Содержание

ВВЕДЕНИЕ

Актуальность

Проблема информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных[72, 106, 113, 61].На любом, даже самом маленьком предприятии, присутствуют средства вычислительной техники, используемые для обработки информации. Нарушение целостности, уничтожение или хищение данных, приводит к причинению ущерба различной степени для организации, что приводит к экономическим убыткам[94, 97, 128]. А если учесть тот факт, что вредоносные программы развиваются параллельно с всеобщей информатизацией, защита автоматизированных систем должна рассматриваться как необходимая мера безопасности [2, 9, 24, 41].

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационными рисками [39, 90]. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий.При неправильном расчете рисков организации есть вероятность понести огромный ущерб, как количественный (потеря прибыли), так и качественный (потеря доверия к организации)[98, 15, 28].

Среди всего многообразия вредоносных программ, выделяется большой класс троянских вирусов. Среди них есть подклассTrojan-Ransom, которому до сих пор уделяется мало внимания, но который способен заблокировать работу операционной системы, несмотря на установленные на ней антивирусные программы. Исследуемый подкласс Trojan-Ransom впервые появился в 2010 году и с тех пор активно развивался.

Троянскими программами (троянскими конями) обычно называют программы, содержащие скрытый модуль, осуществляющий несанкционированные действия.

Эти действия не обязательно могут быть разрушительными, однако практически всегда направлены во вред пользователю[14, 23, 71, 119, 121].

В настоящее время были изучены: вопросы воздействия троянов на АС (дипломные работы Рудакова Е.В и Тонких Н К); вопросы применимости степенного закона распределения для оценки рисков АС; вопросы противодействия вирусным атакам; вопросы проникновения Trojan-Ransomв АС.

В изученных источниках литературы по проблематике не исследованы: вопросы оценки ущербов программ Trojan-Ransom; вопросы построения адекватной математической модели риск-анализа АС при воздействии этого вируса; вопросы минимизации ущерба от воздействия Trojan-Ransom; вопросы оценки экономической эффективности мер информационной защиты от программ Trojan-Ransom.

В дипломной работе проведен риск-анализ автоматизированной системы при воздействии на нее Trojan-Ransom.

Одна из разновидностей троянских программ – троянцы-вымогатели (Trojan-Ransom [23, 71, 119]) – вредоносное ПО, нарушающее работоспособность компьютера посредством полной или частичной блокировки операционной системы или шифрования файлов и вымогающее деньги у пользователей за их восстановление.

После заражения компьютера вредоносные программы Trojan-Ransom, в зависимости от функционала, блокируют доступ к веб-сайтам, шифруют на зараженном компьютере файлы определенных форматов или полностью блокируют доступ к системе[119, 121].

Широкое распространение вирусы-вымогатели получили зимой 2009—2010 года, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета[119]. Второй всплеск активности такого вредоносного ПО пришелся на май 2010 года[22].

В связи с этим анализ программ Trojan-Ransom является в настоящее время актуальным. В дипломном проекте рассматриваются вопросы, связанные с

особенностями функционирования и реализации деструктивных функций программ Trojan-Ransom.

Цель работы построение вероятностной модели воздействия троянских атак Trojan-Ransomна автоматизированные системы, а также разработка алгоритма оценки и управления возникающими в данном случае информационными рисками автоматизированной системы.

Для достижения поставленной цели в дипломной работе необходимо решить следующие задачи:

1. Рассмотреть различные модификации исследуемой «Троянской программыTrojan-Ransom» и способы их проникновения в автоматизированную систему.
2. Разработать вероятностные модели ущербов от воздействия троянской программы на автоматизированную систему.
3. Разработать алгоритм минимизации рисков при воздействии программ Trojan-Ransom
4. Произвести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;
5. Рассмотреть исследуемую проблематику с точки зрения обеспечения безопасности жизнедеятельности.

Объектом исследования являетсяавтоматизированная система, подвергающаяся троянским атакам.

Предметом исследования является статистический риск-анализ деструктивных воздействий троянских атак Trojan-Ransom, а так же организационные меры противодействия им.

Методы исследования

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

Апробация работы. Результаты проведенных исследований обсуждались на 32-ой научно-технической конференции профессорско-преподавательского состава, сотрудников и аспирантов ВГТУ «Вероятностная модель несанкционированного перехвата управления объектом информатизации вирусом Trojan.Ransom.Win32 Владимиров И.В., Москалева Е.А., Муродшоев А.О» (Воронеж, 2012).

На защиту выносятся следующие основные положения работы:

1. Обоснование применимости аппроксимации ущерба, наносимого компонентам автоматизированной системы программойTrojan.Ransom, степенным распределением.
2. Вероятностные риск-модели ущербов от программTrojan.Ransomдля компонент автоматизированных систем, основанных настепенномраспределении.
3. Алгоритм минимизации рисков автоматизированных систем, подвергающихся деструктивному воздействию программ Trojan-Ransom.
4. Оценка экономической эффективности вероятностной риск-модели ущербов от троянских программ Trojan.Ransom.

Полученные результаты и их новизна:

1. Обоснование применимости аппроксимации ущерба,наносимого компонентам автоматизированной системы,отличается тем, что для моделирования деструктивного воздействия программ Trojan.Ransom, было выбрано степенное распределение.
2. Вероятностные риск-моделиущербов от программы Trojan-Ransomдля компонент автоматизированных системотличаются тем, что в основу математической модели была положена интегральная оценка риска ущерба компонентам автоматизированной системы, аппроксимированной степенным распределением.
3. Алгоритм минимизации рисков автоматизированных систем отличается тем, что разработан для управления рисками при воздействии на нее троянских программ Trojan-Ransomна основе предложенной вероятностной модели.
4. Оценка экономической эффективности вероятностной модели ущербов АС отличается тем, что проведена оценка экономической эффективности , расчет

сметной стоимости и договорной цены риск-модели ущербов от программ Trojan-Ransom.

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

projectIT

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

projectIT

ЗАКЛЮЧЕНИЕ

1. На основе проведенных в дипломной работе исследований разработана вероятностная модель ущербов при воздействии программы Trojan.Ransom, позволяющая представить закономерности функционирования «трояна», и алгоритм минимизации рисков, позволяющий количественно оценить ущерб от деструктивного воздействия на автоматизированную систему.

2. В ходе работы выдвинута оригинальная научная гипотеза интегральной оценки ущерба на основе рассмотрения двух вариантов атак: синхронного и асинхронного.

3. В дипломной работе доказана перспективность предлагаемых идей для практического применения. Как показано в ходе исследования, применения изложенного алгоритма минимизации позволит повысить экономическую эффективность.

4. В ходе исследования было уточнено понятие интегральной оценки риска.

5. При проведении исследовании было доказано положениео применимости степенного распределения для моделирования воздействия троянской программы и расширены границы применимости вероятностной модели, основанной на степенном распределении, на область исследований программ Trojan.Ransom.

6. Эффективно использован метод теории вероятности, математической статистики, управления рисками: получена вероятностная модель ущербов и алгоритм минимизации рисков при воздействии программ Trojan.Ransom.

7. В дипломной работе изложены положения теории математической статистики о получении статистических характеристики случайных величин, теория вероятности, теория оценки рисков и экономическая теория.

8. В ходе исследований выявлено противоречие между интенсивным ростом количества модификаций программы Trojan.Ransom и отсутствием информированности персонала, обслуживающего автоматизированную систему, об угрозе, представляемой вирусом Trojan.Ransom, и необходимых мерах защиты от атак программ этого класса.

9. Изучены связи программ Trojan.Ransom с другими троянами и способы их доставки посредством других вирусных программ при рассмотрении вопросов, связанных с особенностями их функционирования.

10. Проведена модернизация вероятностной модели на степенном распределении, в виде обобщения на случай моделирования процесса деструктивного воздействия Trojan.Ransom на автоматизированную систему.

11. Результаты были внедрены при проведении мероприятий ИБ в фирме ООО «Объем-Сервис».

12. Были оценены границы эффективности использования результатов работы для практического применения. В экономической части диплома просчитана упущенная выгода от деструктивного воздействия программы Trojan.Ransom.

13. В результате проведения исследования представлено методическое обеспечение для регулировки рисков проникновения в автоматизированную систему троянской программы Trojan.Ransom.

14. Достоверность проведенных исследований подтверждается согласованностью эмпирических и теоретических данных.

15. Идея работы была почерпнута из анализа большого количества изученного материала (статей в научном журнале, газетах, Интернет-новостях), а также личного опыта восстановления ОС после атак Trojan.Ransom.

16. Полученные в работе расчетные данные совпали с полученными ранее эмпирическими, что подтверждено оценкой ошибок моделирования по критерию Неймана-Пирсона.

17. Использованы современные методики сбора и обработки данных: результаты исследований ведущих фирм-разработчиков антивирусных средств (Dr.Web, Касперский Антивирус, NOD 32, Panda), редакторы MSExcel, MSPowerPointи MSWord.

18. Личный вклад заключается в сборе информации по исследуемой проблематики, проведении апробации результатов исследования, проведения имитационного моделирования, выборе математического аппарата исследования, разработке алгоритма минимизации рисков автоматизированной системы при

воздействии программ Trojan.Ransom, оценки экономической эффективности предлагаемого алгоритма.

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

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

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

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

Список литературы

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

2. Айков, Д. Компьютерные преступления = ComputerCrime:ACrimefighter'sHandbook :Рук.по борьбе с компьютерными преступлениями:Пер.с англ. / Д. Айков ; Д.Айков,К.Сейгер,У.Фонсторх. - М. : Мир, 1999. - 351с. - (Компьютерная безопасность). - ISBN 5-03-003312-2

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

4. 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.

5. Анин, Б.Ю. Защита компьютерной информации / Б. Ю. Анин. - СПб. : BHV, 2000. - 384с. - ISBN 5-8206-0104-1

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

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

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

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

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

11. 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.

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

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

14. Безруков Н.Н. Компьютерная вирусология. Киев: УРЕ, 1991. - 88 с.

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

16. Бэнкс М.А. Информационная защита ПК : Пер. с англ. / М. А. Бэнкс ; Под ред. А.В.Легейды, А.Л.Самотовки. - Киев [и др.] : Век+ [и др.], 2001. - 269с. + 1 CD-ROM. - ISBN 966-7140-18-0

17. Вадзинский Р.Н. Справочник по вероятностным распределениям. - СПб.: Наука, 2001. - 295 с., ил.116.

18. Вентцель Е.С. Введение в исследование операций. - М.: Советское радио, 1964.

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

20. 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.

21. Википедия - свободная энциклопедия - Электрон.дан. - Режим доступа: http //ru.wikipedia.org.

22. Википедия / http://ru.wikipedia.org/wiki/Trojan.Winlock

23. Википедия / http://ru.wikipedia.org/wiki/Троянская_программа

24. Галатенко В. Информационная безопасность - обзор основных положений. - Открытые системы, 1996. - С. 42-45.

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

26. Глоссарий по вирусным базам http://www.securelist.com/ru/descriptions/30086759/Trojan-Ransom.Win32.DoubleEagle.ez

27. Глоссарий по вируснымбазамhttp://www.securelist.com/ru/descriptions/17434217/Trojan-Ransom.Win32.Gimemo.ns

28. 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.

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

30. Гордон Я. Компьютерные вирусы без секретов / Я. Гордон. - М. : Новый изд. дом, 2004. - 319 с. - ISBN 5-9643-0044-8

31. 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.

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

33. 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.

34. 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.

35. 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.

36. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. - М. [и др.] :DiaSoft, 2002. - 671с. - ISBN 966-7992-02-0

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

38. Журнал IT-сектор http://it-sektor.ru/troyan-ili-troyanskiyi-kon.html

39. Завгородний, В.И. Комплексная защита информации в компьютерных системах : учеб.пособие для вузов / В. И. Завгородний. - М. : Логос, 2001. - 262с. - ISBN 5-94010-088-0 :

40. Зангвилл У. Нелинейное программирование. Единый подход: пер. с. англ. / У. Зангвилл - М.: "Сов. Радио", 1973. - 312 с.

41. Зегжда, Д.П. Основы безопасности информационных систем : учеб.пособие для вузов / Д. П. Зегжда, А. М. Ивашко. - М. : Телеком, 2000. - 449с.:ил. - ISBN 5-93517-018-3

42. 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.

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

44. Информационный портал по безопасности SecurityLab.ru.- Электрон.дан. - Режим доступа: http //www.securitylab.ru.

45. 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.

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

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

48. 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.

49. Коэн Ф. Компьютерные вирусы - теория и эксперименты http://www.nf-team.org/drmad/stuff/cohen.htm

50. 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.

51. Курушин, В.Д. Компьютерные преступления и информационная безопасность : Справ. / В. Д. Курушин, В. А. Минаев. - М. : Новый Юрист, 1998. - 256с. - ISBN 5-7969-0022-6

52. 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.

53. 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.

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

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

56. Лысенко А.Г. Расчет рисков нарушений информационной безопасности в сетях с мобильными сегментами / А.Г. Лысенко. Пробл. инф. безопас. компьютер.системы - 2007. - №2 - 104 с.

57. Лысенко А.Г. Расчет рисков нарушений информационной безопасности в сетях с мобильными сегментами / А.Г. Лысенко. Пробл. инф. безопас. компьютер.системы - 2007. - №2 - 104 с.

58. Мазуров В.А. Компьютерные преступления : Классификация и способы противодействия: Учеб.-практ. пособие / В. А. Мазуров. - М. : Палеотип: Логос, 2002. - 147 с. - Мегапроект "Пушкинская б-ка". - ISBN 5-94727-017-X

59. Майерс Д., Социальная психология, С.-Пб., 2002, 560 с.

60. Майерс Д., Социальная психология, С.-Пб., 2002, 560 с.

61. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии. Информационные технологии и вычислительные системы - Электрон.дан. - Режим доступа: http://www.sbiblio.com/biblio/archive/malineckiy_scenarii/

62. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии. Информационные технологии и вычислительные системы - Электрон.дан. - Режим доступа: http://www.sbiblio.com/biblio/archive/malineckiy_scenarii/

63. Малюк, А.А. Введение в защиту информации в автоматизированных системах : учеб.пособие для вузов / А. А. Малюк ; А.А.Малюк, С.В.Пазизин, Н.С.Погожин. - М. : Горячая линия-Телеком, 2001. - 144с. - (Специальность). - ISBN 5-03517-062-0 : 49р.50к. - ISBN 5-7873-0040-8

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

65. Мамаев, М. Технологии защиты информации в Интернете : Спец. справ. / М. Мамаев, С. Петренко. - СПб. [и др.] : Питер, 2002. - 844с. - (Справочник). - ISBN 5-318-00244-7

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

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

68. Мельников В.В. Безопасность информации в автоматизированных системах / В. В. Мельников. - М. : Финансы и статистика, 2003. - 367 с. - ISBN 5-279-02560-7

69. Мельников В.В. Безопасность информации в автоматизированных системах. - Издательство Финансы и статистика, 2003. - 368 с.

70. Мельников В.В. Безопасность информации в автоматизированных системах. - Издательство Финансы и статистика, 2003. - 368 с.

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

72. 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.

73. Мотузко Ф.Я. Охрана труда / Ф.Я. Мотузко. - М.: Высшая школа, 1989.- 336 с.

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

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

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

77. Осмоловский С.А. Стохастические методы защиты информации. - Издательство Радио и связь, 2004. - 320 с.

78. Осмоловский С.А. Стохастические методы защиты информации. - Издательство Радио и связь, 2004. - 320 с.

79. Основы информационной безопасности / Под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: ВИ МВД, 2000. - 464 с.

80. Основы информационной безопасности / Под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: ВИ МВД, 2000. - 464 с.

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

82. 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.

83. 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.

84. 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.

85. Остапенко Г.А., Информационные операции и атаки в социотехнических системах: учебное пособие/ Г.А. Остапенко - Воронеж, ВГТУ, 2005. - 202с.

86. Остапенко Г.А., Информационные операции и атаки в социотехнических системах: учебное пособие/ Г.А. Остапенко - Воронеж, ВГТУ, 2005. - 202с.

87. Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Транин В.А. Риски распределенных систем: методики и алгоритмы, оценки и управление. //Информация и безопасность: Регион.науч.-техн. журнал. - Воронеж. 2010. Вып. 4. с. 485-531.

88. Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Транин В.А. Риски распределенных систем: методики и алгоритмы, оценки и управление. //Информация и безопасность: Регион.науч.-техн. журнал. - Воронеж. 2010. Вып. 4. с. 485-531.

89. 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.

90. Остапенко О.А. Риски систем: оценка и управление: учеб.пособие / О.А. Остапенко, Д.О. Карпеев, В.Н. Асеев; под ред. Ю.Н. Лаврухина. - Воронеж: ГОУВПО "ВГТУ", 2006. - 247 с.

91. Остапенко О.А. Риски систем: оценка и управление: учеб.пособие / О.А. Остапенко, Д.О. Карпеев, В.Н. Асеев; под ред. Ю.Н. Лаврухина. - Воронеж: ГОУВПО "ВГТУ", 2006. - 247 с.

92. Парфенов В.И. Защита информации. Словарь. - Воронеж: Издательство им. Е.А. Болховитинова, 2001. - 292 с

93. 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.

94. Петренко С.А. Управление информационными рисками : Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. - М. : Академия АйТи : ДМК Пресс, 2005. - 381 с. - (Информационные технологии для инженеров). - ISBN 5-98453-001-5 (АйТи)

95. Понтрягин Л.С. Обыкновенные дифференциальные уравнения // М.: Физматгиз, 1961. - 331 с.

96. 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.

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

98. Риски и шансы: оценка и управление./ Под редакцией А.Г. Остапенко - М: Горячая линия - Телеком, 2010. - 125 с.: ил.

99. Розанов В.Н. Системный анализ для инженеров. - СПб.: СпбГУ, 1998.

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

101. Розенвассер Е.Н. Методы теории чувствительности в автоматическом управлении / Е.Н. Розенвассер, Р.М. Юсупов. - Л.: "Энергия", 1971. - 260 с.

102. 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.

103. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. - Изд. 2-е, перераб. и доп. - М. : Радио и связь, 2001. - 375 с. - ISBN 5-256-01518-4

104. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; Под ред. В.Ф.Шаньгина. - М. : Радио и связь, 1999. - 328с. - ISBN 5-256-01436-6

105. Самгин Э.Б. Освещение рабочих мест. - М.: МИРЭА, 1989. - 186 с.

106. 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.

107. 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.

108. 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.

109. 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.

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

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

112. Соколов, А.В. Методы информационной защиты объектов и компьютерных сетей / А. В. Соколов ; А.В.Соколов,О.М.Степанюк. - СПб. ; М. : Полигон:АСТ, 2000. - 269с. - (Шпион.штучки). - ISBN 5-89173-079-0

113. 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.

114. Технические методы и средства защиты информации / Ю.Н.Максимов, В.Г.Сонников, В.Г.Петров и др.; Под общ.ред. В.Г.Сонникова. - СПб. : Полигон, 2000. - 314с. - (Шпион.штучки). - ISBN 5-89173-096-0

115. 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.

116. 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.

117. 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.

118. 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.

119. Троянцы-вымогатели / http://www.securelist.com/ru/analysis/208050728/Troyantsy_vymogateli

120. 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.

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

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

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

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

126. 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.

127. 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.

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

129. Яглом А., Яглом И. Вероятность и информация. М.: Мир, 1985. - 110 с.

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

131. Protect lab - URL http://protectlab.com

132. SecureList / http://www.securelist.com/ru/glossary?glossid=152528302

133. SecureList / http://www.securelist.com/ru/threats/detect?chapter=118