На правах рукописи

ЖАРИКОВ Николай Иванович

МОДЕЛЬ ОЦЕНКИ РИСКА КОМПЬЮТЕРНЫХ СИСТЕМ ПО БАЗОВЫМ И ОБОБЩЕННЫМ ПОКАЗАТЕЛЯМ УЯЗВИМОСТИ

Специальность 05.13.01 – «Системный анализ, управление и обработка информации (промышленность)»

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Челябинск – 2001

Работа выполнена в Южно-Уральском государственном университете.

Научный руководитель –
доктор технических наук, профессор Мельников А. В.

Официальные оппоненты:
доктор технических наук, профессор Карманов Ю. Т.,
кандидат технических наук Михнюкевич Т. А.

Ведущая организация –
Управление ФСБ России по Челябинской области.

Защита состоится 26 сентября 2001 г., в 15 часов, на заседании диссертационного совета Д 212.298.03 в Южно-Уральском государственном университете по адресу: 454080, г. Челябинск, пр. им. В. И. Ленина, 76, конференц-зал ЮУрГУ (ауд. 244).

С диссертацией можно ознакомиться в библиотеке Южно-Уральского государственного университета

Автореферат разослан «____» августа 2001 г.

Ученый секретарь
диссертационного совета А. М. Коровин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В диссертации изложены основные научные результаты, полученные и опубликованные в 1995 – 2001 гг., связанные с разработкой модели оценки риска компьютерных систем (КС) с использованием системного подхода и современных требований по обеспечению информационной безопасности. Под КС *понимается* совокупность аппаратных и программных средств различного уровня и назначения, разного рода носителей информации, собственно данных, а также персонал, обслуживающий перечисленные выше компоненты, а под риском – *выражение величины потерь*.

Исследованию вопросов анализа факторов, влияющих на безопасность КС, а также построения надежных систем защиты информации (ЗИ) посвящены работы Я. Ф. Блейка, С. В. Вихорева, В. А. Вегнера, А. И. Ефимова, В. Ю. Гайковича, Д. П. Зегжды, А. М. Ивашко, И. Г. Иванова, Г. Йеркса, П. А. Кузнецова, А. Ю. Крутякова, В. В. Кульбы, П. Кина, Д. Кэрра, А. В. Лукацкого, К. Льюиса, Д. А. Ловцова, С. Мэдника, А. А. Молдовяна, Н. А. Молдовяна, С. Мафтика, Л. А. Растригина, Ю. В. Романца, Д. Рабина, А. В. Спесивцева, А. А. Степаненко, Д. Сяо, Э. Тайли, П. А. Тимофеева, Б. Д. Уолкера, М. Фратто, Л. Д. Хоффмана, В. Ф. Шаньгина, Г. Шипли и др.

Некоторые методические подходы к оценке эффективности мер ЗИ по величине ущерба от нарушения безопасности информации рассмотрены в работах В. А. Герасименко, М. К. Размахнина, В. Ю. Войналовича, В. А. Мещерякова, С. В. Постникова, В. Н. Швецова, Д. Стенга, С. Мун и др. В диссертации используются также методы математического моделирования, математической логики, принятия решений при нечетких основаниях, получившие развитие в трудах Н. К. Верещагина, В. А. Горбатова, И. В. Ежковой, Н. А. Костина, Д. А. Поспелова, А. Шеня и др.

Актуальность темы связана, с одной стороны, с непрекращающимися случаями нарушения информационной безопасности различных КС, о чем свидетельствуют многочисленные факты, опубликованные в печати; с другой стороны, с отсутствием отечественных практически применимых методик и моделей оценки риска КС.

Необходимость защиты обусловливается наличием в КС информации, которая характеризуется следующими *аспектами* уязвимости: возможность нарушения целостности – уничтожение или модификация (случайная или злоумышленная); опасность несанкционированного (случайного или злоумышленного) получения информации лицами, для которых она не предназначалась.

Анализ защищенности КС доказывает, что применяемые для оценки эффективности защиты инструментальные средства не учитывают в полной мере влияние угроз на безопасность обрабатываемой информации. Это связано с недостаточной изученностью самого механизма возникновения ущерба, отсутствием моделей объектов информатизации (ОИ), процессов обработки информации в них. Отсутствуют отработанные, практически применимые механизмы получения вероятностных характеристик *дестабилизирующих факторов (ДФ), что делает чрезвычайно трудным* решение задачи по оценке риска КС с применением традиционных

количественных методов оценки как наиболее наглядных и удобных при анализе системы защиты. Решение этой проблемы – одна из основных задач, стоящих перед разработчиками ОИ и систем ЗИ для них.

Целью исследовательской работы является разработка модели оценки риска КС по базовым и обобщенным показателям уязвимости при нарушении целостности и несанкционированном получении информации.

В диссертационной работе представлены результаты решения следующих основных ***задач.***

1. Разработка системной модели ЗИ в КС.
2. Определение модели оценки риска КС.
3. Анализ моделей нечетких множеств в применении к оценкам ДФ.
4. Анализ связи субъективных вероятностей с нечеткими частотными оценками и разработка алгоритма получения численной меры степени возможности свершения событий по экспертным оценкам.
5. Получение аналитических моделей определения показателей уязвимости.
6. Разработка методики анализа эффективности системы ЗИ с использованием модели оценки риска КС.
7. Реализация разработанной модели оценки риска КС.

Методика проведения исследований. В качестве методов исследований применялись. теория множеств, нечеткая логика в применении к нечетким событиям, теория вероятностей и теория системного анализа в рамках адаптации накопленного отечественного и зарубежного опыта обеспечения безопасности компьютерных систем.

Научная новизна исследований заключается в следующем:

- по результатам анализа процесса ЗИ формализованы основные составляющие системной модели ЗИ в КС, и на их основе определена модель оценки риска КС;
- проанализирована связь субъективных вероятностей с нечеткими частотными оценками, и на этой основе разработан алгоритм определения численной меры степени возможности свершения событий на базе экспертных оценок;
- путем объединения преимуществ системного и концептуального подходов к ЗИ в КС разработана методика анализа эффективности системы защиты информации на базе модели оценки риска КС.

Практическое значение работы состоит в формировании адекватной модели системы ЗИ в КС, обеспечивающей безопасность информации на заданном уровне. Реализация методики анализа эффективности системы ЗИ в КС позволяет:

- получить необходимые данные по дестабилизирующим факторам, элементам защиты, средствам и мерам противодействия и проанализировать связь между ними;
- обеспечить применение таких средств и мер защиты, необходимость и достаточность которых подтверждена результатами оценки риска;
- повысить безопасность обрабатываемой в КС информации при систематическом анализе эффективности системы ЗИ в КС.

Реализация результатов работы. Модель оценки риска реализована при аттестации по требованиям безопасности информации нескольких ОИ. Из ОИ, успешно прошедших аттестационные испытания в соответствии с действующими нормативными документами и получивших аттестаты соответствия требованиям безопасности информации, отмечаются следующие: локальная информационно-вычислительная система (ЛИВС) Челябинского территориального управления Госрезерва РФ – два ОИ (аттестаты соответствия: №284/8-48 от 11.07.96, №284/8-68 от 25.12.97); компьютеризированная система учета и контроля ядерных материалов (КСУиК ЯМ) РФЯЦ-ВНИИТФ – четыре ОИ с развитой сетевой архитектурой (аттестаты соответствия: №284/8-144 от 21.06.2000, №284/8-148 от 21.06.2000, №284/8-149 от 21.06.2000, №284/8-150 от 21.06.2000). Методология оценки риска КС внедрена в качестве учебного материала при подготовке студентов Снежинского физико-технического института (СФТИ, г. Снежинск) по дисциплине «Защита информации и компьютерная безопасность» в рамках темы «Управление риском». Акты внедрения приведены в диссертации.

Апробация работы. Основные положения диссертационной работы докладывались на международном семинаре «Разработка компьютеризированной системы учета и контроля ЯМ (УКЯМ) России» (г. Дубна, 1999 год); второй Российской международной конференции «Учет, контроль и физическая защита ЯМ» (Обнинск, 2000); информационно-консультативном семинаре «Защита информации в компьютерных системах» (Челябинск, 2000).

Связь с государственными программами. Основные исследования выполнялись в рамках научно-исследовательских работ, проводимых по теме «Информация» Минатома РФ (№ 20310).

Публикации. Базовые положения диссертации отражены в 6 публикациях.

Структура и объем работы. Диссертация состоит из Введения, четырех глав, Заключения и трех приложений, содержание которых изложено на 168 страницах машинописного текста, иллюстрирована 25 рисунками, содержит 27 таблиц, перечень литературы из 105 наименований.

На защиту выносятся следующие основные положения.

1. Результаты анализа существующих методов и способов оценки риска КС, использующих традиционный количественный, а также качественный и комбинированный подходы.
2. Теоретический базис диссертационного исследования с обоснованием принципов и способов разработанной модели оценки риска КС, содержащий описание:
   - системной модели процесса ЗИ в КС;
   - алгоритма получения численной меры степени возможности свершения событий по экспертным оценкам;
   - моделей определения базовых и обобщенных показателей уязвимости.
3. Обоснование методики оценки эффективности системы ЗИ в КС и места в данной методике разработанной модели оценки риска.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Ключевые понятия и термины

Риск – выражение величины потерь.

Дестабилизирующий фактор (ДФ) – случайное событие, влияющее на безопасность КС.

Причины нарушения целостности информации (НЦИ) – ДФ, следствием проявления которых может быть нарушение целостности информации, т.е. ее искажение или уничтожение.

Каналы несанкционированного получения информации (НПИ) – ДФ, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами, не имеющими на это законных полномочий.

Объект защиты (ОЗ) – структурный компонент КС, в котором находится подлежащая защите информация.

Типовой структурный компонент (ТСК) – ОЗ, удовлетворяющий следующим требованиям: осуществление одних и те же функций, связанных с автоматизированной обработкой информации в КС; локализуемость с точки зрения территориального расположения КС.

Элемент защиты (ЭЗ) – находящаяся в КС совокупность данных, содержащая защищаемые сведения и выделяемая по следующим признакам: нахождение в одном и том же ОЗ; локализуемость с точки зрения носителя информации, однородность в смысле воздействия ДФ.

Уязвимость информации – вероятность нарушения установленного статуса или требуемого уровня защищенности информации.

Базовый показатель уязвимости при НЦИ ($P_{tzgkl}^{(ц,Б)}$) – вероятность того, что целостность выходящей из одного ТСК информации нарушена под воздействием одного ДФ и (в случае злоумышленных действий людей) относительно одного нарушителя.

Базовый показатель уязвимости при НПИ ($P_{tzgkl}^{(п,Б)}$) – вероятность несанкционированного получения информации в одном компоненте КС одним злоумышленником по одному каналу НПИ.

Обобщенный показатель уязвимости ($P^{(г,О)}$ $\{A^*\}$) – вероятность нарушения защищенности информации соответствующим подмножеством $\{A^*\}$, где это подмножество может включать: $\{k^*\}$ - несколько нарушителей; $\{g^*\}$ - несколько ДФ; $\{t^*\}$ - несколько ТСК КС.

В диссертационной работе выполнен обзор опубликованных инструментальных средств, применяемых в развитых зарубежных странах для измерения и управления риском КС. Проведен анализ отечественных методов и способов оценки риска КС. Целью исследования являлся поиск общих закономерностей и подходов при создании средств анализа эффективности ЗИ в КС. Проведенный анализ позволил сформулировать постановку задач диссертационного исследования, выявить подходы и методы их решения.

В процессе решения задачи обеспечения информационной безопасности неизбежно встают вопросы, *какую информацию* из перечня

обрабатываемой в КС, необходимо защищать и *какой уровень защиты* требуется для того или иного вида информации; *каковы эффективность и соотношение* технических и организационных мер, необходимых для защиты информации. Обоснованные ответы на эти вопросы могут быть получены с помощью соответствующего методического аппарата анализа угроз (*оценки риска*) безопасности информации и эффективности ЗИ в КС. Только системный, целенаправленный и методологически точный подход к анализу всех факторов, влияющих на информационную безопасность КС, *позволит выявить способы наилучшего распределения ресурсов, определить* и классифицировать объекты защиты, выявить опасные ситуации, которые не являются очевидными, обеспечить наиболее эффективный подход к экономически рациональному планированию и применению средств и мер защиты.

Одним из важных соображений при выборе методологии является то, что полученные результаты должны быть практически полезны при обеспечении защиты КС. Если методология очень сложна при ее использовании, если она требует очень точных исходных данных или если ее результаты слишком сложны, чтобы сделать вывод, каким является реальный риск при использовании КС, то эта методология не будет полезна и не поможет создать эффективную защиту. С другой стороны, если методология не позволяет добиться приемлемой точности при определении значений таких переменных, как потери, вероятности и стоимости, полученные результаты могут оказаться слишком простыми и не отражать истинного риска использования КС.

Принципиально важной при определении модели оценки риска КС является предлагаемая системная модель процесса ЗИ в КС, являющаяся теоретической базой для построения системы защиты информации (задача 1).

Задача 1. Создание и обеспечение функционирования систем защиты информации (СЗИ) предполагают разработку комплекса моделей, адекватно имитирующих работу системы защиты в различных условиях. Моделирование заключается в построении модели изучаемой или разрабатываемой системы и имитации на ней процессов функционирования реальной системы с целью получения необходимых характеристик последней. При моделировании обращается внимание на две важные особенности проблемы защиты информации, а именно: на подавляющее влияние случайных факторов и целенаправленную деятельность людей в процессе защиты информации. Эти особенности в значительной степени определяют математический инструментарий общего процесса моделирования защиты информации, основные свойства которого представлены в работах Н. А. Костина. Математическое представление модели процесса ЗИ в КС (рис. 1) содержит множества Q, D, G, T, Z, C, P, P^s, S и W, экспертные оценки d, g_d, t, z_t, c, s, w, априорные вероятности p, p^s и решающую функцию $A(^q/G,S)$.

<u>*Множество источников ДФ*</u> (D) содержит элементы d по одному на каждый фактор. Каждый источник d может быть реализован различными способами g_d, которые образуют множество G^d. Множество множеств G^d образует <u>*множество способов реализации всех источников ДФ*</u> (G).

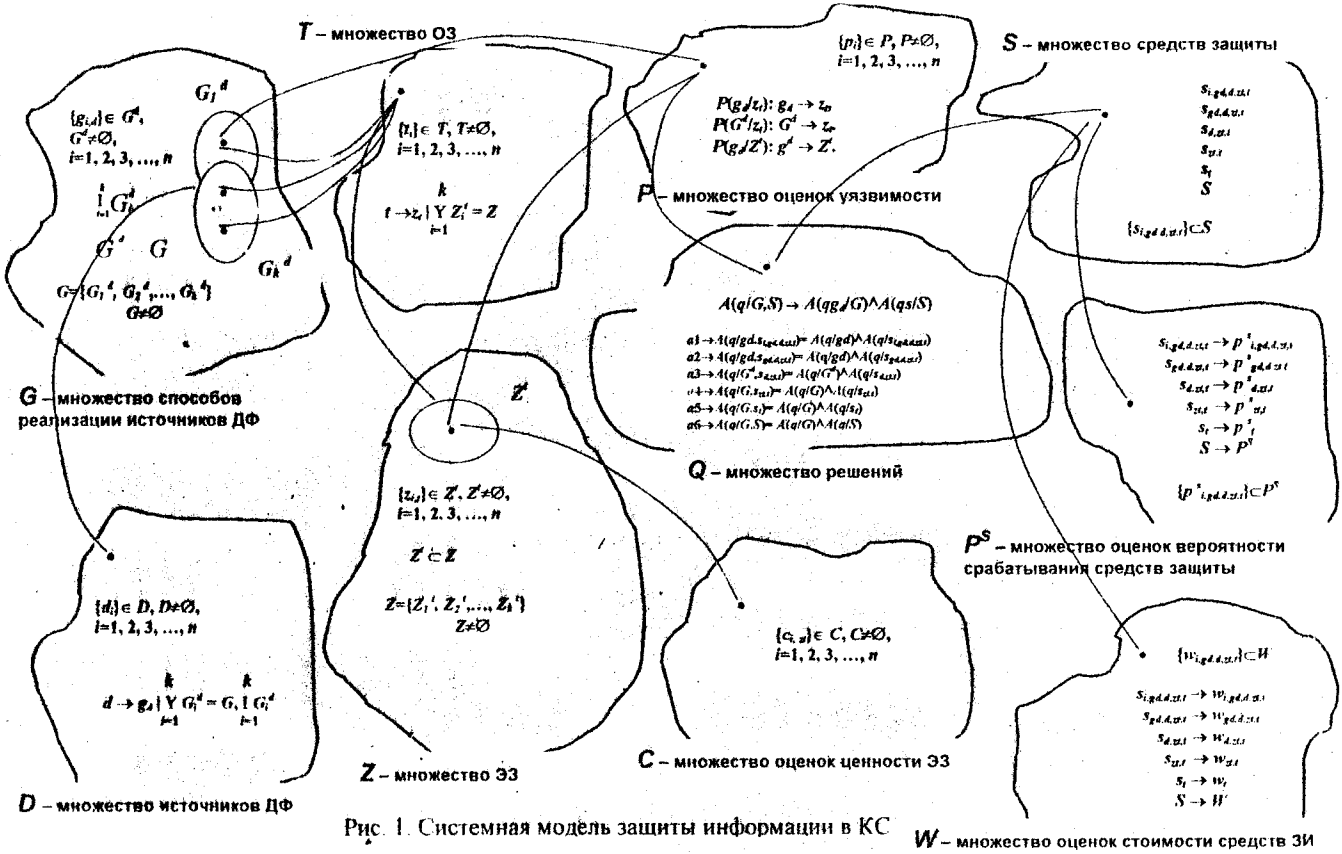


Рис. 1. Системная модель защиты информации в КС

Отображение элементов d множества D на множество G осуществляется экспертным путем.

Множество ОЗ (T) состоит из элементов t, каждому из которых соответствует ТСК КС. В каждом ТСК находится ЭЗ. Таких ЭЗ в одном ТСК может быть несколько, и они образуют множество Z^t. Множество множеств Z^t образует множество ЭЗ (Z). Отображение элементов t множества T на множество Z осуществляется экспертным путем.

Множество оценок ценности ЭЗ (C) содержит элементы c, каждому из которых соответствуют определенные ценность, важность или стоимость ЭЗ.

Множество оценок уязвимости информации (P) состоит из элементов p, каждому из которых соответствует значение вероятности того, что безопасность информации элемента защиты z_t объекта защиты t под воздействием источника ДФ d способом g_d может быть нарушена. Множество оценок уязвимости P может также содержать значения уязвимости, обобщенные по какому-либо параметру, например, по способам реализации ДФ или ТСК.

Множество средств защиты (S) состоит из элементов s, каждому из которых соответствует конкретное средство защиты. При этом элементам $s_{i,gd,d,zt,t}$ соответствует i-е средство по противодействию g_d -му способу реализации d-го источника ДФ на элемент защиты z_t объекта защиты t. Множеству $s_{gd,d,zt,t}$ элементов $s_{i,gd,d,zt,t}$ соответствует вся совокупность средств противодействия, при которой достигается полная (требуемая) защищенность элемента защиты z_t объекта t от g_d-го способа реализации d-й угрозы и т.д. Множеству S элементов $s_{i,gd,d,zt,t}$ соответствует вся совокупность средств противодействия, при которой достигается полная (требуемая) защищенность всех элементов защиты всех объектов от всех угроз.

Множество оценок вероятности срабатывания средств защиты (P^S) включает в себя элементы p^s, каждому из которых соответствует вероятность того, что данный способ g_d реализации d-го источника ДФ на z_t-й элемент защиты объекта защиты t будет предотвращен. Множество $p^s_{gd,d,zt,t}$ элементов $p^s_{i,gd,d,zt,t}$ будет представлять вероятность того, что данный способ g_d источника ДФ (d) z_t-му элементу защиты объекта защиты t будет предотвращен и т. д. Отображение элементов s и их совокупностей множества S на множество P^S осуществляется по экспертным оценкам.

Множество оценок стоимости средств защиты информации (W) содержит элементы w, каждому из которых соответствует значение стоимости конкретного средства противодействия S. При этом элементам $w_{i,gd,d,zt,t}$ соответствует стоимость i-го средства по противодействию g_d-му способу реализации d-го источника ДФ z_t-му элементу защиты объекта защиты t. Множеству $w_{gd,d,zt,t}$ элементов $w_{i,gd,d,zt,t}$ соответствует совокупная стоимость всех средств противодействия, при которой достигается полная (требуемая) защищенность элемента защиты z_t объекта t от g_d-го способа реализации d-й угрозы и т.д. Отображение элементов s множества S на множество W осуществляется по экспертным оценкам.

Множество решений (Q) состоит из элементов q, которые представляют собой решения на основе анализа возможных воздействий g_d источников

ДФ d на элемент защиты z_t объекта защиты t и применения имеющихся средств защиты s. В общем случае решающую функцию можно записать так:

$$a \rightarrow (q_{gd}, I_s), \text{ или } A(q/G,S) \rightarrow A(qg_d/G) \wedge A(qs/S). \qquad (1)$$

Тогда:

$a1$ – алгоритм работы i-го средства ЗИ $s_{i,gd,d,zt,t}$ от одного способа реализации g_d одного источника ДФ (d) одного ЭЗ (z_t) одного ОЗ (t);

$a2$ – алгоритм организации работы всех средств ЗИ $s_{gd,d,zt,t}$ от одного способа реализации одного источника ДФ одного ЭЗ одного объекта защиты;

$a3$ – алгоритм организации работы всех средств ЗИ $s_{d,zt,t}$ от всех способов реализации одного источника ДФ одного ЭЗ одного объекта защиты (для всех $g_d \subset G^d$) и т.д.

Таким образом, системная модель процесса ЗИ в КС (см. рис. 1) содержит все необходимые элементы, участвующие в процессе ЗИ, и отражает связь между ними.

Известно, что наиболее адекватная и физически ясная оценка может быть получена только тогда, когда в качестве интегрального показателя используют величину ущерба (потерь) вследствие воздействия различных ДФ на безопасность информации. В этом случае можно сравнить опасность угроз, последствия их воздействия и достигаемый уровень безопасности информации в результате ее защиты (задача 2).

Задача 2. Методология оценки риска с учетом определений и понятий математической модели процесса ЗИ в КС обеспечивает возможность анализа отношений между элементами множества оценок ценностей защищаемой информации (C), элементами множества оценок уязвимости информации (P), т.е. вероятностью нарушения безопасности информации от реализации угроз, и элементами множества оценок эффективности средств ЗИ в КС (P^S), т.е. вероятностью срабатывания или несрабатывания этих средств защиты. Взаимосвязь между этими необходимыми элементами представлена в виде общей модели оценки риска КС (рис. 2).

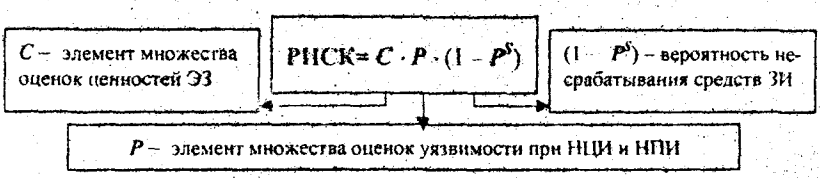


Рис. 2. Общая модель определения риска КС

Для анализа опасностей необходимо знать характеристики всех составляющих элементов указанной модели, а именно: *угрозы* – описание ДФ (источник, наименование, тип, пути или каналы их проявления в ТСК, вероятность их проявления); *защищаемые ценности* – описание ЭЗ (наименование, принадлежность к конкретному ТСК, показатель ценности ЭЗ); *средства и меры ЗИ* - описание применяемых средств и мер защиты (наименование, принадлежность к конкретному ТСК для защиты от конкретного

ДФ, вероятность срабатывания средс в ЗИ). Исходя из этого реализация оценки риска невозможна без применения экспертных и функциональных оценок, априорных вероятностей в случаях, когда отсутствуют необходимые исходные данные.

Проблемы обеспечения информационной безопасности, а следовательно, и риск, связанный с эксплуатацией КС, обусловлены, прежде всего, воздействием на КС различных ДФ. Эти ДФ по своей природе и по степени опасности для защищаемых ценностей КС весьма многообразны и носят случайный характер. Для реализации модели оценки риска КС необходимо получить значения вероятностей проявления возможных угроз (задача 3).

Задача 3. В классическом теоретико-вероятностном подходе если P – нормированная мера над измеримым пространством (Ω, A), то вероятность P(A) события A определяется как мера множества A и является числом из интервала [0, 1]. Однако, даже если A – вполне определенное обычное (не нечеткое) событие, его вероятность P(A) может быть определена плохо. В этом случае неопределенный ответ типа «вполне вероятно», «очень вероятно», «высокая вероятность» и т.п. более соответствовал бы нашему нечеткому представлению о возможности нарушения безопасности информации. Ограничения, обусловленные предположением о том, что A – вполне определенное событие, можно устранить по крайней мере частично, если допустить, что A может быть *нечетким событием*. Это событие можно охарактеризовать как нечеткое подмножество A пространства элементарных событий U, характеризующееся *функцией принадлежности* $\mu_A : U \to [0, 1]$, которая ставит в соответствие каждому $u \in U$ число μ_A из интервала [0, 1]. Важный шаг, который можно предпринять с целью сделать теорию вероятностей применимой к плохо определенным ситуациям, состоит в допущении того, что вероятность P может быть *лингвистической переменной*. Нечеткое ограничение на значения базовой переменной в интервале от 0 до 1 характеризуется *функцией совместимости*, которая каждому значению базовой переменной ставит в соответствие число из интервала [0, 1]. Совместимость лингвистических значений «очень низкая», «низкая», «средняя», «высокая» и «очень высокая» лингвистической переменной *вероятность* в общем виде показана на рис. 3.

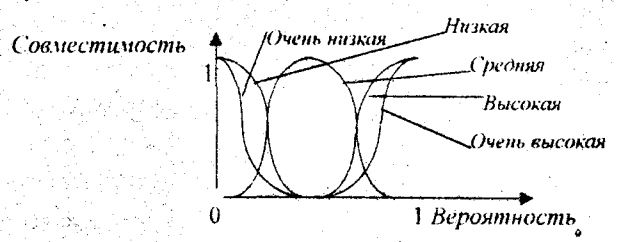
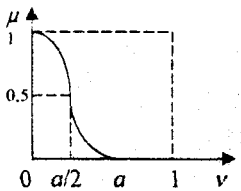


Рис. 3. Функции совместимости значений лингвистической переменной «вероятность»

Функция совместимости значения «низкая» лингвистической переменной *вероятность* показана на рис. 4.

Одно из возможных приближений функции принадлежности значения «низкая» (при $a \neq 0$) определяется выражением



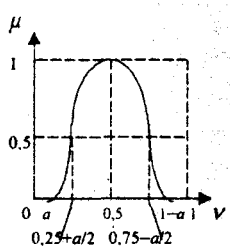
$$\mu_{\text{низкая}}(v) = \begin{cases} 0, \text{ при } v \geq a, \\ 1 - 2\left(\dfrac{v}{a}\right)^2, \text{ при } 0 \leq v \leq a/2, \\ 2\left(\dfrac{v-a}{a}\right)^2, \text{ при } a/2 \leq v \leq a. \end{cases} \quad (2)$$

Рис. 4. Функция совместимости значения «низкая» лингвистической переменной *вероятность*

Здесь точка $v = a/2$ является точкой перехода. Носителем нечеткого множества «низкая» является интервал $[0, a]$.

Функция совместимости значения «средняя» лингвистической переменной *вероятность* показана на рис. 5.

Одно из возможных приближений функции принадлежности значения «средняя» определяется выражением



$$\mu_{\text{средняя}}(v) = \begin{cases} 0, \text{ при } 0 \leq v \leq a, \\ 0, \text{ при } 1 - a \leq v \leq 1, \\ 2\left(\dfrac{v-a}{0.5-a}\right)^2, \text{ при } a \leq v \leq 0{,}25 + a/2, \\ 1 - 2\left(\dfrac{v-0.5}{0.5-a}\right)^2, \text{ при } 0{,}25 + a/2 \leq v \leq 0{,}75 - a/2 \\ 1 - \left(1 - 2\left(\dfrac{v-(1-a)}{0.5-a}\right)^2\right), \text{ при } 0{,}75 - a/2 \leq v \leq 1 - a. \end{cases} \quad (3)$$

Рис. 5. Функция совместимости значения «средняя» лингвистической переменной *вероятность*

Точки $v = 0{,}25 + a/2$, $v = 0{,}5$, $v = 0{,}75 - a/2$ являются точками перехода. Носителем нечеткого множества «средняя» является интервал $[a, 1 - a]$.

Функция совместимости значения «высокая» лингвистической переменной *вероятность* показана на рис. 6.

Функция принадлежности первичного терма «высокая» определяется выражением

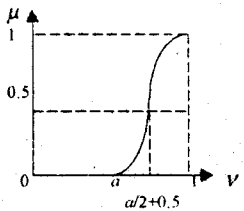


Рис. 6. Функция совместимости значения «высокая» лингвистической переменной *вероятность*

$$\mu_{\text{высокая}}(v) = \begin{cases} 0, \text{ при } 0 \le v \le a, \\ 2\left(\dfrac{v-a}{1-a}\right)^2, \text{ при } a \le v \le 0{,}5 + a/2, \\ 1 - 2\left(\dfrac{v-1}{1-a}\right)^2, \text{ при } 0{,}5 + a/2 \le v \le 1. \end{cases} \quad (4)$$

Здесь точка $v = a/2 + 0{,}5$ является точкой перехода. Интервал $[a, 1]$ является носителем нечеткого множества «высокая».

Если термы являются подмножеством конечного универсального множества значений вероятности $V = 0 + 0{,}1 + 0{,}2 + \ldots + 0{,}9 + 1$, то нечеткое множество, например, «высокая», в соответствии с общей формулой

$$T = \mu_1/v_1 + \ldots + \mu_n/v_n \quad (5)$$

можно определить так:

$$\text{Высокая} = 0{,}4/0{,}6 + 0{,}5/0{,}7 + 0{,}7/0{,}8 + 0{,}9/0{,}9 + 1/1, \quad (6)$$

где такая пара, как, например, 0,5/0,7, означает, что совместимость значения вероятности 0,7 с термом «высокая» равна 0,5.

Модификатор «очень» действует как *лингвистическая неопределенность*, т.е. как модификатор смысла следующего за ним терма. Если в качестве очень простого приближения предположить, что модификатор «очень» действует как оператор концентрирования, то

$$\text{Очень высокая} = \text{CON (высокая)}^2. \quad (7)$$

Семантическое правило для переменной *вероятность* записывается в виде

$$\text{M (очень ... очень высокая)} = \text{Высокая}^{2n}, \quad (8)$$

где n – число вхождений слова «очень» в терм «очень ... очень высокая».

Вычисления с лингвистическими переменными

Предположим, что в точке u степени принадлежности u множествам A и B обозначаются как «высокая» и «средняя» соответственно, причем термины «высокая» и «средняя» определены как нечеткие подмножества множества $U = 0 + 0{,}1 + 0{,}2 + \ldots + 1$ выражениями:

$$\text{Высокая} = 0{,}8/0{,}8 + 0{,}8/0{,}9 + 1/1, \quad (9)$$

$$\text{Средняя} = 0{,}6/0{,}4 + 1/0{,}5 + 0{,}6/0{,}6. \qquad (10)$$

Используя принцип обобщения, получаем:

$$\text{Высокая} \vee \text{Средняя} = (0{,}8/0{,}8 + 0{,}8/0{,}9 + 1/1) \vee (0{,}6/0{,}4 + 1/0{,}5 + 0{,}6/0{,}6) = \\ = 0{,}6/0{,}4 + 1/0{,}5 + 0{,}6/0{,}6 = \text{Средняя}. \qquad (11)$$

Таким образом, когда элементы модели оценки риска КС представлены в виде соответствующих лингвистических переменных, тогда показатель риска будет определен в виде словосочетаний «очень низкий риск», «низкий», «высокий» и т.п.

С целью применения традиционной количественной оценки риска как наиболее наглядного и удобного представления возможных потерь и определения приоритетов по выбору средств и мер защиты разработан алгоритм получения численной меры степени возможности свершения событий на базе лингвистических значений переменной «вероятность», т.е. качественных характеристик (задача 4).

Задача 4. Качественные характеристики можно получить, используя квалификацию, опыт и знание экспертов, входящих в рабочую группу. При этом очень важно установить связь между субъективными вероятностями и нечеткими оценками, выражаемыми словами и словосочетаниями типа «низкий уровень вероятности», «очень низкий», «высокий» и т.п. Основные положения этой связи, базирующейся на нечеткой логике, рассматриваются в работах И. В. Ежковой, Д. А Поспелова и др. Анализ этих связей показывает, что, на самом деле, человек отмечает (регистрирует) не точное значение частоты p_x, а некоторый интервал значений Δp_x. Поэтому человек оценивает частоту не точным значением у, а некоторым интервалом значений Δy. Значение $y = ½$ соответствует норме, интервал $0 \le y \le ½$ – частоте «низкой», «очень низкой», а интервал $½ < y \le 1$ – частоте «высокой», «очень высокой». Фактически Δy является нечетким подмножеством интервала (0, 1).

Таким образом, субъективная вероятность свершения события есть субъективная численная мера степени объективной возможности свершения события за время t, определенная с не известной заранее ошибкой. В практике прогнозирования эксперт применяет следующие разумные способы определения вероятности:

- выбирает из ряда предложенных ему для оценки интервалов шкалы вероятности те, которые с его точки зрения наилучшим образом отражают возможность свершения события;
- оценивает возможность свершения события в форме утвердительного суждения, используя словосочетания «очень низкая», «низкая», «средняя», «высокая» и «очень высокая».

Количественное значение субъективной вероятности в данном случае не определено, однако из содержания рассуждения следует, что, по мнению эксперта, вероятность свершения события находится в пределах указанных им границ шкалы вероятности.

После того, как экспертами определены качественные показатели вероятностей оцениваемых событий, осуществляется перевод качественных показателей в количественные. Механизм перевода реализуется следующим образом. Составляются два массива A и B соответственно из левокрайних и правокрайних интервальных оценок. Затем осуществляются процедуры в соответствии с формулой

$$Y = 2^{-1} d^{-1} \sum_{i=1}^{d} (a_i + b_i), \qquad (12)$$

где

d – число экспертов; a_i – элемент массива A; b_i – элемент массива B.

В качестве шкалы желательности используется шкала Харрингтона (рис. 7.).

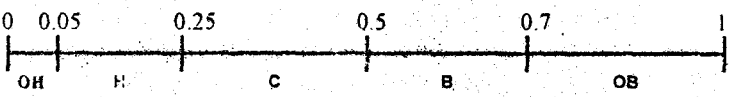


Рис. 7. Интервалы шкалы вероятности для показателей «очень низкая» (ОН), «низкая» (Н), «средняя» (С), «высокая» (В) и «очень высокая» (ОВ)

То есть окончательный результат рассматривается как среднее арифметическое интервальных значений шкалы вероятности и является усредненным интегрированным количественным значением вероятности, отражающим субъективные вероятности экспертов ($P_{cp} = Y$).

Элементы множества оценок уязвимости P (см. рис. 2) рассматриваются как базовые и обобщенные показатели, которые отражают вероятность нарушения безопасности информации в зависимости от выбранных критериев риска: нарушение целостности или несанкционированное получение информации (задача 5).

Задача 5. При рассмотрении общей модели нарушения целостности информации (рис. 9) внимание акцентируется на том обстоятельстве, что целостность информации существенно зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход.

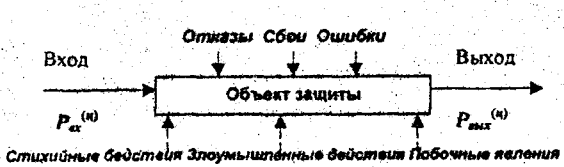


Рис. 9. Общая модель процесса НЦИ

Обозначим:

- $P_{tz}^{(u)}$ *вх* – вероятность того, что на вход t-го ТСК КС поступает информация z-го ЭЗ с нарушенной целостностью;
- $P_{tzgkl}^{(u)}$ – вероятность того, что целостность информации z-го ЭЗ, находящегося в t-м ТСК, будет нарушена под воздействием g-го ДФ и (в случае

злоумышленных действий людей) одним нарушителем. Для тех ДФ, которые не связаны со злоумышленными действиями людей, индекс «k» игнорируется, т.е. значения $P_{tzgkl}^{(н)}$ для всех k одинаковы и зависят только от t и g.

Тогда вероятность того, что целостность выходящей из t-го ТСК информации нарушена ($P_{tzgkl}^{(н)}$ *вых*), определится по формуле

$$P_{tzgkl}^{(н)}\,вых = P_{tz}^{(н)}\,вх + [1 - P_{tz}^{(н)}\,вх]\,P_{tzgkl}^{(н)}. \qquad (13)$$

Значение $P_{tzgkl}^{(н)}$ *вых* и есть базовый показатель уязвимости с точки зрения нарушения целостности информации. Обозначим его через $P_{tzgkl}^{(н,б)}$.

С точки зрения НПИ, главную опасность представляют злоумышленные действия людей. В связи с этим определены и структурированы зоны безопасности КС, т.е. те территории и ресурсы системы, несанкционированный доступ к которым может привести к нарушению информационной безопасности и которые должны быть обеспечены средствами контроля и защиты (рис. 10).

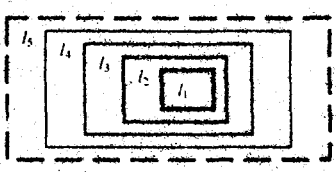


Рис. 10. Общая модель зон безопасности КС

Модель зон безопасности КС содержит:

- l_1 – зону баз данных – ту часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным КС;
- l_2 – зону ресурсов – ту часть помещений, откуда возможен непосредственный доступ к ресурсам КС;
- l_3 – зону контролируемой территории вокруг помещений КС, которая контролируется персоналом или техническими средствами;
- l_4 – зону контролируемой территории вокруг здания, где находятся помещения КС, которая контролируется персоналом или техническими средствами;
- l_5 – внешнюю неконтролируемую зону – территорию вокруг КС, где не применяются средства защиты и не осуществляются никакие мероприятия по защите информации.

Используем следующие обозначения:

- $P_{kl}^{(п,д)}$ – вероятность доступа нарушителя k-й категории в l-ю зону t-го компонента КС;
- $P_{gl}^{(п,к)}$ – вероятность наличия (проявления) g-го канала НПИ в l-й зоне t-го компонента КС;
- $P_{tzl}^{(п,и)}$ – вероятность наличия защищаемой информации в z-м ЭЗ t-го ТСК l-й зоны в момент доступа туда нарушителя.

В соответствии с теоремой умножения вероятностей вероятность несанкционированного получения информации нарушителем k-й категории по g-му каналу НПИ в l-й зоне t-го ТСК КС определится следующей зависимостью:

$$P_{tzgkl}^{(n,l)} = P_{kl}^{(n,\partial)} \cdot P_{gl}^{(n,\kappa)} \cdot P_{tzl}^{(n,u)}. \qquad (14)$$

Но поскольку под базовым показателем уязвимости информации (с точки зрения НПИ) понимается *вероятность* несанкционированного получения информации в <u>*одном*</u> компоненте КС <u>*одним*</u> злоумышленником <u>*одной*</u> категории по <u>*одному*</u> каналу НПИ, то выражение для базового показателя запишется так:

$$P_{tzgkl}^{(n,Б)} = 1 - \prod_{l=1}^{5} [1 - P_{kl}^{(n,\partial)} \cdot P_{gl}^{(n,\kappa)} \cdot P_{tzl}^{(n,u)}]. \qquad (15)$$

<u>*Модели определения обобщенных показателей уязвимости.*</u> При изучении, разработке и эксплуатации систем ЗИ часто необходимо иметь значения показателей уязвимости, обобщенные по какому-либо одному индексу (t, g или k). Они могут быть получены следующим образом.

Для нескольких категорий нарушителей

Пусть $\{k^*\}$ есть интересующее нас подмножество из полного множества потенциально возможных нарушителей. Тогда вероятность нарушения защищенности информации указанным подмножеством нарушителей по g-му фактору в t-м компоненте КС ($P_{tzgl}^{(r)}\{k^*\}$) определяется из выражения

$$P_{tzgl}^{(r)}\{k^*\} = 1 - \prod_{\forall k^*} [1 - P_{tzgkl}^{(Б)}], \qquad (16)$$

где $\forall k^*$ означает перемножение выражений в скобках для всех k, входящих в подмножество $\{k^*\}$. При этом верхний индекс (r) будет обозначаться (u) или (n) в зависимости от того, <u>*какие базовые показатели*</u> используют при расчетах (НЦИ или НПИ).

Для нескольких ДФ

Аналогично, если $\{g^*\}$ есть подмножество представляющих интерес ДФ, то уязвимость информации в t-м компоненте КС по данному подмножеству факторов относительно k-го нарушителя определится по формуле

$$P_{tzkl}^{(r)}\{g^*\} = 1 - \prod_{\forall g^*} [1 - P_{tzgkl}^{(Б)}]. \qquad (17)$$

Для нескольких ТСК КС

Наконец, если $\{t^*\}$ - подмножество интересующих нас ТСК КС, то уязвимость информации в них по g-му фактору относительно k-го нарушителя определится по формуле

$$P_{zkl}^{(r)}\{t^*\} = 1 - \prod_{\forall t^*} [1 - P_{tzgkl}^{(Б)}] \qquad (18)$$

Модели получения значений риска по базовым и обобщенным показателям уязвимости при НЦИ и НПИ

Если обозначить:

$C_{n\backslash z}^{(н)}$ – показатель ценности z-го ЭЗ t-го ТСК, рассматриваемого при НЦИ по g-му способу ДФ для k-го нарушителя, зоны безопасности l;

- $P_{n\backslash tzgkl}^{(н,Б)}$ – значение базового показателя уязвимости при НЦИ z-го ЭЗ t-го ТСК для g-го способа ДФ для k-го нарушителя, зоны безопасности l;
- $P_{n\backslash stzgkl}^{(s,н)}$ – вероятность срабатывания s-го средства защиты при НЦИ z-го ЭЗ t-го ТСК для g-го способа ДФ для k-го нарушителя, зоны безопасности l,

то значения риска по базовым показателям уязвимости при НЦИ определятся по формуле

$$R_{i\backslash tzgkl}^{(н,Б)} = C_{n\backslash z}^{(н)} \cdot P_{n\backslash tzgkl}^{(н,Б)} \cdot [1 - P_{n\backslash stzgkl}^{(s,н)}] \qquad (19)$$

Значения риска по базовым показателям уязвимости при НПИ определяются соответственно по формуле

$$R_{i\backslash tzgkl}^{(п,Б)} = C_{n\backslash z}^{(п)} \cdot P_{n\backslash tzgkl}^{(п,Б)} \cdot [1 - P_{n\backslash stzgkl}^{(s,п)}] \qquad (20)$$

Значения риска по обобщенным показателям уязвимости определяются по формуле

$$R_{l)}^{(г,О)}\{A^*\} = \sum_{n)=1}^{A^*} C_{n\backslash z} \cdot P_{n)}^{(г,О)}\{A^*\} \cdot \prod_{\forall A^*} [1 - P_{n\backslash stzgkl}^{(s)}] \qquad (21)$$

Оценка риска осуществляется в рамках разработанной методики анализа эффективности системы ЗИ в КС (задача 6).

Задача 6. Методика анализа эффективности системы ЗИ в КС содержит следующие необходимые этапы:

1. *Создание экспертной группы.*
2. *Подготовка необходимых исходных данных.*
3. *Оценка риска КС.*
4. *Корректировка системы защиты КС.*
5. *Переоценка риска КС.*

1. *Создание экспертной группы* необходимо для того, чтобы целенаправленно и квалифицированно проанализировать возможные опасные ситуации. В диссертации представлены номенклатура специалистов, которых рекомендуется включать в рабочую группу, их задачи и функции.

2. *Подготовка необходимых исходных данных.*

Определение категорий риска необходимо для оценки как причин, так и видов потерь. В материалах исследовательской работы представлены и описаны основные категории риска КС.

Описание КС:

- архитектура и тип КС;
- состав технических и программных средств обработки информации;
- размещение активного и пассивного сетевого оборудования (территория, здания, помещения);
- зоны безопасности.

Рассмотрена классификация КС по архитектуре и типам с акцентом на концепциях безопасности, соответствующих каждому классу.

Описание модели защиты КС. Для получения основных сведений по защищенности КС разработана модель системы ЗИ, имеющая рубежи защиты:

- периметра контролируемой территории;
- коммуникаций, проходящих по неконтролируемой территории;
- средств, используемых для обработки информации;
- коммуникаций, проходящих в пределах одного и того же помещения;
- коммуникаций, проходящих между различными помещениями на контролируемой территории;
- помещений, расположенных на контролируемой территории.

Определены основные параметры каждого рубежа защиты.

Описание модели нарушителя. При проектировании системы ЗИ в КС с точки зрения возможностей нарушения информационной безопасности необходимо учитывать *модель вероятного нарушителя.* Разработана общая модель нарушителя.

Описание ТСК. При формировании перечня ТСК принимаются во внимание все существующие формы и способы использования современной вычислительной техники. Описание ТСК должно отражать конкретные элементы системы, на которых находится или на которых может находиться защищаемая информация. Проанализированы и систематизированы данные по тридцати шести ТСК.

Описание ЭЗ. Готовится полный список ЭЗ, содержащих защищаемую информацию. Представлены сведения по пятидесяти четырем ЭЗ.

Описание ДФ. Формируется полный перечень возможных типов ДФ и потенциально возможных их источников. При этом описание ДФ должно содержать конкретные сведения о причинах его появления, принадлежности к ОЗ и результатах воздействия. Проанализированы сто двадцать пять способов НЦИ и шестьдесят восемь каналов НПИ.

Описание средств и мер защиты. Средства и меры защиты должны быть конкретно «привязаны» к ТСК и ДФ. В диссертации представлены систематизированные данные по пятидесяти трем средствам и мерам ЗИ.

3. *Оценка риска КС.*

Получение дополнительных исходных данных. Определение вероятностей ДФ (при отсутствии их количественных значений) осуществляют при помощи метода экспертных оценок с последующим переводом качественных показателей в количественные по программе, обеспечивающей автоматизированный перевод.

Определение базовых и обобщенных показателей уязвимости. Используя аналитические модели определения значений базовых и обобщенных показателей уязвимости информации, рассчитывают количественные значения базовых и обобщенных показателей уязвимости для НЦИ и НПИ.

Оценка ценности ЭЗ. Ценность определяется ее значимостью для организации. Оценка ценностей предоставляет руководству сведения, позволяющие принимать решения либо о необходимости принятия соответствующих мер безопасности, либо сделать вывод о том, что в данной системе нет таких ценностей, которые требуют проведения защитных мероприятий. Эксперты определяют численное значение ценности ЭЗ.

Определение вероятностей срабатывания средств защиты проводится в два этапа (при отсутствии количественных значений вероятностей): определение качественных показателей вероятностей экспертным путем (по уровням: ОН, Н, С, В, ОВ); перевод их в количественные.

Определение значений риска КС по показателям уязвимости. Конкретные значения определяют по математическим моделям оценки риска КС по базовым и обобщенным показателям уязвимости при НЦИ и НПИ.

Подготовка принятия решения. Полученные данные по безопасности КС содержат: *характеристики:* ОЗ, ЭЗ, нарушителей, зон безопасности, средств и мер защиты, ДФ; *вероятности:* свершения угроз, срабатывания средств и мер защиты; *показатели уязвимости при НЦИ и НПИ:* базовые, обобщенные; *значения риска, определенные по показателям уязвимости:* базовым, обобщенным.

Они дают возможность внести соответствующие коррективы в систему защиты обрабатываемой в КС информации. Это делают с целью уменьшения риска КС, выбирая наилучший по заданному критерию способ применения тех или иных средств или мер защиты информации. При этом анализируют сведения о всех средствах защиты от всех предполагаемых ДФ для всех ОЗ.

Предложен вариант решения, когда, имея количественные показатели риска для НЦИ и НПИ, корректировку системы защиты КС проводят по остаточному риску. В качестве критерия (т.е. приемлемого риска) выбран показатель среднего значения риска.

4. *Корректировка системы защиты КС.* Проведя сравнение значений риска для каждого ЭЗ с приемлемым риском, выявляют те ЭЗ, риск для которых больше приемлемого. Для таких ЭЗ определяют дополнительные средства или меры защиты, которые могут предотвратить или уменьшить возможный ущерб и снизить показатели риска.

5. *Переоценка риска КС.* При изменении параметров, влияющих на безопасность КС: состава активного и пассивного сетевого оборудования; программного обеспечения; технологии обработки информации; субъектов доступа; обслуживающего персонала; средств и мер защиты и т.п., в соответствии с методологией анализа эффективности СЗИ проводят переоценку риска КС.

Реализация предлагаемой методологии показана на примере оценки защищенности КС1 (задача 7).

Задача 7. В диссертации даны методические рекомендации по практическому применению методики анализа эффективности системы ЗИ в КС на базе модели оценки риска на примере расчета показателей защищенности КС1, основанной на данных, взятых из практики.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ

Проведенные в диссертационной работе исследования являются теоретической и практической основами решения задачи оценки эффективности системы защиты КС с применением количественных показателей уровня защищенности и позволяют сформулировать следующие основные выводы и получить конкретные результаты.

1. Показано, что современные требования по обеспечению информационной безопасности КС выдвигают на первый план управление риском, основным элементом которого является оценка риска, а известные подходы либо слишком сложны для практического применения, либо не позволяют добиться приемлемой точности при определении величины возможных потерь.

2. Определена системная модель процесса ЗИ в КС, содержащая все элементы защиты информации и являющаяся теоретической базой построения системы защиты КС. На ее основе получена модель оценки риска КС, обеспечивающая возможность анализа отношений между необходимыми элементами, участвующими в процессе защиты информации в КС: дестабилизирующими факторами, средствами и мерами защиты, защищаемыми ценностями.

3. Разработан механизм перевода качественных показателей степени возможности свершения событий в количественные, позволяющий проводить оценку риска при отсутствии необходимых статистических исходных данных.

4. Определены и описаны модели системы защиты КС и вероятного нарушителя, являющиеся необходимыми элементами при подготовке исходных данных для оценки риска. Проанализированы и систематизированы основные сведения по дестабилизирующим факторам, способам нарушения целостности и каналам несанкционированного получения информации, типовым структурным компонентам, элементам защиты, средствам и методам ЗИ.

5. Детально рассмотрены процессы нарушения целостности и несанкционированного получения информации, выделены основные элементы, влияющие на безопасность информации в зависимости от выбранных критериев риска. По результатам анализа построены модели определения базовых и обобщенных показателей уязвимости при нарушении целостности и несанкционированном получении информации.

6. Разработана методика анализа эффективности системы защиты информации на базе модели оценки риска КС, обеспечивающая системный подход к анализу всех факторов, влияющих на информационную безопасность. Сформулированы основные требования и рекомендации к содержанию и реализации этапов методики.

7. Практическим результатом исследования является построение системы защиты информации в КС на основе данных, полученных при реализации предложенных принципов, способов, технологий и моделей, обеспечивающих:

- значительное сокращение времени при оформлении необходимых исходных данных за счет использования разработанных шаблонов документов;
- определение необходимых и достаточных средств, методов и мер ЗИ по результатам анализа факторов, влияющих на защищенность КС;
- выработку рекомендаций по корректировке системы защиты, позволяющих совершенствовать ее с целью обеспечения безопасности информации на заданном уровне;
- освоение современных подходов к анализу защищенности КС путем внедрения предлагаемой методологии оценки риска в учебный процесс подготовки специалистов по защите информации и компьютерной безопасности.

Публикации по теме диссертации

1. Жариков Н. И., Крушный В. В. Защита информации и компьютерная безопасность при обработке данных в вычислительных системах и сетях // Первая региональная конференция «Интеллектуальные информационные технологии и стратегии в системной информатизации Уральского региона» (Уралинформ - 94): Тезисы докладов. – Челябинск: Версия, 1995. – Ч.1. – С. 92 – 97.

2. Жариков Н. И. Защита данных и компьютерная безопасность: Учебное пособие. – Снежинск: СФТИ, 1997. – 172 с.

3. Компьютеризированная система учета и контроля ядерных материалов в РФЯЦ-ВНИИТФ им. академик Е. И. Забабахина / В. В. Белов, С. В. Гагаринов, Н. И. Жариков и др. // Материалы международного семинара «Разработка компьютеризированной системы учета и контроля ядерных материалов (УКЯМ) России».– Дубна, 16 – 20 мая 1999 года.

4. Вопросы аттестации 1-й очереди компьютеризированной системы учета и контроля ядерных материалов во ВНИИТФ / В. В. Белов, Н. И. Жариков, В. И. Зуев и др // Вторая Российская международная конференция «Учет, контроль и физическая защита ядерных материалов»: Тезисы докладов. – Обнинск, 22 – 25 мая 2000 года.

5. Жариков Н. И., Мельников А. В. Системно-концептуальный подход к защите информации, обрабатываемой автоматизированным способом // Интеллектика. Логистика. Системология: Сборник научных трудов. – Челябинск, 2001. – Вып. 3. – С.14 – 21.

6. Жариков Н. И., Мельников А. В. Оценка риска – необходимый элемент управления безопасностью компьютерных систем // Сборник докладов межрегионального научно-практического семинара «Информационно-аналитические компьютерные системы и технологии в региональном и муниципальном управлении». – Челябинск: Администрация Челябинской области, ЮУрГУ, 2001. – С. 165 – 170.

Жариков Николай Иванович

МОДЕЛЬ ОЦЕНКИ РИСКА КОМПЬЮТЕРНЫХ СИСТЕМ ПО БАЗОВЫМ И ОБОБЩЕННЫМ ПОКАЗАТЕЛЯМ УЯЗВИМОСТИ

Специальность 05.13.01 – «Системный анализ, управление и обработка информации (промышленность)»

Автореферат диссертации на соискание
ученой степени кандидата технических наук

Издательство Южно-Уральского государственного университета

ИД № 00200 от 28.09.99. Подписано в печать 12.07.01. Формат 60*84 1/16. Печать офсетная. Усл. печ. л. 1,25. Уч.-изд. л. 1.
Тираж 80 экз. Заказ 208/329.

УОП Издательства. 454080, г. Челябинск, пр. им. В. И. Ленина, 76.