УДК 007:519.876.5

СТРУКТУРА ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ВОЗНИКАЮЩИХ КОНФЛИКТНЫХ СИТУАЦИЙ

Ю.Ю. Громов[1], В.О. Драчев[2], Л.Н. Сырицын[2]

Кафедра «Информационные системы», ТГТУ (1);
Воронежский институт высоких технологий (2)

Ключевые слова и фразы: защищенность; интеллектуальная информационная система; конфликтная ситуация; модель безопасности информации; синтез; современные системы защиты информации; целевая функция.

Аннотация: Рассмотрены некоторые вопросы безопасности и защищенности в информационных системах. Проанализированы существующие подходы защищенности информационных систем. Выявлен ряд проблемных вопросов. На основе политики безопасности выработаны направления разработки новых моделей безопасности информации и методов построения защищенных информационных систем.

Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл информационных систем (**ИС**) от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации.

Рассматривая вопросы безопасности информации в информационных системах, можно говорить о наличии некоторых «желательных» состояний данных систем. Эти желательные состояния описывают «защищенность» системы. Понятие «защищенности» принципиально не отличается от любых других свойств технической системы, например «надежной работы», и является для системы внешним, априорно заданным [1].

Интегральной характеристикой защищенности информационных систем является политика безопасности – качественное или качественно-количественное выражение свойств защищенности в терминах, представляющих систему [1].

Важно заметить, что политика безопасности выражает в общем случае нестационарное состояние защищенности. Защищаемая система может изменяться, дополняться новыми компонентами. Очевидно, что политика безопасности должна быть поддержана во времени, следовательно, должны быть определены процедуры управления безопасностью.

С другой стороны, нестационарность защищаемой ИС, а также вопросы реализации политики безопасности в конкретных конструкциях защищаемой системы предопределяют необходимость рассмотрения задачи гарантирования заданной политики безопасности.

Существующие подходы к описанию защищенности базируются на анализе типовых ситуаций и действующих в них закономерностей. Применение таких подходов к сложным информационным системам приводит к тому, что становится невозможным получить свойство целого, исследуя его части.

В связи с этим возникают проблемные вопросы по применению моделей безопасности при выбранной политике безопасности информации.

Несмотря на многообразие средств защиты (**СЗ**) информации, условий их функционирования и взаимодействия, можно выделить общие для них свойства, наиболее существенными из которых являются старение и обновление. Такими же свойствами наделена сама защищаемая информация, обладающая также свойствами концентрации и рассеяния. Существующие методы построения защищенных информационных систем в настоящее время носят описательный характер и не учитывают динамику их изменения во времени [2].

Существование ненулевой вероятности невыполнения системой защиты информации своей целевой функции приводит к тому, что все элементы обязаны реагировать на изменение защищённости и должны менять в соответствии с этим свою поведенческую тактику и стратегию.

В связи с этим немаловажное значение приобретают системные исследования применения существующих, разработки новых моделей безопасности информации и методов построения защищенных информационных систем, а так же выбора их на основе политики безопасности информации.

На современном этапе развития систем защиты информации любая ее модель основывается на определении политики безопасности, которая является руководством при проектировании и эксплуатации.

Согласно требованиям большинства критериев оценки безопасности, системы защиты информации должны строиться на основе определенных математических моделей, с помощью которых должно быть теоретически обосновано соответствие системы защиты требованиям заданной политики безопасности

В настоящее время наиболее часто рассматриваются четыре модели безопасности информации [2].

1. **Модель матрицы доступов HRU** используется для анализа системы защиты, реализующей дискреционную политику безопасности, и ее основного элемента – матрицы доступов. При этом система защиты представляется конечным автоматом, функционирующим согласно определенным правилам перехода.

2. **Модель «Take–Grant»** используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа. В качестве основных элементов модели используются граф доступов и правила его преобразования. Цель модели – дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов. В настоящее время модель «Take–Grant» получила продолжение как расширенная модель "Take–Grant", в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

3. **Модель «Белла–Лападула»** (классическая модель) построена для анализа систем защиты, реализующих мандатное (полномочное) разграничение доступа.

4. **Модель «Low–Water–Mark»** представляет близкий к модели «Белла–Лападула» подход к определению свойств системы безопасности, реализующей мандатную (полномочную) политику безопасности. В модели предлагается порядок безопасного функционирования системы в случае, когда по запросу субъекта ему всегда необходимо предоставлять доступ на запись в объект.

Разработанные модели политик безопасности информации опираются на иерархическую декомпозицию уровней защиты. Верхний уровень иерархии составляет политика безопасности со своими специфическими методами ее анализа. Следующий уровень – основные системы поддержки политики безопасности (мандатный контроль, аудит и т.д.). Затем следует уровень механизмов защиты (криптографические протоколы, криптографические алгоритмы, системы создания защищенной среды, системы обновления ресурсов и т.д.), которые позволяют реализовать системы поддержки политики безопасности. Самый низкий уровень – реализация механизмов защиты (виртуальная память, теговая архитектура, защищенные режимы процессора и т.д.) [2].

Анализ перечисленных моделей политик безопасности выявляет ряд недостатков в построении современных систем защиты информации. Так не существует четких рекомендаций, определяющих применение соответствующей модели безопасности при построении различных информационных систем.

Так, во-первых, существующие модели безопасности, а соответственно построенные на их основе политики безопасности выбираются не на основании четких правил по выбору соответствующих условиям построения информационных систем, а на основе интуитивных рассуждений.

Во-вторых, ни одна из моделей не дает адекватной оценки эффективности применения комплекса средств защиты в разнородных вычислительных сетях.

Это происходит из-за того, что не учитываются:

– особенности воздействия внешней среды на систему защиты информации, которые изменяются во времени (обладают свойством старения и обновления);

– динамические характеристики изменения самой защищаемой информации и выбранного комплекса средств защиты;

– процессы по рассеянию и концентрации защищаемой информации, снижению ее оперативной ценности (то есть своевременности получения информации), динамика процессов старения и обновления.

Проблема обеспечения заданного уровня защиты информации требует для своего решения не просто осуществления некоторой совокупности научно-технических мероприятий и применения специфических средств и методов, но и создания целостной системы организационных мероприятий, а также применения специфических средств и методов защиты информации [3], суть, которых сводится к возрастанию роли следующих направлений деятельности по обеспечению информационной безопасности:

– формирование, направление и рациональное управление информационными ресурсами;

– выявление угроз информационной безопасности и их источников;

– обеспечение информационных прав, их защита от негативных информационных воздействий;

– защита информации от различных видов угроз и возможных несанкционированных доступов и воздействий.

Построение защищенных информационных систем осуществляется в условиях постоянно возникающих потенциальных конфликтных ситуациях (**ПКС**) [4].

Анализ возникающих потенциальных конфликтных ситуаций при построении системы защиты информации в информационных системах предполагается рассматривать на основе системного исследования, суть которого состоит:

– в описании последовательности применения моделей безопасности при построении защищенной системы с учётом всех существующих факторов обнаружения и исследования потенциальных конфликтных ситуаций, механизмов конфликта;

– в предположении, что причина и характер конфликта известны, выделить главный фактор для оценки значимости результатов конфликта.

Для того чтобы построить системную модель конфликтного взаимодействия необходимо:

– ввести множество показателей качества;

– сформировать функциональное пространство системы, определить метрику;

– определить зависимость между показателями качества в функциональном пространстве системы.

Конфликтные зависимости могут иметь так же важные общие свойства [4]:

– многоаспектность оценки;

– возможность скачка (переход из одного устойчивое состояние в другое через временную неустойчивость): при некоторых условиях интенсивность взаимодействия изменяется скачком, хотя эффективности по своей природе такого изменения не допускают;

– многоэкстремальность: в области изменения эффективности конфликтующих моделей интенсивность взаимодействия может иметь несколько максимумов и минимумов;

– неоднозначность: интенсивность взаимодействия может иметь различную зависимость от эффективности конфликтующих моделей;

– неопределенность: в области изменения эффективностей конфликтующих моделей интенсивность взаимодействия может принимать множество, которые неопределимы.

Кроме того, при рассмотрении конфликта возникают следующие виды неопределенности.

1. Незнание конкретных значений случайных величин или функций, которых известны статические и вероятностные свойства. Для конфликта имеют значение не усредненные, а конкретные значения величин и функций.

2. Незнание вида некоторых детерминированных функций, их численных характеристик и значений констант, описывающих внутрисистемные и несистемные процессы, приводит к необходимости аппроксимации.

3. Незнание некоторых факторов, влияющих на ход конфликта, приводит к усредненным описаниям.

4. Невозможность точно учесть все факторы, хотя эти факторы и их характеристики точно изучены.

Для построения интеллектуальной информационной системы в условиях возникающих конфликтных ситуаций необходимо с системных позиций рассмотреть блочную структуру процесса построения защищённой информационной системы.

Технологию принятия решения по применению необходимой политики безопасности на основе существующих и синтезируемых моделей безопасности с последующим применение полученной политики безопасности к информационной системе можно представить в виде обобщенной структуры, изображенной на рис. 1. Здесь представлены взаимосвязи выделенных технологических задач всех уровней на основных этапах принятия решения по применению модели безопасности информации при разработке политики безопасности для предложенной интеллектуальной информационной системы в условиях возникающих потенциальных конфликтных ситуаций между ее элементами.

Предлагается синтезировать логические цепочки, определяющие последовательность действий при анализе возникающих конфликтных ситуаций между элементами системы, защиты информации и принятия решения в условиях конфликта.

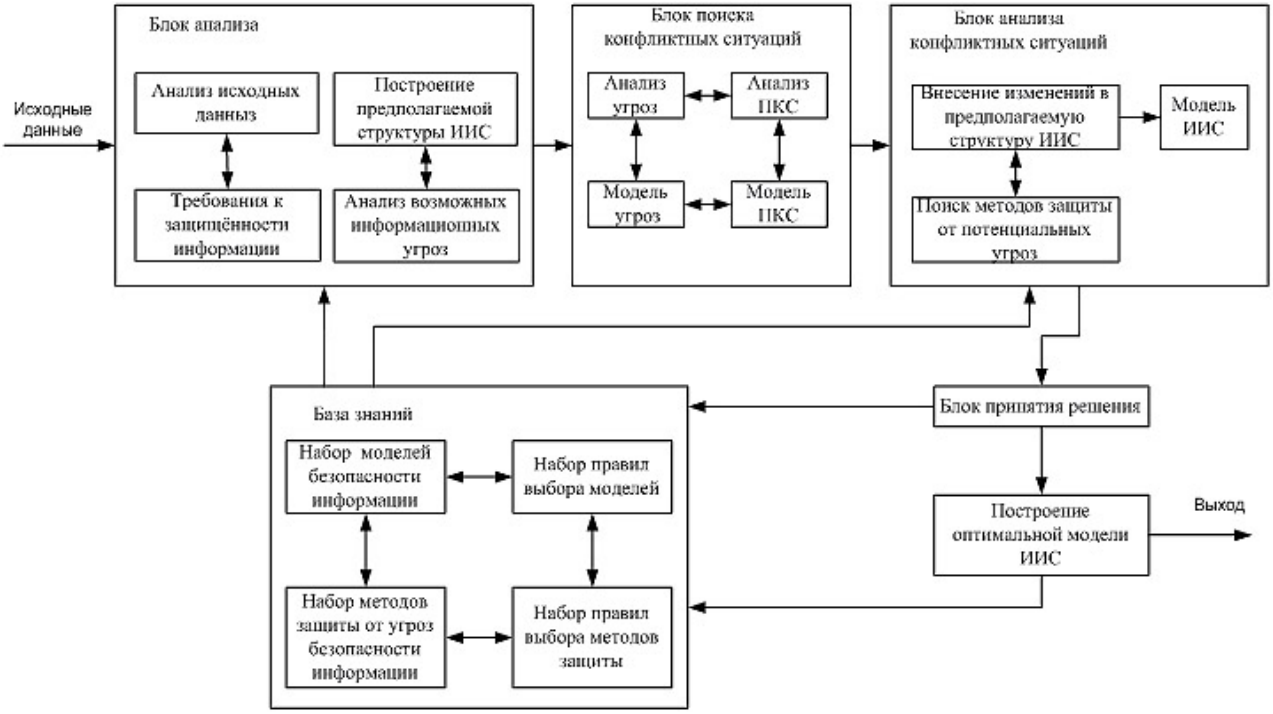

Рис. 1. Блочная структура интеллектуальной информационной системы принятия решений в условиях возникающих конфликтных ситуаций

Для этого обосновывается необходимость формирования состава процедур анализа и диагностики, определения иерархии самих процедур.

В состав предлагается включать:

– оценивание параметров функционирования системы по случайной выборке;

– анализ технологической системы по уровню настройки, точности воспроизведения и структуре связей параметров;

– определение скрытых факторов и причинных взаимосвязей параметров;

– генерирование режимов функционирования системы.

Конфликт определяет сущность системы, ее живучесть и способность к развитию. Поэтому анализ предлагается проводить по, так называемым, ядрам конфликта, который заключается в изучении свойств и поведения в различных условиях функционирования системы путем сравнения ядер конфликта и причинного анализа. Сравнение ядер конфликта позволяет решать следующие основные задачи анализа [5]:

– оценка влияния входных, выходных и структуры связей параметров на эффективность функционирования системы в условиях возникающих конфликтных ситуаций;

– установление механизмов взаимодействия входных и выходных параметров; изучение особенностей функционирования технологической системы в экстремальных условиях;

– определение общих и специфических особенностей развития системы с учетом взаимодействия с внешней средой.

Помимо решения собственно задач анализа, выделение ядер конфликта может быть использовано как средство сокращения выборки параметров, что приводит к значительной экономии затрат на проведение анализа

Заключительным этапом является процесс принятия решений, который заключается в выборе и оценке наилучших вариантов построения ИИС в различных условиях.

Поскольку количество возможных альтернативных вариантов бывает очень велико, а между основными показателями эффективности, как правило, наблюдается конфликт, то возникает проблема выбора, которая приводит к необходимости привлечения экспертов. К сожалению, эксперты не в состоянии одновременно оценивать и сравнивать большое число вариантов. Если же разбить исходную совокупность вариантов на порции допустимого объема, то, переходя от порции к порции, эксперты очень скоро начнут противоречить сами себе. Поэтому предлагается механизм определения экспертных предпочтений по ограниченной выборке с их последующей экстраполяцией на всю исходную совокупность. В результате на последнем этапе анализа решаются следующие задачи [5]:

– установление цели и критериев развития и функционирования ИИС;

– выбор и обоснование критериев эффективности;

– расчет критериев эффективности и упорядочивание вариантов функционирования ИСС;

– формирование множества возможных альтернативных решений.

В результате вышесказанного можно говорить о постановке задачи на проведение исследовательских работ, связанных с изучением возможности создания методологии синтеза интеллектуальной информационной системы принятия решения в условиях возникающих потенциальных конфликтных ситуациях при построении защищенных интеллектуальных информационных систем. Результатом решения данной задачи будет являться методология построения защищенной системы в условиях неопределенности выбора модели безопасности информации.

Для этого необходимо:

– проанализировать причины возникновения потенциальных конфликтных ситуаций для построения интеллектуальной информационной системы;

– формализовать возникающие потенциальные конфликтные ситуаций в процессе построения защищенных систем;

– разработать методы выявления, возникающих потенциальных конфликтных ситуаций в процессе построения защищенных систем;

– синтезировать структуру и алгоритмическое обеспечение интеллектуальной информационной системы принятия решения;

– исследовать и оценить риск при разработке алгоритмического обеспечения ИИС принятия решения.

Список литературы

1. Завгородний, В.И. Комплексная защита информации в компьютерных системах / В.И. Завгородний. – М. : Логос; ПБОЮЛ Н.А. Егоров, 2001. – 254 с.

2. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М. : Горячая линия–Телеком, 2000. – 98 с.

3. Проектирование информационных систем / под ред. Курбакова. – М. : Изд-во Рос. экон.акад., 2000. – 348 с.

4. Сысоев, В.В. Конфликт в структурном представлении систем / В.В. Сысоев, И.Г. Амрахов. – Воронеж : ГТА, 1997. – 218 с.

5. Сысоев, В.В. Конфликт. Сотрудничество. Независимость. Системное взаимодействие в структурно-параметрическом представлении / В.В. Сысоев. – М. : Москов. акад. эконом. и права, 1999. – 312 с.

SYSTEM OF DECISION MAKING IN CONFLICT SITUATIONS

Yu.Yu. Gromov, V.O. Drachev, L.N. Syritsin

Key words and phrases: immunity; intelligent information system; conflict situation; information safety model; synthesis; modern systems of information protection; target function.

Abstract: Some issues of information systems safety and protection are considered. The existing approaches to information systems protection are analyzed. Some problems are discussed. Based on safety policy some directions for new information safety and protection models design and methods of protected information systems construction are developed.