Содержание

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

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

Введение

Актуальность исследования.Обеспечение информационной безопасности – одна из главных задач любой современной организации. Фундаментом для построения системы управления информационной безопасностью являются процессы оценки и управления информационными рисками [1]. Значимость управления информационными рисками заключается в возможности, во-первых, прогнозировать в определенной степени наступление рискового события, во-вторых, заблаговременно принимать необходимые меры к снижению размера возможных неблагоприятных последствий[2].

Из-за неадекватной оценки рисков, связанных с осуществлением угроз информационной безопасности в современном высокотехнологичном обществе, государство, организации и отдельные личности несут весьма ощутимый ущерб [3]. Точность оценки рисков, связанных с осуществлением деятельности по информационной безопасности, является основной характеристикой профессиональной зрелости специалиста в предметной области. При отсутствии адекватной оценки рисков сложно решать вопрос о необходимости и достаточности того или иного набора мер по защите информации и их адекватности существующим рискам [4].

В данной дипломной работе предлагается проведение риск-оценки информационной устойчивости программных продуктов при воздействиях типа «троян».

«Троян» - программа (программный модуль), осуществляющая различные несанкционированные действия: сбор информации иее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях[5].

Программные продукты занимают промежуточное положение между вычислительными процессами низкого уровня (функционирование процессоров) и процессами высокого уровня – взаимодействие с оконечным оборудованием или пользователем. Поэтому программные продукты являются

определяющимиэлементами как для индикации нарушений нормальной работы процессора, так и для контроля в отношении оконечного оборудования или пользователя. Но программные продукты могут существовать только в контексте некоторой компьютерной системы, следовательно, риск-оценку информационной устойчивости программных продуктов необходимо рассматривать как риск-оценку (риск-анализ) информационной устойчивости компьютерной системы, в состав которой они входят.

Под информационной устойчивостью компьютерной системы будем понимать способность компьютерной системы эффективно реализовывать свои целевые функции, т.е. эффективно функционировать[47, 73]. При этом показателем устойчивости может выступать амплитуда отклонения риска компьютерной системы от некоторого заданного значения.

В настоящее время за счет существенного расширения номенклатуры и возможностей троянских программ эффективность средств защиты информации заметно снизилась.Поэтому вопрос оценки рисков, связанных с осуществлением троянских атак на компьютерную систему, является первоочередным и заслуживающим достаточного внимания.

Степень научной разработанности. Исследование вопросов взаимодействия троянских программ с компьютерными системами было начато с задержкой примерно в один год после появления данного класса информационных воздействий. При этом необходимо отметить, что вопросы принципиального построения и алгоритмов функционирования этих программных продуктов обсуждалось задолго до их появления на международной конференции в Киеве[6], в приватных конференциях сетей Fido, рассматривались в [7, 8]. В этих работах в той или иной степени анализировались вопросы взаимодействия средств информационных воздействий с элементами операционных платформ, однако, как таковых вопросов защиты не ставилось, что было обусловлено:

- замкнутостью концепций защиты на гармонизированные критерии «Оранжевой книги» и отсутствием формализованных моделей взаимодействия

конфликтного компонента с изменяющимися во времени элементами операционной среды;

- сведением информационного конфликта только к процессу нейтрализации конфликтного компонента или его удалению на основе сигнатурного поиска в заданном объеме унитарного кода, хранящегося, обрабатываемого или передаваемого другому объекту информатизации;

- отсутствием согласованности концептуальных положений различных школ и течений в области противодействия информационным воздействиям.

Начиная со второй половины 90-х годов, в связи с интенсификацией процесса внедрения информационных технологий в критические приложения систем государственного и военного управления, возрастанием стоимости ошибки, а также появлением класса информационных технологий ускорились разработки и систем защиты. Работы, посвященные этому вопросу, можно условно разделить на два класса: теоретические и практические.

К работам в той или иной степени рассматривающим практические аспекты построения и применения систем защиты информации можно отнести [9-11, 24-31, 89, 95]. Среди теоретических работ посвященных рассмотрению вопросов защиты информации можно выделить [4, 12, 35-43]. Однако, эти работы, также как и указанные выше, ограничивались рассмотрением только вопросов обнаружения и нейтрализации информационных воздействий (в частности троянских программ) и совершенно игнорировали системный подход к вопросам обеспечения информационной безопасности в условия информационного конфликта.

Отказ от изолированного рассмотрения угроз и использование аппарата теории рисков привели в начале нового тысячелетия к постепенному переходу от одностороннего поиска сигнатур информационных воздействий в потоках унитарного кода к анализу процессов взаимодействия информационных систем с учетом потерь и выигрышей в результате информационного конфликта [14-20, 37, 58-63]. В этих работах, несмотря на подход к вопросу обеспечения информационной безопасности с новых позиций, не проводился анализ взаимодействиятроянских программ как с системами защиты,так и самими защищаемыми объектами,

хотяпроцесс реализации своих целевых функций этими воздействиями в операционной среде имеет достаточно много особенностей, которые, в ряде случаев, выходят за рамки основных положений и концепций, рассматриваемых в вышеперечисленных работах.

Поэтому проведение риск-оценки информационной устойчивости программных продуктов при воздействиях типа «троян» является актуальной и практически важной задачей.

Цель и задачи исследования. Цель настоящей работызаключается в построении адекватной вероятностной модели троянских атак на компьютерную систему, а также в разработкеметодики оценки и управления возникающими в данном случае информационными рисками компьютерной системы.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть подходы к определению и классификацию троянских программ, способы их проникновения на компьютеры пользователей, а также их структуру;

- разработать и исследовать вероятностные модели троянских атак на компьютерную систему, из одного и нескольких источников;

- разработатьриск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников и исследовать их с позиций теории чувствительности;

- разработать алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников;

- произвести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;

- рассмотреть исследуемую проблематику с точки зрения обеспечения безопасности жизнедеятельности.

Объект исследования. Объектом исследования в данной работе является компьютерная система, подвергающаяся троянским атакам, причем каждая такая атака может быть либо успешной, либо неуспешной.

Предмет исследования. Предметом исследования является риск-оценка (риск-анализ) информационной устойчивости атакуемой компьютерной системы.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным применением используемых в настоящей работе методов исследования для реализации поставленной цели исследования.

Методы исследования. Для решения поставленных задач исследования в ходе выполнения работы применялись методы теории вероятностей, математической статистики, теории конфликта, теории математического моделирования,теории рисков, теории чувствительности, теории математического анализа, теории оптимального управления и теории нелинейного программирования.

Научная новизна результатов исследования.В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

- разработаны вероятностные модели троянских атак на компьютерную систему из одного и нескольких источников на основе показательного распределения;

- разработаны риск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников;

- построены уравнения движения рисков атакуемой компьютерной системы относительно их параметров на основе проведенного анализа чувствительности рисков;

- разработан алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников, на основе решения оптимизационных задач нелинейного программирования.

На защиту выносятсяследующие результаты работы:

- вероятностные модели троянских атак на компьютерную систему из одного и нескольких источников на основе показательного распределения;

- риск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников;

- уравнения движения рисков атакуемой компьютерной системы относительно его параметров;

- алгоритм управления рисками атакуемой компьютерной системы, основанный на решении оптимизационных задач нелинейного программирования.

Практическая ценность.Практическая ценность полученных в ходе исследования результатов обусловлена тем, что построенные в настоящей работе риск-модели компьютерной системы, подвергающейся троянским атакам, и разработанный алгоритм управления рисками применимы на практике для количественного анализа информационных рисков и оптимального управления ими в условиях информационного конфликта.

Публикации.По материалам данной дипломной работы представлены к опубликованию в журнале «Информация и безопасность» две статьи на следующие темы: «Обзор и исследование троянских программ в контексте оценки их опасности для информационно-телекоммуникационных систем на основе статистического риск-анализа» и «Описание динамики рисков информационно-телекоммуникационных систем, подвергающихся троянским атака».

Структура и объем работы.Работа состоит из введения, шести глав, заключения и списка литературы, включающего 119 наименования.

Содержание работы изложено на 157 страницах машинописного текста, проиллюстрировано 39 рисунками и 17 таблицами.

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

Заключение

В дипломной работе получены следующие основные результаты:

1. Рассмотрены подходы к определению и классификация троянских программ, способы их проникновения на компьютеры пользователей, а также их структура. Для дальнейшего исследования среди троянских программ был выделен подкласс Backdoor, составляющий немногим менее трети всего класса (29,63%), так как представители данного подкласса обладают наибольшей функциональностью и являются наиболее изощренными и развитыми средствами информационного воздействия внутри рассматриваемого класса.

2. На основе показательного распределения разработаны и исследованы вероятностные модели троянских атак на компьютерную систему, из одного и нескольких источников.

3. Разработаны и исследованы с позиций теории чувствительности риск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников. Процесс распределенной троянской атаки на компьютерную систему рассматривался в контексте рассылки с помощью ботнетовспам-писемс вложенными троянскими программами подкласса Backdoor на внутренний почтовый сервер системы. Были получены аналитические выражения функций чувствительности рисков компьютерной системы к изменению параметров троянских атак. В результате расчетов был сделан вывод, что нахождение аналитических выражений функций чувствительности рисков к изменению параметров троянских атак является ключевым моментом в процессе риск-анализа, и последующего нахожденияуравнений движения рисков. С помощью уравнений движения рисковбыло проанализировано влияние параметров вероятностных моделей распределенной и нераспределенной троянских атак на функции рисков компьютерной системы.

4.Разработан алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников, основанный

на решении оптимизационных задач нелинейного программирования с ограничениями в виде неравенств.

5. Произведены оценка экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования. Расчеты показали, что данная работа является экономически эффективной (эффективность $E = 0,793$), а договорная цена работы составила220549,22 рублей.

6.Исследуемая проблематикабыла рассмотрена в контексте обеспечения безопасности жизнедеятельности. В результате был сделан вывод, что разработанная в данной работе методика оценки и управления информационными рисками компьютерной системы, подвергающейся троянским атакам, вреда для окружающей среды не представляет.

Таким образом, все поставленные задачи были решены полностью и цель дипломной работы достигнута.

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.

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

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

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

7 Щербаков Как писать вирусы / 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», Выпуск 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», Выпуск 4. – Воронеж: ВГТУ, 1999. - с.66-67.

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

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, том 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, том 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, том 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 MSDOS / 1990. - 450 с.

22Лефевр 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 МельниковВ. 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 MSDOS. –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 аперля 2001 г., том 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 г.

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.

48Кононов 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. – 52-56 с. – № 3. – 23-31 с.

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

52Остапенко 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.

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

56 Статьев В.Ю., Шарков А.Е. Проблемы защиты корпоративной ин формационной системы в процессе ее интеграции в сети общего пользования // Сборник материалов 5-й Всероссийской конференции «Информационная безопасность России в условиях глобально го 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 IEEE802.11 на основе использования теории нечетких множеств и нечеткой логики / В.Б. Щербаков, С.А. Ермаков, Д.А. Андреев // Информация и безопасность: научный журнал, том 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, том 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, том 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, том 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, том 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, том 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. – 400с.

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

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 №4. 1999.

74Хейес-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, том 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, том 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 ХоффманЛ.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. – 42-45 с.

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. – 44-46 с.

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

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. 31-35 с.

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 г.

106Розенвассер 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.

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