10 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 007.51

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ НА ОСНОВЕ БАЙЕСОВСКОГО ПОДХОДА

И.А. Зикратов, С.В. Одегов

Предложен новый подход к анализу и количественной оценке защищенности ресурсов в облачных системах, основанный на использовании особенностей реализации распределенной вычислительной сети. Для повышения степени достоверности оценки в рамках разработанного подхода предложено использование байесовского подхода.
Ключевые слова: информационная безопасность, облачные вычисления, оценка угроз.

Введение

Проблема оценки информационной безопасности (ИБ) стоит в ряду первостепенных задач при проектировании автоматизированных систем (АС). Под информационной безопасностью понимается состояние рассматриваемой системы, при котором она способна противостоять дестабилизирующему воздействию внешних и внутренних информационных элементов самой системы и внешней среды.

В качестве стандартной модели безопасности часто приводят модель из трех категорий [1]:

1. конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на нее право;
2. целостность – избежание несанкционированной модификации информации;
3. доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

В настоящее время существуют различные системы защиты информации (СЗИ) для автоматизированных систем, разработка и применение которых осуществляется в рамках существующей нормативно-правовой базы. Вместе с тем все более широкое распространение находят системы хранения, обработки и передачи данных, основанные на технологии облачных вычислений. Возникает объективное противоречие между необходимостью совершенствования нормативно-правовой базы, регламентирующей разработку средств защиты информации для современных АС, и отсутствием научно-методического аппарата, описывающего подходы к особенностям построения защиты систем, реализующих технологию облачных вычислений. Одной из задач, решаемых разработчиками СЗИ на этапе аудита АС, является задача оценки угроз ИБ. Под угрозой понимается актуализированная опасность информационного воздействия, т.е. событие, которое потенциально может привести к нарушению безопасности информационно-технического объекта. На основе модели угроз, оценки уязвимостей АС определяются требования к СЗИ, обеспечивающей требуемый уровень защищенности информации. В настоящей работе предложен подход для решения этой задачи, заключающийся в использовании особенностей реализации облачных технологий и применении байесовского подхода для количественной оценки степени защищенности ресурсов распределенной сети.

Понятие облачных вычислений

Облачные технологии являются одним из этапов развития технологии распределенных вычислений и виртуализации сетевых ресурсов. Существуют разнообразные определения того, что называется облачными вычислениями. Облачные вычисления – модель обеспечения сетевого доступа к общему пулу конфигурируемых вычислительных ресурсов, которые могут быть оперативно представлены и освобождены с минимальными эксплуатационными затратами [2]. Применение облачных технологий возрастает с каждым годом. Так, к 2013 г. ожидается увеличение капиталовложений в облачные сервисы до 150 млрд долларов [3], что приведет к прогнозированному увеличению доли таких технологий на рынке поставщиков услуг АС.

Рис. 1 иллюстрирует различия в сфере охвата и контроля между подписчиком и поставщиком услуг для каждой из моделей. Из рис. 1 видно, что сферы управления и контроля различны для каждой сервисной модели облачных вычислений.

Облачный сервис состоит из пяти слоев. Два нижних слоя – это физические элементы облачной среды, которые находятся под полным контролем поставщика услуг, независимо от сервисной модели. Остальные слои содержат логические элементы облачной среды. Инфраструктура для виртуализации включает в себя гипервизоры, представляющие собой операционную систему, например, VMware ESX, виртуальные машины, хранилища данных. На уровне платформы содержатся библиотеки и утилиты. Уровень приложений содержит программные приложения для конечных пользователей [4].

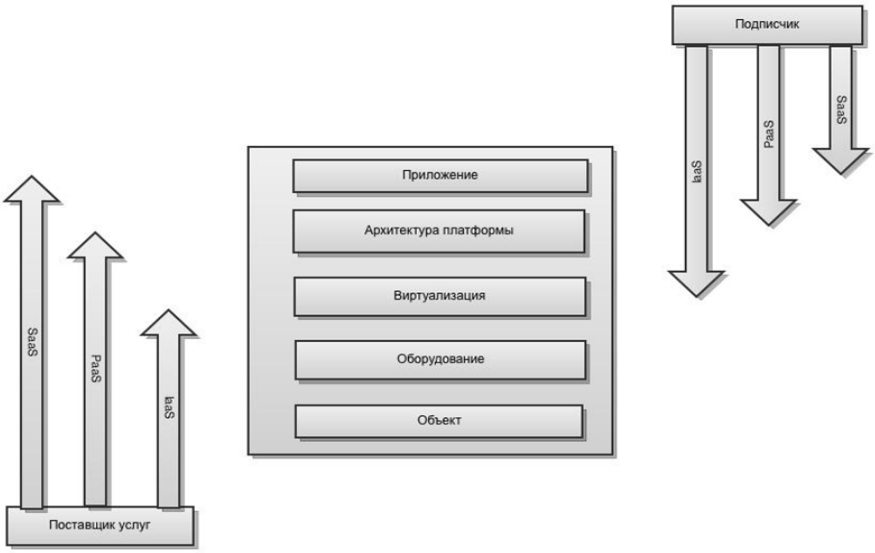

Рис. 1. Архитектура взаимодействия в облачных вычислениях

Таким образом, технология облачных вычислений позволяет утверждать, что ИБ требуется рассматривать с двух точек зрения – поставщика услуг и пользователей обычных ресурсов. С точки зрения поставщика услуг необходимо уяснить и выполнить требования заказчика по безопасности информации в плане обеспечения ее конфиденциальности, целостности и доступности. Реализация этой задачи позволит поставщику определить, какие ресурсы «облака» можно будет использовать в интересах конкретного заказчика, и оценить требования к СЗИ на этих ресурсах. Очевидно, что, так как заказчики могут предъявлять различные требования к моделям безопасности, то для поставщика услуг экономически целесообразно иметь в «облаке» ресурсы с различной степенью защищенности. Например, для регулирования взаимоотношений между поставщиком услуг и пользователем в зарубежных странах применяется соглашение об уровне обслуживания SLA (Service Level Agreement).

Современные угрозы облачным вычислениям

В настоящее время наибольшее распространение получили следующие угрозы облачным вычислениям [5]: злоупотребление доступом и нарушение правил использования сети; инсайдеры; уязвимости технологии облачных вычислений.

Контроль за формированием и динамическим изменением угроз является одним из определяющих факторов для выявления угроз ИБ. Схема, представленная на рис. 2, позволяет оценить качественную картину угроз распределенным системам [5].

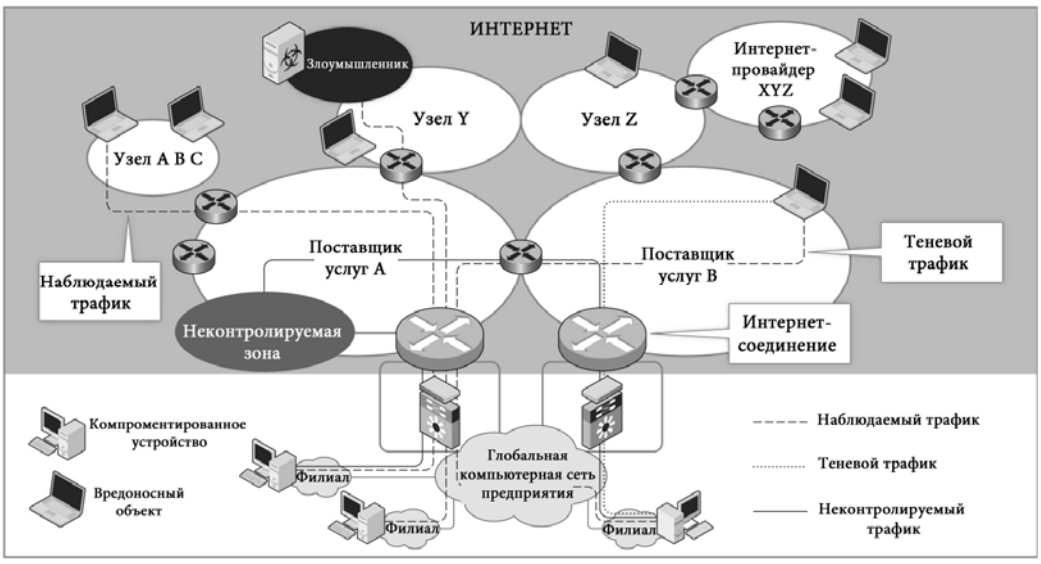

Рис. 2. Схема угроз облачным вычислениям

Из рис. 2 видно, что злоумышленник, используя скомпрометированные компьютеры сети, может получить несанкционированный доступ к вычислительным и конфиденциальным ресурсам облачной сети. Аналогично, инсайдеры могут получить доступ к конфиденциальным данным пользователя, обрабатывающимся в облачной сети. Для количественной оценки уязвимости используют различные методики.

Методика оценки угроз ИБ при использовании облачных вычислений

Из литературы известны различные методики для оценки угроз информации и уязвимостей АС, используемые для локальных вычислительных систем (ЛВС). К наиболее известным из них относятся [1, 6, 7]:

- методика экспертного оценивания системы безопасности информации;
- методика многокритериальной оценки;
- модель СЗИ с полным перекрытием;
- методика на основе базового показателя уязвимости;
- другие методики.

Недостатком существующих методик является сложность применения к современным каналам несанкционированной передачи информации (КНПИ) для распределенных систем. Это обусловлено следующими факторами:

- КНПИ различны для каждой реализации технологии облачных вычислений;
- понятие «контролируемой зоны» становится неактуальным;
- отсутствует возможность получения каких-либо количественных экспертных оценок о вероятности реализации угроз ввиду незнания географии, условий функционирования и степени защищенности ресурсов.

Кроме того, относительная редкость возникновения события в ЛВС – реализация *i*-й угрозы по *j*-му КНПИ – приводит к трудностям при попытке использования статистических методов оценки вероятности угрозы.

В то же время, как следует из рис. 2, основной особенностью облачных сетей является «распределенность» ресурсов. Это означает наличие в «облаке» относительно большого числа разнотипных узлов, что предоставляет возможность создания механизма для статистического «накопления» знаний об угрозах, уязвимостях и успешности их устранения путем сопоставления оценки уязвимости *k*-го узла сети *n*-го типа с аналогичными ресурсами сети при воздействии по нему *i*-й угрозы по *j*-му КНПИ. Реализация такого механизма позволит осуществлять динамическое уточнение модели угроз в процессе эксплуатации АС и адаптивного управления СЗИ.

Методологической основой описанного подхода для оценки угроз облачных вычислений могут служить так называемые интеллектуальные методы анализа данных. Наиболее распространенным из них является байесовский подход, который предоставляет ряд преимуществ:

- возможность получения апостериорной оценки вероятности инцидента;
- возможность отслеживания поступления новых данных;
- выявление зависимость между факторами, влияющими на ИБ;
- логическое объяснение своих выводов, физическая интерпретация и изменение структуры отношений между значениями задачи.

В основе байесовских сетей лежит теорема Байеса. Теорема Байеса – основная теорема элементарной теории вероятности, которая позволяет определить вероятность того, что произошло какое-либо событие при наличии статистических данных.

Привлекательность байесовского подхода состоит в том, что имеющаяся в распоряжении экспертов информация может не отвечать требованиям представительности статистической выборки, что делает использование многих традиционных частотных подходов неправомерным. Более того, ситуация, в которой принимается решение в сфере ИБ, может быть вообще новой и никогда ранее не анализируемой. Эти особенности усложняют процесс принятия решений и могут поставить под сомнение какие-либо выводы и заключения. В этом случае байесовский подход может оказаться весьма полезным и эффективным для количественной оценки факторов.

Пример оценки угроз ИБ при использовании облачных вычислений

Рассмотрим тривиальный пример. На рис. 3 представлен фрагмент распределенной вычислительной системы, в составе которой имеются ресурсы различного уровня (класса) защищенности – «уровень А», «уровень В» и «уровень С», в зависимости от СЗИ, реализованной на данном ресурсе.

Предположим, что необходимо определить степень защищенности ресурсов исследуемой информационной «облачной» системы от некоторой угрозы *Y*:

- 1-я группа («уровень А») – защищенные системы;
- 2-я группа («уровень В») – системы с высокой степенью защищенности;

– 3-я группа («уровень С») – системы с низкой степенью защищенности.

Таким образом, при анализе конкретного ресурса имеются три гипотезы θ_i ее принадлежности n-й группе, n = 1, 2, 3. Пусть из общей статистики воздействия угроз вида Y на узлы «облака» известно, что 50% таких узлов оказались защищенными, 30% узлов имеют высокую и 20% – низкую защищенность. Используя эти данные, можно определить априорные вероятности гипотез $P(\theta_1)=0,5$; $P(\theta_2)=0,3$; $P(\theta_3)=0,2$.

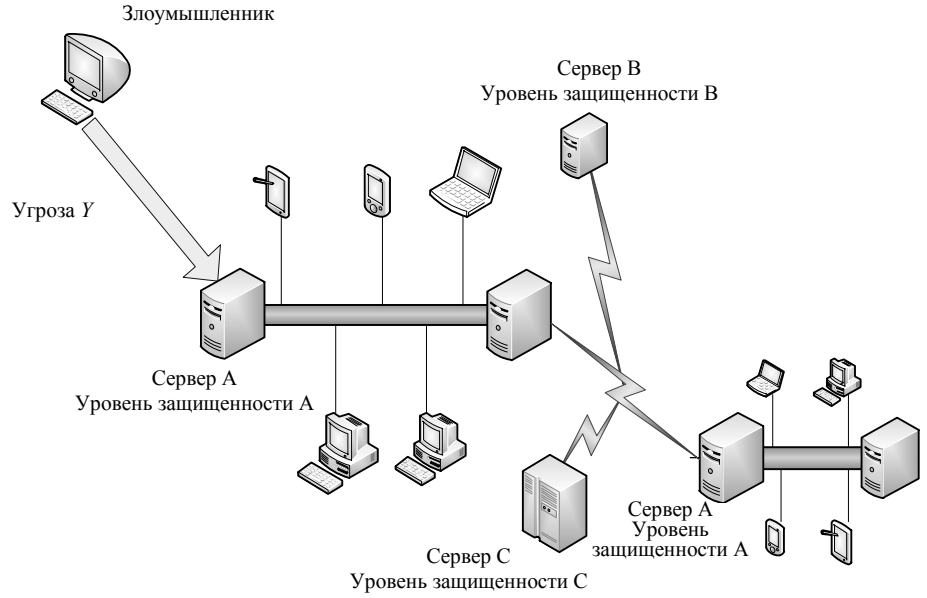

Рис. 3. Фрагмент распределенной вычислительной сети

Очевидно, что признаками защищенности ресурсов в «облаке» могут служить различные показатели, анализ и разработка которых выходит за рамки данной работы.

Для иллюстрации использования байесовского подхода в рассматриваемом примере из всего кортежа возможных показателей защищенности системы защиты выберем три: способность СЗИ обеспечить конфиденциальность информации при воздействии угрозы Y (y_1), способность СЗИ обеспечить целостность информации (y_2) и способность СЗИ обеспечить доступность информации (y_3). Допустим, что из анализа угроз такого типа известно, что при воздействии на ресурсы 1-й группы конфиденциальность обеспечивалась в 60% случаев, при воздействии на ресурсы 2-й группы – в 80% случаев, на ресурсы 3-й группы – в 15% случаев. Отсюда можно записать условные вероятности $P(y_1/\theta_1)$=0,6; $P(y_1/\theta_2)$=0,8 и $P(y_1/\theta_3)$=0,15. Также известно, что при воздействии угрозы Y имеющиеся СЗИ узлов 1-й группы позволили обеспечить целостность информации в 70% случаев. Для СЗИ 2-й и 3-й группы защищенности такие показатели равны соответственно 90% и 2%. Тогда можно записать условные вероятности $P(y_2/\theta_1)$=0,7, $P(y_2/\theta_2)$=0,9 и $P(y_2/\theta_3)$=0,02.

По аналогии примем показатели защищенности узлов 1, 2 и 3-й групп при воздействии угрозы Y в отношении модели доступности:

$P(y_3/\theta_1)$=0,8, $P(y_3/\theta_2)$=0,9 и $P(y_3/\theta_3)$=0,5.

Предположим, что достоверно выявлено воздействие угрозы рассматриваемого типа на исследуемый или аналогичный ресурс, оснащенный одинаковыми СЗИ. При этом нарушения конфиденциальности информации, хранимой на атакованном ресурсе, не произошло. Учитывая показатель y_1, вычислим апостериорные вероятности гипотез для одного свидетельства:

$$P(\theta_1/y_1)=\frac{P(y_1/\theta_1)P(\theta_1)}{\sum_{i=1}^{3}P(y_1/\theta_i)P(\theta_i)}=0,53,$$

$$P(\theta_2/y_1)=\frac{P(y_1/\theta_2)P(\theta_2)}{\sum_{i=1}^{3}P(y_1/\theta_i)P(\theta_i)}=0,42,$$

$$P(\theta_3 / y_1) = \frac{P(y_1 / \theta_3) P(\theta_3)}{\sum_{i=1}^{3} P(y_1 / \theta_i) P(\theta_i)} = 0{,}05.$$

Из результатов расчета следует, что после того, как y_1 произошло, доверие к гипотезам θ_1 и θ_2 возросло, а к гипотезе θ_3 – снизилось.

Очевидно, что если в результате опыта выяснилось, что СЗИ не обеспечила конфиденциальность информации при воздействии угрозы, то необходимо рассматривать противоположные события $P(\overline{y}_1 / \theta_i) = 1 - P(y_1 / \theta_i)$. Тогда получим $P(\theta_1 / \overline{y}_1) = 0{,}47$, $P(\theta_2 / \overline{y}_1) = 0{,}14$ и $P(\theta_3 / \overline{y}_1) = 0{,}40$. Таким образом, доверие к гипотезе о низкой защищенности исследуемого ресурса существенно возрастает, а доверие к гипотезе о высокой степени надежности резко уменьшается.

В процессе сбора фактов вероятности гипотез будут повышаться, если факты поддерживают их, или уменьшаться, если факты опровергают их. Если одновременно получены два показателя y_1 и y_2, т.е. установлено, что обеспечены конфиденциальность и целостность, то при условии их независимости можно воспользоваться формулой

$$P(\theta_i / y_1, y_2) = \frac{P(y_1 / \theta_i) P(y_2 / \theta_i) P(\theta_i)}{\sum_{i=1}^{3} P(y_1 / \theta_i) P(y_2 / \theta_i) P(\theta_i)}.$$

Вероятности гипотез в этом случае будут равны $P(\theta_1 / y_1, y_2) = 0{,}49$; $P(\theta_2 / y_1, y_2) = 0{,}51$; $P(\theta_3 / y_1, y_2) = 0$.

По сравнению с результатами, полученными по одному показателю y_1, доверие к первой и третьей гипотезе снизилось, а ко второй – возросло. Исходя из этого, с вероятностью 0,51 исследуемый узел можно отнести к группе ресурсов с высокой степенью защищенности по отношению к воздействию угрозы типа *Y*. При получении показателя y_3 расчеты проводятся аналогично.

Осуществив подобные расчеты для всех угроз безопасности в соответствии с моделью угроз и зная требования заказчика по обеспечению моделей безопасности, можно принимать обоснованные решения на предоставление ресурсов той или иной степени защищенности, а также, при необходимости, конфигурировать СЗИ для ресурсов различных групп.

Таким образом, приведенный пример, не претендуя на глубокий анализ байесовского подхода, иллюстрирует его практическую применимость в задачах построения СЗИ и управления информационной безопасностью в распределенных вычислительных сетях.

Заключение

Широкое распространение облачных вычислений на рынке поставщиков IT-услуг приводит к необходимости совершенствования научно-методического аппарата для построения систем защиты информации. Предлагаемый подход позволяет на основе модели угроз, требований заказчика к обеспечению конфиденциальности, целостности и доступности информации осуществлять количественную вероятностную оценку защищенности ресурсов при использовании облачных вычислений.

Особенностью подхода, предлагаемого авторами, является использование не только априорных, но и апостериорных оценок защищенности ресурсов облачной сети на основе анализа функционирования узлов с различными системами защиты информации и байесовского решающего правила. Это позволит принимать обоснованные решения по предоставлению услуг на обработку информации различной степени конфиденциальности.

Работа выполнена по ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технического комплекса России на 2007–2013 годы» в рамках государственного контракта № 07.524.12.4009 на выполнение опытно-конструкторских работ.

Литература

1. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004. – 282 с.
2. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. Draft NIST Special Publication 800-144. – Gaithersburg, 2011. – 52 p.
3. CNews Analytics (CNA). Влияние кризиса на рынок IT-услуг [Электронный ресурс]. – Режим доступа: http://www.cfin.ru/anticrisis/companies/branch/it.shtml, свободный. Яз. рус. (дата обращения 25.02.2012).
4. Catteddu D., Hogben G. Cloud Computing: Benefits, risks and recommendations for information security. – Heraklion: ENISA, 2009. – 125 p.
5. Macaulay T. Upstream Intelligence Use Cases // IANewsletter. – 2011. – V. 14. – P. 18–22.

6. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ТИД «ДС», 2008. – 688 с.
7. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997. – 537 с.

Зикратов Игорь Алексеевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, доцент, зав. кафедрой, zikratov@cit.ifmo.ru

Одегов Степан Викторович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, odegov.sv@gmail.com