Содержание

Введение

Актуальность исследования.

К обмену новостями (информацией) люди стремились во все времена [120]. Поэтому передача информации на расстояние – одно из самых замечательных достижений человечества. Люди стремились предавать информацию на максимально возможное, практически неограниченное расстояние. Не случайно названия основных видов связи начинаются с греческого слова «теле», что означает «вдаль, далеко». Телеграфирование – это запись на расстоянии; телефонирование – это звучание на расстоянии; телевидение – передача изображений на расстояние. С древних времѐн средства передачи информации прошли путь от «живого телефона», сигнальных костров, гонгов, телеграфа, до телефона, радио, телевидения, мобильной связи и интернета в наши дни.

Современная сеть передачи информации базируется на трѐх китах. Первый – это абонентские устройства, например телефоны. Второй кит – станции, обеспечивающие соединение абонентов между собой, распределение потоков информации по направлениям. Третий кит – линии связи, соединяющие абонентов со станциям и станции между собой [120].

Одним из серьѐзных достижений в сфере информационных технологий на современном этапе их развития является интегрирование средств обработки информации и средств еѐ обмена [129]. Появившийся в результате такого интегрирования новый класс систем – информационно-телекоммуникационные (ИТКС) нашѐл широкое применение в жизни современного общества [135]. 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 серьѐзный факт:

увеличение объѐмов циркулирующей в ИТКС информации приводит к возрастанию потенциальных угроз их информационной безопасности [128, 129].

Негативным последствием информатизации общества является появление компьютерной преступности [3, 4, 5, 7, 8, 68, 90, 124]. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных, включая и жизнеобеспечивающие, объектов, серьезное нарушение работы ЭВМ и их систем. Несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям. Опасность компьютерных преступлений многократно возрастает, когда они совершаются в отношении функционирования объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики [12, 65].

Большой ущерб информационно-телекоммуникационным системам (ИТКС) могут нанести различные вредоносные программы, среди которых особое место занимают троянские программы [5, 7, 12, 13, 57, 68, 124].

Троянская программа (также – троян, троянец, троянский конь) – вредоносная программа, распространяемая людьми. В отличие от вирусов и червей, которые распространяются самопроизвольно. Название «троянская» восходит к легенде о «Троянском коне» – дарѐном деревянном коне, послужившим причиной падения Трои. Большая часть троянских программ действует подобным образом – маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своѐм компьютере [5, 13, 57].

Троянские программы распространяются людьми – как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах.

Для достижения последнего, троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы [3, 12, 13, 68].

Для маскировки троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных (например картинки), как для запуска пользователем, так и для маскировки в системе своего присутствия.

Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для распределенных DoS-атак на удаленные ресурсы сети) [5].

Хакеры постоянно работают над повышением эффективности работы различных вредоносных программ, в том числе и троянов [5, 7, 8, 9, 12, 13, 35, 57]. Следовательно, 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, во-первых, прогнозировать в определенной степени наступление рискового события, во-вторых, заблаговременно принимать необходимые меры к снижению размера возможных неблагоприятных последствий [1, 2, 9,14, 15, 41, 52, 64, 77, 121, 122]. Поэтому тема диплома, посвящѐнная изучению тенденций развития троянов, и предотвращение ситуаций нанесения ими ущерба информационно-телекоммуникационной системе является актуальной.

Соответствие темы диплома специальности.

Данная работа посвящена изучению воздействий троянов на информационно-телекоммуникационные системы, предотвращению ситуаций нанесения ими ущерба ИТКС, т.е. обеспечению безопасности ИТКС. Поэтому можно сделать вывод о соответствии темы данной работы специальности Безопасность телекоммуникаций.

Объектом исследования являются информационно-телекоммуникационные системы подвергающиеся воздействиям типа «троян».

Предметом исследования является риск-оценка информационной устойчивости информационно-телекоммуникационных систем в условиях реализации воздействия типа «троян».

Цель и задачи исследования.

Целью настоящей работы является построение вероятностной модели троянских атак на информационно-телекоммуникационную систему и разработка методики оценки и управления возникающими в данном случае информационными рисками ИТКС.

Для реализации данной цели необходимо решить приведенные ниже задачи:

1. Рассмотреть подходы к определению и классификацию троянских программ, способы их проникновения на компьютеры пользователей, а также их структуру.
2. Разработать и провести исследование вероятностной модели троянских атак на ИТКС.
3. Разработать риск-модели ИТКС системы, подвергающейся троянским атакам.
4. Разработать алгоритм управления рисками ИТКС, подвергающейся троянским атакам.
5. Произвести оценку экономической эффективности предложенного алгоритма управления рисками ИТКС, подвергающейся троянским атакам. Рассчитать экономический ущерб от воздействия типа «троян».

Методы исследования.

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

Обоснование математической модели.

Для исследования воздействия троянских программ на ИТКС в данной работе прибегнем к методу математического моделирования. Так как часто на практике точный вид плотности распределения вероятности реальных процессов не известен, для аппроксимации воспользуемся обобщѐнным распределением Эрланга вида $k(1)$. Использование данного распределения обосновывается в работе.

При построении математической модели воздействия трояна на ИТКС

На защиту выносятся следующие основные положения работы:

1. Классификация троянских программ, способов их проникновения на компьютеры пользователей, а также обобщенные варианты их структуры.

2. Вероятностная модель троянских атак на ИТКС.
3. Риск-модели компьютерной системы, подвергающейся троянским атакам.
4. Алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам.
5. Оценка экономической эффективности предложенного алгоритма управления рисками ИТКС, подвергающейся троянским атакам.

Научная новизна исследования.

1. Проведена классификация троянских программ, отличающаяся тем, что с учетом проведенного исследования подходов к определению троянских программ, способов их проникновения на компьютеры пользователей, а также их структуры выработаны обобщенные варианты их структуры, которые выбраны за основу классификации.
2. Предложены вероятностные модели троянских атак на ИТКС, основанные на распределении Эрланга, отличающиеся тем, что в основу разработки моделей положен принцип предлагаемой классификации.
3. Впервые предложен алгоритм управления рисками ИТКС, подвергающейся троянским атакам.
4. Впервые проведена оценка экономической эффективности предложенного алгоритма управления рисками ИТКС, подвергающейся троянским атакам.

Практическая ценность работы заключается в том, что:

1. Результаты исследований подходов к определению и классификация троянских программ, способов их проникновения на компьютеры пользователей, а также их структуры могут быть использованы для ознакомления пользователей программных продуктов с троянскими программами с целью снизить вероятность неправильных действий

пользователя, позволяющих трояну проникнуть в ИТКС. Кроме того, выявленные особенности работы троянских программ могут помочь программистам, создающим программное обеспечение, позволяющее отслеживать подозрительную активность действующих программ.

2. Разработанная вероятностная модель троянских атак на компьютерную систему, может служить математической базой для оценки рисков и защищенности компьютерных систем, подвергающихся троянским атакам.
3. Риск-модели компьютерной системы, подвергающейся троянским атакам, позволяют указать области эффективного управления рисками.
4. Алгоритм управления рисками ИТКС, подвергающейся троянским атакам, может быть использован при оптимизации параметров ИТКС с целью минимизации рисков.

Заключение

Дипломный проект посвящен вопросам проведения исследований рисков информационной устойчивости информационно-телекоммуникационных систем в условиях реализации воздействия типа «троян».

В ходе выполнения работы были получены следующие основные результаты:

- проведена классификация троянских программ на основе обобщенных вариантов их структуры. На основе полученного результата выбрана вероятностная модель троянских программ;
- предложена вероятностная модель троянских атак на ИТКС. Эта модель была принята за математическую базу при проведении риск-анализа защищенности компьютерных систем, подвергающихся троянским атакам;
- предложена риск-модель компьютерной системы, подвергающейся троянским атакам. На основе риск-модели выбраны области эффективного управления рисками;
- предложен алгоритм управления рисками ИТКС, подвергающейся троянским атакам. При помощи предложенного алгоритма можно оптимизировать параметры ИТКС с целью минимизации рисков;
- оценена экономическая эффективность предложенного алгоритма управления рисками ИТКС, подвергающейся троянским атакам. Проведенная оценка показала экономическую целесообразность применения предложенных моделей и алгоритмов при исследовании риска ущерба ИТКС за счет троянских атак.

Список литературы

1 Симонов С. Анализ рисков, управление рисками. JetInfo, №1, 1999.

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

3 Астахов С.А. Актуальные вопросы выявления сетевых атак / С.А. Астахов. – М., 2002. – 169 с.

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

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

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

7 Щербаков. А.А. Как писать вирусы / А.А. Щербаков. – М.: 1993.

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

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

10 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», Вып. 3. – Воронеж: ВГТУ, 1998. – С. 125-129.

11 Герасименко В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений. // Региональный научно-технический

вестник «Информация и безопасность», Вып. 4. – Воронеж: ВГТУ, 1999. - С. 66-67.

12 Расторгуев С.П. Информационная война / С.П. Расторгуев – М.: «Радио и связь», 1998. – 416 с.

13 Белоусов С.А. Троянские кони. Принципы работы и методы защиты: учебное пособие / С.А. Белоусов, А.К. Гуц, М.С. Планков. – Омск: Издательство Наследие. Диалог-Сибирь, 2003 – 84 с.

14 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.

15 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.

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

17 Кулаков В.Г. Риск-анализ информационных систем / В.Г. Кулаков, Д.О. Карпеев, А.Г. Остапенко // Информация и безопасность: научный журнал, Т. 11, Ч. 1. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 1. – С. 7-30.

18 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.

19 Остапенко О.А. Методология оценки риска и защищенности систем // журнал «Информация и безопасность». – Воронеж: Воронеж. Гос. Техн. Ун-т. – 2005. Вып. 2. – С. 28-32.

20 В.И. Клейменов Инновации и риски: механизмы и практика создания региональной инновационной системы Воронежской области //

Информация и безопасность: научный журнал, Т. 11, Ч. 3. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 3. – С. 331-336.

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

22 Лефевр В.А. Конфликтующие структуры. Изд. третье. / В.А. Лефевр. – М.: Институт психологии РАН, 2000. - 136 с.

23 Прилепский В.В. Конфликты в информационно-телекоммуникационных системах: учеб. пособие / В.В. Прилепский. – Воронеж: Воронеж. гос. техн. ун-т, 2004. – 144 с.

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

25 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.

26 Federal Criteria for Information Technology Security (FC), Draft Version 1.0, (Volumes I and II). - National Institute of Standards and Technology, National Security Agency, US Government, 1993.

27 Скрыль С.В. Показатель эффективности защиты информации в автоматизированных системах. // Материалы Международной конференции –Информатизация правоохранительных систем”. ч.2. - М.: Академия управления МВД России. 1997. С. 36-38.

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

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

30 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.

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

32 Касперский Е.В. Компьютерные вирусы в MS DOS. –М.: «Эдель» – «Ренесанс», 1992.

33 Frank A. Stevenson. Cracked WINDOWS. PWL. FIDO area LV.MTASK, 05.12.95.

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

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

36 Костин Н.А. Общие основы теории информационной борьбы. «Военная мысль», 1997, №3.

37 Павлов В.А., Пятунин А.Н., Сидоров Ю.В., Толстых Н.Н. Оценка возможности применения метода координации при моделировании конфликтного функционирования автоматизированных телекоммуникационных систем. Сборник трудов 7 международной конференции «Радиолокация, навигация, связь», Воронеж, 24-26 апреля 2001, Т. 2 — С. 1047-1060.

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

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

40 Расторгуев С.П. Философия информационной войны. М.: 2002.

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

42 Howard J. D. An Analysis of Security Incidents on the Internet. - Pittsburgh, Pennsylvania, 15213 USA, 1997.

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

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

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

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

47 Толстых Н.Н. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: Учебное пособие // Н.Н. Толстых, В.А. Павлов, Е.И. Воробьева – Воронеж: Воронежский государственный технический университет, 2003. – 93 с.

48 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.

49 Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления – М.: Гостехиздат, 1968. – 607 с.

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

51 Эрроусмит Д., Плейс К. Обыкновенные дифференциальные уравнения: Качественная теория с приложениями. – М.: Мир, 1986. – 243 с.

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

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

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

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

56 Статьев В.Ю., Шарков А.Е. Проблемы защиты корпоративной информационной системы в процессе ее интеграции в сети общего пользования // Сборник материалов 5-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества», - М., 2003. - С. 184-186.

57 Мищенко Е. Троянские программы: ликбез и самостоятельная защита // КомпьютерПресс, вып. №4, 2005.

58 Щербаков В.Б. Пример оценки риска информационной безопасности беспроводных сетей стандарта IEEE 802.11 на основе использования теории нечетких множеств и нечеткой логики / В.Б. Щербаков, С.А. Ермаков, Д.А. Андреев // Информация и безопасность: научный журнал, Т. 11, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 2. – С. 249-252.

59 Радько Н.М. Расчет рисков ИТКС с учетом использования мер и средств противодействия угрозам удаленного и непосредственного доступа к

ее элементам / Н.М. Радько, И.О. Скобелев, Д.В. Паниткин // Информация и безопасность: научный журнал, Т. 11, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 2. – С. 257-260.

60 Карпеев Д.О. Анализ динамики рисков информационных систем // Информация и безопасность: научный журнал, Т. 11, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 2. - С. 284-287.

61 Дмитриева Е.Ю. Параметры и характеристики рисков отказов серверов приложений / Е.Ю. Дмитриева, С.В. Фурсов // Информация и безопасность: научный журнал, Т. 11, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 4. – С. 537-542.

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

63 Тишков С.А. Динамические модели риска отказов в обслуживании / С.А. Тишков, А.Г. Остапенко // Информация и безопасность: научный журнал, Т. 11, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 4. – С. 609-610.

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

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

66 Розанов В.Н. Системный анализ для инженеров. – СПб.: СпбГУ, 1998.

67 Райзберг Б.А., Фатхутдинов Р.А. Управление экономикой. – М.: Издательство ЗАО Бизнес-школа, 1999.

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

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

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

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

72 Базара М. Нелинейное программирование. Теория и алгоритмы: пер. с англ. / М. Базара, К. Шетти. – М.: Мир, 1982. – 583 с.

73 Толстых Н.Н. Обобщенная модель процесса функционирования автоматизированных систем в режиме информационного конфликта / Н.Н. Толстых, В.А. Павлов, Р.В. Павлов // Информация и безопасность – Воронеж: ГОУ ВПО «Воронежский государственный технический университет» 1999. № 4.

74 Хейес-Рот Ф. Построение экспертных систем. – М.: Мир, 1987. – 370 с.

75 Понтрягин Л.С. Обыкновенные дифференциальные уравнения // М.: Физматгиз, 1961. – 331 с.

76 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.

77 Остапенко Г.А. Оценка влияния на риск сложных информационно-телекоммуникационных систем рисков отдельных подсистем / Г.А. Остапенко, А.Е. Иохвидова // Информация и безопасность: научный журнал, Т. 11, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 2. – С. 280-283.

78 Тишков С.А. Риск-модели распределенных атак отказа в обслуживании // Информация и безопасность: научный журнал, Т. 11, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2008. Вып. 4. – С. 613-614.

79 Матвеев. Н.М. Лекции по аналитической теории дифференциальных уравнений. – СПб.: Изд-во СПбУ, 1995. – 436 с.

80 Ланнэ А.А. Нелинейные динамические системы: Синтез, оптимизация идентификация – СПб.: Военная академия связи, 1985. – 88 с.

81 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.

82 Басовский Л.Е. Управление качеством / Л.Е. Басовский, В.Б. Протасьев. – М: ИНФРА-М, 2001. – 212 с.

83 Лагунов В.С. Безопасность и экологичность в дипломном проекте: Учеб. пособие по дипломному проектированию / Лагунов В.С. – 2-е изд., перераб. и доп. – Воронеж: ВГТУ, 2003. – 124 с.

84 Остапенко А.Г. Анилиз и синтез линейных радиоэлектронных цепей с помощью графов // А.Г. Остапенко, - М: Радио и связь, 1985. – 280 с.

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

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

87 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.

88 Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186 с.

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

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

91 Хоффман Л.Д. Информационная война. Институт инженерных и прикладных проблем. Вашингтон, 1995.

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

93 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.

94 Бахвалов Н. С. Численные методы: анализ, алгебра, обыкновенные дифференциальные уравнения. – М.: Наука, 1975. – 631с.

95 Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. –М.: Гротек, 1997. – 248 с.

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

97 Соколов С. В., Шаньгин В. Ф. Защита информации в распределенных сетях и системах. – М.: ДМК Пресс, 2002.

98 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.

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

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

101 Галатенко В. Информационная безопасность – обзор основных положений. – Открытые системы, 1996. – С. 42–45.

102 Кокунин П. А. Полигауссовы модели и методы в многоуровневой иерархической концепции построения инфокоммуникационных систем // Динамика и развитие иерархических (многоуровневых) систем (теоретические и прикладные аспекты). — Казань : Волга Пресс, 2003. — С. 44-46.

103 Розенвассер Е.Н. Достаточные условия применимости первого приближения в задачах теории чувствительности – Автоматика и телемеханика, 1980. – № 03. – С. 43-47.

104 Шляхин В.М. Обобщенный показатель устойчивости систем в условиях их конфликтного взаимодействия // Информационный конфликт в спектре электромагнитных волн. Приложение к журналу «Радиотехника». 1994. № 4. С. 31-35.

105 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.

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

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

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

109 ГОСТ Р 51898-02 "Аспекты безопасности. Правила включения в стандарты".

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

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

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

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

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

115 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.

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

117 Безопасность жизнедеятельности / Под ред. Н.А. Белова - М.: Знание, 2000. – 364 с.

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

119 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.

120. Шарле Д.Л. По всему земному шару. – М.: Радио и связь, 1985. – 320 с., ил.

121. 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: научный журнал, Т. 12, Ч. 3. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 3. – С. 363-379.

122. Остапенко А.Г., Карпеев Д.О., Плотников Д.Г. Перспективы развития методологии риск-анализа систем // Информация и безопасность: научный журнал, Т. 12, Ч. 3. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 3. – С. 419-425.

123. Фурсов С.В, Рудаков Е.В. Описание динамики рисков информационно-телекоммуникационных систем, подвергающихся троянским атакам // Информация и безопасность: научный журнал, Т. 12, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 4. – С. 537-548.

124. Андреев Д.А., Брянский А.Е. Вирусы и риски заражения систем: обзор и построение обобщѐнных вероятностных моделей // Информация и безопасность: научный журнал, Т. 12, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 4. – С. 519-536.

125. Бегишев И.Р. О некоторых способах совершения противоправных деяний в современных информационно-телекоммуникационных системах обращения цифровой информации // Информация и безопасность: научный журнал, Т. 12, Ч. 4. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 4. – С. 607-610.

126. 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.

127. Громов Ю.Ю., Драчѐв В.О., Войтюк В.В., Мартемьянов Ю.Ф., Громова А.Ю. Классификация видов атакующих воздействий на информационную систему // Информация и безопасность: научный журнал, Т. 12, Ч. 3. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2009. Вып. 3. – С. 413-418.

128. 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.

129. 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.

130. Скрыль С.В, Зарубин В.С., Фомин А.Я. Проблема оптимизации процессов защиты информации в информационно-телекоммуникационных системах сферы критических приложений . // Информация и безопасность: научный журнал, Т. 13, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2010. Вып. 2. – С. 239-242.

131. Остапенко Г.А., Плотников Д.Г., Дуплищева А.Ю. К вопросу об управлении рисками распределѐнных информационных систем // Информация и безопасность: научный журнал, Т. 13, Ч. 2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2010. Вып. 2. – С. 419-425.

132. 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.

133. 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.

134. Пахомова А.С. Определение киберпространства и его отличительные особенности // Информация и безопасность: научный журнал, Т. 14, Ч. 1. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2011. Вып. 1. – С. 137-140.

135. 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.

136. Вадзинский Р.Н. Справочник по вероятностным распределениям. – СПб.: Наука, 2001. — 295 с., ил.116.

137. Вентцель Е.С. Введение в исследование операций. — М.: Советское радио, 1964.

138. Пресс-релиз компании Яндекс. Электрон. дан. — Режим доступа: www./company.yandex.ru/press_releases/2010/0301/index.xml.

139. Тихонов В.И. Статистическая радиотехника. — М.: Радио и связь, 1982. — 624 с.

140. Остапенко Г.А., Плотников Д.Г., Дуплищева А.Ю. К вопросу об управлении рисками распределѐнных информационных систем // Информация и безопасность: научный журнал, Т. 13, Ч.2. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2010. Вып. 2. – С. 59-60.

141. Остапенко А.Г. Функция возможности в оценки рисков, шансов и эффективности систем. // Информация и безопасность: научный журнал, Т. 13, Ч. 1. – Воронеж: ГОУ ВПО «Воронежский государственный технический университет», 2010. Вып. 1. – С. 17-20.