Министерство образования и науки Российской Федерации
Федеральное агенство по образованию
Государственное образовательное учреждение
Высшего профессионального образования
Алтайский государственный технический университет
им. И.И.Ползунова

НАУКА И МОЛОДЕЖЬ – 2009

VI Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ И ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

подсекция

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТА ИНФОРМАЦИИ

Барнаул – 2009

ББК 784.584 (2 Рос 537) 638.1

VI Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь – 2009". Секция «Информационные и образовательные технологии». Подсекция «Безопасность информационных технологий и защита информации». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2009. – 43 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей 24 апреля 2009 г.

Компьютерная верстка: Сорокин А.В.

СОДЕРЖАНИЕ

РАЗРАБОТКА ЭЛЕМЕНТОВ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ БАНКА

Авраменко А.А. - студент, Никитин В.М. - к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Современную рыночную систему невозможно представить без адекватной ей финансово-кредитной инфраструктуры, центральное место в которой занимают банки.

Развитие и укрепление банковской системы Российской Федерации, а так же обеспечение эффективного и бесперебойного функционирования платежной системы Российской Федерации являются целями деятельности Банка России. Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности банковских технологических процессов, автоматизированных банковских систем, эксплуатирующихся организациями банковской системы Российской Федерации.

Деятельность, относящаяся к обеспечению ИБ, должна контролироваться. Для обеспечения контроля этой деятельности необходимо иметь сбалансированную и четко регламентированную систему управления информационной безопасности (рисунок 1).

Управление информационной безопасностью - это циклический процесс, включающий осознание степени необходимости защиты информации; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала; мониторинг функционирования механизмов контроля.

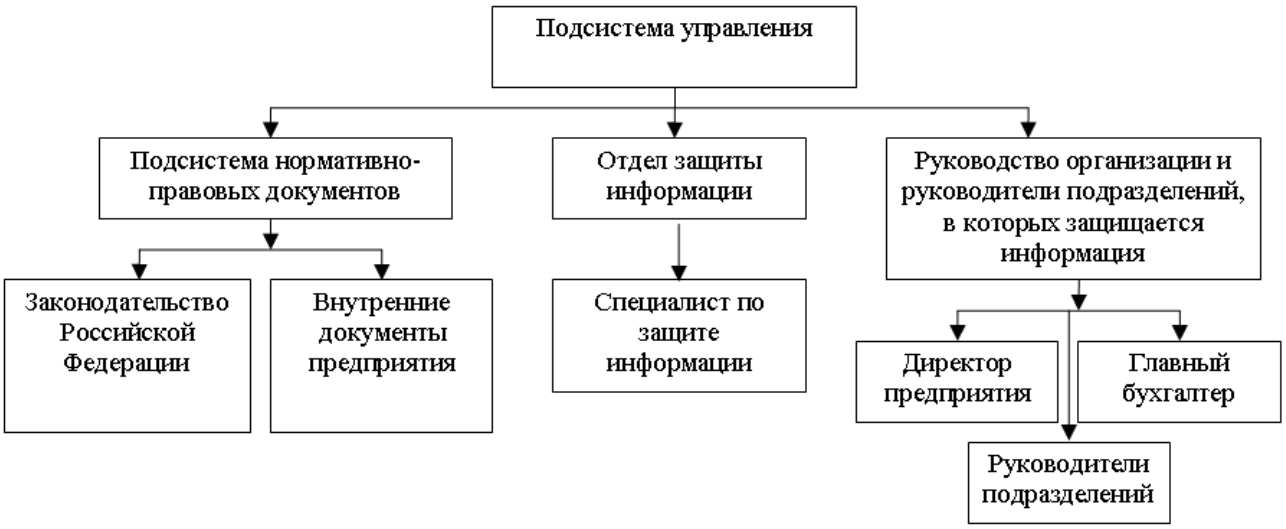


Рисунок 1 – Структура подсистемы управления информационной безопасности

Задачами СУИБ являются систематизация процессов обеспечения ИБ, расстановка приоритетов компании в области ИБ, достижение адекватности системы ИБ существующим рискам, достижение ее «прозрачности». Последнее особенно важно, так как позволяет четко определить, как взаимосвязаны процессы и подсистемы ИБ, кто за них отвечает, какие ресурсы необходимы для их обеспечения. Создание СУИБ позволяет также обеспечить эффективное отслеживание изменений, вносимых в систему информационной безопасности, отслеживать процессы выполнения политики безопасности, эффективно управлять системой в критичных ситуациях.

Перед формированием нормативно методической базы, необходимой для нормального функционирования режима информационной безопасности, необходимо определить к какому уровню зрелости в области информационной безопасности оно относится.

В зависимости от организационной зрелости организации различна степень использования информации.

Можно классифицировать этапы развития и существования предприятия в зависимости от того, как оно обрабатывает и использует информацию в процессе своей деятельности [3]. Уровни (таблица 1) различаются степенью использования информации, накапливаемой в компании. А также применением средств защиты информации, как сертифицированных, так и не имеющих сертификата, включая аппаратные, программные, программно-аппаратные средства защиты. Помимо этого, уровни зрелости организации различаются полным наличием, отсутствием или наличием не в полном объеме нормативных документов, регламентирующих обеспечение ИБ, ответственности персонала, работающего с такого рода информацией и так далее [5].

Таблица 1 – Уровень зрелости организации в области информационной безопасности и их характеристики

Уровень зрелости	**Средства защиты**	**Персонал, ответственный за защиту**	**Регламентация**
1) Хаос (спонтанные информационные связи, хаотичность, непоследовательность)	Отсутствуют	Отсутствует	Отсутствуют
2) Фрагментарная защита (базовые процессы, повторяемые операции)	Используются фрагментарно	Назначены ответственные за защиту	Имеются отдельные документы, регламентирующие защиту
3) Системная защита (стандартизация процессов, интеграция, наличие процедур)	Используются сертифицированные средства защиты, объединённые в систему	Сформирована служба защиты информации	Деятельность по защите регламентирована нормативными документами
4) Управляемая защита	Функционирует КСЗИП	Персонал, ответственный за ЗИ имеет специальную подготовку (образование, переподготовка)	Внедрена система управления информационной безопасностью организации на основе ISO/МЭК 17799
5) Управление качеством ИБ (оптимизируемый)	Функционирует КСЗИП	Персонал ответственный за ЗИ имеет специальную подготовку (образование, переподготовка)	Внедрены: – СУИБ на основе ISO/МЭК 17799; – система менеджмента качества информационной безопасности на основе ISO/МЭК 27001

В рассматриваемом подразделении банка процессы являются формализованными и настолько повторяемыми, что их можно описать и задокументировать. В организации существуют описания ролевых функций сотрудников внутри организации и список задач, которые должен выполнять сотрудник внутри того или иного подразделения.

Все процессы стандартизированы, документированы и объединены в общий информационный поток. Благодаря этому в организации появляется возможность анализа информации по всем аспектам управленческой деятельности, а также получения оперативной информации о степени использования ресурсов [3]. Сформирована служба защиты информации. Используются сертифицированные средства защиты, объединенные в систему. Деятельность по защите регламентирована нормативными документами. Следовательно, данное подразделение банка относится к третьему уровню зрелости в области

информационной безопасности.

Для перехода на четвертый уровень зрелости руководству банка была предложена модель комплексной системы защиты информации, которая создает условия надежной и безопасной работы посредством применения комплекса мер защиты, которые отвечают главным требованиям:

– успешно отражать большую часть вероятных атак;

– при существенных нарушениях нормального функционирования, которые могут возникать при внешних воздействиях разного рода (в том числе, и в результате реализованных атак) система должна иметь способность либо к полному самовосстановлению, либо к восстановлению за нормативные сроки и с минимальными потерями;

– при построении системы должно соблюдаться оптимальное соотношение (цена системы)/вероятные потери [2].

Персонал, ответственный за защиту информации, имеет специальную подготовку, образование и/или переподготовку.

Очень важно отметить тот факт, что была разработана и частично внедрена система управления информационной безопасностью на основе ISO/МЭК 17799.

Также была разработана и одобрена руководством, политика безопасности, с которой ознакомлены все сотрудники. Данный документ состоит из отдельных положений, определяющих требования к различным аспектам обеспечения информационной безопасности [1].

В документе, определяющем политику информационной безопасности, выражена поддержка со стороны руководства и сформулирован принятый в организации подход к управлению информационной безопасностью.

Документ, определяющий политику, содержит следующие положения:

– определение информационной безопасности, ее общие цели и область применения, а также сведения о значении безопасности как механизма, позволяющего совместно использовать информацию;

– краткое пояснение политик безопасности, принципов, стандартов и требований о соответствии, имеющих особое значение для организации;

– определение общих и частных обязанностей по управлению информационной безопасностью, в том числе предоставление отчетов по инцидентам информационной безопасности;

– ссылки на документацию, которая может поддерживать политику, например, более подробные описания политик и процедур для конкретных информационных систем или правила безопасности, которые должны соблюдать пользователи [4].

Политика информационной безопасности доведена до сведения пользователей по всей организации в уместной, доступной и понятной для предполагаемого исполнителя форме.

Аналогичным образом определены и документированы конкретные меры и обязанности отдельных лиц по соблюдению этих требований.

Список литературы

1. Типовые документы для внедрения СУИБ [электронный ресурс].– http://www.globaltrust.ru/produkty/tipovye-organizacionno-rasporyaditelnye-dokumenty-po-informacionnoi-bezopasnosti
2. М.В. Никитин. Конспект лекций по предмету комплексная система защиты информации – электронный вид, АлтГТУ им И.И. Ползунова, кафедра ЗИРСС
3. Пять уровней организационной зрелости предприятий по классификации Capability Maturity Model [электронный ресурс].– http://www.microsoft.com/Rus/Business/Vision/Strategy/Levels.mspx

4. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управлению информационной безопасностью»
5. Загинайлов Ю.Н., Донских Ю.В. Методические рекомендации по внедрению системы управления информационной безопасностью организации на основе международного стандарта ИСО/МЭК 17799 / Алт.гос.техн.ун-т им.И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2008-68с.

РАЗРАБОТКА КОМПОНЕНТОВ КОМПЛЕКСНОЙ ЗАЩИТЫ СЛУЖБ ОБМЕНА ЭЛЕКТРОННЫМИ ПОЧТОВЫМИ СООБЩЕНИЯМИ

Божок Д.О. – студент, Шарлаев Е.В. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

С ростом использования услуг информационных систем, в частности услуг служб обмена электронными почтовыми сообщениями, становится очень актуальным вопрос защиты данных служб. Деятельность по защите должна вестись по направлению обеспечения трех основных свойств защищаемой информации: конфиденциальности, целостности и доступности. Требования к обеспечению конфиденциальности приведены в Конституции РФ в ч. 2 ст. 23 [1]. Требования к обеспечению целостности и доступности информации санкционированному пользователю данной информации любой категории конфиденциальности оговорены в федеральных законах РФ, в том числе в соответствии с Уголовным кодексом РФ оговорены состав преступлений в информационной сфере и соответствующие наказания.

В ходе анализа деятельности как коммерческих, так и некоммерческих организаций города Барнаула, связанной с обменом электронными сообщениями, были выявлены проблемы защиты служб обмена электронными сообщениями от целого спектра угроз, в особенности проблема определения компонентов защиты этих служб на предприятии и состава данных компонентов.

Решение задачи определения структуры комплексной защиты объекта информатизации можно осуществлять несколькими способами, однако для решения данной задачи целесообразней применять компонентный подход, который заключается в разделении комплексной защиты объекта на компоненты, которые объединены по функциональным или типовым признакам. Сущность данного подхода состоит в определении структуры комплексной защиты объекта и функций каждого структурного компонента.

При построении комплексной защиты объектов информатизации следует выполнять следующие требования, которые позволяют построить комплексную защиту в соответствии с реально существующими угрозами информационной безопасности данных объектов [2]:

– успешно отражать большую часть вероятных атак;

– при существенных нарушениях нормального функционирования компоненты комплексной защиты должны иметь способность либо к полному самовосстановлению, либо к восстановлению за нормативные сроки и с минимальными потерями;

– при построении комплексной защиты должно соблюдаться оптимальное соотношение (цена системы)/вероятные потери;

– комплексная защита объектов информатизации должна быть полностью управляемой без потери свойств защищенности объекта при использовании данных средств управления;

– компоненты комплексной защиты должны иметь свойства масштабируемости и возможности обновления отдельных компонент без потери защищенности объекта;

– должны проводиться в рамках мероприятий по комплексной защите объектов информатизации регулярные проверки на уровень защищенности объекта.

Построение комплексной защиты объекта информатизации состоит из следующих этапов [2]:

– определение структуры комплексной защиты;

– определение функций необходимых компонентов комплексной защиты объекта;

– определение требований к компонентам комплексной защиты объекта, данные требования должны учитывать особенности построения информационной системы объекта, в том числе используемые информационные технологии;

– определение инструментария реализации требований в рамках реализации каждой компоненты комплексной защиты объекта информатизации, то есть средства защиты информации и состав мероприятий по защите информации на объекте.

Для определения структуры следует определить типовую структуру комплексной защиты объекта информатизации, которая позволяет с учетом конкретного объекта определить требуемую структуру данного объекта.

В комплексной защите любого объекта следует выделить следующие компоненты:

– управления информационной безопасностью.

– технической укрепленности.

– технической защиты информации.

Группа компонентов управления информационной безопасностью предусматривает применения организационных мер обеспечения безопасности, а также регламентацию работы компонентов комплексной защиты. Это достигается путем подготовки и издания набора нормативных, методических и прочих документов.

В общем случае компоненты технической укрепленности включают в себя объекты:

– контроля доступа;

– охранно-пожарной сигнализации и контроля;

– автоматического пожаротушения;

– контроля параметров окружающей среды;

– обеспечения бесперебойного энергоснабжения;

– видеонаблюдения.

Эти компоненты применяют для обеспечения правильного функционирования информационных систем за счет неизменности внешних условий функционирования и для существенного затруднения непосредственного проникновения злоумышленника на объект информатизации для осуществления несанкционированных действий на нем.

Компоненты, которые обеспечивают неизменность внешних условий для информационной системы, наиболее важны для таких объектов, работа которых связанна с непрерывностью обработки информации, что позволяет обеспечить доступность информационных ресурсов системы в большинстве предусмотренных ситуаций. Также данные компоненты необходимы для обеспечения целостности информационных ресурсов системы, за счет контроля параметров среды, в которой происходит обработка информация на объекте.

Компоненты контроля доступа, а также видеонаблюдения, необходимы в первую очередь для контроля лиц, которые находились в контролируемой зоне объекта информатизации для предотвращения несанкционированных действий или для выявления нарушителя при удачных попытках данных действий.

Группу компонентов технической защиты информации можно разбить на следующие основные составляющие:

– антивирусная защита;

– парольная защита;

– защита электронных документов с информацией ограниченного распространения;

– обеспечение информационной безопасности ЛВС;

– защиты систем и каналов связи;

– обеспечение информационной безопасности технологий обработки информации;

– центр управления ключевыми системами;

– аудит информационной безопасности.

Элементы данных компонентов осуществляют защиту информационных ресурсов, систем и технологий на логическом уровне, что сопряжено с особенностями реализации и функционирования, как самого объекта информатизации, так и его комплексной защиты.

Необходимость элементов каждого из перечисленных компонентов в реальных условиях определяется структурой, особенностями и свойствами объекта информатизации, а также прочими показателями необходимости защиты информационных систем.

На основании типовой структуры комплексной защиты объектов информатизации с учетом специфики организации служб обмена электронными почтовыми сообщениями была выработана структура комплексной защиты этих служб, показанная на рисунке 1.

Рисунок 1 – структура комплексной защиты служб обмена электронными сообщениями

1. Физическая защита сервера и помещения необходима для реализации принципа недопущения посторонних лиц в контролируемую зону, а также в защищаемое помещение.
2. Обеспечение бесперебойного энергоснабжения необходимо для реализации возможности непрерывной работы служб обмена электронными почтовыми сообщениями.
3. Защита от несанкционированного доступа необходима для обеспечения свойств конфиденциальности, целостности и доступности информации, обрабатываемой с помощью служб обмена электронными почтовыми сообщениями.
4. Антивирусная защита необходима как составной компонент защиты всей организации от вирусов и прочих дестабилизирующих программных средств.
5. Защита от спама необходима для реализации возможности наиболее качественной работы всех сотрудников организации в условиях отсутствия посторонней информации.
6. Защита от утечки по техническим каналам необходима для предотвращения утечки информации за счет побочных электромагнитных излучений и наводок, как на прочие основные технические средства в помещении с сервером и шлюзом.
7. Аудит информационной безопасности предполагает своевременное выявление вновь возникающих слабых мест в комплексной защите объекта в связи с изменяющимися условиями работы объекта информатизации и/или внешних условий по отношению к нему.

На основании полученной структуры комплексной защиты были определены функции всех компонентов, требования к ним, основанные на особенностях организации, и на основании данных требований были выработаны рекомендации по организации комплексной защиты служб обмена электронными почтовыми сообщениями. Результаты работы

использовались при организации защиты обмена электронными почтовыми сообщениями в организации ООО «ЕРКЦ».

Список литературы

1. Конституция Российской Федерации. Принята 12 декабря 1993 г.
2. Северин В. А. Комплексная защита информации на предприятии. – М.: Издательство "Городец", 2008. –366С.

ИССЛЕДОВАНИЕ НЕКОТОРЫХ ФУНКЦИЙ ПРИНАДЛЕЖНОСТИ НЕЧЕТКИХ МНОЖЕСТВ

Быков Р.В. – студент, Архипова А.Б. – аспирант
Белов В.М. – к.ф.-м.н., д.т.н, профессор
Алтайский государственный технический университет (г. Барнаул)

Одним из наиболее распространенных классов задач с практическим применением является проблема принятия решения или проблема выбора альтернатив. Для решения таких задач в ряде случаев используют методы, построенные на нечетких множествах.

С понятием нечеткости связаны классы, в которых существует градация степени принадлежности объектов к указанному классу. Модели, построенные с использованием нечеткой математики, являются более гибкими и адекватными реальному миру. По сравнению с традиционными моделями они позволяют быстрее получить окончательные результаты через специфическое построение и простоту используемых операций.

Рассмотрим базовые понятия, которые применяют в теории нечетких множеств.

Нечетким множеством A на универсальном множестве X называют совокупность пар $A = \{\langle \mu_A(x) / x \rangle\}$. Функцию принадлежности нечеткого множества A обозначают как $\eta_A: X \rightarrow [0,1]$. Значение функции принадлежности $\eta_A(x)$ для элемента $x \in X$ называют степенью принадлежности.

Для реализации многих приложений используют множества α-уровня. Множеством α-уровня нечеткого множества A есть множество A_α всех элементов универсального множества X, степень принадлежности которых больше или равняется α:

$$A_\alpha = \{x \in X \mid \eta_A(x) \geq \alpha\} \text{ [1].}$$

Треугольная функция принадлежности

Треугольную форму нечеткого множества определяет тройка вида $A=(a,b,c)_{LR}$, где $a(c)$ – нижняя (верхняя) граница нечеткого A на нулевом α-уровне; b – значение нечеткого A на единичном α-уровне; L и R – линейные функции. Такое описание отвечает функции принадлежности, имеющей следующий аналитический вид и показанной на рис. 1:

$$\mu_A = \begin{cases} 0, & если x < a \\ (x-a)/(b-a), & если a \leq x < b \\ (c-x)/(c-b), & если b \leq x < c \\ 0, & если x > c \end{cases}$$

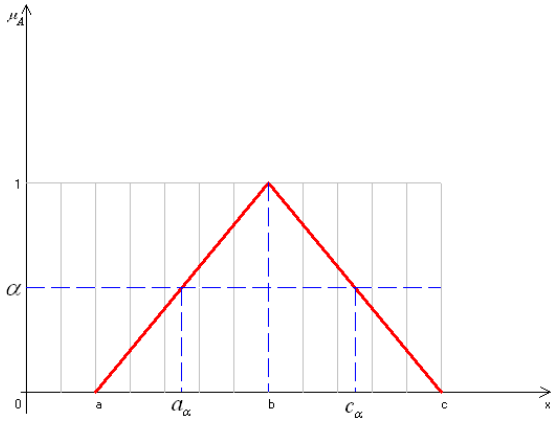


Рис. 1 Нечеткое число A с треугольной ФП

Носитель нечеткого A в этом случае есть интервал $[a,c]$, а ядро – число b. Переход к α – уровневому описанию $A = \bigcup_{a\in[0,1]} (a_\alpha, c_\alpha)$ выполняют по формулам:

$$a_\alpha = a + (b-a)\alpha;\ c_\alpha = c - (c-b)\alpha.$$

Рассмотрим случай формирования нечеткого числа в треугольной интерпретации. Пусть X={4,10,15} – множество, которое определяет количество символов длины секретного ключа. Нужно построить нечеткое множество $\tilde{A}$, формализующее понятие «достаточная длина секретного ключа для обеспечения конфиденциальности информации, составляющая десять символов».

Здесь носителем нечеткого числа $\tilde{A}$ будет служить интервал [4,15], его ядром – число 10, то есть $\tilde{A}$=(4,10,15) $_{LR}$, где a = 4, b = 10, c = 15. Графическое изображение треугольного нечеткого числа показано на рис. 2.

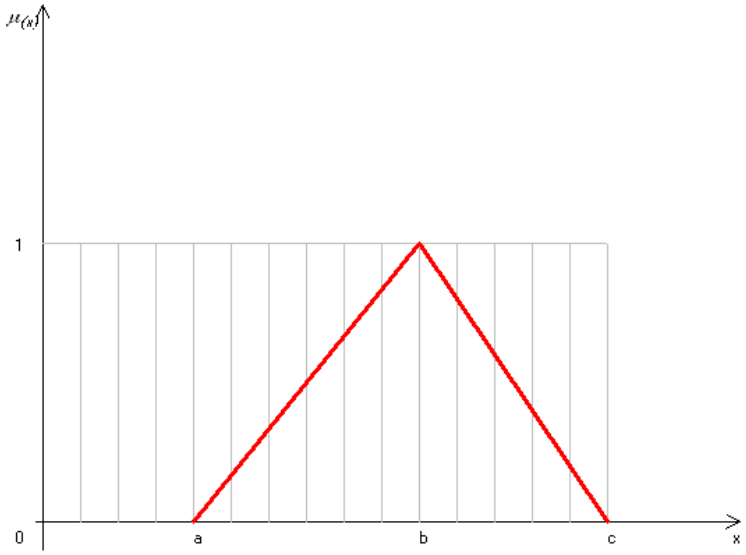


Рис. 2 Треугольное нечеткое число

Трапециевидная функция принадлежности

Трапециевидную форму параметрического нечеткого $\tilde{A}$ определяет четверка: $\tilde{A}$ =$(a,b_1,b_2,c)_{LR}$, где $a(c)$ – нижняя (верхняя) граница нечеткого $\tilde{A}$ на нулевом α-уровне; $b_1(b_2)$ – нижняя(верхняя) граница нечеткого $\tilde{A}$ на единичном α-уровне; L и R – линейные функции. Такое описание отвечает функции принадлежности имеющей следующий аналитический вид:

$$\mu_A = \begin{cases} 0, & \text{если } x < a; \\ (x-a)/(b_1-a), & \text{если } a \le x < b_1; \\ 1, & \text{если } b_1 \le x < b_2 \\ (c-x)/(c-b_2), & \text{если } b_2 \le x < c; \\ 0, & \text{если } x > c. \end{cases}$$

Графически она изображена на рис. 3.

В этом случае носитель нечеткого $\tilde{A}$ в этом случае есть интервал *[a,c]*, а ядро – *[b_1,b_2]*.

Переход к α – уровневому описанию $\tilde{A} = \bigcup_{a \in [0,1]} (a_\alpha, b_\alpha)$ выполняется по формулам:

$$a_\alpha = a + (b_1 - a)\alpha;\ c_\alpha = c - (c - b_2)\alpha.$$

Рассмотрим случай формирования нечеткого числа в трапециевидной интерпретации. Пусть X={4,10,12,15} – множество, которое определяет количество символов длины секретного ключа. Нужно построить нечеткое множество $\tilde{A}$, формализующее понятие «достаточная длина секретного ключа для обеспечения конфиденциальности информации, находящееся в интервале от 10 до 12».

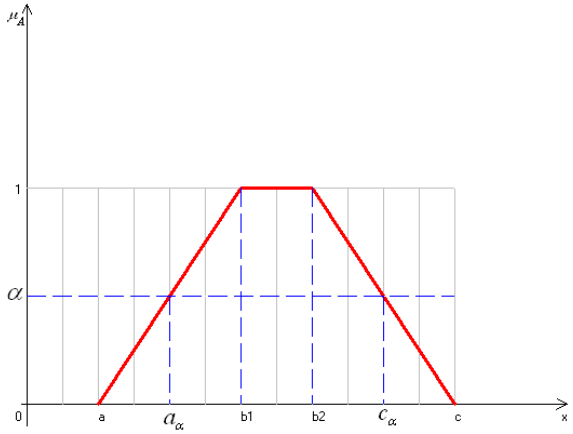


Рис. 3 Нечеткое число $\tilde{A}$ с трапециевидной ФП

В этом случае для нечеткого числа $\tilde{A}$: a = 4, b_1 = 10, b_2 = 12, c = 15.Полученное нечеткое число представлено на рис. 4.

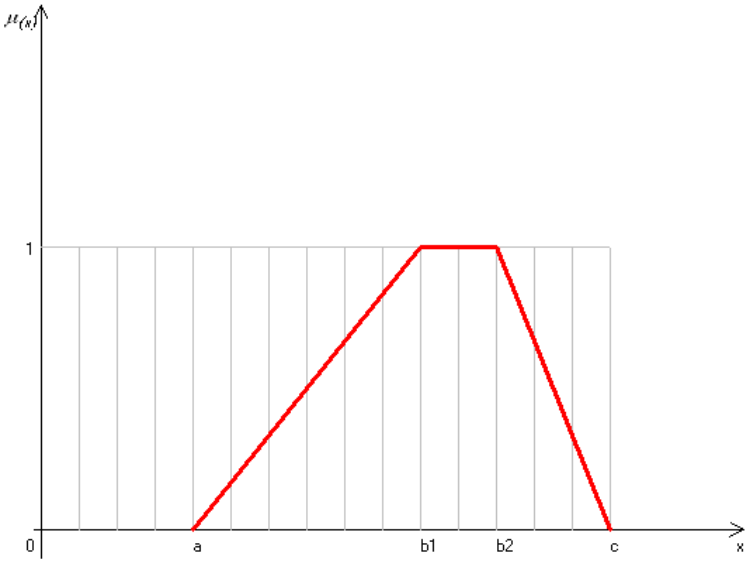


Рис. 4 Трапециевидное нечеткое число

Переход от *l* – формы нечеткого числа $\tilde{q}$ к треугольной форме

l – формой неопределенного параметра *q* (нечеткого числа $\tilde{q}$) будем называть тройку вида:

$$\tilde{q} = \langle \underline{q}, \bar{q}, l \rangle,$$

где $\underline{q}(\bar{q})$ - нижняя (верхняя) граница изменения параметра *q*; *l* – лингвистическая оценка параметра *q* диапазона $[\underline{q}, \bar{q}]$, причем $l \in L = \{l_1, l_2, ..., l_m\}$.

L – линейно - упорядоченное по принципу от "меньшего" к "большему" множество лингвистических термов для качественной оценки параметра.

При переходе от *l*-формы нечеткого числа $\tilde{q}$ к треугольной форме предполагают следующее:

- носителем нечеткого числа $\tilde{q}$ является интервал $[\underline{q}, \bar{q}]$;
- для первого терма $l_1 : q_1(l_1) = \underline{q}$;
- для последнего терма $l_m : q_1(l_m) = \bar{q}$;
- для соседних термов l_j и $l_i\,(j = i+1)$ расстояние между ядрами $\Delta = q(l_j) - q(l_i)$ является постоянной величиной, где $q(l_1), q(l_m), q(l_i), q(l_j)$ - ядра нечеткого числа $\tilde{q}$ соответствующие термам l_1, l_m, l_i, l_j.

Таким образом, переход от *l*-формы нечеткого числа $\tilde{q}$ к треугольной форме осуществляют по следующим формулам:

$$\underline{q}(l_i) = \underline{q}; \quad \bar{q}(l_i) = \bar{q};$$

$$q(l_i) = \underline{q} + \frac{(i-1)(\bar{q} - \underline{q})}{(m-1)},$$

где $\underline{q}(l_i)(\bar{q}(l_i))$ нижняя (верхняя) граница носителя нечеткого числа $\tilde{q}$, выраженного лингвистической оценкой l_i; $q(l_i)$ - ядро нечеткого числа $\tilde{q}$, выраженного лингвистической оценкой l_i. [2]

Переход от *l* - формы к треугольной в случае шести термов показан на рис. 5.

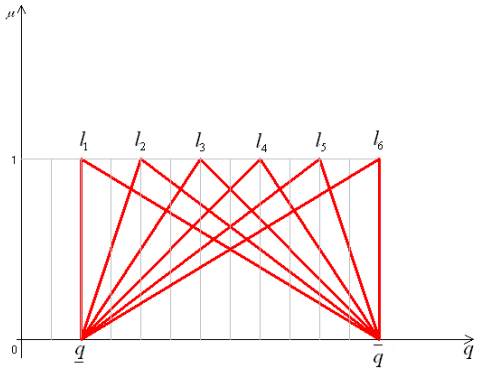


Рис. 5 Переход от *l* – формы к треугольной в случае шести термов

Рассмотрим случай представления числа $\tilde{t}$ в треугольной форме. Пусть информация о длине секретного ключа задана *l* – формой нечеткого числа $\tilde{t} = \langle 4, 15, \textit{высокое} \rangle$. Множество лингвистических оценок имеет вид *L={низкое, среднее, высокое, очень высокое}*.

Количество лингвистических термов равно четырем. Лингвистическая оценка <*высокое*> в множестве *L* имеет порядковый номер *i=3*. Применяя формулы, получаем $\underline{t} = 4;\ \bar{t} = 15;\ t = 11.3.$

Функция принадлежности нечеткого числа $\tilde{t}$ показана на рис. 6.

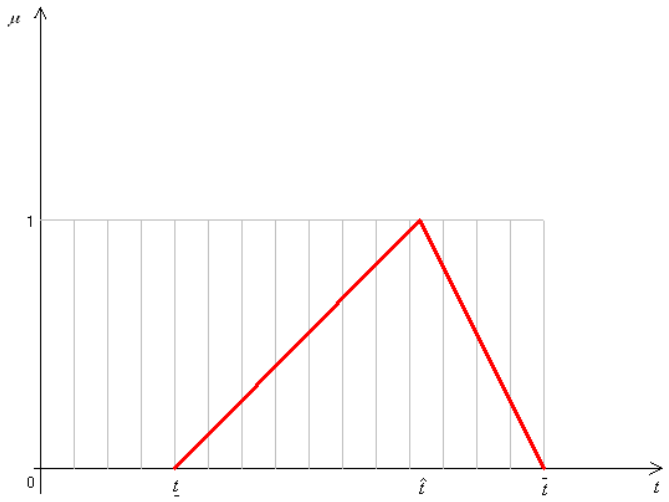


Рис. 6 Функция принадлежности нечеткого числа $\tilde{t}$

Переход от *l* – формы нечеткого числа $\tilde{q}$ к трапециевидной форме

При переходе от *l*-формы нечеткого числа $\tilde{q}$ к трапециевидной форме предполагают следующее:

- носителем нечеткого числа $\tilde{q}$ является интервал $[\underline{q}, \bar{q}]$;
- для первого терма $l_1 : \underline{q}_1(l_1) = \underline{q}$;
- для последнего терма $l_m : \bar{q}_1(l_m) = \bar{q}$;
- для соседних термов l_j и $l_i\,(j = i+1)$; $\underline{q}_1(l_j) = \underline{q}_1(l_i) + 2 \cdot \Delta$, где $\underline{q}_1(l_j)$ и $\underline{q}_1(l_i)$ - нижние границы ядра нечеткого числа $\tilde{q}$ выраженного лингвистическими оценками l_j и l_i, соответственно;
- размер ядра Δ нечетного числа $\tilde{q}$ зависит от мощности (m) терм-множества L, носителя $[\underline{q}, \bar{q}]$ и не зависит от лингвистической переменной.

Если неопределенный параметр q задан l - формой нечеткого числа $\tilde{q} = \langle \underline{q}, \bar{q}, l \rangle$, где $l \in L = \{l_1, l_2, ..., l_m\}$, то переход от *l*-формы к трапециевидной форме осуществляется по формулам:

$$\underline{q}_0(l_i) = \underline{q};\ \bar{q}_0(l_i) = \bar{q};$$

$$\underline{q}_1(l_i) = \underline{q} + \frac{(2i-1)(\bar{q} - \underline{q})}{(2m-1)};$$

$$\bar{q}_1(l_i) = \underline{q} + \frac{(2i-1)(\bar{q} - \underline{q})}{(2m-1)},$$

где $\underline{q}_0(l_i)(\bar{q}_0(l_i))$ - нижняя (верхняя) граница носителя нечеткого числа $\tilde{q}$, оцениваемого лингвистическим термом l_i;

$\underline{q}_1(l_i)(\bar{q}_1(l_i))$ - нижняя {верхняя) граница ядра нечеткого числа $\tilde{q}$, оцениваемого лингвистическим термом l_i [3].

Переход от *l* - формы к трапециевидной в случае четырех термов показан на рис. 7.

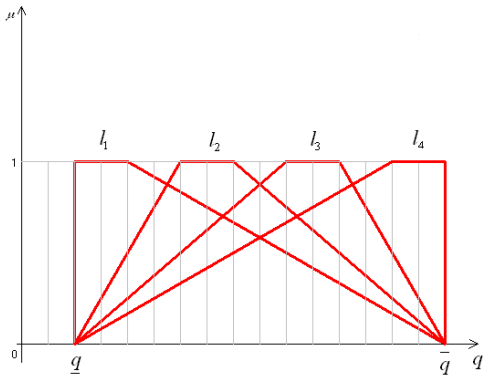


Рис. 7 Переход от *l* – формы к трапециевидной в случае четырех термов

Список литературы

1. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.
2. Корченко А. Г. Построение систем защиты информации на нечетких множествах. - Киев: МК-Пресс, 2006. – 316 с.
3. Ротштейн А. П. Интеллектуальные технологии идентификации. – Винница: Универсум Винница, 1999. – 320 с.

МЕТОД ПАРНЫХ СРАВНЕНИЙ С ИСПОЛЬЗОВАНИЕМ РАНГОВЫХ ОЦЕНОК

Быков Р.В. – студент, Архипова А.Б. – аспирант
Белов В.М. – к.ф.-м.н., д.т.н, профессор
Алтайский государственный технический университет (г.Барнаул)

В работе [1] предложен метод парных сравнений на основе ранговых оценок, где в качестве исходных данных используют матрицу парных сравнений.

Пусть *S* - некоторое свойство, которое рассматривают как лингвистический терм. Нечеткое множество, с помощью которого формализуют терм *S*, представляет собой совокупность пар:

$$S = \left\{ \frac{\mu_S(u_1)}{u_1}, \frac{\mu_S(u_2)}{u_2}, \ldots, \frac{\mu_S(u_n)}{u_n} \right\},$$

где $\{u_1, u_2, \ldots, u_n\} = U$ - универсальное множество, на котором задают нечеткое множество $S \subset U$;

$\mu_S(u_i)$ - степень принадлежности элемента $u_i \in U$ нечеткому множеству *S*.

Задача состоит в том, чтобы определить значения $\mu_S(u_i)$ для всех $i = \overline{1,n}$. Совокупность этих значений и будет составлять неизвестную функцию принадлежности.

Под рангом элемента $u_i \in U$ понимают число $r_S(u_i)$, которое характеризует значимость этого элемента в формировании свойства, которым описывают нечеткий терм *S*.

Обозначим $r_S(u_i) = r_i$, $\mu_S(u_i) = \mu_i$, $i = \overline{1,n}$.

Тогда правило распределения степеней принадлежности можно задать в виде соотношения (1), для которого прибавляют условие нормирования (2):

$$\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} = ... = \frac{\mu_n}{r_n} \quad (1)$$

$$\mu_1 + \mu_2 + ... + \mu_n = 1 \quad (2)$$

Используя соотношение (1), можно определить степени принадлежности всех элементов универсального множества через степень принадлежности опорного элемента. Если опорным является элемент $u_1 \in U$ с принадлежностью μ_1, то

$$\mu_2 = \frac{r_2}{r_1}\mu_1,\ \mu_3 = \frac{r_3}{r_1}\mu_1, ..., \mu_n = \frac{r_n}{r_1}\mu_1. \quad (3)$$

Для опорного элемента $u_2 \in U$ принадлежностью μ_2 получаем:

$$\mu_1 = \frac{r_1}{r_2}\mu_2,\ \mu_3 = \frac{r_3}{r_2}\mu_2, ..., \mu_n = \frac{r_n}{r_2}\mu_2. \quad (4)$$

И, наконец, для опорного элемента $u_n \in U$ с принадлежностью μ_n имеем:

$$\mu_1 = \frac{r_1}{r_n}\mu_n, ..., \mu_{n-1} = \frac{r_{n-1}}{r_n}\mu_n. \quad (5)$$

Учитывая условие нормирования (2), из соотношений (3) - (5) находим:

$$\begin{cases} \mu_1 = \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + ... + \frac{r_n}{r_1}\right)^{-1}; \\ \mu_2 = \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + ... + \frac{r_n}{r_2}\right)^{-1}; \\ ..... \\ \mu_n = \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + ... + 1\right)^{-1}. \end{cases} \quad (6)$$

Полученные формулы дают возможность вычислять степени принадлежности $\mu_S(u_i)$ элементов $u_i \in U$ к нечеткому терму *S* двумя независимыми путями:

1) по абсолютным оценкам уровней r_i, $i = \overline{1,n}$, которые определяют согласно методикам, предложенных в теории структурного анализа систем. Для экспертных оценок рангов можно использовать 9-ти бальную шкалу (1 - наименьший ранг, 9 - наибольший ранг);

2) по относительным оценкам рангов $\frac{r_i}{r_j} = a_{ij}$, $i, j = \overline{1,n}$, которые образуют матрицу [2]:

$$A = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \frac{r_3}{r_1} & ... & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \frac{r_3}{r_2} & ... & \frac{r_n}{r_2} \\ ... & ... & ... & ... & ... \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \frac{r_3}{r_n} & ... & 1 \end{bmatrix}.$$

Эта матрица обладает следующими свойствами:

- она диагональная, т. е. $a_{ii} = 1, i = \overline{1,n}$;

- элементы, которые симметричны относительно главной диагонали, связаны зависимостью: $a_{ij} = 1/a_{ji}$;
- она транзитивна, т. е. $a_{jk} \cdot a_{kj} = a_{ij}$, поскольку $\frac{r_i}{r_k} \cdot \frac{r_k}{r_j} = \frac{r_i}{r_j}$.

Наличие этих свойств приводит к тому, что при известных элементах одной строки матрицы A легко определить элементы всех других строк. Если известная r-я строка, т. е. элементы a_{kj}, $k, i = \overline{1,n}$, то произвольный элемент a_{ij} находят следующим образом:

$$a_{ij} = a_{kj} / a_{ki},\ i, j, k = \overline{1,n}.$$

Поскольку матрица A может быть интерпретирована как матрица парных сравнений рангов, то для экспертных оценок элементов этой матрицы можно использовать 9-ти бальную шкалу Саати: $a_{ij} = \frac{r_i}{r_j}$. В нашем случае эту шкалу можно сформировать так:

1 - при отсутствии преимущества r_j над r_i;

3 -при слабом преимуществе r_j над r_i;

5 -при существенном преимуществе r_j над r_i;

7 -при явном преимуществе r_j над r_i;

9-при абсолютном преимуществе r_j над r_i;

2,4,6,8 - промежуточные сравнительные оценки [1].

Таким образом, с помощью полученных формул (6), экспертные знания о рангах элементов или их парные сравнения преобразуют в функцию принадлежности нечеткого терма.

Пример нечеткого числа, полученного с помощью метода парных сравнений на ранговых оценках при четырех лингвистических переменных, показан на рис. 1.

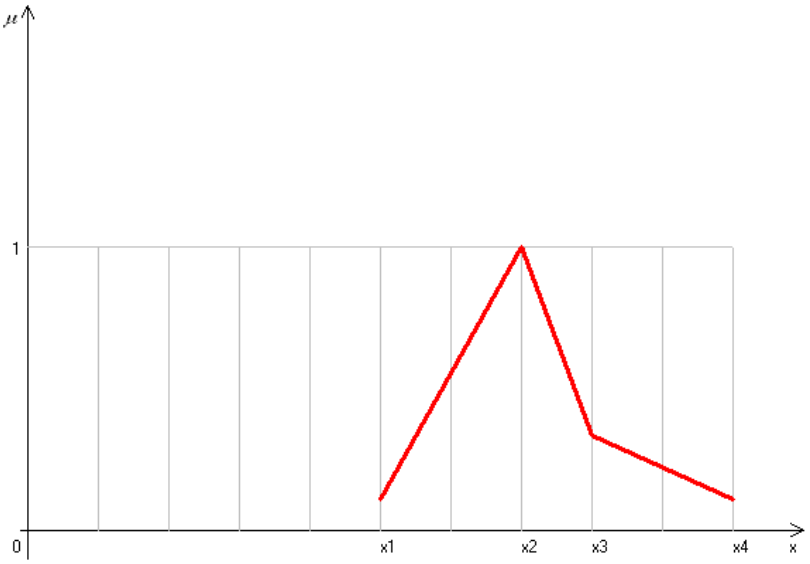
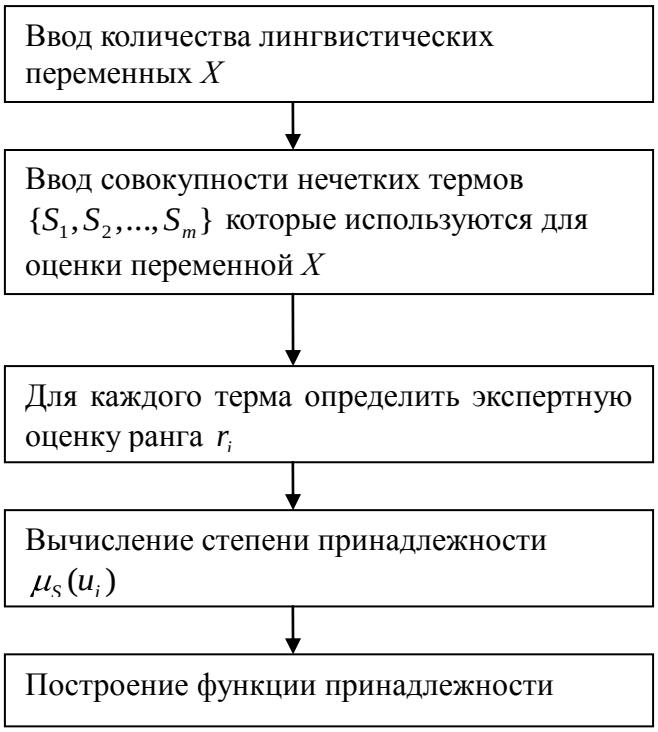


Рис. 1 Пример нечеткого числа, полученного с помощью метода парных сравнений на ранговых оценках

Алгоритм программы по абсолютным оценкам уровней r_i, $i = \overline{1,n}$, выглядит следующим образом:



Рассмотрим лингвистическую переменную «длина секретного ключа для обеспечения конфиденциальности информации», которая определена на универсальном множестве {5, 7, 8, 10}. Экспертные оценки рангов имеют вид {1, 9, 3, 1}.

Здесь степени принадлежности после нормализации принимают вид:

$$\mu(u_1) = 0{,}111;\ \mu(u_2) = 1;\ \mu(u_3) = 0{,}333;\ \mu(u_4) = 0{,}111.$$

Полученная функция принадлежности показана на рис. 2.

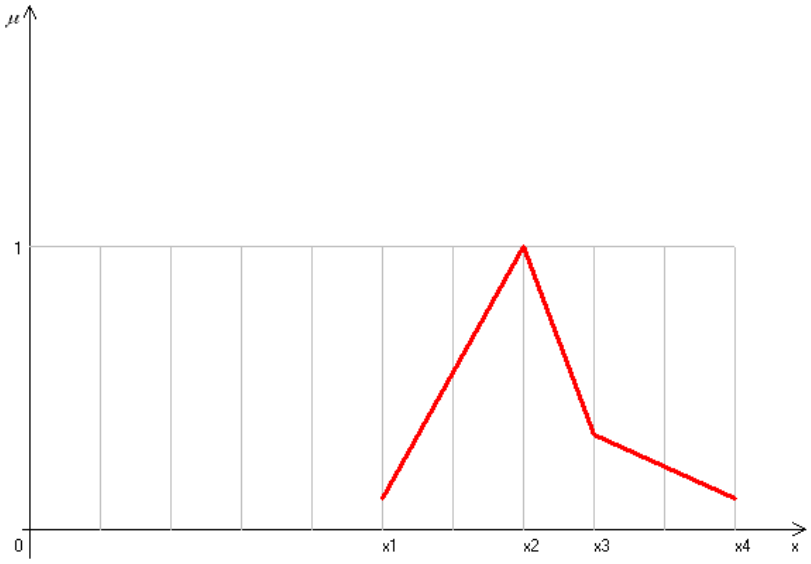


Рис. 2 Функция принадлежности нечеткого множества

Список литературы

1. Ротштейн А. П. Интеллектуальные технологии идентификации. – Винница: Универсум Винница, 1999. – 320 с.
2. Корченко А. Г. Построение систем защиты информации на нечетких множествах. - Киев: МК-Пресс, 2006. – 316 с.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НАХОЖДЕНИЯ ПАРАМЕТРОВ НЕКОТОРЫХ ФУНКЦИЙ ПРИНАДЛЕЖНОСТИ

Архипова А.Б. – аспирант, Быков Р.В. – студент
Белов В.М. – к.ф.-м.н., д.т.н, профессор
Алтайский государственный технический университет (г. Барнаул)

Задача “Исследования некоторых функций принадлежности” нечетких множеств используется при решении проблем принятия решений или проблем выбора альтернатив.

Программа предоставляет пользователю следующие возможности:

- построение треугольной функции принадлежности;
- построение трапециевидной функции принадлежности;
- построение функций принадлежности на основе метода парных сравнений на ранговых оценках;
- переход от *l*-формы представления нечеткого числа к треугольной функции принадлежности;
- переход от *l*-формы представления нечеткого числа к трапециевидной функции принадлежности;
- использование методических данных по всем используемым функциям принадлежности;
- сохранение результатов решения на диск.

Для того, чтобы работать с программным продуктом, необходимо первоначально установить программу. Для этого выполните следующие действия:

1. вставить диск, содержащий дистрибутив программы в привод CD-ROM;
2. скопировать с диска Мастер установки программы Setup.exe;
3. запустить его, и следую инструкция Мастера установить программный пакет.

Для запуска программы достаточно запустить исполняемый файл CCFB.exe.

Решение данной задачи призвано обеспечить:

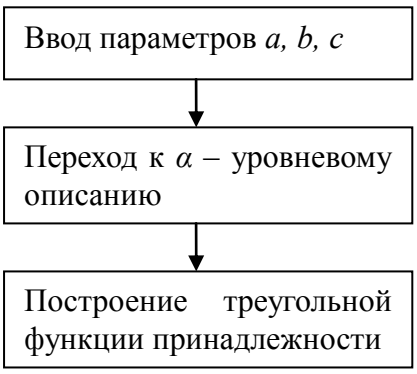
- быстрое и удобное построение функций принадлежности нечетких множеств;
- определение всех параметров функции принадлежности;
- сохранение графиков функций принадлежности и решений на диск.

Программа реализована на алгоритмическом языке Object Pascal в среде Delphi. Работает в любой среде совместимой с Windows 98 SE, 2000, XP, Vista. Дисковой памяти для запуска программы требуется не менее 10 Mb. Оперативной памяти для нормальной работы программы требуется не менее 15 Mb. Хотя программа может работать и с другой конфигурацией.

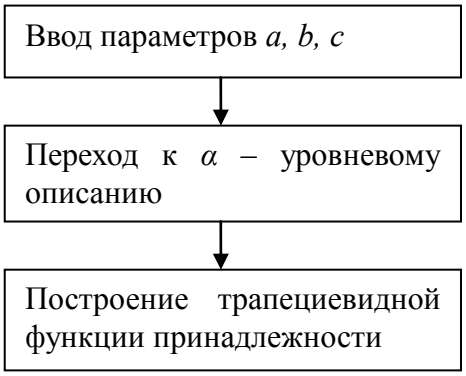
Рассмотрим алгоритмы подпрограмм, которые реализуют решения функций принадлежности данной программы.

Для построения треугольной и трапециевидной функций принадлежности алгоритмы подпрограмм выглядят следующим образом:

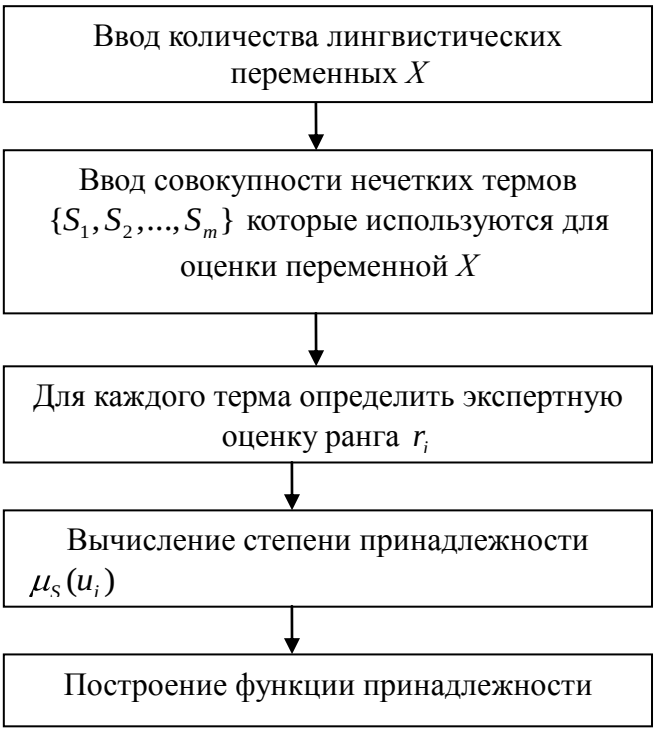
- для треугольной функции принадлежности:



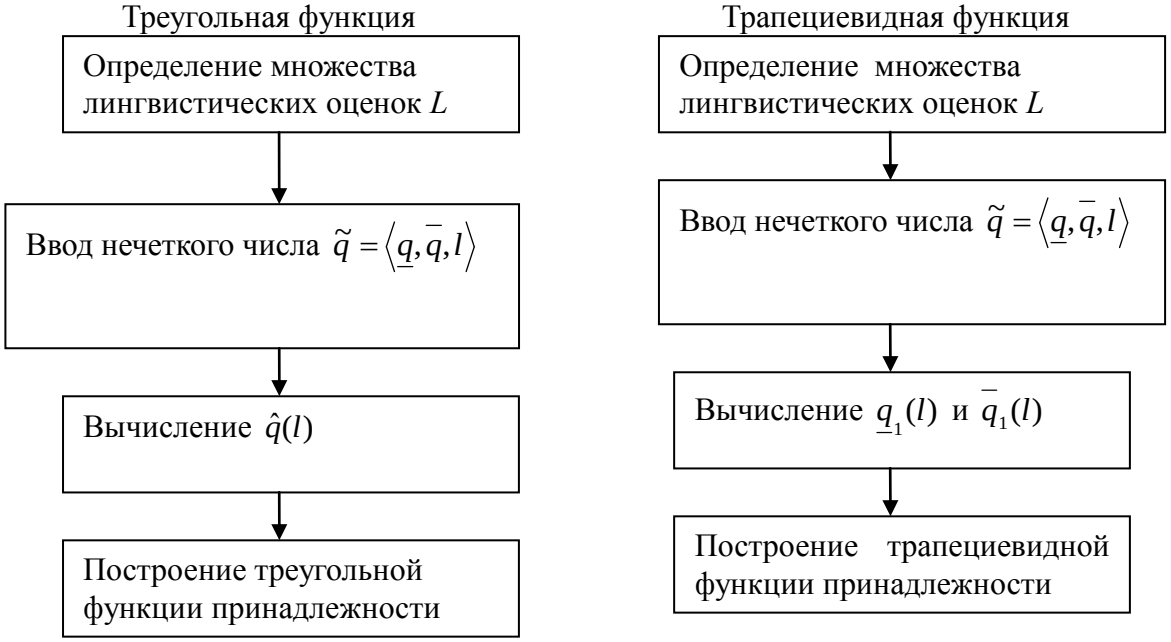
- для трапециевидной функции принадлежности:



Для построения функции принадлежности методом парных сравнений, основанном на использовании ранговых оценок, алгоритм подпрограммы выглядит следующим образом:



Рассмотрим алгоритм подпрограммы перехода от l – формы нечеткого числа к трапециевидной и треугольной функции принадлежности:



ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ЭКСПОНЕНЦИАЛЬНОЙ ФУНКЦИИ ПРИНАДЛЕЖНОСТИ

Курилова Т.И. – студентка, Архипова А.Б. – аспирант
Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

В любом виде деятельности очень важную роль играет процесс руководства, ведь от принимаемых решений зависит многое. В обеспечении безопасности информации неверное решение «сверху» может обернуться утечкой или потерей информации.

Под принятием решений понимается выбор одной альтернативы из полученного или заданного множества альтернатив. Реализация любой альтернативы предполагает наступление некоторых последствий, анализ и оценка которых по векторному критерию эффективности полностью характеризуют альтернативу. Решение задач сводится к выявлению и исследованию предпочтений лица, принимающего решения (далее, ЛПР), а также к построению на этой основе адекватной модели выбора наилучшей в некотором конкретном смысле альтернативы. Важной особенностью задач принятия решений является необходимость учета субъективных суждений ЛПР при формализации предпочтений и выборе наилучшей альтернативы. Эта особенность означает, что различные ЛПР в одной и той же ситуации принятия решений, на основе одной и той же модели могут получить различный результат.

Сложность связей ситуации принятия решений, отсутствие точного прогноза последствий приводят к тому, что при оценке и выборе альтернатив возможно, а зачастую и необходимо использовать и обрабатывать качественные нечеткие оценки.

Будем полагать, что в ситуациях принятия решений, когда хотя бы один из элементов (исходы, критерии, предпочтения и так далее) описывается качественно, нечетко, имеют место задачи многокритериального принятия решений при нечеткой исходной информации.

Перспективным направлением разработки методов принятия решений при нечеткой исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной. К настоящему времени в этом направлении получены конкретные практические и теоретические результаты. Их анализ позволяет сформулировать основные вопросы, возникающие при разработке и реализации методов и моделей принятия решений при нечеткой исходной информации. К ним можно отнести следующие:

– построение функций принадлежности нечетких множеств;
– выполнение операций над нечеткими числами;
– сравнение и упорядочение нечетких множеств и чисел;
– разработка моделей принятия решений [8].

Для использования в моделях принятия решений информации, формализованной на основе теории нечетких множеств, необходимы процедуры построения соответствующих функций принадлежности. Построение последних является важным компонентом в формализации задач принятия решений. От того, насколько адекватно построенная функция отражает знания эксперта или экспертов, во многом зависит качество принимаемых решений.

Следует отметить, что обработка и представление извлеченной экспертной информации о технологии решения задач принятия решений применительно к этапам рассматриваемого процесса может осуществляться посредством функций принадлежности (ФП) различными способами, выбор которых зависит от того, какие цели преследуются данным процессом и в зависимости от вида задачи принятия решения.

При решении задач защиты информации, моделирование процессов принятия решений в нечетких условиях и других прикладных задачах можно использовать многочисленные методы формирования функции принадлежности [6].

Данный метод построения ФП основан на использовании нечетких чисел, приблизительно равных некоторому четкому числу, и приближенных интервальных оценок, отражающих мнения экспертов по рассматриваемому вопросу. Задача сводится к отысканию параметров заранее заданной (экспоненциальной) функции, при решении которой используются результаты экспертного опроса.

Для построения функции принадлежности чисел, которые приблизительно равняются некоторому K, можно использовать функцию:

$$\mu_K(x) = e^{-\alpha(K-x)^2},$$

где α определяется по выражению:

$$\alpha = -4\ln(0{,}5)/\beta^2,$$

β - расстояние между точками перехода (a и b), то есть точками, в которых функция $\mu_K(x)$ приобретает значение 0,5. Параметр β определяется по специальному алгоритму и таблице, построенной по данным экспертного опроса (таблица 1).

Таблица 1 Расстояние между точками перехода

U	β(u)
1,2,3,4,5,6,7,8,9	0,46(u)
10,20,30,40,60,70,80,90	(0,357-0,00163u)u
35,45,55,65,75,85,95	(0,213-0,00067u)u
5	2,8
15	6,48
25	6,75
50	24
Другие двузначные числа	0,5(β(10E(u/10)+5)+ β(u-10E(u/10)))

Рассмотрим натуральное число K, в котором q – разряд младшей значащей цифры. Возможные значения q разбиваем на классы остатков по модулю три ($q \ mod \ 3$). Вводим переменную d, значение которой – представители данных классов {0,1,2} и получаем классы эквивалентности M_d $\{d=0,1,2\}$. Потом используем целочисленную переменную U, которая определяется в пределах от 1 до 99. По результат опроса выяснено, что в зависимости от U можно находить значение $\beta(u)$. Значение $\beta(u)$ зависит также и от того, к какому классу M_i принадлежит число K:

r_q – цифра, которая находящаяся в q-м разряде числа K.

– если $K \in M_0$ (например, 300, 300000 и т.п.), то β зависит только от r_q: $u=10r_q$, $\beta = \beta(u)10^{q-2}$, где β находится по таблице 1.

– если $K \in M_1$ (например, 101, 202000 и т.п.), то, возможны два варианта:

– $r_{q+1} = 0$, тогда β зависит только от r_q: $u=r_q$, $\beta = \beta(u)10^{q-1}$;

– $r_{q+1} \neq 0$, тогда β зависит от двух последних значащих цифр числа K: $u=10r_{q+1}+r_q$, $\beta = \beta(u)10^{q-1}$.

– если $K \in M_2$ (например, 2140,20 и т.п.) также возможны два варианта:

– $r_{q+1} = 0$, тогда $u=10r_q$, $\beta = \beta(u)10^{q-2}$;

– $r_{q+1} \neq 0$, тогда $u=10r_{q+1}+r_q$, $\beta = \beta(u)10^{q-1}$.

На основе β находятся значения α, а дальше строят ФП $\mu_K(x)$. Точки перехода определяются по следующим формулам:

$$a = K - \beta/2,\ b = K + \beta/2.$$

В таблице 1 выражение $E(u/10)$ означает антье (целая часть числа x, то есть наибольшее целое число, не превосходящее x) от $(u/10)$.

Пример: Достаточная длина секретного ключа для обеспечения конфиденциальности информации составляет 11 символов.

В данном случае K=11, следовательно, q=1, а $d=q \bmod 3=1 \bmod 3=1$, класс эквивалентности $M_d=M_1$. Так как $K \in M_1$ и $r_q=r_1=1$, то $r_{q+1}=r_2=1 \neq 0$, тогда $u=10r_{q+1}+r_q=10\times1+1=11$, следовательно $\beta = \beta(u)10^{q-1}$, по таблице 1 определяем $\beta(u)$, тогда:

$$\beta = \beta(u)10^{q-1} = \beta(11)10^{2-2} = 0{,}5(\beta((11/10)) \times 10 + 5) + \beta(11 - 10 \times (11/10))) = 0{,}5(\beta(15) + \beta(1)) =$$
$$= 0{,}5(6{,}48 + (0{,}46 \times 1)) = 0{,}5 \times 6{,}94 = 3{,}47$$

, зная расстояние между точками перехода, определяем α: $\alpha = -4\ln(0{,}5)/\beta^2 = -4 \times -0{,}693/12{,}041 = 0{,}23$ и строим функцию $\mu_K(x)$. Точки перехода будут равны:

$$a = 11 - 3{,}47/2 = 9{,}265;$$
$$b = 11 + 3{,}47/2 = 12{,}735;$$

$$\mu_K(x) = e^{-0{,}23(11-x)^2}.$$

Графическое изображение $\mu_K(x)$:

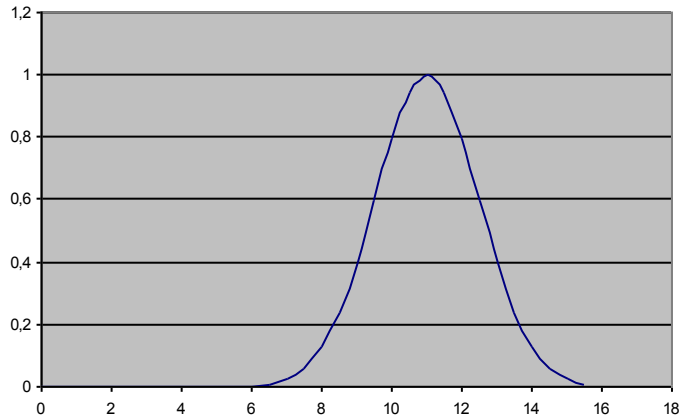


Рисунок 1 – График функции $\mu_K(x) = e^{-0{,}23(11-x)^2}$.

Таким образом, данный метод построения функции принадлежности основан на

использовании нечетких чисел, приблизительно равных некоторому четкому числу, и приближенных интервальных оценок, отражающих мнения экспертов по рассматриваемому вопросу. Задача сводится к отысканию параметров заранее заданной (экспоненциальной) функции, при решении которой используются результаты экспертного опроса.

Из анализа различных источников [1-5], посвященных методам построения функций принадлежности, данный метод целесообразнее всего использовать при решении задач выработки и оценки альтернатив.

Список литературы

1. Вилкас Э. Й., Майминас Е. З. Решения: теория, информация, моделирование. – М., Радио и связь, 1981.
2. Борисов А.Н., Алексеев А.В., Меркурьев Г.В. и др. Обработка нечеткой информации в системах принятия решений. – М., Радио и связь, 1989.
3. Аверкин А. Н., Батыршин И. З., Блишун А. Ф. и др. Нечеткие множества в моделях управления и искусственного интеллекта. – М., Наука, 1986.
4. Кофман А. Введение в теорию нечетких множеств. – М., Радио и связь, 1982.
5. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решения на основе нечетких моделей: примеры использования. – Рига, ”Знание”, 1990, 184 с.
6. Захаров В. А. О выборе методов построения функций принадлежности для формализации задач принятия решений. [электронный ресурс].- http://www.smolensk.ru/user/sgma/MMORPH/N-12-html/borisov/zakharov/zakharov.htm
7. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - К.: МК-Пресс, 2006. - 320с, ил.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. [электронный ресурс].- http://domarev.com.ua/book-02/oglav.htm

ОБ УЧЕБНО-МЕТОДИЧЕСКОМ КОМПЛЕКСЕ ПО ДИСЦИПЛИНЕ «ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ»

Наволокин Р.В. – студент, Белов В.М. –к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

В системе высшего профессионального образования все большее распространение получают учебно—методические комплексы (УМК). УМК специально разрабатывают для преподавателей и студентов по каждой дисциплине.

При разработке УМК авторы и ведущие преподаватели дисциплин руководствуются следующими главными требованиями к его содержанию:

- УМК по полноте содержания составляют таким образом, чтобы минимизировать обращение обучающегося к дополнительной учебной информации;
- УМК содержат модульный принцип построения содержания;
- УМК имеют рекомендации и инструкции по изучению материала и организации самостоятельной работы;
- УМК имеют в качестве обязательных элементов контрольные задания, глоссарий, вопросы для самопроверки с ответами, тренировочные тесты.

Студент обращается к УМК как к своеобразному «самоучителю», содержащему всю информацию о существующих требованиях к знаниям и умениям обучаемого, и, самое главное, сведения об источниках, из которых эти знания можно получить. Применять УМК в самостоятельной работе студентов необходимо в соответствии с основными методическими принципами обучения:

1. Целостности. УМК должен давать полное представление об изучаемой дисциплине. Это может быть достигнуто специальным структурированием учебного материала, например, в виде учебных модулей.

2. Структурирования. УМК должен быть построен таким образом, чтобы каждая тема, раздел, занятие имели одну и ту же структуру и представляли собой законченный учебный элемент.

3. Цикличности. УМК должен быть многоуровневым. Каждый уровень или учебный модуль рассчитан на определенную степень готовности к восприятию знаний; переход от одного уровня (модуля) к другому реализуется по мере накопления и усвоения знаний, формирования навыков и умений по дисциплине.

4. Проблемности. Знания должны не передаваться в готовом виде, а приобретаться в результате поисково-творческого процесса.

5. Наглядности. Представление новой информации обеспечивается техническими и мультимедийными средствами обучения, проведением опыта или постановкой эксперимента и анализом результатов.

6. Положительной мотивации познания. Оценка деятельности студента должна побуждать желание успешно выполнить поставленную задачу, положительную мотивацию и интерес к будущей деятельности на перспективу.

7. Индивидуализации. Методы и сроки изучения УМК должны быть выбраны и реализованы в зависимости от имеющегося уровня знаний, целей обучения и психологических особенностей личности.

8. Самообразования. УМК должен быть рассчитан на самостоятельную работу студентов.

В результате проведенного мною анализа существующих УМК и другой литературы по дисциплине «Экономика защиты информации» выяснилось, что большая ее часть не соответствует выше приведенным принципам и не может предоставить студентам систему знаний об экономической безопасности государства, отдельных организаций и фирм, об основных экономических проблемах защиты информации, таких, как:

- основные подходы к определению экономического ущерба, нанесенного информации, и затрат на ее защиту;
- определение экономической эффективности защиты информации и инвестиций в комплексные системы защиты информации;
- использование страхования как способа экономической защиты информации.

Поэтому на кафедре «Защиты информационных ресурсов и систем связи» в рамках дипломной работы было принято решение разработать учебно-методический комплекс по дисциплине «Экономика защиты информации», который позволит студентам специальности получить следующие основные знания:

- об основных экономических понятиях и критериях определения эффективности хозяйственно-экономической деятельности;
- о месте информации в структуре общественного производства, ее роли как ресурса экономики и фактора производства;
- об основах обеспечения экономической безопасности государства, общества, личности;
- об уровнях и объектах экономической безопасности, методах ее обеспечения;
- о правовых основах и основных положениях определения экономической эффективности защиты информации;
- и другие.

Учебно-методический комплекс будет включать в себя следующие основные разделы:

1) теоретический материал по программе курса, состоящий из нижеперечисленных основных блоков:

- Введение;
- Экономические проблемы информационных ресурсов и защиты информации;
- Экономическая безопасность;

-Определение экономической эффективности защиты информации – основные положения;

- Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту информации.

- Производственно-хозяйственная деятельность организаций как потребитель и источник экономической информации, подлежащей защите;

- Страхование как метод защиты информации.

2) лабораторный практикум, состоящий из вопросов и задач по каждой теме;

3) контрольно-измерительные задания (контрольные работы, тестирования, а также вопросы к экзамену).

Комплекс позволит будущим специалистам в области защиты информации экономически обоснованно решать проблемы выбора и использования прогрессивных технологий защиты информации, создания комплексных систем защиты и обеспечения бесперебойного их функционирования.

ЭКОНОМИЧЕСКИ ОПТИМАЛЬНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Киселев Н.О. – студент, Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

С каждым годом все больше предприятий и организаций во избежание потерь от несанкционированного использования конфиденциальной информации инвестируют средства в системы защиты информации. Как показывает практика, определить оптимальный объем эффективных инвестиций в системы защиты информации довольно сложно, поскольку теория данного вопроса лежит в пересекающейся плоскости экономических и информационных наук.

Инвестиции в разработку проектов защиты объекта, закупку необходимых элементов безопасности и эксплуатацию систем защиты для владельца информации есть ни что иное, как материализованный экономический ущерб. Идя на эти траты, пользователь надеется избежать большего ущерба, связанного с возможным нарушением конфиденциальности. Возникает дилемма: внести плату (частично реализовав ущерб) за возможность уклонения с долей вероятности или допустить возможность ущерба в полной мере, не тратя ничего. Разумное решение состоит в определении оптимальных вложений в системы защиты, обеспечивающих минимальные финансовые потери владельца информации при несанкционированных действиях с нею.

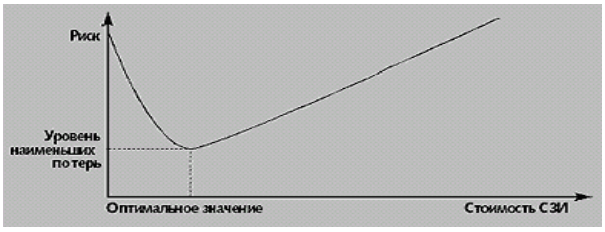
Перед пользователем стоит задача создания оптимальной, с экономической точки зрения, системы защиты информации. Эта задача не так характерна для государственных организаций, однако весьма актуальна для хозяйственно самостоятельных субъектов, ориентированных на деятельность в рыночных условиях.

Наиболее надежными системами защиты информации (СЗИ) являются те, в которых комплексно реализованы все возможные и доступные меры — морально-этические, законодательные, организационные, экономические и технические. Однако комплексные решения очень дороги и могут быть реализованы далеко не всегда. Кроме того, ущерб от утраты защищаемой информации или от разного рода несанкционированных действий с ней может быть гораздо меньше стоимости СЗИ. Поэтому уровень финансовых средств, выделяемых на создание и эксплуатацию СЗИ, должен быть сбалансированным и соответствовать масштабу угроз. Если стоимость СЗИ по сравнению с предполагаемым ущербом мала, то основным фактором риска собственника являются экономические потери от несанкционированных действий с принадлежащей ему информацией. В противоположной ситуации основные потери связаны с чрезмерно высокой стоимостью СЗИ. Необходимо при этом отметить, что затраты на СЗИ носят детерминированный характер, поскольку они уже

материализованы в конкретные меры, способы и средства защиты, а вот ущерб, который может быть нанесен при несанкционированных действиях, — величина случайная.

Такой качественный анализ позволяет предполагать, что существует область экономически оптимальных СЗИ, обеспечивающих наименьший риск собственника информации. В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации в течение определенного периода времени. Проведенное автором исследование, основанное на количественном моделировании риска, подтвердило это предположение, обеспечив оценку параметров экономически оптимальных СЗИ.

Моделирование риска собственника информации при создании и эксплуатации СЗИ осуществлялось на основе функциональных зависимостей между риском R, стоимостью СЗИ S, вероятностью преодоления СЗИ и нанесения ущерба собственнику p и размером возникающего при этом ущерба U.

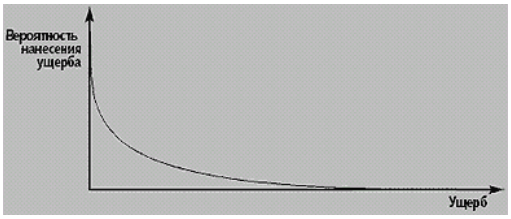


Не останавливаясь на конкретных моделях, отметим, что принципиально возможны три случая ($\partial p/\partial s<0$, $\partial p/\partial s=0$ и $\partial p/\partial s>0$), которые во многом предопределяют облик оптимальных решений и соответствующих СЗИ, их реализующих.

Типичная зависимость уровня риска от стоимости СЗИ, полученная при условии того, что вероятность нанесения ущерба p уменьшается с ростом стоимости системы S (т.е. соответствующая производная отрицательна, $\partial p/\partial s<0$) приведена на рисунке. Ее анализ показывает, что применение даже недорогих способов и средств защиты информации резко снижает суммарные потери собственника. Таким образом, вложение средств в СЗИ уже в сравнительно небольших размерах является очень эффективным. При некоторой стоимости СЗИ риск имеет наименьшее значение. Эта стоимость является оптимальной. Дальнейший, сверх оптимального значения, рост затрат на СЗИ будет вести к увеличению экономических потерь собственника информации. Его выигрыш в повышении надежности системы защиты и соответствующем снижении вероятности ущерба от несанкционированных действий будет нивелироваться и обесцениваться чрезвычайно высокой стоимостью самой СЗИ. Поэтому наилучшей стратегией собственника информации будет, очевидно, использование СЗИ, обеспечивающих минимум риска. Эффективность такого решения подтверждается результатами численного моделирования, в соответствии с которыми использование экономически оптимальных СЗИ приводит к снижению суммарных ожидаемых потерь примерно на порядок по сравнению с базовыми решениями.

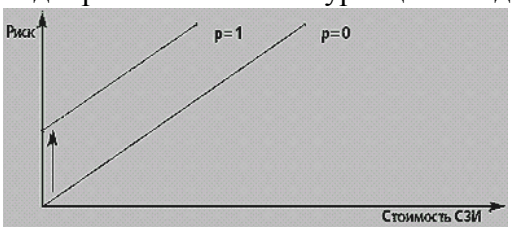
Чем больше оценка размера вероятного ущерба, тем выше и оптимальная стоимость СЗИ, однако эта зависимость достаточно гладкая, особенно в диапазоне больших значений ожидаемого ущерба. Следовательно, даже если ценность защищаемой информации возросла, то это отнюдь не означает необходимости пропорционального наращивания технических возможностей и соответствующего удорожания СЗИ.

Результаты численного моделирования подтвердили, что экономически оптимальная СЗИ не является самой безопасной. Более того, вероятность ущерба от несанкционированных действий при реализации такой системы может превышать в несколько раз минимально возможные значения показателей безопасности защиты информации. Поэтому применение изложенного подхода ограничено областью экономической целесообразности. В случаях, когда доминирующим требованием является обеспечение абсолютной безопасности информации, реализация концепции экономически оптимальной СЗИ не применима. Это относится, например, к сведениям, составляющим государственную тайну. Тем не менее, оптимальные СЗИ обеспечивают адаптацию требований безопасности к размеру возможного ущерба.



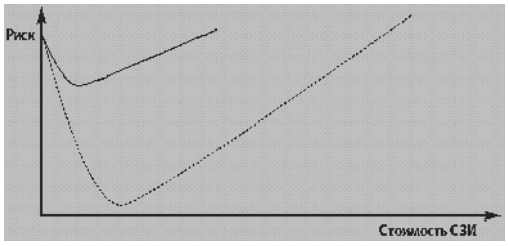
На рисунке приведена зависимость вероятности несанкционированных действий с защищаемой информацией при оптимальной СЗИ от величины ущерба. Изложенные результаты базируются на вполне логичном предположении о том, что более высокий уровень безопасности достигается за счет увеличения стоимости СЗИ. Для придания завершенности, рассмотрим и два других случая.

Уровень универсальной обобщенной характеристики безопасности СЗИ — вероятности нанесения ущерба не зависит от стоимости системы защиты ($\partial p \partial s=0$). К сожалению, такой случай правдоподобен. Например, если организация-подрядчик, осуществляющая проектирование СЗИ, предлагает своему заказчику более дорогое решение, хотя такой же уровень безопасности может быть достигнут и за меньшую плату. Оказывается, что такое недобросовестное решение приводит к зависимости риска владельца защищаемой информации от стоимости СЗИ, показанной на рисунке, где p — вероятность нанесения ущерба, а стрелкой показано направление изменения риска при увеличении этой вероятности. Подобная зависимость технических характеристик СЗИ от ее стоимости может реализовываться и в случае монополизма поставщика, инфляционных процессах, недобросовестной конкуренции и т.д.



Если СЗИ фактически обладает высокими характеристиками безопасности, то для снижения своего риска владельцу информационного ресурса необходимо добиваться снижения стоимости системы. Если же изначально характеристики безопасности СЗИ неудовлетворительны, то единственно разумным решением является отказ от нее.

Уровень универсальной характеристики безопасности СЗИ имеет тенденцию в некотором ценовом диапазоне к снижению с ростом ее стоимости ($\partial p/\partial s>0$). Такая ситуация также возможна — например, когда элементы защиты содержат невыявленные ошибки, а СЗИ «совершенствуется» путем наращивания из таких элементов. В этом случае зависимость риска владельца защищаемой информации от стоимости СЗИ показана на рисунке, где для сравнения пунктиром дан риск при $\partial p/\partial s<0$.



В связи с тем, что общий уровень риска возрастает во всем стоимостном диапазоне, необходимо провести тщательный анализ и поиск оптимального решения.

Стоимость СЗИ можно существенно снизить при использовании страховых инструментов. Эффективность этого метода во многом зависит от точности определения страховой стоимости защищаемых информационных ресурсов, а также степени соответствия тарифной ставки вероятности несанкционированных действий. Реализации страхования информации мешает фундаментальная проблема отсутствия достаточно точных практических методик по определению ее стоимости и обоснованию тарифов. Сколь сложен этот вопрос, можно судить хотя бы по дискуссиям по смежной теме — концепции общей стоимости владения информационной системой (TCO — total cost of ownership). ИТ-специалисты отмечают множество проблем при практическом использовании данной концепции, хотя в основе информационных систем и лежат вполне материальные вещи, имеющие известную стоимость. Поэтому попытки использования экспертного метода или декларируемого рыночного подхода, основанного на оценке популярности и востребованности информационного ресурса, во многих случаях заведомо неприемлемы.

Необходимо приложение дополнительных усилий для разработки практических методик оценки стоимости информации.

В заключение отметим, что оптимальные СЗИ наиболее целесообразны для экономически самостоятельных субъектов, которые в своей деятельности вынуждены соблюдать баланс между затратами на СЗИ и возможным ущербом. Реализация таких систем защиты информации возможна при тщательном учете всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь. Оценка экономически оптимальных параметров должна являться основой формирования конкретного технического облика СЗИ. К сожалению, сегодня проектирование СЗИ обычно осуществляется с ориентацией на произвольно выделяемый бюджет, не имеющий объективного обоснования по системе критериев «стоимость информации — размер возможного ущерба — риски». При этом владелец информационных ресурсов, если не проводит тщательного анализа и не оптимизирует размер выделяемых на СЗИ средств, практически всегда оказывается в экономическом проигрыше.

В данной работе рассмотрены основные варианты зависимостей риска собственника при инвестировании средств в те или иные системы защиты информации. Основной задачей при продолжении исследований в направлении экономической оценки систем защиты на предприятиях должна стать разработка конкретных методик расчета допустимых инвестиций в СЗИ и оценки их эффективности после начала работы систем.

СПОСОБ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НСД

Иващенко М.С. – студент, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В текущем году проблема защиты персональных данных проявилась особенно остро. В 2006 году был принят федеральный закон №152 – ФЗ «О персональных данных», в котором были изложены основные положения по вопросам, связанным с защитой персональных данных. Статья 25, пункт 3, устанавливает: «Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года». В связи с этим положением возникла необходимость во всех организациях, в которых действуют информационные системы персональных данных (ИСПДн), созданные до 27 июля 2006 года, привести их в соответствие с требованиями Федерального закона [1]. Такая задача стала актуальной и в отделе вневедомственной охраны при ОВД по Октябрьскому району г. Барнаула.

Информационная система персональных данных, вышеуказанной организации была создана до принятия Федерального закона «О персональных данных». Управлением вневедомственной охраны были выпущены приказы, в которых указаны необходимые мероприятия по приведению ИСПДн в соответствии с требованиями законодательства и нормативно-методическими документами Федеральной службы по техническому и экспортному контролю.

Среди основных требований есть следующее: «Жесткий регламент по использованию портов ввода вывода информации на СВТ, устройств записи на отчуждаемый носитель». Для выполнения данного требования необходимы выбор, установка и настройка соответствующих программных или программно-аппаратных средств защиты, а также разработка организационно-методических документов. Выбор должен производиться так, чтобы соотношение цена/возможности было оптимальным [2].

Среди средств контроля доступа к портам ввода-вывода информации на СВТ самыми известными в настоящее время являются DeviceLock и Zlock. Для обоснования выбора

средства выполнен сравнительный анализ указанных продуктов по критерию оптимальности для версий: DeviceLock Version Light и Zlock 2.5.

DeviceLock Version Light как и Zlock 2.5 позволяет использовать на компьютере только USB-устройства, предназначенные для обеспечения информационной безопасности (USB-ключи и смарт-карты eToken), и полностью блокировать доступ пользователей ко всем остальным типам USB-устройств, а также последовательным и параллельным портам, CD и DVD-накопителям, накопителям для дискет, внешним жестким дискам, флеш-дискам, ZIP-накопителям и так далее. Некоторое преимущество у комплекса DeviceLock Version Light заключается в том, что разрабатывался он специально в комплексе с продуктами Aladdin, вследствие чего совместимость с eToken выше чем у Zlock 2.5.

Оба рассматриваемых комплекса имеют возможность настройки так называемых «белых» списков устройств. Устройствами, занесенными в такие списки, разрешено пользоваться вне зависимости от установленных правил.

Оба рассматриваемых продукта обеспечивают выполнение следующих функций:

– блокировку доступа одних пользователей к устройствам и в то же самое время разрешение доступа к этим же устройствам другим пользователям;

– разрешение доступа "только чтение" для сменных носителей, жестких дисков и CD дисков;

– блокировку доступа к USB-порту, с разрешением использования заранее авторизованных устройств по принципу «белого списка»;

– многоуровневый контроль доступа – контроль на уровне интерфейса (USB-порта), контроль доступа на уровне типа устройств (по классам устройств) и вышеупомянутый контроль по «Белому списку»;

– протоколирование и аудит использования отдельных устройств на локальном компьютере, как отдельными пользователями, так и их группами. DeviceLock Version Light регистрирует все контролируемые события;

– централизованное управление доступом с помощью групповых политик в домене Active Directory.

DeviceLock Version Light сертифицирован на соответствие требованиям Руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» – по 3 уровню контроля и имеет сертификат соответствия ФСТЭК РФ № 1018/1 от 01 ноября 2006 года [3].

Система Zlock имеет Сертификат № 1653 от 28 июля 2008 года. Он удостоверяет, что средство защиты информации Zlock соответствует 3 уровню контроля по отсутствию недекларированных возможностей и имеет оценочный уровень доверия ОУД4 в соответствии с требованиями руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»[4].

Как видно, основным требованиям, предъявляемым к системам контроля доступа к портам ввода/вывода, рассматриваемые системы удовлетворяют. Безусловно, у комплекса Zlock 2.5 больше возможностей. Этот комплекс позволяет осуществлять теневое копирование и предоставляет возможность разрешить пользователям доступ к устройствам, используя лишь телефонную связь с администратором Zlock. В рассматриваемой организации данные возможности излишни. Они только усложняют установку и настройку комплекса.

Следующий вопрос - цена решения. Для применения комплекса Zlock 2.5 необходимо приобрести установочный комплект Zlock за 5250 рублей и лицензии на рабочие станции (по 1490 рублей за каждую лицензию, так как пользователей меньше 25). Комплекс DeviceLock Version Light распространяется бесплатно вместе с продукцией компании Aladdin.

Подводя итог, отметим, что основным требованиям к системам контроля портов ввода/вывода отвечают оба рассмотренных комплекса. У комплекса Zlock больше дополнительных возможностей, в которых нет необходимости, и которые лишь усложнят

установку и настройку системы. Комплекс DeviceLock Version Light является бесплатным.

В рассмотренном случае DeviceLock Version Light является оптимальным решением.

После выбора системы контроля доступа к портам ввода/вывода был разработан комплекс организационно-методических документов по установке, настройке и использованию этой системы, так как предоставляемая разработчиками документация описывает комплекс только как программный продукт, а возможности и задачи политики безопасности в ней не содержаться.

Комплекс содержит два документа. Первый содержит описание системы и инструкцию по установке. Второй представляет собой инструкцию по настройке и использованию.

Описание состоит из следующих частей [3]:

1) функциональные и качественные характеристики;

2) компоненты DeviceLock Version Light;

3) системные требования.

В части «компоненты DeviceLock Version Light» описываются ядро системы и консоль управления.

В инструкции по установке рассмотрены возможные способы установки:

1) интерактивная установка - установка программного обеспечения с помощью диалоговых окон;

2) удаленная установка - установка с помощью консоли управления DeviceLock Enterprise Manager Version Light;

3) установка через групповые политики - централизованная установка в Active Directory с помощью msi-пакета.

Каждый из описанных способов имеет свои преимущества и недостатки. Для установки интерактивной установки необходим непосредственный доступ к рабочей станции, на которую устанавливается система. Преимуществом данного способа установки является то, что нет дополнительной нагрузки на локальную (глобальную) сеть и сервер DeviceLock Version Light.

Для удаленной установки с помощью консоли управления DeviceLock Enterprise Manager Version Light нет необходимости в непосредственном доступе к рабочей станции, на которую устанавливается система, но эта станция должна быть включена в тот же домен, что и сервер DeviceLock Version Light. Нагрузка на сеть повысится при таком способе установки.

Для централизованной установки в Active Directory с помощью msi-пакета нет необходимости в непосредственном доступе к рабочей станции, на которую устанавливается система, но эта станция должна быть включена в домен, в котором создана групповая политика по установке системы. При таком способе установки помимо нагрузки на сеть возрастет нагрузка на контроллер домена.

Во втором документе больше внимания уделяется инструкции по настройке системы. Инструкция по настройке составлена для осуществления принятой в организации политики разграничения доступа к портам ввода/вывода. Эта политика подразумевает, что запрещено использование любых средств беспроводной связи. Компакт-диски и DVD-диски разрешается только читать некоторым сотрудникам, остальным запрещено даже чтение CD и DVD-дисков. Устройства Fire-Wire запрещено использовать. К floppy-дискам полный доступ только у администратора безопасности, у всех остальных доступ только на чтение. С USB-устройствами ситуация следующая. За сотрудниками закреплены flash-накопители и пользоваться разрешено только своими рабочими flash-накопителями, некоторым сотрудникам ввиду содержания их работы разрешено чтение информации с любых flash-накопителей (запись – только на закрепленные). В инструкции приведена последовательность действий для установки настроек таких, чтобы реализовывалась политика разграничения доступа к портам ввода/вывода. Также в инструкции по настройке отображены меры по предотвращению несанкционированного завершения работы системы DeviceLock Version Light.

Описанный способ защиты ИСПДн от НСД, обеспечивающий жёсткую регламентацию

использования портов ввода/вывода реализован в отделе вневедомственной охраны при ОВД по Октябрьскому району г.Барнаула. Планируется использование данного способа в других организациях города решающих задачи по защите информации в ИСПДн..

Список литературы

1. Федеральный закон №152-ФЗ от 27 июля 2006 года «О персональных данных». [электронный ресурс].- ПСС «Гарант».
2. Соколов А. Средства защиты персональных данных: проблемы оценки соответствия / Соколов А., Тачков – Connect. -2008, №12
3. Официальный сайт производителя средства контроля доступа DeviceLock. [электронный ресурс].- http://www.devicelock.com/ru/dl/index.htm
4. Официальный сайт производителя средства контроля доступа Zlock. [электронный ресурс].- http://www.securit.ru/products/info/zlock/

РАЗРАБОТКА ПРОГРАММЫ И МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО ОРГАНИЗАЦИИ И ТЕХНОЛОГИИ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

Володкович А.М. – студентка, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Организация мер по защите коммерческой тайны – проблема крайне сложная, методологически в нашей стране, в силу ее новизны, не проработанная. Литература по этому вопросу, к сожалению, сводится к комментариям закона. Практики в стране мало, да и делиться ее результатами особого желания ни у кого нет. Введение Четвертой части Гражданского кодекса РФ в 2008 году и новой редакции Федерального закона «О коммерческой тайне» расширяют возможности по реализации защиты информации, составляющей коммерческую тайну, однако требуют осознания и квалифицированного применения норм, что невозможно без соответствующей дополнительной подготовки. А такую подготовку можно получить лишь на курсах повышения квалификации.

Зарубежный, а теперь и российский опыт показывает, что без эффективного построения системы охраны коммерческих секретов, в том числе - с привлечением государственных институтов к защите интересов обладателя конфиденциальных сведений обойтись невозможно. Противодействовать недобросовестной конкуренции можно только законными методами, среди которых институт коммерческой тайны занимает важнейшее место [1].

Следовательно, надо учиться, в первую очередь – менеджменту, причем учиться у практиков или у тех, кто существующую практику в состоянии обобщить. А потом учить тех, кто работает с конфиденциальными сведениями на предприятии, причем не только сотрудников службы безопасности. Учить управленцев – владельцев бизнес-процессов, юристов, делопроизводителей, ИТ-специалистов, специалистов по защите информации. Переводить в цивилизованное русло отношения с персоналом, контрагентами, государственными чиновниками, внешними членами советов директоров и правлений, собственными акционерами. Решить эту проблему собственными силами предприятие не в состоянии [3]. Такая задача под силу лишь специализированным центрам и вузам ведущим подготовку специалистов в области информационной безопасности.

В связи с актуальностью рассматриваемой проблемы, наличием соответствующих лицензий по образованию в области информационной безопасности, практического опыта подготовки специалистов, в АлтГТУ на кафедре ЗИРСС выполняется инициативная НИР по теме «Разработка программ и методического обеспечения курсов повышения квалификации по защите информации», в том числе разработка программы и методического обеспечения курса повышения квалификации по организации и технологии защиты коммерческой тайны.

Чтобы программа курса обучения была успешной она должна быть научно обоснованной, соответствовать требованиям к образовательным программам, предъявляемым Министерством образования и науки РФ, а учебно-методическое и лабораторное обеспечение современным требованиям, предъявляемым к высшей школе. Кроме этого она должна быть полезной, уместной, интересной, отвечать нуждам фирмы, и нуждам конкретного отдела и нуждам каждого работника в отдельности.

Программа курса повышения квалификации разрабатывается для того, чтобы слушатели курса получили практические знания и навыки, позволяющие эффективно реализовывать механизмы защиты коммерческой тайны, определенные Федеральным законом и другими нормативными актами, обеспечивать условия предоставления правовой охраны государством интересов обладателей конфиденциальных сведений, организовать эффективный административный и технический контроль соблюдения режима коммерческой тайны.

Для научного обоснования программы были решены следующие задачи:

- выполнен анализ законодательства в области дополнительного образования и требований, предъявляемых к вузам по их организации и обеспечению[4];
- изучен опыт специализированных центров по повышению квалификации в области защиты коммерческой тайны;
- выполнен анализ литературы и новых методических документов по защите информации, и в частности по защите коммерческой тайны;
- определён состав знаний, умений и навыков необходимый и достаточный для слушателя курса, чтобы обеспечить организацию и реализовать технологии защиты коммерческой тайны на предприятии.

Анализ программ повышения квалификации учебных центров в этой области показал, что существующие курсы рассчитаны на специалистов, имеющих высокий уровень знаний в области защиты информации. Как следствие, программы курса краткосрочные и направлены на углубленное изучение определенных аспектов. Кроме того, они не отвечают требованиям, предъявляемым Минобрнауки к продолжительности курсов (не менее 72 часов), т.е. время проведения курсов значительно (в 2-3 раза) меньше минимального необходимого, позволяющего выдавать удостоверения об окончании курсов.

На основе состава знаний, умений и навыков необходимого и достаточного для слушателя разработана (составлена) рабочая программа.

Особое внимание в курсе уделяется практическим аспектам реализации режима конфиденциальности, в частности, разработке и вводу в действие внутренних нормативных документов предприятия, регулированию трудовых отношений, связанных с доступом к коммерческой тайне, способам минимизации рисков, вызванных угрозами конфиденциальным сведениям, в том числе с использованием механизмов лицензирования, сертификации и страхования. В курсе анализируются изменения системы охраны коммерческих секретов в связи со вступлением в действие с 1 января 2008 года Четвертой части Гражданского кодекса РФ и новой редакции Федерального закона "О коммерческой тайне".

Программа курса охватывает весь спектр мероприятий по защите коммерческой тайны в организации в рамках комплексной системы защиты. Объем курса – 72 часа, что позволяет слушателям получить достаточно подробные сведения в этой области, приобрести необходимые навыки и умения. Учебные занятия распределены по видам следующим образом (время в академических часах):

- Лекции-20;
- семинары- 12;
- практические занятия -8;
- самостоятельная работа -28;
- зачёт – 4.

В целом можно выделить следующие преимущества разработанной программы курса

повышения квалификации, в отличие от существующих на рынке образовательных услуг в специализированных центрах:

1. Программа является научно обоснованной и соответствует требованиям к образовательным программам, предъявляемым Министерством образования и науки РФ.

2. В программу курса включены как лекции – теоретический материал, так и программы проведения семинаров и практических занятий, которые позволяют закрепить полученные знания и приобрести практические навыки, в том числе по технической защите.

3. Разработка осуществлялась с учетом регионального фактора, что делает программу более доступной и актуальной.

Наряду с программой курса, разработана структура и состав методического обеспечения, которое включает в себя учебно-методический комплекс с необходимыми теоретическими материалами, а также планы семинаров и практических заданий. Методическое обеспечение предусматривает широкое использование информационных технологий и мультимедийных средств.

Учебно- методический комплекс включает:

- учебно-методическое пособие, содержащее хрестоматию по всем темам курса;
- методические рекомендации к семинарским и практическим занятиям;
- комплект «визуальных» лекций;
- тестовую систему;
- пакет слушателя, который выдаётся на компакт-диске и включает законодательство, нормативные документы и методические рекомендации по организации и технологии защиты коммерческой таны в организации, «визуальные» лекции.

Учебно-методическое пособие включает 5 разделов:

1. Место и роль коммерческой тайны в комплексной системе обеспечения безопасности деятельности предприятия.
2. Правовой институт коммерческой тайны.
3. Работа со сведениями, составляющими коммерческую тайну, в организации.
4. Техническая защита сведений, составляющих коммерческую тайну на предприятии.
5. Лицензирование деятельности и основные сведения о страховании информационных рисков.

Список литературы

1. Столяров Н. Зарубежный опыт защиты информации в процессе организации работы с кадрами (на примере США) [электронный ресурс] http://sec4all.net/usa-infoprot.html.
2. Емельянников М. Вы обладаете коммерческой тайной? // CIO 2007, №2.
3. Сарин С.В. Новое в законодательстве о коммерческой тайне. // Журнал НСБ «Хранитель» [электронный ресурс] - http://www.psj.ru.
4. Федеральный закон «Об образовании» (в редакции Федерального Закона Российской Федерацииот 01.12.2007 № 309-ФЗ).

РАЗРАБОТКА ПРОГРАММЫ И МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Мисюк А.С. – студент, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В июле 2006 года был утвержден федеральный закон N152 «О персональных данных» [1]. В сферу действия этого нормативно-правового акта попадают все юридические и физические лица, обрабатывающие персональные данные других граждан. Новый закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т.д., обеспечила конфиденциальность всей этой информации.

На принятие закона огромное влияние оказал выход России на международные рынки. Серьезным толчком для законодателей стало начало процесса вступления страны во Всемирную торговую организацию (ВТО).

После принятия закона правительством РФ приняты постановления, в которых даны наиболее общие, высокоуровневые требования, которые затем конкретизируются в нормативно-методических документах ФСТЭК, ФСБ и Минкомсвязи России.

Невыполнение требований нормативно-правовых актов, а также нормативных документов ФСБ и ФСТЭК по вопросам обработки персональных данных, приводит к утечкам данных из информационных систем государственных органов, банков, операторов связи, медицинских и других учреждений все это наносит ущерб и нарушает основные права на неприкосновенность частной жизни, закреплённые Конституцией РФ, а также дискредитирует государственные органы, осуществляющие контроль и надзор в данной сфере деятельности (Россвязькомнадзор, ФСБ России, ФСТЭК России). Руководители организаций, не выполняющих требования федерального закона, привлекаются к административной или иным видам ответственности. Возможны также гражданские иски к организации, принудительное приостановление или прекращение обработки персональных данных в организации, при определенных условиях возможно приостановление действия или аннулирование лицензий.

Согласно закону о персональных данных до 1 января 2010 года нужно привести в порядок все информационные системы персональных данных в соответствие с новым законодательством, в первую очередь – их подсистем информационной безопасности.

В соответствии с постановлением Правительства Российской Федерации от 17 ноября 2007 N 781[2] перечень задач по обеспечению безопасности персональных данных при их обработке в информационных системах состоит из большого количества этапов, а по каждому из этапов на предприятии должны быть разработаны соответствующие нормативные документы. К тому же здесь очень остро встает вопрос непонимания требований закона. Операторы, не имеющие квалифицированных специалистов в области ИБ, не смогут самостоятельно построить модель актуальных угроз безопасности и спроектировать систему защиты, обеспечивающую нейтрализацию этих угроз. Поэтому для более быстрого и качественного приведения подсистем информационной безопасности персональных данных к требованиям Федерального закона, необходимо провести переподготовку и обучение персонала. Эта проблема является актуальной и для организаций - операторов информационных систем персональных данных (ИСПДн) города Барнаула и Алтайского края.

Обладая соответствующими лицензиями, квалифицированными преподавателями АлтГТУ планирует проводить курсы повышения квалификации по защите персональных данных на базе Центра подготовки работников режимно-секретных подразделений Алтайского края, что сделает курс более доступным для слушателей г. Барнаула и Алтайского края. Для этой цели в рамках инициативной НИР кафедры ЗИРСС АлтГТУ по теме «Разработка программ и методического обеспечения курсов повышения квалификации по защите информации» ведётся разработка программы и методического обеспечения по указанной тематике.

Изучение и анализ, существующих программ повышения квалификации, в этой области показали, что существующие курсы, в основном, проводятся в Московских учебных центрах, краткосрочные и имеют высокую стоимость.[4]

Для разработки программы курса был проведен анализ международных соглашений, законодательства РФ в области персональных данных и в сфере информационной безопасности, а также подзаконных актов и методических документов ФСБ, ФСТЭК и Минкомсвязи России. В результате чего были выявлены наиболее важные и актуальные вопросы, касающиеся обеспечения безопасности персональных данных. На основе проведенного анализа и требований нормативных документов Министерства образования и науки РФ к программам дополнительного образования была составлена программа курса

повышения квалификации по защите персональных данных.

Программа курса рассчитана на 72 часа, что позволяет рассмотреть весь комплекс мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных регуляторов, а слушатели таких курсов получат удостоверение образца Минобрнауки. Распределение времени приводится в таблице 1.

Таблица 1 - Распределение учебного времени по видам занятий

Кол-во дней	Учебные занятия (в часах)						Число курсо- вых проек - тов, раб.	Зачет (часов)
	Общий объем	в том числе						
		Аудиторные				самост. работа		
		всего	из них					
			лекции	семин.	практ.			
8-10	72	40	20	12	8	28	нет	4

Для методического обеспечения программы разработана структура и определён состав методического обеспечения с учётом широкого использования компьютерных технологий и мультимедийных средств обучения слушателей. Учебно- методический комплекс включает:

– учебно-методическое пособие, содержащее хрестоматию по всем темам курса;

– методические рекомендации к семинарским и практическим занятиям;

– практические задания;

– комплект «визуальных» лекций;

– тестовую систему;

– пакет слушателя, который выдаётся на компакт-диске и включает нормативные документы и методические рекомендации о организации и технологии защиты ИСПДн.

Учебно- методическое пособие состоит из 5 разделов:

– персональные данные как объект защиты информации;

– правовое регулирование отношений, связанных с обработкой персональных данных в информационных системах;

– обеспечение безопасности персональных данных в организации;

– техническая защита персональных данных в информационных системах;

– лицензирование деятельности по технической и криптографической защите конфиденциальной информации.

Разработанный курс, поможет широкому кругу специалистов различных категорий, организовать обработку персональных данных в соответствии с требованиями российского законодательства.

Курсы предназначены для:

– руководителей организаций и их структурных подразделений, в ведении которых находится обработка персональных данных;

– руководителей и специалистов, непосредственно отвечающих за обеспечение информационной безопасности предприятий, охрану конфиденциальности информации;

– работников кадровых органов организаций и предприятий;

– юристов предприятий-операторов персональных данных;

– специалистов, реализующих мероприятия по технической защите конфиденциальной информации.

По окончании обучения слушатели приобретут знания:

– по проблемам охраны конфиденциальности персональных данных физических лиц в Российской Федерации;

– по вопросам правовой защиты персональных данных, организации контроля возможных каналов утечки;

– современных методов и средств технической защиты персональных данных.

Можно выделить следующие преимущества данного курса повышения квалификации:

– использование «визуальных» лекций делает курс более наглядным, доступным и понятным;

– все изученные материалы будут предоставлены слушателю курса, в виде пакета слушателя на компакт-диске с нормативно-правовой базой;

– после обучения, слушателям выдают государственные удостоверения о повышении квалификации.

Список литературы

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [электронный ресурс]- ПСС Гарант.
2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 17 ноября 2007 г. N 781) [электронный ресурс]- ПСС Гарант.
3. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15 сентября 2008 г. N 687) [электронный ресурс] - ПСС Гарант.
4. Защита персональных данных [электронный ресурс] - http://www.itsecurity.ru/

РАЗРАБОТКА МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Редькина Д.С. – студентка, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Вопросы, связанные с государственной тайной и ее охраной были и остаются актуальными во все времена. Защита государственной тайны является одним из наиболее важных направлений защиты информации в целом, так как от уровня защищённости государственных секретов зависит национальная безопасность страны. Немаловажным фактором при решении задач защиты государственной тайны выступает подготовка, переподготовка кадров и повышение их квалификации. В Алтайском крае Центром подготовки работников режимно-секретных подразделений Алтайского края созданным на базе Алтайского государственного технического университета проводятся курсы повышения квалификации по защите государственной тайны. При внедрении в процесс обучения информационных технологий, и в частности мультимедийных средств, возник ряд проблем, обусловленный различными особенностями этих курсов.

К таким особенностям относятся:

– слушатели курсов имеют различное (экономисты, технические специалисты) высшее образование;

– большой объем информации для слушателей, в связи со сжатыми сроками проведения курсов повышения квалификации;

– лекции по различным темам ведут преподаватели с различным уровнем педагогического мастерства (преподаватели университета, представители уполномоченных органов в области безопасности, краевой администрации);

– законодательство и нормативное регулирование в области защиты государственной тайны совершенствуется и изменяется;

Ещё одной важной особенностью, является то, что работникам режимно-секретных подразделений постоянно приходится сталкиваться с большим количеством различных форм документов, сложных по структуре и объемных по содержанию. Как показало анкетирование слушателей в 2008 году, эта проблема является актуальной для 90% слушателей.

Особенности и проблемы курсов обусловили необходимость разработки универсальной формы представления учебного материала, позволяющей удовлетворить потребности, как преподавателей, так и слушателей курсов. В качестве такой формы разработана «визуальная лекция» – информационная технология, предусматривающая отображение как графического материала, так и текстового, используемого лектором при чтении лекции а слушателями как «виртуального подсказчика».

Каждая такая лекция содержит необходимое количество специально подготовленных визуальных изображений, которые выполнены в схематичном или символическом виде (рисунки, схемы, формы документов). На слайды выносится информация в графической форме представления подкрепленная фрагментами текста лекции, в то время как в обычной лекции учебный материал воспринимается слушателями на слух. Наглядное представление особенно необходимо тогда, когда объекты не доступны непосредственному наблюдению, а слово преподавателя оказывается недостаточным, чтобы дать представление об изучаемом объекте. В этом случае система графических обозначений может взять на себя функции языка [1, 3]. Применение графического представления информации в обучении способствует восприятию предметов и изучаемых процессов, формирует представления об объективной действительности, а также способствует формированию полноценных образов изучаемых понятий. Качество и степень освоения учебного материала, при этом существенно возрастают [2, 4].

В наглядной форме может быть представлен основной материал лекции, а также наиболее сложные для понимания моменты и примеры, в том числе примеры заполнения различных форм документов.

Сочетание комментариев преподавателя с видеоинформацией или анимацией значительно активизирует внимание слушателей к содержанию излагаемого учебного материала и повышает интерес к изучаемой теме. При этом существенно изменяется роль преподавателя в учебном процессе. Преподаватель эффективнее использует учебное время лекции, сосредоточив внимание на обсуждении наиболее сложных фрагментов учебного материала [5].

Кроме того, использование визуальной лекции облегчает подготовку преподавателя к лекции. Обучающийся по такой лекции имеет возможность быстрого повторения наиболее значимых вопросов по рисункам и схемам.

Для решения проблемы обучения слушателей курсов составлению и заполнению документов и форм лекция снабжена необходимыми примерами и разъяснениями (виртуальные подсказки). При этом существует возможность перехода от формы документа непосредственно к примеру ее заполнения (рисунок 1), а также к описанию и особенностям заполнения отдельных граф формы (виртуальному подсказчику) – рисунок 2.

Рисунок 1 –Пример перехода от бланка формы к образцу

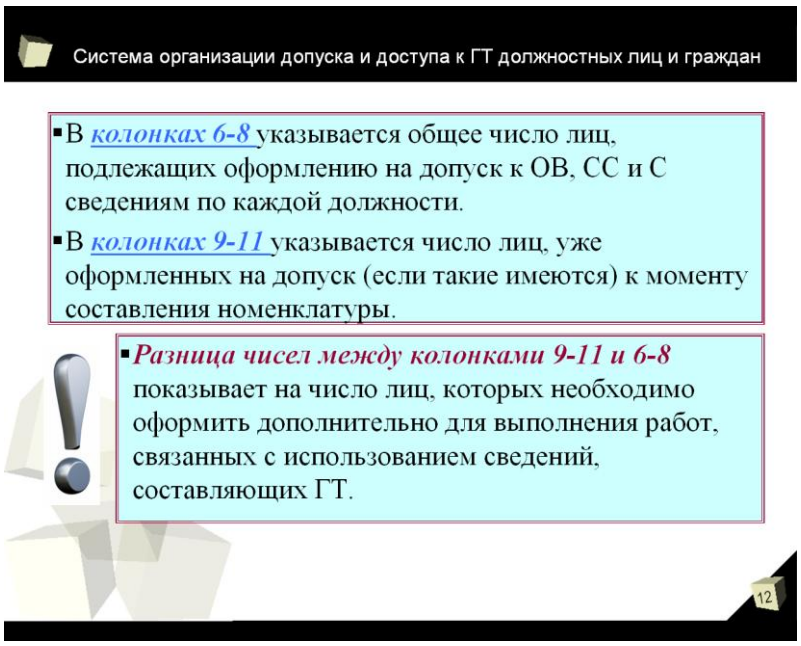


Рисунок 2 – Пример перехода к виртуальному подсказчику

Представление визуальной лекции осуществляется с помощью проектора и персонального компьютера на большой экран в лекционной аудитории. При этом преподаватель имеет возможность управлять показом очередного изображения, переходить по своему желанию к нужному фрагменту материала.

Разработанное с использованием рассмотренной технологии методическое обеспечение включается в пакет слушателя, который выдаётся на электронных носителях (компакт-дисках) и может использоваться слушателем прошедшим обучение на своём рабочем месте как электронное учебное и методическое пособие.

Рассматриваемая технология разработана в рамках выполнения инициативной НИР кафедры ЗИРСС АлтГТУ по теме «Разработка программ и методического обеспечения курсов повышения квалификации по защите информации», реализована для основных тем курсов по защите государственной тайны и планируется к использованию в учебном процессе по дисциплинам специальности «Комплексная защита объектов информатизации».

Список литературы

1. Петрова А.В., Глушков С.П. Опыт использования медиасредств в обучении безопасности жизнедеятельности. – Новосибирск: Сибирский университет потребительской кооперации, [электронный ресурс] - http://www.sibupk.nsk.su/confer/2009/doklad19.doc
2. Демин В.А., Демина Л.М. Новые информационные технологии как активные формы обучения в высшем образовании. – Московский государственный индустриальный университет. [электронный ресурс] - http://www.conf.muh.ru/010305/doc/demin.doc
3. Зайцева Е.А., Пунина Т.Г. Компьютерная графика: Учебно-методическое пособие. – Тамбов: Тамбовский государственный технический университет, 2006
4. Гудилина С.И. Наглядность в медиаобразовательных технологиях, 2007 [электронный ресурс] - http://www.art.ioso.ru/vmuza/naglyadnost/naglyadnost.htm
5. Смирнова М. А., Вилькер Д. В. Дидактические возможности применения мультимедиа в учебном процессе высшей школы: Интернет журнал СахГУ «Наука, образование, общество», 2006 [электронный ресурс] - http://journal.sakhgu.ru/work.php?id=13

ОРГАНИЗАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СИСТЕМЫ ZLOCK В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ БАНКА

Шимонаева А.Г. – студентка, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г.Барнаул)

Прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий. На практике для финансовых компаний наиболее эффективный способ обеспечить информационную безопасность в своих подразделениях — опереться на продуманный стандарт. Эту роль законодательной нормы обеспечения информационной безопасности выполняет Стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [1].

Согласно результатам исследований компании InfoWatch [2] при реализации его положений банки испытывают трудности при разработке пакета документов, рекомендованных Стандартом.

Для усиления информационной безопасности банка и повышения конкурентоспособности на финансовом рынке в 2008 году началось практическое внедрение Стандарта в одном из банков Алтайского края (Банк).

Так как авторы Стандарта поставили инсайдеров во главу угла — именно на минимизацию внутренних рисков в первую очередь должна быть направлена система информационной безопасности, а вопрос выбора конкретных мер, методов и аппаратных или программных средств её обеспечения оставили за собственником конкретной кредитной организации, то Банком было принято решение о внедрении специализированного программного продукта Zlock для противодействия инсайдерам [3].

Приказом руководства Банка была назначена группа сотрудников, ответственная за реализацию проекта, в состав которой вошел автор. Была поставлена задача по разработке нормативно-распорядительных документов по эксплуатации системы.

Для решения задачи проанализирована существующая система документооборота, определены нормативные акты, с которыми необходимо обеспечить совместимость как в краткосрочном периоде, так и в средне и долгосрочной перспективе, проведена оценка имеющихся мероприятий, направленных на борьбу с инсайдерами, разработана программа внедрения системы, включающая в себя проводимые мероприятия, срок исполнения и ответственных лиц.

По результатам проведенных мероприятий было определено, что больших изменений в документообороте производится не будет, а для регламентации порядка защиты информации в Банке с использованием программно-аппаратных средств противодействия инсайдерам необходимо разработать следующие организационно-распорядительные документы: порядок эксплуатации системы Zlock и инструкцию администратора. Требования к нормативно-распорядительным документам описаны в п.8.6 Стандарта.

Разработанный Порядок эксплуатации системы определяет функции структурных подразделений Банка при эксплуатации средства, а также:

– порядок администрирования и сопровождения системы, включая разделение обязанностей между подразделениями информатики и безопасности;

– процедуры автоматизированной установки и обновления программного обеспечения системы на автоматизированных рабочих местах сотрудников Банка;

– порядок согласования и предоставления доступа сотрудникам банка к информационным ресурсам;

– ответственность сотрудников за исполнение возложенных на них функций по эксплуатации системы, за выполнение политики безопасности по минимизации прав пользователей.

Кроме этого, в Порядке отражена политика ограничения по использованию портов ввода-вывода, как основного канала распространения конфиденциальной информации. Она включает в себя следующие правила разграничения доступа к аппаратным ресурсам компьютера:

– для внешних носителей – полный запрет личных носителей, ограничение использования по принципу необходимости, строгий учёт используемых носителей, назначение ответственных за информационную безопасность в каждом подразделении;

– для дополнительных устройств - отключения неиспользуемых устройств, запрет/контроль самостоятельной установки/подключения дополнительных устройств.

Определение полномочий пользователей по доступу к ресурсам средств вычислительной техники, осуществление административной поддержки (правильная настройка, контроль и оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.) вошло в функции службы безопасности. Общий контроль выполнения требований Порядка закреплен за подразделением безопасности.

Инструкция администратора безопасности системы Zlock – это правовой акт, содержащий правила, регулирующие деятельность сотрудников, контролирующих систему. Она определяет действия, обязанности и права администратора системы, ответственного за её функционирование, эксплуатацию, применение политики доступа к портам ввода – вывода.

При разработке документов, автор руководствовался следующими требованиями: документ должен позволять устанавливать персональную ответственность за участок работ, снижать вероятность нарушения установленного порядка обеспечения и халатного отношения к вопросам информационной безопасности, разрабатывать процедуры её обеспечения на всех этапах создания и развития и надежно управлять непрерывностью бизнеса.

Контроль за выполнением внутренних регулирующих документов в части, касающейся информационной безопасности, закреплен за службой информационной безопасности.

После успешного завершения опытной эксплуатации средство было введено в промышленную эксплуатацию. Разработанные автором организационные документы внедрены в действие в структурных подразделениях Алтайского банка Сбербанка России.

Список литературы

1. Стандарт Банка России СТО БР ИББС-1.0-2008 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения”
2. Официальный сайт компании InfoWatch. Аналитика. [электронный ресурс – 07.04.2009г.]. - http://www.infowatch.ru/analytics
3. Руководство администратора ZLock, SecurIT 2002-2007

О ПОСТАНОВКЕ ЗАДАЧИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ С ИНТЕРВАЛЬНО-ЗАДАННЫМИ ПАРАМЕТРАМИ

Микуров С.Н. – студент, Белов В.М. – к.ф.-м.н., д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Это заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Процесс разработки системы информационной безопасности, по сути, является процессом управления информационной безопасностью объекта и реализуется системой управления, включающей в себя помимо самого управляемого объекта, средства контроля его состояния, механизм сравнения текущего состояния с требуемым и формирователь управляющих воздействий для локализации и предотвращения ущерба вследствие угроз. Критерием управления в данном случае целесообразно считать минимизацию максимального информационного ущерба при минимальных затратах на обеспечение информационной безопасности, а целью управления - обеспечение требуемого уровня защищенности.

Сложные многоуровневые иерархические системы управления сталкиваются с неопределенностью параметров, невозможностью представить их в виде детерминированных или вероятностных параметров. Все это справедливо и для сферы информационной безопасности. Примером может служить управление информационными рисками одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации[4].

Качественные методики управления рисками, как правило, на основе требований международного стандарта ISO 177992002, принятые на вооружение во многих странах, несмотря на свою популярность, относительную простоту и разработанность, не подходят для решения различных оптимизационных задач, которые часто возникают в реальной жизни. Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих[4]. Для решения этих задач и разрабатываются методы и методики количественной оценки и управления рисками. У специалистов по информационной безопасности не всегда есть возможность дать количественную оценку риска в виде детерминированных или вероятностных величин.

Применение для оперирования с неопределенными величинами аппарата теории вероятности приводит к тому, что фактически неопределенность, независимо от ее природы, отождествляется со случайностью. Учет фактора неопределенности при решении задач во многом изменяет методы принятия решения: меняется принцип представления исходных данных и параметров модели, становятся неоднозначными понятия решения задачи и оптимальности решения. Наличие неопределенности может быть учтено непосредственно в моделях соответствующего типа с представлением недетерминированных параметров как случайных величин с известными вероятностными характеристиками, как нечетких величин с заданными функциями принадлежности или как интервальных величин с фиксированными интервалами изменения.

Впервые в отечественной литературе основы и методы интервального анализа были систематически изложены в[7]. В качестве последних работ в области интервального анализа можно привести монографию[6]. Монография еще закончена, но уже вполне пригодна к чтению.

Интервальный анализ используется в различных областях вычислительной и прикладной математики, при планировании экспериментов, в метрологии, при определении характеристик методов измерений; при решении задач управления сложными системами с интервально заданными параметрами. Алгоритмы решения интервальных задач обладают рядом преимуществ. Они ориентированы на использование ЭВМ, а кроме того, возможность получать на ЭВМ решение задач вместе с полным и строгим анализом ошибок вычислений.

При неопределенности данных интервальные методы являются естественным аппаратом оценивание погрешностей конечных результатов, дающий надежные двухсторонние границ искомых решений [1]. Несмотря на явные преимущества и отсутствие конкурентов, данные методы не получили широко распространения. В первую очередь из-за сложности и трудоемкости алгоритмов. Кроме того решения интервальных алгоритмов чувствительны к ошибочным результатам измерений, а соответственно к надежности исходных данных предъявляются повышенные требования. Перечисленные недостатки можно рассматривать как руководство к действию. Трудоемкость интервальных алгоритмов важно всегда ставить в соответствие с условием решаемой задачи. Требование надежности исходных данных одинаково как для детерминированных, так и для вероятностных методов[1]. Применение интервального анализа не требуется знание вероятностных характеристик неопределенных факторов, кроме того, во всех случаях даются гарантированные двусторонние аппроксимации искомых решений.

Не смотря на наличие работ в ряде областей, интервальный анализ в области информационной безопасности еще практически не применялся. Большая часть решений принимается на основе опыта или интуиции. Кроме того, широко применяющиеся экспертные оценки, часто представляются в интервальном виде, что является одной из причин актуальности применения интервального анализа для решения задач информационной безопасности.

На сегодняшний день необходимо адаптировать уже существующие методы оценивания параметров [1,3], оценивания фазового состояния[5], оптимизации[2] к задачам обеспечения информационной безопасности.

Список литературы

1. Белов В.М., Унгер Ф.Г., Карбаинов Ю.А., Пролубников В.И.. Тубулов Н.П. Оценивание параметров эмпирических зависимостей методом центра неопределенности. – Новосибирск: Наука, 2001. – 176 с.
2. Вощинин А. П., Сотиров Г. Р. Оптимизация в условиях неопределенности. — М.:МЭИ, София: Техника, 1989. — 224 с.
3. Гончаров С.А.. Белов В.М., Рябова Е.В., Гетманов В.Т. Оценивание параметров линейных экспериментальных зависимостей обобщенным методом центра неопределенности. – Рубцовск: РИО, 2005. – 130 с.
4. Петренко С. Методики и технологии управления информационными рисками [электронный ресурс – 06.04.2009]. - http://www.citforum.idknet.com/security/articles/risk/
5. Черноусько Ф.Л. Оценивание фазового состояния динамических систем. Метод эллипсоидов. – М.: Наука. Главная редакция физико-математической литературы, 1988. – 320 с.
6. Шарый С.П. Конечномерный интервальный анализ. – Издательство «XYZ», 2009. – 726с.
7. Шокин Ю.И. Интервальный анализ. – Новосибирск: Наука, 1981. – 112 с.