УДК 303.725.23

01.00.00 Физико-математические науки

СТАТИСТИЧЕСКИЕ МОДЕЛИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Степанов Владимир Васильевич
д.т.н., профессор

Кучер Виктор Алексеевич
к.т.н., профессор
vvs04367@mail.ru
Кубанский государственный технологический университет, Россия 350000, Краснодар, Красная д. 135, к-123

В статье рассмотрены математические модели по управлению принятия решений для выбора варианта защиты АС, основываясь на достаточной статистической информации об атаках на элементы АС. Количество априорной неопределенности о выборе варианта защиты в СЗИ описывается энтропией Больцмана. Введение величины, которая в рамках шенновского определения называется взаимной информацией связи случайной величины, позволяет снять неопределенность в отношении действий противника, даёт возможность ЛПР выбирать варианта защиты. Рассматриваемая в статье модель принятия решений по выбору варианта защиты АИС основывается на достаточной статистической информацией об атаках на элементы системы. В идеальном случае, для принятия решений используется большая выборка статистических данных, что обеспечивает высокую точность управления системой защиты информации. На основе имеющегося количества информации, которой располагает СЗИ, в отношении действий СИН выбрать решение по выбору варианта защиты

Ключевые слова: КОЛИЧЕСТВО ИНФОРМАЦИИ, МАТЕМАТИЧЕСКАЯ МОДЕЛЬ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ, ПРИНЯТИЕ РЕШЕНИЙ, ФУНКЦИЯ ЗАЩИЩЕННОСТИ, МЕТОД ХАРТЛИ, МЕТОД ШЕННОНА, АПОСТЕРИОРНАЯ ЗАЩИЩЕННОСТЬ

UDC 303.725.23

Physical-Mathematical sciences

STATISTICAL MODELS DECISION SUPPORT FOR INFORMATION SECURITY MANAGEMENT IN AN AUTOMATED SYSTEM

Stepanov Vladimir Vasilyevich
Dr.Sci.Tech., professor

Kucher Viktor Alexeyevich
Cand.Tech.Sci., professor
vvs04367@mail.ru
Kuban state technological university, Russia Krasnodar,350000 Red 135, 123

The article deals with mathematical models of management decision-making to select the option to protect the AU, based on sufficient statistical information about attacks on the AU. The amount of a priori uncertainty about the choice of protection option in GIS was described with Boltzmann's entropy. Introduction of the value within Shannon’s definition of mutual information is called the context random variables, it allows removing the uncertainty regarding the actions of the enemy, and it enables decision-makers to choose protection options. The model of decision for choosing the type of protection of the AIS presented in the article is based on sufficient statistical information about the attacks to the system components. In the ideal case, for decision-making, we use large sample statistical data that provides high accuracy control system for protection of information. Based on the available amount of information available to the IPA, against the acts of SIN, it is possible to choose a decision on the choices you make

Keywords: AMOUNT OF INFORMATION, MATHEMATICAL MODEL, SYSTEM OF INFORMATION PROTECTION, INFORMATION SECURITY, DECISION-MAKING, FUNCTION OF PROTECTION, METHOD OF HARTLEY, METHOD OF SHANNON, POSTERIORI PROTECTION

Автоматизированные информационные системы (АИС) сегодня становятся одним из главных инструментов управления бизнесом, важнейшим средством производства современного предприятия. Однако

применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности из-за наличия угроз информации.

В средствах массовой информации регулярно появляются данные об ущербе мировой экономике от компьютерных нападений, что свидетельствует, что применяемые в современных АИС традиционные комплексы систем защиты информации (СЗИ) практически не позволяют обеспечивать выполнение требований по защите информации в течение всего периода функционирования информационных систем. Сложная ситуация в сфере информационной безопасности усугубляется в связи с появлением неизвестных ранее типов разрушающих информационных воздействий и использованием глобальной сети для внешних и внутренних электронных транзакций предприятий. Таким образом, без должной степени защиты компонентов АИС внедрение информационных технологий может оказаться экономически необоснованным и невыгодным.

Кроме того, обеспечение компьютерной безопасности создает неудобства и ограничения в работе пользователей, отнимает вычислительные ресурсы, гарантирует сохранение конфиденциальности, целостности, доступности с вероятностью, пропорциональной затратам.

В связи с заявленным выше напрашивается вывод, что обеспечение безопасности АИС должно быть не однократным действием, а постоянно действующим процессом, и для успешного использования современных информационных технологий необходимо эффективное управление системой защиты информации.

Основными задачами системы управления защитой информации в АИС являются определение оптимальных или хотя бы рациональных наборов средств защиты при варьировании требований к уровню защищенности:

- управление составом;
- количеством;
- компонентами устройств;
- программного обеспечения.

Для описания ситуаций принятия решений по управлению защитой информации, построения адекватных математических моделей этих процессов большое значение имеет учет степени информированности конфликтующих сторон (системы информационного нападения (СИН), с одной стороны, и системы защиты информации (СЗИ) - с другой стороны) о целях и возможных вариантах действий соперников. При описании неопределенностей и рисков чаще всего используется вероятностно-статистический подход.

Для этих целей разработаны различные способы описания неопределенностей: вероятностные модели, теория нечеткости, интервальная математика, используют методологию теории конфликта, основой которой является теория игр.

Следовательно, логичным является использование игровых моделей для формализации понятия информированности сторон конфликта. С этой целью используем известные игровые модели, учитывающие информационные аспекты, в частности ценности имеющейся информации для игроков, которую они в дальнейшем используют для принятия оптимального решения.

На основании изложенного рассмотрим следующие математические модели принятия решений, учитывающие информационность участников конфликта о целях и намерениях действий, основанные на статистической природе исходных данных [1,2,3]:

- ***модель принятия решения по управлению СЗИ на основе хартлиевского количества информации;***

• ***модель принятия решения по управлению СЗИ на основе шенноновского количества информации.***

Рассмотрим каждую из представленных моделей в отдельности.

1. Модель поддержки принятия решений на основе хартлиевского количества информации, которая заключается в определении информационной емкости сообщения и эта величина зависит от объема передаваемого сообщения в символах и количества двоичных разрядов, необходимых для представления каждого символа.

За основу возьмем модель принятия решения по защите информации, схематично представленную на рисунке 1.

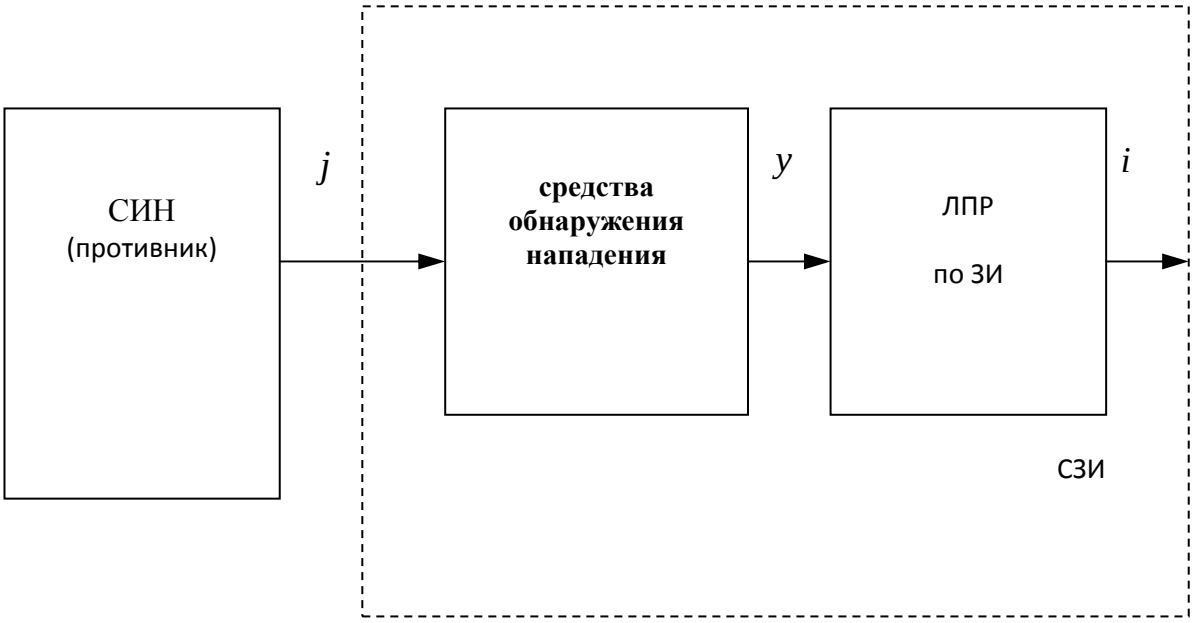

Рисунок 1. Модель принятия решения по защите информации в системе информационного противоборства

Обозначим через множество вариантов нападения на защищаемые объекты в автоматизированной системе со стороны системы информационного нападения, а - номер варианта действия противника. Средства обнаружения нападения являются элементами системы защиты информации АИС.

Предположим, что однозначно установить номер варианта действия противника с помощью средств обнаружения невозможно из-за неопределенности действий противника и технического несовершенства самих средств обнаружения нападения.

Средства обнаружения на основе анализа некоторых признаков могут выделить номер k некоторой области E_k пространства $G = E_1 \cup E_2 \cup E_k, ..., \cup E_M$, $(\forall l,n\ E_l \cap E_n = \varnothing)$, к которому принадлежит вариант действий, выбранный противником. Средства обнаружения нападения выдают для принятия решения информационный сигнал $y = \overline{1,M}$. Количество областей разбиения M пространства G определяется количеством информации I по Хартли [1, 2,3]

$$M = \text{int}(e^I), \qquad (1)$$

где $\text{int}(\alpha)$ - целая часть числа α.

На основе информационного сигнала y лицо, принимающее решение (ЛПР), выбирает решение на применение i-го варианта защитных действий из допустимого множества вариантов $i = \overline{1,m}$. Будем считать, что на множестве вариантов действий СЗИ и СИН задана некоторая функция защищенности $R(i,j)$, соответствующая функции выигрыша при выборе i - го варианта защиты, противостоящему j - му варианту нападения.

Целью СЗИ является максимизация функции защищенности $R(i,j)$. Для этого средства обнаружения нападения должны оптимальным образом разбивать пространство G на области $E_1, ..., E_M$, а в процессе принятия решения должен выбираться наиболее адекватный вариант защиты, максимизирующий условное математическое ожидание $Z = M[R(j,i)/E_k]$.

Применение данной модели позволяет выявить следующие недостатки:

1. В модели определяется только целая часть числа $M = e^I$ и неясно как будет влиять на защищенность информации дробная часть числа e^I.

2. Хартлиевское количество информации $I = \ln M$, определяющее приращение защищенности, не имеет характера разности двух энтропий, поэтому определение физического смысла его затруднено.

Модель будет адекватной, если в качестве информационной меры использовать шенноновское количество информации.

2. Модель поддержки принятия решений на основе шенноновского количества информации (рисунок 2).

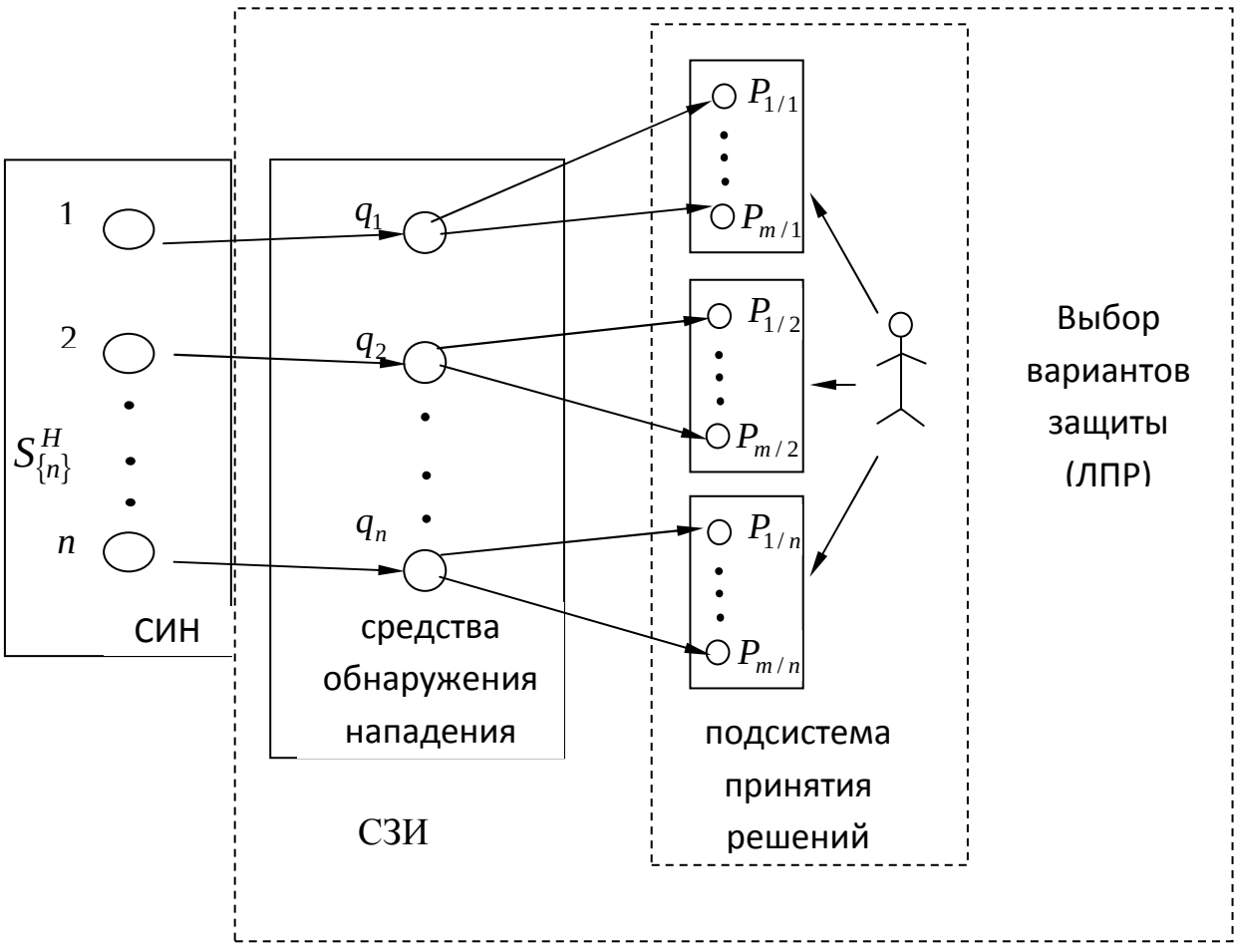

Рисунок 2. Модель принятия решения по выбору варианта

системы защиты АИС на основе шенноновского
количества информации

Модель принятия решения по выбору варианта защиты на основе шенноновского количества информации рассмотрим на основе схемы представленной на рисунке 2.

Вариант защиты выбирается также на основе получения определенного количества информации. Однако в отличие от предыдущего случая количество информации определяется как разность априорной и апостериорной энтропий (энтропия - мера неупорядоченности, мера недостатка информации в системе). Изменение энтропии во много раз превышает количество полученной информации.

Рассматриваемая в статье модель принятия решений по выбору варианта защиты АИС основывается на достаточной статистической информации об атаках на элементы системы. В идеальном случае для принятия решений используется большая выборка статистических данных, что обеспечивает высокую точность управления системой защиты информации.

Вариант построения системы защиты выбирается на основе получения определенного количества информации. Количество информации определяется как разность априорной и апостериорной энтропий.

Пусть множество вариантов действий системы защиты информации задается рядом априорного распределения возможных альтернатив применения средств защиты при нападении противника на АИС.

$$P_{€}(i) = \{p_1, p_2, ..., p_i, ..., p_m\}$$

Количество априорной неопределенности о выборе варианта защиты в СЗИ можно описать энтропией Больцмана [1,2,3]

$$H_i = -\sum_{i=1}^{m} p_i \ln p_i \ . \qquad (2)$$

Примем, что средства обнаружения нападения не могут полностью определить используемый противником вариант нападения. Они могут только произвести вероятностную оценку применения этого варианта, задаваемого рядом распределения

$$Q_{\text{€}}(j) = \{q_1, q_2, ..., q_j, ..., q_n\}.$$

Результаты определения номера варианта действий противника j от средств обнаружения поступают в подсистему принятия решения для выбора варианта защиты. Этот выбор описывается условным распределением вероятностей

$$P_{\text{€}/j}(i) = \{P_{1/j}, P_{2/j}, ..., P_{i/j}, ..., P_{m/j}\}.$$

Условная энтропия данного распределения выражает апостериорную неопределенность при получении номера j и определяется как [1]:

$$H_{i/j} = -\sum_{j=1}^{n}\sum_{i=1}^{m} P(i, j) \ln P_{i/j} \ , \qquad (3)$$

где $P(i, j)$ - совместное распределение случайных величин € и €.

Введем величину

$$I = H_i - H_{i/j},$$

которая в соответствии с шенноновским определением [1] называется **взаимной информацией связи** случайных величин € и €.

Физический смысл этой величины можно рассматривать как количество информации об €, которое содержится в € (другими словами -

снятие неопределенности в отношении действий противника), используемое ЛПР для принятия решения по выбору варианта защиты.

Используя выражения (2) и (3), с учетом того, что $\sum_{j=1}^{n} P(i, j) = p_i$, получаем:

$$I = -\sum_{i=1}^{m} p_i \ln p_i + \sum_{j=1}^{n}\sum_{i=1}^{m} P(i, j) \ln P_{i/j} = \sum_{j=1}^{n}\sum_{i=1}^{m} \ln \frac{P_{i/j}}{p_i} P(i, j) \qquad (4)$$

Таким образом, количество информации I, которым располагает СЗИ в отношении действий СИН, определяет принятие решения по выбору варианта защиты. Очевидно, что этот выбор должен быть оптимальным, что предполагает максимизацию функции защищенности объектов АИС, задаваемых на множестве действий вариантов СЗИ и СИН.

В рассмотренных моделях для принятия решений используется большая выборка статистических данных, что обеспечивает высокую точность управления СЗИ.

Литература:

1. Гаценко О.Ю. Защита информации. - СПб.: Изд. дом «Сентябрь», 2001. – 228 с.
2. Орлов, А.И. Теория принятия решений: учеб. - М.: Экзамен, 2006. - 575 с.
3. Петровский, А. Б. Теория принятия решений : учеб.: рек. УМО. - М.: Академия, 2009. - 400 с.

References:

1. Gacenko O.Ju. Zashhita informacii. - SPb.: Izd. dom «Sentjabr'», 2001. – 228 s.
2. Orlov, A.I. Teorija prinjatija reshenij: ucheb. - M.: Jekzamen, 2006. - 575 s.
3. Petrovskij, A. B. Teorija prinjatija reshenij : ucheb.: rek. UMO. - M.: Akademija, 2009. - 400 s.