Содержание

ВВЕДЕНИЕ

Актуальность

Для современного этапа развития общества характерен непрерывный процесс информатизации и совершенствования информационных технологии. Сфера внедрения телекоммуникационных и вычислительных систем постоянно расширяется, затрагивая все новые стороны жизни общества [70].

Одним из серьезных достижений в сфере информационных технологий на современном этапе их развития является интегрирование средств обработки информации и средств ее обмена [82]. Появившийся в результате такого интегрирования новый класс систем – информационно-телекоммуникационные

(ИТКС) нашел широкое применение в жизни современного общества [84]. Основная функция подобного рода систем – организация функционирования сегментов корпоративных и глобальных компьютерных систем. Вместе с тем в процессе совершенствования этого класса систем приходится констатировать и довольно серьезный факт: увеличение объемов циркулирующей в ИТКС информации приводит к возрастанию потенциальных угроз их информационной безопасности [82, 34].

Одной из угроз безопасности ИТКС являются вредоносные программы. Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы ИТКС. К данной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников [7, 53].

Особое место в этом списке занимают вирусы-черви. Червь (сетевой червь) — тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия [101].

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

1. Проникновения на удаленные компьютеры;
2. Запуска своей копии на удаленном компьютере;
3. Дальнейшего распространения на другие компьютеры сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, интернет-пейджеры, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами и т.д. [81,78].

Для проникновения на удаленные компьютеры и запуска своей копии сетевые черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в

конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений [7, 41].

Некоторые сетевые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, содержат троянские функции или заражают выполняемые файлы на локальном диске, т. е. имеют свойства троянской программы и/или компьютерного вируса [40].

Одной из разновидностей сетевых червей является IRC-Worm. Вредоносная программа, обладающая способностью к несанкционированному пользователем размножению через InternetRelayChats (IRC) [83].

У этого типа червей существует два способа распространения по IRC-каналам, напоминающие способы распространения почтовых червей. Первый способ заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю IRC-канала. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение) [8].

Хакеры постоянно работают над повышением эффективности работы различных вредоносных программ, в том числе и сетевых червей [93]. С самого начала развития ИТКС и по настоящее время угроза вирусного заражения является лидирующей среди всех угроз безопасности информации. По данным статистики, ежегодный ущерб мировой экономике измеряется в миллиардах долларов [26]. А с учетом все возрастающей степени информатизации всех сфер человеческой деятельности и тесной связи мировой экономики и глобальных вычислительных сетей такие ущербы будут только расти [3]. Исходя из этого, обеспечение информационной безопасности – одна из главных задач любой современной организации. Фундаментом для построения системы управления информационной безопасностью являются процессы оценки и управления информационными рисками, значимость которых заключается в возможности, прогнозирования наступления рискового события и заблаговременно принимать необходимые меры по снижению размера возможных неблагоприятных последствий [20, 53]. Поэтому

тема диплома, посвященная исследованию и защите ИТКС, атакуемых сетевым вредоносным обеспечением типа IRC-Worm является актуальной.

Соответствие темы диплома специальности

Данная работа посвящена построению вероятностной модели информационно-телекоммуникационной системы, адекватно отражающей процесс воздействия на нее сетевых атак типа IRC-Worm, а также разработке методики оценки и управления возникающими в данном случае информационными рисками ИТКС. Поэтому тема данной работы соответствует специальности Безопасность телекоммуникаций.

Объектом исследованияявляются ИТКС, в отношении которых реализуются сетевые атаки типа «IRC-Worm», оказывающие деструктивное воздействие на субъекты защищаемой ИТКС.

Предметом исследованияявляется риск-оценка информационной устойчивости информационно-телекоммуникационных систем в условиях реализации сетевых атак типа «IRC-Worm».

Цель и задачи исследования

Цель работысостоит в риск-анализеинформационно-телекоммуникационных систем (ИТКС) как объекта защиты от сетевых атак типа «IRC-Worm», направленных на нарушение целостности, доступности и конфиденциальности защищаемой в ИТКС информации.

Для реализации данной цели необходимо решить следующие задачи:

1. Проанализировать различные модификации исследуемого вредоносного программного обеспечения IRC-Worm и способы проникновения в ИТКС.
2. Разработать аналитическую модель атаки программы класса IRC-Worm на ИТКС.
3. Разработать аналитическую модель рисков ИТКС, подвергающейся атаке программы класса IRC-Worm.

4. Разработать алгоритм управления рисками ИТКС, подвергающейся сетевой атаки типа «IRC-Worm».

5. Провести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;

6. Рассмотреть исследуемую проблематику с точки зрения обеспечения безопасности жизнедеятельности.

Методы исследования

Для решения поставленных задач необходимо использовать методы теории вероятности, математической статистики, теории риска, теории чувствительности, теории управления, элементы теории сложных систем, элементы теории экономического планирования.

Обоснование математической модели

Для исследования воздействия червей типа IRC-Worm на ИТКС в дипломном проекте будет проводиться математическое моделирование. Из-за того, что на практике часто точный вид плотностей распределения вероятности реальных процессов не известен, для аппроксимации используется экспоненциальное распределение. Применимость данного распределения при решении поставленных в работе задач обосновывается в работе.

На защиту выносятсяследующие основные положения работы:

1. Классификация вредоносного программного обеспечения типа «IRC-Worm», способов их проникновения на компьютеры пользователей;

2. Аналитическая модель атак программ класса IRC-Worm на ИТКС;

3. Риск-модель ИТКС, подвергающейся атаке программы класса IRC-Worm;

4. Алгоритм управления рисками ИТКС, подвергающейся атаке программы класса IRC-Worm;

5. Оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования.

Научнаяновизнаисследования

1. Классификация вредоносного программного обеспечения, способов проникновения в ИТКС, отличается от известных тем, что классификация проведена для ПО типа «IRC-Worm». На основе предложенной классификации выработана их обобщенная структура.

2. Аналитическая модель атак чатовых червей на ИТКС, основанная на экспоненциальном распределении, отличается тем, что в основу разработки моделей положен принцип предлагаемой классификации.

3. Алгоритм управления рисками ИТКС, подвергающейся атакам вредоносного программного обеспечения типа «IRC-Worm», отличается тем, что минимизация риска ИТКС проводится путем моделирования разработанной в проекте аналитической модели.

4. Оценка экономической эффективности предложенного алгоритма управления рисками ИТКС, подвергающейся атакам программ класса IRC-Worm, отличается тем, что проведена для вариантов построения систем защиты на основе предложенных моделей и алгоритма.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена исследованию и защите ИТКС, атакуемых сетевым вредоносным программным обеспечением типа «IRC-Worm». В ходе ее выполнения были получены следующие основные результаты:

1. На основании выполненных исследований, разработан новый подход к регулированию интегрального риска реализации асинхронных атак в информационно-телекоммуникационной системе путем корректировки среднего значения ущерба и среднеквадратического отклонения в компонентах системы через

изменение параметров экспоненциального распределения и параметров эпидемиологической SIS-модели ущерба.

2. Предложены суждения по оценке интегрального риска и его экстремумов для случая асинхронных сетевых атак типа «IRC-Worm» в информационно-телекоммуникационной системах, плотность вероятности наступления ущерба, в компонентах которых имеет экспоненциальное распределение.

3. Предложенная оценка экстремумов интегрального риска является перспективным подходом для улучшения качества построения риск-моделейИТКС, регулирования рисков и повышения защищенности систем.

4. Путем математического моделирования была обоснована применимость подхода по регулированию риска ИТКС, плотность вероятности наступления ущерба,в компонентах которых имеет экспоненциальноераспределение.

5. При решении задач, применительно к проблематике работы, результативно использовались методы теории сетей Петри-Маркова, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

6. В работе изложенподход к описанию ущерба наносимого ИТКС сетевой атакой типа «IRC-Worm» при помощи эпидемиологической SIS-модели.

7. Выявлены проблемы защиты ИТКС от сетевых атак типа «IRC-Worm», связанные с неэффективным применением средств защиты от атак данного типа. Решением этой проблемы является построение риск-модели, способных выявить уязвимые компоненты систем и снизить риски реализаций сетевых атак типа «IRC-Worm».

8. В работе изучен генезис процесса подготовки и реализации сетевых атак типа «IRC-Worm», при помощи построения сетей Петри-Маркова и анализа данных поведения червя в системе.

9. На основе оценки экстремумов интегрального риска для систем, состоящих из двух компонентов, была произведена оценка экстремумов

интегрального риска для систем, состоящих из n компонентов в общем виде, в компонентах которых плотность вероятности наступления ущерба имеют экспоненциальноераспределение.

10. На практике, результаты, полученные в данной работе, являются перспективным средством как для повышения защищенности уже существующих ИТКС от сетевых атак типа «IRC-Worm», так и для создания новых защищенных информационно-телекоммуникационных систем от атак данного типа.

11. Решению проблемы защиты ИТКС от сетевых атак посвящено значительное количество работ, однако не существует универсального подхода к управлению рисками в ИТКС, подвергающимся сетевым атакам типа «IRC-Worm». Совершенствованиестарых и разработка новых методов управления позволит решить эту проблему.

12. Оценка достоверности результатов исследования основана на произведении анализа статистических данных по распределению ущерба, предоставленных сайтомsecuritylist.com.

13. Идея работы базируется на попытке расширенного подхода и анализа опыта и практики применения методов оценки, регулирования и управления рисков применительно к сетевым атакам типа «IRC-Worm» на информационно-телекоммуникационные системы.

14. В работе использованы результаты применения современных систем сбора и обработки исходной информации, в частности, сбора и обработки статистических данных, применялись методы их анализа и предварительной обработки.

СПИСОК ЛИТЕРАТУРЫ

1 А. Лукацкий. Атаки на информационные системы. Типы и объекты воздействия. Электроника: Наука, Технология, Бизнес. №1, 2000.

2 Грановский А.В. Основы технологии проектирования систем защиты информации в информационно-телекоммуникационных системах: монография / А.В. Грановский, В.И. Мамай, И.Г. Назаров, Ю.К. Язов. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 260 с.

3 Андреев Д.А., Котрахов В.В., Остапенко А.Г. Компьютерные вирусы: классификация и статистический анализ // Информация и безопасность: научный журнал, Т. 13, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2010. Вып. 2. – С. 295-296.

4 Асташкин В.П. Надежность и техногенный риск: учеб.пособие / В.П. Асташкин. – Воронеж.гос. тех. ун-т, 2002. – 127 с.

5 Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юридическая литература 1991.

6 Безопасность жизнедеятельности: учебник / под ред. проф. Э.А. Арустамова – 10-е изд., перераб. и доп. – М.: «Дашков и Ко», 2006 – 476 с.

7 Безруков Н.Н. Компьютерные вирусы / Н.Н. Безруков. – М.: Наука, 1991.

8 Безруков Н.Н. Компьютерная вирусология. Часть 1: Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в операционной системе MSDOS / 1990. - 450 с.

9 Брайсон А. Прискладная теория оптимального управления / А. Брайсон, Хо Ю-Ши. – М.: Мир, 1972. – 544 с.

10 Вентцель Е.С. Теория вероятностей: учеб.для втузов. - М.: Высш. шк., 1998. - 574 с.

11 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения / Е.С. Вентцель, Л.А. Овчаров. - учеб. пособие для втузов. - 2-е изд., стер. - М.: Высш. шк., 2000. - 383 с.

12 Вероятность и математическая статистика: энциклопедия / Гл. ред. акад. РАН ПрохоровЮ.В. – М.: БольшаяРоссийскаяэнциклопедия, 1999. – 910 с.

13 Википедия — свободная энциклопедия – Электрон.дан. – Режим доступа: http //ru.wikipedia.org.

14 Вирусная энциклопедия Касперского – Электрон. Дан. – Режим доступа: http://www.securelist.com.

15 Вирусная энциклопедия Касперского – Электрон. Дан. – Режим доступа: http://www.viruslist.com.

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

17 Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: Издательство «Единая Европа», 1994.

18 Галатенко В. Информационная безопасность – обзор основных положений. – Открытые системы, 1996. – 42-45 с.

19 Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994. - 400 с.

20 Герасименко В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений. // Региональный научно-технический вестник «Информация и безопасность», Выпуск 4. – Воронеж: ВГТУ, 1999. - с.66-67.

21 Гетманцев А.А. и др. Безопасность ведомственных информационных телекоммуникационных систем. СПб: ВАС, 1997. − 200с.

22 Гилл Ф. Практическая оптимизация: перев.с англ. / Ф. Гилл, У. Мюррей, М. Райт. – М.: Мир, 1985. – 509 с.

23 Глухов Д.О., Яковлев Д.С., Линец Е.А. Риск-анализ компьютерных преступлений на основе статистических данных // Информация и безопасность: научный журнал, т. 12, ч.4. - Воронеж: ГОУ ВПО "Воронежский государственный технический университет", 2009. Вып. 4. - С. 549 558.

24 Горелик В.А., Анализ конфликтных ситуаций в системах управления / В.А.Горелик, М.А.Горелов, А.Ф.Кононенко. – М.: Радио и связь, 1991. – 288 с.

25 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.

26 Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения. М.:Дело и сервис, 2002.

27 Гмурман В.Е. Теория вероятностей и математическая статистика: уч. пособие, 12-е изд., перераб. – М.: Высшее образование, 2006. – 479 с.

28 Дмитриева Е.Ю. Динамические модели оценки чувствительности рисков компьютерных систем при отказах серверов приложений // Информация и безопасность: научный журнал, том 11, ч.4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 4. – с.577-580.

29 Елманова Н. Средства управления корпоративными сетями и приложениями // Компьютер-Пресс. – 2002. – №10.

30 Иванов В. П. Математическая оценка защищенности информации от несанкционированного доступа // Специальная техника. 2004, N 1. С. 58—64.

31 Завгородний М. Г., Махинов Д. В., Скрыль С. В. Способ формирования аналитических выражений для оценки своевременности реакции подсистемы защиты информации. // В сборнике «Прикладные вопросы защиты информации», Воронеж, Изд-во Воронежской высшей школы МВД России, 1996.

32 Зангвилл У. Нелинейное программирование. Единый подход: пер. с. англ. / У. Зангвилл – М.: «Сов. Радио», 1973. – 312 с.

33 Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. Под научной редакцией Зегжды Д.П. и Платонова В.В. – СПб: Мир и семья-95, 1997. – 312с.

34 Зегжда П.Д. Теория и практика обеспечения информационной безопасности / П.Д. Зегжда – М.: Издательство «Яхтсмен», 1996. – 192 с.

35 Зорич В.А. Математический анализ. В 2-х частях. – М.: Фазис, 1997. – 787 с.

36 Злобина И.А. Методические указания к выполнению организационно-экономической части дипломных проектов научно-исследовательского направления для студентов специальности «Информационная безопасность» дневного обучения / И.А. Злобина. – Воронеж, 2003 г. – 26 с.

37 Казьмин О.А. Программное обеспечение риск-анализа систем / О.А. Казьмин, А.Г. Остапенко, А.В. Гребенников // Информация и безопасность: научный журнал, т. 10, ч.2. – Воронеж: Воронеж. гос. техн. ун-т. - 2007. Вып. 2. – С.247-258.

38 Карпычев В.Ю., Минаев В.А. Цена информационной безопасности // Системы безопасности. 2003, № 5. С.128-130.

39 Карташев А.П., Рождественский Б.Л. Обыкновенные дифференциальные уравнения и основы вариационного исчисления. – М.: Наука, 1986. – 464 с.

40 Касперский Е.В. Компьютерные вирусы в MSDOS. –М.: «Эдель» – «Ренесанс», 1992.

41 Касперский Е.В. Компьютерные вирусы и методы борьбы с ними. – М: 1991.

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

43 Кобзарь М., Калайда И. Общие критерии оценки безопасности информационных технологий и перспективы их использования. JetINFO, № 1(56), 1998 г.

44 Кононов А.А. Управление безопасностью региональной информационной инфраструктуры // сб.статей «Проблемы управления информационной безопасностью» под ред. д.т.н., профессора Черешкина Д.С., РАН ИСА, - М., Едиториал УРСС, 2002. - С.36-53.

45 Кривошеин Д.А. Экология и безопасность жизнедеятельности: учеб. пособие для вузов/ Д.А. Кривошеин, Л.А.Муравей, Н.Н. Роева; под ред. Л.А. Муравья. – М.: ЮНИТИ-ДАНА, 2000. – 447 с.

46 Лагунов В.С. Экологическая безопасность и охрана труда: учеб. пособие ч.1 / В.С.Лагунов, М.П.Козорезов, Э.Х. Милушев. – Воронеж: Изд-во ВГТУ, 1999. -61 с.

47 Лазарев И.А. Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений // РАЕН МАИПиТ, Московский городской центр научно-технической информации, - М., 1997.

48 Липаев В.В. Анализ и сокращение рисков проектов сложных программных средств / В.В. Липаев – М.: СИНТЕГ, 2005. – 224 с.

49 Ловцов Д.А. Контроль и защита информации в АСУ. – М.: ВА им. Ф.Э. Дзержинского. 1997. – 240 с.

50 Львович Я.Е., Скрыль С.В. Распределенная защита информации как фактор повышения эффективности мер по борьбе с преступлениями в сфере компьютерной информации. // Региональный научно-технический вестник «Информация и безопасность», Выпуск 3. – Воронеж: ВГТУ, 1998. - с.125-129.

51 Мамаев М., Петренко С. Технология защиты информации в Интернете: Специальный справочник. – СПб.: Питер, 2002.

52 Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с англ. -М: Мир, 1993. – 216 с.

53 Мельников В. Защита информации в компьютерных системах / В. Мельников – М.: «Финансы и статистика», «Электронинформ», 1997.

54 Методические указания по проведению организационно-экономической части производственной и преддипломной практик студентами всех спец. ФАЭМ, РТФ, ФТФ, ЕГФ всех форм обучения. Сост. Г.Ф. Салова и др. – Воронеж: ВГТУ, 1995. - 23 с. (№ 133-95)

55 Методические указания к выполнению организационно-экономической части дипломных проектов научно-исследовательского направления для студентов специальности 200200 «Микроэлектроника и полупроводниковые приборы» дневного обучения. Сост. В. Ф. Савенкова – Воронеж: ВГТУ, 1999. - 24 с. (№ 99-99)

56 Микроэлектроника. Учеб. пособие для втузов. В 9 кн. / Под ред. Л.А. Коледова. Кн. 9. Экономика и организация разработок, освоения и производства изделий микроэлектроники / А.В. Проскуряков и др. -М.: Высш. шк., 1987. - 160 с.

57 Моделирование информационных операций и атак в сфере государственного у муниципального управления. В.Г. Кулаков, В.Г. Кобяшев, А.Б. Андреев и др; Под. ред. Борисова. – Воронеж: ВИ МВД России, 2004. – 144 с.

58 Мотузко Ф.Я. Охрана труда / Ф.Я. Мотузко. – М.: Высшая школа, 1989.– 336 с.

59 Н.А. Костин. Общие основы теории информационной борьбы. М.: Академия ГШ, 2000, 308 с.

60 Омнов П.И. Безопасность жизнедеятельности в производственной среде учеб. пособие / П.И. Омнов. – Воронеж. гос. тех. ун-т, 1992, - 320 с.

61 Организация, планирование и управление предприятиями электронной промышленности / Под ред. П.М. Стуколова. М.: Высш. шк., 1986. -319с.

62 Орлова И.Г., Преображенский Б.Г. Методические указания по выполнению организационно-экономической части дипломных работ исследовательского

характера для студентов специальностей 230100 и 230300. - Воронеж: ВГТУ, 1994. - 39 с. (№ 36-94)

63 Остапенко А.Г., Линец Е.А., Пархоменко Д.А. Исследование компьютерной преступности на основе статистического риск-анализа // Информация и безопасность: научный журнал, Т. 13, Ч. 2. - Воронеж: ГОУ ВПО "Воронежский государственный технический университет", 2010. Вып. 2. - С. 185-194.

64 Остапенко Г.А. Информационные операции и атаки в социотехнических системах: уч. пособие для вузов / Под ред. чл.-корр. РАН В.И. Борисова. – М.: Горячаялиния - Телеком, 2007. – 134 с.

65 Остапенко О.А. Риски систем: оценка и управление / О.А. Остапенко, Д.О. Карпеев, В.Н. Асеев; Под редакцией Ю.Н. Лаврухина. – М: Горячая линия - Телеком, 2007. – 247 с.

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

67 Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов.

68 Преображенский Б.Г. и др. Основы экономики производства. - Воронеж: ВГТУ, 1998. - 100 с.

69 Протоколы Internet. С. Золотов. – СПб.: BHV – Санкт-Петербург, 1998. – 212 с.

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

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

72 Розенвассер Е.Н. Чувствительность систем управления / Е.Н. Розенвассер, Р.М. Юсупов – М.: Наука, Главная редакция физико-математической литературы. 1981. – 464 с.

73 Российская Газета - Федеральный выпуск №4131. Электрон. дан. — Режим доступа: http://www.rg.ru/2006/07/29/informacia-dok.html

74 Романец Ю. В., Тимофеев П. А. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.

75 Румянцев А.А. Экономическая эффективность научных исследований (методология измерения). М.: Экономика, 1974. - 167 с.

76 Сборник докладов международной конференции «Компьютерные вирусы и другие преднамеренные программные воздействия». – Киев: 1991. – 502 с.

77 Сетевые графики в планировании / И.М. Разумов и др. М.: Высш. шк, 1981.-168 с.

78 Скрыль С.В. Информатика: учебник для высших учебных заведений МВД России. Т. 2. — Информатика: Средства и системы обработки данных / С.В. Скрыль [и др.]. – М.: Маросейка, 2008. – 544 с.

79 Скрыль С.В. Информатика: учебник для высших учебных заведений МВД России. Том 2. Информатика: Средства и системы обработки данных / С.В. Скрыль [и др.]. – М.: Маросейка, 2008. – 544с.

80 Скрыль С.В. Показатель эффективности защиты информации в автоматизированных системах. // Материалы Международной конференции «Информатизация правоохранительных систем". Ч.2. - М.: Академияуправления МВД России. 1997. с. 36-38.

81 Скрыль С.В., Лаврухин Ю.В., Курило А.П., Багаев Д.А. Обоснование показателей для оценки эффективности информационных процессов в информационно-телекоммуникационных системах в условиях противодействия угрозам информационной безопасности // Информация и безопасность: научный журнал, Т. 12, Ч. 3. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 3. – С. 429-432.

82 Скрыль С.В. [и др.] Информационная безопасность телекоммуникационных систем (технические вопросы): учебное пособие для системы высшего профессионального образования России. – М.: Радио и связь, 2004. – 388с.

83 Собейкис В.Г. Азбука хакера 3. Компьютерная вирусология. – М.: Майор, 2006. – 512 с.

84 С. Симонов. Аудит безопасности информационных систем. JetInfo, №9, 1999.

85 Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. - М.: Издательство «Яхтсмен», 1996.

86 Толстых Н.Н. К вопросу об оценке информационной защищенности автоматизированных телекоммуникационных систем / Н.Н. Толстых, В.А. Павлов, А.Н. Пятунин // Сборник трудов 8 Международной конференции «Радиолокация, навигация, связь», Воронеж, 23–25 апреля 2002 г.

87 Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»

88 Федотов Н. В. «Оценка и нейтрализация рисков в информационных системах»: Методическое пособие по курсу «Основы информационной безопасности»/ Н.В. Федотов, В.А. Алешин; Под ред. Н.В. Медведева. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2004, - 52 с.

89 ХоффманЛ.Д. Информационная война. Институт инженерных и прикладных проблем. Вашингтон, 1995.

90 Цыпкин Я.З. Адаптация и обучение в автоматизированных системах. – М.: Наука, 1968. – 400 с.

91 Шевченко Е.Н. Математическое моделирование риспределения риска при независимых случайных величинах вероятностей исходных событий и ущерба // Фундаментальные исследования. – 2011. – № 12 (часть 3). – с. 604-608

92 Штарьков Ю.М. Некоторые теоретико-информационные задачи защиты дискретных данных. – Проблемы передачи информации. 1994. – Т. 30. – № 2. – 49 – 60 с.

93 Щербаков. Как писать вирусы / Щербаков. – М.: 1993.

94 Экономика и управление в отраслевых НТО / Под ред. П.Н. Завлина, А.К. Казанцева, - М: Экономика, 1990. - 447 с.

95 Экономика машиностроительного производства / Под ред. И.Э. Берзиня и В.П. Калинина. - М: Высш. шк., 1988. - 304с.

96 Экономика электронной промышленности / Под ред. П.М. Стуколова. - М.: Высш. шк., 1983. - 192с.

97 Юсупов Р.М. Вопросы кибернетики. Теория чувствительности и ее применение. – М.: Связь, 1977. – 280 с.

98 Юсупов Р.М., Пальчун Б.П. Безопасность компьютерной инфосферы систем критических приложений. // Вооружение. Политика. Конверсия. 1993. – № 2. – 52-56 с. – № 3. – 23-31 с.

99 Яглом А., Яглом И. Вероятность и информация. М.: Мир, 1985. – 110 с.

100 Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Международные отношения, 2000. – 400 с.

101 IRC вирусы. Электрон. дан. — Режим доступа: http://hack-area.narod.ru/irc1.html

102 Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. Вып. 4. – СПб.: Наука, 2007.

103 Остапенко А.Г. Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств / А.Г. Остапенко, Ю.К. Язов, Р.В. Батищев, О.А. Середа // Информация и безопасность. – 2001. – №2. С. 4-11.

104 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.

105 Остапенко А.Г. Функция возможности в оценке рисков, шансов и эффективности систем. // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 1., С. 17-20.

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