КРАТКИЕ СООБЩЕНИЯ

УДК 004.9

КОНЦЕПЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В.А. ВИШНЯКОВ, М.М. ГОНДАГ САЗ, М.Г. МОЗДУРАНИ ШИРАЗ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 11 марта 2016

Представлена концепция итнегрированной корпоративной информационной сети (ИКИС) с использованием облачных вычислений (ОВ), показаны варианты таких структур. Проанализированы основные проблемы информационной безопасности (ИБ) при использовании ОВ, механизмы аутетификации пользователей. Приведены направления развития ИБ в ИКИС с использованием интеллектуальных технологий. Предложены модели ИБ в ИКИС с использованием многоагентных технологий. Представлена концепция построения архитектуры ИБ в ИКИС и направления ее развития на базе интеллектуального управления и семантических технологий.

Ключевые слова: КИС, интеллектуальные технологии, информационная безопасность, облачные вычисления.

Для автоматизации и информатизации управления на предприятиях с 70-х годов 20 века используются корпоративные информационные системы (КИС), в основе которых лежат два основных стандарта: MRP (material requirements planning) (с 70-х гг.), ERP (enterprise requirements planning) (с конца 80-х гг.) [1]. По предложению Gartner Group, концепция ERP-систем нового поколения (с начала 2000-х гг.) на основе применения интернет-технологий в практике корпоративного управления, получает название ERP II (Enterprise Resource and Relationship Processing – управление ресурсами и внешними отношениями предприятия) [2]. Особое изменение КИС претерпевают с развитием и использованием новой парадигмы «облачные вычисления» (интегрированная КИС − ИКИС) [3].

Развитие технологий и сред облачных вычислений (СОВ) вносит новые источники угроз, которые необходимо учитывать при обеспечении безопасности компьютерных систем и сервисов. Наметилась тенденция использования СОВ в корпоративных системах управления (КИС) организациями. Динамический характер процессов информационного взаимодействия затрудняет возможности оперативной оценки рисков нарушения конфиденциальности, целостности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа.

Технологии облачных вычислений (ОВ). «Облачная обработка данных» – это парадигма, в рамках которой информация постоянно хранится на серверах в Интернете (датацентрах) и временно кэшируется на клиентской стороне, на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т.д. [4]. До облачных вычислений Вэб-сайты и серверные приложения выполнялись на отдельно взятых системах. С приходом облачных вычислений ресурсы используются как объединенный виртуальный компьютер. Виртуальная машина эмулирует работу реального компьютера и включает в себя: сконфигурированную ОС, Веб-сервер, базу данных, защиту (firewall), почтовый сервер, а также большое число настроек, от

которых зависят надежность, производительность и безопасность Веб-проекта. Используются 3 основных технологии ОВ: ПО как услуга – (SaaS), инфраструктура как услуга – (IaaS), платформа как услуга – (PaaS) [4].

Структуры ИКИС. Разделим ИКИС по технологиям применения ОВ: малые − на базе SaaS, средние − на базе IaaS, большие на базе PaaS. Большинство предприятий будет работать по гибридной модели, предоставляя и потребляя облачные услуги, которые при необходимости будут интегрироваться в традиционные модели ИТ. Формируется новая модель информационных систем: вместо установки пакетов приложений на свои компьютеры компании будут использовать браузеры, чтобы получить доступ к широкому ассортименту облачных услуг, доступных по первому требованию. Аренда облачных услуг позволяет: отнести расходы, связанные с использованием информационных систем, к переменным, а не постоянным издержкам; создавать системы анализа данных, отображающие работу предприятия, интегрируя данные из отдельно систем CRM и ERP; создавать прототипы новых продуктов и инновационные проекты, развивая взаимодействие между сотрудниками, преодолевая границы организаций и государств [4].

Угрозы информационной безопасности в малых ИКИС. Поскольку малые ИКИС используют ПО, рассмотрим угрозы от его облачного использования. Исследование области обеспечения безопасности СОВ проводились как российскими, так и зарубежными учеными, среди которых следует отметить: Danish Jamil провел типизацию угроз для сред облачных вычислений и предложил ряд решений, позволяющих противодействовать рассмотренным угрозам; Michael Miller провел анализ механизмов безопасности сред облачных вычислений и выделил общие неустранимые недостатки [5].

Анализ состояния ИБ в СОВ выявил применение технологий адаптивных систем защиты, которое не всегда позволяет осуществлять контроль за информационными потоками, поскольку они функционируют на верхних уровнях иерархии; классические методы поиска вредоносного программного кода не позволяют обнаруживать новые образцы вредоносного ПО (ВПО), реализующего технологии DKOM и VICE, так как они встраиваются в ОС на более «низком» уровне, чем модули адаптивных систем защиты; обычные методы перехвата системных функций гостевых ОС не позволяют обнаруживать программные «закладки», осуществляющие внедрение в ОС на этапе загрузки [6].

Применение сред ОВ ведет к появлению новых проблем ИБ, таких как: распространение ВПО посредством сред ОВ; доверие поставщику услуг среды ОВ; проблема выявления ВПО, ориентированного на среды ОВ; проблема выявления ПО, не являющегося вредоносным, но содержащим в себе ошибки разработчика.

Построение перспективных механизмов обеспечения безопасности в среде ОВ связывается не с защитой от выявленных уязвимостей, а заключается в возможности предотвращения новых неизвестных методов проведения атак, в разработке новых моделей угроз и методов предотвращения или отражения компьютерных атак на информационные ресурсы, которые используют возможности предикативной идентификации скрытых каналов и потенциально опасных процессов информационного взаимодействия. Необходимо разработать: модели скрытых угроз информационной безопасности в среде ОВ; модели операций, происходящих с данными при их обработке в СОВ; метод обнаружения скрытых угроз; алгоритм предикативной идентификации скрытых угроз в гостевой ОС и гипервизоре [6].

Механизмы аутентификации и атак в среде ИКИС. Они анализируются в зависимости от факторов: «знание» используется при вводе пароля или ответа на секретный вопрос, «электроника» означает применение электронных идентификаторов (USB-ключи, смарт-карты, другие *е*-токены), «био» применяется в системах распознавания отпечатков пальцев, геометрии руки, оболочки глаза, голоса, почерка и т.д., «социальный» использует разговор с оператором. Механизмы аутентификации можно рассмотреть по приоритету их использования: основные − при штатном входе в систему, резервные (почтовый ящик) − при потере пароля либо взломе учетной записи, последние (last resort) − при вмешательстве администрации информационной системы [7].

Проанализированы системы обнаружения атак (СОА): Snort, Bro, Prelude, OSSEC, Suricata, тенденции их развития. Перечень критериев, которым должна удовлетворять СОА: многоуровневость наблюдения за системой; адаптивность (способность обнаруживать

модифицированные реализации известных атак и новые виды атак); проактивность, (обладание встроенными механизмами реакции на атаку); открытость (возможность добавления новых анализируемых ресурсов); совмещение централизованного и распределенного управления; защищенность (иметь средства защиты своих компонентов [8].

Направления развития ИБ в ИКИС можно определить следующим образом:

− разработка моделей нарушения и противодействия ИБ в ИКИС на основе выбора оптимального варианта реагирования на события безопасности;

− совершенствование архитектур систем ЗИ для ИКИС, обеспечивающих эффективное управление в условиях неопределенности состояния информационной среды;

− совершенствование инструментальных программных комплексов с интеллектуальной поддержкой принятия решений с исследованием эффективности методов, моделей и алгоритмов;

− развитие технологий многоагентных систем для обнаружения атак, противодействия угрозам нарушения ИБ, оценки уровня защищенности информации в ИКИС;

− разработка моделей и средств защиты ИКИС на базе облачной инструментальной платформы проектирования ИС ИБ на основе семантических технологий.

Модели для информационной безопасности в ИКИС. Входом модели, учитывающей динамический характер ресурсов и структуру протоколов сетевого взаимодействия, является поток сетевых пакетов, которые поступают в межсетевые экраны системы ЗИ в среде ОВ, а выходом является разделение пакетов на виртуальные соединения, принадлежность соединению и определение подмножества правил фильтрации для них [9]. Модель противодействия угрозам ИБ в КИС, в которой решение о варианте реагирования принимается в зависимости от вероятности атаки, оцениваемой с использованием механизма нечеткого логического вывода [9].

Для развития моделей ИБ в ИКИС предложено использовать алгебру объектов [3]. В ней разработано описание носителей и коммуникаторов в вычислительной среде, а также уровней абстракции объектов; дано представление не связанных, параллельных, конкурирующих объектов на одном уровне абстракции; введено описание развивающегося, приостановленного, создаваемого, несуществующего, объектов, что позволило показать, что основные дизъюнкты (правило, факт, запрос, пустой) аналогичны этим видам объектов [3]. В моделях ИБ объекты трансформируются в модели агентов [10]. В общем виде модель ИБ в ИКИС представим в виде: $M_{ik} = (M_t, M_a, M_s, M_p)$, где M_a − модель обнаружения угроз, M_t − модель аутентификации пользователей, M_s − модель анализа и оценки ПО (позволяющая получать вывод о наличии или отсутствии его деструктивных свойств), M_p − модель противодействия угрозам.

С учетом многоагентного подхода эта модель трансформируется в следующий вид: $M_{ik} = (A_t, A_a, A_s, A_{ta}, A_p, A_c)$, где A_t − агенты обнаружения угроз, A_a − агенты, разграничивающих права доступа пользователей, A_s − агенты анализа и оценки ПО, A_{ta} − определения типа атаки, A_p − агенты, строящих сценарий поведения для отражения атак, A_c − агенты координаторы всей многоагентной системы. Для малой ИКИС эта модель сократится до вида $M_{ik} = (A_a, A_s, A_p, A_c)$.

Концепция архитектуры ИБ с использованием интеллектуальных технологий. Такая архитектура включает систему ввода воздействий, базу знаний на основе правил продукций и фреймов, решатель с использованием механизма логического вывода, базу агентов, средства коммуникации с агентами, координатор. Для задачи обнаружения вирусных атак, система ввода воздействий передает факты о внешних воздействиях в базу знаний. Решатель на основе логического вывода вырабатывает решение, которое передается координатору об изменениях внешней среды. Для распределенного решения координатор может использовать из базы агентов разные их типы: субкоординатор, исполнители, интегратор.

Агенты могут быть связаны между собой в виде многоуровневой архитектуры. Для решения задачи обнаружения вирусных атак подходит такая многоуровневая архитектура агентов. С учетом специфики решаемой задачи проектируемая многоагентная архитектура должна включать несколько видов агентов, которые выполняют различные функции. В результате анализа информационного процесса обнаружения вирусных атак в сетях ИКИС можно рассматривать таких агентов: аутентификации пользователей сети, обнаружения атак,

определения их типов, строящих сценарий поведения для отражения вирусной атаки, являющийся субкоординатором всей многоагентной архитектуры.

Состав инструментальной платформы ИБ в ИКИС. Предложены (расширенные) решения по инструментальной платформе на базе многоагентной технологии [11]:

– разработка структуры многоагентной системы обнаружения атак, включающая в себя агентов рабочих станций, серверов, маршрутизаторов, гипервизора и позволяющая делать вывод о атаках, состоянии и перспективах ее защиты;

– получение метода принятия агентами совместного решения, позволяющего сформировать общение агентов и на основании результатов анализа сведений, полученных из различных источников, оценить состояние ОВ в целом;

– выработка методики обнаружения атак с использованием многоагентных технологий, позволяющая обучить многоагентную систему и использовать ее для дальнейшего обнаружения неизвестных воздействий ОВ;

– расчет эффективности предложенных методов, используя разработанные программные решения.

Такая инструментальная платформа включает в себя конструктор варианта, библиотеку агентов, базу правил, базу методов. На основании описания требований к варианту ИБ конструктор генерирует вариант системы ИБ для конкретной ИКИС.

Выводы

1. Показано, что изменения КИС претерпевают с использованием парадигмы облачных вычислений, появляются интегрированные КИС (ИКИС). ИКИС разделены по технологиям применения ОВ: малые, средние и большие на базе IaaS. Создавая инструментальные платформы бизнес-процессов в ИКИС, корпорации могут приобрести дополнительные возможности для инноваций, повышения производительности и удовлетворения спроса, предъявляемого современными рынками. Архитектура ИБ с использованием интеллектуальных технологий включает систему ввода воздействий, базу знаний на основе правил продукций и фреймов, решатель с использованием механизма логического вывода, базу агентов, средства коммуникации с агентами, координатор.

2. Одним из направлений в СЗИ ИКИС является разработка моделей, методов, архитектур и аппаратно-программных средств управления ИБ для решения проблемы защиты на базе облачной инструментальной платформы, созданной на основе семантических технологий.

CONCEPT OF CORPORATE INFORMATION SYSTEMS WITH CLOUDING COMPUTING AND ITS INFORMATION SECURITY

U.A. VISHNIAKOU, M.M. GONDAG SAS, M.G. MOZDURANI SHIRAZ

Abstract

Concept of integration corporate information systems (ICIS) with clouding computing (CC) is represented. Variants such ICIS are shown. Main problems of information security (IS) in CC area and mechanism of authentification are analyzed. Development directions of IS in ICIS with use of intelligent technologies are given. Models of IS in ICIS with use of multi agents technologies are proposed. Concept of architecture building of IS in ICIS and its development on the base of intelligent management and semantic technologies are represented.

Ключевые слова: corporate information systems, intelligent technologies, information security, clouding computing.

Список литературы

1. Информационные технологии в бизнесе. / Под ред. Железны М. СПб., 2012.
2. Meeker M. Internet Trends. [Электронный ресурс]. – Режим доступа: http://www.slideshare.net/kleinerperkins/kpcb-internet-trends-2011-9778902. – Дата доступа: 20.02.2016.
3. *Вишняков В.А.* Информационное управление и безопасность: методы, модели, программно-аппаратные решения. Минск, 2014.
4. *Фингар П.* Облачные вычисления – бизнес-платформа XXI века. М., 2011.
5. *Туманов Ю.М.* Защита сред облачных вычислений путем верификации программного обеспечения на наличие деструктивных свойств: Автореф. дис. ... канд. техн. наук. М., 2012.
6. *Моляков А.С.* Модели и метод противодействия скрытым угрозам информационной безопасности в среде облачных вычислений: Автореф. дис. ... канд. техн. наук. СПб, 2014.
7. *Малков А.А.* Технология аутентификации с помощью доверенных лиц: Автореф. дис. ... канд. техн. наук. Уфа, 2013.
8. *Никишева А.В.* Многоагентная система обнаружения атак на информационную систему предприятия: Автореф. дис. ... канд. техн. наук. Волгоград, 2013.
9. *Машкина И.В.* // Системы управления и информационные технологии. 2008. № 2 (32). С. 98–104.
10. *Лукашин А.А*. Система защиты информационного взаимодействия в среде облачных вычислений: Автореф. дис. ... канд. техн. наук. СПб, 2012.
11. *Вишняков В.А., Гондаз Саз М.М., Моздурани Шираз М.Г.* // Матер. 5 Междунар. научн.-техн. конф. «OSTIS-2015». Минск, 2015. С. 173–176.