OSTIS-2015
(Open Semantic Technologies for Intelligent Systems)

УДК УДК 004.9

КОНЦЕПЦИЯ ИНСТРУМЕНТАЛЬНОЙ ПЛАТФОРМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Вишняков В.А., Гондаз Саз М.М., Моздуоани Шираз М.Г.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

vish2002@list.ru

Проанализированы основные проблемы информационной безопасности при использовании облачных вычислений (ОВ) и направления их решений. Показано использование интеллектуальных технологий в информационной безопасности. Представлены направления совершенствования интеллектуального управления с использованием ОВ и получение корпоративного интеллекта. В качестве концепции предложено создание инструментальной платформы, объединяющей интеллектуальные системы защиты для облачной среды на основе семантических технологий.
Ключевые слова: интеллектуальные технологии, информационная безопасность, облачные вычисления, инструментальная платформа

Введение

Развитие технологий и сред облачных вычислений (СОВ) вносит новые источники угроз, которые необходимо учитывать при обеспечении безопасности компьютерных систем и сервисов. При этом динамический характер процессов информационного взаимодействия затрудняет возможности оперативной оценки рисков нарушения конфиденциальности, целостности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа [Моляков А.С., 2014].

Традиционные средства обеспечения информационной безопасности (ИБ) такие как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи. Поэтому угрозы, реализуемые посредством скрытых каналов передачи информации не могут быть блокированы. В связи с этим необходимо использовать интеллектуальные технологии защиты от угроз, которые формируются посредством скрытых каналов информационного воздействия или внутри периметра безопасности корпоративной компьютерной сети [Электр. ресурс, 2013].

1. Угрозы информационной безопасности в среде ОВ

Исследование области обеспечения безопасности СОВ проводились как российскими, так и зарубежными учеными, среди которых следует отметить: Danish Jamil провёл типизацию угроз для сред облачных вычислений и предложил ряд решений, позволяющих противодействовать рассмотренным угрозам; Michael Miller выполнил анализ механизмов безопасности сред облачных вычислений и выделил общие неустранимые недостатки [Туманов Ю.М., 2012].

Анализ состояния ИБ в СОВ выявил применение технологий адаптивных систем защиты, которые 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. Традиционные методы перехвата системных функций гостевых ОС не позволяют обнаруживать программные «закладки», которые внедряются в ОС на этапе загрузки [Моляков А.С., 2014].

Применение сред ОВ ведет к появлению новых проблем ИБ, таких как: распространение ВПО посредством сред ОВ; доверие поставщику услуг

среды ОВ; выявление ВПО, ориентированного на среды ОВ; выявление ПО, не являющегося вредоносным, но содержащим в себе ошибки разработчика.

Построение перспективных механизмов обеспечения безопасности в среде облачных вычислений связывается не только с защитой информации (ЗИ) от выявленных уязвимостей, а с возможностью предотвращения новых неизвестных методов проведения атак, а также 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. Для этого 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.

Механизмы аутентификации в среде ОВ классифицируются 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 [Малков А.А., 2013].

2. Направления интеллектуализации в информационной безопасности

Основные задачи, которые должны решать интеллектуальные системы ЗИ СОВ (ИСЗИ): обнаружение неизвестных вторжений; поддержки принятия решения о перераспределении ресурсов систем ЗИ; возможности автоматического изменения свойств и параметров в зависимости от изменения условий среды функционирования; дезинформации нападающей стороны о свойствах и параметрах защиты. ИСЗИ, обеспечивающие обнаружения атак, в качестве интеллектуального инструмента используют нейронные сети (НС), системы нечеткой логики и экспертные системы (ЭС).

В ИСЗИ на основе ЭС в базе знаний содержится описание правил, соответствующим профилям легальных пользователей и сценариям атак. Недостатки ИСЗИ на базе ЭС: система не является адаптивной и не обнаруживаются неизвестные атаки. Если НС представлена в виде системы обнаружения атак, при обработке трафика происходит анализ информации на наличие злоупотреблений. Случаи с указанием на атаку перенаправляются к администратору безопасности. Подход быстродействующий, поскольку используется один уровень анализа. Основной недостаток НС является «непрозрачность» формирования результатов анализа. В системах обнаружения атак с применением НС и ЭС, если идентифицируются новые атаки, то базу следует обновить. Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет хранить нечеткие предикатные правила, которые автоматически корректируются в процессе обучения НС. Свойство адаптивности нечетких НС позволяет решать задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, автоматически формировать новые правила при изменении типа угроз [Калач А.В., 2011].

Предложена концепция построения ИСЗИ предприятия, основанная на сочетании принципов функциональной интеграции, иерархической организации, комплексирования моделей, методов и алгоритмов, стандартизации систем ЗИ, что позволяет построить архитектуру автоматизированной системы защиты информации, основанной на многоагентном подходе [Погорелов Д. Н., 2008].

3. Направления защиты информацион-ных ресурсов в среде ОВ

Одним из направлений является разработка, включающая: математическую модель представления ПО, позволяющая получать формальный вывод о наличии или отсутствии его деструктивных свойств; описание классифицирующего признака ПО, обладающего деструктивным свойством; алгоритм классификации ПО, использующий подход к оценке подобия различных экземпляров ПО; методику верификации ПО на наличие деструктивных свойств для сред ОВ [Туманов 2012];

Для решения задачи обнаружения вирусных атак в сети Интернет предложена архитектура на основе продукционной системы с многоуровневой вертикальной моделью агентов. Архитектура включает базу знаний в виде правил продукций, механизм логического вывода, рецепторы и эффекторы агента, модуль коммуникации с другими агентами. Применительно к задаче обнаружения вирусных атак, рецепторы передают факты о внешних воздействиях в базу знаний. В результате логического вывода вырабатывается решение, которое передается эффектору об изменениях внешней среды. Для распределенного решения задач используются разные типы агентов: агент-субординатор, множество агентов исполнителей, агент-интегратор. Агенты связаны между собой в

виде многоуровневой архитектуры, которая может быть горизонтальной или вертикальной. Для решения задачи обнаружения вирусных атак подходит вертикальная многоуровневая архитектура агентов. С учетом специфики решаемой задачи многоагентная система должна включать несколько агентов, которые выполняют в системе различные функции. В результате анализа информационного процесса обнаружения вирусных атак в сетях ОВ можно рассматривать агентов: разграничивающих права доступа пользователей сети, обнаружения вторжений, обнаружения типа атаки, строящих сценарий поведения для отражения вирусной атаки, агент, являющийся посредником-координатором всей многоагентной системы [Берестов А.А, 2011].

Проанализированы системы обнаружения атак (СОА): Snort, Bro, Prelude, OSSEC, Suricata, тенденции их развития. Определен 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 [Никишева А.В. 2013].

Модель, включающая формализацию и контроль информационного взаимодействия в форме виртуальных соединений с помощью межсетевых экранов учитывает динамический характер выделяемых ресурсов и структуру протоколов сетевого взаимодействия. Входом модели является поток сетевых пакетов, которые поступают в межсетевые экраны системы ЗИ в среде ОВ, а выходом является разделение пакетов на виртуальные соединения. Классификация пакетов дана на принадлежность соединению и определению подмножества правил фильтрации для них [Лукашин А.А., 2013].

Модель противодействия угрозам ИБ, в которой решение о варианте реагирования принимается в зависимости от вероятности атаки, оцениваемой с использованием механизма нечеткого логического вывода [Машкина И.В., 2009].

4. Интеллектуализация управления в средах ОВ

На базе Web 3.0 развивается управление в СОВ. Онтология формирует семантику, создавая новые возможности для интеллектуальных агентов (ИА), выполняющих запросы пользователей. Открытое извлечение информации (Information Extraction − IE) обеспечит работу новых форм поиска, освобождая пользователей от задачи по исследованию документов, выданных поисковой машиной. Широко применяются серверы исполнения деловых регламентов (BRE − Business Rules Engine). Чтобы справиться со сложностью бизнес-процессов, связывающих несколько предприятий или цепочку создания иноваций в Web 3.0, компании требуется создания новых процессов, превосходящих современные серверы исполнения регламентов [Вишняков В.А. 2014, Фингар П. 2011].

Распределенный искусственный интеллект − DAI (Distributed Artificial Intelligence) основывается на агентных технологиях. Стандартный программный агент имеет три свойства: автономность, способность реагировать и выйти на связь. Простые программные агенты могут общаться с другими «сущностями»: пользователями, программными агентами или объектами. Добавив к этому способность планировать и ставить цели, поддерживать модели представлений, рассуждать о действиях и повышать уровень знаний и качество работы через обучение, получим главные компоненты ИА.

ИА могут быть интегрированы в структуры ОВ, содержащие конкретные функции по решению задач, обработки данных и управления. Они поддерживают естественное соединение информации и технологий, основанных на знаниях и процесс логических рассуждений, образуя интеллектуальные КИС (ИКИС). ИА позволяют включить функцию обучения и самосовершенствования как на уровне инфраструктуры (адаптивная маршрутизация), так и на уровне приложения (адаптивные пользовательские интерфейсы) [Фингар П. 2011].

ИА используются для сбора бизнес-аналитики − BI (Business Intelligence) и процессов обработки сложных событий − CEP (Complex Event Processing). Показатель посещений страниц устарел, важно количество связей в социальных сетях, отправленных сообщений и время, проведенное на конкретном сайте. Получение информации и непрерывный анализ в реальном времени в ОВ − это следующая задача для ИКИС, для этого надо переходить от «поиска в данных» к «поиску в блогах». В ИКИС необходимо выйти за пределы поисковиков, обработать Интернет-данные, чтобы понять, что же происходит в отрасли, оценить ситуацию о товарах и услугах компании, т.е. нужна аналитика Web 3.0. Когда компании выводят управление бизнес-процессами в сложную деловую экосистему, ценность обработки сложных событий становится опорой для корпоративного интеллекта необходимых для того, чтобы создать и улучшить постоянно меняющиеся бизнес-процессы [Фингар П. 2011].

Данные принципы интеллектуального управления будут использованы в ИС ЗИ для сред ОВ при построении инструментальной платформы [Вишняков В.А., 2014].

5. Концепция инструментальной платформы ЗИ в среде ОВ

Предложены тенденции развития ИТЗИ в СОВ [Машкина И.В., 2009, Вишняков В.А., 2014]:

– совершенствование архитектуры систем ЗИ, обеспечивающих эффективное управление в условиях неопределенности состояния информационной среды;
– разработка новых моделей противодействия угрозам нарушения ИБ на основе выбора оптимального варианта реагирования на события безопасности;
– совершенствование инструментальных программных комплексов с интеллектуальной поддержкой принятия решений и исследованием эффективности методов, моделей и алгоритмов;
– развитие технологий многоагентных систем для обнаружения атак, противодействия угрозам нарушения ИБ, оценки уровня защищенности информации;
– разработка основ, моделей и средств защиты облачной инструментальной платформы проектирования интеллекуальных систем на основе семантических технологий.

Для реализации этих тенденций необходимо построение инструментальной платформы ЗИ в среде ОВ. Платформа будет использоваться для создания пользовательских прикладных ИС. Предложены следующие решения по инструментальной платформе на базе многоагентной системы:

– разработка структура и состав многоагентной системы обнаружения атак, включающая в себя агентов рабочих станций, серверов, маршрутизаторов и сетей 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 решения.

Заключение

Одним из направлением в СЗИ СОВ 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.

Библиографический список

[Моляков А.С. 2014] Моляков, А.С. Модели и метод противодействия скрытым угрозам информационной безопасности в среде облачных вычислений / А.С. Моляков / Автореферат канд. дисс. по спец. 05.13.19. СПб, 2014. – С.17.

[Электронный ресурс, 2013]. Intelligence Community Information Technology Enterprise (ICITE) [Электронный ресурс], режим доступа: http://www.insaonline.org/i/d/a/Resources/ICITE_Doing.aspx (дата доступа 22.10.2013.

[Туманов Ю.М., 2012] Туманов Ю.М. Защита сред облачных вычислений путём верификации программного обеспечения на наличие деструктивных свойств. /Ю.М. Туманов / Автореферат канд. дисс. по спец. 05.13.19, М.: МИФИ, 2012. – 19 с.

[Малков А.А, 2013] Малков, А.А. Технология аутентификации с помощью доверенных лиц / А.А. Малков / Автореферат канд. дисс. по спец. 05.13.19. Уфа: УГАТУ, 2013. – С.16.

[Калач А.В., 2011] Калач, А.В., Немтина Е.С. Интеллектуальные средства и моделирование систем защиты информации @Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 3 (37) – 2011. – С.3-11.

[Погорелов Д.Н., 2006] Погорелов, Д. Н. Защита информационных ресурсов предприятия на основе многоагентной технологии / Д. Н. Погорелов // Автореферат канд. дисс. по спец. 05.13.19. Уфа, 2007. – С.16.

[Берестов А.А, 2011] Берестов, А.А. Архитектура интеллектуальных агентов на основе продукционной системы для защиты от вирусных атак в сети Интернет / А.А. Берестов // Материалы . XV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы» М.: МИФИ, 2011. – С.24-25.

[Никишева А.В, 2013] Никишева, А.В. Многоагентная система обнаружения атак на информационную систему предприятия /А.В. Никишева / Автореферат канд. дисс. по спец. 05.13.19. Волгоград, 2013. – С.19.

[Лукашин, А.А., 2012] Лукашин, А.А. Система защиты информационного взаимодействия в среде облачных вычислений /А.А. Лукашин / Автореферат канд. дисс.по спец. 05.13.19, СПб, 2012.

[Машкина И.В., 2009] Машкина, И.В. Модели и метод принятия решений по оперативному управлению защитой информации / И.В. Машкина // Системы управления и информационные технологии. Москва - Воронеж, 2008. №2 (32). С. 98 – 104.

[Фингар П.., 2011] Фингар П. Облачные вычисления – бизнес-платформа XXI века. Пер. с англ. Захаров А.В. / П. Фингар / – М.: Аквамариновая Книга, 2011. – 256 с.

[Вишняков, В.А., 2014] Вишняков, В.А. Информационное управление и безопасность: методы, модели, программно-аппаратные решения. Монография. / В.А. Вишняков. – Минск: МИУ, 2014. – 287с.

CONCEPTION INSTUMENTAL PLATFORM INFORMATION SECURITY IN CLOUD COMPUTING WITH INTELLIGENCE TECHNOLOGIES

Vishniakou U.A., Gongas Sas M.M., Mosdurani Shiras M.G.

Belorusian State University of Informatic and Radioelectronic,
Minsk, Republic of Belarus

vish2002@list.ru

The main problems of information defense in cloud computing and its decisions are presented. The using of intelligence technologies in information defense are shown. The directions of intellectual management development with cloud computing use (corporative intelligence) are presented. The concept of instrumental platform joined intelligence subsystems defensed for cloud computing area on the base of semantic technologies is proposed.