Содержание

Введение 9

Глава 1 Выработка подходов к моделированию массовых рассылок электронной почты 9

1 1 1 Звуковые наркотики 20

1 1 2 Фишинг 20

1 1 3 Письма с вредоносными вложениями 21

1 2 Ущербы наносимые спамом 23

1 2 1 Нагрузка на коммуникации 23

1 2 2 Раздражение и недовольство 24

1 2 3 Криминализация спама 24

1 2 4 Ущерб пользователям 26

1 2 5 Ущерб бизнесу 27

1 2 6 Ущерб провайдерам 27

1 2 7 Ущерб государственным организациям 28

1 2 8 Ущерб обществу в целом 29

1 3 Анализ методов и технологий рассылки сообщений и борьбы с «антиспам» фильтрами 30

1 3 1 Технологические цепочки 30

1 3 1 1 Сбор и верификация списков адресов 30

1 3 1 2 Подготовка точек рассылки 32

1 3 1 3 Программное обеспечение для рассылки спама 34

1 3 1 4 Поиск клиентов 35

1 3 2 Приемы обхода спам-фильтров 37

1 4 Методики борьбы с нежелательными электронными сообщениями в телекоммуникационных сетях 38

1 4 1 Профилактика спама 38

1 4 2 Методы борьбы со спамом 39

1 4 2 1 Процедурные методы борьбы со спамом 39

1 4 2 2 Распределенные методы распознавания спама 47
1 4 2 2 1 Формальные методы 47
1 4 2 2 2 Лингвистические методы 51
1 5 Выбор и обоснование методов моделирования процессов распространения электронной почты 59
1 5 1 Модель распространения электронной почты 59
1 5 2 Модель входного потока сообщений 60
1 5 3 Модель почтового сервера 62
1 5 4 Реальная организация почтового сервера 62
1 6 Основные результаты первой главы 63
Глава 2 Построение математической модели массовых рассылок электронных сообщений 65
2 1 Основы математического моделирования 65
2 1 1 Требования предъявляемые к математическим моделям 67
2 1 2 Задачи математического моделирования 68
2 1 3 Составление математических моделей 68
2 2 Классификация математических моделей 69
2 2 1 Классификация по способу представления объекта 70
2 2 1 1 Структурные и функциональные модели 70
2 2 1 2 Содержательные и формальные модели 70
2 2 1 3 Статические и динамические модели 71
2 2 1 4 Непрерывные, дискретные и гибридные модели 72
2 2 1 5 Детерминированные и стохастические модели 73
2 1 1 6 Аналитические и имитационные модели 73
2 2 2 Методы построения аналитических моделей 74
2 3 Математическая модель системы массового обслуживания 75
2 4 Построение математических моделей телекоммуникационных сетей в виде СМО в условиях осуществления массовых рассылок сообщений 79
2 5 Выводы по второй главе 85
Глава 3 Риск-модели информационно-телекоммуникационных систем, атакуе-

мых спамом 87
3 1 Оценка вероятности наступления ущерба 87
3 1 1 Последовательная модель фильтрации сообщений 87
3 1 2 Параллельная модель фильтрации сообщений 88
3 1 3 Многоканальная модель фильтрации сообщений 90
3 1 4 N-одноканальных моделей фильтрации с отказами на обслуживание 91
3 2 Нахождение аналитических выражений и моментов риска 93
3 2 1 Многоканальная модель фильтрации сообщений с отказами на обслуживание 93
3 2 2 N-одноканальных моделей фильтрации сообщений с отказами на обслуживание 94
3 3 Построение динамических риск-моделей «спам-атаки» 95
3 3 1 Многоканальная модель фильтрации сообщений с отказами на обслуживание 96
3 3 2 N-одноканальных моделей фильтрации сообщений с отказами на обслуживание 99
3 4 Выводы по третьей главе 100
Глава 4 Управление защищенностью информационно-телекоммуникационных систем в условиях противодействия спаму 101
4 1 Выработка критериев качества управления риском 101
4 2 Алгоритмизация управления рисками атакуемых ИТКС 112
4 3 Выводы по четвертой главе 122
Глава 5 Организационно-экономическая часть 123
5 1 Формирование этапов и перечня работ по разработке алгоритмов управления защищенностью атакуемых информационно-телекоммуникационных систем 123
5 2 Определение трудоемкости процесса разработки математической модели подсистемы обнаружения и фильтрации нежелательной

корреспонденции 123

5 3 Разработка календарного плана проведения работ по разработке математических моделей 128

5 4 Расчет сметной стоимости и договорной цены научно-исследовательской работы математического моделирования массовых рассылок 135

5 5 Прогнозирование ожидаемого экономического эффекта от использования результатов работы 137

5 6 Расчет экономического ущерба вследствие реализации многократных атак на компьютерную систему 145

5 7 Выводы по пятой главе 147

6 Безопасность и экологичность 148

6 1 Идентификация вероятных поражающих, вредных и опасных факторов при работе операторов компьютерных систем 148

6 2 Защита от вероятных вредных и опасных факторов при работе операторов компьютерных систем 152

6 2 1 Проектирование оптимальной системы освещения 152

6 2 2 Рациональная организация и планировка рабочего места 156

6 2 3 Соблюдение требований к помещениям для размещения компьютерных систем 158

6 2 4 Ослабление электромагнитного излучения 159

6 2 5 Соблюдение правильного режима труда и отдыха 160

6 2 6 Использование систем кондиционирования 161

6 3 Экологичность 162

Заключение 164

Список использованной литературы 165

Введение

Актуальность исследования связана с тем, что потери российской экономики от нежелательной рассылки (спама) в 2008 году составили 1,3-1,9 млрд. долларов.

В 2009 году российские спамеры нанесли ущерб экономике страны уже на 14,1 миллиардов рублей.

Бурное развитие информационных и коммуникационных технологий принесло не только хорошие результаты, но и плохие, одними из которых стали массовые анонимные рассылки нежелательных сообщений в сетях электронной почты именуемые также как «спам».

Спам (англ. spam) — массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать. Легальность массовой рассылки некоторых видов сообщений, для которых не требуется согласие получателей, может быть закреплена в законодательстве страны. Например, это может касаться сообщений о надвигающихся стихийных бедствиях, массовой мобилизации граждан и т. п. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Незапрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM

Появившись в 1998 году, спам быстро доказал свою эффективность в области продвижения различных товаров и услуг. Определенная часть получателей навязчивой рекламы так или иначе проявляет к ней интерес, что способствует высочайшей прибыльности индустрии спама. В результате доход получает и заказчик рассылки, и ее источник. К сожалению, потенциал развития спама оказался столь значителен, что в 2003 году превзошел даже самые оптимистические прогнозы аналитиков. По общемировой статистике, спам составляет 90% всей корреспонденции. По России эта цифра несколько ниже.

Потери российской экономики от нежелательной рассылки (спама) в 2008 году составили 1,3-1,9 млрд. долларов.

В 2009 году российские спамеры лишили экономику страны уже 14,1 миллиардов рублей.

Ущерб оценивался по потерям рабочего времени всех занятых в экономике людей, пользующихся электронной почтой. 7 из 10 главных спамеров планеты - выходцы из России.

Например, крупнейшая в мире организация, зарабатывающая на распространении фармацевтического спама, так называемая партнерская программа Glavmed, создана и поддерживается гражданином России и жителем Москвы.

Основную долю в спамерских рассылках занимает реклама поддельных лекарственных препаратов и копий товаров элитных марок. Для распространения спама используются управляемые бот-сети, сформированные из подключенных к интернету персональных компьютеров, зараженных вирусами. На нее приходится 73,7% мирового спама.

Кроме того, доходы российских спамеров в 2009 году составили 3,7 млрд рублей или 118 млн долларов. Подсчеты проводились исходя из объема рассылок и их средней стоимости. Директор департамента аудита "Информзащиты" Максим Эмм Оценку РАЭК считает завышенной: при средней цене рассылки в 2000 рублей вряд ли спамеры заработали даже 1 млрд. Цена рассылки в России начинается от 3000 рублей. По оценке экспертов, до клиентов доходит 0,01% спамерских сообщений, из них 5% «конвертируется» в покупки.

По оценке Commtouch, в последнем квартале минувшего года уровень спама в нефильтруемом почтовом трафике в среднем составлял 77% при пиковом показателе 98% (ноябрь), а к концу декабря снизился до 68%.

Основной тематикой спам-рассылок являлась реклама фармацевтических препаратов, доля которой в общем объеме спама увеличилась до 81%. Перед Новым годом появилась несколько необычная разновидность фармаспама — с рекламным текстом, воспроизводимым в звуковом (mp3) формате. Эксперты Commtouch зафиксировали также ряд вредоносных спам-рассылок, включая ложные сообщения о проведении в США всеобщей вакцинации от «свиного» гриппа и поздравительные открытки к Хэллоуину.

Особой агрессивностью отличалась спам-кампания по распространению зловредов семейства Mal-Bredo A (Backdoor.Win32.Bredolab). В прошлом квартале письма с вредоносным zip-вложением имели форму уведомления о посылке или денежном переводе. В отчетный период вложенный файл с бэкдором позиционировался как новый пароль, якобы высланный службой техподдержки Facebook или MySpace в связи с введением новой политики безопасности. Исследователи отмечают, что в настоящее время число вариантов Mal-Bredo A не достигает и тысячи, тогда как в ноябре их насчитывалось около 10 тысяч, но число спам-рассылок с опасным зарядом возросло.

Осознавая общественную опасность спама ряд государств приняли законы, связанные с ограничением или запрещением незапрашиваемых массовых почтовых рассылок коммерческого или некоммерческого содержания.

Неудивительно, что лидером в регулировании предметных общественных отношений выступили США. В данном государстве в различных штатах с 1998 стали появляться специальные нормы, а на федеральном уровне ведется разработка ряда федеральных законов.

В ряде стран принимаются законодательные меры против спамеров. Попытки законодательного запрещения или ограничения деятельности спамеров наталкиваются на целый ряд сложностей. Непросто определить в законе, какая рассылка является законной, а какая нет. Хуже всего то, что компания (или лицо), рассылающая спам, может находиться в другой стране. Для того, чтобы такие законы были эффективными, необходимо выработать согласованное законодательство, которое действовало бы в большинстве стран, что представляется труднодостижимым в обозримом будущем.

В России спам запрещѐн «Законом о рекламе» (ст.18, п.1):

«Распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламорас-

пространитель не докажет, что такое согласие было получено»

В официальных комментариях Федеральной антимонопольной службы, уполномоченной осуществлять функции контроля за соблюдением этого закона, указывалось на применимость данной нормы к интернет-рассылкам. За нарушение статьи 18 рекламораспространитель несѐт ответственность в соответствии с законодательством об административных правонарушениях. Однако ФАС не имеет полномочий для проведения оперативно-розыскных мероприятий по установлению лица, ответственного за спам, а уполномоченные на это органы не могут их проводить в связи с отсутствием в российском административном и уголовном законодательстве ответственности за рассылку спама. Поэтому, несмотря на периодические публикации материалов о привлечении нарушителей к ответственности, в настоящее время данная законодательная норма малоэффективна.

С 1 января 2004 года в США действует федеральный закон, получивший название Can-Spam Act. Делаются попытки привлечь спамеров к суду, и иногда такие попытки оказываются успешными.

Американец Роберт Солоуэй проиграл процесс в федеральном суде против небольшой оклахомской фирмы-провайдера интернет-услуг, оператор которой обвинил его в рассылке спама. Приговор суда включал в себя возмещение убытков в размере $10 075 000.

В октябре 2009 года социальная сеть Facebook отсудила у американца Сэнфорда Уоллеса, занимавшегося спамом на этом сайте, 711 миллионов долларов. Примечательно, что для Уоллеса по прозвищу «король спама» это был далеко не первый суд: в 2006 году он был оштрафован на 4 миллиона долларов за незаконную в США рекламу с помощью всплывающих окон, а в 2008 году — на 234 миллиона долларов за спам в социальной сети MySpace.

Интересен пример истории с российским провайдером Majordomo, заблокированным за рассылки спама, якобы ведшиеся с принадлежавших ему адресов.

Принимаемые законы по борьбе со спамом могут противоречить конституции. Так Верховный Суд Вирджинии отменил приговор спамеру Джереми Джейнсу и признал неконституционным закон о борьбе со спамом как нару-

шающий право на свободу слова.

Существует несколько признаков по которым можно классифицировать сообщение как «спам»:

1 рассылаются массово;

2 являются незапрошенными, то есть, рассылаются по каналам e-mail, ICQ, IRC и другим подобным, где пользователь не может исключить получение сообщений, не ограничивая себя существенно, при этом рассылаются без явного или неявного согласия получателя либо после явного выражения им несогласия;

3 содержат рекламу (в том смысле, как она определена в законе «О рекламе», то есть, в широком смысле;

4 являются анонимными, то есть, не содержат идентификации рекламораспространителя, либо содержат неверные данные о рекламораспространителе.

В зависимости от различных комбинаций указанных признаков можно поразному оценивать законность спама в РФ. Причем, до принятия предметных норм и возникновения правоприменительной (в первую очередь, судебной) практики, любые научные характеристики будут являться умозрительными – законодательство РФ к названному комплексному предмету отношений не приспособлено.

Основной проблемой которую несет с собой «спам» является «засорение» канала передачи данных. Зачастую пользователи просто не обращают внимания на сетевую рекламу, удаляя такие сообщения из своих почтовых ящиков. На самом деле пагубность таких рассылок заключается в том, что атакующему это практически ничего не стоит, зато дорого обходится всем остальным, как получателю «спама» так и его провайдеру. Большое количество рекламной корреспонденции может привести к излишней нагрузке на каналы и почтовые серверы провайдера, из-за чего обычная почта, которую, возможно, очень ждут получатели, будет проходить значительно медленнее. «Рассыльщик» практически ничего не платит за то, что передает почту. За все расплачивается получатель спама,

оплачивающий своему провайдеру время в Сети или трафик, затрачиваемые на получение не запрошенной корреспонденции с почтового сервера.

Именно поэтому наибольший вклад в борьбу со «спамом» вносят провайдеры, которые имеют возможность настраивать для этой цели собственные системы и ресурсы. Пользователи же провайдеров также могут бороться со спамом используя клиентские фильтры электронных сообщений, но эффективность этих фильтров значительно ниже.

Провайдеры для борьбы со спамом используют, в первую очередь, такие способы как фильтрация (селекция и уничтожение почтовых сообщений) и блокировка (идентификация и отказ в принятии сообщений). Также они, используя механизмы саморегуляции, объединяются друг с другом и пытаются совместными организационно-техническими действиями повышать эффективность действий по борьбе с массовыми почтовыми рассылками и со «спамерами».

В предлагаемой работе будет предпринята попытка разработать методику количественного анализа информационных рисков касательно массовых рассылок нежелательных сообщений. Данная методика опирается на методы теории вероятностей, и ориентирована на рассмотрение объема ущерба как случайной величины с определенным законом распределения.

Объектом исследования является КС в условиях постоянного получения нежелательных электронных сообщений, в котором субъект информационной атаки многократно воздействует на КС в пределах одного определенного метода распространения, причем каждая такая попытка воздействия может быть успешной либо неуспешной.

Предметом исследования является анализ и управление рисками КС в процессе постоянной массовой безадресной рассылки нежелательных сообщений.

Таблица В1 - Спам-статистика за период 8-14 февраля 2010 г.

№	Тематика	Описание	Доля тематики	Изменения за неделю
1	Образование	Реклама семинаров, тренингов, курсов.	19,00%	2,20%
2	Отдых и путешествия	Предложения туристических поездок, а также организации и проведения различных развлекательных мероприятий.	16,30%	16,30%
3	Другие товары и услуги	Предложения других товаров и услуг.	16,00%	-2,40%
4	Медикаменты; товары/услуги для здоровья	Предложения приобрести лекарственные препараты, БАДы и т.п. в online. Предложения медицинских и оздоровительных услуг, а также сопутствующих товаров.	15,70%	-4,10%
5	Компьютерное мошенничество	Фишинг, "нигерийские" письма, поддельные извещения о выигрыше в лотерею и пр. попытки мошенничества.	6,40%	-1,30%
6	Компьютеры и Интернет	Предложения приобрести ПО, компьютерную технику, расходные материалы; также предложения для владельцев сайтов (хостинг, обмен баннерами и т.п.).	5,60%	1,40%
7	Реплики элитных товаров	Копии часов, аксессуаров, обуви и других товаров известных марок.	4,30%	-0,60%
8	Реклама спамерских услуг	Предложения организовать спамерскую рассылку, программы для рассылок, базы электронных адресов и т.п.	4,30%	0,90%
9	Юридические услуги и аудит	Предложения юридических услуг	3,20%	1,10%
10	Спам "для взрослых"	Предложения скачать/получить/ознакомиться с контентом "для взрослых". Знакомства и т.п.	2,70%	0,10%
11	Недвижимость	Предложения сдать/снять недвижимость, строительство, риелторские услуги и пр.	2,20%	0,60%
12	Личные финансы	Предложения по страхованию, уменьшению кредитной задолженности, выгодным условиям займов и т.п. В подавляющем большинстве англоязычные письма.	Менее 2%	-0,40%
13	Полиграфия	Визитки, календари, печать, услуги типографии и пр.	Менее 2%	0,80%

Таблица В2 - Спам-статистика за период 15-21 февраля 2010 г.

№	Тематика	Описание	Доля тематики	Изменения за неделю
1	Образование	Реклама семинаров, тренингов, курсов.	17,8%	-1,2%
2	Отдых и путешествия	Предложения туристических поездок, а также организации и проведения различных развлекательных мероприятий.	17,6%	+1,3%
3	Медикаменты; товары/услуги для здоровья	Предложения приобрести лекарственные препараты, БАДы и т.п. в online. Предложения медицинских и оздоровительных услуг, а также сопутствующих товаров.	12,7%	-3,0%
4	Другие товары и услуги	Предложения других товаров и услуг.	11,7%	-4,3%
5	Компьютерное мошенничество	Фишинг, "нигерийские" письма, поддельные извещения о выигрыше в лотерею и пр. попытки мошенничества.	10,9%	+4,5%
6	Компьютеры и Интернет	Предложения приобрести ПО, компьютерную технику, расходные материалы; также предложения для владельцев сайтов (хостинг, обмен баннерами и т.п.).	6,9%	+1,3%
7	Реплики элитных товаров	Копии часов, аксессуаров, обуви и других товаров известных марок.	5,7%	+1,4%
8	Недвижимость	Предложения сдать/снять недвижимость, строительство, риелторские услуги и пр.	3,5%	+1,4%
9	Реклама спамерских услуг	Предложения организовать спамерскую рассылку, программы для рассылок, базы электронных адресов и т.п.	3,4%	-0,9%
10	Спам "для взрослых"	Предложения скачать/получить/ознакомиться с контентом "для взрослых". Знакомства и т.п.	3,1%	+0,4%
11	Юридические услуги и аудит	Предложения юридических услуг.	2,5%	-0,7%
12	Личные финансы	Предложения по страхованию, уменьшению кредитной задолженности, выгодным условиям займов и т.п. В подавляющем большинстве англоязычные письма.	Менее 2%	+1,0%
13	Полиграфия	Визитки, календари, печать, услуги типографии и пр.	Менее 2%	-0,6%

В настоящее время имеется большое разнообразие методик и стандартов анализа и управления рисками: международные стандарты: ISO/IEC 27001, ISO/IEC 27002(ISO/IEC 17799), ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006; национальные стандарты и методики: BS7799, BSI, NIST 800-30, CRAMM, COBIT, GAO и FISCAM. Эти методики преимущественно касаются

качественного подхода к оценке рисков. Но так как риск – категория вероятностная, то очевидна необходимость рассмотрения количественного подхода к оценке риска.

На сегодняшний день аппарат теории вероятностей, математической статистики, теории массового обслуживания, системного анализа, теории риска и математического анализа, а также теории чувствительности хорошо разработан, что позволяет учесть при моделировании стохастический характер массовых рассылок электронных сообщений.

Цель настоящей работы заключается в разработке и исследовании адекватных вероятностных моделей КС в условиях массовых рассылок электронных сообщений, сопровождающихся информационным риском.

Для достижения указанной цели дипломной работы предполагается решить следующие задачи:

- на основе анализа статистических данных выявить классы методик массовой рассылки сообщений, которые по своим характерным особенностям подчиняются некоторому закону распределения, выдвинуть соответствующую гипотезу и доказать еѐ;
- построить вероятностные модели КС в условиях массовой рассылки сообщений выбранных методов на основе выбранного закона распределения, включая параметры риска необходимые для анализа;
- оценить влияние изменения параметров массовой рассылки сообщений на поведение построенной модели риска, определение множества оптимальных решений задачи численного поиска области допустимого риска;
- на основе обоснованных критериев качества управления риском и введенных ограничений на процесс управления разработать алгоритмы реализации оптимального управления риском в атакуемой КС;
- оценить экономические показатели эффективности разработанных алгоритмов.

Научная новизна ожидаемых результатов заключается в построении математической модели различных современных организациях систем фильтрации сообщений с учетом новейших статистических данных, определении информа-

ционного риска для этих моделей как функция нормированного ущерба, построении имитационной модели позволяющей проследить динамику изменения риска с помощью методов теории вероятностей, системного анализа, теории конфликта, математического и имитационного моделирования для построения вероятностной модели информационных атак на КС; методов теории рисков, математического анализа и теории чувствительности для проведения анализа рисков атакуемых КС и установления аналитической формулы расчета риска; методов математической статистики и статистического анализа временных рядов для построения статистической модели массового распространения нежелательных электронных сообщений и оценки параметров вероятностного распределения; методов теории управления и оптимизации, вариационного и операционного исчисления для решения задачи оптимизации управления информационным риском.

Практическая ценность работы заключается в возможности создания на основе проведенных исследований принципиально новых как программных, так и программно-аппаратных средств борьбы со СПАМом в практических любых масштабах.

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

Заключение

В дипломной работе получены следующие основные результаты.

1 Для описания процесса массовых рассылок нежелательных сообщений предлагается использование пуассоновского потока событий. На основе анализа статистических выборок из экспериментальных данных для потока сообщений доказаны гипотезы об их принадлежности распределению Паскаля.

2 На основе выявленных моделей архитектурной организации спам-систем, получены соответствующие вероятностные модели для риск-анализа атакуемых. Причем риск предлагается рассматривать как функцию нормированного ущерба.

3 Выявлены особенности расчета ущерба и защищенности КС. Получены соответствующие характеристики, являющиеся необходимой математической базой для оценки рисков и защищенности исследуемой КС.

4 Определены меры риска и защищенности ИТКС атакуемых спамом

5 Проведена алгоритмизация управления защищенностью атакуемых информационно-телекоммуникационных систем.

6 Численно доказана экономическая эффективность настоящей работы по исследованию процессов многократных атак на КС, так как показатель общенаучного и учебно-исследовательского эффекта равен 0,91.

7 Проведена оценка безопасности жизнедеятельности операторов КС в условиях информационного конфликта. Полученные выводы подтверждают, что разработанная в данной дипломной работе методика вреда для окружающей среды и оператора КС не представляет.

Таким образом, была достигнута цель настоящей работы, состоящая в разработке и исследовании адекватных вероятностных моделей КС в условиях массовых рассылок электронных сообщений, сопровождающихся информационным риском.

Литература

1 Акофф Р.Л. Планирование в больших экономических системах / Р.Л. Акофф. – М.: Сов. радио, 1972. – 248 с.

2 Александров А.Г. Оптимальные и адаптивные системы / А.Г. Александров. – М.: Высшая школа, 1989. – 287 с.

3 Алексеев В.М. Оптимальное управление / В.М. Алексеев. – М.: Наука, 1979. – 316 с.

4 Альтовский Е. Что попадает под определение «спам» // Е. Альтовский. – AntiSpam – 2005.

5 Афанасьев В.Н. Математическая теория конструирования систем управления / В.Н. Афанасьев, В.Б. Колмановский, В.Р. Носов. – М.: Высшая школа, 1989. – 447 с.

6 Антоняна Ю.М. Этнорелигиозный терроризм / Ю.М. Антоняна. – М.: Аспект-Пресс, 2006. – 318с.

7 Анцупов А.Я. Конфликтология: учебник для вузов / А.Я. Анцупов. - М.: Юнити, 2002. - 591 с.

8 Аоки М. Введение в методы оптимизации / М. Аоки. – М.: Наука, 1977. – 344 с.

9 Арустамов Э.А. Безопасность жизнедеятельности при работе с компьютерной техникой / Э.А. Арустамов, Т.А. Акимова. – М.: РУДН, 2007. – 320с.

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

11 Афанасьев В.Н. Математическая теория конструирования систем управления / В.Н. Афанасьев, В.Б. Колмановский, В.Р. Носов. – М.: Высшая школа, 1989. – 447 с.

12 Баранник А.А. Концептуальное моделирование процессов информационной сферы / А.А. Баранник, А.В. Киба, А.Н. Левченков // Известия ТРТУ. Тематический выпуск. - 2005. - № 4 (48). –С. 13-19.

13 Барсуков В.С. Современные технологии безопасности /

В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с.

14 Балдин К.В. Управление рисками / К.В. Балдин, С.Н. Воробьев. – М.: ЮНИТИ-ДАНА, 2005. – 511 с.

15 Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. - М.: Мир, 1991.-215 с.

16 Белецкая С.Ю. Моделирование и поиск оптимальных решений при проектировании сложных систем: Монография / С.Ю. Белецкая. – Воронеж: ВГТУ, 2005. – 175 с.

17 Бершадский А.В. Что могут дать технологии управления рисками современному бизнесу? / А.В. Бершадский // Управление и обработка информации: модели процессов: сб. ст. МФТИ. – М., 2001. – С. 34-51.

18 Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, Ф.Г. Гурвич. 2-е изд. - М.: Статистика, 1980. - 263 с.

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

20 Березин А.С. Сейф для бизнеса / А.С. Березин, С.А. Петренко // Конфидент. - 2002. - № 4-5. - С.132-136.

21 Березина Л.Ю. Графы и их применение / Л.Ю. Березина. – М.: Просвещение, 1979. – 276 с.

22 Бережная Е.В. Математические методы моделирования экономических систем / Е.В. Бережная, В.И. Бережной. – М: Финансы и статистика, 2006. – 432 с.

23 Боровков А. А., Вероятностные процессы в теории массового обслуживания / А. А. Боровков. - М.: Наука, 1972.

24 Боголюбов А.Н. Основы математического моделирования / А.Н. Боголюбов. - М.: Дрофа, 2003. - 137 с.

25 Большев Л.Н. Таблицы математической статистики / Л.Н. Большев, Н.В. Смирнов. – М.: Наука, 1983. – 297 с.

26 Борисов А.Н. Принятие решения на основе нечетких моделей: примеры использования / А.Н. Борисов, О.А. Крумберг, И.П. Федоров. – Рига: Знание, 1990. - 184 с.

27 Борисов В.И. Моделирование информационных операций и атак в сфере государственного и муниципального управления / В.И. Борисов. – Воронеж: ВИ МВД России, 2004. – 144 с.

28 Борисов А.Н Принятие решений на основе нечетких моделей. Примеры использования. / Борисов А.Н., Крумберг О.А., Федоров И.П. Рига:// "Зинатне", 1990.

29 Браверман Э.М. Структурные методы обработки эмпирических данных / Э.М. Браверман, И.В. Мучник. – М.: Наука, 1983. – 417 с.

30 Брахман Т.Р. Многокритериальность и выбор альтернативы в технике / Т.Р. Брахман. – М.: Радио и связь, 1984. – 287 с.

31 Бриль В.М. Оценка показателей уязвимости информации при несанкционированном доступе / В.М. Бриль, С.Д. Нестеренко, В.В. Шаталюк. - Киев: Нсб. ЗИ, 2000. - 156 с.

32 Васильев В.И. Алгоритм проектирования оптимальной структуры комплексной системы защиты информации на основе анализа риска / В.И. Васильев, Т.А. Иванова // Информационная безопасность: материалы VI междунар. науч.-практ. конф. - Таганрог: Изд-во ТРТУ, 2005. – С.270-274.

33 Васильев П.П. Безопасность жизнедеятельности: Экология и охрана труда; Количественная оценка и примеры: учеб. пособие для вузов – М.: ЮНИТИ-ДАНА, 2003. – 188 с.

34 Васильев Ф.И. Численные методы решения экстремальных задач / Ф.И. Васильев. – М.: Наука, 1988.

35 Васютин С.В. Построение агентов мониторинга системы обнаружения атак / С.В. Васютин, С.В. Лебедев // Информационная безопасность: материалы VI междунар. науч.-практ. конф. - Таганрог: Изд-во ТРТУ, 2004. – С. 181-184.

36 Вентцель Е.С. Теория вероятностей: учебник для вузов / Е.С. Вентцель. – М.: Высш. шк, 1998. – 576 с.

37 Вентцель Е.С. Теория вероятностей и ее инженерные приложения: учеб. пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. – М.: Высш. шк, 2003. – 464 с.

38 Вероятность и математическая статистика: энциклопедия / Гл. ред. акад. РАН Ю.В. Прохоров. – М.: Большая Российская энциклопедия, 1999. – 910 с.

39 Власова А. «Спам»-активность 2005-2007 / А.Ф. Власова // spamtest.ru. – 2008.

40 Волков И.М. Проектный анализ. Вероятностные методы анализа рисков / И.М. Волков, М.В. Грачева. – М.: ИНФРА-М, 2004. – 124 с.

41 Волобуев С.В. Философия безопасности социотехнических систем / С.В. Волобуев. – М.: Вузовская книга, 2002. – 360 с.

42 Воробьев Э.И. Моделирование и анализ сложных систем / Э.И. Воробьев. – Воронеж: ВГТУ, 2005. – 118 с.

43 Ворожейкин И.Е. Конфликтология: учебник / И.Е. Ворожейкин. - М.: ИНФРА, 2002. - 240 с.

44 Гаценко О.Ю. Защита информации. Основы организационного управления / О.Ю. Гаценко. – СПб.: Сентябрь, 2001.- 228 с.

45 Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. - М.: МОПО РФ - МГИФИ, 1997. – 500 с.

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

47 Гнеденко Б.В. Математические методы в теории надежности / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М.: Наука, 1965. – 333 с.

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

49 Горский Д.М. Информационные аспекты управления и моделирования / Д.М. Горский. - М.: Наука, 1978. - 213 с.

50 Гузик С. Управление и аудит информационных технологий. Особенности проведения внешнего аудита // Jet Info, №1(116). - М.,2003.-С.3-24

51 Дарьялов Н.К. Вред, наносимый спамом // Microsoft, Информационный бюллетень №23.

52 Девянин П.Н. Теоретические основы компьютерной безопасности: учеб. пособие / П.Н. Девянин, О.О. Михальский, Д.И. Правиков. - М.: Радио и связь, 2000. – 192с.

53 Дифференциальные уравнения. Некоторые математические задачи оптимального управления: сб. ст. / Труды математического института имени В.А. Стеклова. – М.: Наука, 2001. – Т. 233. – 207 с.

54 Дмитриев А.В. Конфликтология: учеб. пособие / А.В. Дмитриев. - М.: Гардарики, 2003. - 320 с.

55 Домарев В.В. Энциклопедия безопасности информационных технологий. Методология создания систем защиты информации / В.В. Домарев. – Киев: ТИД ДС, 2001. – 688 с.

56 Модели риск-анализа социотехнических систем: учеб. пособие / В.П. Дуров, Р.В. Батищев, С.М Колбасов, В.Н. Асеев, Д.Е. Морев. – Воронеж: ГОУВПО «ВГТУ», 2007. – 208 с.

57 Жаринов А.Б. Терроризм и террористы: справочник / А.Б. Жаринов. – М.: Харвест, 2004. – 608с.

58 Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. М.:Мир, 1976.

59 Замула А.А. Методология анализа рисков и управления рисками / А.А. Замула // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2002. – Вып. 126. – 219 с.

60 Захаров С.А. Нечеткие множества и лингвистические комбинации в анализе рисков: учеб. пособие / С. А. Захаров, Н. В. Медведев, Н. В. Румянцев. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2005г. - 75 с.

61 Зражевский В.В. Основные направления совершенствования системы управления рисками / В.В. Зражевский. – М., 1999. – 465 с.

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

63 Корн Г. Справочник по математике для научных работников и инженеров: Определения. Теоремы. Формулы / Г. Корн. – 6-е изд., стер. – СПб.: Лань, 2003. – 832 с.

64 Коул Э. Руководство по защите от хакеров / Э. Коул. – М.: Вильямс, 2002. – 640 с.

65 Кениг Д. Методы теории массового обслуживания: Пер. с нем. /Под. ред. Г.П.Климова. М., 1981.

66 Крылов В.В., Самохвалов С.С. Теория телетрафика и ее приложения. – СПб.: БХВ-Петербург, 2005.

67 Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – 2-е изд. – СПб.: БХВ - Петербург, 2003.– 608 с.

68 Марков А. Управление рисками — нормативный вакуум информационной безопасности /А. Марков, В. Цирлов / Открытые системы. – 2006. – №11.

69 Медведовский И.Д. ISO 17799: эволюция стандарта с 2002 по 2005 год / И.Д. Медведовский // Jet Info. – 2005. – №6.

70 Научный форум «Системы, процессы и безопасность 2007-2008». Межрегиональная науч.-практ. конф. «Информационные риски и безопасность» Воронежское отделение Российской инженерной академии. Сб. науч. трудов. – Воронеж: МИКТ, 2007. – 102с.

71 Ивченко Г. И. Теория массового обслуживания: учебное пособие для вузов. / Ивченко Г. И., Каштанов В. А., Коваленко И. Н. – М.: Высш. школа, 1982. – 256.

72 Карпов Ю.А. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. / Карпов Ю.А. – СПб:БХВ-Петербург, 2006. – 400с.

73 Кофман А. Массовое обслуживание. Теория и приложения. / Крюон Р. — М.:Мир, 1965.

74 Кофман А. Введение в теорию нечетких множеств. М.: Радио и связь, 1982.

75 Морева О.Д. Разработка методики оценки информационной защищенности социотехнических систем с использованием функций чувствительности: дис. канд. техн. наук: 05.13.19 / Морева О.Д. – Воронеж, 2006.

76 Наумов В. Спам: юридический анализ явления // В. Наумов. – Russian Law – 2001.

77 Нартов А.В. Обзор антиспамерских продуктов // securitylab.ru, Уязвимости и аналитика.

78 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.

79 Остапенко Г.А. Информационные операции и атаки в социотехнических системах: учеб. пособие / Г.А. Остапенко. – Воронеж: ВГТУ, 2005. – 202 с.

80 Орловский С.А. Проблемы принятия решений при нечеткой исходной информации. М.: Наука, 1981.

81 Поспелова Д.А. Нечеткие множества в моделях управления и искусственного интеллекта //Под ред. Д.А. Поспелова. М., 1986.

82 Ракитина Е.А. Информатика и информационные системы в экономике: учеб. пособие. Ч 1. / Ракитина Е.А., Пархоменко В.Л. – Тамбов: Изд-во ТГТУ, 2005.–148с.

83 Розенберг В. Я. Что такое теория массового обслуживания / Розенберг В. Я., Прохоров А. И. - М.: Наука, 1965.

84 Саати Т.Л. Элементы теории массового обслуживания и ее приложения-М.: 1971.

85 Саульев В.К. Математические модели теории массового обслуживания – М.: 1979.

86 Севастьянов Б.А. Вероятностные модели / Б.А. Севастьянов. – М.: Наука, 1992. – 175 с.

87 Симонов С.В. Методики и технологии управления информационными рисками / С.В. Симонов, С.А. Петренко// IT Manager. – 2003. – № 3.

88 Симонов С.В. Методология анализа рисков в информационных систе-

мах / С.В. Симонов // Конфидент. – 2001. – № 1.

89 Смагин В.И. Локально-оптимальное управление в дискретных системах с неизвестными постоянными возмущениями и параметрами / В.И. Смагин // Изв. вузов. Приборостроение. – 1997. – Т. 40. – № 1. – С. 37 – 41.

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

91 Советов Б.Я. Моделирование систем / Б.Я. Советов, С.А. Яковлев. – М.: Высшая школа, 1998. – 138 с.

92 Стефанов Н. Управление, моделирование, прогнозирование / Н.Стефанов, Н. Яхиел, С. Качаунов. – М.: Экономика, 1972. – 437 с.

93 Субботин А.И. Минимаксные неравенства и уравнения Гамильтона-Якоби / А.И. Субботин. – М.: Наука, 1991. – 216 с.

94 Сысойкина М. Безопасность как основа непрерывности бизнес-процессов // Журнал «Безопасность». – 2006. - №6.

95 Трубачев А. Концептуальные вопросы оценки безопасности информационных технологий. // Jet Info. – 1998. - № 5-6.

96 Толстых Н.Н. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем / Н.Н. Толстых. – Воронеж: ВГТУ, 2003. – 169 с.

97 Тутубалин А. Эволюция способов рассылки спама / Спамтест, 2004 – Аналитика.

98 Томашевский В. Имитационное моделирование в среде GPSS / В. Томашевский, Е. Жданов. – М.:Бестселлер, 2003. – 416с.

99 Федотов Н.В. Оценка и нейтрализация рисков в информационных системах: метод. пособие / Н.В. Федотов, В.А. Алешин / под ред. Н.В. Медведева. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2004. - 52 с.

100Федосеев Ю.Н. Методы анализа систем массового обслуживания. М.: Изд. МИФИ, 1982.

101Флеминг У. Оптимальное управление детерминированными и стохас-

тическими системами / У. Флеминг, Р. Ришел. – М.: Мир, 1978. – 320 с.

102Ханика Ф.П. Новые идеи в области управления / Ф.П. Ханика. – М.: Прогресс, 1969. – 318 с.

103Хинчин А. Я., Работы по математической теории массового обслуживания, М., 1963.

104Хохлов Н.В. Управление риском / Н.В. Хохлов. – М.: ЮНИТИ-ДАНА, 1999. – 239 с.

105Цирлин А.М. Вариационные методы оптимизации управляемых объектов / А.М. Цирлин. – М.: Энергия, 1976. – 162 с.

106Черняк Ю.И. Системный анализ в управлении экономикой / Ю.И. Черняк. – М.: Экономика, 1975. – 393 с.

107Шапкин А.С. Теория риска и моделирование рисковых ситуаций / А.С. Шапкин, В.А. Шапкин. – М.: Дашков и К, 2005. – 879 с.

108Шикин Е.В. Математические методы и модели в управлении / Е.В. Шикин, А.Г. Чхартишвили. – М.: Дело, 2000. – 440 с.

109Шурыгин А.М. Прикладная стохастика: робастность, оценивание, прогноз / А.М. Шурыгин. – М.: Финансы и статистика, 2000. – 224 с.

110Щетинин И. Риск - менеджмент в управлении ИТ. // Журнал "Открытые системы". – 2006. - №2.

111Язов Ю.К. Моделирование процессов непосредственного проникновения в операционную среду компьютера: учеб. пособие / Ю.К. Язов, Н.М. Радько, А.Ф. Мешкова. – Воронеж: ГОУВПО «ВГТУ», 2007. – 146 с.

112Язов Ю.К. Основы технологии в телекоммуникационных системах: учеб. пособие. – Воронеж: ВГТУ, 2005 – 341с.

113Ярочкин И.В Безопасность информационных систем.– М.:Ось-89, 1996.– 240 с.