Содержание

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

Введение

Актуальность исследования

Одним из главных направлений развития науки в настоящее время является внедрение информационных технологий во всесферы жизнедеятельности человека.

Трудно переоценить важность задачи своевременного и оперативного получения необходимой информации. Первая сложность при решении этой задачи заключается в том, что информационные потоки существенно возросли, что не может не затруднять процесс поиска качественной и действительно необходимой информации. Вторая проблема становится одной из глобальных и весомых в современном мире, она заключается в обеспечении безопасности информации, циркулирующей в информационно-телекоммуникационных системах [41, 51, 73].

Большинство таких систем включают в себя множество элементов, то есть являются распределенными. Универсальное решение проблемы безопасности информации, циркулирующей в таких системах, к настоящему моменту не найдено [57, 58, 59, 60]. Атаки компьютерных вирусов, а также других вредоносных программ способны нанести огромный ущерб организациям и отдельным пользователям [1, 2, 31 ,34].

Вредоносные технологии совершенствуются с каждым днем. Вирусы, троянские программы, черви – все эти классы вредоносного ПО «на слуху» у рядовых пользователей, в том числе за счет ежедневного создания все новых и новых вредоносных объектов данных типов. Вредоносные действия рассматриваемых объектов в общем случае различны, носледует понимать, что даже безвредные,на первый взгляд, вирусы, не являются таковыми.

Совершенствование вирусов является результатом многих процессов. Можно выделитьповышение скорости их распространения;появление новых деструктивных функций;реализация новых средств маскировки, которые позволяютвирусам бытьневидимыми для многих средств защиты; появление возможности распространения по нескольким каналам одновременно. Есть и

другие направления развития и совершенствования вредоносного программного обеспечения.

В связи с этим, рассмотрение методов противодействия вирусным атакам – крайне актуальная задача. Она является сложной и многогранной, так как требует исследования множества факторов. Одним из таких факторов является математическое моделирование вирусных атак, которое позволит оценить, во-первых, возможный ущерб от успешной атаки на заданную распределенную компьютерную систему, во-вторых - эффективность используемых средств защиты.

В данном случае под математическим моделированием понимается построение риск-моделей вирусных атак на распределенные компьютерные системы. Данные модели являются необходимым инструментом для изучения и противодействия вирусным атакам.

Степень научной разработанности

Существует достаточное большое количество работ, в которых осуществляется попытка управления риском и защищенностью КС. При этом в них может рассматриваться определенный тип атак на данную КС, плотности вероятности распределения ущербов в этих системах распределены по определенному закону. Тем не менее, исследование возможности применения выборочного нормального закона распределения для анализа ущербов КС является актуальной задачей. Таким образом, исходя из актуальности и степени научной разработанности данной проблемы, можно сделать вывод о целесообразности проведения исследований в данном направлении.

Целью настоящей работы является построение риск-моделей вирусных атак на распределенную компьютерную систему и исследование возможности применения выборочных нормальных распределений ущерба для оценки и регулирования риска защищаемой КС.

Для реализации цели необходимо решить следующие задачи:

1. Проведение анализа предметной области, рассмотрение существующих моделей вредоносных программ, выявление перспективных направлений в этой области.

2. Анализ семейства выборочных нормальных распределений плотности вероятности наступления ущерба и их характеристик, а также выявление областей эффективного применения законов этих распределений.

3. Формулирование риск-моделей вирусных атак на распределенные КС на основе выборочного нормального распределения, описание параметров моделей.

4. Исследование динамики риска распределенных КС, подвергающихся синхронным и асинхронным вирусным атакам.

5. Оценка экономических показателей эффективности разработанных методов.

6. Рассмотрение исследуемого вопроса с точки зрения обеспечения безопасности жизнедеятельности.

Объектом исследования является класс распределенных КС, состоящих из элементов, плотность вероятности наступления ущерба которых имеет заданные виды распределений.

Предметом исследования являются вероятностные модели вирусных атак, как класса вредоносного ПО, построенные для проведения риск-анализа обеспечения безопасности компьютерной системы.

Методологическая, теоретическая и эмпирическая база исследования.

В данной работе для решения поставленных задач используются методы теории рисков, теории информационной безопасности, теории вероятностей, математической статистики.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе обеспечивается корректным использованием методов теории вероятностей и математической статистики;

На защиту выносятся:

1. Анализ семейства выборочных нормальных распределений плотности вероятности наступления ущерба распределенной компьютерной системы и их характеристик;

2. Математическая модель вирусных атак на распределенную компьютерную систему на основе выборочного нормального распределения ущерба;

3. Аналитические выражения для расчета рисков и защищенности распределенных компьютерных систем, подвергаемых вирусным атакам;

4. Разработанные методы управления рисками и защищенностью в распределенных компьютерных системах, подвергаемых вирусным атакам.

Научная новизна

1. Впервые получены выражения для расчета рисков и защищенности распределенных компьютерных систем, подвергаемых вирусным атакам. При этом рассматриваемые атаки подлежат классификации, разделению на виды;

2. Исследованы характеристики риска для выборочных нормальных распределений плотности вероятности наступления ущерба, а также области эффективного применения законов этих распределений;

3. Проведено исследование динамики рисков распределенных компьютерных систем, подвергаемых вирусным атакам. Получены выражения для чувствительности и движения.

Практическая значимость работы заключается в том, что разработанные методы управления рисками и защищенностью распределенных компьютерных систем могут использоваться при оценке рисков успешной вирусной атаки на рассматриваемые компьютерные системы. Полученная оценка рисков позволяет:

1. Реализовывать комплексный анализ эффективности проводимых процедур защиты от вирусных атак в рассматриваемых компьютерных системах;
2. Эффективно выполнять проектирование защищаемой распределенной компьютерной системы;
3. Производить оптимальный выбор мер по созданию и модификации системы защиты.

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

projectIT

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

projectIT

Заключение

Работа посвящена оценке и регулированию рисков распределенной КС, подвергающихся синхронным и асинхронным вирусным атакам на основе выборочных нормальных распределений плотности вероятности наступления ущерба. В ходе ее выполнения были получены следующие основные результаты:

1. Рассмотрено и проанализировано семейство выборочных нормальных распределений плотности вероятности наступления ущерба и их характеристик.
2. Получены аналитические выражения риск-моделей компонент распределенных компьютерных систем, подвергающихся вирусным атакам. При этом плотность вероятности наступления ущербов от вирусных атак распределена по выборочномунормальному распределению.
3. Проведена оценка и регулирование общего риска системы при воздействии синхронных и асинхронных вирусных атак.
4. Проведено исследование динамики рисков распределенных компьютерных систем, подвергающихся синхронным и асинхронным вирусным атакам. Получены выражения для чувствительности и движения.

Результаты исследования имеют солидную область применения. Построенный математический аппарат позволяет строить адекватные системы защиты распределенных компьютерных систем, подвергающихся синхронным и асинхронным вирусным атакам.

ЛИТЕРАТУРА

1 Андреев Д.А., Брянский А.Е. Вирусы и риски заражения систем: Обзор и построение обобщенных вероятностных моделей // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 4. - С. 519 – 536.

2 Андреев Д.А., Котрахов В.В., Остапенко А.Г. Компьютерные вирусы: классификация и статистический анализ // Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2010. – Том. 13. – Часть. 2. - С. 295 – 296.

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

4 Бартон Т. Комплексный подход к безопасности сетей / Т. Бартон, У. Шенкир, П. Уокер. – М.: Издательский дом "Вильямс", 2003. – 208 с.

5 Безруков Н.Н. Компьютерная вирусология / Безруков Н.Н. - Киев: УРЕ, 1991. – 88 с.

6 Бендат Дж., Пирсол А. Прикладной анализ случайных данных. М.: Мир, 1989.– 540 с.

7 Боровиков А.А. Теория вероятностей /А.А. Боровиков – М.: Наука, 1986. – 432 с.

8 Бостанджиян В.А. Пособие по статистическим распределениям/ В.А. Бостанджиян. - Черноголовка: ИПХФ, 2000. – 1006 с.

9 Буянов В.П., Уфимцев Ю.С. Методика информационной безопасности. М.: «Экзамен», 2004. – 148 с.Вадзинский Р.Н. Справочник по вероятностным распределениям – Санкт-Петербург.: «Наука», 2001. – 149 с.

10 Вентцель Е.С. Теория вероятностей и ее инженерные приложения. Учеб. пособие для втузов. / Е.С. Вентцель, Л.А. Овчаров. – М.: Высш. шк, 2003. – 464 с.

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

12 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.

13 Выгодский М.Я. Справочник по высшей математике / М.Я. Выгодский – М.: Наука, 1973. – 872 с.

14 Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

15 Герик Т. Информационная база для оценки риска / Т. Герик //LAN: журнал сетевых решений, 2006. – №9. – С. 22-25.

16 Гмурман В. Е. Теория вероятностей и математическая статистика.– М.: Высшая школа, 2004.– 148 с.

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

18 Гончаренко Л.П. Риск-менеджмент: учебное пособие / Под ред. д-ра тех. наук. проф., засл. деятеля науки РФ Е.А. Олейникова; Л.П. Гончаренко, С.А. Филин. – М.: КНОРУС, 2006. – 216 с.

19 ГОСТ 12.1.003-83. Шум. Общие требования безопасности. — М.: Изд-во стандартов, 1986. — 9 с.

20 ГОСТ 12.1.005-88. Воздух рабочей зоны. Общие санитарно-гигиенические требования. — М.: Изд-во стандартов, 1988. — 75 с.

21 ГОСТ 12.1.032-78. Рабочее место при выполнении работ сидя. Общие эргономические требования. — М.: Изд-во стандартов, 1992. — 9 с.

22 ГОСТ 12.1.030-81. Электробезопасность. Защитное заземление, зануление. — М.: Изд-во стандартов, 1986. — 9 с.

23 ГОСТ 12.1.019-79. Электробезопасность. Общие требования. — М.: Изд-во стандартов, 1986. — 6 с.

24 ГОСТ 12.1.004-91. Пожарная безопасность. Общие требования. — М.: Изд-во стандартов, 1991. — 77 с.

25 Громов Ю.Ю. Классификация видов атакующих воздействий на информационную систему / Ю.Ю. Громов, В.О. Драчев, В.В. Войтюк, Ю.Ф. Мартемьянов, А.Ю. Громова // Журнал «Информация и безопасность». – Воронеж: ВГТУ, 2010. – Вып. 3 – С. 413-418.

26 Грушо А.А.. Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агентства «Яхтсмен». 1996. – 192 с.

27 Гусак А.А. Высшая математика: учебник для студентов вузов / А.А. Гусак. – Мн.: ТетраСистемс, - 2004. – 5-е изд. - Т.2- 448 с.

28 Естественное и искусственное освещение. СНиП 23/05-95. — М.: Стройиздат, 1995. — 48 с.

29 Зайденберг А.П. Законы распределения случайных величин / А.П. Зайденберг– Омск: Омский институт инженеров железнодорожного транспорта, 1971. – 253 с.

30 Зражевский В.В. Основные направления совершенствования системы управления рисками / В.В. Зражевский. – М.: 1999. – 465 с.

31 Зубань С.С., Иохвидова А.Е., Остапенко О.А. Методический подход к синтезу распределенных систем с заданным уровнем риска // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 2. - С. 203 – 208.

32 Кадлоф А. Вирусы / А. Кадлоф. // Компьютер. -1990. - №1. – с. 44-47.

33 Карпеев Д.О., Плотников Д.Г., Дуплищева А.Ю. Расчет рисков атакуемых компонент информационно-вычислительных систем для дискретных законов распределения вероятности наступления ущербов // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 2. - С. 195 – 202.

34 Карпеев Д.О., Татаринцев А.Ю., Яковлев Д.С., Заряев А.В. Идентификация параметров нечетких моделей оценки информационных рисков информационных систем // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 1. - С. 37 – 42.

35 Касперски К. Записки исследователя компьютерных вирусов / К. Касперски - Издательство: Питер, 2005. – 316 с.

36 Кейт Дж. Джонс, Майк Шема, Бредли С. Джонсон. Анти-хакер. Средства защиты компьютерных сетей. - Издательство СП ЭКОМ, 2004. – 700 с.

37 Кендалл М. Теория распределений/ М. Кендалл, А. Стьюарт. – М.: Наука, 1966. – 590 с.

38 Кокс Д. Статистический анализ последовательностей событий / Д. Кокс, Льюис П. – М.: Издательство "МИР", 1969. – 312 с.

39 КоролюкВ.С., ПортенкоН.И., СкороходА.В., ТурбинА.Ф.Справочник по теории вероятностей и математической статистике/ – М.: Наука. Главная редакция физико-математической литературы, 1985. – 640с.

40 Куликов Е.И. Методы измерения случайных процессов/ Е.И. Куликов – М.: Радио и связь, 1986. – 272 с.

41 Куликов Е.И. Прикладной статистический анализ: Учеб.пособие для вузов/ Е.И. Куликов. – М.: Радио и связь, 2003. – 376 с.

42 Курило А.П. О проблеме компьютерной безопасности // Научно-техническая информация. Сер. 1. Орг. и методика информ. работы. – 1993. - №8. - 412 с.

43 Куринной Г.Ч. Математика: справочник. М.: Фолио, 2000.– 464 с.

44 Курносов Ю.В., Конотопов П.Ю. Аналитика: метрология, технология и организация информационно-аналитической работы / Ю.В.Курносов, П.Ю.Конотопов– М.: РУСАК, 2004. – 512с.

45 Лагунов В.С. Безопасность и экологичность в дипломном проекте: Учеб. пособие по дипломному проектированию. — Воронеж: Воронеж. гос. техн. ун-т, 2003. — 124 с.

46 Левин М. Как стать хакером / М. Левин– Издательство Новый издательский Дом, 2004. – 320 с.

47 Левин М. Руководство для хакеров 2. Электронные корсары / М. Левин– Издательство Новый издательский дом, 2005. – 208 с.

48 Линч Ф. Уильям, Стив Манзуик, Райян Пемех и др. Защита от хакеров корпоративных сетей. – Издательство ДМК Пресс, 2005. – 864 с.

49 Липаев В.В. Анализ и сокращение рисков проектов сложных программных средств / В.В. Липаев– Издательство «Синтег», 2005. – 208 с.

50 Локхарт Э. Антихакинг в сети. Трюки / Э. Локхарт - Издательство: Питер, 2005. – 296 с.

51 Малошевский С.Г. Теория вероятностей: Учеб. пособие. Часть 1. Вероятностное пространство. Дискретные случайные величины / С.Г. Малошевский – СПб: Петербургский гос. ун-т путей сообщения, 1999.– 92 с.

52 Малюк А.А. Защита информации / А.А. Малюк – М.: МИФИ, 2002. – 52с.

53 Методические указания к выполнению организационно-экономической части дипломных проектов научно-исследовательского направления для студентов специальности 090102, 090105, 090106 дневного обучения / Воронеж, гос. техн. ун-т; Сост. И. А. Злобина. Воронеж, 2004. 26 с.

54 Михайлов С.Ф., Петров В.А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. – М.: МИФИ, 1995. – 112 с.

55 Мирошников Б.Н. Борьба с преступлениями в сфере информационных технологий // Системы безопасности. 2002, №5(47). – 104 с.

56 Найт Ф.Х. Риск, неопределенность и прибыль. Пер. с англ. / Ф.Х. Найт– М.: Дело, 2003. – 360 с.

57 «О пожарной безопасности». ФЗ № 69 от 21.12.1994 г.

58 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.

59 Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Траниин В.А.Риски распределенных систем: Методики и алгоритмы оценки и управления/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 4. - С. 485 – 530.

60 Остапенко Г.А., Карпеев Д.О.Методическое и алгоритмическое обеспечение расчета параметров рисков распределенных систем на основе параметров рисков их компонентов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 373 – 380.

61 Остапенко Г.А., Маслихов П.А., Субботина Е.В. Способы регулирования рисков распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 435 – 438.

62 Остапенко Г.А., Мешкова Е.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия / Г.А. Остапенко, Е.А. Мешкова; Под редакцией Ю.Н. Лаврухина. – М: Горячая линия - Телеком, 2007. - 295 с.

63 Остапенко Г.А., Плотников Д.Г., Мешкова Е.А.Методическое и алгоритмическое обеспечение расчета параметров рисков для компонентов распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 335 – 350.

64 Остапенко Г.А., Транин В.А.Алгоритмическое обеспечение риск-анализа систем в диапазоне ущербов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 447 – 450.

65 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.

66 Остапенко О.А., Карпеев Д.О., Асеев В.Н., Морев Д.Е., Щербаков Д.Е. Риски систем: оценка и управление. – Воронеж: МИКТ, 2007. – 261 с.

67 Партыка Т.Л. Информационная безопасность / Т.Л. Партыка– Издательство «Форум», 2005. – 290 с.

68 Парфенов В.И. Защита информации (Словарь) / Парфенов В.И.– В.: НП РЦИБ «Факел», 2003. – 293 с.

69 Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, 2000. – 368 с.

70 Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность. / С.А. Петренко, С.В. Симонов. – М.: АйТи - Пресс, 2004. – 381 с.

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

72 Пикфорд Дж. Управление рисками / Дж. Пикфорд – М.: ООО "Вершина", 2004. – 352 с.

73 Поллард Дж. Справочник по вычислительным методам статистики / Дж Поллард. – М.: Финансы и статистика, 1982. – 575 с.

74 Приходько А.Я. Информационная безопасность в событиях и фактах / А.Я. Приходько– М.: СИНЕГ, 2001. – 260с.

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

76 Просветов Г.И. Управление рисками: задачи и решения: Учебно-практическое пособие / Г.И. Просветов– М.: Альфа-Пресс, 2008. – 416 с.

77 Радько Н.М., Скобелев И.О. // Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт., 2010. – 230с.

78 Розенвассер Е.Н. Методы теории чувствительности в автоматическом управлении/Р.Н. Розенвассер, Р.М. Юсупов. – Л.: «Энергия», 1971. – 260 с.

79 Розенвассер Е.Н. Чувствительность систем управления/Р.Н. Розенвассер, Р.М. Юсупов. – М.: Наука, 1981. – 464 с.

80 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. Шаньгина В.Ф. М.: Радио и связь, 1999. - 328 с.

81 Саати Т. Математические модели конфликтных ситуаций: Пер. с англ. / Т.Саати – М.: Сов. Радио, 1977. – 304 с.

82 Сачков В.Н. Введение в комбинаторные методы дискретной математики/ В.Н.Сачков. - М.: МЦНМО, 2004. – 421 с.

83 Севастьянов Б.А. Вероятностные модели / Б.А. Севастьянов. – М.: Наука, 1992. – 176 с.

84 Симонов С.В. Анализ рисков, управление рисками / С. В. Симонов //Jet Info. Информационный бюллетень, 1999. – № 1. – С. 2-28.

85 Таненбаум Э., ван Стеен М. Распределенные системы/ Э.Таненбаум, М. ван Стеен - Спб: Питер, 2003 – 877 с.

86 Томович Р. Общая теория чувствительности / Р. Томович, М. Вукобратович. Пер. с сербск. и с англ., под ред. Я.З. Цыпкина. – М.: Советское радио, 1972. – 240 с.

87 Унсельд И. Управление рисками и выполнение правил / И. Унсельд // LAN: журнал сетевых решений, 2006. – №8. – С. 86-88.

88 Феллер В. Введение в теорию вероятностей и ее приложения. В 2-х томах. Т.1: Пер. с англ / В. Феллер – М.: Мир. 1984. – С. 137-139.

89 Фомичев А.Н. Риск-менеджмент: Учебное пособие / А.Н. Фомичев – М.: Зорин В.А. Элементы теории процессов риска. / В.А. Зорин, В.И. Мухин. – Н. Новгород: ННГУ.2003. – 25 с.

90 Фурсов С.В., Рудаков Е.В., Толстых Н.Н. Обзор и исследование троянских программ в контексте оценки их опасности для информационно-телекоммуникационных систем на основе статистического риск-анализа // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 3. - С. 363 – 378.

91 Фурсов С.В., Рудаков Е.В. Описание динамики рисков информационно-телекоммуникационных систем, подвергающихся троянским атакам // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 4. - С. 538 – 548.

92 Хастингс Н. Справочник по статистическим распределениям/ Н. Хастингс, Дж. Пикок. Пер. с англ. А.К. Звонкина. – М.: Статистика, 1980. – 95 с.

93 Хенли Э. Дж. Надежность технических систем и оценка риска / Э. Дж. Хенли, Х. Кумамото – М.: Машиностроение, 1984. – 528 с.

94 Хохлов Н.В. Управление риском: Учеб. Пособие для вузов / Н.В. Хохлов – М.: ЮНИТИ-ДАНА, 1999. – 239 с.

95 Черешкин Д.С. Оценка эффективности систем защиты информационных ресурсов / Д.С. Черешкин. – М.: Институт системного анализа РАН, 1998. – 455 с.

96 Чернова Г.В. Управление рисками: Учебное пособие / Г.В. Чернова, А.А. Кудрявцев. – М.: ТК Велби, Изд-во Проспект, 2003. – 160 с.

97 Шаньгин В.Ф. Защита компьютерной информации / В.Ф. Шаньгин– М.: ДМК пресс, 2008. – 544 с.

98 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин– М.: Форум, Инфра-М, 2008. – 416 с.

99 Шилов И.А. Экология. — М.: Высшая школа. 1997. — 512 с.

100 Шиверский А. Защита информации: проблемы теории и практики / А.Шиверский – М.: Юристь, 1996. – 112 с.

101 Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: учеб. пособие для вузов/ А.Г. Шоломицкий – М.: Изд. дом ГУ ВШЭ, 2005. – 400 с.

102 Язов Ю.К. Основы методологии количественной оценки защищенности и эффективности защиты информации в компьютерных системах / Ю.К. Язов – Ростов-на-Дону: Издательство СКНЦ ВШ, 2006. – 274 с.

103 Ярочкин В.И. Информационная безопасность /В.И. Ярочкин– М.: Летописец, 2000.– 399 с.