Содержание

ВВЕДЕНИЕ 9
1 КОМПЬЮТЕРНАЯ СИСТЕМА КАК СРЕДА РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 14
1.1 Понятийный аппарат информационной безопасности компьютерных систем 14
1.2 Компьютерная система, как распределенная компьютерная система 15
1.3 Классификация компьютерных систем по типу переменных состояний защищенности 18
1.4 Классификация угроз безопасности компьютерных систем 19
1.5 Числовые показатели информационной безопасности компьютерных систем 22
1.6 Периодичность переменных состояний защищенности. 23
1.7 Общие сведения о семействе законов распределения экстремальных значений 27
1.7.1 Предельные распределения экстремумов 27
1.7.2. Распределение Гумбеля 31
1.7.3 Распределение Мизеса 33
1.8 Алгоритм анализа статистических данных для формирования совокупности экстремальных значений случайной величины 35
1.9 Основные выводы по главе 38
2 РАЗРАБОТКА И ИССЛЕДОВАНИЕ РИСК-МОДЕЛЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ ЭКСТРЕМАЛЬНЫХ ЗНАЧЕНИЙ ПЕРЕМЕННЫХ СОСТОЯНИЙ ЗАЩИЩЕННОСТИ 40
2.1 Дискретизация риска 46
2.2 Параметры риска для переменных состояний защищенности, плотность вероятности наступления ущерба в которых распределены по закону Гумбеля. 54
2.3 Параметры риска для переменных состояний защищенности, плотность вероятности наступления ущерба в которых распределены по закону Мизеса. 62
2.4 Риск-анализ компьютерных систем на основе параметров рисков их переменных состояний защищенности. 69

2.4.1 Интегральная оценка рисков компьютерных систем для ущербов распределенных по законам Гумбеля и Мизеса в переменных состояний защищенности. 73

2.4.2 Оценка общего риска компьютерной системы при переходе от непрерывного к дискретному закону распределения. 77

2.5 Риск-анализ компьютерных систем в диапазоне ущербов 79

2.6 Основные выводы по главе 85

3 УПРАВЛЕНИЕ РИСКАМИ КОМПЬЮТЕРНЫХ СИСТЕМ 87

3.1 Стратегии управления рисками систем 87

3.2 Определение чувствительности параметров безопасности 90

3.3 Определение чувствительности функции риска по параметрам масштаба, положения и нелинейности для распределения Гумбеля. 95

3.4 Определение чувствительности функции риска по параметрам масштаба, положения и параметру нелинейности для распределения Мизеса. 104

3.5 Алгоритм минимизации риска на основании выражений функций чувствительности 115

3.6 Алгоритм наискорейшего спуска 120

3.7 Выводы по третьей главе 125

4 ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКАЯ ЧАСТЬ 126

4.1 Определение трудоемкости по разработке и построению риск-моделей информационно-телекоммуникационных сетей на основе экстремальных значений переменных состояний защищенности распределенных по законам Гумбеля и Мизеса. 126

4.2 Построение календарного плана разработки и построения риск-моделей информационно-телекоммуникационных сетей на основе экстремальных значений переменных состояний защищенности распределенных по законам Гумбеля и Мизеса 131

4.3 Расчет сметной стоимости и договорной цены разработки и построения риск-моделей информационно-телекоммуникационных сетей на основе экстремальных значений переменных состояний защищенности распределенных по законам Гумбеля и Мизеса 140

4.4 Прогнозирование ожидаемого экономического эффекта от использования результатов разработки и построения риск-моделей информационно-телекоммуникационных сетей на основе экстремальных значений переменных состояний защищенности распределенных по законам Гумбеля и Мизеса 145
4.5 Пример расчета экономического ущерба, вследствие превышения уровня переменных состояний защищенности больше допустимого уровня 153
5 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ 156
5.1 Анализ вероятных вредных и опасных факторов при работе с персональным компьютером 156
5.1.1 Освещенность рабочей зоны 157
5.1.2 Шум на рабочем месте 159
5.1.3 Воздействие электрического тока 160
5.1.4 Ионизирующие излучения в рабочей зоне 162
5.1.5 Электромагнитное излучение в рабочей зоне 162
5.1.6 Микроклимат рабочей зоны 164
5.2 Защита от вероятных и опасных процессов 165
5.2.1 Расчет необходимой освещѐнности рабочей зоны 165
5.2.2 Режим труда и отдыха оператора 169
5.3 Обеспечение безопасности жизнедеятельности в экстремальных ситуациях 171
5.3.1 Требования по противопожарной безопасности 171
ЗАКЛЮЧЕНИЕ 174
СПИСОК ЛИТЕРАТУРЫ 177

8 (952) 106-88-60 vk.com/a.projectit a.projectit

ВВЕДЕНИЕ

Актуальность исследования. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всѐ более и более актуальными – и одновременно более сложными.

Результаты и перспективы информатизации общества свидетельствуют о наличии устойчивой тенденции интегрирования компьютерных средств и средств связи в рамках нового класса систем – компьютерных систем (КС) [43,64,88]. Системы данного класса с каждым днем находят все более широкое применение в [12,31,38,44,59], самых различных областях общественной жизни: начиная от деятельности телекоммуникационных компаний в рамках отдельных регионов и заканчивая деятельностью важнейших государственных институтов, таких как органы государственного управления, обороны, внутренних дел и т.д. При этом, [49] неконтролируемый рост числа абонентов КС, увеличение объемов хранимой и передаваемой ими информации, их территориальная распределенность приводит к возрастанию потенциально возможного количества преднамеренных и непреднамеренных нарушений безопасности, возможных каналов несанкционированного проникновения в сети с целью чтения, копирования, подделки программного обеспечения, текстовой и другой информации. При этом по сравнению с изолированными (автономными) автоматизированными системами в разветвленной КС появляются дополнительные возможности нарушения безопасности информации. [12,32,43,64]

Технологии непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Отсюда, все более актуальной становится проблема обеспечения безопасности КС, под которой понимается состояние информации, технических средств и технологии, характеризующееся свойствами конфиденциальности, целостности и доступности информации [88].

КС, в силу своего исторического развития, представляют собой распределенные, сложные структуры. КС представляет собой многоуровневую

иерархическую структуру, включающую в себя множество узлов, связанных между собою определенным образом [28, 60]. Свойство уязвимости присуще такой конструкции, в силу присутствия многочисленных узлов и связей между ними.

Универсальных методов защиты не существует[88,91], поэтому во многом успех при построении механизмов безопасности для реальной системы будет зависеть от еѐ индивидуальных особенностей, учѐт которых плохо поддаѐтся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа. [28] За практическими приѐмами построения систем защиты лежат общие закономерности, которые не зависят от технических особенностей их реализации. Очевидно, что решение проблемы обеспечения безопасности КС должно осуществляться системно на основе оценки технологии защиты информации, передачи ее по каналам связи, и не должно рассматриваться как чисто техническая задача, которая может быть решена попутно с разработкой элементов КС. [3,4]

Изучение свойств распределений экстремальных значений в течение долгого времени находилось несколько в стороне от основных направлений статистической теории распределений. В настоящее время теория распределения экстремальных значений является составной частью многих естественнонаучных дисциплин. Распределениями экстремальных значений первоначально интересовались абстрактные вероятностники, да специалисты в прикладных областях — инженеры и гидрологи. Только с недавних пор эти распределения вошли в сферу существенных интересов специалистов по статистике. [81]

Распределение экстремальных значений основывается на предельных распределениях для максимумов или минимумов (крайние значения) независимых, одинаково распределенных случайных величин, по мере увеличения размера выборки. Теория экстремальных значений моделирует события, которые происходят с очень малой вероятностью. Отсюда следует полезность в моделировании рисков для событий с малой вероятностью.[84,85,87,89,92,94]

При построении риск-модели КС на основе переменных состояний защищенности (ПСЗ) статистическому временному ряду свойственен большой объем выборки и определенная периодичность колебания, вследствие работы персонала и пользователей КС[100,104,108,124]. В свою очередь вероятность возникновения ущерба является относительно малой. Из этого следует, что для построения риск-модели КС целесообразно использовать экстремальные значения ПСЗ, что позволит сократить объем обрабатываемой информации и построить риск-модель на основе большего промежутка времени, а следовательно и большей точностью [85,86,88,80,94,96].

Степень научной разработанности. Существует достаточное большое количество работ, в которых осуществляется попытка построения риск-модели КС. При этом в них может рассматриваться определенный тип угроз и атак на данную КС, плотности вероятности распределения ущербов в этих системах распределены по определенному закону. Тем не менее, исследование возможности применения законов распределений экстремальных значений для построения риск-модели является актуальной задачей. Таким образом, исходя из актуальности и степени научной разработанности данной проблемы, можно сделать вывод о целесообразности проведения исследований в данном направлении.

Цели и задачи исследования. Целью дипломной работы является разработка и исследование риск-моделей компьютерных систем (КС) переменные состояния защищенности которых являются периодическими и имеют свойства цикличности, и распределены на основе законов, описывающих распределение экстремальных значений состояния информационной безопасности.

Для достижения этой цели необходимо решить следующие задачи:

1. Определить множество численных характеристик состояния информационной безопасности, характеризующих работу КС с периодическими переменными состояния защищенности (ПСЗ) с позиции обеспечения конфиденциальности, целостности и доступности информации и нарушение которых является признаком возникновения инцедентов информационной безопасности;

2. Построить аналитические выражения для оценки наносимого ущерба в зависимости от значения порога безопасности переменного состояния;

3. Разработать методику риск-анализа КС с периодическими ПСЗ на основе законов Гумбеля и Мизеса;

4. Разработать алгоритм минимизации риска КС с периодическими ПСЗ на основе законов Гумбеля и Мизеса.

Объектом исследования являются периодические переменные состояния защищенности компьютерных систем (КС) с заданными порогами допустимых значений экстремумов, которые не превышают заданного порогового уровня безопасности.

Предметом исследования является риск-анализ состояния защищенности компьютерных систем (КС) в условиях приближения экстремальных значений периодических переменных состояний к порогам безопасности.

Методы исследования. Для решения поставленных задач предполагается использовать методы системного анализа и математического моделирования, основанные на теории вероятностей и математической статистики, применительно к описанию распределений экстремальных значений переменных состояний защищенности.

Степень обоснованности научных положения, выводов и рекомендаций, сформулированных в дипломной работе предполагается обеспечить рациональным и обоснованным применением математических методов в приложении обозначенному предмету исследования.

Научная новизна исследования предположительно будет заключаться в:

1. Сформированном множестве числовых показателей ИБ КС с периодическими ПСЗ.

2. Разработанной риск-модели КС с периодическими переменными состоя, основанной на законах, описывающих распределение экстремальных значений переменных состояний защищенности КС с периодическими ПСЗ.

3. Методике прогнозирования возможных экстремальных значений числовых показателей ИБ КС с периодическими ПСЗ.

Практическая ценность работы заключается в том, что:

1. Рассмотренный подход, учитывающий построение риск-моделей КС с периодическими ПСЗ на основе экстремальных значений числовых показателей защищенности КС, позволяет повысить точность оценки и прогнозирования риска в КС по сравнению с методом экспертных оценок.

2. Полученные риск-модели КС с периодическими ПСЗ могут быть использованы для проектирования и построения компьютерных систем, устойчивых к инцидентам ИБ, влекущим за собой превышение допустимого порогового уровня ПСЗ.

3. Разработанная методология оценивания и созданный на ее основе алгоритм минимизации уровня риска позволяют измерить риски в режиме реального времени, снизить риски для уязвимых узлов системы, диапазон ущербов для системы в целом, а также осуществлять их краткосрочное прогнозирование, повышая точность и быстродействие системы управления в КС.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена разработке и исследованию риск-моделей информационно-телекоммуникационных систем, а именно компьютерных систем с периодическими переменными состояний защищенности. В ходе ее выполнения были получены следующие основные результаты:

1. Рассмотрены и проанализированы законы распределения Гумбеля и Мизеса из семейства законов распределений экстремальных значений. Выявлены области применения этих распределений для задач информационной безопасности компьютерных систем с использование переменных состояний защищенности.

2. Сформировано множество числовых показателей ИБ компьютерных систем, для которых характерно свойство периодичности.

3. При решении задач, применительно к проблематике работы, результативно использовались методы численные методы расчета и анализа, методы теории рисков, теории вероятности и системного анализа.

4. Предложена оценка риска компьютерных систем с периодическими ПСЗ не превышающими заданных порогов безопасности, распределенными по законам Гумбеля и Мизеса является перспективным подходом для улучшения качества построения риск-моделей КС с периодическими ПСЗ, регулирования рисков и повышения защищенности компьютерных систем.

5. Получены аналитические выражения риск-моделей компонент компьютерных систем, плотность вероятности наступления ущербов в которых распределены по законам Гумбеля и Мизеса.

6. Исследованы аналитические риск-модели компьютерных систем, с периодическими ПСЗ, в которых ПСЗ не превышают заданный пороговый уровень. Получены аналитические выражения для расчета параметров риска для распределений Гумбеля и Мизеса, нахождения риска в диапазоне ущербов, оценка интегрального риска системы, проведена дискретизация риска. Проведена оценка и регулирование общего риска системы.

7. Получены риск-модели КС с периодическими ПСЗ, которые могут быть полезными для проектирования и построения компьютерных систем, устойчивых к

инцидентам ИБ, влекущих за собой превышение допустимого порогового уровня ПСЗ.

8. Найдены выражения для определения параметров чувствительности рисков КС с периодическими переменными состояний защищенности, а также построены уравнения движения риска КС с периодическими ПСЗ распределенными по законам Гумбеля и Мизеса.

9. На основе оценки риска компьютерных систем, состоящих из двух компонентов, была произведена оценка рисков для компьютерных систем, состоящих из n компонентов в общем виде, в компонентах которых плотность вероятности наступления ущебра имеют распределения Гумбеля и Мизеса.

10. Исследованы методики и алгоритмы управления информационными рисками системы, базирующиеся на основе стратегии оптимизационного снижения риска, и приведена адаптация алгоритма наискорейшего спуска для решения данной оптимизационной стратегии.

11. Разработана методология оценивания и созданный на ее основе алгоритм минимизации уровня риска позволяют измерить риски в режиме реального времени, снизить риски для уязвимых узлов системы, диапазон ущербов для системы в целом, а также осуществлять их краткосрочное прогнозирование, повышая точность и быстродействие системы управления в КС.

12. Проведена оценка экономических показателей эффективности разработанных риск-моделей компьютерных систем на основе периодических переменных состояний защищенности КС с заданными порогами допустимых значений экстремумов, не превышающих заданного порогового уровня безопасности.

Результаты исследований имеют солидную область применения.

Построенный математический аппарат, а также приведенные методики и алгоритмы управления риском позволят проектировать и строить компьютерные системы, устойчивые к инцидентам ИБ, и влекущим за собой превышения заданных допустимых порогов уровней ПСЗ, а также адекватные системы предупреждения и

защиты компьютерных систем в условия недетерминированных проявлений дестабилизирующих инцидентов ИБ.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

СПИСОК ЛИТЕРАТУРЫ

1 Абергауз Г.Г. Справочник по вероятностным расчетам / Г.Г. Абергауз. - М.: Воениздат, 1970.- 245 с.

2 Балдин К.В. Управление рисками: Учеб. пособие / К.В. Балдин, С.Н. Воробьев. -М.: ЮНИТИ-ДАНА, 2005. - 511с.

3 Бармен С. Разработка правил информационной безопасности. Изд-во «Вильяме», 2002. С. 25-37.

4 Белоножкин В.И., Остапенко Г.А. Информационные аспекты противодействия терроризму. - М.: Горячая линия - Телеком, 2009. - 112 с.

5 Бершадский А.В. Что могут дать технологии управления рисками современному бизнесу? // Управление и обработка информации: модели процессов: Сб. ст. МФТИ. М., 2001. - С. 34-51.

6 Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев. М.: Статистика, 1990. - 287 с.

7 Биркгов Г. Современная прикладная математика / Г. Биркгов.— М.: Мир, 1976.-400 с.

8 Болыпев JI.H. Таблицы математической статистики. / JI.H. Болынев, Н.В. Смирнов М.: Наука, 1983. - 297 с.

9 Бостанджиян В. А. Пособие по статистическим распределениям/ В.А. Бостанджиян. Черноголовка: ИПХФ, 2000. — 1006 с.

10 Вентцель Е. С. Теория вероятностей (первые шаги)/ Е.С.Вентцель- М.: Знание, 1977.-226 с.

11 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения. Учеб. пособие для втузов. / Е.С. Вентцель, JI.A. Овчаров. — М.: Высш. шк, 2000. 383 с.

12 Вишневский, В.М. Состояние и перспективы развития информационно-вычислительных сетей в России / В.М. Вишневский // Электросвязь. – 1998. – № 7. – С. 20 – 23.

13 Воронцовский А.В. Управление рисками: Учеб. пособие. 2-ое изд., испр. и доп / А.В. Воронцовский СПб: Изд-во С.-Петерб. ун-та, 2000; ОЦЭиМ, 2004. - 458 с.

14 Гмурман В. Е. Теория вероятностей и математическая статистика / В. Е. Гмурман.-М.: Высш. шк., 2004 148 с.

15 Гнеденко Б. В. Курс теории вероятностей / Б.В. Гнеденко.- М.: Наука, 1988.-98 с.

16 Гнеденко Б.В. Математические методы в теории надежности. / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. М.: Наука, 1965. - 333 с.

17 ГОСТ 17799-2005 Практические правила управления информационной безопасностью.

18 ГОСТ 27001:2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

19 ГОСТ Р 50922-96 Защита информации: основные термины и определения М. Изд. стандартов, 1996.

20 ГОСТ Р 51901.11-2005 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство.

21 ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем

22 ГОСТ Р 51901.12-2007 Менеджмент риска. Метод анализа видов и последствий отказов.

23 ГОСТ Р 51901.14-2007 Менеджмент риска. Структурная схема надежности и булевы методы.

24 ГОСТ Р 51901.15-2005 Менеджмент риска. Применение марковских методов.

25 ГОСТ Р 51901-2002. Управление надежностью. Анализ риска технологических систем.

26 ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.

27 Гражданкин А.И. Использование вероятностных оценок при анализе безопасности опасных производственных объектов. / А.И. Гражданкин, М.В. Лисанов, А.С. Печеркин // Безопасность труда в промышленности. -2001.-№5.-С. 33-36.

28 Громов Ю.Ю. Анализ живучести информационных сетей / Ю.Ю. Громов, Д.Е. Винокуров, Т.Г. Самхарадзе, И.И. Пасечников // Информационные системы и управление. - 2006. - № 1. – С. 138–156.

29 Грушо А.А. Теоретические основы защиты информации. / А.А. Грушо, Е.Е. Тимонина. М.: Яхтсмен, 1966. - 235 с

30 Губарев В.В. Вероятностные модели / В.В. Губарев. Новосибирск: Новосибирский электротехнический институт, 1982. - 164 с.

31 Гундарь К. Ю. Защита информации в компьютерных системах / К. Ю. Гундарь, А. Ю. Гундарь, Д.А.Янишевский. Киев: Корнейчук, 2000. - С. 20-25.

32 Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. М.: Издательский центр «Академия», 2005. - 144 с.

33 Джонсон Н.Л. Одномерные непрерывные распределения. В 2 частях. Часть 2 / Н.Л. Джонсон, С. Коц, Н. Балакришнан // Бином. Лаборатория знаний, 2012. - 600 с.

34 Екушов А.И. Моделирование рисков в коммерческом банке. Электрон, дан. - Режим доступа: http://exsolver.narod.ru/Artical/Bank/modrisk.html

35 Задачи оптимизации иерархических структур / Дементьев В.Т. и др. – Новосибирск : Изд-во Новосибирского ун-та. – 1996. – 200 с.

36 Зорин В.А. Элементы теории процессов риска. / В.А. Зорин, В.И. Мухин. Н. Новгород: ННГУ.2003. - 25 с

37 Зражевский В.В. Основные направления совершенствования системы управления рисками. М.: 1991 - 465 с

38 Кобзарь М. Методология оценки безопасности информационных тенологий по общим критериям/ Сидак А.

39 Колесов Ю.Б., Сениченков Ю.Б. Имитационное моделирование сложных динамических СНСТеМ//http://www.exponenta.ru/others/mvs/ds sim.asp

40 Комаров Л.Б. Статистические методы обработки экспериментальных данных. Учеб. пособие. Часть 2 / Л.Б. Комаров — СПб.: Ленинград, 1972. — 208 с.

41 Конев И. Классификация как основа управления информационными рисками// Директор ИС #05/2006 http://www.osp.ru/text/302/2040771/

42 Королюк В. С. Полумарковские процессы и их приложения / В. С. Королюк, А. Ф. Турбин Киев.: Науковая думка, 1976.-256 с.

43 Котенко И.В. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Труды СПИИРАН. – Спб.: СПИИРАН, 2006. – В.3, Т.2. – С. 30-49.

44 Крис Касперский. Техника сетевых атак. Том 1. М.: СОЛОН Р, 2001. - 396 с.

45 Крылов В.В., Самохвалова С.С. Теория телетрафика и еѐ приложения. – СПб.: БХВ-Петербург, 2005. – 288с.

46 Крысин А. В. Информационная безопасность. Практическое руководство. М.: СПАРРК, К: ВЕК+, 2003. 320 с.

47 Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний //Журнал сетевых решений LAN, июнь 2005

48 Куринной Г.Ч. Математика: справочник / Г.Ч. Куринной. М.: Фолио, 2000.- 464 с.

49 Лукацкий А. Атаки на информационные системы. Типы и объекты воздействия / А. Лукацкий // Электроника: Наука, Технология, Бизнес,-2000.-№1.-С. 9-11.

50 Лукацкий А.В. Адаптивное управление защитой сети / А.В. Лукацкий // Глобальные сети и телекоммуникации.-1999.- №10. С. 20-21.

51 Лукацкий А.В. Обнаружение атак своими силами// http://bugtraq.ru/library/security/luka/autodetect.html

52 Люцарев В. С. Безопасность компьютерных сетей на основе WINDOWS NT. М.: СОЛОН Р, 1998. - 356.

53 Малашенко, Ю.Е. Модели неопределенности в многопользовательских сетях / Ю.Е. Малашенко, Н.М. Новикова. – М. : Эдиториал УРСС, 1999. – 247 с.

54 Малашенко, Ю.Е. Анализ многопользовательских сетевых систем с учетом неопределенности. VII. Задача нормативного анализа уязвимости многопродуктовой потоковой сети / Ю.Е. Малашенко, Н.М. Новикова // Изв. РАН. Теория и системы управления. – 1999. – № 4.

55 Малашенко, Ю.Е. Многокритериальный синтез потоковых сетей с гарантией живучести / Ю.Е. Малашенко, Н.М. Новикова, И.И. Поспелова // Изв. РАН. Теория и системы управления. – 2001. – № 1. ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И УПРАВЛЕНИЕ. – 2006. – № 1 155

56 Малашенко, Ю.Е. Многокритериальный синтез сетей с гарантией живучести / Ю.Е. Малашенко, Н.М. Новикова, И.И. Поспелова // Изв. РАН. Теория и система управления – М. : – 2001. – № 1.

57 Марков А.В., Цирлов В.А. Управление рисками — нормативный вакуум информационной безопасности // Электронный ресурс.

58 Материал из Википедии — свободной энциклопедии. Имитационное моделирование // http://ru.wikipedia.org/wiki/

59 Медведовский И. Д. Атаки через Интернет / И. Д. Медведовский, П. В. Семьянов, В. В. Платонов. НПО "Мир и семья-95", 1997. - 250 с.

60 Мельников, Ю.Е. Модель комплексной оценки и обеспечения живучести распределенных информационно-вычислительных систем : материалы II Всесоюзн. науч.-техн. конф. / Ю.Е. Мельников, Ж.С. Сарыпбеков. – М., 1988.

61 Минаев В. Экономические аспекты информационной безопасности //Вестник связи International №8/2003 стр.23-25

62 Мойзер П. Современный стандарт безопасности для беспроводныхсетей. // Журнал сетевых решений LAN, 05.2005, 104 - 107с.

63 Моисеев Н.Н. Математические задачи системного анализа / Н.Н. Моисеев. -М.: Наука, 1975. 576 с.56. .

64 Молчанов А.А. Моделирование и проектирование сложных систем / А.А. Молчанов.- Киев: Выща. шк., 1988. 359 с.

65 Научный форум «Системы, процессы и безопасность» 2007/2008. Межрегиональная научно-практическая конференция «Информационные риски и безопасность» Воронежского отделения Российской инженерной академии. Сборник научных трудов. Воронеж: МИКТ, 2007. 102 с.

66 Новиков А.А. Уязвимость и информационная, безопасность телекоммуникационных технологий: Учебное пособие для вузов. / А.А. Новиков, Г.Н: Устинов. М:: Радио и связь, 2003. - 296 с.

67 Новоселов А.А. Математическое моделирование финансовых рисков. Теория измерения / А.А. Новоселов. — Новосибирск: Наука, 2001. 212 с.

68 Новосельцев В.И. Системная конфликтология / В.И. Новосельцев. — Воронеж: Издательство Кварта, 2001. 176 с.

69 Остапенко О.А. Риски систем: оценка и управление / О.А. Остапенко, Д.О. Карпеев, В.Н. Асеев и др; под ред. Ю.Н. Лаврухина, А.Г. Остапенко. Воронеж: МИКТ, 2007 - 261 с.

70 Остапенко Г.А. Информационные операции и атаки в социотехнических системах. - М.: Горячая линия - Телеком, 2007. - 134 с.

71 Остапенко Г.А. Информационные операции и атаки в социотехнических системах: / Г.А. Остапенко; Под редакцией В.И. Борисова. М: Горячая линия-Телеком, 2006. - 184 с.

72 Остапенко Г.А. Информационные операции и атаки в социотехнических системах: организационно правовые аспекты. Учеб. пособие / Г.А. Остапенко, Е.А. Мешкова; под ред. В.Г. Кулакова,- М.: Горячая линия - Телеком, 2008.-208 с.

73 Остапенко Г.А. Информационные операции и атаки в социотехнических системах: учеб. пособие / Г.А. Остапенко; под ред. чл.-корр. РАН В.И. Борисова.- М.: Горячая линия Телеком, 2007.-134 с.

74 Остапенко Г.А. Информационные технологии и системы государственного и муниципального управления (в условиях противодействия

информационным операциям и атакам). Часть 1. – Воронеж: НОУВПО «Международный институт компьютерных технологий», 2008. – 202 с.

75 Остапенко Г.А. Информационные технологии и системы государственного и муниципального управления (в условиях противодействия информационным операциям и атакам). Часть 2. – Воронеж: НОУВПО «Международный институт компьютерных технологий», 2008. – 190 с.

76 Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин / Г.А. Остапенко // Информация и безопасность: Регион, науч.-техн. журнал. Воронеж. 2005. - Вып. 2. - С. 70 - 75.

77 Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин / Г.А. Остапенко // Информация и безопасность: Регион, науч.-техн. журнал. Воронеж. 2005. - Вып. 2. - С. 70 — 75.

78 Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайныхвеличин / Г.А. Остапенко // Информация и безопасность: регион, науч.—техн. журнал. Воронеж: ВГТУ, 2005. Вып. 2. - С. 70 - 72.

79 Остапенко Г.А., Мешкова Е.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия. - М.: Горячая линия - Телеком, 2008. - 208 с.

80 Остапенко О.А. Методология оценки риска и защищенности систем/ 0:А. Остапенко // Информация и безопасность: Регион, науч.-техн. журнал. Воронеж. 2005. - Вып. 2. - С. 28 - 32.

81 Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион, науч.-техн. журнал. Воронеж. 2005. - Вып. 2.-С. 28-32.

82 Петренко В.В. Рыночные риски: системный подход //Доклад на конференции "Международный опыт риск-менеджмента" // Москва, 2004 г

83 Петренко С.А. Метод оценивания информационных рисков организации. // сб.статей «Проблемы управления информационной безопасностью» под ред. д.т.н., профессора Черешкина Д.С., РАН ИСА, М., Едиториал УРСС, 2002.- С.112-124.

84 Покровский П. Оценка информационных рисков. // Журнал сетевых решений LAN, 10.2004, 91 - 95с.

85 Приходько А.Я. Словарь-справочник по информационной безопасности. М.: СИНТЕГ, 2001.- 124 с.

86 Прохоров Ю. В. Теория вероятностей / Ю. В. Прохоров, Ю. А. Розанов- М.:Наука, 1967.-162 с.

87 Пустыльник Е.И. Статистические методы анализа и обработки наблюдений / Е.И. Пустыльник. М.: Наука, 1971. - 192 с.

88 Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. - М: РадиоСофт; 2010. – 232 с.

89 Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М.: Гостехкомиссия России, 1992.

90 Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации. М.: Гостехкомиссия России, 1992.

91 Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М.: Гостехкомиссия России, 1992.

92 Рыбина Г.В. Принципы построения имитационных моделей сложных технических систем для интегрированных экспертных систем реального времени //

93 Севастьянов Б.А. Вероятностные модели / Б.А. Севастьянов. М.: Наука, 1992.- 176 с.

94 Симонов С. В. Анализ рисков, управление рисками // Jet Info, 2, 2003.76.

95 Cox D. R., Miller H. D. The theory of stochastic processes / Cox D. R., Miller H. D.- Methuen, 1965. p. 94.

96 Фрэнк, Г. Сети, связь и потоки / Г. Фрэнк, И. Фриш ; под. ред. Д.А. Поспелова. – М.: Связь, 1978. – 448 с.

97 Щербаков В. Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. - М:РадиоСофт, 2010. – 256 с.

98 Юсупова Р.М. и Кофанова Ю.Н. Вопросы кибернетики. Теория чувствительности и ее применение / Р.М. Юсупова и Ю.Н. Кофанова — М.: Наука, 1981.-194 с.

99 Artzner P. (1997), Thinking coherently. / Artzner P., Delbaen F., Eber J. & Heath D. // RISK 1997. – № 10. – С. 68–71.

100 Beirlant J. (1996), Practical analysis of extreme values. / Beirlant J., Teugels J. & Vynckier P. // Leuven: Leuven University Press, 1996. – 170 с.

101 Beirlant J. Statistics of Extremes: Theory and Applications. / Beirlant J., Goegebeur Y., Segers J., Teugels,J. // England: Wiley, 2004. – 485 с.

102 Boehm B.W. Software risk management. IEEE Computer Society Press. Washington. 1989.-p. 121

103 Castillo E. Extreme Value and Related Models with Applications in Engineering and Science. / Castillo E., Hadi A.S., Balakrishnan N., Sarabia, J.M. // New Jersey: John Wiley & Sons, Hoboken, 2005. – 353 с.

104 Danielsson J. Tail index and quantile estimation with very high frequency data. / Danielsson J., de Vries C. // Journal of Empirical Finance 1997. – №4. – С. 241–257.

105 David H.A.Order Statistics, 3rd edition. / David H.A., Nagaraja H.N. // New Jersey: Wiley, Hoboken, 2003. – 488 с.

106 De Haan L. Extreme Value Theory: An Introduction. / De Haan L., Ferreira A. Boston: Springer Series in Operations Research and Financial Engineering, 2006. – 436 с.

107 de Haan L. On Regular Variation and its Application to the Weak Convergence of Sample extremes / de Haan L. Amsterdam: Mathematisch Centrum, Math. Centre Tracts vol. 32, 1970. – 124 с.

108 Diebold F. Pitfalls and opportunities in the use of extreme value theory in risk management. / Diebold F., Schuermann T. & Stroughair J. // Amsterdam: Kluwer Academic Publishers, 1999. – 13 с.

109 Embrechts P. Correlation and dependency in risk management: properties and pitfalls. / Embrechts P., McNeil A., Straumann D. // Cambridge: University of Cambridge, 2002. – С. 176 – 223.

110 Embrechts P. Modelling Extremal Events for Insurance and Finance, 3rd edition / Embrechts P., KluËppelberg C., Mikosch T. // Berlin : Springer, Heidelberg, 2001. – 655 с.

111 Fisher R.A. Limiting forms of the frequency distribution of the largest and smallest member of a sample. / Fisher R.A., Tippett L.H.C. // Proc. Camb. Phil. Soc., 24, 1928. – С. 180–190.

112 Frerchet M. Sur la loi de probabilit de l'ercart maximum. / Frerchet M. Cracovie: Ann. Soc. Polon. Math. 6, 1927. – С. 93–116.

113 Gnedenko B.V. Sur la distribution limite du terme maximum d'une serrie aleratoire. / Gnedenko B.V. // Ann. Math., 44, 1943. – С. 423–453.

114 Gumbel E.J. Statistics of Extremes. / Gumbel E.J. New York: Columbia University Press, 1958. – 375 с.

115 ISO/IEC 17799 information technology — Code of practice for information security management.

116 ISO/IEC TR 13335-2 «Информационная технология Рекомендации по управлению безопасностью ИТ - Часть 2: Управление и планирование безопасности ИТ»// Технический отчет.

117 Jenkinson A.F. The frequency distribution of the annual maximum (or minimum) values of meteorological elements // Quart. J. Roy. Meteo. Soc., 81, 1955. – С. 158–171.

118 Johnson N.L. Continuous Univariate Distributions - Volume 2, Second edition / Johnson N.L., Balakrishnan N. and Kotz S. // New York: John Wiley & Sons, 1995. – 719 с.

119 Kotz S. Extreme Value Distributions: Theory and Applications. / Kotz S., Nadarajah S. // London: Imperial College Press, 2002. – 187 c.

120 McNeil A. Estimating the tails of loss severity distributions using extreme value theory. / McNeil A., ASTIN Bulletin, 1997. – № 27. – С. 117–137.

121 Neves C., Fraga Alves M. I. Testing extreme value conditions - an overview and recent approaches. / Neves C., Fraga Alves M. I. // REVSTAT - Statistical Journal, Vol 6,1, 2008. – С. 83–100

122 Reiss R.-D. Statistical Analysis of Extreme Values, with Application to Insurance, Finance, Hydrology and Other Fields, 3rd edition, / Reiss R.-D., Thomas M. // Birkhuser Verlag, 2007. – 530 с.

123 Risk Management Guide for Information Technology Systems //NIST, Special Publication 800-30

124 Smith, R. Multivariate threshold methods, in J. Galambos, ed., ‘Extreme Value Theory and Applications’. / Smith, R., Kluwer Academic Publishers, 1994. – С. 225–248.

125 von Mises R. La distribution de la plus grande de n valeurs. Reprinted in Selected Papers Volumen II / von Mises R. Providence: American Mathematical Society, R.I., 1954. – С. 271–294.

8 (952) 106-88-60 vk.com/a.projectit a.projectit