УДК 681.5:004(07)

ВИШНЯКОВ В. А., ГОНДАЗ САЗ М. М., МОЗДУОАНИ ШИРАЗ М. Г. БГУИР,
Минский университет управления

АНАЛИЗ И КОНЦЕПЦИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИС И ОБЛАЧНОЙ ПЛАТФОРМЫ НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Представлены две проблемы использования интеллектуальных технологий в защите информации (ИТ в ЗИ) – создание специализированных БЗ с моделированием угроз и повышение уровня безопасности в корпоративных сетях и облачных вычислениях. Дан анализ направлений из второй проблемы ИТ в ЗИ: интеллектуальные поддержки принятия решений, использование многоагентных систем, элементы защиты в облачных вычислениях. В качестве тенденций развития рассмотрены совершенствования методов, моделей, архитектур, аппаратно-программных решений ИТ в ЗИ в КИС. В качестве концепции предложено развития ИТ в ЗИ для облачной инструментальной платформы проектирования интеллектуальных систем на основе семантических технологий.

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.

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 [1].

Выходом является внедрение на всех этапах защиты интеллектуальных технологий (ИТ), 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) [2].

Направления исследований ИБ на базе интеллектуальных технологий

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 на НС, последняя 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 ИСЗИ на 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 [2, 3**].**

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 [2, 3].

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 [2, 3].

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.

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 [4] 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 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;

– разработано алгоритмическое обеспечение подсистемы поддержки принятия решений (ПППР) по оперативному управлению защитой информации, позволяющее с одной стороны минимизировать влияние угроз на защища-

емую информацию, с другой – уменьшить вероятность того, что ответные действия повлияют на нормальное функционирование защищаемого объекта.

– предложена архитектура построения интеллектуальной СЗИ, позволяющей обеспечить ППР 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 следующие результаты получены в работах [1, 9]:

– модель противодействия угрозам нарушения ИБ, базирующихся на использовании адаптированного 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 трехуровневой модели защиты разрабатываются морфологические матрицы для каждого из уровней, генерируются варианты аппаратных средств, разрабатывается система иерархических критериев качества средств защиты на основе их технических характеристик, выбирается рациональный вариант набора для каждого уровня защиты по целевой функции, максимизирующей отношение суммарного показателя «защищенность информации» к суммарному показателю «издержки». В состав системы ЗИ включаются наборы, суммарная стоимость которых не превышает выделенных на защиту ресурсов.

Защита информационных ресурсов предприятия на основе многоагентной технологий. В работе [5] предложен подход к созданию команд агентов, участвующих в моделировании атак, направленных на нарушение доступности информационных ресурсов, и механизмов 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. Разрабатываются формальные модели поведения сложных систем в Интернете, совершенствование среды моделирования, более глубокое исследование эффективности механизмов кооперации команд и внутрикомандного взаимодействия агентов, реализация механизмов адаптации и самообучения агентов.

В работе [6] предложена концепция построения ИСЗИ предприятия, основанная на сочетании принципов функциональной интеграции, иерархической организации, комплексирования моделей, методов и алгоритмов, стандартизации систем ЗИ, построения информационных систем. Это позволило построить архитектуру автоматизированной системы ЗИ, основанная на многоагентном подходе.

Для решения задачи обнаружения вирусных атак в сети Интернет предлагается архитектура на основе продукционной системы с многоуровневой вертикальной моделью агентов [7]. 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 горизонтальной или вертикальной архитектуры. Для решения задачи обнаружения вирусных атак подходит вертикальная многоуровневая архитектура агентов. В результате анализа информационного процесса обнаружения вирусных атак в сетях КИС можно рассматривать агентов, разграничивающих права доступа пользователей сети, агентов обнаружения вторжений, агентов обнаружения типа атаки, агентов, строящих сценарий поведения для отражения вирусной атаки, агентов, являющийся посредником-координатором всей многоагентной системы.

В работе [8] проанализированы 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:

– СОА должна собирать сведения о состоянии ИС из различных источников на различных уровнях наблюдения: 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 [8]:

1. Структура и состав многоагентной системы обнаружения атак, включающая в себя агентов рабочих станций, серверов, маршрутизаторов и сетей и позволяющая делать вывод об атаках, состоянии КИС и перспективах ее защиты;

2. 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;

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

4. Оценка эффективности всех предложенных методов, используя разработанные программные решения.

Результаты и их обсуждение

Элементы защиты информации в облачных вычислениях. В связи с широким использованием технологий облачных вычислений (ОВ) актуальна проблема ЗИ для них. Рассмотрим отдельные результаты в этой области. В работе [10] по ЗИ в среде облачных вычислений получено:

– математическая модель представления программного обеспечения (ПО) в терминах теории графов и теории множеств, позволяющая анализировать процесс его выполнения;

– способ формального описания классифицирующего признака ПО;

– алгоритм классификации на ПО, обладающее заданным признаком и не обладающее им;

– подход к оценке подобия различных экземпляров программного обеспечения, основанный на мере Дамерау – Левенштейна;

– синтезирована методика верификации ПО на наличие деструктивных свойств для сред облачных вычислений, использующая предложенный подход к оценке подобия различных экземпляров.

В работе [11] предложена формализация и контроль информационного взаимодействия в форме виртуальных соединений с помощью межсетевых экранов. Разработанная модель учитывает динамический характер выделяемых ресурсов и структуру протоколов сетевого взаимодействия, что позволяет осуществлять разграничение доступа с учетом текущего состояния защищаемой среды. 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 каждого дана на принадлежность соединению и определения подмножества правил фильтрации для них.

Разработанный алгоритм классификации виртуальных соединений, использующий технологии организации параллельных вычислений и структуру стека TCP/IP, позволил повысить производительность межсетевых экранов и более эффективно использовать вычислительные ресурсы аппаратных платформ, что, в свою очередь, снижает потери от наличия средств разграничения доступа в среде облачных вычислений.

Резюмируя вышеизложенное, констатируем. В качестве тенденций развития интеллектуальных технологий и ИСЗИ для КИС и ОВ можно представить следующее [9, 12]:

– развитие архитектур систем ЗИ в КИС, обеспечивающих эффективное управление в ус-

ловиях неопределенности состояния информационной среды;

– разработка новых моделей противодействия угрозам нарушения ИБ в КИС на основе интеллектуального ПР по оптимальному варианту реагирования на события безопасности;

– развитие инструментальных программных комплексов с интеллектуальной ППР по выбору эффективных методов, моделей и алгоритмов в КИС и ОВ;

– развитие технологий многоагентных систем для обнаружения атак, противодействия угрозам нарушения ИБ, оценки уровня защищенности информации в КИС и ОВ.

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

Предложена концепция разработки моделей и построения средств защиты облачной инструментальной платформы проектирования интеллекуальных систем, базирующаяся с одной стороны на результатах, полученных в открытом проекте создания технологии компонентного проектирования интеллектуальных систем [13], с другой на результатах, полученных при защите в облачных вычислениях [10, 11].

Заключение

Первым направлением в ИСЗИ является дальнейшая разработка моделей, методов, архитектур и аппаратно-программных средств управления ЗИ для решения проблемы защиты КИС и облачной инструментальной платформы проектирования интеллектуальных систем на основе семантических технологий. В этом направлении очерчена концепция разработки моделей и средств защиты облачной инструментальной платформы проектирования интеллектуальных систем. Другим направлением ИСЗИ является разработка моделей, методов, архитектур и аппаратно-программных средств сбора, структуризации информации из Интернете, формирования специализированных баз знаний и поддержки принятия решений по всему накопленному аспекту задач ИБ.

Литература

1. **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.

2. Современные технологии обеспечения информационной безопасности. – [Электронный ресурс]. – Код доступа: http:// ipb. mos. ru/ttb l. – Дата доступа 9.12.2013.

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

4. **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.

5**. Kotenko, I. Multiagent** modeling and simulation of agents' competition for network resources availability / I. Kotenko, A. Ulanov // Second International Workshop on Safety and Security in Multiagent Systems. Utrecht, The Netherlands. 2005. – PP. 123–125.

6. **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.

7. 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.

8. **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.

9. **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.

10. **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, 2009. – 18 с.

11. **Лукашин, А. А.** Система защиты информационного взаимодействия в среде облачных вычислений / А. А. Лукашин // Автореферат канд. дисс. по спец. 05.13.19 СПб. 2012. – 18 с.

12. **Вишняков, В. А.** Состояние, тенденции и концепция развития интеллектуальных технологий в защите информации / В. А. Вишняков // Материалы 4 межд. науч.-технической конференции OSTIS-2014 – Минск: Изд-во БГУИР, 2014. – С. 391–394.

13. **Голенков В. В.,** Открытый проект, направленный на создание технологии компонентного проектирования интеллектуальных систем Материалы 3 межд. науч.-технической конференции OSTIS-2013 / В. В. Голенков, Н. А Гулякина // – Минск: Изд-во БГУИР, 2013. – С. 55–78.