В.А.ВИШНЯКОВ[1], С.М.ГОНДАГ[2], Ш.М.МОЗДУОАНИ[2]

МОДЕЛЬ И ПРОГРАМНАЯ ПОДДЕРЖКА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В ИНТЕГРИРОВАННЫХ КОРПОРАТИВНЫХ СИСТЕМАХ УПРАВЛЕНИЯ

[1]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь,*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*.

В докладе представлена концепция интнегрированной КИС с использованием облачных вычислений (ОВ), показанны варианты такиз структур. Проанализированы основные проблемы информационной безопасности (ИБ) при использовании ОВ, механизмы аутетификации пользователей. Приведены направления развития ИБ в ИКИС с использование интеллектуальных технологий. Предложены модели ИБ в ИКИС с использованием многоагентных технологий. Представлена концепция построения программного обеспечеия (ПО) ИБ в ИКИС и направления ее развития на базе.

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. Средства безопасности в корпоративных системах управления (КИС) предусматривают уровни защиты по периметру безопасности, такие как межсетевые экраны, системы предотвращения вторжений, зашифрованное сетевое туннелирование [1].

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 [2].

Проанализированы системы обнаружения атак (СОА), 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.

С учетом многоагентного подхода модель ИБ 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.

Структура ПО 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.

ЛИТЕРАТУРА

1. Intelligence Community Information Technology Enterprise (ICITE) [Электронный ресурс], режим доступа : http://www.insaonline.org/i/d/a/Resources/ ICITE_Doing.aspx (дата доступа 22.09.2015.

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