Содержание

Введение.

Актуальность темы обусловлена стремлением людей защитить наиболее ценную информацию. Ценность информации в общем случае определить очень сложно, но есть практические случаи, когда ценность информации определяется свыше. Одним из таких важных случаев является информация, получаемая в ходе проектирования чего-то нового (вещи, плана, комплекса мероприятий). За такой информацией злоумышленник охотится в первую очередь, поэтому предметной основой указанной темы является процесс функционирования систем автоматизированного проектирования[2,7,13-19]. Компьютерную основу этой системы составляет локальная вычислительная сеть. Защищенность информации подвергается воздействию угроз создаваемых злоумышленником, поэтому процесс взаимодействия получения информации и воздействия угроз является принципиально конфликтным, то есть имеющий совершенно противоположные цели. Конфликт очень сложное явление и поэтому очень важно найти приемлемую математическую модель, которая более просто зафиксирует закономерности его ведения.[3,10,23]. Одной из конструктивных моделей является модель гибели и размножения, реализованная на Марковской цепи, на цепи состояний исследуемых процессов. Такая модель и принята за основу дипломной работы[11,45,46,53-56].

Математическая модель гибели и размножения была разработана биологами для исследования закономерности взаимосвязи (а не взаимодействия) хищника и жертвы[63,67]. Эта аналогия стала широко использоваться для анализа технических систем с противоположными свойствами. Применительно к защите информации рассматривается впервые (с учетом специфических свойств информационной системы)[1,26,72]. Для ограничения широты информационного представления используется в качестве объекта системы автоматизированного проектирования какого-либо изделия. Это сложная организационно техническая система по созданию (получению) новой информации.

Техническую основу систем автоматизированного проектирования составляет локальная вычислительная сеть различной мощности, она является кибернетическим помощником коллективу проектировщиков решающих задачи

различной сложности соответствующих содержанию идеи (завязки проекта)[35,38].

В ходе проектирования люди обмениваются полученными результатами, обращаются к источникам данных общего пользования, проверяют правильность полученных результатов экспериментально на моделирующих стендах. Все указанные процедуры подвержены воздействию злоумышленников различных рангов, способных уничтожить и исказить полученную информацию[86,87,100]. Тем самым мы имеем дело не только с «чистым хищником», стремящимся уничтожить, но и с косвенным, стремящимся исказить информацию.

Исходя из устройства локальной вычислительной сети систем автоматизированного проектирования, источником негативного воздействия на получаемые данные является: автоматизированные рабочие места, серверы данных и приложений, моделирующие стенды и каналы передачи данных, а так же значение интенсивности и вероятности негативных воздействий и включение их управления модели «гибели и размножения», учитывающих и штатные закономерности получения данных в системе автоматизированного проектирования[28,31].

Объектом исследования является локальная вычислительная сеть систем автоматизированного проектирования, учитывающая не только закономерности получения новых данных, но и процесс воздействия злоумышленника на них.

Предметом исследования выступает математическая модель, разработанная на основе теории «гибели и размножения».

Цель настоящей работы заключается в разработке и исследовании математической модели оценивания эффективности защиты информации в локальной вычислительной сети, обеспечивающей процесс проектирования нового объекта путем представления ее функций цепью Маркова в которой взаимодействуют два процесса: за сохранение добытой информации (процесс рождения) и ее уничтожение действиями злоумышленника (процесс гибели). Чувствительность модели к мероприятиям защиты, обеспечиваются разработкой

алгоритма направленной на уменьшение интенсивности процесса «гибели» информации.

Для достижения указанной цели предполагается решить ряд задач:

- Сформулировать постановку задачи применительно к типовой локальной вычислительной сети систем автоматизированного проектирования.
- Систематизировать виды угрозинформационной безопасности наиболее опасных для локальной вычислительной сетисистем автоматизированного проектирования;
- Разработка математической модели на основе «гибели и размножения» введя в нее коррективы учитывающие специфику воздействия угроз отличных от эффективности воздействия «хищника на жертву»;
- Оценить экономические показатели эффективности разработанной модели «гибели и размножения».

Новизна работы

- Определена структурная основа модели «размножения и гибели» информации в локальной вычислительной сети систем автоматизированного проектирования;
- Построена риск-модель, которая позволяет рассчитать риски для локальной вычислительной сети систем автоматизированного проектирования;
- Заключается в применении теории «гибели и размножения» к локальной вычислительной сети систем автоматизированного проектирования. В отличие от классических задач «жертва» (информация) у нас не дискретная, а непрерывная, но дискредитируемая техническими средствами ее создания.

На защиту выносится

- Описательная модель локальной вычислительной сети систем автоматизированного проектирования, как среды реализации информационных операций;

- Формализация потока угроз, расчет параметров риска для локальной вычислительной сети систем автоматизированного проектирования;
- Математическая модель «гибели и размножения» информации в локальной вычислительной сети систем автоматизированного проектирования, как инструмент оценивания ее защищенности от угроз информационной безопасности.

Практическая ценность

- Множество различных действий по созданию и уничтожению данных представляются двумя наглядными понятиями: «гибели и размножения», для взаимосвязи этих понятий разработаны обоснованные математические модели, обладающие большой предметной общностью;
- Разработанная в работе риск-модель позволяет рассчитать риски для локальной вычислительной сети систем автоматизированного проектирования, на которую воздействуютс помощью атак, направленных на «гибель» информации;
- Представленная обобщенная модель локальной вычислительной сети систем автоматизированного проектирования может послужить теоретической основой для ее создания в режиме реального масштаба времени, в условиях ограниченности ресурсов.

Заключение

В дипломной работе получены следующие результаты:

1. Описан процесс функционирования локальной вычислительной сети систем автоматизированного проектирования, как средства получения и обработки данных, необходимых для принятия решения. Описаны информационные процессы на каждом из этапов подготовки и принятия решения, показана последовательность обработки информации, необходимой для принятия решения, с помощью технических средств.

2. Рассмотрен состав угроз информационной безопасности, которые могут воздействовать на локальную вычислительную сеть САПР на различных этапах его функционирования. Построена и описана математическая модель формализации потока угроз на ЛВС систем автоматизированного проектирования в соответствии с заданными параметрами системы. Так же построена модель оценивания защищенности локальной вычислительной сети систем автоматизированного проектирования.

3. Представлена вероятностная модель связи процессов, «рождения» и «гибели» информации в локальной вычислительной сети САПР. Разработана методика оценивания опасностей угроз информационной безопасности в локальной вычислительной сети систем автоматизированного проектирования на основании «гибели и размножения».

4. Проведена оценка экономических показателей эффективности разработанной математической модели защиты информации в локальной вычислительной сети систем автоматизированного проектирования на основе математической модели «гибели и размножения».

5. Данная тема была рассмотрена в контексте обеспечения безопасности жизнедеятельности.

Список используемой литературы

1 Авен О.И. Оценка качества и оптимизация вычислительных систем / Гурин Н.Н.. Коган Я.А. – М.: Наука, 1982. – 464 с.

2 Александров Е.А. Основы теории эвристических решений / Е.А. Александров.— М: Советское радио, 1975. — 256 с.

3 Ахо А. Построение и анализ вычислительных алгоритмов / Хопкрофт Дж., Ульман Дж. - М.: Мир, 1979. - 536 с.

4 Баруча-Рид А. Т. Элементы теории марковских процессов и их приложения. М., «Наука», 1969. - 511 с.

5 Баранов А.П. Теоретические основы информационной безопасности (дополнительные главы). Учебное пособие. / Зегжда Д.П., Зегжда П.Д., Ивашко А.М., Корт С.С.– СПб.: Санкт-Петербургский государственный технический университет, 1998. С. 87-128.

6 Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / Михальский О.О., Першаков А.С. и др. - М.: Радио и связь, 1999. - 168 с.

7 Бергхаузер Т. Система автоматизированного проектирования AutoCAD:Справочник:Пер.с англ. / Шлив П. – М.:Радио и связь, 1989. –256 с.

8 Бочаров П.П. Теория массового обслуживания / Печинкин А.В. — М.: РУДН, 1995. — С. 530.

9 Будя А. П. Справочник по САПР / Кононюк А. Е., Куценко Г. П. и др.; под ред. Скурихина В. –К.: Тэхника, 1988. -375 с.

10 Василевский И.В. Найти и обезвредить. Техника защиты информации // Система безопасности. - 1995. - №6. - С. 11-15.

11 Вихорев С. Практические рекомендации по информационной безопасности / Ефимов А. // Jet Info, № 10-11, 1996.

12 Венецкий И.Г.Основные математико-статистические понятия и формулы в экономическом анализе / Венецкая В.И.- М.:Статист.,1979.–284 с.

13 Вентцель Е. С. Исследование операций - М., «Советское радио», 1972. -552 с.

14 Вентцель Е.С. Теория вероятностей: учеб. для втузов / Е.С. Вентцель – М.: Высш. шк, 1998. – 576 с.

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

16 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения /Овчаров Л.А.– М: Издательский центр «Академия»,2003.–432 с.

17 Волков И. К. Случайные процессы / Зуев С. М., Цветкова Г. М. 1999. - 448 с.

18 Волеводз А.Г. Противодействие компьютерным преступлениям / А.Г. Волеводз. — М.: Юрлитинформ, 2002. —496 с.

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

20 Гнеденко В.Б. Математические методы теории надежности / Беляев Б.К., Соловьев А.Д. -М.: Наука.-1969.-623 с.

21 Герасименко В.А. Системно-концептуальный подход к защите информации в современных системах ее обработки/ Герасименко В.А., Малюк А.А., Погожин Н.С. // Безопасность информационных технологий. 1995, №3, С. 46 - 64.

22 Гейн А.Г. Основы информатики и вычислительной техники. 3-е изд / Житомирский В.Г. – М.: Просвещение, 1993. – 254 с.

23 Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика.- М.: Наука. Физматлит, 1999. – 216 с.

24 Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: учеб. пособие / В.М. Гранатуров. – М.: Дело и Сервис, 1999. – 112 с.

25 Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. Кн.1. – 400 с.

26 Грушо А.А. Теоретические основы защиты информации / А.А. Гру-шо, Е.Е. Тимонина.— М.: Яхтсмен, 1966. — 192 с.

27 Гузик С. Управление и аудит информационных технологий. Особенности проведения внешнего аудита // Jet Info, №1. - М.,2003.-С.3-24

28 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – 12-е изд., стереотип. – М.: Высшая школа, 2005. – 479 с.

29 Гусева А. И. Работа в локальных сетях Novell NetWare 3.11 - 4.12. - М.: Диалог - МИФИ,1997г., 234 с.

30 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты /В.В.Домарев -Киев:ООО ТИД ДС 2001.- 688 с.

31 Домарев В.В. Защита информации и безопасность компьютерных систем. Киев: Изд. «Диасофт», 1999 – 104 с.

32 Демидович Б.П. Краткий курс высшей математики: Учеб. пособие для вузов / Кудрявцев В.А. - М.: Астрель,2003. - 656 с.

33 Емельянов В. В., Курейчик В. М., Курейчик В. В. Теория и практика эволюционного моделирования. — М.: Физматлит, 2003. — 432 с.

34 Епанешников А.М. Локальные вычислительные сети / Епанешников В.А. — Санкт-Петербург, Диалог-МИФИ, 2005 г.- 224 с.

35 Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. — М.: Горячая линия Телеком, 2000.—452 с.

36 Злобина И.А. Экономика информационной безопасности / И.А. Злобина. – Воронеж: ВГТУ, 2005. – 196 с.

37 Зыков А.А Теория конечных графов - Новосибирск: Наука, 1969. - 206 с.

38 Кельтон В. Имитационное моделирование. Классика CS. 3-е изд / Лоу А. – СПб.: Питер; Киев: Издательская группа BHV, 2004. – 847 с.

39 Клейнрок Л. Теория массового обслуживания — М.: Машиностроение, 1979. — С. 432.

40 Комени Дж. Конечные цепи Маркова / Снелл Дж. – М.: Наука, 1982. – 320 с.

41 Корн Г. Справочник по математичке для научных работников и инженеров. – М.: Наука, 1977. – 832 с.

42 Козлов В.А. Открытые информационные системы / В.А. Козлов.— М.: Финансы и статистика, 1999. — 224 с.

43 Климанов В. П. Методы разработки аналитических моделей для анализа многоканальных вычислительных сетей, используемых в управлении технологическими процессами. М.- МЭИ. 1995. - 115 с.

44 Кузовлев В.И. Разработка САПР. Математические методы анализа производительности и надежности САПР / Шкатов П.Н. – М.: Высшая школа, 1990. – 144 с.

45 Лаврухин Ю.Н. Проблемы технической защиты конфиденциальной информации. / Лаврухин Ю.Н. // Информация и безопасность: Материалы межрегиональной научно-практической конференции. Вып. 2. - Воронеж: ВГТУ, 2002, С. 14- 16.

46 Ли К. Основы САПР (CAD/CAM/CAE).–СПб.:Питер, 2004.–560 с.

47 Липаев В.В., Колин К.К., Серебровский Л.А. Математическое обеспечение управляющих ЭВМ. – М.: Советское радио, 1972. – 528 с.

48 Лукацкий А.В. Средства анализа защищенности. - Мир Internet. 1999, № 3, С. 16.

49 Макконнелл Дж.. Основы современных алгоритмов. 2-е дополненное издание Москва: Техносфера, 2004. – 368 с.

50 Мозгалевский А. Системотехника: методы и приложения / В.Николаев В. И., Брук В. М.— Л.: Машиносроение, Ленингр. отд-ние, 1985.— 199 с.

51 Меерович Г. А. Эффект больших систем. - М.:Знание,1985.—192 с.

52 Натан А. А. Случайные процессы: Учебное пособие. – М.: МФТИ, 1978. – 118 с.

53 Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004. – 122 с.

54 Осовецкий Л. Построение средств межсетевой защиты информации / Л. Осовецкий. — М.: НТЦ «Критические информационные технологии», 1997.— 300 с.

55 Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин.// Информация и безопасность. Регион, науч. - техн. журнал. Воронеж, 2005, вып.2, С.70-75.

56 Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В. Риски распределенных систем: методики и алгоритмы оценки и управления // Информация и безопасность, 2010. - №4. – С. 485-530.

57 Парфенов В.И. Защита информации (Словарь). – Воронеж: НП РЦИБ "Факел", 2003. – 293 с.

58 Пивоварова Н.В., Трудоношин В.А. Системы автоматизированного проектирования. Математические модели технических объектов. – М.: Высшая школа, 1986. – 160 с.

59 Поллард Дж. Справочник по вычислительным методам статистики. - М.: Финансы и статистика, 1982. -575 с.

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

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

58. Прохоров А.В. Задачи по теории вероятностей. Основные понятия. Предельные теоремы. Случайные процессы / Ушаков В.Г., Ушаков Н.Г. – М.: Наука, 1986. – 328 с.

59. Поспелова Д.А. Нечеткие множества в моделях управления и искусственного интеллекта //Под ред. Д.А. Поспелова. М., 1986. – 263 с.

60. Расторгуев СП. Программные методы защиты информации в компьютерах и сетях / СП. Расторгуев. — М.: Яхтсмен, 1993. — 188 с.

61. Розанов Ю.А. Введение в теорию случайных процессов. – М.: Наука, 1979. – 984 с.

62. Симонов С. В. Методология анализа рисков в информационных системах. Конфидент, 2001, № 1, С. 72-76.

63. Сердюк В. Системы обнаружения компьютерных атак и их роль в защите информационных сетей. BYTE/Россия.2000, С. 28-31.

64. Смирнов Н.В. Курс теории вероятностей и математической статистики для технических приложений / Н.В. Смирнов, И.В. Дунин-Барковский. – М.: Наука, 1969. – 512 с.

65. Спесивцев А. В. Защита информации в персональных ЭВМ / Вегнер В.А., Крутяков А.Ю. - М.: Радио и связь, 1992.-200 с.

66. Стенг Д. Секреты безопасности сетей. / Мун С. Киев: Диалектика», 1995. - 100 с.

67. Степаненко А.А. Организация защиты информации в корпоративной сети. Системы безопасности, связи и телекоммуникаций. 1998, №4, С. 4-8.

68. Степанов Е.А. Предпосылки защиты и механизм утечки конфиденциальной информации // Секретарское дело. 1998, №1, С.8-12.

69. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюкова. – М.: МЦНМО, 2002. – 146 с.

70. Соколов А. В. Методы информационной защиты объектов и компьютерных сетей / Степанюк О. М. — СПб.: Полигон, 2000. — 272 с.

71. Спесивцев А.В. Защита информации в персональных ЭВМ. – М.: Радио и связь, 1992. – 190 с.

72. Таненбаум Э. Компьютерные сети. -С-Пб.: Питер, 2002 -848 с.

73. Тимофеев П.А. Принцип защиты информации в компьютерных системах // «Защита информации. Конфидент». – 1998, №3. – С. 72-76.

74. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности. – М.: Гелиос АРВ, 2005. – 960 с.

75. Томас Л. С. Математические модели конфликтных ситуаций.- М.: Сов. радио, 1977. – 145 с.

76. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». М.: СИНТЕГ, 2000. – 559 с.

77. Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1995. - 300 с.

78. Флинт Д. Локальные сети ЭВМ: архитектура, принципы построения, реализация. –М.: Финансы и статистика, 1986. 359 с.

79. Флейшман Б.С. Элементы теории потенциальной эффективности сложных систем. М.: Советское радио, 1971. — 224 с.

80. Халяпин Д. Б. Основы защиты информации / Ярочкин В. И. М.: 1ЛТКИР, 1994. - 127 с.

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

82. Хокс Б. Автоматизированное проектирование и производство: Пер. с англ. — М.: Мир, 1991. — 296 с.

83. Хорев А.А. Защита информации. Технические каналы утечки информации. -М.: ГТК, 1998. - 320 с.

84. Хофман Л. Д. Современные методы зашиты информации. М—: Сов. Радио, 1980. - 264 с.

85. Черняк Ю.И. Системный анализ в управлении экономикой / Ю.И. Черняк. – М.: Экономика, 1975. – 393 с.

86. Чопоров О.Н. Система поддержки информационной безопасности и менеджмента / О.Н. Чопоров, Л.Г. Попова // Информация и безопасность: Региональный научный вестник. - Воронеж: ВГТУ, 2002. - Вып.1, С.40 - 42.

87. Шиверский А.А. Защита информации: проблемы теории и практики. - М.: Юрист, 1996. - 112 с.

88. Шварц М. Сети ЭВМ. Анализ и проектирование: Пер. с англ./ Под ред. В.А.Жожикашвили. – М.: Радио и связь, 1981. – 336 с.

89. Шелупанов А.А. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений / Скрыль С.В. – М.: Машиностроение, 2008. – 138 с.

90. Щербаков А.Ю. Введение в компьютерную безопасность / А.Ю. Щербаков. — М.: Издательство СВ. Молгачева, 2001. — 352 с.

91. Щеглов А.Ю. Круговая оборона. Сети и системы связи / Тарасюк М.В. 1999, №3, С.44-47.

92. Юрочкин А.Г. Применение экспертных систем для обнаружения атак на вычислительную сеть / А.Г. Юрочкин, А.В. Колычев, Д.Е. Морев // Информация и безопасность: Региональный научный вестник. — Воронеж: ВГТУ, 2000. — Вып.1. — С.92 — 93.

93. Яни С. А. Компьютеры и преступность / Черных А.В. - Социалистическая законность, 1989, № 6, с. 66.

94. Ярочкин И. В. Безопасность информационных систем. – М.: Ось-89, 1996.– 240 с.

95. Ярочкин В. И. Технические каналы утечки информации. М.: ИПКИР, 1994. - 200 с.

96. Ярочкин В. И. Что приводит к неправомерному овладению конфиденциальной информацией / М.: Частный сыск и охрана, № 10. 1993. - С. 42-46.

97. Ярочкин В. И. Основы защиты информации. Служба безопасности предприятия / Халяпин Д. Б. - М.: ИПКИР, 1993.-100 с.

98. Ярочкин В.Н. Словарь терминов и определений по безопасности и защите информации / Шевцова Т.А. М, 1996. - 180 с.

99. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

100. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

101. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

102. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – М.: Изд-во стандартов, 1999.