на правах рукописи

Нестеров Сергей Александрович

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ПРОЕКТИРОВАНИЯ ИНФРАСТРУКТУРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специальность:

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург

2002

Работа выполнена в Санкт-Петербургском государственном техническом университете.

Научный руководитель:
доктор технических наук, профессор Козлов В.Н.

Официальные оппоненты:
доктор технических наук, профессор Птицына Л.К.
доктор технических наук, профессор Сычев М.П.

Ведущая организация:
Санкт-Петербургский институт информатики и автоматизации РАН

Защита диссертации состоится «___» июня 2002 г. в $16^{\underline{00}}$ часов на заседании диссертационного совета Д 212.229.22 Санкт-Петербургского государственного технического университета по адресу:
195251, Санкт-Петербург, Тихорецкий пр., 21, ЦНИИ РТК.

С диссертацией можно ознакомиться в фундаментальной библиотеке Санкт-Петербургского государственного технического университета.

Автореферат разослан «___» _____ 2002 г.

Ученый секретарь диссертационного совета
д.т.н., проф. Шашихин В.Н.

Общая характеристика работы.

Актуальность. Широкое распространение в государственных структурах, на предприятиях и в организациях автоматизированных систем обработки информации (АС) и важность задач обеспечения целостности, конфиденциальности и доступности обрабатываемых в них данных, определяют актуальность вопросов, связанных с обеспечением информационной безопасности (ИБ) АС.

Сделанные на этапе проектирования инфраструктуры обеспечения ИБ АС ошибки в определении необходимого уровня защищенности, распределении ресурсов, выборе средств и механизмов защиты, могут негативно повлиять на функциональность подсистемы защиты в целом. Поэтому при проектировании особенно важно использовать научно обоснованные формальные методы. Разработке подобных методов и посвящена настоящая работа.

Диссертационная работа опирается на исследования таких отечественных и зарубежных ученых, как В.А.Герасименко, П.Д. Зегжда, А.А.Малюк, Б.П. Пальчун, Б.А. Погорелов, М.П. Сычев, Л.М. Ухлинов, Р.М. Юсупов, Л. Хоффман, Т. Оловсон и др. В ней развиваются отдельные положения известных работ применительно к задаче проектирования подсистемы защиты АС. В частности, разработан метод формирования проектов инфраструктуры обеспечения ИБ по заданному описанию АС и набору функциональных требований к подсистеме защиты. Предложен и обоснован теоретико-игровой подход к задаче выбора внедряемого проекта. Разработанные теоретические методы реализованы в прототипе системы поддержки принятия решений в области построения инфраструктуры обеспечения ИБ АС.

Целью работы является создание взаимосвязанных методов синтеза проектов инфраструктуры обеспечения ИБ и анализа их ожидаемой эффективности.

Для достижения поставленной цели в работе решались следующие задачи:

- анализ существующих подходов к построению инфраструктуры обеспечения ИБ АС;
- разработка теоретико-множественной модели для описания состава и структуры АС, предъявляемых к ней требований в области безопасности, доступных средств и механизмов обеспечения ИБ;
- разработка метода синтеза проектов инфраструктуры обеспечения

информационной безопасности по заданному описанию АС и заданным требованиям;

- обоснование применимости методов математической теории игр для выбора оптимального проекта и разработка игровой модели конфликта «защитник-нарушитель»;
- апробация предложенных методов путем создания на их базе прототипа системы поддержки принятия решений в области проектирования инфраструктуры обеспечения ИБ АС.

Предметом исследования является процесс построения инфраструктуры обеспечения ИБ АС.

Методы исследования. Для решения поставленных в работе задач использовались методы теории множеств, теории графов, математической теории игр, методы интервального исчисления, системного анализа, теории реляционных баз данных и объектно-ориентированного программирования.

Научная новизна диссертационной работы заключается в следующем:

1. Разработана теоретико-множественная модель, описывающая состав и структуру защищаемой АС, предъявляемые требования к уровню защищенности, доступные средства и механизмы обеспечения ИБ.
2. Разработан метод синтеза проектов инфраструктуры обеспечения ИБ по заданному описанию АС, выдвинутым функциональным требованиям и ограничениям. Метод базируется на алгоритме поиска с возвратом.
3. Разработана одношаговая конечная игровая модель конфликта «защитник-нарушитель», исследование которой позволяет сделать обоснованный выбор проекта инфраструктуры обеспечения ИБ на базе оценок стоимости проекта и ожидаемых потерь от реализации угроз ИБ. Предложено решение задачи выбора проекта для случая интервальных оценок потенциальных потерь от реализации угроз ИБ АС.
4. Разработан прототип программной системы поддержки принятия решений в области проектирования инфраструктуры обеспечения ИБ АС.

Практическая ценность работы заключается в том, что использование предложенных методов при проектировании подсистемы защиты АС позволяет научно обосновать выбор необходимого уровня защищенности, алгоритмизировать

процесс формирования проекта подсистемы защиты и сократить количество возможных ошибок при проектировании.

Результаты работы использованы в исследованиях по гранту, выполненному в рамках программы Министерства образования РФ и Фонда содействия развитию малых форм предприятий в научно-технической сфере "Студенты и аспиранты - малому наукоемкому бизнесу (Ползуновские гранты)" (2001г.).

Разработан учебный курс «Информационная безопасность и защита информации» для студентов, обучающихся по направлению бакалаврской и магистерской подготовки «Системный анализ и управление» (акт об использовании от СПбГТУ).

Апробация работы. Основные результаты и положения работы обсуждались на Всероссийской научно-технической конференции «Фундаментальные исследования в технических университетах» (Санкт-Петербург, 1999г.), межрегиональной конференции «Информационная безопасность регионов России» (Санкт-Петербург, 1999г.), Российской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2000г.), Политехническом симпозиуме «Молодые ученые – промышленности Северо - Западного региона» (Санкт-Петербург, 2000, 2001 гг.), Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы» (Москва, 2001г.), научно-технической конференции «Безопасность информационных технологий» (Пенза, 2001г.), Всероссийской научно-практической конференции «Студенты и аспиранты – малому наукоемкому бизнесу (Ползуновские гранты)» (Казань, 2001 г.).

Проекты, реализованные в рамках работы над диссертацией, в 2000 и 2001 годах побеждали на Санкт-Петербургском конкурсе персональных грантов для студентов, аспирантов, молодых ученых и специалистов.

Публикации. По теме диссертации опубликовано 10 работ.

Основные положения, выносимые на защиту.

1. Теоретико-множественная модель, описывающая состав и структуру защищаемой АС, предъявляемые требования к уровню защищенности, доступные средства и механизмы обеспечения безопасности.
2. Метод синтеза проектов инфраструктуры обеспечения ИБ по заданному

описанию АС, выдвинутым функциональным требованиям и ограничениям.

3. Игровая модель конфликта «защитник-нарушитель».
4. Прототип программной системы поддержки принятия решений в области проектирования инфраструктуры обеспечения ИБ АС.

Объем и структура работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы и двух приложений.

Содержание работы.

Введение посвящено краткой характеристике работы. В нем обоснована актуальность рассматриваемой проблемы, коротко описаны методы ее решения, перечислены основные результаты, полученные в диссертации.

Глава 1 содержит обзор литературы и анализ комплекса проблем, связанных с построением инфраструктуры обеспечения ИБ АС. Описаны базовые понятия и основные принципы обеспечения ИБ, рассмотрены существующие подходы к проектированию подсистем защиты АС, проведен обзор математических моделей, описывающих различные этапы проектирования подсистемы защиты АС. Особое внимание уделено отечественным и зарубежным нормативным документам, регламентирующим деятельность в сфере ИБ. В заключение главы дается уточненная постановка задач, решаемых в диссертационной работе.

Под инфраструктурой обеспечения ИБ в работе понимается совокупность физических, технических и программных средств и механизмов, создаваемая и поддерживаемая для обеспечения защиты АС от угроз ИБ. В качестве синонима в работе также используется термин «подсистема защиты АС». Определяемый в руководящих документах Гостехкомиссии России термин «комплекс средств защиты» является более узким, т.к. обозначает только совокупность средств защиты от несанкционированного доступа к информации.

В ходе эволюции подходов к задаче обеспечения ИБ был выработан ряд принципов, которые необходимо учитывать как при эксплуатации АС, так и в процессе разработки инфраструктуры обеспечения ИБ. К ним относятся принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления и применения, открытости алгоритмов и механизмов защиты,

простоты применения защитных мер и средств. В частности, принцип разумной достаточности постулирует, что создать абсолютно непреодолимую систему невозможно, поэтому важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

Процесс построения инфраструктуры обеспечения ИБ АС можно условно разделить на два этапа:

1. Определение на качественном уровне структуры и состава подсистемы защиты АС.
2. Определение оптимальных количественных характеристик подсистемы защиты, в частности, ее стоимостных показателей.

Первый этап может быть описан в терминах модели, аналогичной разработанной Л. Хоффманом модели системы безопасности с полным перекрытием. Суть ее заключается в том, что с каждым объектом АС, требующим защиты, связывается подмножество угроз ИБ, которые может реализовать нарушитель в отношении данного объекта. Система обеспечения ИБ строится таким образом, чтобы создать «барьеры», препятствующие осуществлению всех выявленных угроз. Однако исследование данной модели не дает ответа на вопрос о необходимом уровне защищенности АС и требуемых затратах на защиту.

Для решения этих задач используются так называемые стоимостные модели. К ним, в частности, относится стоимостная модель «защитник-нарушитель». Она основана на представлении потерь защитника (владельца АС) и прибыли нарушителя в виде дифференцируемых функций от затрат на защиту АС и стоимости организации атаки на нее. На основе необходимых условий экстремума определяются уравнения, решение которых позволяет разработчику подсистемы защиты найти оптимальный объем затрат на приобретение средств обеспечения ИБ. Недостаток модели заключается в том, что на практике получить используемые в ней зависимости не всегда возможно. Данная модель также не позволяет учесть тот факт, что затрачиваемые на защиту средства могут быть распределены различным образом (направлены на приобретение различных по эффективности средств защиты).

В работах отечественных авторов (В.А.Герасименко, А.А.Малюка) высказывается предположение о перспективности теоретико-игровой интерпретации конфликта «защитник-нарушитель», которое развито в диссертационной работе. При

таком подходе, множество игровых стратегий защитника формируется на базе множества проектов подсистемы защиты информации: игровая стратегия заключается в реализации одного из возможных проектов. Таким образом, этапу построения и анализа игры должно предшествовать формирование проектов подсистемы защиты. Существенное влияние на этот процесс оказывают стандарты, действующие в сфере ИБ.

В диссертационной работе кратко описаны требования таких стандартов, как руководящие документы Гостехкомиссии России (Показатели защищенности средств вычислительной техники от несанкционированного доступа и Критерии защищенности автоматизированных систем обработки данных) и Общие критерии безопасности информационных технологий. Выполнен анализ структуры определяемых этими нормативными актами требований к подсистеме защиты АС.

Для реализации сформулированного выше принципа разумной достаточности, началу разработки подсистемы защиты информации должна предшествовать оценка объема потенциальных потерь от различных угроз ИБ АС. Подобную оценку включает в себя анализ рисков, по результатам которого может быть принято решение об уменьшении риска, уклонении от риска, изменении характера риска или его принятии.

На данный момент единой общепризнанной методики анализа рисков нет ни в России, ни за рубежом. Различия проявляются даже на уровне базовых подходов: если британская методика CRAMM нацелена на получение оценки рисков на качественном уровне (ранжирование рисков), то при использовании таких инструментальных средств, как @Risk, предполагается получения количественной оценки степени риска. Есть инструментальные средства, сочетающие оба подхода (например, RiskWatch). Для построения игровой модели конфликта «защитник-нарушитель» требуются количественные оценки риска, на базе которых определяется функция выигрыша.

В результате проведенного анализа литературы были выделены задачи, решаемые в ходе работы над диссертацией:

1. Разработка формальной модели, описывающей защищаемую АС, требования в области ИБ, доступные средства и механизмы защиты;
2. Разработка метода синтеза проектов инфраструктуры обеспечения ИБ АС;

3. Построение теоретико-игровой модели, позволяющей определить оптимальный проект подсистемы защиты АС;
4. Создание программного обеспечения, реализующего разработанные методы.

Глава 2 диссертационной работы посвящена описанию разработанных теоретических моделей, представляющих различные аспекты процесса проектирования подсистемы защиты АС.

Синтез проектов подсистемы защиты предлагается проводить по следующей схеме. Сначала в рамках разработанной теоретико-множественной модели производится описание АС, доступных средств защиты и предъявляемых к системе требований, после чего строится множество «допустимых» проектов. Далее проводится исследование полученного множества проектов в рамках теоретико-игровой модели, по результатам которого определяется оптимальный по соотношению затрат и ожидаемого эффекта проект подсистемы защиты.

Краткое описание элементов теоретико-множественной модели приведено в табл.1. Предполагается, что защищаемая АС логически разделена на зоны безопасности – области, в которых действуют единые требования к уровню безопасности и функциональности подсистемы защиты АС. В частном случае такая зона может быть только одна.

В рамках зоны безопасности требования к уровню защищенности определяются выбранным для нее набором функциональных требований. Набор требований $p \in \mathbf{P}$ описывается в модели множеством пар $<r_i,v_i>$, где $r_i \in \mathbf{R}$ – название требования, $v_i \in \mathbf{V_i}$ – соответствующее требованию значение. Множество $\mathbf{V_i}$ (множество значений, которые могут быть сопоставлены требованию r_i) линейно упорядочено отношением "≤". Запись $v'_i \le v''_i$ означает, что требование $<r_i,v''_i>$ является не менее строгим, чем $<r_i,v'_i>$ (здесь $r_i \in \mathbf{R}$; $v'_i, v''_i \in \mathbf{V_i}$). Набор требований может формироваться, например, на основе Профиля защиты «Общих критериев».

Множество **P** частично упорядоченно отношением "≤": если $p',p'' \in \mathbf{P}$ и $p'=\{<r_1,v'_1>,\ldots,<r_m,v'_m>\}$, $p''=\{<r_1,v''_1>,\ldots,<r_m,v''_m>\}$, то $p' \le p'' \Leftrightarrow v'_k \le v''_k \ \forall\, k \in \{1,...,m\}$.

Таблица 1. Элементы теоретико-множественной модели

Название	Описание
Множество зон безопасности в АС	**Z**
Множество требований к подсистеме обеспечения ИБ	**R**
Множество значений для требования $r_i \in \mathbf{R}$	$\mathbf{V_i}=\{v_i\}$, задана операция ≤, множество линейно упорядочено
Множество наборов требований	$\mathbf{P}=\{p \mid p=\{<r_i,v_i>\}, r_i \in \mathbf{R}, v_i \in \mathbf{V_i}\}$
Задание на разработку подсистемы обеспечения ИБ в АС	$\mathbf{T}=\{t \mid t=<z,\mathbf{P'},\mathbf{R'}>, z \in \mathbf{Z}, \mathbf{P'} \subseteq \mathbf{P}, \mathbf{R'} \subseteq \mathbf{R}\}$ Для $\forall z'' \in \mathbf{Z}$ $\exists t'' \in \mathbf{T} \mid t''=<z'',\mathbf{P''},\mathbf{R''}>$, $\mathbf{P''} \subseteq \mathbf{P}$, $\mathbf{R''} \subseteq \mathbf{R}$
Множество аппаратных платформ	**H**
Множество операционных систем	**OS**={os | os=<os_name, os_ver>}
Встроенные механизмы защиты операционных систем	**OSS**={oss | oss=<os, **RV**, **SERT**>} $os \in \mathbf{OS}$, $\mathbf{RV}=\{<r_i,v_i> \mid r_i \in \mathbf{R}, v_i \in \mathbf{V_i}\}$, **SERT** – множество сертификатов, подтверждающих функциональность механизмов защиты
Множество универсального программного обеспечения (ПО)	**S**={s | s=<s_name, s_ver, **H_OS** >}, где $\mathbf{H\_OS}=\{<h,os> \mid h \in \mathbf{H}, os \in \mathbf{OS}\}$
Встроенные механизмы защиты ПО	**SS**={ss | ss=<s, **RV**, **SERT**>}
Множество специализированных средств защиты	**SEC**={sec | sec=<sec_name, sec_ver, **H_OS**, **RV**, **SERT**, cost>}
Множество элементов АС	$\mathbf{E}=\{e \mid e=<name, h, os, \mathbf{S'}, \mathbf{Z'}, \mathbf{R'}, N>, h \in \mathbf{H}, os \in \mathbf{OS}, \mathbf{S'} \subseteq \mathbf{S}, \mathbf{Z'} \subset \mathbf{Z}, \mathbf{R'} \subseteq \mathbf{R}\}$ name – название элемента; **S'** – установленное ПО; **Z'** – зоны безопасности, к которым относится элемент; **R'** – множество требований к защите, которые нужно выполнить в отношении данного элемента; N – число однотипных элементов в данной зоне.

Структура задания на разработку подсистемы защиты АС (в табл.1 - **T**) позволяет для одной зоны указать несколько допустимых наборов требований $p \in \mathbf{P}$, которые формируют подмножество $\mathbf{P'} \subseteq \mathbf{P}$. При построении проекта подсистемы защиты из них выбирается один. В задании каждой зоне безопасности сопоставляется подмножество требований $\mathbf{R'} \subseteq \mathbf{R}$, которые должны быть выполнены для зоны в целом (например, требования по физической защите помещений).

Часть проекта подсистемы защиты АС для одной зоны предлагается строить следующим образом. Пусть зоне $z \in \mathbf{Z}$ в задании сопоставлен элемент $t=<z,\mathbf{P'},\mathbf{R'}>$ и выбран набор требований $p' \in \mathbf{P'}$. Подмножество $\mathbf{p^{(1)}}$ – требования, которые надо выполнить в отношении всей зоны – определяется следующим образом:

$$\mathbf{p^{(1)}}=\{<r,v>|\ r \in \mathbf{R'},\ <r,v> \in \mathbf{p'}\},$$
$$(\forall r \in \mathbf{R'})\ \&\ (\exists v\ |\ <r,v> \in \mathbf{p'}) \Rightarrow <r,v> \in \mathbf{p^{(1)}}.$$

Иными словами, если требование r относится к рассматриваемой зоне z «в целом» и оно вместе с соответствующим значением v входит в выбранный для данной зоны набор **p'**, то элемент <r,v> включается в подмножество $\mathbf{p^{(1)}}$.

Для реализации этих требований необходимо использовать подмножество средств защиты (СЗ) $\mathbf{sec^{(i)}}$ (индекс i указывает порядковый номер), отвечающее следующим условиям:

$$\mathbf{sec^{(i)}} \subseteq \mathbf{SEC}\ ,\ \text{для}\ \forall <r,v> \in \mathbf{p^{(1)}}\ \exists\ sec=<\ldots,\ \mathbf{RV},\ \ldots> \in \mathbf{sec^{(i)}}\ |\ (\exists\ <r,v'> \in \mathbf{RV}\ |\ v \le v') \qquad (1)$$

Дополнительные ограничения на выбор СЗ (например, ограничения по стоимости, требование использовать только сертифицированные средства, поддерживать определенный стандарт, протокол и т.д.) описываются в виде предикатов $O_i(\ldots)$, истинность которых проверяется в ходе формирования $\mathbf{sec^{(i)}}$.

Подмножеств СЗ, удовлетворяющих условию (1), может быть несколько. Процесс формирования проекта предлагается отобразить в форме ориентированного дерева (рис.1).

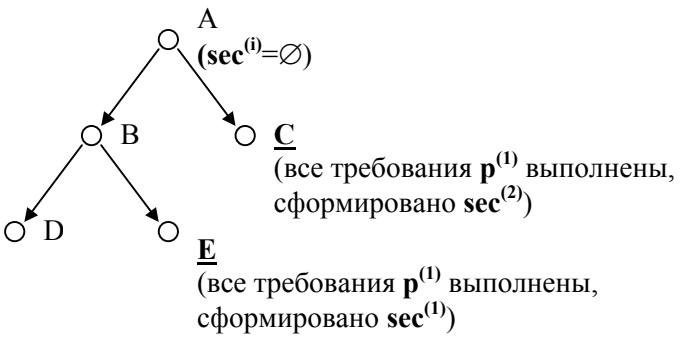

Рис.1. Дерево поиска для построения фрагмента проекта.

Каждый узел на рис.1 соответствует некоторому подмножеству СЗ. В корне дерева это будет пустое множество. Переход по дуге от исходного узла к порожденному приводит к добавлению в формируемое подмножество очередного СЗ, обеспечивающего выполнение части не выполненных на данном уровне требований из $\mathbf{p}^{(1)}$. Достижение концевого (терминального) узла дерева означает, что все требования выполнены (на рисунке такие узлы подчеркнуты) или дальнейшее построение проекта невозможно.

Наличие дуги указывает, что добавление СЗ не противоречит наложенным ограничениям и не вносит избыточности. Из узла не может выходить двух или более дуг, соответствующих одному и тому же СЗ.

Избыточность проявляется в том, что добавление нового СЗ позволяет безболезненно исключить часть СЗ, добавленных на предыдущих шагах. Пусть на рис.1 переход из узла А в В означает добавление СЗ “X”, а из А в С – добавление СЗ “Y”, причем “Y” выполняет все требования из $\mathbf{p}^{(1)}$. В этом случае, из вершины В не выходит дуги, соответствующей добавлению “Y”, т.к. множество {X,Y} будет избыточно – для выполнения всех требований достаточно {Y}. Если задание предполагает дублирование некоторых функций защиты, это указывается с помощью специальных значений для требований.

Для того, чтобы сформировать все возможные подмножества СЗ, отвечающих условию (1), предлагается использовать алгоритм поиска с возвратом по построенному дереву. Надо отметить, что при таком подходе мощность

сформированного множества СЗ будет меньше или равна мощности множества требований $\mathbf{p}^{(1)}$.

После построения всех наборов СЗ для зоны «в целом», создаются проекты защиты отдельных элементов АС. Каждый элемент (сервер, рабочая станция и т.д.) принадлежит как минимум одной зоне. Из заданного для зоны набора выбираются требования, «актуальные» для рассматриваемого элемента (например, требования по защите сетевого трафика не актуальны для компьютера, не подключенного к сети). Часть этих требований может быть выполнена механизмами защиты операционной системы и установленного на элементе прикладного программного обеспечения. Для удовлетворения оставшихся требований используются СЗ, подмножество которых формируется описанным выше способом.

Для граничных элементов АС (т.е. элементов, которые включены более чем в одну зону) набор СЗ формируется несколько иначе. Пусть элемент e относится к зонам z и z'. Для этих зон определены наборы **p** и **p'**, соответственно. Тогда суммарные требования к безопасности будут представлены набором **p"**, куда включены все требования, присутствующие в **p** или **p'**. Причем, если $<r,v>\in\mathbf{p}$, $<r,v'>\in\mathbf{p'}$ и $v\neq v'$, то в **p"** включается наиболее строгое требование (например, <r,v'> при условии $v\leq v'$). После формирования **p"** процедура выбора СЗ для граничного элемента аналогична рассмотренной выше.

Проект подсистемы защиты включает в себя проекты для каждой зоны и каждого элемента АС. Он формируется таким образом, чтобы все выдвинутые требования и ограничения выполнялись для всех зон, на всех элементах АС и для проекта в целом (например, ограничения на суммарную стоимость СЗ). Таких проектов может быть несколько. Для выбора из них оптимального предлагается моделировать ситуацию конечной одношаговой бескоалиционной игрой двух игроков.

Стратегии игрока I («защитника») заключаются во внедрении в АС одного из проектов защиты или отказе от каких-либо действий. Обозначим множество проектов подсистемы защиты АС через **C**, а текущее состояние системы как $\hat{C}$. Тогда «защитник» будет выбирать стратегии, соответствующие элементам множества $\mathbf{C}\cup\{\hat{C}\}$.

Обозначим через **U** конечное множество обобщенных угроз информационной

безопасности защищаемой АС. Обобщенная угроза – это подмножество угроз ИБ, сходных по оказываемому на АС воздействию и причиняемому ущербу. Подобное разбиение множества угроз ИБ формируется на базе экспертных оценок. Тогда игровая стратегия «нарушителя» (игрока II) - выбор элемента из $\mathbf{U} \cup \{\hat{U}\}$, где $\hat{U}$ - отказ от реализации угроз ИБ. В данной модели «нарушитель» рассматривается как источник всех угроз безопасности: и преднамеренных, и случайных. Конечная одношаговая антагонистическая игра (матричная игра) задается в виде:

$$\Gamma = <\mathbf{X}, \mathbf{Y}, \mathbf{H}>,$$

где $\mathbf{X}$ – множество стратегий «защитника», $\mathbf{X} = \mathbf{C} \cup \{\hat{C}\}$; $\mathbf{Y}$ – множество стратегий «нарушителя», $\mathbf{Y} = \mathbf{U} \cup \{\hat{U}\}$; $\mathbf{H}$ – матрица выигрышей. При $|\mathbf{X}| = m$, $|\mathbf{Y}| = n$ предлагается использовать матрицу выигрышей следующего вида (перед началом строк и над столбцами указаны соответствующие элементы множеств $\mathbf{X}$ и $\mathbf{Y}$):

$$H = \begin{array}{c} \\ C_1 \\ \dots \\ C_{(m-1)} \\ \hat{C} \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & \dots & U_{(n-1)} & \hat{U} \end{array} \\ \begin{bmatrix} -h_1 - \bar{h}_{11} & \dots & -h_1 - \bar{h}_{1(n-1)} & -h_1 \\ \dots & \dots & \dots & \dots \\ -h_{(m-1)} - \bar{h}_{(m-1)1} & \dots & -h_{(m-1)} - \bar{h}_{(m-1)(n-1)} & -h_{(m-1)} \\ -\bar{h}_{m1} & \dots & -\bar{h}_{m(n-1)} & 0 \end{bmatrix} \end{array},$$

где $\bar{h}_{ij}$ - оценки потерь от реализации «нарушителем» j-й обобщенной угрозы в отношении АС, где реализован i-й проект подсистемы защиты; h_i - затраты на реализацию i-го проекта. Обе составляющие берутся со знаком минус, т.к. для «защитника» это потери (отрицательный выигрыш).

Построенная антагонистическая игра отражает ситуацию наиболее пессимистичного прогноза: предполагается, что «нарушитель» всемогущ и имеет цель нанести максимальный вред. Если можно достоверно оценить возможности «нарушителя» и ценность для него результатов атаки на АС, то предлагается использовать биматричные игровые модели. Биматричная игра определяется следующим образом:

$$\Gamma = < \mathbf{X}, \mathbf{Y}, \mathbf{H}, \mathbf{H_2}>,$$

где $\mathbf{X}$ и $\mathbf{Y}$ – множества стратегий игроков I и II, $\mathbf{H}$ - матрица выигрышей

«защитника», $\mathbf{H_2}$ – матрица выигрышей «нарушителя».

$$H_2 = \begin{array}{c} \\ C_1 \\ \dots \\ C_{(m-1)} \\ \widehat{C} \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & \dots & U_{(n-1)} & \widehat{U} \end{array} \\ \begin{bmatrix} \widetilde{h}_{11} - \widehat{h}_{11} & \dots & \widetilde{h}_{1(n-1)} - \widehat{h}_{1(n-1)} & 0 \\ \dots & \dots & \dots & \dots \\ \widetilde{h}_{(m-1)1} - \widehat{h}_{(m-1)1} & \dots & \widetilde{h}_{(m-1)(n-1)} - \widehat{h}_{(m-1)(n-1)} & 0 \\ \widetilde{h}_{m1} - \widehat{h}_{m1} & \dots & \widetilde{h}_{m(n-1)} - \widehat{h}_{m(n-1)} & 0 \end{bmatrix} \end{array},$$

где $\widetilde{h}_{ij}$ - оценка выигрыша «нарушителя» от реализации j-й угрозы в отношении АС, где реализован i-й проект; $\widehat{h}_{ij}$ - оценка затрат «нарушителя» на реализацию этой угрозы. Для угроз, источниками которых являются случайные события (например, сбой оборудования), принимаем $\widehat{h}_{ij} = 0$, а $\widetilde{h}_{ij}$ - равным по модулю соответствующему элементу матрицы выигрышей игрока I. Нули в последнем столбце матрицы $\mathbf{H_2}$ соответствуют отказу от атаки на АС. Данная модель отражает менее пессимистичный прогноз, основанный на наличии некоторых дополнительных знаний о «нарушителе».

Исследование антагонистической модели предлагается начать с выбора наиболее предпочтительной стратегии (проекта подсистемы защиты) в соответствии с классическими критериями теории принятия решений. Например, можно использовать критерий Вальда (максиминный критерий) или Лапласа (критерий недостаточного основания). Первый из них отражает позицию владельца АС, готовящегося к самому худшему исходу, а второй – позицию «снижения среднего значения ожидаемых потерь». В реальной ситуации представляется целесообразным применение нескольких критериев и сравнение результатов. Дополнительную информацию дает решение игры.

Если для построенной игры существует решение в чистых стратегиях, то это указывает наиболее предпочтительный проект (или проекты) подсистемы защиты. Для антагонистической игры в этом случае оптимальные игровые стратегии будут совпадать с оптимальными стратегиями, выбранными в соответствии с критерием Вальда. Значение игры покажет максимальные ожидаемые потери при реализации наилучшего проекта. Если решение существует только в смешанных стратегиях, оно нуждается в дополнительной интерпретации: в реальной АС невозможно поочередно использовать различные проекты защиты, как это предполагается определением

смешанной стратегии. В этом случае можно отобрать проекты, попавшие в спектр оптимальной стратегии, и попытаться сформировать компромиссный вариант, объединяющий их сильные стороны.

В случае, когда достоверные оценки ожидаемых потерь в виде вещественного числа получить затруднительно, предлагается использовать интервальные оценки. При этом матрица выигрышей будет содержать интервальные числа вида $[\underline{h}_{ij}, \overline{h}_{ij}]$, где $\underline{h}_{ij}$ и $\overline{h}_{ij}$ - оценки снизу и сверху ($\underline{h}_{ij}, \overline{h}_{ij} \in R$ и $\underline{h}_{ij} \le \overline{h}_{ij}$).

На множестве интервальных чисел **I(R)** определено отношение "≤", что позволяет использовать для упорядочения альтернатив названные выше критерии принятия решений. Но надо учитывать, что на множестве **I(R)** критерий Лапласа не будет являться совершенным упорядочением, т.е. не каждые две альтернативы будут сравнимы. Неопределенность может возникнуть и при использовании критерия Вальда. Подобные случаи исследуются отдельно.

Достоинством предложенной игровой модели «защитник-нарушитель» является то, что она позволяет учесть не только стоимость, но и особенности внедряемого проекта (через изменение оценок ожидаемых потерь).

Глава 3 посвящена описанию разработанного прототипа программной системы поддержки принятия решений в области проектирования инфраструктуры обеспечения ИБ АС, реализующей предлагаемые в работе методы. Для хранения данных в ней используется СУБД MS Access'2000, а генерация проектов и решение игр осуществляется внешним программным модулем, написанным на языке Visual Basic. Поиск решения игр в смешанных стратегиях производится путем сведения к задаче линейного программирования и решения ее симплекс-методом.

Глава 4 посвящена тестированию разработанной программы и сравнению ее возможностей с возможностями коммерческих инструментальных средств анализа рисков, таких как RiskWatch и CRAMM.

Результаты решения тестовых задач соответствуют теоретически предсказанным.

Сравнительный анализ разработанного прототипа с существующими коммерческими продуктами в области анализа рисков показал преимущество предлагаемого решения с точки зрения более гибкого подхода к созданию проектов подсистемы защиты (названные коммерческие продукты предлагают лишь выбор

одного из шаблонов) и более четкого математического обоснования выбора проекта.

Заключение. В работе предложен набор взаимосвязанных методов проектирования подсистемы ЗИ в АС и получены следующие основные результаты:

- разработана теоретико-множественная модель для описания состава и структуры АС, предъявляемых к ней требований, доступных средств и механизмов обеспечения ИБ;
- разработан метод синтеза проектов инфраструктуры обеспечения ИБ по заданному описанию АС и заданным требованиям;
- разработана игровая модель конфликта «защитник-нарушитель», исследование которой позволяет выбрать оптимальный проект;
- произведена апробация предложенных методов путем создания на их базе прототипа системы поддержки принятия решений в области проектирования инфраструктуры обеспечения ИБ АС.

Основные результаты диссертации изложены в 10 печатных работах:

1. Козлов В.Н., Нестеров С.А. Технологии исследования информационной безопасности методами системного и статистического анализа // Материалы III Всероссийской научно-технической конференции «Фундаментальные исследования в технических университетах». СПб.: Изд-во СПбГТУ, 1999. С.40-41.
2. Козлов В.Н., Нестеров С.А. Методы формального представления компьютерной системы при анализе ее информационной безопасности // Межрегиональная конференция «Информационная безопасность регионов России». Тезисы докладов. Часть 2. СПб.: Изд-во СПбГТУ, 1999. С. 44-45.
3. Козлов В.Н., Нестеров С.А. Теоретико-игровые модели в задачах защиты информации // Проблемы информационной безопасности. Компьютерные системы. 2000. № 1. С.31-34.
4. Козлов В.Н., Нестеров С.А. Использование игровой модели при проектировании комплекса средств защиты информации в автоматизированной системе // Методы и технические средства обеспечения безопасности информации. Тезисы докладов. СПб.: Изд-во СПбГТУ, 2000. С.42-43.
5. Нестеров С.А. Один из подходов к исследованию эффективности внедрения

средств защиты информации в компьютерных системах с помощью конечных игровых моделей // Пятая Санкт-Петербургская ассамблея молодых ученых и специалистов. Тезисы докладов. СПб: Изд-во Санкт-Петербургского университета, 2000. С. 40.

6. Козлов В.Н., Нестеров С.А. Использование одношаговых конечных игровых моделей при анализе экономической эффективности средств защиты информации в автоматизированных системах // VIII Всероссийская научно-практическая конференция “Проблемы информационной безопасности в системе высшей школы”. Сборник научных трудов. М.: МИФИ, 2001. С. 44-45.
7. Козлов В.Н., Нестеров С.А. Использование одношаговых конечных игровых моделей при анализе экономической эффективности средств защиты информации в автоматизированных системах // Безопасность информационных технологий. 2001. №1. С.29-31.
8. Нестеров С.А. Об использовании конечных игровых моделей для оценки экономической эффективности систем защиты информации // Труды научно-технической конференции “Безопасность информационных технологий”. Том № 1. Пенза: Изд-во ПНИЭИ, 2001. С.31-33.
9. Нестеров С.А. Разработка системы поддержки принятия решений в области проектирования комплекса средств защиты информации для компьютерных систем // Студенты и аспиранты – малому наукоемкому бизнесу (Ползуновские гранты). Всероссийская научно-практическая конференция. Сборник трудов. Казань: ЗАО «Новое знание», 2001. С.36-37.
10. Нестеров С.А. О подходе к проектированию подсистемы защиты информации для компьютерной сети предприятия // Политехнический симпозиум «Молодые ученые – промышленности Северо-Западного региона». Материалы конференций «Компьютерные технологии, коммуникации, численные методы и математическое моделирование», «Охрана окружающей среды». СПб: Изд-во СПбГТУ, 2001. С. 10.