УДК 004.036

В. А. ЛАХНО (УКРАИНА)

О ПОСТРОЕНИИ ДИСКРЕТНЫХ ПРОЦЕДУР РАСПОЗНАВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ДАННЫХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Предлагаемый в работе системный подход к решению задач информационной безопасности (ИБ), предусматривающий интеграцию математических моделей обработки и защиты информации, соединяет неуязвимость и гибкость по каждому из трех аспектов защищенности (конфиденциальность, доступность и целостность) информации на основе конструктивной унификации указанных противоречий. Разработан метод моделирования политики безопасности (ПБ) для обеспечения высоконадежной обработки информации (ВНОИ), отличающийся использованием нового проблемно-ориентированного теоретико-графового аппарата эталонной модели защищенной автоматизированной системы обработки данных критического применения (АСОД КП) для соединения гибкости дискреционной модели с принципиальной безопасностью моделей конечных состояний ПБ. В статье предложен новый подход к конструированию дискретных процедур распознавания угроз информационной АСОД КП. Предложенные процедуры могут быть использованы при создании комплексов систем защиты информации предприятий и компаний.

Ключевые слова: информационная безопасность; автоматизированная система обработки данных; угроза; информационная атака.

The system approach to solving problems of information security, proposed in this work provides for the integration of mathematical models of the processing and protection of information, connecting invulnerability and flexibility for each of three aspects of security (confidentiality, availability and integrity) of information based on structural unification of these contradictions. The article discusses the use of discrete procedures to detect threats for information resources. The method for modeling the security policy (SP) to provide a highly reliable information processing (HRIP) that differs by using a new problem-based graph-theoretic unit of standard model of the protected automated system for connection flexibility the discretionary model with the principled security of models of the final states of the SP has been developed. Analysis of existing methods of HRIP modeling that affect the security of information conducted in this research has revealed the impossibility of ensuring for the level of models of invulnerability of processing technology and information transfer using flexible protective mechanisms, due to the lack of integration of mathematical models of the processing and protection of information.

Key words: information security; automated control systems; threat; information attack.

Постановка проблемы

Сложившийся подход к обеспечению ИБ поддерживается на международном уровне стандартом ISO/IEC 15408. Согласно этому подходу надежный информационный процесс (ИП) успешно противодействует заданным угрозам защищенности при заданных внешних условиях его функционирования [1–3].

Целью исследований, результаты которых изложены в данной статье, является разработка теоретических основ моделирования процессов ВНОИ, обеспечивающей как недопущение ее уязвимости угрозами различных классов непреднамеренного и преднамеренного характера, так и гибкость защитных механизмов за счет интеграции математических моделей обработки и защиты информации.

Данная цель потребовала решения следующих задач:

- разработки аппарата конструирования дискретных процедур распознавания угроз (ДПРУ) ИБ для АСОД КП;
- разработки метода моделирования ПБ с учетом классов угроз ИБ для обеспечения ВНОИ.

Методы исследований

Обозначим через *MI* общее число угроз информации; *PA* – число возможных целей нарушителя в защищаемой АСОД КП; B_{p_a} – множество номеров угроз информации, реализуемых нарушителем при достижении p_a-й цели.

Обеспечение конфиденциальности моделируется как выполнение комплекса ПБ на эталонной модели защищенной автоматизированной системы (ЭМЗАС) или на ее определенном блоке (модуле).

Состав ЭМЗАС, для которой предлагаются ДПРУ ИБ, задается следующим образом: L – число уровней ЭМЗАС (обычно L = 13), $k=\overline{1,L}$, $l=\overline{1,L}$, $k\neq l$; S – множество состояний АСОД КП, $S = Q \cup P \neq \varnothing$, $Q \cap P = \varnothing$, $|S|<\infty$, $|Q|=|P|$; Q, P – множества простых и разрешающих состояний, $|Q|<\infty$, $|P|<\infty$, $Q=\bigcup_{l=1}^{L} Q_l \neq \varnothing$, $Q_k \cap Q_l = \varnothing$, $P=\bigcup_{l=1}^{L} P_l \neq \varnothing$, $P_k \cap P_l = \varnothing$; Q_l, P_l – множества простых и разрешающих состояний l-го уровня, $|Q_l|=|P_l|\neq 0$; U – множество модулей ЭМЗАС, $U=\bigcup_{l=1}^{L} U_l \neq \varnothing$, $|U|<\infty$, $U_k \cap U_l = \varnothing$; U_l – множество модулей l-го уровня; $I(u)=i_1.i_2....i_{L-l}$ – индекс модуля $u\in U_l$ и блока, у которого этот модуль верхний (№ 0 в блоке), в частности $I(u)=0$ при $l=L$; $K[I]$ – число нижних модулей в блоке с индексом I; $I.j$ – индекс нижнего модуля с номером $j=\overline{1,K[I]}$ в блоке с индексом I; если I, J – индексы модулей, то $(J\subset I)\Leftrightarrow(I\supset J)\Leftrightarrow(I=J.i_1.i_2....i_k)$, $(J\subseteq I)\Leftrightarrow(I\supseteq J)\Leftrightarrow((J\subset I)\vee(I=J))$.

Формальное представление модуля ЭМЗАС заданной структуры имеет вид [1, 4]

$$u=\langle I, q=q[I,\lambda],\ p=p[I,\lambda]\rangle\in U_l,$$

где $I=I(u)$ – индекс модуля; $q=q[I,\lambda]\in Q_l$, $p=p[I,\alpha]\in P_l$, $\lambda=\overline{1,N}$ – номер авторизации.

Формальное представление структуры ЭМЗАС следующее [1, 2]:

$$\varepsilon=\langle N, K=K[I], r=r[I,\lambda], M_{\text{in}}=M_{\text{in}}[I,\lambda], M_{\text{out}}=M_{\text{out}}[I,\lambda]\rangle,$$

где $M_{\text{in}}=M_{\text{in}}[I,\lambda]$, $M_{\text{out}}=M_{\text{out}}[I,\lambda]$ – входная и выходная функции разметки, определяющие маркировку входных и выходных позиций модулей ЭМЗАС.

Далее рассмотрим глобальную, локальную, дискреционную и блочную ПБ для модулей ЭМЗАС соответственно – ГПБ, ЛПБ, ДПБ, БПБ.

ГПБ (g) и ДПБ l-го уровня задаются множеством разрешенных ими позиций: $\Psi_g\subseteq P_l$; $\Psi_{dl}\subseteq P_l$, а уровневая ЛПБ (l) имеет вид

$$\Psi_{ll}=\left\{\langle I(u),\lambda,r[I(u),\lambda]\rangle \middle| u\in U_l,\lambda=\overline{1,N}\right\},$$

где N – число номеров авторизации, $\lambda=\overline{1,N}$ – номер авторизации; $r=r[I,\lambda]$ – булевый признак допустимости авторизации λ в модуле с индексом I.

БПБ (b) задается установкой признаков допустимости всевозможных авторизаций во всех модулях данного блока (модуля), согласованной по следующим правилам ($\lambda=\overline{1,N}$, $I=I(u)$, $u\in U\setminus U_1$):

$$\left(\exists_j\in\overline{1,K[I]}\right)\left(r[I.j,\lambda]=1\right)\Rightarrow\left(r[I,\lambda]=1\right);$$

$$\left(r[I,\lambda]=0\right)\Rightarrow\left(\forall_j\in\overline{1,K[I]}\right)\left(r[I.j,\lambda]=0\right).$$

ЛПБ задается следующим образом:

$$\Psi_1=\bigcup_{l=1}^{L}\Psi_{ll}=\left\{\langle I(u),\lambda,r[I(u),\lambda]\rangle \middle| u\in U,\lambda=\overline{1,N}\right\},$$

где $r[I(u),\lambda]$ – взаимно согласованы по всем блокам в соответствии с правилами $\left(\lambda=\overline{1,N}, I-I(u)\right)$:

$$\left(r[I,\lambda]=1\right)\Rightarrow\left(\forall J\subset I\right)\left(r[J,\lambda]=1\right), u\in U\setminus U_L;$$

$$\left(r[I,\lambda]=0\right)\Rightarrow\left(\forall J\supset I\right)\left(r[J,\lambda]=0\right), u\in U\setminus U_1.$$

ДПБ задается своим разрешающим $\Psi_{\partial p}$ либо глобализованным $\Psi_{\partial g}$ представлением

$$\left(p[I,\lambda]\in\Psi_{\partial g}\right)\Leftrightarrow\left(\left(p[I,\lambda]\in\Psi_{\partial p}\right)\wedge\left(\forall J\supset I\right)\left(p[J,\lambda]\notin\Psi_{\partial p}\right)\right);$$

$$\Psi_{\partial p}=\bigcup_{l=1}^{L}\Psi_{\partial l}\subseteq P,\ \Psi_{\partial g}\subseteq\Psi_{\partial p},\ \lambda=\overline{1,N},\ I=I(u),\ u\in U,$$

причем множества $\Psi_{\partial l}$ согласованы по правилам $\left(\lambda=\overline{1,N}\right)$:

$$\left(p[I,\lambda]\in\Psi_{\partial p}\right)\Rightarrow\left(\forall J\subset I\right)\left(p[J,\lambda]\in\Psi_{\partial p}\right),\ I=I(u),\ u\in U\setminus U_L;$$

$$\left(p[I,\lambda]\notin\Psi_{\partial p}\right)\Rightarrow\left(\forall J\supset I\right)\left(p[J,\lambda]\notin\Psi_{\partial p}\right),\ I=I(u),\ u\in U\setminus U_1.$$

Активация уровней ДПБ, ГПБ означает, что $\Psi_g = \Psi_{\partial g}$, а ЛПБ, ДПБ –

$$\left(\forall p = p\left[I,\lambda\right] \in P\right)\left(\left(p \in \Psi_{\partial p}\right) \Leftrightarrow \left(r\left[I,\lambda\right] = 1\right)\right).$$

Стандартная постановка задачи распознавания угроз для АСОД КП заключается в следующем [5–7]. Изучается некоторое множество объектов, в нашем случае это *PA* – число возможных целей нарушителя. Объекты данного множества описываются системой признаков $\{p_{ax1}, ..., p_{axn}\}$. Известно, что множество *PA* представимо в виде объединения непересекающихся подмножеств (классов) угроз информации – $(KL_1, ..., KL_l) = (B_{p_{a1}}, ..., B_{p_{al}})$. Имеется конечный набор объектов $\{sp_{a1}, ..., sp_{am}\}$ из *PA*, о которых известно, к каким классам они принадлежат (это прецеденты, т. е. объекты, используемые для обучения (ОИО)). Требуется по предъявленному набору значений признаков, т. е. описанию некоторого объекта sp_{an} из *PA*, о котором, вообще говоря, неизвестно, к какому классу угроз ИБ он принадлежит, определить этот класс и соответственно выстроить работу систем защиты информации (СЗИ) таким образом, чтобы она могла эффективно противодействовать угрозе в рамках данного класса.

При построении ДПРУ ИБ вводится понятие элементарного классификатора [5, 6], под которым понимается фрагмент описания объекта, используемого для обучения. Для каждого класса угроз ИБ $\left(KL_1, ..., KL_l\right) = \left(B_{p_{a1}}, ..., B_{p_{al}}\right)$ строится некоторое множество элементарных классификаторов с заранее заданными свойствами. Простейшим примером корректного алгоритма является следующий. Распознаваемый объект sp_{an}, например из информационного или программного массива АСОД КП, сравнивается с каждым из ОИО $\{sp_{a1}, ..., sp_{am}\}$. В случае, если описание объекта sp_{an} совпадает с описанием ОИО объекта sp_{ai}, объект sp_{an} относится к тому классу, которому принадлежит объект sp_{ai}, в противном случае алгоритм отказывается от распознавания. Данный алгоритм является корректным, однако он не сможет распознать ни один объект sp_{ai}, характеристика которого не совпадает с описанием ни одного из ОИО.

Модель уязвимостей для АСОД КП можно представить в следующем виде:

$$S_R = \left(EUM^*, SDN, RDN \cup ADN \cup MIF, IR\right),$$

где EUM^* – множество сущностей, в состав которого входит: подмножество узлов АСОД КП – um^*, потенциально содержащих уязвимости; *SDN* – множество субъектов АСОД КП; *RDN* – множество ребер графа состояний АСОД КП S_R, в том числе соответствующих правам доступа пользователей к EUM^*; *ADN* – множество ребер графа состояний системы S_R, соответствующих полученному доступу к EUM^*; *MIF* – множество ребер графа состояний системы S_R, соответствующих информационным потокам между EUM^* $\left(um^* \subset EUM^*\right)$; *IR* – функция иерархии EUM^*.

Таким образом, принципиальная схема построения алгоритмов вычисления оценок (АВО) для СЗИ будет следующая. В системе признаков $\left\{p_{a_1}, ..., p_{a_{jMI}}\right\}$ выделяется совокупность различных подмножеств вида $NP_{p_a} = \left\{p_{aj_1}, ..., p_{a_{MI}}\right\}$, $r_{p_a} \le MI$. В дальнейшем выделенные подмножества называются опорными множествами алгоритма, а их совокупность обозначается через ΩMI.

Далее зададим следующие параметры: po_{sp_a} – параметр, характеризующий значимость цели (объекта ИП) sp_{ai}, $i = 1, 2, ..., PA$; $po_{NP_{pa}}$ – параметр, характеризующий значимость объекта опорного множества $NP_{p_a} \in \Omega MI$; $MC^{AL}\left(KL\right)$ – множество элементарных классификаторов угроз для ИП АСОД КП.

Далее проводится процедура вычисления оценок. Распознаваемый объект ИП sp_{an} сравнивается с каждым ОИО sp_{ai} по каждому опорному множеству.

Для каждого класса уязвимостей АСОД КП *KL*, $KL \in \left\{KL_1, ..., KL_l\right\}$, вычисляется оценка принадлежности $\Gamma\left(sp_a, KL\right)$ объекта sp_a классу *KL*, которая имеет вид

$$\Gamma\left(sp_a, KL\right) = \frac{1}{|LW_{KL}|} \sum_{sp_{ai} \in KL} \sum_{NP_{pa} \in \Omega MI} po_{sp_a} \cdot po_{NP_{pa}} \cdot BN\left(sp_a, sp_{ai}, NP_{p_a}\right),$$

где $|LW_{KL}| = |KL \cap \left\{sp_{a1}, ..., sp_{aMI}\right\}|$.

В качестве информативной значимости признака p_{axj} для выбранных ГПБ, ЛПБ, ДПБ, БПБ будем рассматривать величину

$$IZ_{p_{axj}} = \frac{\sum\limits_{\substack{\left(sp'_a, NP_{pa}\right) \in MC^{AL}(KL) \\ p_{axj} \in NP_{pa}}} \mathrm{vop}_{\left(sp'_a, NP_{pa}\right)}}{\sum\limits_{\substack{\left(sp'_a, NP_{pa}\right) \in MC^{AL}(KL) \\ p_{axj} \in NP_{pa}}} \mathrm{vop}_{\left(sp'_a, NP_{pa}\right)}},$$

где $\mathrm{vop}_{\left(sp'_a, NP_{pa}\right)}$ – функция значимости элементарного классификатора.

Объект sp_{an} относится к тому классу, который имеет наибольшую оценку.

Распознавание объекта sp_{an} осуществляется на основе вычисления величины $BN\left(\sigma_{DOP}, sp_a, NP_{pa}\right)$ для каждого элемента $\left(\sigma_{DOP}, NP_{pa}\right)$ множества $MC^{AL}(KL), KL \in \left\{KL_1, ..., KL_l\right\}$, т. е. по каждому элементу множества $MC^{AL}\left(KL\right)$ осуществляется процедура вычисления оценки $\Gamma\left(sp_a, KL\right)$ принадлежности объекта sp_a классу KL. Таким образом, каждый распознающий алгоритм AL из рассматриваемого семейства определяется множеством элементарных классификаторов $MC^{AL}\left(KL\right)$ и способом вычисления оценки $\Gamma\left(sp_a, KL\right)$.

Предложенная математическая модель конструирования дискретных процедур распознавания с использованием аппарата логических функций была реализована в среде MATLAB 7.

Для каждого класса угроз ИБ обучающие выборки состояли из 10–95 объектов $\left(sp_{an}\right)$, разбитых на 22 класса (таблица).

Для каждого класса количество признаков варьировалось от 3 до 9. Информативность признака изменялась в диапазоне от –1 до +1. Для оценки эффективности процедур распознавания использовался метод скользящего контроля.

Возможные каналы утечки информации при реализации бизнес-процессов в компаниях

№ п/п	Возможные каналы утечки и потери информации
1	За счет структурного звука в стенах и перекрытиях офисов
2	Производственные и технологические отходы
3	По цепям заземления
4	По сети вентиляции, отопления, газо- и водоснабжения, электропитания
5	Радиозакладки или диктофон в стенах и мебели офиса компании
6	Лазерный съем акустической информации с окон офиса
7	По охранно-пожарной сигнализации
8	Дистанционный съем видеоинформации (оптика)
9	Хищение носителей информации
10	Внутренние каналы (через персонал)
11	Несанкционированное копирование
12	За счет побочного излучения терминала автоматизированного рабочего места (АРМ)
13	Съем информации с клавиатуры, принтера, сканера и т. п.
14	Съем информации с дисплея по электромагнитному каналу
15	Визуальный съем информации с дисплея и принтера или бумажных носителей
16	Через сетевые коммуникации и линии связи
17	Съем информации с использованием видеозакладок
18	По трансляционной сети и громкоговорящей связи
19	Съем информации с принтера, USB-накопителя, плохо очищенных дисков и т. п.
20	Компьютерные вирусы и т. п.
21	Программно-аппаратные закладки
22	Другие каналы

Основные результаты, полученные в ходе моделирования информативности значений признаков попыток несанкционированного доступа (НСД) к информационным ресурсам АСОД КП, представлены на рис. 1, 2.

Диаграммы показывают распределение весов значений признаков. Из рис. 2 видно, что объекты из разных классов угроз ИБ трудно отделимы друг от друга, что и является причиной низкой эффективности классического алгоритма распознавания. Также видно, что в задаче анализа информационных атак на АСОД КП часть значений признаков имеют вес, близкий к нулю, но при этом много таких значений, которые обладают довольно большим весом, т. е. очень типичны для одного из классов.

Для повышения эффективности ДПРУ ИБ был предложен критерий оценки качества функционирования сервиса контроля целостности (КЦ) как объекта управления – адекватность функционирования АСОД КП – E_{af}.

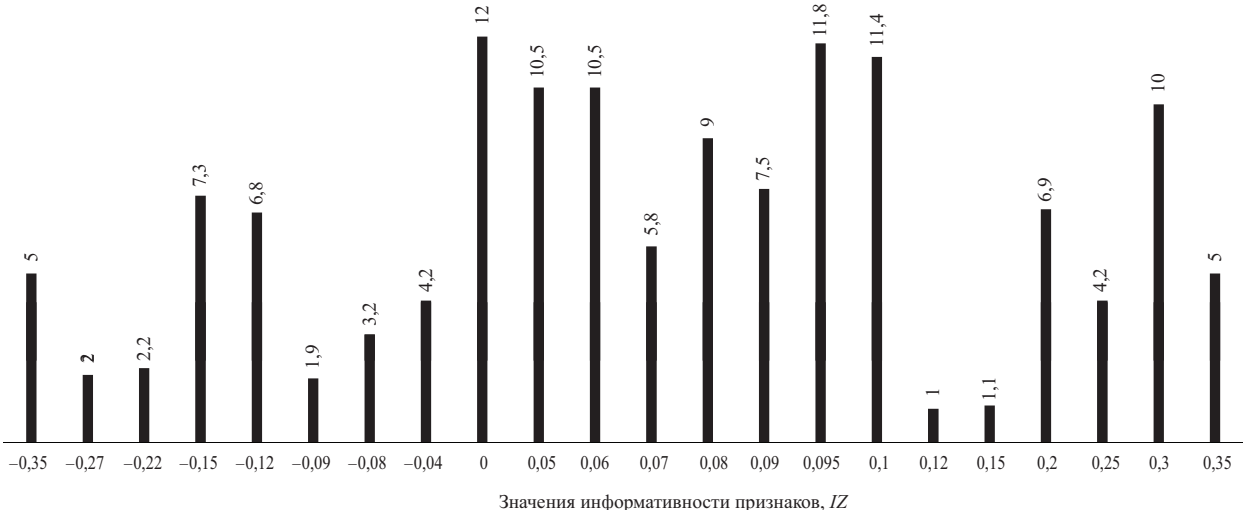

Рис. 1. Распределение типичности значений информативности признаков для возможных каналов утечки информации, %

Рис. 2. Распределение типичности значений информативности признаков для задачи компьютерной атаки, %

С помощью разработанного пакета программ [4] проведено комплексное исследование возможности применения ДПРУ ИБ и качества функционирования типовой СЗИ от НСД в условиях информационной атаки применительно к функционированию АРМ на базе ЭВМ в составе АСОД КП. Итоги этих исследований изложены в работах [4, 5].

Результаты и их обсуждение

При решении задач распознавания угроз ИБ для АСОД КП с использованием представительных наборов пришлось отказаться от требования тупиковости представительного набора, так как проверка тупиковости значительно снижает скорость работы алгоритма. Для анализа использовались представительные наборы, имеющие ограниченную длину. Максимальная длина набора бралась равной 3. При меньшей максимальной длине большая часть объектов не содержала ни одного представительного набора. А рост максимальной длины до 4 резко увеличивал время работы алгоритма. Был получен следующий результат. Если расположить признаки класса в порядке убывания информативности, то, как правило, в каждом классе есть выделенная группа признаков с большой информативностью, далее идет некоторый разрыв и потом оставшиеся признаки выстраиваются в ряд с плавно уменьшающейся информативностью.

В ходе исследований также разработаны математические модели и алгоритмы оптимального управления целостностью обрабатываемой информации, позволяющие находить баланс между распознаванием угроз ИБ АСОД КП, обеспечением информационной целостности и эффективностью обработки данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Дидюк Ю. Е., Дубровин А. С., Макаров О. Ю., Мещеряков Ю. А., Марков А. В., Рогозин Е. А. Основные этапы и задачи проектирования систем защиты информации в автоматизированных системах // Телекоммуникации. 2003. № 2. С. 29–33.

2. Козиол Дж., Личфилд Д., Эйтэл Д., Энли К., Эрен С., Мехта Н., Хассель Р. Искусство взлома и защиты систем / пер. с англ. Е. Матвеева. СПб., 2006.

3. Минаев В. А. Информационно-аналитические системы обеспечения безопасности: проблемы и решения // Системы безопасности связи и телекоммуникаций. 2001. № 42 (6). С. 20–21.

4. Лахно В. А., Петров А. С. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок. Луганск, 2010.

5. Lahno V. A., Petrov A. S. Task The Research of the conflict Request Threads in the Data Protection Systems // Marketing and logistics problems in the management of organization / ed. H. Howaniec, W. Waszkielewicz. 2011. Chap. XV. P. 230–251.

6. Баскакова Л. В., Журавлев Ю. И. Модель распознающих алгоритмов с представительными наборами и системами опорных множеств // Журн. вычисл. матем. и матем. физики. 1981. Т. 21, № 5. С. 1264–1275.

7. Колегов Д. Н. ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестн. Сиб. гос. аэрокосмич. ун-та им. академика М. Ф. Решетнева. 2009. Вып. 1 (22), ч. 1. С. 49–54.

Поступила в редакцию 05.11.2013.

Валерий Анатольевич Лахно – кандидат технических наук, доцент кафедры экономической кибернетики Луганского национального аграрного университета (Украина).