УДК 303.725.23

01.00.00 Физико-математические науки

ФОРМАЛИЗАЦИЯ ПРОЦЕССА ПРИНЯТИЯ РЕШЕНИЯ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕ БАЙЕСОВСКОГО ПОДХОДА

Степанов Владимир Васильевич
д.т.н., профессор

Кучер Алексей Викторович
к.т.н., профессор
vvs04367@mail.ru
Кубанский государственный технологический университет, г.Краснодар, Россия

В работе представлена модель выбора решений из множества альтернатив, в результате которого получается подмножество альтернативы или несколько альтернатив, основанной на использовании байесовского подхода, на базе сформулированного понятия функции защищенности, как априорной оценки последствий принятия решения. Последнее способствует уменьшению прогнозируемого параметра и, как следствие, увеличению значения функции защищенности. Таким образом, рассмотренные показатели защищенности информации отражают сущность Байесовского подхода к принятию решений по управлению СЗИ, и позволяет сформировать оптимальные решающие правила

Ключевые слова: КОЛИЧЕСТВО ИНФОРМАЦИИ, МАТЕМАТИЧЕСКАЯ МОДЕЛЬ, ЗАЩИТА ИНФОРМАЦИИ, ПРИНЯТИЕ РЕШЕНИЙ, ФУНКЦИЯ ЗАЩИЩЕННОСТИ, АПОСТЕРИОРНАЯ ЗАЩИЩЕННОСТЬ

UDC 303. 725.23

Physical-Mathematical sciences

FORMALIZATION OF PROCESS OF DECISION-MAKING ON MANAGEMENT OF SAFETY OF INFORMATION IN THE AUTOMATED SYSTEMS ABOUT USE OF BAYESIAN APPROACH

Stepanov Vladimir Vasilyevich
Dr.Sci.Tech., professor

Kucher Alexey Viktorovich
Cand.Tech.Sci., professor
vvs04367@mail.ru
Kuban state technological university, Krasnodar, Russia

The article presents a model for choosing a variety of alternative solutions, in which we have a subset of turns or more alternative options, based on the use of the Bayesian approach, based on the formulated concept of security functions as a priori estimate of the effects of the decision. This reduces the projected parameters and, therefore, increases the values of security. Thus, the considered indicators of data protection reflect the essence of Bayesian approach to decision making and management of GIS, so it allows to generate optimal decision rules

Keywords: AMOUNT OF INFORMATION, MATHEMATICAL MODEL, INFORMATION SECURITY, DECISION-MAKING, SECURITY FUNCTION, APOSTERIORNY SECURITY

На практике существуют три подхода к принятию решения [1]:

1. Дескриптивный. Данный подход связан с процессом выбора решения человеком. При этом учитывается, что люди не всегда прибегают к систематизированным методам, а действуют интуитивно, проявляя непоследовательность, что приводит к противоречивым результатам. Этот подход даёт возможность определить, что может и чего не может человек, оказавшись перед выбором.

2. Нормативный подход. Используются идеализированные теории, рассчитанные на рационального человека с мощным интеллектом и с разработкой соответствующей нормативной базы.

3. Перспективный подход. Основывается на действиях человека с обычным интеллектом при его готовности напряженно и систематизировано работать в области принятия решений. Данный подход не гарантирует оптимального решения, а лишь обеспечивает выбор решения при использовании определённой методологии.

Кроме рассмотренных выше подходов к принятию решений широко применяется весь арсенал методов прикладной математики.

Рассмотрим математическую модель, описывающую целенаправленное поведение лица, принимающего решение (ЛПР) по управлению защитой информации в автоматизированной системе (АС) может быть представлена в виде функционала (1) , включающего семь компонент, связанных между собой:

$$P_{def} = < Z, A, K, R, F, Q, D > \qquad (1),$$

где Z – цели задачи для решения рассматриваемой проблемы с максимальным разбиением на отдельные подзадачи;

A – множество альтернатив выбора механизмов защиты, которые применимы в конкретной ситуации информационного противоборства;

K – критерии оценки степени достижения цели;

R – множество шкал измерения по критериям (порядковые, интервальные, шкалы наименования и отношения);

F – отображение множества допустимых альтернатив на множество критериальных оценок;

Q – система предпочтений лица, принимающего решения;

D – решающее правило, отображающее систему предпочтений

Основу выбора решения составляет теория выбора. Эта теория предполагает принятие решения как действие над множеством альтернатив, в результате которого получается подмножество выбранной альтернативы или несколько альтернатив. Сужение множества возможно, если имеется способ сравнения альтернатив между собой с учётом системы критериев эффективности (критериев предпочтения при выборе). При выборе возможны следующие варианты:

- Множество решений $P_j, j = \overline{1,p}$ может быть конечным, счётным или континуальным (очень большое, но счётное);
- оценка отдельных альтернатив P_j может осуществляться по одному или нескольким критериям, сами критерии могут иметь качественный или количественный характер;
- правило выбора может быть однократным или повторяющимся, при этом допускается обучение на опыте;
- последствия выбора могут быть известны (выбор в условиях определённости), иметь вероятностный характер (выбор в условиях риска), или иметь неоднозначный исход (выбор в условиях неопределенности);
- ответственность за выбор может быть односторонней (индивидуальный выбор) либо многосторонней (групповой выбор);
- степень согласованности целей при многостороннем выборе изменяется от полного совпадения интересов сторон (кооперативный выбор) до их противоположности (выбор в конфликтных случаях).

Отсюда следует, что выбор решения в сложных ситуациях информационного противоборства осуществляется в условиях **риска и неопределённости**. Это связано с тем, что исходные данные, необходимые

для планирования процессов защиты, синтеза и управления системой защиты информации (СЗИ) имеют вероятностный характер. Работа аппаратных и программных средств АС сопровождается случайными сбоями, отказами, статистические характеристики которых не всегда удаётся определить и учесть в технологических процессах. Ещё сложнее обстоят дела в задачах управления активной информационной борьбой, где помимо естественной нехватки информации всегда есть вероятность навязывания ложной информации.

Поэтому задачи планирования процессов защиты информации, управления СЗИ представляют собой сложные многоэкстремальные и многокритериальные задачи. Подходы к решению таких задач можно разделить на три класса, связанных с математическим, эвристическим и эволюционным программированием.

Рассмотрим кратко каждый из подходов. Задача математического программирования состоит в следующем: выбор решения заключается в выборе вектора или вектор-функции из некоторой допустимой области, обращающих в максимум или в минимум (в зависимости от постановки задачи) некоторый функционал – критерий качества.

Эвристическое программирование состоит в моделировании методов переработки информации и выбора решений живыми организмами.

В отличие от эвристического программирования, при эволюционном программировании процесс моделирования деятельности организма заменяется моделированием его эволюции.

Характерной особенностью современных СЗИ является тот факт, что ограниченность во времени не позволяет откладывать процедуру принятия решения до получения полной информации. Однако последовательное накопление информации даёт возможность корректировки и совершенствования решения. Тогда рациональные предварительные решения должны учитывать прогнозируемые значения статистических

характеристик ещё не реализованных случайных параметров задачи. Поэтому при планировании СЗИ рассматривают возможность использовать все три подхода для решения данной задачи.

Для процесса принятия решения по управлению СЗИ в АС характерны следующие особенности:

1. Решение на применение тех или иных средств защиты (СрЗ) направлено на достижение требуемого или максимального выигрыша СЗИ в отношении системы информационного нападения (СИН).

2. Решение принимается с помощью имеющейся у ЛПР информации: априорных сведений о противнике и совокупных данных наблюдения $\boldsymbol{x}$, получаемых от средств контроля СЗИ в процессе выработки решения.

3. Информация, необходимая ЛПР при принятии решения и последствия от принятия того или иного варианта решения, имеют нечёткую природу.

4. Выбор решения из множества альтернатив допускает элементы случайности (рандомизации).

Задачей ЛПР является выбор такого решения, которое исходя из поставленной цели, приводило бы к наиболее благоприятным последствиям. Это означает, что правила принятия решения D, определяющие порядок его выбора с использованием имеющейся информации, должны быть оптимальными.

Для формализации поставленной задачи введём следующие обозначения.

Пусть $\boldsymbol{P_j, j = \overline{1,p}}$ - множество возможных решений, а $\boldsymbol{j \epsilon P}$ - его элементы, $\boldsymbol{x}$ -есть совокупность данных наблюдения о противнике, которые ЛПР получает от средств контроля СЗИ в процессе выработки решения. В случае идеального информационного конфликта (все процессы детерминированы) информация $\boldsymbol{x}$ представляет собой номер $\boldsymbol{I}$ варианта

нападения противника из множества $N, i = \overline{1,n}$ возможных альтернатив его поведения. Решение ***j*** может состоять из совокупности частных решений ***j=1,2…,p.***

Введём описание правила принятия решения. В качестве такого правила выберем алгоритм обработки данных наблюдения ***x***. В случае детерминированного процесса принятия решения задание этого правила есть задание какого-либо однозначного соответствия между ***x*** и ***j*** , т.е. преобразование ***j=j(x)*** , при $x \epsilon X, j \epsilon P$. В зависимости от способа задания множеств ***X*** и ***P*** преобразование ***j=j(x)*** может быть функцией скалярного или векторного аргументов, функционалом, функцией множества.

Совокупность различных преобразований ***j=j(x)*** образует множество ***P(X)*** всех решающих правил с использованием данных наблюдения ***x.***

При наличии рандомизации для конкретного варианта поведения противника $i \epsilon N$ могут приниматься различные решения по защите $j \epsilon P$ с некоторой условной вероятностью ***r(j/x)*** , которая определяет вероятность принятия конкретного решения ***j*** при данном ***x***; ***r(j/x)*** называется рандомизированным правилом принятия решения [1,2].

Рассмотренные правила принятия решений подводят нас к формализации понятия защищенности информации в многоальтернативных ситуациях информационного противоборства на основе функции выигрыша, используемой в теории статистических решений.

Эффективность решений по управлению СЗИ ***W*** может быть представлена следующим вектором

$$W<R,T,C> \qquad (2)$$

где ***R***– результативность;

T – оперативность;

C – ресурсоемкость (стоимость).

Принятие того или иного решения по управлению защитой информации приводит к определенным последствиям. Эти последствия необходимо оценивать с точки зрения соответствия поставленной цели и задачи.

Целью управления СЗИ является обеспечение требуемой степени защищенности информации в АС. Для достижения этой цели расходуются определенные ресурсы и время. При этом определяются следующие ограничения на выбор оптимального решения:

1) стоимость ресурсов, которые необходимо затратить на реализацию выбранной стратегии защиты, должна быть не более величины возможного ущерба от действий противника при отсутствии данной стратегии защиты;

2) время достижения цели СЗИ должно быть не больше времени достижения цели СИН.

Выберем для каждого из возможных альтернативных решений количественную меру защищенности информации как целевой эффект ***R***, задающий выигрыш СЗИ от принятия данного решения. В теории принятия решений эта количественная мера отождествляется с функцией выигрыша СЗИ или **функцией защищенности**. Будем считать, что выбранное решение по управлению СЗИ приводит к наиболее благоприятным последствиям, если оно максимизирует величину защищенности информации.

Пусть ***R(j)*** – значение функции защищенности для ***j***-го решения. Если бы последствия решения ***j*** и их количественная мера ***R(j)*** зависели только от значения ***j***, то вопрос о выборе оптимального решения по управлению СЗИ решался бы очень просто: необходимо было бы выбрать то решение ***j***, для которого значение $R(j) \rightarrow max$.

Однако, на практике последствия принятия решения, а значит и функция защищенности зависят от ряда факторов, которые могут

изменяться во времени и в зависимости от складывающейся обстановки в ходе информационного противоборства СЗИ и СИН. Например, защищенность информации в АС может зависеть от следующих факторов:

-какими средствами информационного нападения располагает противник в момент времени ***t;***

-какой вариант действий предпринял противник в конкретной ситуации;

-как своевременно было обнаружено нападение СЗИ;

-насколько точно были идентифицированы эти атаки;

-какова надежность средств защиты;

-надежность и живучесть структуры АС и т.д.

Поэтому функция ***R(j)*** зависит также от некоторых параметров ***λ,*** описывающих реальную ситуацию в АС, в которой принимается решение ***j***. Эти параметры образуют некоторое множество ***Λ*** такое, что для каждого $j \in m$ и $\lambda \in \Lambda$ можно определить значение ***R(j,Λ),*** описывающее последствия принятия решения ***j*** в ситуации ***Λ***.

Для дискретного пространства функция защищенности $R(j,\lambda)=L_i$, где ***j*** – номер решения, ***i*** – номер истинной ситуации в АС.

В качестве примера такой функции в случае абсолютно надежных средств защиты может быть **вероятность события**, заключающегося в том, что на интервале времени ***[0,T]*** случайное время ***t*** реализации стратегии защиты с функцией распределения $F_i(t_i)$ будет меньше, чем случайное время $\hat{\tau}_j$ реализации стратегии нападения с функцией распределения $F\tau_j(\tau_j)$:

$$R_{\hat{t}_j}(T) = \int_0^T F_{\hat{t}_i}(t_l)\,dF_{\hat{t}_i}(\tau_l) \quad (3)$$

Функция защищенности ***R(j.λ)*** представляет собой априорную оценку последствий принятия решения ***j*** в ситуации, характеризуемой

наличием не наблюдаемых, а прогнозируемых параметров λ. Если же при принятии решения в распоряжении ЛПР имеется совокупность $x \epsilon X$ наблюдаемых данных о действиях сторон информационного противоборства в АС, то функция защищенности примет следующий вид $R(i,\lambda)=R(j,\lambda,x)$.

В отношении данных наблюдения $x \epsilon X$ следует учитывать следующие обстоятельства:

данные x имеют вероятностный характер из-за того, что сам процесс наблюдения имеет стохастическую сущность;

данные x всегда связаны с параметрами λ, характеризующими ситуацию противоборства СИН и СЗИ, в которой принимается решение.

Значит, данные x как и λ влияют на последствия от принятия решения. Только при наличии такой взаимосвязи эти последствия имеют ценность с точки зрения уменьшения неопределенности значений λ и увеличения значения функции $R(j,\lambda,x)$ от принятия решения.

Эти обстоятельства позволяют для описания взаимосвязи данных наблюдения x наблюдаемых параметров λ ввести вероятностную меру, зависящую от λ и заданную на множестве Λ. В качестве такой меры выберем условную плотность вероятности $f_{\frac{x}{\lambda}}(x/\lambda)$. Эта величина

называется **функцией правдоподобия**.

Задание вероятностных мер для j,λ,x позволяет заранее определить ожидаемое значение выигрыша от принятия решения путем вычисления математических ожиданий функции защищенности $R(j,\lambda,x)$. Назовем математическое ожидание показателя защищенности информации **средней защищенностью.**

Выбор оптимального решения заключается в максимизации ожидаемой средней защищенности. Определяя математическое ожидание

R(j,λ,x)., получим среднее значение защищенности информации при принятии решения по управлению СЗИ в АС ВН

$$R_{ср}(f_{j/x}) = \iiint R(j,\lambda,x) f_{\underset{x}{L}}(j/x) f_{\frac{x}{\lambda}} f_{\lambda}(\lambda) dj dx d\lambda \qquad (4),$$

$f_{\underset{x}{L}}(j/x)$- условная плотность вероятности при принятии решения ***j*** и

при данном значении ***x***, определяющая **решающее правило** управления СЗИ в АС.

Оптимизация правила принятия решения заключается в выборе такой функции $f_{\underset{x}{L}}(j/x)$, которая обеспечивает максимум $R_{ср}(f_{j/x})$/

Однако при разработке системы управления безопасностью информации в АС важным для решения задачи оптимизации является **показатель апостериорной защищенности** – условное математическое ожидание функции защищенности для решения ***j***при данном значении ***x***. Это математическое ожидание определяется путем усреднения функции защищенности по апостериорному распределению вероятности для параметров $\lambda \epsilon \Lambda$**.** Оно находится с помощью формулы Байеса:

$$f_{\frac{\lambda}{x}}\left(\frac{\lambda}{x}\right) = \frac{f_{\frac{x}{\lambda}}(x/\lambda) f_{\lambda}(\lambda)}{\int f_{\frac{x}{\lambda}}\left(\frac{x}{\lambda}\right) f_{\lambda}(\lambda)\, d\lambda} = \frac{f_{\frac{x}{\lambda}}(x/\lambda) f_{\lambda}(\lambda)}{f_{x}(x)} \qquad (5)$$

В отличие от априорного распределения $f_{\lambda}(\lambda)$ апостериорное распределение описывают неопределенность в значениях λ после наблюдения ***x***. Апостериорная защищенность $R^{\Lambda}(j,x)$ определяется следующим выражением [1,2,3]:

$$R^{\Lambda}(j,x) = \int R(j,\lambda,x) f_{\frac{\lambda}{x}}\left(\frac{\lambda}{x}\right) d\lambda = \frac{\int R(j,\lambda,x) f_{\frac{x}{\lambda}}\left(\frac{x}{\lambda}\right) f_{\lambda}(\lambda)\, d\lambda}{\int f_{\frac{x}{\lambda}}\left(\frac{x}{\lambda}\right) f_{\lambda}(\lambda)\, d\lambda} \qquad (6)$$

Выражение (6) представляет собой ожидаемое значение защищенности информации при реализации принятого решения $j \epsilon P$,

соответствующее данному значению x, которое получается в процессе наблюдения сенсорами средств защиты СЗИ за действиями СИН. Поэтому $R^{\Delta}(j,x)$ является оценкой последствий принятия решения j при данном значении x. Средняя и апостериорная защищенности связаны между собой следующим соотношением:

$$R_{\text{ср}}\left(f_{\underset{x}{\underline{\lambda}}}\right) = \int R(j,\lambda,x)\cdot f_{\underset{x}{\underline{\lambda}}}(j/x)\cdot f_x(x)\,dj\,dx \qquad (7)$$

В заключении можно отметить, что в данной работе сформулировано понятие функции защищенности как априорная оценка последствий принятия решения j в ситуации, характеризуемой наличием не наблюдаемых, а прогнозируемых параметров λ, при этом данные наблюдений x имеют вероятностный характер, поскольку сам процесс имеет стахостическую сущность.

В ситуации характеризующей противоборство СИН и СЗИ данные x всегда связаны с прогнозируемыми параметрами λ и влияют на последствия принятия решения, что способствует уменьшению значений λ и, как следствие увеличению значения функции защищенности $R(j,\lambda,x)$, являющейся показателем средней защищенности, а при выборе оптимального решения ее необходимо максимизировать.

Рассмотренные показатели защищенности информации отражают сущность Байесовского подхода к принятию решений по управлению СЗИ и позволяет сформировать оптимальные решающие правила.

Литература:

1. Орлов, А.И. Теория принятия решений: учеб. - М.: Экзамен, 2006.-575с.
2. Петровский, А. Б. Теория принятия решений : учеб.: рек. УМО. - М.: Академия, 2009. - 400 с.
3. Мендель А.В. Модели принятия решений: учебное пособие [Электронный ресурс] - М.: ЮНИТИ-ДАНА, 2012. - 465 с.

References

1. Orlov, A.I. Teorija prinjatija reshenij: ucheb. - M.: Jekzamen, 2006.-575s.

2. Petrovskij, A. B. Teorija prinjatija reshenij : ucheb.: rek. UMO. - M.: Akademija, 2009. - 400 s.

3. Mendel' A.V. Modeli prinjatija reshenij: uchebnoe posobie [Jelektronnyj resurs] - M.: JuNITI-DANA, 2012. - 465 s.