СОДЕРЖАНИЕ

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



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

# ВВЕДЕНИЕ

**Актуальность исследования.**

Актуальность обеспечения информационной безопасности телекоммуникационных систем возрастает в связи с рядом объективных причин. Одна из них это высокий уровень популярности ИТКС, которым доверяют самую ответственную работу, от качества которой зависит жизнь и благосостояние многих людей. При этом ИТКС, открывая новые возможности в организации человеческой деятельности, повышения ее качества и эффективности, в то же время становятся одной из наиболее уязвимых компонент, притягивая к себе злоумышленников, как изнутри, так и из вне [3].

Сегодня с помощью ИТКС в электронном режиме может производиться учет, открывать кредиты, переводиться значительные суммы, поэтому незаконное манипулирование информацией подобного характера может привести к серьезным ущербам. Кроме того, данные циркулирующие в ИТКС, затрагивают интересы большого количества юридических и физических лиц. Как правило, информация конфиденциальна. В то же время она должна быть доступна и актуальна, что обуславливает существенную ответственность ИТКС за обеспечение вышеуказанных качеств информации [48, 25].

Всплеск многообразия используемых системно-технических платформ и номенклатуры сетевых сервисов приводит к расширению списка уязвимостей ИТКС и повышает требования к средствам их защиты. Установка в ИТКС стандартных средств защиты таких, как межсетевые экраны, виртуальные частные сети, средства защиты от несанкционированного доступа и пр. является необходимым, но уже не достаточным условием построения надежной и эффективной безопасности [25, 28].

Отсюда вытекает необходимость снижения уровня риска ИТКС от реализации внутренних и внешних угроз и, в конечном счете, минимизации ущерба от деструктивных деяний. В такой ситуации базовой процедурой является риск-анализ, который позволит всесторонне исследовать атакуемые

ИТКС организации, оценить текущий уровень состояния ИБ, выявить уязвимые места в системе защиты, создать модели возможных угроз ИТКС, проверить правильность подбора и настройки средств защиты при реализации атак [48].

В результате риск-анализа ИТКС выявляются уязвимые технологические потоки как электронной, так и бумажной информации, топологии сети, незащищенные или неправильные сетевые соединения, производится анализ настроек межсетевых экранов и других средств защиты. Целью проведения такого анализа является разработка ряда методик, моделей и организационных документов, которые в дальнейшем могут явиться основой для построения защищенной ИТКС.

В этой связи чрезвычайно актуальной является задача нахождения универсальных методик и алгоритмов управления информационными рисками, базирующихся на анализе возможного ущерба ИТКС от ожидаемых атак [3].

Сетевые атаки на ИТКС, вредоносными программами –сетевые черви" становятся панацеей нынешнего времени.

Любая ИТКС может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трѐх свойств информации - конфиденциальности, целостности или доступности. Рассмотрим эти свойства более подробно. Свойство конфиденциальности позволяет не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам [38].Характерным примером нарушения конфиденциальности информации является кража из системы секретной информации с целью еѐ дальнейшей перепродажи. Целостность информации подразумевает еѐ способность не подвергаться изменению или уничтожению в результате несанкционированного доступа. В качестве примера нарушения этого свойства можно привести ситуацию, при которой злоумышленник

преднамеренно искажает содержимое одного из электронных документов, хранящихся в системе [5]. И, наконец, доступность информации определяется как еѐ свойство быть доступной и используемой по запросу со стороны любого уполномоченного пользователя. Таким образом, в результате нарушения конфиденциальности, целостности или доступности информации злоумышленник тем самым может нарушить бизнес-процессы компании[1,4].

Основной ущерб в ИТКС от атак вредоносных программ «сетевые черви» является потеря информации, документов, баз данных, программного обеспечения, видео-аудио и тд., то есть риском является полное или частичное уничтожение данных.

Одни из первых экспериментов по использованию компьютерных червей в распределѐнных вычислениях были проведены в исследовательском центре Xerox Альто Джоном Шочем (John Shoch) и Йоном Хуппом (Jon Hupp) в 1978 году. Термин возник под влиянием научно-фантастических романов Дэвида Герролда «Когда ХАРЛИ исполнился год» и Джона Браннера «На ударной волне» [5].

Зачастую «сетевые черви» даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счѐт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве, также из зараженных ИТКС возможна организация ботнета для проведения сетевых атак[5,13].

Одним из наиболее известных компьютерных червей является «Червь Морриса», написанный Робертом Моррисом-младшим, который был в то время студентом Корнельского Университета. Распространение червя началось 2 ноября 1988, после чего червь быстро заразил около 10 % всех компьютеров, подключѐнных в то время к Интернету [38].

Актуальность данной работы заключается в разработке методики оценки рисков при воздействие на ИТКС атак вредоносными программами

«сетевой червь», а также выработка предложений об увеличении эффективности существующих механизмов противодействия данным атакам.

**Степень научной разработанности.**

В настоящее время активно ведутся исследования возможности применения, для обеспечения информационной безопасности различных автоматизированных систем, риск-моделей различных атак на компоненты распределенных систем и возникающих от их реализации ущербов[3]. Многовариантность и непредсказуемость таких атак не позволяют создать детерминированное описание описания этих процессов и возникающих от их реализации ущербов. Поэтому, при создании защищенных автоматизированных систем, вполне обоснованно рассмотрение ущерба как случайной величины. В этом случае описание принято осуществлять с использованием различных законов распределения, среди которых наибольшей популярностью пользуются регулярные законы [93].

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

**Объект исследования.** Объектом исследований является распределенная локальная вычислительная сеть, как цель программно-математического воздействия типа «сетевые черви».

**Предмет исследования.**Методы оценки и регулирования рисков в распределенной локальной вычислительной сети, являющихся целью атак, направленных на реализацию программно-математического воздействия типа «сетевые черви».

**Цель и задачи исследования.**

Целью настоящей работы является исследование и разработка подходов для оценки и регулирования рисковвраспределенной локальной вычислительной сети, подвергающихся угрозам программно-математического воздействия типа «сетевые черви».

Для достижения поставленной цели в работе решались следующие задачи:

1. Анализ уязвимости враспределенной локальной вычислительной сети, которые могут быть использованы для реализации программно-математического воздействия типа «сетевые черви».

2. Оценка вероятности реализации угроз программно-математического воздействия типа «сетевые черви», в распределенной локальной вычислительной сети.

3. Оценка ущерба от реализации гроз программно-математического воздействия типа «сетевые черви», в распределенной локальной вычислительной сети.



4. Вычисления рискаот реализации угроз программно-математического воздействия типа «сетевые черви», в распределенной локальной вычислительной сети.

5. Регулирование рисковот реализации угроз программно-математического воздействия типа «сетевые черви», в распределенной локальной вычислительной сети.

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

**Методы исследования.**



Для реализации намеченной цели исследования и решения поставленных задач используются методы построения систем защиты информации, теории рисков, теории вероятности, математической статистики и системного анализа, теории информации, методы имитационного моделирования.

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

1. Определена линейная зависимость количественной меры ущерба и атак через коэффициент Пирсона;

2. Предложена математическая модель, учитывающая возможность показательного распределения оценки и регулирования рисков

3. Разработана характеристика общего риска системы, состоящей из одной-двух и n- независимых друг от друга компонентов.

**Научная новизна исследования.**

1. Получена зависимость силы линейной зависимости ущерба и атак;

2. Обоснована возможность применения показательного распределения;

3. Получена характеристика общего риска системы, состоящей из одной-двух и n- независимых друг от друга компонентов.

**Практическая ценность** работы заключается в разработке подхода общего риска системы, которая состоит из одной-двух и n- независимых друг от друга компонентов.

# СПИСОК ЛИТЕРАТУРЫ

1 Богатырев В.А. Надежность компьютерных сетей//Информационные технологии. -2006 -№ 9. С. 25-30.

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

3 Володин А.В., Устинов Г.Н. Сеть передачи данных —модель угроз информационной безопасности // Вестник связи. 1999, № 4, С. 52-57.

4 Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 09.09.2000.

5 Ефремов А. Сетевые атаки и средства борьбы с ними // Computer Weekly № 14, 1998, С. 14-17.

6 Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. Учебное пособие. Е.А. Карпов, И.В. Котенко, М.М. Котухов, А.С. Марков, Г.А. Парр, А.Ю. Рунеев. СПб.:ВУС, 2000. 190 с.

7 Злобина И.А. Экономика информационной безопасности: учеб. пособие / И.А. Злобина –Воронеж: Воронежский государственный технический университет, 2005. – 196 с.

8 Карайчев Г.В., Нестеренко В.А. Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети. Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки. 2008, №1, С.10-13.

9 Карпов Ю. Имитационное моделирование систем. Введение в моделирование с Anylogic 5. -СПБ.: БВХ-Петербург, 2005. - 400 с.

10 Колмогорцев Е.Л. Модель производительности распределенной иерархической системы управления с резервированием коммуникационной

подсистемы//Информационные технологии моделирования и управления. - 2006 -№ 9(34). С. 1172-1178.

11 Концепция национальной безопасности Российской Федерации. Утверждена указом Президента РФ от 17 декабря 1997 года №1300.

12 Котенко И.В., Степашкин М.В., Михайлов Д.Ю. Система сбора анализа и хранения данных аудита работы пользователей // Методы и технические средства обеспечения безопасности информации. Материалы XII общероссийской научно-технической конференции. 4-5 октября 2004 года, Санкт-Петербург. Издательство политехнического университета. 2004. С. 23-25.

13 Котенко, И. В. Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации И. В. Котенко, М. В. Степашкин, В. Богданов Изв. вузов. Приборостроение. СПб, 2006. С. 13-18.

14 Котенко, И. В. Модели и методика интеллектуальной оценки уровня защищенности компьютерных сетей И. В. Котенко, М. В. Степашкин, В. Богданов Труды Международных научно-технических конференций «Интеллектуальные системы (AIS-06)» и «Интеллектуальные САПР (CAD-2006)». М Физматлит, 2006. С. 321-322.

15 Котенко, И. В. Модель атак для имитации действий злоумышленника в системе анализа защищенности компьютерных сетей И. В. Котенко, М. В. Степашкин, В. Богданов Труды IV Межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2005)». С. 22-25.

16 Котенко, И. В. Прототип имитатора информационной системы: архитектура и сценарии проведения экспериментов И. В. Котенко, М. В. Степащкин Труды конференции «Информационная безопасность регионов России (ИБРР-2003)». СПб.: Издательство Политехника, 2003. С. 68-72

17 Ларичев О.И. Теория и методы принятия решений / О.И. Ларичев М.: Логос, 2002.-392 С. 123-125.

18 Лукацкий А.В. Обнаружение атак.: БХВ-Петербург, 2001. 128 с.

19 Магауенов Р.Г. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. / Р.Г. Магауенов. – М.: Мир и безопасность, 1997 – №1. – С.118-126.

20 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов / А.А. Малюк М.: Горячая линия – Телеком, 2004. С. 125-131.

21 Матвеевский В.Р. Надежность технических систем. Учебное пособие – Московский государственный институт электроники и математики. М., 2002 г. С. 28-30.

22 Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 18.05.2007.С. 121-122.

23 Мишин К.Н. Имитационное моделирование аномальных явлений в компьютерных сетях. Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. 2007, 120 с.

24 Общие требования безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 18.05.2007.

25 Олифер В., Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. - СПБ.: Питер, 2010.944 с.

26 Остапенко А.Г. Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств / А.Г. Остапенко, Ю.К. Язов, Р.В. Батищев, О.А. Середа // Информация и безопасность. – 2001. – №2.С. 4-11.

27 Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. – 2005. – Вып. 2.С. 28-32.

28 Павлов А.А. Основы системного анализа и проектирования автоматизированных систем управления: учеб. пособие / А.А. Павлов. – Киев: Выща школа, 1991. 364 с.

29 Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2004. 384 с.

30 Прангишвили И.В. Системные закономерности и системная оптимизация / И.В. Прангишвили, В.Н. Бурков. – М.: Синтег. 2004. – 208 с.

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

32 Пугачев В.С. Теория вероятностей и математическая статистика: учеб. пособие. – 2-е изд., исправл. и дополн. – М.: ФИЗМАТЛИТ, 2002. 496 с.

33 Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 19.11.2007.

34 Риндле К. Динамические инфраструктуры. Журнал сетевых решений/LAN. 2010, №7.31 с.

35 Руднев М. Хранение данных и, резервное копирование в сетях. Компьютер-Пресс, 2000, № 7 (Тематический выпуск: хранение и защита данных), С. 40-43.

36 Селезнев А.В. Организация резервного копирования в локальных и корпоративных сетях. Сети и системы связи. 1996, № 10.С. 110-111.

37 Смирнов Н.В., Дунин-Барковский И.В. Краткий курс математической статистики для технических приложений. – М.: Физмагиз. 1959.

38 Соколов А.В., Методы информационной защиты объектов и компьютерных сетей, изд. Полигон, 2000 г.С. 51-53.

39 Спитцнер Л. HoneynetProject: ловушка для хакеров // Открытые системы, № 07, 2003 С. 25-27.

40 Степашкин М.В. Модели и методика анализа защищенности компьютерных. / Санкт-Петербург. С. 196-198.

41 Строгалев В.П., Толкачева И.О. Имитационное моделирование: Учеб. пособие. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. С. 280-289.

42 Сулицкий В.Н. Методы статистического анализа в управлении / В.Н. Сулицкий. – М.: Дело, 2002. С.520-521.

43 Таненбаум Э. Современные операционные системы. 3-е изд. - Спб.: Питер, 2011. 120 с.

44 Торокин А.А. Основы инженерно-технической защиты информации. – М: Ось-89, 1998. 336 с.

45 Трайнер В.А. Информационная безопасность предприятия: учеб. пособие / В.А. Трайнер, А.А. Федулов: Международная академия наук информации, информационных процессов и технологий (МАН ИПТ). – М.: Дашков и К, 2004. – 336 с.

46 Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. -М.: Радио и связь, 1991. -132 с.

47 Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

48 Царегородцев А.В. Информационная безопасность в распределенных управляемых системах А.В. Царегородцев. – М.: РУДН, 2003. – 217 с.

49 Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: учеб. пособие для вузов/ А.Г. Шоломицкий – М.: Изд. дом ГУ ВШЭ, 2005. – 400 с.

50 Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества / Р. Шторм. – М.: Издательство "МИР", 1970. – 368 с.

51 Шумский А.А. Системный анализ в защите информации: учеб. пособие / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

52 Язов Ю.К. Использование аппарата теории нечетких множеств в интересах комплексной оценки эффективности технической защиты информации в распределенных компьютерных системах / Ю.К. Язов, И.М. Седых // Вестник ВИ МВД России. – 2003. – №3(15). С.179-182.

53 Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах / Ю.К. Язов. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 274 с.

54 Язов Ю.К. Основы технологии проектирования системы защиты информации в информационно-телекоммуникационных системах: Монография / А.В. Аграновский, В.И. Мамай, И.Г. Назаров, Ю.К. Язов. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 260 с.

55 Язов Ю.К., Седых И.М. Метод количественной оценки защищенности информации в компьютерной системе. Телекоммуникации. 2006, №6, С.46-48.

56 Воронцовский А.В. Управление рисками: Учеб. пособие. 2-ое изд., испр. и доп / А.В. Воронцовский – СПб: Изд-во С.-Петерб. ун-та, 2000; ОЦЭиМ, 2004. – 458 с.

57 А. Ф. Чипига Информационная безопасность автоматизированных систем, 2010. – 321 с.

58 Ф. Чипига Информационная безопасность автоматизированных систем, 2010 – 321 с.

59 Гультяев А.К., Интернет, E-mail, Антивирусы , - М.: Бином, 2006. Безруков Н.Н. Компьютерная вирусология. - К.: УРЕ, 1991 – 180 с.

60 Безруков Н.Н. Компьютерные вирусы. - М.: Логос, 2004. – 105 с.

61 Могилев А. В., Пак Н. И, Хѐннер Е. К. Информатика. - М.: ИНФРА-ДАНА, 2004. – 120 с.

62 Мостовой Д.Ю. Современные технологии борьбы с вирусами. - М.: ИНФРА-М, 2011 – 178 с.

63 Айвазян С.А. Прикладная статистика: Исследование зависимостей / С.А. Айвазян – М.: Финансы и статистика, 1985 – 423 с.

64 Андреев Д.А., Тишков С.А., Сердечный А.Л., Плотников Д.Г. К вопросу о классификации атак типа ―Отказ в обслуживании‖. // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 1. С. 47-54.

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

66 Бартон Т. Комплексный подход к безопасности сетей / Т. Бартон, У. Шенкир, П. Уокер. – М.: Издательский дом "Вильямс", 2003. – 208 с.

67 Бостанджиян В.А. Пособие по статистическим распределениям/ В.А. Бостанджиян. - Черноголовка: ИПХФ, 2000. – 106 с.

68 Буянов В.П. Рискология (управление рисками): Учебное пособие. – 2-ое изд., испр. и доп. / В.П. Буянов, К.А. Кирсанов, Л.М. Михайлов. – М.: Издательство "Экзамен", 2003. – 384 с.

69 В. М. Шишкин Степенное распределение и управление рисками критических систем // Труды ИСА РАН 2007. Т. 31. – 401 с.

70 Воронцовский А.В. Управление рисками: Учеб. пособие. 2-ое изд., испр. и доп / А.В. Воронцовский – СПб: Изд-во С.-Петерб. ун-та, 2000; ОЦЭиМ, 2004. – 458 с.

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

72 Вычислительные системы, сети и телекоммуникации. Пятибратов и др. – ФИС, 1998. – 262 с.

73 Герик Т. Информационная база для оценки риска / Т. Герик //LAN: журнал сетевых решений, 2006. – №9. – С. 22-25.

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

75 Гончаренко Л.П. Риск-менеджмент: учебное пособие / Под ред. д-ра тех. наук. проф., засл. деятеля науки РФ Е.А. Олейникова; Л.П. Гончаренко, С.А. Филин. – М.: КНОРУС, 2006. – 216 с.

76 Гончарова Г.А. Элементы дискретной математики.– М.: 2003.– 127 с.

77 Гражданкин А.И. Использование вероятностных оценок при анализе безопасности опасных производственных объектов. / А.И. Гражданкин, М.В. Лисанов, А.С. Печеркин // Безопасность труда в промышленности. – 2001. – № 5. – С. 33-36.

78 Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения / В.М. Гранатуров – М.: Издательство "Дело и Сервис", 2002. – 160 с.

79 Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агентства «Яхтсмен». 1996. – 192 с.

80 Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

81 Дорот В.Л. Толковый словарь современной компьютерной техники / В.Л. Дорот, Ф.А. Новиков. – СПб.: БВХ-Перербург, 2002. – 512 С.

82 Евдокимова Л.С., Бочаров Б.Ф., Цепи Маркова.– Л.: Академия им. Кузнецова Н. Г., 1990. – 105 с.

83 Зима В.М., Молдвян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 С.

84 Зорин В.А. Элементы теории процессов риска. / В.А. Зорин, В.И. Мухин. – Н. Новгород: ННГУ.2003. С. 25-27.

85 Зражевский В.В. Основные направления совершенствования системы управления рисками / В.В. Зражевский. – М. С. 1999. – 465 с.

86 Кулаков В.Г. Концепция региональной информационно-аналитической системы в интересах обеспечения информационной безопасности// Информация и безопасность.– 2004. №1. С.114-118.

87 Лукацкий А.В. Обнаружение атак. СПб.: БХВ - Петербург, 2001 624 с.

88 Мак-Клар С. Секреты хакеров. Безопасность сетей – готовые решения, 2-е издание / С. Мак-Клар, Д. Скембрей, Д. Курц. – М.: Издательский дом «Вильямс», 2005г. С. 656-658.

89 Медведовский И.Д. Атака через Internet / И.Д. Медведовский, П.В. Семьянов, В.В. Платонов; под. ред. П.Д. Зегжды — СПб.: Мир и семья, 1997. — 296 с.

90 Михайлов С.Ф., Петров В.А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. – М.: МИФИ, 1995. С. 112-114.

91 Молчанов А.А. Моделирование и проектирование сложных систем. - К.: Высшая школа, 1988. С. 359-362.

92 Теория измерения. А.А. Новоселов. – Новосибирск: Наука 2001 212 с.

93 Остапенко А.Г. Функция возможности в оценке рисков, шансов и эффективности систем. // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 1., С. 17-20.

94 Остапенко А.Г., Линец Е.А., Пархоменко Д.А. Исследование компьютерной преступности на основе статистического риск-анализа // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 2., С. 185-202.

95 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.



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