OSTIS-2014
(Open Semantic Technologies for Intelligent Systems)

УДК 33:518/519

СОСТОЯНИЕ, ТЕНДЕНЦИИ И КОНЦЕПЦИЯ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ В ЗАЩИТЕ ИНФОРМАЦИИ

Вишняков В.А.

Минский институт управления,
г. Минск, Республика Беларусь
vish2002@list.ru

В докладе представлены две проблемы использования интеллектуальных технологий в защите информации (ИТвЗИ) – создание специализированных БЗ с моделированием угроз и повышение уровня безопасности в корпоративных сетях и облачных вычислениях. Дан анализ двух направлений из второй проблемы ИТвЗИ: интеллектуальные поддержки принятия решений и использование многоагентных систем. В качестве тенденций развития рассмотрены совершенствования методов, моделей, архитектур, аппаратно-программных решений ИТвЗИ в КИС. В качестве концепции предложено развития ИТвЗИ для облачной инструментальной платформы проектирования интеллекуальных систем на основе семантических технологий.
Ключевые слова: интеллектуальные технологии, защита информации, многоагентные системы, защита в облачной инструментальной платформе

Введение

Для современного этапа развития теории и практики обеспечения защиты информации (ЗИ) характерна такая ситуация: с одной стороны, усиленное внимание к безопасности информационных объектов, повышение требований по ЗИ, принятие международных стандартов в области информационной безопасности (ИБ), растущие расходы на обеспечение защиты, с другой – возрастающий ущерб, причиняемый владельцам информационных ресурсов, о чем свидетельствуют публикуемые данные об ущербе мировой экономике от компьютерных атак [Машкина И.В., 2008].

Выходом является внедрение на всех этапах защиты интеллектуальных технологий, приобретающих все большее распространение в системах ЗИ. С одной стороны, сбор и обработка информации из Интернета о состоянии, направлении развития и уровне угроз тех или иных процессов в мировом сообществе и синтез знаний, отраженных в тех или иных источниках, осуществленный на основе их интеллектуальной обработки, дает новое интегративное качество, позволяющее спрогнозировать, смоделировать и предупредить развитие тех или иных угроз безопасности. С другой стороны, применение интеллектуальных технологий обработки данных дает возможность повысить уровень безопасности различных корпоративных информационных систем (КИС) [Электр. ресурс, 2013] .

1. Направления интеллектуализации в защите информации

Основные задачи, которые должны решать интеллектуальные системы ЗИ (ИСЗИ):

- обеспечение обнаружения неизвестных вторжений;
- обеспечение автоматической поддержки принятия решения о перераспределении ресурсов СЗИ КИС;
- обеспечение возможности автоматического изменения своих свойств и параметров в зависимости от изменения условий среды функционирования;
- обеспечение дезинформации нападающей стороны об истинных свойствах и параметрах КИС.

ИСЗИ, обеспечивающие обнаружения атак, в качестве интеллектуального инструмента используют нейронные сети (НС), системы нечеткой логики и основанные на правилах экспертные системы (ЭС).

В ИСЗИ ЭС в базе знаний содержат описание классификационных правил, соответствующим профилям легальных пользователей и сценариям атак на КИС. Недостатки ИСЗИ на базе ЭС: система не является адаптивной; не всегда обнаруживаются неизвестные атаки [Калач А.В., **2011].** Если НС представлена в виде отдельной 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. Одним из основных недостатков нейронной сети является "непрозрачность" формирования результатов анализа.

В системах обнаружения атак можно выделить применение нейронных сетей, дополненных ЭС. Чувствительность системы возрастает, так как экспертная система получает данные только о событиях, которые рассматриваются в качестве подозрительных. Если нейронная сеть за счет обучения стала идентифицировать новые атаки, то экспертную систему следует обновить [Калач А.В., 2011].

Использование гибридных нейро-экспертных или нейро-нечетких систем позволяет отразить в структуре системы нечеткие предикатные правила, которые автоматически корректируются в процессе обучения нейронной сети. Свойство адаптивности нечетких нейронных сетей позволяет решать отдельно взятые задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, автоматически формировать новые правила при изменении поля угроз [Калач А.В., 2011].

Недостатками этих систем являются: необходимость наличия экспертов высокой квалификации; трудности, возникающие при адаптации методов к потребностям конкретной организации; невозможность оценить эффективность конкретного комплекса средств защиты, применяемого на объекте защиты; требование наличия на предприятии достоверной статистики по инцидентам информационной безопасности.

2. Поддержка принятия решений в интеллектуальной системе защиты информации

Одна на сегодняшний день научная проблема в области построения ИСЗИ - это обеспечение интеллектуальной поддержки принятия решений (ИППР) по всему комплексу задач, решаемых ИСЗИ. В работе [Рахимов, Е. А. 2008] сделаны отдельные предложения по данной проблеме:

– предложено рассматривать множество угроз как множество каналов несанкционированного доступа, утечки информации и деструктивных воздействий (НСДУВ), реализуемых злоумышленником или нарушителем. Угроза рассматривается, с одной стороны, как сложная последовательность компонентов угроз при манипулировании злоумышленником информационными потоками, с другой - в виде графа структуризации на множестве элементов физической среды распространения носителя информации. Подход позволяет использовать как статистические оценки уровней компонентов угроз, так и экспертные оценки: уровни компонентов угроз вычисляются с использыванием аппарата нечеткой логики;

- разработана методика численной оценки уровня защищенности информации, в которой используются данные интегральной структурной вербальной модели каналов НСДУВ, позволяющая сравнивать различные комплексы средств защиты по уровню защищенности, проводить количественный анализ состояния информационной безопасности ОИ с целью выработки решений по усилению или ослаблению функций защиты.

- предложен метод синтеза рациональных наборов средств защиты, состоящих из совместимых программно-аппаратных продуктов, по целевой функции, максимизирующей отношение суммарного показателя защищенности к сумме показателей издержек, включающих стоимость, причем численные значения показателей защищенности и издержек определяются с использованием метода анализа иерархии. Метод позволяет осуществить синтез рациональных наборов средств защиты, состоящих из совместимых программно-аппаратных продуктов, с априорно заданными свойствами, удовлетворяющими требованиям к защищенности информации на ОИ.

- разработано алгоритмическое обеспечение подсистемы поддержки принятия решений (ППРР) по оперативному управлению защитой информации, позволяющее с одной стороны минимизировать влияние угроз на защищаемую информацию, с другой - уменьшить вероятность того, что ответные действия повлияют на нормальное функционирование защищаемого ОИ.

- предложена архитектура построения интеллектуальной СЗИ, позволяющей обеспечить автоматизированную поддержку принятия решений по выбору рационального ее состава и изменению его в процессе эксплуатации, по выбору варианта оперативного реагирования при возникновении потенциально опасных ситуаций в условиях неопределенности информационных воздействий.

По проблеме ИППР соедующие результаты получены в работах [Машкина И.В., 2008, 2009]:

– модель противодействия угрозам нарушения информационной безопасности, базирующихся на использовании адаптированного для выбора рационального варианта реагирования метода принятия решений, *заключается* в том, что решение о выборе варианта реагирования принимается в зависимости от вероятности атаки, которая оценивается с использованием механизма нечеткого логического вывода, на основе оперативных данных о событиях безопасности от различных обнаружителей

– метод формирования рационального комплекса средств защиты заключающийся в том,

что на основе трехрубежной модели защиты разрабатываются морфологические матрицы для каждого из рубежей, генерируются варианты наборов средств защиты с использованием вспомогательных матриц совместимости программно-аппаратных средств, разрабатывается система иерархических критериев качества средств защиты на основе их технических характеристик, выбирается рациональный вариант набора для каждого рубежа защиты по целевой функции, максимизирующей отношение суммарного показателя «защищенность информации» к суммарному показателю «издержки», в состав системы защиты информации включаются рациональные наборы, суммарная стоимость которых не превышает выделенных на защиту ресурсов, что позволяет получить комплекс средств защиты, сертифицированных по заданному классу защищенности, удовлетворяющий требованиям к допустимым затратам на его реализацию.

3. Защита информационных ресурсов предприятия на основе многоагентной технологии

В работе [Kotenko et al., 2005] предложен подход к созданию команд агентов, участвующих в информационном. Подход позволяет моделировать атаки, направленные на нарушение доступности информационных ресурсов, и механизмы защиты от них. Проведено большое количество разнообразных экспериментов, в которых исследовались параметры эффективности механизмов защиты от топологии и конфигурации сети, структуры и конфигурации команд атаки и защиты, которые показали, что использования кооперации команд защиты приводит к повышению эффективности защиты. Планируется разработка формальных моделей поведения сложных систем в Интернет, совершенствование среды моделирования, более глубокое исследование эффективности механизмов кооперации различных команд и внутрикомандного взаимодействия агентов, реализация механизмов адаптации и самообучения агентов.

В работе [Погорелов Д. Н., 2008] предложена новая концепция построения интеллектуальной системы защиты информации предприятия, основанная на сочетании принципов функциональной интеграции, иерархической организации, комплексирования моделей, методов и алгоритмов, стандартизации систем защиты информации, построения информационных систем, что позволяет обеспечить согласованную работу всех подсистем защиты информации. Это позволило построить архитектуру автоматизированной системы защиты информации, основанная на многоагентном подходе.

Для решения задачи обнаружения вирусных атак в сети Интернет предлагается архитектура на основе продукционной системы с многоуровневой вертикальной моделью агентов [Берестов А.А, 2011].

Данная архитектура включает базу знаний в виде правил продукций, механизма логического вывода, рецепторов и эффекторов 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 могут быть использованы разные типы агентов: агент-субординатор, множество агентов исполнителей, агент-интегратор. Агенты могут быть 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 проектируемая многоагентная система должна включать несколько агентов, которые выполняют в системе различные функции. В результате анализа информационного процесса обнаружения вирусных атак в сетях КИС можно рассматривать агентов, разграничивающих права доступа пользователей сети, агентов обнаружения вторжений, то есть изменения состояния окружающей среды в сети, агентов обнаружения типа атаки, агентов, строящих сценарий поведения для отражения вирусной атаки, агентов, являющийся посредником-координатором всей многоагентной системы.

В работе [Никишева А.В, 2013] **п**роанализированы основные распространяемые системы обнаружения атак (СОА): Snort, Bro, Prelude, OSSEC, Suricata и рассмотрены основные тенденции их развития. В результате этого был определен перечень критериев и их значений, которым должна удовлетворять СОА:

– многоуровневость наблюдения за системой. СОА должна собирать сведения о состоянии ИС из различных источников на различных уровнях наблюдения – уровень сети, сервера и хоста;

– адаптивность, т.е. способность СОА обнаруживать модифицированные реализации известных атак и новые виды атак.

– проактивность, СОА должна обладать встроенными механизмами реакции на атаку

– открытость, СОА должна обладать возможностью добавления новых анализируемых ресурсов информационной системы.

– тип управления. СОА должна совмещать как централизованное, так и распределенное управление.

– защищенность. СОА должна обладать средствами защиты своих компонентов.

В результате представлены следующие решения по многоагентной системе обнаружения атак на КИС:

– структура и состав многоагентной системы обнаружения атак, включающая в себя агентов рабочих станций, серверов, маршрутизаторов и сетей и позволяющая делать вывод о атаках, состоянии КИС и перспективах ее защиты;

– метод принятия агентами совместного решения, позволяющий сформировать круглый стол агентов и на основании их результатов анализа сведений, полученных из различных источников, оценить состояние КИС в целом;

– методика обнаружения атак с использованием многоагентных технологий, позволяющая обучить многоагентную систему обнаружению атак и использовать ее для дальнейшего обнаружения неизвестных воздействий.

– оценка эффективности всех предложенных методов, используя разработанные программные решения.

4. Тенденции и концепция развития

В качестве тенденций и концепции развития по использованию ИТвЗИ можно представить следующее [Машкина И.В., 2009, Вишняков В.А., 2013]:

– совершенствование архитектур систем ЗИ в КИС, обеспечивающих эффективное управление в условиях неопределенности состояния информационной среды;

– разработка новых моделей противодействия угрозам нарушения ИБ в КИС на основе выбора оптимального варианта реагирования на события безопасности;

– 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 КИС.

– разработка теоретических основ, моделей и средств защиты облачной инструментальной платформы проектирования интеллекуальных систем на основе семантических технологий.

Заключение

Первым направлением в СЗИ является дальнейшая разработка моделей, методов, архитектур и аппаратно-программных средств управления ЗИ для решения проблемы защиты КИС и облачной инструментальной платформы проектирования интеллекуальных систем на основе семантических технологий.

Другим направлением СЗИ является разработка моделей, методов, архитектур и аппаратно-программных средств сбора, структуризации информации из Интернете, формирования специализированных баз знаний и поддержки принятия решений (на базе ИТ) по всему накопленному аспекту задач ИБ.

Библиографический список

[Машкина И.В., 2008] Машкина, И.В. Идентификация угроз на основе построения семантической модели информационной системы / И.В. Машкина // Вестник УГАТУ: Науч. журн. Уфимск. гос. авиац. техн. ун-та. Сер. Управление, вычислительная техника и информатика. 2008. №11. С. 208 – 214.

[Электр. ресурс, 2013] Современные технологии обеспечения информационной безопасности. Электронный ресурс. Код доступа: http://ipb.mos.ru/ttb Время доступа 9.12.2013.

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

[Рахимов, Е. А. 2006] Рахимов, Е. А. Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации. /Е.А. Рахимов/ Автореферат канд. дисс. по спец. 05.13.19. Уфа, 2006. – С.18.

[Kotenko et al., 2005] Kotenko, I., Ulanov A. Multiagent modeling and simulation of agents' competition for network resources availability // Second International Workshop on Safety and Security in Multiagent Systems. Utrecht, The Netherlands. 2005.

[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.

[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

[Вишняков, В.А., 2013] Вишняков, В.А. Анализ методов и средств защиты информации и использование интеллектуальных агентов для ее совершенствования / В.А. Вишняков // Материалы межд. научной конференции ИСиТ. Мн.: БГУИР, 2013. – С.130-131.

STATE, TRENDS AND CONCEPTION DEVELOPMENT OF INTELLIGENCE TECHNOLOGIES IN INFORMATION DEFENSE

Vishniakou U.A.

Minsk Management Institute,
Minsk, Republic of Belarus

vish2002@list.ru

Two problems the use of intelligence technologies in information defense (ITID) – creating specialized knowledge bases with threats simulation and high the security level in corporative nets and cloud computing are presented. The analysis of two directions of the second ITID problem: the intelligence decision support systems and the malty agent system use are given. As trends and conception development of intelligence technologies are the perfection of methods. models, architectures, and hard-sotware tools for ITID in corporative systems and cloud computing.