана.

2. Top Threats to Cloud Computing V1.0 / Cloud Security Alliance, March 2010 [Электронный ресурс] – Режим доступа: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, свободный. – Заглавие с экрана.

3. Cloud Computing. Benefits, risks and recommendations for information security / ENISA, November 2009. [Электронный ресурс] – Режим доступа: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment, свободный. – Заглавие с экрана.

4. Peter R. Stephenson. A Formal Model for Information Risk Analysis Using Colored Petri Nets. Colored Petri Nets (CPN), 2004 [Электронный ресурс] – Режим доступа: http://daimi.au.dk/CPnets/proxy.php?url=/CPnets/workshop04/cpn/papers/index, свободный. Заглавие с экрана.

5. Badger L. DRAFT Cloud Computing Synopsis and Recommendations / L. Badger, T. Grance // NIST Special Publication [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf, свободный. Заглавие с экрана.

Богданов Валентин Викторович
Канд. техн. наук, директор департамента информационной безопасности ООО «УЦСБ»
Тел.: 8 (343) 379-98-34
Эл. почта: bogdanov.valentin@gmail.ru

Новоселова Юлия Сергеевна
Аспирант каф. алгебры и дискретной математики Уральского федерального университета
Тел.: 8 (343) 379-98-34
Эл. почта: yulia.novoselova@yandex.ru

Bogdanov V.V., Novoselova J.S.

Topicality of information security provisioning in cloud computing systems, cloud computing systems, threats sources analysis

Characteristic features of cloud computing systems are suggested. A topicality of a task of analysis of information security threats for cloud computing systems is justified, peculiarities of a solution of that task in comparison with the analysis of information security threats of conventional information systems are shown. The mathematical model of cloud computing systems is constructed. A research of threats sources in cloud computing systems is conducted.

Keywords: cloud computing system, information security threat, threats sources.