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

МОНИТОРИНГ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МОДЕЛИ АДАПТИВНОЙ ЗАЩИТЫ

Для построения перспективных информационных систем (ИС), прежде всего глобальных компьютерных систем, ориентированных на критические сферы применения, такие как институты государственной власти, финансовые структуры, предприятия ВПК, необходимы эволюционирующие адаптивные средства мониторинга безопасности в составе ИС. Рассматриваются архитектурные решения средств интеллектуальной защиты ИС и основы методологии мониторинга безопасности ИС, ориентированные на принцип биосистемной аналогии.

Актуальность принципа биосистемной аналогии в современных информационных технологиях (ИТ) обусловлена высокой защищенностью жизненно важных информационных процессов в биосистемах. Необходим анализ механизмов защиты биосистем и разработка основ методологии мониторинга ИС на основе биосистемной аналогии.

В качестве информационной среды существующие ИС, как правило, используют глобальные телекоммуникационные сети (например, Интернет), объединяющие информационные сети локального и корпоративного уровней [1, 2]. Аналогия в архитектуре ИС наиболее полно проявляется в наличии иерархической организации уровней глобальных информационных сред.

Биосистемная аналогия в структуре защиты ИС базируется на иерархии средств обеспечения информационной безопасности (ИБ), встроенных механизмах иммунной защиты и информационно-полевой форме накопления опыта.

Известные средства защиты, как правило, ограничиваются реализацией функций нижнего уровня системы информационной безопасности (СИБ) и антивирусной направленностью средств иммунной защиты. Согласно [3], около 70 % вирусных атак осуществляются извне через точку входа в защищаемую сеть и только около 30 % изнутри. Первые можно отнести к внешним угрозам жизнеобеспечению системы, вторые — ко внутренним. В обоих случаях задействуется иерархия механизмов иммунной защиты: первый уровень — почтовых шлюзов и межсетевых экранов, следующий — серверный уровень (файл-серверы, серверы групповой работы и пр.) и третий уровень — рабочих станций (Рис. 1).

Реализация идеи иммунной защиты [3] связана со следующим процессом: обнаружение в ИС признаков заражения, отправление образца нового вируса в антивирусный центр, получение, спустя некоторое время, обновления антивирусной базы, которое распространяют по корпоративной сети прежде, чем успеет распространиться вирус.

Названный подход входит в противоречие с принципом биосистемной аналогии, в частности с *внутрисистемной* реализацией иммунной защиты, так как в рассмотренной системе антивирусной защиты (в отличие от биосистемы) большая часть механизмов иммунной защиты находится в антивирусном центре, расположенном за пределами корпоративной сети.

Размещение антивирусного центра *вне* защищаемой ИС позволяет злоумышленникам: 1) под видом обновления антивирусной базы сформировать канал для загрузки вирусов и троянских коней, 2) в случае автоматической отправки на анализ подозреваемых на наличие вируса файлов получить доступ к конфиденциальной информации.

Время реакции подобной иммунной защиты измеряется часами [3], что неприемлемо для большинства критических приложений ИС и ограничивает сферу применения подхода только задачами восстановления корпоративной сети (аналог процесса реанимации больного биологического организма).

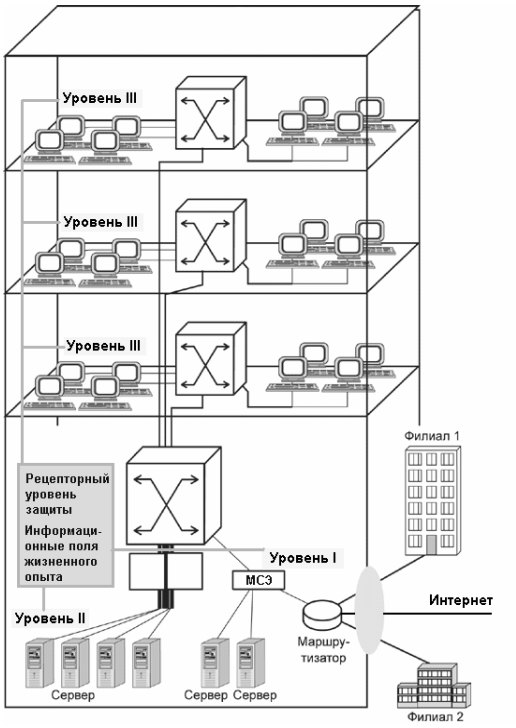

Рис. 1. Уровни защиты в корпоративной сети

В биосистемах функции иммунной защиты реализуются через *внутренние* механизмы *оперативной реакции* на угрозы и дестабилизирующие воздействия, распределенные по уровням *иерархии* средств защиты, — *долговременные процессы* накопления жизненного опыта, носящие эволюционный характер [4, 5].

Биосистемная аналогия в *эволюционных процессах* основана на реализации в ИС совокупности механизмов наследования, развития, адаптации и отбора, свойственных биосистемам, в то время как при построении перспективных средств защиты основное внимание уделяют лишь свойству адаптивности разрабатываемых интеллектуальных средств выявления атак и несанкционированных информационных процессов в корпоративной сети [6–8].

Средства защиты уровня почтовых шлюзов и межсетевых экранов в большей мере ориентированы на выявление внешних атак, а средства защиты серверного уровня — на нейтрализацию внутренних угроз в корпоративной системе (Рис. 1). Известные интеллектуальные средства защиты, как правило, реализуют только механизмы *оперативной реакции* и нейтрализации угроз, практически не уделяя внимания координирующей роли, которую играет нервная система — верхний уровень иерархии защиты биологических систем в реализации эволюционного процесса накопления жизненного опыта системы (*долговременного запоминания* системной информации). В биосистемах имеют место процессы постепенной адаптации иерархической системы жизнеобеспечения и защиты с использованием всего арсенала средств эволюционных процессов.

В ИС помимо иммунного уровня средств защиты необходима *иерархия уровней защиты*, и прежде всего наличие верхних уровней защиты (например, рецепторного уровня защиты), выполняющих функции нервной системы биологического организма по накоплению жизненного опыта, координации и установлению ассоциативных (долговременных) связей между процессами, происходящими на нижних

уровнях средств защиты, — атаками и изменением множества угроз. Т. е. необходим иерархический уровень накопления жизненного опыта по нейтрализации атак, представленного в форме *структурированных информационных полей*, удобных для наследования в последующих реализациях системы.

Биосистемная аналогия в *представлении информации* в форме структурированного информационного поля нейросетевых систем (НС) позволяет решить комплекс задач повышения информационной безопасности ИС за счет распределенного избыточного представления знаний, избыточного *пространственного представления* информационных процессов, функционально устойчивой параллельной обработки данных при распределенной реализации программируемых информационных процессов.

Биосистемная аналогия в *программировании* ИС реализуется путем формирования и коррекции распределенных избыточных информационных полей НС, относящихся к иерархической модели средств защиты. Структурированная программа, подобно потоковым машинам [9] описывающая топологию взаимосвязанных компонентов, обеспечивает:

– универсальный характер описания взаимосвязи множества известных угроз и используемых механизмов защиты (МЗ) в виде системы предикатных правил и информационных полей НС,

– автоматическую коррекцию информационных полей НС в процессе адаптации ИС к изменению множества угроз или условий эксплуатации,

– наследование опыта по нейтрализации угроз путем переноса структурированных информационных полей НС в последующие модификации ИС.

Основы методологии мониторинга безопасности ИС

Метод проектирования адаптивных средств защиты ИС базируется на основных свойствах НС и нечетких систем, связанных с адаптивностью, возможностью представления опыта специалистов ИБ в виде системы нечетких правил.

Возможность *обучения* рассматривается как одно из наиболее важных качеств нейросетевых систем, которое позволяет адаптироваться к изменению входной информации. Обучающим фактором являются избыточность информации и скрытые в данных закономерности, которые видоизменяют информационное поле НС в процессе адаптации. НС, уменьшая степень избыточности входной информации, позволяет выделять в данных *существенные признаки*, а соревновательные методы обучения — классифицировать поступающую информацию за счет *механизма кластеризации*: подобные векторы входных данных груп-пируются нейронной сетью в отдельный кластер и представляются конкретным формальным нейроном — ФН-прототипом. НС, осуществляя кластеризацию данных, находит такие усредненные по кластеру значения функциональных параметров ФН-прототипов, которые минимизируют ошибку представления сгруппированных в кластер данных.

Согласно подходу проектирования адаптивных средств защиты необходимы:

1) формирование матриц *адаптируемых экспертных оценок* и на их основе создание исходных *систем нечетких правил* и *классификаторов* (на нижних уровнях защиты — классификаторов «признаки атаки — угрозы», на верхних уровнях защиты — классификаторов «угрозы—МЗ»);

2) *идентификация* выявленной *угрозы* и при расширении множества известных угроз — *кластеризация угроз* с последующей адаптацией информационных полей путем обучения НС уровней защиты;

3) *кластеризация* вследствие изменения множества угроз сопровождается *коррекцией* или *расширением системы нечетких правил*;

4) *изменение множества угроз* вызывает *коррекцию систем нечетких правил* и матриц *экспертных оценок* в результате обучения иерархии классификаторов;

5) при расширении системы нечетких правил формируется *описание* нового (отсутствующего) *механизма защиты*;

6) «прозрачность» системы нечетких правил позволяет сформулировать *спецификацию на создание* отсутствующего МЗ;

7) на основании анализа комплекса оценок защищенности ИС (в случае экономической целесообразности) включают новый МЗ в состав средств защиты.

Таким образом, мониторинг безопасности ИС на базе адаптивной модели мониторинга безопасности ИС включает этапы [10]:

1) формирование *структурной модели* СИБ в виде иерархии уровней механизмов защиты в соответствии с техническим заданием на проектирование средств мониторинга безопасности ИС;

2) решение задачи *классификации* угроз по вектору признаков атак и механизмов защиты по вектору угроз; производится соотнесение *посылок* (на нижних уровнях защиты — нечеткого вектора признаков атак, на верхних уровнях защиты — нечеткого вектора угроз) с классификационными *заключениями* (на нижних уровнях — выявленными угрозами, на верхних уровнях — механизмами защиты, необходимыми для нейтрализации множества известных угроз);

3) формирование матриц *экспертных оценок* для определения степени соответствия на нижних уровнях защиты — угроз признакам атаки и на верхних уровнях защиты — механизмов защиты полю угроз;

4) представление в виде *систем нечетких правил* результатов п. 1 и 3, полученных в процессе нечеткого логического вывода классификационных заключений по нечетким посылкам (на нижних уровнях защиты — соотношения «признаки атаки — угрозы», на верхних уровнях защиты — соотношения «угрозы—МЗ»);

5) реализация систем нечетких правил в виде специализированных нейросетевых структур (на нижних уровнях защиты — классификаторов «признаки атаки — угрозы», на верхних уровнях защиты — классификаторов «угрозы—МЗ»);

6) решение задачи *кластеризации* угроз по признакам атак и МЗ по вектору угроз как саморазвитие классификации при расширении множества угроз; производится разбиение входных векторов на группы (на нижних уровнях защиты — векторов признаков атак, на верхних уровнях защиты — векторов угроз) и отнесение вновь поступающего входного вектора к одной из групп либо формирование новой группы (на нижних уровнях — группы угроз, на верхних уровнях — группы механизмов защиты, необходимых для нейтрализации множества известных угроз);

7) реализация результатов п. 2 в виде *четких классификаторов* на основе самообучающейся НС (на нижних уровнях защиты — классификаторов «признаки атаки — угрозы», на верхних уровнях защиты — классификаторов «угрозы—МЗ»);

8) *наследование опыта* адаптивных средств защиты по обеспечению ИБ, приобретенного в процессе эксплуатации подобной ИС, в проектируемые средства защиты путем перенесения информационных полей четких и нейро-нечетких классификаторов (на нижних уровнях защиты — классификаторов «признаки атаки — угрозы», на верхних уровнях защиты — классификаторов «угрозы—МЗ»);

9) *обучение классификаторов* по п. 5, 6 на обучающей выборке — подмножестве входных векторов (на нижних уровнях защиты — векторов признаков атак, на верхних уровнях защиты — векторов угроз) с целью формирования информационных полей четких и нейро-нечетких классификаторов;

10) *адаптация* в процессе эксплуатации ИС *информационных полей* четких и нейро-нечетких классификаторов (на нижних уровнях защиты — классификаторов «признаки атаки — угрозы», на верхних уровнях — классификаторов «угрозы—МЗ»);

11) *коррекция* адаптируемых матриц *экспертных оценок* (п. 3) и систем *нечетких правил* (п. 4) по результатам адаптации;

12) *формулирование новых* нечетких *правил* в случае расширения классификации по результатам п. 2 и 9 (на нижних уровнях защиты — классификации «признаки атаки — угрозы», на верхних уровнях — классификации «угрозы—МЗ»);

13) *формирование* комплекса *оценок защищенности* ИС исходя из результатов п. 10 и распределения механизмов защиты по иерархии средств защиты;

14) *анализ структуры связей* нейро-нечетких классификаторов, «прозрачной» *системы нечетких правил* и комплекса *оценок защищенности* по п. 12 для выявления наиболее используемых или отсутствующих в ИС механизмов защиты;

15) *формирование спецификации* на разработку отсутствующих МЗ;

16) *коррекция структуры* системы информационной безопасности за счет расширения перечня используемых МЗ и их размещения в иерархии средств адаптивной защиты.

Модель адаптивной защиты и этапы жизненного цикла ИС

Целью этапов проектирования с учетом жизненного цикла ИС является формирование корректной (без несанкционированных возможностей) безопасной ИС. На начальном этапе жизненного цикла в соответствии с требованиями спецификации на проектирование ИС осуществляется формирование ИС и средств защиты с заданной совокупностью свойств.

Для реализации функции средств защиты, соответствующих системе нечетких предикатных правил (например, для классификации механизмов защиты), формируются адаптивные информационные поля адаптивных уровней защиты прикладной ИС. Производится предэксплуатационное обучение нейро-нечетких классификаторов и нейросетевых кластеризаторов с применением корректных алгоритмов, т. е. выполняется адаптация информационных полей НС под задачи информационной защиты.

Процессы настройки (обучения) производятся в режиме адаптации системы при непосредственном участии и под контролем доверенных лиц, в частности администратора ИС. Процесс настройки завершается блокировкой режима адаптации и переводом сформированной системы в режим работы.

Многоуровневая модель информационной безопасности системы на первом этапе соответствует минимальной активации потенциальных механизмов защиты и полноте информационного множества известных угроз.

Целью этапа эксплуатации жизненного цикла системы является корректное исполнение системой заданных функций. Основной режим — работа. Предусмотрен режим адаптации функций системы защиты информации, который использует механизм адаптации для реагирования на изменение внешних факторов — происходит дальнейший рост, самообучение системы и изменение информационных полей средств защиты. Как и на предыдущем этапе, процессы коррекции функций средств защиты производятся в режиме адаптации системы при непосредственном участии администратора ИС. Процесс настройки завершается блокировкой режима адаптации и переводом системы в режим работы.

Многоуровневая модель средств адаптивной защиты на втором этапе динамически пополняется путем перевода механизмов защиты из статуса «потенциальный» в статус «активированный» и привязки активированного механизма к соответствующему эшелону модели средств защиты. Увеличивается число элементов в подмножестве заданных угроз как за счет включения элементов из множества известных угроз, так и за счет пополнения самого множества известных угроз ранее неизвестными угрозами. В последнем случае возможно расширение множества потенциальных механизмов защиты за счет описания в виде нечетких предикатных правил и последующей реализации ранее отсутствующих МЗ.

Целью этапа вывода системы из эксплуатации является постепенное сворачивание прикладных функций системы при корректной работе средств защиты и сохранении основных системных функций.

Многоуровневая модель информационной безопасности ИС достигает максимального насыщения как механизмами защиты, так и полнотой информационного поля известных угроз. Накопленный опыт средств защиты подлежит анализу и использованию (наследованию) в создаваемых прикладных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. *Минаев В. А.* Перспективы развития IT-security в России // Межотраслевой тематический каталог «Системы безопасности-2003». 2003. С. 218–221.
2. *Олифер В. Г., Олифер Н. А.* Основы сетей передачи данных. Интернет-университет информационных технологий – ИНТУИТ.ру. 2003. – 248 с. (www.INTUIT.ru).
3. *Касперски К.* Атака на Windows NT // LAN / Журнал сетевых решений. Вкладка «Обзор антивирусных средств от AIDSTEST до информационной иммунной системы». Декабрь 2000. С. 88–95.
4. *Яковлев Н. Н.* Жизнь и среда: Молекулярные и функциональные основы приспособления организма к условиям среды. Л., 1986.
5. *Мелик-Гайназян И. В.* Информационные процессы и реальность. М., 1998. –192 с.
6. *Корнеев В. В., Маслович А. И. и др.* Распознавание программных модулей и обнаружение несанкционированных действий с применением аппарата нейросетей // Информационные технологии. 1997. № 10.
7. *Котенко И. В.* Модели противоборства команд агентов по реализации и защите от распределенных атак «Отказ в обслуживании» // Труды междунар. конф. IEEE AIS'03 и CAD-2003. М., 2003. Т. I. С. 422–428.
8. *Гриняев С. Н.* Интеллектуальное противодействие информационному оружию. М., 1999.
9. *Mayers G. J.* Advances in computer architecture. 2nd edition. JONH WILLEY & SONS, 1982.
10. *Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г.* О применении нейро-нечетких сетей в адаптивных системах информационной защиты // Нейроинформатика-2005: Материалы VII Всерос. научно-техн. конф. М., 2005. Ч. 1. С. 163–171.