УДК 004.75

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДОВ ТЕОРИИ ИГР

В.А. КУЧЕР, Е.С. ТАРАСОВ

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2
электронная почта: vakucher@bk.ru

В статье описан подход к применению методов теории игр при оптимизации и моделировании процессов управления безопасностью автоматизированных систем и реагирования на инциденты. Приведена математическая постановка задачи, формальное описание игр и соответствующих стратегий управления системами защиты информации с учетом специфики конкретных объектов защиты.
Ключевые слова: принятие решений и управление, теория игр, информационное противоборство, стратегии защиты.

Жизнь современного общества невозможна без повсеместного использования компьютерных технологий. Сегодня компьютерные информационно-телекоммуникационные системы (ИТКС) определяют надежность систем жизнеобеспечения общества, обеспечивают хранение, обработку, передачу и предоставление информации потребителям.

Управление ИТКС в настоящее время практически полностью автоматизируется. Причем развитие современной науки об управлении идет в направлении повышения обоснованности принимаемых решений и уменьшения времени на сбор и обработку управленческой информации. Выходом из этого положения является передача все большего числа функций средствам электронно-вычислительной техники и разработанным на их основе системам управления. Важнейшим классом таких систем являются автоматизированные системы (АС).

Современная АС является сложной системой управления. Она объединяет в единый контур большое число разнородных территориально распределенных объектов, включающих в себя специализированные и универсальные вычислительные машины, системы, комплексы и устройства передачи данных, удаленные автоматизированные рабочие места пользователей

(рисунок 1). Управление системой осуществляется с центра управления АС. В зависимости от назначения компоненты АС могут объединяться в различные информационно-вычислительные сети (ИВС).

Но создание АС и ИВС привело к появлению целого ряда негативных последствий, таких как компьютерные злоупотребления и преступления. Защиты требуют как информационные ресурсы, так и все компоненты АС.

Процесс защиты информации в АС представляет собой случайный многошаговый процесс принятия решений и реализации этих решений с помощью механизмов и средств защиты информации. Так как данный процесс является направленным на решение целевых задач АС, то приемлемые результаты при анализе и синтезе систем защиты можно получить с использованием теории эффективности целенаправленных процессов [1]. При этом неопределенность принятия решений в ходе процессов информационного противоборства требует использовать методы теории конфликтов.

Одним из актуальных направлений в области информационной безопасности является развитие теории управления процессами обеспечения безопасности информации, позволяющей повысить эффективность защиты за счет организации управления функционированием системы средств и механизмов защиты, а также системы контроля защищенности информации в АС (рисунок 1). Это возможно при наличии математических моделей защиты информации и методов их применения, а также моделей и алгоритмов управления процессами защиты информации в условиях действия случайных и специально организованных дестабилизирующих факторов.

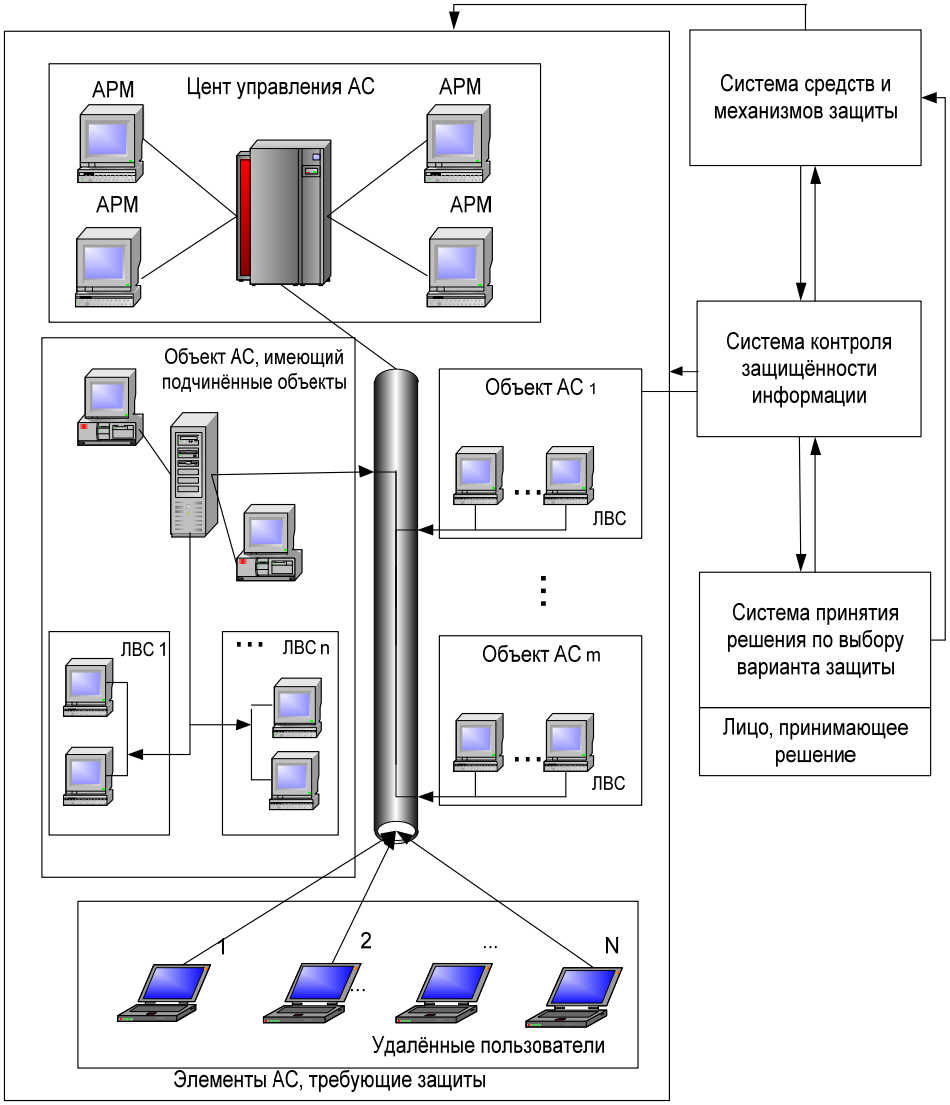

Рисунок 1. Структура АС и контур управления защитой информации

Комплексный анализ проблем защиты информации в АС невозможен без определения ключевых терминов данной предметной области, среди которых центральное место занимает понятие «защищенности информации». Наиболее целесообразным является определение понятия защищенности информации с позиции системного подхода [1].

Системный подход предполагает комплексное рассмотрение исследуемого объекта как системы с учетом существующих внутренних и внешних связей [2-4]. Применительно к защите информации и защищенности информации, как результату защиты, системный подход предполагает исследование конфликта участников информационного противоборства, а также факторов, влияющих на достижение целей (выигрыша) каждой из сторон.

Концептуальная модель информационного противоборства в АС представлена на рисунке 2 [1]. С точки зрения системного подхода защищенность информации является свойством системы защиты информации (СЗИ) достигать целевого эффекта при взаимодействии с системой информационного нападения (СИН).

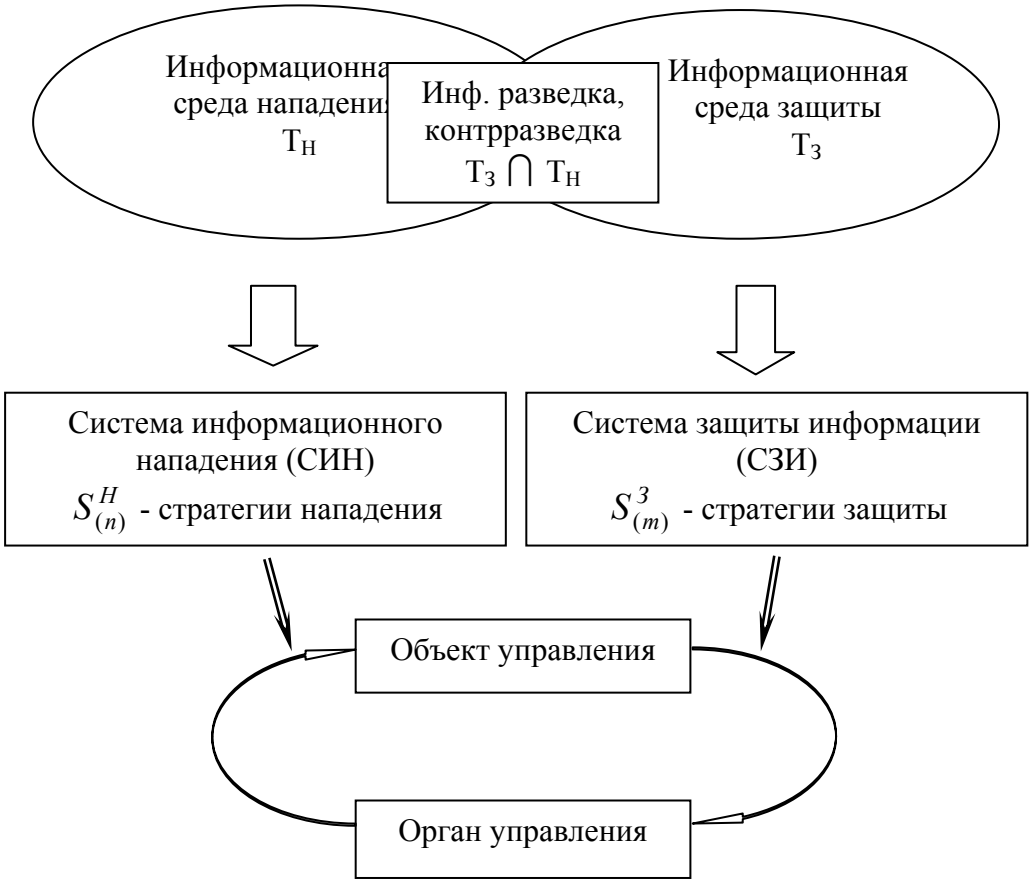

Рисунок 2. Модель информационного противоборства в АС

Степень защищенности информации оценивается значениями соответствующих показателей в фиксированные моменты времени. На практике наиболее часто используется интегральный количественный показатель защищенности *Zu*, который носит вероятностный характер и показывает выигрыш СЗИ на заданном временном интервале [0,T]. Выигрыш СЗИ зависит от двух составляющих [1]:

K – показатель полноты учета возможных стратегий нападения, на которые настроены СЗИ;

R – показатель эффективности заложенных в СЗИ стратегий защиты на интервале [0,T].

$$Zu(T) = F\{K, R(T)\}. \quad (1.1)$$

Если известно распределение вероятностей $K_i, i = \overline{1,n}$ применения СИН всех возможных стратегий нападения, то показатель K может быть представлен в следующем виде

$$K = \sum_{i=1}^{n} k_i, \quad (1.2)$$

где n – количество стратегий нападения, на которые настроена данная СЗИ.

Показатель R, с позиций теории эффективности, можно рассматривать как вероятность выполнения задачи в информационной системе в условиях информационного противоборства при некоторых ограничениях на возмущающие факторы (технические и программные сбои, ошибки, отказы и т.д.)

Таким образом, свойство защищенности информации формируется только в условиях информационного противоборства двух систем - СЗИ и СИН. Для АС предметом противоборства может являться вычислительная система, компьютерная сеть или отдельные (в том числе удаленные) автоматизированные рабочие места (АРМ).

Будем рассматривать лишь информационное противоборство и информированность нападающей и защищающейся сторон, которые определяют сущность управления и принятия решения по защите информации в АС.

Основой информационного противоборства является информированность конфликтующих сторон о действиях друг друга. Каждая из сторон обладает определенной информационной средой (рисунок 2). Под информационной средой нападения T_H или защиты $T_З$ будем понимать общее количество

информации, которой обладает каждая из сторон конфликта [1]. Из информационной среды приемник информации извлекает определенную семантическую информацию, составляющую тезаурус. Тезаурус каждой из сторон конфликта представляет собой совокупность знаний в данной проблемной области. Получение новой информации проявляется в изменении соответствующего тезауруса.

Очевидно, что информационное противоборство возможно только для тех участников конфликта, тезаурусы которых имеют область пересечения. Данная область определяет информационную разведку и контрразведку. Источниками получения информации являются открытые публикации об объектах нападения, результаты работы сетевых анализаторов, сканеров, агентурная работа и т.д. Именно на основе этих сведений формируются соответствующие стратегии нападения $S^{H}_{(n)}$, представляющие собой возможности противника по воздействию на объекты АС и стратегии защиты $S^{З}_{(m)}$ - варианты и последовательность использования механизмов и средств защиты информации (МСрЗИ). Очевидно, что такие исследования должны проводиться с учетом специфики конкретной АС и классификации угроз безопасности функционирования МСрЗИ.

Контур управления защитой информации в АС представлен на рисунке 1. Необходимость образования в этом контуре системы принятия решения по выбору вариантов защиты обусловлена тем, что с увеличением количества угроз безопасности информации со стороны СИН и количества вариантов средств защиты со стороны СЗИ, часто бывает затруднительно сформировать оптимальное решение, определяющее наилучшее управляющее воздействие в данных условиях функционирования АС. Синтез алгоритмов оптимальных управляющих воздействий основывается на математических моделях, методиках и методах, разработка которых представляет собой решение важной научной задачи.

Задача принятия решений характеризуется следующими компонентами [5,6]: цель задачи; множество допустимых альтернатив для решения поставленной задачи; лицо, принимающее решение; критерий оценки степени достижения цели; средства измерения; исходы; решающее правило, отражающее систему предпочтений.

Применительно к задачам управления защитой информации с понятием исходы будем связывать лицо принимающее решение (ЛПР), которое учитывает, что в зависимости от выбранного варианта защиты в условиях воздействия противника, результат будет измеряться по соответствующему критерию, т.е. иметь соответствующую ценность (полезность, выигрыш).

Решающее правило в системе управления защитой информации дает возможность выбрать наиболее предпочтительное решение (с точки зрения минимума потерь защищенности). Решающее правило, отражающее систему предпочтений, определяет алгоритм выбора наиболее предпочтительного решения из множества допустимых альтернатив.

ЛПР для принятия решения по управлению защитой информации использует, как правило, несколько критериев. Для этого необходимо построить численную функцию (так называемую функцию полезности), отражающую предпочтение ЛПР.

В условиях информационного противоборства ЛПР по управлению защитой не имеет полной информации обо всех факторах, влияющих на это решение. Каждое действие может привести к одному из возможных исходов и вероятности этих исходов зачастую бывают неизвестными. Для описания таких систем можно использовать математическую теорию конфликтов, которая называется теорией антагонистических игр.

На практике возникают задачи, когда необходимо принимать решения в условиях неопределенности, в частности, когда две или более сторон преследуют различные цели и результаты действий каждой стороны зависят от действий другой.

Рассматриваются стохастические игровые ситуации с участием двух сторон, преследующих противоположные цели. Принимаемые решения будут направлены на достижение максимальной полезности. Такое поведение индивида в теории игр называют рациональным поведением [1].

Поскольку даже при рациональном поведении существует множество выборов (решений) для достижения цели, возникает задача найти лучшее решение среди множества рациональных решений. Такое решение, если оно существует, называют оптимальным.

Совокупность оптимальных решений составляет оптимальную стратегию, которая служит основой принятия окончательного стратегического решения.

Для описания ситуаций принятия решений по управлению защитой информации, построения адекватных математических моделей большое значение имеет учет степени информированности конфликтующих сторон о целях и возможных вариантах действий соперников. Логичным является использование игровых моделей для формализации понятия информированности сторон конфликта. С этой целью используем игровую модель, учитывающую информационные аспекты, в частности ценность имеющейся информации у игроков, которую они используют для принятия оптимального решения.

Рассмотрим следующую математическую модель принятия решений, учитывающую информационность участников конфликта о намерениях действий сторон.

Математическая постановка задачи. Обозначим через I_1 игру, в которой первый игрок – СЗИ выбирает вариант защиты $i \in M$, а второй игрок – СИН выбирает вариант нападения $j \in N$. Действия сторон происходят одновременно. Примем, что оба участника конфликта знают множества вариантов действий M и N, но им не известен конкретный выборы i и j. Для первой стороны в качестве целевой функции выберем априорную функцию защищенности информации в данной АС - $R_A(j,i)$. Функция $R_A(j,i)$ определена и ограничена на $N \times M$. Обозначим в терминах теории игр число

$S_1 = \sup\limits_{i \in M} \inf\limits_{j \in N} R_A(j,i)$ (верхняя граница $R_A(j,i)$) есть наилучший гарантированный исход в I_1 для СЗИ (нижнее значение игры I_1). Аналогично, I_2 – это игра, в которой СИН выбирает $j \in N$, а затем СЗИ, зная выбор СИН, выбирает $i \in M$. Число $S_2 = \inf\limits_{j \in N} \sup\limits_{i \in M} R_A(j,i)$ (нижняя граница $R_A(j,i)$) есть наилучший гарантированный исход для СЗИ в I_2 (верхнее значение игры I_2).

Игры I_1 и I_2 соответствуют двум крайним уровням информированности СЗИ о выборе СИН. В I_2 есть точная информация о выборе варианта нападения СИН, тогда, как в I_1 известно, что выбор варианта нападения j осуществляется из некоторого множества N. Если реализация S_1 для СЗИ в I_1 не связана с поведением СИН, то для реализации S_2 в I_2 необходимо иметь точную информацию о выборе СИН. Если $S_1 = S_2$, то функция защищенности $R(j,i)$ имеет седловую точку на множестве $N \times M$ (т.е достижение равновесного состояния, от которого не желают отклоняться участники игры; в этом случае говорят, что игры I_1 и I_2 имеют решение в чистых стратегиях). Тогда гарантированный исход S_2 достигается при любом варианте действий СИН. Этот исход достижим СЗИ и в I_1.

Рассмотрим более сложную ситуацию, когда одна из участвующих в информационном противоборстве сторон получает информацию о возможных вариантах действий соперника (назовём ее игра $I_в$).

Пусть подмножество $\{N_k, k \in K\}$ определяет примененную СИН стратегию, причем при всех $k \in K$ выполняется условие $N_k \subseteq N$; $N_k \neq \varnothing$; $\bigcup\limits_{k \in K} N_k = N$.

Содержание игры $I_в$ с информационной структурой $\{N_k, k \in K\}$ состоит в следующем. Сначала СИН выбирает вариант нападения $j \in N$. Затем СЗИ, зная заранее информационную структуру и получив данные о действиях СИН (указывается подмножество N_k), выбирает вариант защиты $i \in M$. Варианты

разбиения множества N на подмножества $N_k, k \in K$ могут быть различными. На основании этого введем множество $K(j)$, где $k \in K(j)$ при условии $k \in K, j \in N$. Значения $k \in K(j)$ и $j \in N$ являются неконтролируемые СЗИ неопределенные факторы. В этом случае игру $Iв$ можно рассматривать как игру с разведкой, которую применяет СЗИ. Результатом разведки является параметр k, смысл которого состоит в том, что СИН применила стратегию нападения j из множества стратегий N_k. При этом множество $K(j)$ рассматривается как множество результатов разведки при условии, что СИН применила стратегию $j \in N$, а $k \in \bigcup_{j \in N} K(j)$ - есть множество всех возможных результатов.

Стратегиями защиты СЗИ в $Iв$ будут функции $i(k)$, определенные на k со значениями в M. Наилучший гарантированный исход для СЗИ в $Iв$ будет число $Sв$

$$Sв = \sup_{i(k)} \inf_{j \in N} \inf_{k \in K(j)} R_A\left(j, i(k)\right) =$$

$$= \sup_{i(k)} \inf_{k \in K} \inf_{j \in N_k} R_A\left(j, i(k)\right) = \inf_{k \in K} \sup_{i \in M} \inf_{j \in N_k} R_A\left(j, i\right). \quad (1.3)$$

Для информационной структуры $\{N_k, k \in K\}$

$$S_1 = \sup_{i \in M} \inf_{j \in N_k} R_A\left(j, i\right), \quad S_2 = \inf_{j \in N} \sup_{i \in M} R_A\left(j, i\right). \quad (1.4)$$

Как было принято ранее, наилучший гарантированный исход в I_1 для первого игрока (СЗИ) $S_1 = \sup_{i \in M} \inf_{j \in N_k} R_A\left(j, i\right), k \in K$.

Аналогично, в I_2 наилучший гарантированный исход для СЗИ $S_2 = \inf_{j \in N_k} \sup_{i \in M} R_A\left(j, i\right), k \in K$.

Так как $S_1 = \inf_{k \in K} S_1(k)$, $S_2 = \inf_{k \in K} S_2(k)$ и $S_2(k) \geq S_1(k)$, для всех $k \in K$, то $S_1 \leq Sв \leq S_2$.

Введем величину $C_1 = Sв - S_1$ - ценность информации, получаемой от разведки СЗИ. Величина $C_2 = S_2 - Sв$ показывает насколько информация в игре I_2 ценнее информации, получаемой от разведки в игре I_r.

При $S_1 = Sв$ имеем $C_1 = C_2 = 0$, то есть информированность участников конфликта о действиях сторон отсутствует.

ЛИТЕРАТУРА

1. Гаценко О.Ю. Защита информации. Основы организационного управления: моног. - СПб.: Изд. дом «Сентябрь», 2001. - 228 с.

2. Симанков В.С., Сундеев П.В. Системный анализ функциональной стабильности критических информационных систем: моног. - Краснодар: КубГТУ, ИСТЭК, 2004. - 204 с.

3. Северцев Н.А. Системный анализ и моделирование безопасности. - М:Высшая школа, 2006 г., - 462 с.

4. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. - М.: Гелиос АРВ, 2005. - 224 с.

5. Орлов, А.И. Теория принятия решений: учеб. - М.: Экзамен, 2006. - 575с.

6. Петровский, А. Б. Теория принятия решений : учеб.: рек. УМО. - М.: Академия, 2009. - 400 с.

REFERENCES

1. Gacenko O.Ju. Zashhita informacii. Osnovy organizacionnogo upravlenija: monog. - SPb.: Izd. dom «Sentjabr'», 2001. - 228 p.

2. Simankov V.S., Sundeev P.V. Sistemnyj analiz funkcional'noj stabil'nosti kriticheskih informacionnyh sistem: monog. - Krasnodar: KubGTU, ISTJeK, 2004. - 204 p.

3. Severcev N.A. Sistemnyj analiz i modelirovanie bezopasnosti. - M:Vysshaja shkola, 2006 g., - 462 p.

4. Shumskij A.A., Shelupanov A.A. Sistemnyj analiz v zashhite informacii. - M.: Gelios ARV, 2005. - 224 p.

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

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

MATHEMATICAL MODELING OF INFORMATION SECURITY MANAGEMENT SYSTEMS PROCESSES, BASED ON GAME THEORY AUTOMATED METHODS

V.A. KUCHER, E.S. TARASOV

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: vakucher@bk.ru

This article describes an approach to the use of methods of game theory for optimization and simulation of safety management systems and processes, automated incident response: mathematical formulation of the problem, a formal description of the used games, and appropriate management strategies to protect information systems tailored to specific objects of protection.

Key words: decision-making, security management, game theory, information warfare, security strategy.