## Содержание

## ВВЕДЕНИЕ

### Актуальность исследования

В современном мире от информационных технологий зависит успех деятельности организаций разных уровней: от небольших фирм до градообразующих предприятий и государственных структур. С появлением сети Интернет стал возможен мгновенный обмен информацией, новостями, мультимедийным контентом. Непрерывно растèт популярность средств электронных коммуникаций, в том числе и электронной почты. Большинство организаций регистрирует электронные почтовые ящики на каждого сотрудника, практически все пользователи всемирной паутины имеют свой электронный почтовый ящик, притом зачастую несколько. Поток электронных сообщений постоянно увеличивается, этому способствует простота использования электронной почты, мгновенная доставка писем и бесплатность. [4,10]

Преимущества электронной почты сделали возможным рассылку нежелательных электронных сообщений (спама). По итогам 2011 года доля спама в потоке электронной почты составила 80,26%.[99, 103, 104] С помощью несанкционированных рассылок может осуществляться реклама или антиреклама организации, вымогательство денег, хищение данных или паролей, внедрение вредоносных программ. [8]

Спам в современном Интернете является неправомерным занятием, и в законодательстве ряда стран предусмотрены различные виды ответственности за такую деятельность. Например, в США один из крупнейших провайдеров Интернет AOL (AmericaOnline) ежемесячно выдвигает по несколько судебных исков к злоумышленникам, которые занимаются систематической рассылкой несанкционированных электронных сообщений по адресам еè клиентов.[30]

Нежелательные сообщения пользователь удаляет, зачастую даже не просматривая. Проведенный эксперимент исследователей университета Калифорнии показал, что из 12,5 миллионов разосланных сообщений со спамом только одно находит отклик у адресата и приводит к покупке рекламируемого товара, то есть эффективность спам рекламы 0,000008%.[102] Несмотря на столь

низкие показатели эффективности, услуги по рассылке спама пользуются популярностью, а, как известно, где есть спрос – есть и предложение.

По оценкам различных компаний, занимающихся проблемами информационной безопасности, основная доля спама рассылается с использованием сетей компьютеров обычных пользователей, превращенных в компьютеры – зомби при помощи уязвимости в ПО или использования вирусных технологий. Такие сети называют ботнетами, доля спам сообщений, разосланных при помощи сетей компьютеров-зомби, превышает 70% (по данным компании SophosLabs).[8]Ботнеты позволяют злоумышленникам не только рассылать огромное количество писем, но и оставаться безнаказанными, скрывая истинные источники рассылок. [1]

Пагубность спама том, что для злоумышленника отправка спам сообщения практически ничего стоит, но дорого обходится как получателю, так и провайдеру. Большое количество рекламной корреспонденции может привести к излишней нагрузке на серверы и провайдера, замедляя доставку электронных писем обычных пользователей.[5] Получатель спама тратит своѐ время, время в сети Интернет, затрачиваемое на получение незапрошенной корреспонденции. Помимо этого, открытие ссылки в спам письме может обернуться для получателя потерей денег с электронных кошельков или банковских карт, заражением компьютера вирусом или троянской программой, утратой паролей от популярных сервисов.

Резюмируя вышесказанное, можно сделать вывод о важности исследований в области несанкционированных массовых рассылок. Ведущие компании в области информационной безопасности постоянно ведут разработку новых алгоритмов, методов, средств и систем защиты пользователей отспам сообщений.

Пожалуй, особый интерес имеют риск-модели, учитывающие не только вероятность наступления ущерба, но и его величину в случае успешного проникновения спама в автоматизированную систему. Данное направление исследования представляется весьма актуальным и слабо проработанным.

**Степень научной разработанности**

В настоящее время активно ведутся исследования в области подсчета риска проникновения спама в автоматизированную систему.

Довольно успешно [48-52] развивается методология риск-анализа, широко применимая в теории и практике обеспечения информационной безопасности. Еѐ совершенствование в контексте повышения защищенности субъектов АС от проникновения спама представляется весьма актуальным. Для изучения рисков в данном случае можно применить хорошо разработанный математический аппарат теории случайных функций

Таким образом, исходя из актуальности и степени научной разработанности данной проблемы, можно сделать вывод о целесообразности проведения комплексных исследований в данном направлении.

**Цель работы** состоит в оценке и регулировании рисков реализации несанкционированной рассылки электронных сообщений в отношении автоматизированной системы, а также разработка рекомендаций по противодействию спаму. Для достижения поставленной цели необходимо решить следующие**задачи**:

1. Классифицировать незаконные массовые рассылки в отношении автоматизированной системы, рассмотреть способы рассылки и маскировки спам-сообщений;
2. Разработать риск-модель спам-атак в распределенных автоматизированных системах, плотность распределения ущерба в которых имеет заданный вид, найденный после анализа статистики ущербов от незаконных массовых рассылок. Рассмотреть основные параметры распределения;
3. Разработать новый подход к регулированию рисков, основанный на изменении параметров отдельных компонент РАС, применительно к распределенным автоматизированным системам, подверженных угрозам спам-атак.

**Объектом исследования** являетсяраспределеннаяавтоматизированная система (РАС), в отношении которой реализуется несанкционированная рассылка электронных сообщений, способная оказать деструктивное воздействие на функционирование системы.

**Предметом исследования** являетсяриск-анализ реализации незаконных рассылок электронных сообщений в отношении автоматизированной системы, ущерб или количество которых представимо в виде временного ряда.

**Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе,** обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

**В исследовании используются методы** теории системного анализа, методы экспертных оценок и математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

**Научная новизна ожидаемых результатов** заключается в следующем:

1 В отличие от аналогов, процесс исследования не запрошенных массовых рассылок в распределенных автоматизированных системах учитывал результаты их количественного и качественного развития, а также особенности реализации при различных условиях и типах объектов.

2 В отличие от аналогичных, полученная риск-модель спам-атак на распределенные автоматизированные системы включает в себя выражения для экстремумов интегрального риска распределенных автоматизированных систем.

3 В отличие от аналогов, алгоритм регулирования интегрального риска реализации асинхронных спам-атак на распределенные автоматизированные системы отличается особенностью управления общего риска с помощью регулирования среднего значения ущерба и среднеквадратического отклонения в компонентах системы, с учетом распределения риска в них.

**На защиту выносятся** следующие основные положения работы:

1 Понятие спам-атак в распределенных автоматизированных системах, основные виды спама, способы рассылки и маскировки спам-сообщений;

2 Риск-модель спам-атак в распределенных автоматизированных системах;

3 Алгоритм регулирования рисков в распределенных автоматизированных системах, подверженных угрозамспам-атак.

**Практическая ценность** работы заключается в том, что:

1 Классификация основных видов спам-атак в распределенных автоматизированных системах позволяет выявить наиболее опасные их виды в

зависимости от цели и направленности атаки и дает возможность уделить особое внимание защите от этих типов не запрошенных массовых рассылок.

2 Построенная риск-модель может применяться для оценки рисков спам-атак на распределенные автоматизированные системы, а также для построения систем, устойчивых к не запрошенным массовым рассылкам. Полученные выражения для интегрального риска данных систем и его экстремумов позволяют оценить защищенность системы в целом, а также выявить наиболее уязвимые компоненты.

3 Алгоритм регулирования интегрального риска в случае реализации асинхронных атак может применяться для снижения риска спам-атак на распределенные автоматизированные системы, в частности, он позволяет снизить среднее значение ущерба, наносимого организации, в целом, а так же среднеквадратическое отклонение, путем регулирования тех же параметров в компонентах системы. Это позволяет проводить мероприятия по управлению рисками выборочно, уделяя внимание лишь защите самых уязвимых компонентов, что уменьшает затраты на защиту.

## ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию распределенных автоматизированных систем и риск-анализу воздействия на них спам-атак. Основные научные и практические результаты, полученные в ходе выполнения работы:

1. На основании проведенных исследований предложена новая экспериментальная методика регулирования риска реализации спам-атак на распределенные автоматизированные системы.

2. Предложены оригинальные суждения по оценке суммарного риска для случая спам-атак на распределенные автоматизированные системы, у которых плотность вероятности наступления ущерба в компонентах имеет бета-распределение второго рода.

3. Возможностью применения построенной риск-модели для оценки рисков спам-атак в РАС доказана перспективность и состоятельность использования полученных выражений для экстремумов интегрального риска, с целью его анализа в распределенных автоматизированных системах, выявления уязвимых компонент, защите которых необходимо уделить особое внимание, а также для построения защищенных РАС.

5. Исследованы аналитические риск-модели распределенных автоматизированных систем, подвергающихся синхронному или асинхронному воздействию дестабилизирующих факторов, а также проведена оценка и регулирование общего риска системы при данных воздействиях.

6. При решении задач, применительно к проблематике работы, эффективно использован комплекс базовых методов исследования, таких как метод системного анализа, теории риска, теории вероятности, математической статистики.

7. В работе изложены подходы к оценке и регулированию риска в распределенных автоматизированных системах, на основании которых разработана методика обработки риска реализации спам-атак на компоненты РАС, плотность вероятности наступления ущерба в которых имеет бета-распределение.

8. Выявлена проблема поиска минимумов суммарного риска информационной безопасности распределенной автоматизированной системы, состоящей из нескольких компонент, подвергающихся спам-атакам.

9. В ходе работы изучено влияние внесения нового компонента системы на вид огибающей суммарного риска информационной безопасности распределенной автоматизированной системы, подвергающейся спам-атакам.

10. На основе оценки экстремумов суммарного риска для систем, состоящих из двух компонентов, была произведена оценка экстремумов интегрального риска для систем, состоящих из n компонентов в общем виде, в компонентах которых плотность вероятности наступления ущерба имеют бета-распределение.

11. Основные результаты работы были использованы для построения защищенной распределенной автоматизированной системы, подвергающейся спам-атакам.

12. Полученные результаты исследований имеют практическое применение для повышения защищенности распределенных автоматизированных систем от спам-атак.

13. Решению проблемы защиты распределенных автоматизированных систем от спам-атак посвящено значительное количество работ, однако не существует универсального подхода к управлению рисками. Совершенствование и разработка новых методов управления позволит решить эту проблему.

14. Оценка достоверности полученных результатов исследования основана на проведении анализа статистических данных успешных спам-атак на распределенные автоматизированные системы в период с января 2004 года по март 2012 года.

15. Идея проводимых исследований базируется на обобщении полученных ранее результатов, а также на анализе рисков распределенных автоматизированных систем, компоненты которой подвергаются спам-атакам.

16. При проведении исследований было использовано сравнение данных, полученных ранее по рассматриваемой тематике. Установлено, что полученные

ранее результаты являются неполными, и была выполнена дополнительная обработка данных в ходе выполнения исследования по рассматриваемой тематике.

17. В работе использованы результаты применения современных систем сбора и обработки исходной информации, в частности, сбора и обработки статистических данных.

18. Личный вклад состоит в участии на всех этапах процесса исследования, непосредственном участии в получении исходных данных, участии в апробации результатов исследования, подготовке основных публикаций по выполненной работе.

**Список литературы**

1 А.Таранов, О. Слепов. Безопасность корпоративной системы электронной почты. – JetInfo. -2003. №6.

2 Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. Учебное пособие. -Горячая Линия – Телеком. -2001. -148 с.

3 Галатенко В.А. Основы информационной безопасности. - Интернет-университет информационных технологий - ИНТУИТ.ру, 2008 г.

4 Альянах И.Н. Моделирование вычислительных систем. Л.: Машиностроение. Ленингр. отд-ние, -1988. -233 с.

5 Рудик К.П. Способы сбора сетевой информации о нарушителе. - «Безопасность информационных технологий» М. МИФИ. -2004. - №2.–С. 76-79.

6 Калинин А.В. Применимость Байесовского классификатора для задачи определения спама. Материалы конференции "Проблема спама и ее решения". - 2004.

7 Петенко А., Петренко А.А. Аудит безопасности Internet. -М. ДМК Пресс, - 2002.

8 Колмановская Е.С. Спам - болезнь роста Сети. -"Управление защитой информации". -2003. - том 7 №3.

9 Левин М. Руководство для хакеров – М.: Бук пресс, - 2006.

10 Левин М. E-mail «безопасная»: Взлом, «спам» и «хакерские» атаки на системы электронной почты Internet. - М.: Майор, -2002.-189с.

11 Пауэл Т.А, Уитворт Д. HTML - справочник программиста, Москва - Минск: Изд-во –АСТ Харвест”, -2003. - 383 с.

12 Слепов О.И. Борьба со спамом. Информационный бюллетень «JetInfo» №9 от 2004 года. - М.: Джет Инфо Паблишер, -2004.

13 Фейнштайн К. Защита ПК от спама, вирусов, всплывающих окон и шпионских программ. – М.: НТ ПРЕСС, -2006.

14 Харрис Р. Психология массовых коммуникаций (Секреты воздействия). - С-Пб: Изд-во –Прайм-ЕВРОЗНАК”, -2001. - 448 с.

15 Сайт спам-фильтра Яндекс.Спамоборона. – Электрон.дан. – Режим доступа: http://so.yandex.ru.

16 Информационный новостной порталAntiSpamNews. – Электрон.дан. – Режим доступа: http://www.eserv.ru/AntiSpamNews

17 Информационный портал против спама. – Электрон.дан. – Режим доступа: http://spamtrackers.eu/

18 Ашманов И. Как и где фильтровать спам? -Электронный журнал «Спамтест» - 17 июня 2003. – Электрон.дан. –Режим доступа: http://www.spamtest.ru/document?pubid=1&context=1.

19 Бекетов Хасан. Незаконные рекламные рассылки старше интернета. – Электрон.дан. - Режим доступа: http://www.compulenta.ru/dk/slydecision/24993/.

20 Борьба со спамом: история и методы. – Электрон.дан. –Режим доступа: http://bio.fizteh.ru/student/diff_articles/no_spam.esp.

21 KasperskyAnti-Spam. – Электрон.дан. –Режим доступа: http://www.kaspersky.ru/anti-spam .

22 Apache Software Foundation. The Apache SpamAssassin Project– Электрон. дан. – Режимдоступа: http://spamassassin.apache.org .

23 Использование правил для фильтрации спама./Фильтрация спама по стоп-словам в теме писем. –Электрон.дан. - Режим доступа: http://antispamsniper.com/ru/art_rules.html .

24 Барабаши А. Л., –Сети без масштабов”, В мире науки. ScientificAmerican, - 2003. № 8, С. 55–63

25 Венцель Е.С. Теория вероятности — 1969 г. — 564 с.

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

27 Воробьев Н. Н. Теория игр для экономистов-кибернетиков.—М.: Наука, 1985.Гантмахер Ф. Р., Теория матриц, 4-е изд., Наука, М., -1988, -272 с.

28 Ахо А., Хопкрофт Дж., Ульман Д., «Структуры данных и алгоритмы». - Вильяме, -2000.

29 ГоловановС.А. Kaspersky Security Bulletin. Развитие угроз в 2008 году, статья, 2008 – Электрон.дан. – Режим доступа: http://www.securelist.com/ru/downloads/vlpdfs/ksb_part1.pdf .

30 Переводы и публикации сотрудников компании НИП «Информзащита», – Электрон.дан. – Режим доступа: http://www.infosec.ru/press/pub_main.html.

31 Емельянов В.В., Курейчик В.В., Курейчик В.Н. Теория и практика эволюционного моделирования. – М: Физматлит, -2003. -432 с.

32 Иванов В. П. Математическая оценка защищенности информации от несанкционированного доступа // Специальная техника. -2004. N 1. С. 58—64.

33 Куканова Н. Методы и средства анализа рисков и управление ими в ИС // Byte/Россия. -2005. № 12. С. 69—73.

34 Ландау Л. Д., Лифшиц Е.М. Курс теоретической физики.—М.: Физ-матлит, -1968.-618с.

35 Лифшиц Ю. А. Структура ложных сетей, –Алгоритмы для интернета” - 2006.-14 с.

36 Лукацкий А.В. Безопасность Commerce. Системы безопасности, связи и телекоммуникаций. -2000. №4, С. 24-26.

37 Лукацкий А.В. Как защититься от хакеров? Документальная электросвязь. -2000. №3. 48-50с.

38 Лукацкий А.В. Комплексный подход к обеспечению информационной безопасности. – Системы безопасности, связи и телекоммуникаций. -1998. – №1. – 50 с.

39 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.

40 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/ .

41 Малишевский А. В., Качественные модели в теории сложных систем, Наука, М., -1998, -432с.

42 Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET. – М.: НПО Мир и семья-95, -1997. – 296 с.

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

44 Мэзон С. Электронные цепи, сигналы и системы / С. Мэзон, Г. Циммерман. - М.: ИЛ, -1963. – 360 с.

45 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — СПб.: Питер, -2001. — 672 с.

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

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

48 Остапенко А.Г. Анализ и синтез линейных радиоэлектронных цепей с помощью графов: Аналоговые и цифровые фильтры. - М.:
Радио и связь, -1985. - 280 с.

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

50 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.

51 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.

52 Д.О.Глухов Риск-анализ компьютерных преступлений на основе статистических данных. – Информация и безопасность. -2009. 549-558 с.

53 Ю.К. Язов Основные стратегии защиты информации в компьютерных системах. – Информация и безопасность. -2008. 118-122с.

54 Оуэн Г., Теория игр, г. Москва, Мир, -1971.-229 с.

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

56 Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, -2000. – 368 с.

57 Поспелов Д.А. Логико-лингвистические модели в системах управления. – М.: Энергоиздат, -1981. – 232 с.

58 Руководящий документ ГостехкомиссииРоссии "Защита от несанкционированного доступа к информации. Термины и определения". М.: ГТК РФ, -1992. — 13 с.

59 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. М.: Издательский дом Дашков и К, -2005. – 335 с.

60 Соложенцев Е.Д. Особенности логико-вероятностной теории риска с группами несовместимых событий// АиТ. – 2003. - №3.

61 Тоффлер Э. Третья волна. - М.АСТ, -2002.

62 Уэбстер Ф. Теории информационного общества / Фрэнк Уэбстер; Пер. с англ. М.В.Арапова, Н.В.Малызиной; под ред. Е.Л.Вартановой. – М.: Аспект Пресс, -2004. – 400 с.

63 Чхартишвили А. Г., Теоретико-игровые модели информационного управления, ПМСОФТ, М., -2005. С. 587-604.

64 Шмидский Я. К. MATHEMATICA 5. Самоучитель. М.: Диалектика, -2004. 592 с.

65 LaurentOudot, «FightingSpammersWithHoneypots». – Электрон.дан. – Режим доступа: http://www.securityfocus.com/infocus/1747.

66 Deirdre Day-MacLeod, «Viruses and spam». -New York : Rosen Central, 2008.

67 Albert R, Jeong H, Barabasi A-L. 1999. Diameter of theWorld-WideWeb. Nature 401:130–31.

68 Anderson RM, May RM. 1991. Infectious Diseases of Humans. Oxford: OxfordUniv. Press :37.

69 Axelrod, Robert (1997), The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration, Princeton: Princeton University Press.

70 Bailey N. The Mathematical Theory of Infectious Diseases and Its Applications.—New York: Hafner Press, 1975:67.

71 Bailey NTJ. 1975. The Mathematical Theory of Infectious Diseases and Its Applications. New York: Hafner: 120.

72 Barabasi A-L, Albert R, Jeong H. 2000. Scalefree characteristics of random networks: the topology of the World Wide Web. Physica A 281:69–77.

73 Bollobas B. 1998. Modern Graph Theory. NewYork: Springer: 71–102.

74 Broder A, Kumar R, Maghoul F, Raghavan P, Rajagopalan S, et al. 2000. Graph structure in the web. Comput. Netw. 33:309–20.

75 Eguffluz V., Klemm K. Epidemic Threshold in Structured Scale-free Networks / Physical Review Letters. 2002. № 89. P. 108701.

76 F. Cohen, –Computer Viruses: Theory and Practice", Computers & Security, vol. 6, pp. 22–35, Feb. 1987.

77 Goldenberg J., LibaiB., Muller E. Talk of the Network: A Complex Systems Look at the Underlying Process of Word-of-Mouth / Marketing Letters. 2001.
№ 2. P. 11-34.

78 Granovetter MS. 1973. The strength of weak ties. Am. J. Sociol. 78:1360–80.

79 J. C. Frauenthal. Mathematical Modeling in Epidemiology, Springer-Verlag, New York, 1980.

80 J. O. Kephart and S. R. White. –Measuring and Modeling Computer Virus Prevalence", Proceedings of the IEEE Symposium on Security and Privacy, 1993.

81 Kempe D., Kleinberg J., Tardos E. Maximizing the Spread of Influence through a Social Network / Proceedings of the 9-th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2003. P. 137-146.

82 Kephart, J.O., White, S.R.: Directed-graph epidemiological models of computer viruses. In: IEEE SymposiumonSecurityandPrivacy.

83 Kermack WO, McKendrick AG. 1927. A contribution to the mathematical theory of epidemics. Proc. R. Soc. London Ser. A 115:700–21.

84 Kuperman M, Abramson G. 2001. Small world effect in an epidemiological model. Phys. Rev. Lett. 86:2909–12.

85 Leskovec, J, Krause, A, Guestrin, C, Faloutsos, C, VanBriesen, J, and Glance, N. Costeffective outbreak detection in networks. In 13th ACM SIGKDD International onference on Knowledge Discovery and Data Mining, 2007.

86 May RM, Lloyd AL. 2001. Infection dynamics on scale-free networks. Phys. Rev. E 6406:066112.

87 Newman, M. E. J. and Watts, D. J., Scaling and percolation in the small-world network model, Phys. Rev. E60, 7332-7342 (1999).

88 Newman. M. E. J. A measure of betweenness centrality based on random walks, 2003.

89 O'sullivan,D. and Haklay, M.Agent-based models and individualism: Is the world agent-based? Environment and Planning A32:1409-25,2000.

90 Pastor-Satorras, R. and Vespignani, A., Epidemic spreading in scale-free networks, Phys. Rev. Lett. 86,3200-3203 (2001).

91 Potterat JJ, Rothenberg RB, Muth SQ. 1999. Network structural dynamics acid infectious disease propagation. Int. J. STD AIDS 10:182–85.

92 RiskWatch Official website// Risk Watch, Inc. Available at: http://www.riskwatch.com/.

93 Rogers EM. 1995. Diffusion of Innovations. New York: Free Press. 519.

94 Solomonof, R. and Rapoport, A., Connectivity of random nets, Bulletin of Mathematical Biophysics 13, 107-117 (1951).

95 Watts D., Dodds P. Influentials, Networks, and Public Opinion Formation // Journal of Consumer Research. — December, 2007. — P. 123—134.

96 Watts DJ. 2002. A simple model of information cascades on random networks. Proc. Natl. Acad. Sci. USA 99:5766–71.

97 West DB. 1996. Introduction to Graph Theory. Upper Saddle River, NJ: Prentice Hall.

98 Википедия — свободная энциклопедия – Электрон.дан. – Режим доступа: http //ru.wikipedia.org.

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

100 Glossary on control Theory and its Applications –URL http://glossary.ru.

101 Oxford English Dictionary –URL http://askoxford.com.

102 Protect lab – URL http://protectlab.com.

103 Информационный новостной портал. – Электрон.дан. – Режим доступа: http://planetasmi.ru/.

104 Информационный портал по безопасности Securelist.com. – Электрон.дан. – Режим доступа: http://www.securelist.com.

105 Остапенко Г.А. Карпеев Д.О. Методическое и алгоритмическое обеспечение расчета рисков распределенных систем на основе параметров рисков их компонент. // Информация и безопасность: Регион.науч-техн. журнал. – Воронеж. 2010. Вып. 3., С. 373-380.