А. В. Суханов (к. т. н.)
ЗАО «Эврика», Санкт-Петербург,
Л. Г. Нестерук (к. э. н.)
Санкт-Петербургский государственный университет экономики и финансов

К ПРОЕКТИРОВАНИЮ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье с позиций биосистемной аналогии рассмотрены методологические вопросы проектирования сложных кибернетических систем, к которым в полной мере относятся средства мониторинга безопасности информационных систем (ИС). Предложен подход к построению защищенных ИС, определяющий основные положения и методологию создания защищенных интеллектуальных ИС. Данный подход основан на аналогии архитектуры и механизмов защиты биологических систем и сложных кибернетических систем.

Применение интеллектуальных средств для целей защиты информационных систем (ИС) является характерной чертой текущего этапа эволюции информационных технологий (ИТ) [1, 2]. Основное внимание исследователей и разработчиков систем защиты направлено на обнаружение и оперативную нейтрализацию последствий сетевых атак [3—5], а также обучение в режиме онлайн интеллектуальных средств защиты для выявления несанкционированных действий в телекоммуникационных сетях и ИС [6, 7].

Актуальность проектирования защищенных ИС обусловлена высокими темпами развития, усложнением инфраструктуры и расширением функциональных возможностей ИТ. Прослеживается параллель между эволюцией видов биосистем и процессами развития современных ИТ [8]. Биосистемы развиваются благодаря совершенной защите информационных процессов, а дальнейшее развитие ИТ связано с обеспечением защищенности ИС, адекватной росту сложности информационных технологий. Перспективным методом разработки систем информационной безопасности (СИБ) является использование в искусственных системах аналогии с механизмами защиты (МЗ) информационных процессов и ресурсов, характерных для биосистем.

Статья посвящена методологическим вопросам проектирования сложных кибернетических систем, поставленным с позиции биосистемной аналогии [9]. Предложено осуществлять проектирование ИС и средств обеспечения безопасности ИС как единый процесс построения иерархической адаптивной системы с внутренне присущим свойством «защищенность». Процесс проектирования предполагается начинать с выбора надежной элементной базы, соответствующей требованиям функциональной устойчивости, алгоритмической универсальности и защищенности. Согласно принципу биосистемной аналогии с уровня элементной базы следует применять дублирование и избыточное кодирование информации, что свойственно элементному базису нейронных сетей (НС).

По аналогии с биосистемами при проектировании ИС следует осуществлять программную настройку нейросетевых базовых блоков, в процессе которой:

· в базовых блоках формируется набор взаимосвязанных интерфейсом функциональных устройств (аналогов органов), оговоренных в спецификации на проектирование и выполненных на основе формальных нейронов (аналогов клеток) (ФН);

· обмен информацией между функциональными устройствами организуется через интерфейс в виде закодированных сообщений;

· в процессе создания устройств в базовых блоках формируются адаптивные информационные поля НС, соответствующие функциям отдельных устройств ИС и интеллектуальных средств защиты;

· интеллектуальные средства защиты имеют иерархическую структуру;

· иммунная защита нижнего иерархического уровня осуществляет проверку сообщений, передаваемых по интерфейсу, по критерию «свой — чужой»;

· защита верхнего иерархического уровня служит для накопления опыта нейтрализации механизмами защиты множества известных угроз.

Функциональная ориентация устройств производится настройкой межнейронных связей НС, записью в локальную память базовых блоков системной информации в виде адаптивных информационных полей НС; функции хранения системной информации (долговременная память), обработки и записи/считывания данных (оперативная память) должны быть разнесены для исключения несанкционированного изменения системной информации.

В процессе эксплуатации могут изменяться в режиме адаптации как функции отдельных устройств, так и ИС в целом:

· добавление функции в информационную систему производится аналогично процедуре формирования дополнительного устройства;

· изменение имеющихся функций связано с коррекцией в долговременной памяти системной информации соответствующего устройства, т.е. адаптацией информационного поля конкретной НС;

· адаптация информационных полей НС ассоциируется с процессом роста биосистемы, так как при изменении или добавлении функции информационной системы могут выделяться дополнительные ФН и происходить их интеграция в систему; при этом наблюдается естественное сочетание свойств стабильности (сохранение информации) и пластичности (настройка параметров ФН).

Функции защиты ИС реализуются описанным выше образом и корректируются в режиме адаптации НС при изменении множества угроз и наличии дестабилизирующих воздействий.

Основы методологии построения адаптивных средств защиты информации

Методология построения адаптивных средств защиты базируется на эволюционных свойствах нейронных сетей, связанных с адаптивностью, самообучением, возможностью представления опыта экспертов информационной безопасности (ИБ) в виде системы предикатных правил.

В процессе функционирования интеллектуальных средств защиты должна быть отражена последовательность выполнения следующих основных операций:

1) *классификация* угроз информационным ресурсам ИС — соотнесение выявленной угрозы со множеством известных угроз информационной безопасности (нижний уровень иерархии средств защиты);

2) *кластеризация* угроз информационным ресурсам ИС как саморазвитие классификации при расширении множества угроз;

3) описание в виде *системы предикатных правил* соотношений «угрозы — механизмы защиты» (верхний уровень иерархии средств защиты);

4) реализация системы предикатных правил в виде специализированной нейросетевой структуры,;

5) *адаптация* информационных полей НС (соответственно, и системы предикатных правил);

6) *анализ* структуры межнейронных связей информационных полей НС и «*прозрачной*» системы предикатных правил для выявления наиболее используемых МЗ;

7) *формулирование* новых правил для *формирования* спецификации на разработку отсутствующих в ИС механизмов защиты.

Системный подход к моделированию интеллектуальных средств защиты обуславливает методологию, которой необходимо руководствоваться при разработке кибернетических систем. Базовыми принципами системного подхода являются [10]: целеобусловленность, относительность, управляемость, связность и моделируемость.

Моделируемость служит основным средством разработки и верификации, позволяющим предотвратить ошибки проектирования кибернетических систем, к которым относятся системы защиты. В соответствии с принципом *связности* при разработке эффективной средств защиты ИС целесообразно рассматривать объект защиты комплексно, как составную часть сложной кибернетической системы, объединяющей в единой модели объект защиты, среду, средства защиты и угрозы злоумышленника как взаимосвязанные элементы [11].

Динамика множества угроз в процессе эксплуатации защищаемой ИС проявляется через новые уязвимости, не отраженные в исходной модели, и возникает потенциальная возможность реализации новых угроз безопасности информационным ресурсам и процессам. В связи с этим целесообразно рассматривать модель средств защиты в динамике, начиная с начального этапа жизненного цикла системы, а нейросетевые средства, обладающие свойствами адаптивности и самообучения, — в качестве базы для построения защищенных ИС.

Динамичный характер множества угроз выдвигает свойство *адаптивности* в разряд первоочередных качеств, необходимых средствам защиты. Не менее важным качеством является возможность реализации в ИС *накопленного опыта* нейтрализации угроз в информационных полях НС. Свойство *адаптивности* позволяет при ограниченных затратах на организацию средств защиты обеспечить заданный уровень безопасности ИС за счет оперативной реакции на изменение множества угроз.

Опыт средств защиты может храниться и передаваться в поколениях (модификация ИС) в виде распределенных адаптивных информационных полей: поля *известных угроз* на нижнем, иммунном уровне и поля *жизненного опыта* на верхнем, рецепторном уровне средств защиты (рис. 1).

Процесс адаптации поля известных угроз связан с решением задач классификации, кластеризации. Изменение множества известных угроз отражается на верхнем уровне средств защиты в соответствующей модификации информационного поля жизненного опыта, реализованного в виде специализированной нейросетевой структуры, которая, в свою очередь, описывается системой предикатных правил. Процесс адаптации поля жизненного опыта связан с обучением НС, которое адекватно видоизменяет систему предикатных правил, ставящую в соответствие известным угрозам механизмы защиты.

Анализ взаимосвязанных пар «угроза — уязвимость» позволяет поставить в соответствие каждой угрозе, оговоренной в спецификации на проектирование защищаемой ИС, уязвимости ИС. Экономически целесообразно закрыть механизмами защиты все выявленные уязвимости системы, а изменение множества угроз — сопровождать процессом адаптации информационных полей известных угроз и жизненного опыта средств защиты.

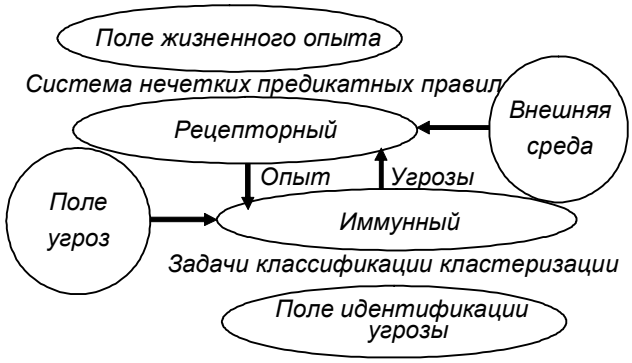

Рис. 1. Иерархия уровней интеллектуальных средств защиты

Если в качестве базовой выбрать одну из многоуровневых моделей СИБ [12, 13], то вначале модель будет содержать минимальное количество МЗ, достаточное для защиты выявленных уязвимостей ИС, которые будут пополняться при расширении множества угроз.

Методика проектирования адаптивных средств защиты информации

Пусть информационное поле нижнего уровня средств защиты обучено на всем поле известных угроз, т.е. возможна идентификация каждой из известных угроз, и нейросетевые средства защиты находятся в режиме работы. Пусть заданным угрозам x_i, $i=\overline{1, N}$ в процессе проектирования системы поставлены в соответствие выявленные уязвимости v_j, $j=\overline{1, J}$ и назначены МЗ z_k, $k=\overline{1, K}$. Механизмы

защиты будем подразделять на активированные, потенциальные (известные, но еще не активированные МЗ) и отсутствующие (недоступные для использования в данной ИС). Без потери общности изложения ограничим поле угроз поступлением в систему «чужих» сообщений x_ρ, $\rho=\overline{1, P}$, где $P \geq N$.

1. При поступлении в интерфейс системы «чужого» сообщения x_ρ информационным полем нижнего уровня средств защиты будет идентифицирована угроза, если она принадлежит множеству известных угроз $\{x_\rho, \rho=\overline{1, P}\}$.

2. Если выявленная угроза соответствует подмножеству заданных угроз $\{x_i, i=\overline{1, N}\}$, то «чужое» сообщение изымается из процесса обработки и фиксируется статистика активации в информационных системах данной угрозы.

3. Если же выявленная в процессе классификации угроза не из подмножества $\{x_i, i=\overline{1, N}\}$, то выполняются действия по п. 2 и перестройка средств защиты. Под контролем администратора безопасности системы осуществляются перевод в режим адаптации и обучение НС иммунного уровня, соотнесение новой угрозы с выявленными или потенциальными уязвимостями, перевод в режим адаптации и обучение НС верхнего уровня для нейтрализации ранее неспецифицированной угрозы x_ρ имеющимися МЗ из множества $\{z_k\}$.

4. Если невозможна нейтрализация выявленной угрозы имеющимися МЗ, необходимо расширение множества $\{z_k\}$ за счет активации адекватных угрозе механизмов защиты. При этом происходит коррекция многоуровневой модели средств защиты путем активации ряда потенциальных механизмов защиты информации и обучения НС верхнего уровня.

5. Если исчерпаны потенциальные МЗ и не получено соотнесение угрозы со средствами для ее нейтрализации, то под контролем администратора безопасности системы выполняются перевод нейросетевых средств защиты верхнего уровня в режим адаптации, расширение информационного поля НС верхнего уровня (введение дополнительного ФН) и обучение НС для нейтрализации ранее неспецифицированной угрозы x_ρ *отсутствующими* МЗ информации. В последнем случае анализ обученной НС верхнего уровня позволяет сформулировать *систему требований* к отсутствующим в системе МЗ.

Перестройка многоуровневой модели средств защиты может быть реализована с привлечением механизма нечеткого логического вывода и архитектурных решений нейро-нечетких сетей и сетей адаптивного резонанса [14—16].

Механизмы реализации адаптивных свойств средств защиты информации

Основными механизмами реализации *адаптивных свойств* средств защиты следует считать: способность распределенного информационного поля НС к *накоплению знаний* в процессе обучения; механизм *логического вывода*, который позволяет представить опыт экспертов в области защиты информации в виде системы предикатных правил и использовать его для *предварительного обучения* НС; способность нейросетевых средств к *классификации и кластеризации*.

Логический вывод. Нечеткое отношение $R=A\rightarrow B$ отражает знания эксперта $A\rightarrow B$ в виде причинного отношения посылки (угрозы) и заключения (механизма защиты), где операция $\rightarrow$ соответствует нечеткой импликации. Отношение R можно рассматривать как нечеткое подмножество прямого произведения $X\times Y$ полного множества угроз X и механизмов защиты Y, а процесс получения нечеткого результата вывода B' по посылке A' и знаниям $A\rightarrow B$ — в виде композиционного правила: $A'=B'\bullet R=A'\bullet(A\rightarrow B)$, где $\bullet$ — операция, например, max-min-композиции.

Механизм логического вывода основан на базе знаний, формируемой специалистами предметной области в виде системы предикатных правил вида:

$П_1$: если x есть A_1, то y есть B_1,
$П_2$: если x есть A_2, то y есть B_2,
...
$П_n$: если x есть A_n, то y есть B_n,

где x и y, соответственно, входная переменная (например, угроза) и переменная вывода (к примеру, механизм защиты), а A_i и B_i — функции принадлежности непрерывных переменных (НП).

Логический вывод, как правило, включает следующие этапы [15]:

1) *введение нечеткости*: по функциям принадлежности, заданным на области определения входных НП, исходя из фактических значений НП, назначается степень истинности каждой угрозы для каждого правила;

2) *логический вывод*: по степени истинности угроз формируются заключения по каждому из правил, образующие нечеткое подмножество для каждого МЗ;

3) *композиция*: нечеткие подмножества для каждого МЗ объединяются с целью формирования нечеткого подмножества для всех МЗ (по всем правилам);

4) *приведение к четкости*: сводится к преобразованию нечеткого набора выводов по всем правилам в четкое значение итоговой защищенности системы.

Нейросетевая классификация и кластеризация в адаптивных средствах защиты могут быть реализованы с использованием нечетких НС или НС адаптивного резонанса [16, 17].

Нейро-нечеткие сети (рис. 2) [18] используют механизм нечеткого логического вывода и базу знаний, формируемую экспертами ИБ, в виде системы правил:

Π_1: если $\tilde{x}_1$ есть A_{11} и ... $\tilde{x}_n$ есть A_{1n}, то $\tilde{y} = B_2$,

Π_2: если $\tilde{x}_1$ есть A_{21} и ... $\tilde{x}_n$ есть A_{2n}, то $\tilde{y} = B_2$,

...

Π_k: если $\tilde{x}_1$ есть A_{k1} и ... $\tilde{x}_n$ есть A_{kn}, то $\tilde{y} = B_k$,

где $\tilde{x}$ и $\tilde{y}$ — нечеткие входная переменная и переменная вывода, а A_{ij} *и* B_i, $i=\overline{1,k}$, $j=\overline{1,n}$ — соответствующие функции принадлежности.

При реализации системы предикатных правил в топологии нейро-нечеткой сети находят отражение следующие этапы нечеткого логического вывода:

· *введение нечеткости* — по функциям принадлежности, заданным на области определения посылок, исходя из фактических значений нечетких переменных $\tilde{x}_i$, определять степень истинности каждой посылки;

· *логический вывод* — по степени истинности посылок формировать заключения по каждому из правил, образующие нечеткое подмножество для каждой переменной вывода по каждому из правил;

· *композиция* — полученные на предыдущем этапе нечеткие подмножества для каждой переменной вывода по всем правилам объединять с целью формирования нечеткого подмножества для всех переменных вывода.

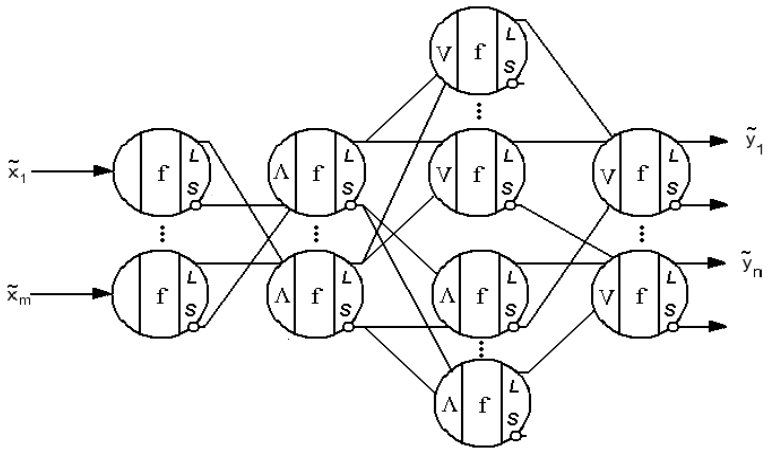

Рис. 2. Нейро-нечеткий классификатор

Сети теории адаптивного резонанса (Adaptive Resonance Theory Network, ART) [16] применяются для кластеризации многомерных векторов. Сети ART имеют множество модификаций, но интерес для дальнейших исследований представляет Cascade ARTMAP (рис. 3) [19], которая позволяет включать в информационное поле ART-сети априорное знание, представленное в виде системы предикатных правил.

Наличие исходной базы знаний не только позволяет повысить эффективность обучения НС, но и дополнить информационное поле НС знаниями, отсутствующими в обучающих примерах. Причем неполные или частично достоверные правила могут быть откорректированы нейронной сетью в процессе обучения.

Используя алгоритм извлечения правил, информационное поле обученной НС может быть преобразовано обратно в систему предикатных правил, что позволяет сравнить исходные правила и модифицированную сетью базу знаний. Результаты экспериментов показали, что априорное знание увеличивает точность классификации, особенно при ограниченном наборе обучающих примеров [19].

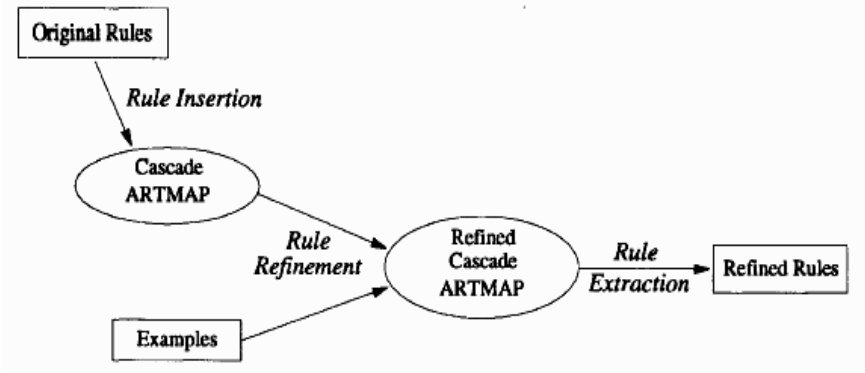

Рис. 3. Cascade ARTMAP, использующая априорные знания

Накопление опыта в интеллектуальных средствах защиты происходит в информационных полях НС в процессе обучения.

Изначально в средствах защиты формируется система предикатных правил для всех известных МЗ $\{z_k,\ k=\overline{1,\ K}\}$, так же как и нейросетевые средства идентификации угроз обучены на всем поле известных угроз $\{x_\rho,\ \rho=\overline{1,\ P}\}$. Незаданным угрозам во входном векторе x соответствуют нулевые значения координат, а деактивированным МЗ — близкие к 0 значения степени использования данного механизма защиты в формировании значения итоговой защищенности системы.

Задавая пороговые значения для величин $z_k,\ k=\overline{1,\ K}$, можно определять как наименее задействованные, так и наиболее эффективно используемые механизмы в обеспечении безопасности защищаемой системы.

После активации всех потенциальных механизмов защиты информации и введения дополнительных ФН в последний скрытый слой НС, соответствующий размерности вектора известных механизмов защиты, происходит *расширение системы предикатных правил*. Таким образом, средства защиты самостоятельно формируют правило, описывающее отсутствующий МЗ в защищаемой ИС. При последующей адаптации произойдет обучение нейронных сетей под отсутствующий МЗ, направленный на нейтрализацию ранее не специфицированной угрозы x_ρ. Анализ дополнительного предикатного правила позволяет сформировать спецификацию на проектирование отсутствующего в системе механизма защиты.

СПИСОК ЛИТЕРАТУРЫ

1. *Гриняев С. Н.* Интеллектуальное противодействие информационному оружию. М.: СИНТЕГ, 1999.
2. *Tambe M., Рynadath D. V.* Towards Heterogeneous Agent Teams // Lecture Notes in Artificial Intelligence. V. 2086, Springer Verlag, 2001.

3. *Бочков М. В.* Реализация методов обнаружения программных атак и противодействия программному подавлению в компьютерных сетях на основе нейронных сетей и генетических алгоритмов оптимизации // Сб. докл. VI Международной конф. SCM'2003. СПб.: СПГЭТУ, 2003. Т. 1. С. 376–378.
4. *Норткатт С.* Анализ типовых нарушений безопасности в сетях. М.: Издательский дом «Вильямс», 2001.
5. *Noureldien A. N.* Protecting Web Servers from DoS/DDoS Flooding Attacks. A Technical Overview. International Conference on Web-Management for International Organisations. Proceedings. Geneva, October, 2002.
6. *Городецкий В. И., Карсаев О. В., Котенко И. В.* Программный прототип многоагентной системы обнаружения вторжений в компьютерные сети // Труды конгресса «Искусственный интеллект в XXI веке». ICAI'2001. Т. 1. М.: Физматлит, 2001.
7. *Городецкий В. И., Котенко И. В.* Командная работа агентов-хакеров: применение многоагентной технологии для моделирования распределенных атак на компьютерные сети // Труды VIII конф. по искусственному интеллекту. КИИ-2002. М.: Физматлит, 2002.
8. *Осовецкий Л. Г.* Научно-технические предпосылки роста роли защиты информации в современных информационных технологиях // Изв. вузов. Приборостроение. 2003. Т. 46. № 7. С. 5–18.
9. *Осовецкий Л. Г., Нестерук Г. Ф., Бормотов В. М.* К вопросу иммунологии сложных информационных систем // Изв. вузов. Приборостроение. 2003. Т. 46. № 7. С. 34–40.
10. *Красносельский Н. И. Ворон-цов Ю. А., Аппак М. А.* Автоматизированные системы управления в связи: Учебник для вузов. М.: Радио и связь, 1988.
11. *Вихорев С. В., Кобцев Р. Ю.* Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент. 2002. № 2.
12. *Осовецкий Л., Шевченко В.* Оценка защищенности сетей и систем // Экспресс электроника. 2002. № 2–3. С. 20–24.
13. *Мельников В. В.* Защита информации в компьютерных системах. М.: Финансы и статистика: Электронинформ, 1997.
14. *Fuller R.* Neural Fuzzy Systems. Abo: Abo Akademi University, 1995.
15. *Круглов В. В., Борисов В. В.* Искусственные нейронные сети. Теория и практика. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2002.
16. *Carpenter G.A., Grossberg S., Markuzon N., Reynolds J. H., Rosen D. B.* Fuzzy ARTMAP: An adaptive resonance architecture for incremental learning of analog maps. // Proc. of the International Joint Conference on Neural Network. 1992.
17. *Negnevitsky M.* Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.
18. *Нестерук Ф. Г., Молдовян А. А., Нестерук Г. Ф., Нестерук Л. Г.* Квазилогические нейронечеткие сети для решения задач классификации в системах защиты информации // Вопросы защиты информации. 2007. № 1. С. 23–31.