УДК 681.3.06:519.248.681

А. В. СНЕГУРОВ, канд. техн. наук

РЕФЛЕКСИВНАЯ МОДЕЛЬ ВЫБОРА СРЕДСТВ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Введение

К критическим следует отнести информационные системы (ИС) финансовых организаций, системы управления жизнеобеспечением населенных пунктов, системы управления гражданской авиации, телекоммуникационные системы, системы управления стратегически важными объектами и другие [1]. Выход из строя (снижение качества функционирования) таких систем может привести к значительным потерям.

Сбой в работе таких систем может происходить как вследствие ошибок, заложенных при проектировании, так и вследствие преднамеренных и непреднамеренных воздействий на систему в ходе ее эксплуатации. Объективным фактором функционирования современных информационных систем является наличие деструктивных воздействий (ДВ) на их элементы.

Критические информационные системы можно рассматривать как совокупность трех системно-информационных компонентов: структуры (способа внутренней организации элементов и связей), алгоритмов (реализующих функции обработки информации), языка представления и взаимодействия элементов. Тогда средства деструктивного воздействия на информационную систему можно объединить в три соответствующие группы, такие как: средства и способы воздействия на структуру информационных систем; средства и способы воздействия на алгоритмы функционирования систем; средства и способы дезинформации и дезориентации информационных систем. То есть, к деструктивным воздействиям могут относиться такие действия, которые направлены на вывод из контура функционирования (управления) различных элементов системы (или снижение эффективности их функционирования до минимально критического значения), изменение алгоритма функционирования системы (вплоть до срыва его выполнения), уничтожение или искажение информации, циркулирующей в системе. Причем ДВ могут воздействовать комплексно на ИС – вывод из строя элемента системы ведет к изменению алгоритма ее функционирования и т.д.

Особенностью защиты ИС от преднамеренных ДВ является неопределенность относительно вида воздействия, времени воздействия, нападающей стороны. Осуществление таких деструктивных воздействий может подчиняться некоторым принципам. К ним можно отнести внезапность и активность воздействия (для этого нападающая сторона может заблаговременно изучить слабые и уязвимые стороны ИС, оценить способы защиты, выбрать наиболее эффективные свои действия), комплексность воздействия (воздействие на разные подсистемы, воздействие разными способами, согласование данных воздействий по времени).

Деструктивное воздействие может быть осуществлено в наиболее неблагоприятный для ИС временной промежуток: ночь, выходные, периоды наибольшей нагрузки на ИС, периоды времени, когда ИС решает важнейшие задачи. Нападающей стороной может быть как одиночка-хакер, так и организация, оснащенная эффективными средствами ДВ.

Вопросам выбора средств защиты информационных систем от деструктивных воздействий посвящено ряд научных работ [2 – 6 и др.]. Однако актуальной задачей остается поиск методов и методик выбора эффективных вариантов защиты критически важных информационных систем в условиях конфликтного взаимодействия.

Цель статьи – разработка математического аппарата выбора вариантов защиты критически важных информационных систем с использованием рефлексивной модели прогнозирования действий нападающей стороны.

Решение поставленной задачи

При рассмотрении конфликта «система защиты информационной системы» – «нападающая сторона» в вышеуказанных условиях в статье предлагается использовать гео-

рию рефлексии, основные положения которой для систем управления были разработаны В. Е. Ярушеком.

С точки зрения теории рефлексии поведение нападающей и защищающейся сторон может быть охарактеризовано несколькими моделями:

1) Рефлексия нулевого уровня.

Нападающая сторона определяет множество уязвимых элементов ИС $\left\{ {}^{нс}_{ис}y_i \right\}_{i=1}^{I}$. Зная свои возможности по нападению (множество средств деструктивного воздействия $\left\{ {}^{нс}_{ис}ДВ_j \right\}_{j=1}^{J}$) формирует матрицу ${}^{нс}_{ис}\mu_{ij}$, $i=\overline{1,I}, j=\overline{1,J}$, ${}^{нс}_{ис}\mu_{ij}=[0,1]$, которая определяет степень эффективности j-го деструктивного воздействия на i-й уязвимый элемент. Выбирает подмножество $\left\{ {}^{нс}_{ис}ДВ_h \right\}_{h=1}^{H}$ наиболее эффективных (целесообразных) средств деструктивного воздействия и способ их реализации $S_{нап}=f\left({}^{нс}_{ис}\mu_{ij}^{R}, \left\{ {}^{нс}_{ис}ДВ_h \right\}_{h=1}^{H} \right)$.

В свою очередь, система защиты ИС оценивает множество уязвимых элементов защищаемой ИС $\left\{ {}^{ис}y_k \right\}_{k=1}^{K}$, множество возможных угроз (деструктивных воздействий) $\left\{ {}^{ис}_{нс}ДВ_n \right\}_{n=1}^{N}$, где ${}^{ис}_{нс}\mu_{kn}$, $k=\overline{1,K}, n=\overline{1,N}$ – степень «опасности» n-го деструктивного воздействия для k – го уязвимого элемента, ${}^{ис}_{нс}\mu_{kn}=[0,1]$, на основании множества имеющихся средств защиты $\left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G}$ выбирается наиболее эффективные средства защиты и вариант их применения $S_{защ}=f\left({}^{ис}_{нс}\mu_{kn}, \left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G} \right)$.

2) Рефлексия первого уровня.

Помимо действий, соответствующих нулевому уровню рефлексии, нападающая сторона вырабатывает свое понимание того, как система защиты видит варианты нападения. То есть нападающая сторона формирует (прогнозирует) множество $\left(\left\{ {}^{ис}_{нс}ДВ_n \right\}_{n=1}^{N} \right)^{*}$, матрицу показателей $\left({}^{ис}_{нс}\mu_{kn} \right)^{*}$ и критерии выбора варианта нападения.

При выборе модели поведения рефлексии первого уровня система защиты ИС должна выработать понимание того, как нападающая сторона оценивает варианты защиты уязвимых элементов ИС. То есть формируется множество $\left(\left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G} \right)^{*}$, оценивается матрица показателей $\left({}^{ис}_{нс}\mu_{kn} \right)^{*}$, определяется – как нападающая сторона видит критерии выбора варианта защиты.

Множества $\left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G}$ и $\left(\left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G} \right)^*$ могут не совпадать. Точно также могут не совпадать множества $\left\{ {}^{ис}_{нс}ДВ_n \right\}_{n=1}^{N}$ и $\left(\left\{ {}^{ис}_{нс}ДВ_n \right\}_{n=1}^{N} \right)^*$. Все зависит от эффективности аналитической работы нападающей стороны и системы защиты ИС, наличия информации о противоборствующей стороне. Кроме того, могут проводиться обеими сторонами конфликта мероприятия по введению противоборствующей стороны в заблуждение путем как скрытия тех или иных действий, так и навязывания ложной информации.

При принятии противоборствующими сторонами модели поведения рефлексии более высоких уровней процесс принятия решения существенно усложняется. Необходимо отметить, что как нападающая сторона, так и система защиты ИС могут выбрать разные уровни рефлексии в зависимости от степени их развитости. Преимущество в конфликте имеет та сторона, которая выбирает более высокий уровень рефлексии. Уровни рефлексии от третьего и выше не используются вследствие сложности их реализации.

Выбор варианта защиты критически важной информационной системы в данных условиях может быть следующим.

Пусть имеется множество уязвимых элементов территориально сосредоточенного объекта информационной системы $\left\{ {}^{ис}У_k \right\}_{k=1}^{K}$. К уязвимому элементу можно, например, отнести персональные ЭВМ, объединенные беспроводной сетью (Wi-Fi) и находящиеся в отдельном здании. Существует множество средств деструктивного воздействия, которые может применить нападающая сторона $\left\{ {}^{ис}_{нс}ДВ_n \right\}_{n=1}^{N}$. К ним можно отнести атаки на сеть с использованием программных средств, использование постановщиков радиопомех в диапазоне частот Wi-Fi, использование генераторов мощных электромагнитных импульсов для вывода из строя электроники и другие. Каждое из данных средств деструктивного воздействия имеет свою эффективность, ряд средств имеет ограниченную дальность действия. Имеется множество средств защиты, которые система защиты может использовать $\left\{ {}^{ис}_{нс}З_g \right\}_{g=1}^{G}$. Каждое из данных средств также имеет свою эффективность по защите от конкретного деструктивного воздействия.

Построим матрицу R нечеткого бинарного отношения:

$$R = \begin{vmatrix} {}^{ис}_{нс}\mu^{дв}_{11} & {}^{ис}_{нс}\mu^{дв}_{12} & \cdots & {}^{ис}_{нс}\mu^{дв}_{1n} \\ {}^{ис}_{нс}\mu^{дв}_{21} & {}^{ис}_{нс}\mu^{дв}_{22} & \cdots & {}^{ис}_{нс}\mu^{дв}_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ {}^{ис}_{нс}\mu^{дв}_{k1} & {}^{ис}_{нс}\mu^{дв}_{k2} & \cdots & {}^{ис}_{нс}\mu^{дв}_{kn} \end{vmatrix},$$

где ${}^{ис}_{нс}\mu^{дв}_{kn}$, $k = \overline{1,K}, n = \overline{1,N}$, ${}^{ис}_{нс}\mu^{дв}_{kn} = [0,1]$. – нечеткая степень возможности применения n-го типа деструктивного воздействия на k-й уязвимый элемент информационной системы. Данный показатель позволяет учесть выбор системой защиты рефлексивной модели поведения нулевого или первого уровня. Так при принятии модели рефлексии первого уровня система защиты ИС должна выработать понимание того, как нападающая система прогнозирует

варианты защиты и выбирает перечень средств нападения. Здесь может быть осуществлен учет того, что нападающая сторона может выбрать неординарный способ нападения.

В качестве примера можно привести ситуацию, когда вокруг уязвимого элемента ИС есть охраняемая зона, которая, с точки зрения системы защиты, исключает применение генератора мощного электромагнитного импульса. При этом уязвимый элемент ИС может быть просто не защищен другими способами от данного вида деструктивного воздействия. Нападающая сторона, просчитав такой вариант защиты, может принять решение о внесении генератора электромагнитного импульса в охраняемую зону (например, путем подкупа охраны или другим способом).

Учет эффективности средств защиты осуществляется путем построения матрицы W нечеткого бинарного отношения

$$W = \begin{vmatrix} {}^{ис}_{нс}\mu^{з}_{11} & {}^{ис}_{нс}\mu^{з}_{12} & \cdots & {}^{ис}_{нс}\mu^{з}_{1g} \\ {}^{ис}_{нс}\mu^{з}_{21} & {}^{ис}_{нс}\mu^{з}_{22} & \cdots & {}^{ис}_{нс}\mu^{з}_{2g} \\ \cdots & \cdots & \cdots & \cdots \\ {}^{ис}_{нс}\mu^{з}_{n1} & {}^{ис}_{нс}\mu^{з}_{2} & \cdots & {}^{ис}_{нс}\mu^{з}_{ng} \end{vmatrix},$$

где ${}^{ис}_{нс}\mu^{з}_{ng}$, $n = \overline{1,N}, g = \overline{1,G}$, ${}^{ис}_{нс}\mu^{з}_{ng} = [0,1]$ – степень эффективности g -го средства защиты от n-го средства деструктивного воздействия. Для тех средств защиты, которые не предназначены для защиты от определенных средств деструктивного воздействия (как, например, экранирование помещения не может защитить от программных средств воздействия), данный показатель приравнивается нулю.

Из матриц R и W формируется матрица T:

$$T = \begin{vmatrix} {}^{ис}_{нс}\mu^{уэ\_з}_{11} & {}^{ис}_{нс}\mu^{уэ\_з}_{12} & \cdots & {}^{ис}_{нс}\mu^{уэ\_з}_{1g} \\ {}^{ис}_{нс}\mu^{уэ\_з}_{21} & {}^{ис}_{нс}\mu^{уэ\_з}_{22} & \cdots & {}^{ис}_{нс}\mu^{уэ\_з}_{2g} \\ \cdots & \cdots & \cdots & \cdots \\ {}^{ис}_{нс}\mu^{уэ\_з}_{k1} & {}^{ис}_{нс}\mu^{уэ\_з}_{k2} & \cdots & {}^{ис}_{нс}\mu^{уэ\_з}_{kg} \end{vmatrix},$$

элементы которой определяются функцией принадлежности:

$${}^{ис}_{нс}\mu^{уэ\_з}_{kg} = \frac{\sum_{n=1}^{N} {}^{ис}_{нс}\mu^{дв}_{kn} \cdot {}^{ис}_{нс}\mu^{з}_{ng}}{\sum_{n=1}^{N} {}^{ис}_{нс}\mu^{дв}_{kn}}, \text{ для всех } k = \overline{1,K}, g = \overline{1,G}. \qquad (1)$$

Данный показатель определяет эффективность защиты k-го уязвимого элемента каждым из имеющихся средств защиты с учетом возможности применения тех или иных средств деструктивного воздействия.

Выбор перечня средств защиты для каждого k-го уязвимого элемента может заключаться в определении порогового значения показателя ${}^{ис}_{нс}\mu^{уэ\_з}_{kg}$, при превышении которого средст-

во защиты включается в перечень рекомендованных для использования. Как вариант определения данного порогового значения может использоваться следующий [7]:

$$L = \min_{g,g+1} \max_{k} \min \left[\mu_{\substack{ис \\ нс}}^{уэ\_з}{}_{kg}, \mu_{\substack{ис \\ нс}}^{уэ\_з}{}_{k(g+1)} \right]. \quad (2)$$

Механизм выбора перечня средств защиты может выглядеть следующим образом:

$$M_k = \left\{ k / \mu_{\substack{ис \\ нс}}^{уэ\_з}{}_{kg} \right\} \geq \min_{g,g+1} \max_{k} \min \left[\mu_{\substack{ис \\ нс}}^{уэ\_з}{}_{kg}, \mu_{\substack{ис \\ нс}}^{уэ\_з}{}_{k(g+1)} \right], \text{ для всех } k = \overline{1,K}. \quad (3)$$

В соответствии с выражением (3) для каждого k-го уязвимого элемента ИС выбирается множество средств защиты с учетом возможности применения нападающей стороной каждого из существующих средств деструктивного воздействия и эффективности использования выбираемых средств защиты.

Выводы

Данный подход к определению множества средств защиты критически важной информационной системы позволяет учесть возможность выбора нападающей стороной ассиметричного варианта нападения, являющегося наиболее опасным из-за неготовности к нему системы защиты.

Список литературы: 1. *Петренко С. С., Беляев А. В.* Проблема обнаружения компьютерных атак в критически важных инфраструктурах // Защита информации. INSIDE, № 2. 2008. С. 32-36. 2. *Мистратов Л. Е.* Метод оценки эффективности применения комплексов информационной индивидуальной и групповой безопасности организационно-технических систем в конфликтной неопределенности. // Информационные технологии. 2008. № 5. С. 26-30. 3. *Машкина И. В., Васильев В. И.* Подход к разработке интеллектуальной системы защиты информации // Информационные технологии. 2007. № 6. С. 2-6. 4. *Душкин А. В.* Распознавание и оценка угроз несанкционированного воздействия на защищенные информационно-телекоммуникационные системы // Информационные технологии. 2008. № 3. С. 71-75. 5. *Балашов П. А., Кисилов Р. И., Безгузиков В. П.* Оценка рисков информационной безопасности на основе нечеткой логики // Защита информации. Конфидент. 2003. № 4. С. 56-59; 2003. №5. С. 60-65. 6. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения. К.: МК-Пресс, 2006. 320 с. 7. *Нечеткие* множества и теория возможностей. Последние достижения: Пер. с англ./ Под ред. Р. Р. Ягера. М.: Радио и связь, 1986. 408 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 04.11.2008