УДК 004.681.3

В.А. Хорошко, Ю.Е. Хохлачева

Национальный авиационный университет, Киев

ОПТИМАЛЬНОЕ ПЛАНИРОВАНИЕ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рассмотрена проблематика исследований информационной безопасности и разработана модель планирования мониторинга информационной безопасности автоматизированных систем, то есть математическое обеспечение порядка исследования характеристических признаков информационных объектов (ресурсов) автоматизированных систем, определяющих их состояние безопасности. Главная цель создания системы защиты информации – выявлять с минимальными ресурсными затратами поражение информационно-вычислительных компонентов до возникновения потребностей в их непосредственном использовании, обеспечивая гарантированный уровень защищенности функционирования автоматизированных систем.

Ключевые слова: *информационная безопасность, автоматизированные системы, мониторинг информационной безопасности, планирование мониторинга.*

Введение

На сегодняшний день общепризнано множество исследований [1], методология которых обеспечивает информационную безопасность (ИБ) автоматизированных систем (АС), должно исходить из обязательной предпосылки о необходимости формирования функциональной структуры средств защиты информации (ЗИ) на базе применения комплексов взаимосвязанных формализованных методов, математических моделей и алгоритмов управления процессами обеспечения безопасности информации при функционировании АС. Это гарантирует выработку и принятие добротных, качественных проектно-технических решений по организации системы ЗИ, имеющих достаточно высокий уровень обоснованности. Все более усиливающаяся потребность и эффективность именно такого подхода к созданию систем ЗИ, а также не совсем достаточная адекватность, корректность и системность используемых логико-математических моделей, актуализируют исследования по рассмотрению и совершенствованию базового математического обеспечения решения прикладных задач по ИБ объектов и ресурсов АС.

Цель работы. Содержательная направленность тематики настоящей статьи соответствует этой проблематике исследований по ИБ и посвящена разработке модели планирования мониторинга ИБ АС, то есть математическому обеспечению порядка обследования характеристических признаков информационных объектов (ресурсов) АС, определяющих их состояние безопасности.

Основная часть

Сделаем некоторые методические замечания общего характера. Во-первых, при создании систем ЗИ широко используется их функциональная структурная декомпозиция. Так, например, в [2] выделено семь функций защиты, внимательный анализ которых показывает, что в каждой из них одной из решаемых задач является мониторинг информационного объекта на предмет оценки его уровня безопасности. Именно эта задача рассматривается в статье. Во-вторых, разрабатываемая модель мониторинга основывается на обобщении моделей технической диагностики с учетом особенностей отличной от них прикладной интерпретации, что вполне приемлемо для создания начального остова искомой абстрактной конструкции аналитического типа. В-третьих, при таком подходе к выбору модели оригинальность нижеприводимых исследований заключается в учете специфики прикладной интерпретации в области ПО средств ЗИ и в выборе методов решения с последующим уточнением конструктивности предлагаемых вычислительных схем.

Процесс проведения мониторинга ИБ АС будем рассматривать на функциональных уровнях абстрактного описания. На первом уровне обследуется состояние ИБ и отдельно взятого объекта АС (или нескольких объектов воспринимаемых как единое целое). Здесь выделяется ряд характеристических параметров (свойств), распознавание состояний которых позволяет определять текущее состояние безопасности функционирования объекта. На втором уровне обследуется множество различимых объектов АС первого уровня. Здесь возникает задача проведения прерывистого во времени контроля состояния безопасности множества сгруппированных объектов, вложенных в некоторый класс иерархических структур [3].

Далее подробней остановимся на постановке задачи обследования состояния безопасности от-

дельно выделенного информационного объекта АС. Будем считать, что в исследуемом объекте выделен ряд информационных параметров, поддавшихся конструктивному анализу на предмет определения его (количественного или логико-семантического) значения. Каждый из этих параметров может быть отождествлен либо с некоторым типом дестабилизирующего фактора, оказавшим негативное воздействие на тот или иной информационно-вычислительный ресурс объекта, либо с каким-то обобщенным событием, выводящим объект из безопасного состояния.

Предположим, что множество определяемых состояний при анализе каждого параметра равно двум и соответствует состояниям «имеет» или «не имеет» место нарушения безопасности свойства объекта, сопоставляемого с анализируемым параметром. Отрицательный результат анализа хотя бы по одному из параметров свидетельствует о разрушении целостности исследуемого объекта и о его переходе в состояние «безопасность нарушена».

Алгоритм проверки текущего состояния каждого информационного свойства объекта выбирается из некоторого множества алгоритмов и заранее закладывается в систему ЗИ в виде программно реализованной процедуры. Различие алгоритмов проявляется в вероятностных характеристиках эффективности контроля и в пространственно-временных вычислительных ресурсах, затрачиваемых на хранение и выполнение процедур.

Перейдем к разработке искомой модельной конструкции, начиная со структуризации исходных данных и формализованной постановки задачи оптимального назначения алгоритмов обследования по каждому информационному параметру.

Дано:

1. Множество $\{a_1,...,a_i,...,a_n\}$ информационных параметров, по совокупностям значений которых определяется факт нахождения выделенного объекта А в безопасном или не безопасном состоянии. В течении одного цикла обследования, каждый параметр $a_i(i=1,2,...,n)$ находится в состоянии, отвечающем сохранению безопасности с вероятностью и в P_i отличном от него состоянии с вероятностью $Q_i = 1 - P_i$.

2. Конечные подмножества $H_1,...,H_i,...,H_n$ алгоритмов $\{h_i(a_i),...,h_j(a_i),...,h_{mi}(a_i)\}$, в соответствии с которыми может быть организован контроль текущего состояния каждого информационного параметра $a_i(i=1,2,...,n)$ с принятием решения на двухальтернативной основе: текущее состояние параметра a_i отвечает безопасному состоянию объекта А или нет. Предполагается, что состояние объекта a_i в течении одного цикла обследования объекта не изменяется.

Учитывая возможности воздействия случайных или преднамеренных дестабилизирующих факторов на сам процесс обследования, эффективность процесса проверки состояния параметра $a_i(i=1,2,...,n)$ по алгоритму $h_i(a_i)(j=1,2,...,m_j)$, оценивается вероятностными характеристиками принятия решения в соответствии с матрицей

$$\left\| \begin{matrix} 1 & a_i & a_{ij} \\ \beta_i & 1 & \beta_{ij} \end{matrix} \right\|, \; i=1,2,...,n; j=1,2,...,m_i,$$

где a_{ij} – вероятность ошибки первого рода (объект А находится в небезопасном состоянии по параметру a_i, но при проверке состояния параметра a_i по алгоритму $h_i(a_i)$ этот факт не обнаружен), т.е. a_{ij} – вероятность правильной оценки состояния параметра a_i при нахождении объекта А в безопасном состоянии;

β_{ij} – вероятность ошибки второго рода (объект А находится в безопасном состоянии по параметру a_i, но принятое решение при проверке состояния параметра a_i по алгоритму $h_j(a_i)$ обратное), т.е. β_{ij} – условная вероятность обнаружения факта нарушения безопасности объекта А по состоянию параметра a_i, выявленное алгоритмом $h_j(a_i)$.

3. Временные и пространственные характеристики программной реализации алгоритмов a_i:

$\tau_{ij}(i=1,2,...,n; j=1,2,...,m_i)$ – среднее время проверки текущего состояния параметра a_i и принятия решения о его соответствии «безопасному» или «опасному» состоянию объекта А при использовании алгоритма $h_j(a_i)$;

q_{ij} – потребление некоторого вида ресурсов (например, памяти) при использовании алгоритма $h_j(a_i)$.

Требуется:

Определить порядок обследования объекта А по выявлению его истинного состояния информационной безопасности путём назначения для проверки состояния каждого из его информационных параметров $a_i(i=1,2,...,n)$ одного из алгоритмов $h_j(a_i)$ допустимого множества H_i, при котором обеспечивается повышенная достоверность конечных результатов мониторинга и минимизируется потребление пространственно-временных вычислительных ресурсов.

Математическая постановка задачи

Формализованную постановку задачи выполним, оперируя показателями эффективности, отражающими следующие свойства процесса мониторинга информационного объекта А, достоверность конечных результатов и длительность проведения одного цикла обследования объекта, а также объем информационно-вычислительных ресурсов, потребляемых мониторинговой подсистемой системы ЗИ.

Достоверность оценим двумя условными апостериорными вероятностями $D_{бс}$ и $D_{нс}$ наличия соответствия между принятым решением о состоянии ИБ обследуемого объекта и его фактическим состоянием: $D_{бс}$ – достоверность принятого решения о нахождении объекта в безопасном состоянии, $D_{нс}$ – достоверность решения о наличии небезопасного состояния. Достоверность принятых решений только по одному параметру a_i при использовании алгоритма $h_j(a_i) \in H_i$ определяется следующим образом

$$D_{бс}^{(i)} = \frac{P_i(1-a_{ij})}{P_i(1-a_{ij})+(1-P_i)\beta_{ij}},$$

$$D_{нс}^{(i)} = \frac{(1-P_i)(1-\beta_{ij})}{P_i a_{ij}+(1-P_i)(1-\beta_{ij})}. \qquad (1)$$

На множестве результатов проверок всех параметров $a_1,...,a_i,...,a_n$ с использованием зафиксированного ряда алгоритмов проверок

$$h_{r1}(a_1) \in H_1,...,h_{rj}(a_j) \in H_j,...,h_{rn}(a_n) \in H_n$$

будет принято решение о нахождении объекта в безопасном состоянии при наличии положительных решений о нахождении объекта в безопасном состоянии, а также при наличии положительных решений по всем проверяемым параметрам. Достоверность этого события равна

$$D_{бс} = \prod_{i=1}^{n} D_{бс}^{(i)} = \prod_{i=1}^{n} \frac{P_i(1-a_{i(ri)})}{P_i(1-a_{i(ri)})+(1-P_i)\beta_{i(ri)}}. \qquad (2)$$

Решение о небезопасном состоянии обследуемого объекта принимается при получении хотя бы по одному параметру $a_i (i=1,2,...,n)$ неблагоприятного результата. Опуская промежуточные логические рассуждения, приведем окончательное соотношение по оценке значения достоверности определения небезопасного состояния:

$$D_{нс} = 1 - \frac{\prod_{i=1}^{n} P_i - \prod_{i=1}^{n} P_i(1-a_{i(ri)})}{1-\prod_{i=1}^{n}(P_i(1-a_{i(ri)})+(1-P_i)\beta_{i(ri)})}. \qquad (3)$$

Качество планирования порядка проведения процесса обследования объекта оценивается пороговыми значениями достоверности $D_{нс}^{*}$ и $D_{бс}^{*}$ и выделяемых ресурсов Q^{*}. При этом оптимизация совокупности алгоритмов, назначенных для распознавания состояний параметров $a_i (i=1,2,...,n)$, должна обеспечить минимизацию времени однократного мониторинга объекта АС.

Тогда математическая постановка задачи будет следующей.

Найти значения булевых переменных $X_{ij} (i=1,2,...,n; j=1,2,...,m_i)$, где

$$X_{ij} = \begin{cases} 1, \text{если для распознавания} \\ \text{состояния функционального} \\ \text{параметра } a_i \\ \text{предлагается назначить} \\ \text{алгоритм } h_j(a_i) \in H_i, \\ 0 \text{ в противном случае,} \end{cases}$$

которые минимизируют функционал

$$\Phi = \sum_{i=1}^{n}\sum_{j=1}^{m_i} X_{ij}\tau_{ij}, \qquad (4)$$

и обеспечивают выполнение ограничений (5), (6) и (7):

$$\prod_{i=1}^{n} \frac{P_i \sum_{j=1}^{m_i} X_{ij}(1-a_{ij})}{P_i \sum_{j=1}^{m_i} X_{ij}(1-a_{ij}) + (1-P_i)\sum_{j=1}^{m_i} X_{ij}(1-\beta_{ij})} \geq D_{бс}^{*};$$

$$1 - \frac{(1-\prod_{i=1}^{n}(\sum_{j=1}^{m_i} X_{ij}(1-a_{ij})))\prod_{i=1}^{n} P_i}{(1-\prod_{i=1}^{n}(P_i\sum_{j=1}^{m_i} X_{ij}(1-a_{ij}) + (1-P_i)\sum_{j=1}^{m_i} X_{ij}\beta_{ij}} \geq D_{нс}^{*};$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m_i} X_{ij}Q_{ij} \leq Q^{*};$$

$$\sum_{j=1}^{m_i} X_{ij} = 1 \text{ для всех } i = 1,2,...,n.$$

Решение

Логически наиболее оправданным и естественным способом поиска оптимального решения сформулированной выше задачи дискретного программирования (4), (5), (6), (7) является организация направленного перебора вариантов назначения алгоритмов по каждому проверяемому параметру в рамках применения метода «ветвей и границ». В соот-

ветствии с этим методом последовательно просматриваться возможные варианты назначения алгоритмов для проверки параметров $a_1,...,a_i,...,a_n$ и строится дерево решений, на котором на первых же шагах начинается отсечение неперспективных ветвей в соответствии с прогнозируемыми оценками целевой функции.

Вычислительная сложность всех этих методов определяется сложностью расчетных соотношений по оценке целевой функции и собственно процедур ветвления и не всегда отвечает требованиям методик инженерного анализа.

Решение задачи (4) с ограничениями (5), (6), (7) можно упростить как в содержательном, так и в техническом аспектах, если принять во внимание, что $a_{ij} \ll 1$, и $\beta_{ij} \ll 1$ для всех $i = 1,2,...,n$ и $j = 1,2,...,m_i$.

Тогда, имеет место следующая линейная аппроксимация:

$$\prod_{i=1}^{n}(1-\lambda) \approx 1-\sum_{i=1}^{n}\lambda$$

если $\lambda \ll 1$ при всех $i = 1,2,...,n$.

Таким образом, от неравенств (5) и (6) можно перейти к их линейной аппроксимации следующего вида

$$1-\sum_{i=1}^{n}\sum_{j=1}^{m_i}X_{ij}a_{ij} \geq \frac{D^*_{бс}}{1-D^*_{бс}}\sum_{i=1}^{n}\frac{1-P_i}{P_i}\left(\sum_{j=1}^{m_i}X_{ij}a_{ij}\right); \quad (8)$$

$$\left(\prod_{i=1}^{n}P_i\right)^{-1} - \sum_{i=1}^{n}\frac{1-P_i}{P_i}\left(\sum_{j=1}^{m_i}X_{ij}\beta_{ij}\right) \geq$$

$$\geq 1+\frac{D^*_{нс}}{1-D^*_{нс}}\sum_{i=1}^{n}\sum_{j=1}^{m_i}X_{ij}a_{ij}. \quad (9)$$

В результате рассматриваемая задача оптимизации трансформируется в задачу целочисленного линейного программирования, решение которой поддерживается широким спектром апробированных математических методов и технологических пакетов прикладных программ.

Выводы

Решение задачи оптимального планирования порядка установления правильности функционирования автономных информационно-вычислительных объектов является основой для перехода к формированию структурного облика подсистемы мониторинга безопасности функционирования всей АС.

Главная цель создания этой подсистемы в рамках создания системы ЗИ – выявлять с минимальными ресурсными затратами поражение информационно-вычислительных компонентов до возникновения потребностей в их непосредственном использовании, обеспечивая гарантированный уровень защищенности функционирования АС.

Список литературы

1. Хохлачева Ю.Е. Обработка информационных потоков и составление для них расписаний в системах защиты информации / Ю.Е. Хохлачева, В.А. Хорошко, Е.В. Иванченко // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4. №3. – С. 256-263.

2. Хорошко В.А. Особенности защиты информации в сетях связи / В.А. Хорошко, Ю.Е. Хохлачева // Вісник СНУ ім. В.Даля. – 2013. – № 15(204), ч.1. – С. 219-222.

3. Флейшман Б.С. Элементы теории потенциальной эффективности сложных систем / Б.С. Флейшман. – М.: Сов.радио, 1971. – 224 с.

Поступила в редколлегию 17.02.2015

Рецензент: д-р техн. наук, ст. наук. сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

ОПТИМАЛЬНЕ ПЛАНУВАННЯ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ

В.О. Хорошко, Ю.Є. Хохлачова

У даній статті розглянута проблематика досліджень інформаційної безпеки та розроблено модель планування моніторингу інформаційної безпеки автоматизованих систем, тобто математичне забезпечення порядку дослідження характеристичних ознак інформаційних об'єктів (ресурсів) автоматизованих систем, що визначають їх стан безпеки. Головна мета створення системи захисту інформації – виявляти з мінімальними ресурсними витратами поразку інформаційно-обчислювальних компонентів до виникнення потреб в їх безпосередньому використанні, забезпечуючи гарантований рівень захищеності функціонування автоматизованих систем.

Ключові слова: *інформаційна безпека, автоматизовані системи, моніторинг інформаційної безпеки, планування моніторингу.*

OPTIMAL SCHEDULING OF INFORMATION SECURITY MONITORING IN AUTOMATED SYSTEMS

V.A. Khoroshko, J.E. Hohlachova

In this paper the problems of information security research and planning model developed information security monitoring automated systems, is a software research agenda of the characteristic features of information objects (resources) automated systems that determine their security state. The main purpose of creating security solutions detect minimal resource costs lesion data-processing components to the emergence of needs in their immediate use, ensuring a guaranteed level of protection operation of automated systems.

Keywords: *information security, automated systems, information security monitoring, planning monitoring.*