На правах рукописи

Строкань Дмитрий Александрович

ИММУННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: МОДЕЛИРОВАНИЕ И АНАЛИЗ ПОТРЕБИТЕЛЬСКОГО КАЧЕСТВА

Специальность 08.00.13 – Математические и инструментальные методы экономики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата экономических наук

Ростов-на-Дону – 2012

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Ростовский государственный экономический университет (РИНХ)».

Научный руководитель: доктор экономических наук, доцент
Тищенко Евгений Николаевич

Официальные оппоненты: Щербаков Сергей Михайлович
доктор экономических наук, доцент,
ФГБОУ ВПО «РГЭУ (РИНХ)», проф. каф. экономической информатики и автоматизации управления

Коротаев Никита Васильевич
кандидат экономических наук,
ООО «Офисный мир КМ»,
ведущий программист

Ведущая организация: ФГАОУ ВПО «Южный федеральный университет»

Защита состоится «24» мая 2012 года в 13:30 на заседании диссертационного совета ДМ 212.209.03 в ФГБОУ ВПО «РГЭУ (РИНХ)» по адресу: 344002, г. Ростов-на-Дону, ул. Б. Садовая 69, ауд. 302.

С диссертацией можно ознакомиться в научной библиотеке Ростовского государственного экономического университете (РИНХ).

Электронная версия автореферата размещена на официальном сайте ВАК Минобрнауки России: http://vak2.ed.gov.ru, а также на сайте ФГБОУ ВПО «РГЭУ (РИНХ)» www.rsue.ru.

Автореферат разослан «20» апреля 2012 года.

Ученый секретарь диссертационного совета И.Ю. Шполянская

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В последние годы большое внимание уделяется вопросам защиты информации, накапливаемой, хранимой и обрабатываемой в информационных системах, о чем свидетельствуют публикации в отечественной и зарубежной печати. Особую роль в области информационной безопасности занимают вопросы создания иммунных информационных систем.

Отмечено, что принципы работы и механизмы иммунной системы используются для построения алгоритмов анализа данных, оптимизации и распознавания, систем информационной безопасности, оценки финансовых рисков и других приложений. Системы, строящиеся по аналогии с естественной иммунной системой, называются искусственными иммунными системами.[1]

В диссертационном исследовании под иммунной информационной системой понимается система, способная противостоять программным кодам деструктивного воздействия, сохраняя свою целостность и функциональность. Предустановленный иммунитет обусловлен имеющимися в программно-аппаратных базовых составляющих (например, операционная система) защитными механизмами и механизмами контроля протекающих в них процессов. Приобретенный иммунитет формируется за счет конфигурирования и установки дополнительных элементов защиты.

Под автономными программными кодами деструктивного воздействия понимаются программные коды, функционирующие независимо от пользователя после первоначальной их активации, обладающие мобильностью и нарушающие конфиденциальность, целостность и функциональность информационных систем.

Актуальность данной проблемы обусловлена ростом атак с применением автономных программных кодов деструктивного воздействия на информационные системы, что влечет за собой целый спектр различного рода убытков. По статистическим данным «Лаборатории Касперского» в 2008 году было зафиксировано 23680646 атак на пользователей через интернет, в 2009 году — 73619767, в 2010 году это число составило 580371937. Ущерб от программных кодов деструктивного воздействия – одна из основных статей убытков в сфере информационных технологий. Библиография по исследуемой проблеме насчитывает сотни наименований. Проводятся различные конференции и семинары, на которых обсуждаются вопросы, связанные с построением систем защиты от программных кодов деструктивного воздействия (ежегодная конференция Virus Bulletin и др.). Вопросы построения иммунных информационных систем включены в

1 Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты. Пер. с англ. под ред А.А. Романюхи. — М.: ФИЗМАТЛИТ, 2006. — 344 с.

программу подготовки специалистов в области информационной безопасности и информационных технологий. Сформировался значительный рынок программных средств защиты от программных кодов деструктивного воздействия, на котором представлены разработки как отечественных, так и зарубежных компаний (решения от Лаборатории Касперского, ESET NOD32, Dr.Web, Symantec, McAfee и др.).

Процессы глобализации и информационной интеграции, происходящие в мировой экономике, приводят к применению иммунных распределенных информационных систем, вследствие чего усложняются средства, методы и формы защиты, все более обостряется проблема оценки их качества, выработки критериев, которым должен соответствовать тот или иной тип системы защиты. Это особенно актуально в контексте создания, внедрения и эксплуатации комплексных систем защиты от программных кодов деструктивного воздействия для распределенных информационных систем, в связи с тем, что именно защищенность как показатель потребительского качества иммунных распределенных информационных систем выходит в современных условиях на первый план.

Известно, что при организации тех или иных сетевых и телекоммуникационных топологий потенциальная уязвимость информационной системы от программных кодов деструктивного воздействия резко возрастает. Это обуславливается возникновением много вариантности возможных каналов доступа к процессорным узлам сети, массивам хранимой информации и сегментам сетевых топологий.

Представляется, что именно задача создания иммунных информационных систем является наиболее актуальной, так как качественная реализация защиты от автономных программных кодов деструктивного воздействия позволяет перекрыть практически все каналы воздействия на информационные системы.

Степень разработанности проблемы. Вопросам оценки качества информационных систем посвящено множество трудов отечественных и зарубежных ученых: Г.Н.Хубаева, Е.Н.Тищенко, Е.Н.Ефимова, И.Ю.Шполянской , А.И.Долженко, С.М.Щербакова, В.И.Конявского, Г.А.Титоренко, В.В.Дика, А.Н.Ткачева, Дж.Брауна, Г.Майерса, и других.

Вопросам информационной безопасности посвящены работы: Г.Н.Хубаева, Е.Н.Тищенко, А.А.Малюка, О.Б.Макаревича, В.В.Домарева, А.А.Кононова, С.А.Петренко и других.

Вопросам создания иммунных информационных систем посвящены работы: Ю.С.Булыгин, С.В.Новикова, Д.В.Бабинина, Р.Ривеста, Б.Шнайера, Дж.Брауна.

Ими были проанализированы отдельные методы и средства защиты, рассмотрены некоторые существующие системы.

Однако, нам не известны опубликованные в открытой печати исследования, посвященные сравнительному анализу и совершенствованию механизмов защиты от автономных программных кодов деструктивного

воздействия при построении иммунных информационных систем. Также нет работ, посвященных выбору оптимальной структуры системы защиты от программных кодов деструктивного воздействия для информационной системы.

Таким образом, актуальность работы обусловлена потребностью выделения критериев и разработки методологических подходов к оценке потребительского качества механизмов защиты и поиска путей совершенствования структуры комплексной системы защиты от программных кодов деструктивного воздействия для информационных систем.

Задача построения иммунной информационной системы должна разбиваться на такие подзадачи как качественная сегментация топологии информационной системы, оптимальный выбор программных средств защиты от программных кодов деструктивного воздействия, повышение отказоустойчивости центров управления системой защиты.

Целью диссертационного исследования является развитие инструментария оценки потребительского качества механизмов защиты от программных кодов деструктивного воздействия на основе анализа их параметров и разработки методик для принятия решения при создании, эксплуатации и развитии иммунных информационных систем.

Поставленная в работе цель обусловила решение следующих задач:

- Анализ отечественных и зарубежных исследований, посвященных построению иммунных информационных систем.
- Разработка методики оценки потребительского качества иммунных информационных систем.
- Разработка методики совершенствования системы управления иммунными механизмами информационных систем.
- Программная реализация модуля статистической отчетности работы иммунных механизмов защиты информационных систем.

Объектом исследования являются организации и предприятия всех форм собственности, ведомственных принадлежностей и организационно-правовых форм, использующие в своей деятельности иммунные информационные системы.

Предметом исследования являются процессы проектирования и использования иммунных информационных систем.

Теоретическую и методологическую базу исследования составляют научные труды российских и зарубежных ученых по экономико-математическому моделированию, системному анализу, теории выбора и принятия решений, а также теоретические и методологические вопросы построения иммунных информационных систем.

Работа проведена в рамках пунктов Паспорта специальности 08.00.13 – математические и инструментальные методы экономики: 2.6 «Развитие теоретических основ, методологии и инструментария проектирования,

разработки и сопровождения информационных систем субъектов экономической деятельности: методы формализованного представления предметной области, программные средства, базы данных, корпоративные хранилища данных, базы знаний, коммуникационные технологии».

Эмпирической базой исследования явились экспериментальные и статистические данные, собранные в процессе эксплуатации информационных систем ряда организаций, использующих системы защиты от программных кодов деструктивного воздействия. Основные выдвигаемые научные положения и рекомендации экспериментально подтверждены. Поставленные эксперименты составляют основу предлагаемой методологии исследования.

Инструментарий исследования составили классические методы анализа защищенности распределенных информационных систем, методы сравнения программных систем по критерию функциональной полноты, методы целочисленного программирования, а также программные средства общего и специального назначения.

Нормативно-правовой базой исследования являются:

- Федеральный закон от 27.07.2006 г. «Об информации, информационных технологиях и защите информации» № 149-ФЗ.
- ГОСТ Р 51188-98 «Испытания программных средств на наличие компьютерных вирусов».
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

Научную новизну исследования содержат следующие положения:

- Сформирован перечень функциональных операций (более 290), выполняемых программными средствами защиты иммунной информационной системы, включающий проверку составных файлов, восстановление параметров защиты по умолчанию, статистику защиты файлов и др., позволяющий сравнивать системы защиты по критерию функциональной полноты.
- Адаптирована методика определения функциональной полноты программных средств защиты иммунных информационных систем, отличающаяся возможностью контроля соответствия средств защиты перечню функциональных операций, и позволяющая проводить сравнительную оценку иммунных информационных систем по критерию защищенности.
- Предложена методика оценки потребительского качества программных средств защиты иммунной информационной системы, отличающаяся учетом временных характеристик (минимальное, максимальное и вероятное время) блокировки базовых операций, совершаемых программными кодами деструктивного воздействия, и позволяющая определить вероятность преодоления системы защиты

иммунной информационной системы программными кодами деструктивного воздействия за заданное время.

- Предложен алгоритм оценки потребительского качества и совершенствования распределенной системы управления программными средствами защиты иммунной информационной системы, отличающийся учетом таких параметров как удаленность центра управления от программных средств защиты и нагрузка на центр управления. Алгоритм позволяет определить вероятность срабатывания системы управления программными средствами защиты и рассчитать оптимальное количество центров управления по критерию пропускной способности.

Положения диссертации, выносимые на защиту:

- Перечень функциональных операций (более 290), выполняемых программными средствами защиты иммунной информационной системы.
- Методика определения функциональной полноты программных средств защиты иммунной информационной системы на основе перечня выделенных функциональных операций.
- Методика оценки потребительского качества программных средств защиты иммунной информационной системы на основе вероятностного подхода.
- Алгоритм оценки потребительского качества и совершенствования распределенной системы управления программными средствами защиты иммунной информационной системы.

Практическая значимость исследования определяется тем, что основные положения, рекомендации, выводы, модели, методы и алгоритмы ориентированы на широкое использование экономико-математического обеспечения и инструментальных средств и могут быть использованы предприятиями и организациями любых форм собственности для принятия решения в области проектирования, внедрения и эксплуатации иммунных информационных систем.

Апробация и внедрение результатов исследования. Основные положения и выводы диссертационной работы обсуждались на международных и всероссийских конференциях:

- III Межвузовская научно-практическая конференция «Статистика в современном мире: методы, модели, инструменты» (май 2009 г.).
- IV Всероссийская научно-практическая Интернет-конференция «Проблемы информационной безопасности» (июнь 2009 г.).
- Региональная научно-практическая конференция «Экономические информационные системы и их безопасность: разработка, применение, сопровождение » (октябрь 2009 г.).

- III Межрегиональная научно-практическая конференция «Проблемы создания и использования информационных систем и технологий» (декабрь 2009 г.).
- XII Международная научно-практическая конференция «Экономико-организационные проблемы проектирования и применения информационных систем» (май 2011г.).
- IV Межрегиональная научно-практическая конференция «Проблемы создания и использования информационных систем и технологий» (май 2011 г.).

Основные положения, полученные в результате проведенного исследования, используются при чтении курсов специальностей «Организация и технология защиты информации» («Защита информационных процессов в компьютерных системах», «Компьютерная вирусология») и «Прикладная информатика» («Информационная безопасность») в «Ростовском государственном экономическом университете (РИНХ)».

Отдельные результаты представленного научного исследования реализовались в рамках НИР на тему «Разработка иммуностойкого электронного внутреннего документооборота» по договору с РГЭУ (РИНХ) №1293/11 от 01.10.2011 г. Документы, подтверждающие внедрение, прилагаются к диссертации.

Публикации. Основные результаты диссертационного исследования опубликованы в 8 научных работах, 3 из которых – журналы рекомендованные ВАК РФ, общим объемом 2,57 п.л. (лично автора 2,2 п.л.).

Структура работы. Структура диссертации состоит из введения, трех глав, заключения, библиографического списка и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулированы цели и задачи исследования, определены объект, предмет и методы исследования, приведены элементы научной новизны.

В первой главе «Структурные и функциональные особенности иммунных информационных систем» рассмотрены принципы формирования иммунных информационных систем, проведен анализ угроз для информационных систем со стороны автономных программных кодов деструктивного воздействия.

Статистика последних лет показывает рост атак на информационные системы с применением программных кодов деструктивного воздействия (рисунок 1, рисунок 2), что влечет за собой целый спектр разного рода убытков.

Происходит значительное изменение в составе организаторов кибератак и их целей. Целью преступной деятельности все чаще становится получение

денежной прибыли, кража и дальнейшее использование любой доступной информации.

Рисунок 1 – Статистика вредоносных программ

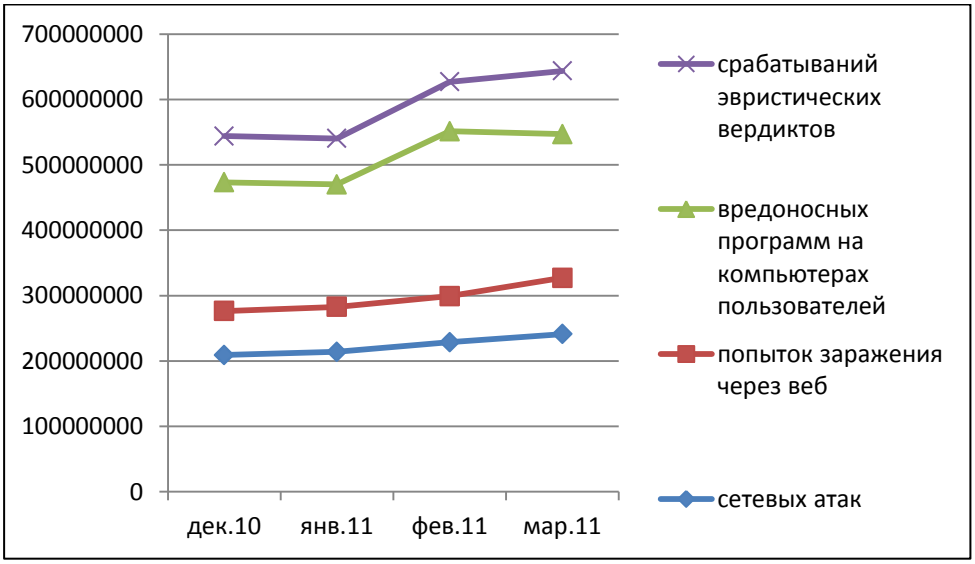


Рисунок 2 – Статистика угроз со стороны автономных программных кодов деструктивного воздействия

Определение качественного сценария при проектировании комплексной системы защиты от программных кодов деструктивного воздействия, а также при последующей модификации ее структуры, является одним из главных условий дальнейшего адекватного функционирования иммунной информационной системы. Данное условие в значительной степени влияет на экономическую эффективность информационной системы.

Рассмотрены наиболее распространенные системы защиты от программных кодов деструктивного воздействия и подходы к построению комплексной системы защиты, выявлены их достоинства и недостатки (таблица 1, таблица 2).

Таблица 1 – Преимущества и недостатки организации системы защиты на базе программных средств одного производителя

Организации КСЗ от ПКДВ на базе ПСЗ одного производителя	
Преимущества	**Недостатки**
Совместимость ПО	Сужение круга систем при выборе оптимального программного решения
Общие антивирусные базы	Проблемы с антивирусными базами
Единая система управления	
Единая точка обслуживания	
Обучение специалистов	

Таблица 2 – Преимущества и недостатки организации системы защиты на базе совокупности программных средств от различных производителей

Организация КСЗ от ПКДВ на базе совокупности ПСЗ от различных производителей	
Преимущества	**Недостатки**
Гибкость и естественная неоднородность	Сложность в освоении
Повышенная вероятность обнаружения	Независимое управление
Локализация заражения	Использование различных антивирусных баз
Более полное соответствие требованиям	Возможные конфликты между продуктами
	Сложности при поддержке

На первый взгляд может показаться, что иммунная информационная система, построенная на базе программных средств одного производителя, является более предпочтительной, так как имеет меньше недостатков. Для небольших организаций это предположение зачастую верно. Однако, при проектировании больших распределенных корпоративных и межкорпоративных информационных систем с большим количеством процессорных узлов, разнообразием структуры и функциональности обрабатываемой информации наиболее предпочтительным является гетерогенный подход к построению иммунных информационных систем, который позволяет учитывать перечисленные выше особенности и стоимостные характеристики систем защиты. Данный вывод подтверждается анализом существующих распределенных информационных систем.

Проектирование комплексной системы защиты от программных кодов деструктивного воздействия является сложнейшей задачей, которая на данный момент не имеет строго описанного метода решения. На основе принципа построения модели сетевого взаимодействия DOD, заключающегося в наличии 4-х уровней и принципе инкапсуляции нижних

уровней в верхние, была разработана схема функционирования и взаимодействия иммунных механизмов информационных систем:

- уровень управления;
- уровень сетевых узлов;
- прикладной уровень;
- уровень компонентов.

Уровень управления. На этом уровне осуществляется управление системой защиты. Уровень управления имеет иерархическую структуру, состоящую из нескольких центров управления, каждый из которых является самостоятельной единицей. Центр управления может состоять из нескольких серверов администрирования, каждый из которых управляет определенным сегментом системы защиты, построенным на базе конкретного программного продукта. В случае использования гетерогенной системы защиты в состав центра управления могут входить сервера администрирования, построенные на базе различных платформ. Управление комплексной системой защиты осуществляется за счет политик безопасности, в которых задаются правила функционирования для всех классов программных средств защиты.

Уровень сетевых узлов. Фактически данный уровень представляет собой категории программных средств защиты, ориентированных на защиту различных процессорных узлов сети (сервера, шлюзы, рабочие станции, мобильные устройства). На этом уровне определяются типы и количество процессорных узлов, происходит их сегментация, определяются соответствующие типы программных средств защиты. Также на этом уровне определяется степень распределенности проектируемой комплексной системы защиты от программных кодов деструктивного воздействия.

Прикладной уровень. Данный уровень представляет собой программное обеспечение, ориентированное на защиту процессорных узлов сети в зависимости от их функционального назначения и операционной системы. Этот уровень влияет на гетерогенность проектируемой комплексной системы защиты от программных кодов деструктивного воздействия, количество лицензий, а также определяет типы политик безопасности.

Уровень компонентов. Этот уровень представляет собой набор модулей, входящих в состав программного обеспечения и ориентированных на защиту от конкретных угроз.

Описанная выше схема позволяет создать шаблон системы защиты от программных кодов деструктивного воздействия на базе сформированного ранжированного перечня функциональных операций, выполняемых системой защиты.

Шаблон системы защиты состоит из:

- набора функциональных операций, выполняемых иммунными механизмами защиты;

- набора функциональных операций, выполняемых системой управления программными средствами защиты.

Для оценки функциональной полноты и выбора программных средств защиты для построения иммунной информационной системы необходимо сравнить полученный шаблон комплексной системы защиты с существующими системами, предлагаемыми производителями.

Таким образом, проведя сравнительный анализ, мы можем построить комплексную информационную систему защиты от программных кодов деструктивного воздействия на основе программных средств защиты, наиболее удовлетворяющих нашим условиям.

Для формирования шаблона системы защиты, оценки потребительского качества и выбора программных средств защиты, был составлен перечень функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами. Также производился анализ перечня функциональных операций для выявления наиболее значимых и важных с точки зрения их применяемости в иммунных информационных системах. Основой для составления перечня послужили программные продукты и информация из научных изданий.

Следует учесть и тот факт, что в данном исследовании необходимо полагаться на эрудированность экспертной группы, так как выявление критериев значимости функциональных операций трудно апробировать на практике.

В качестве экспертов нами выбрано 7 специалистов, обладающих достаточным опытом в исследуемой области, чья профессиональная деятельность непосредственно связана с обеспечением информационной безопасности в организациях.

Опрос экспертов осуществлялся в три этапа. На каждом этапе экспертам выдавалась анкета, в которой необходимо было проранжировать функциональные операции с точки зрения их опыта и предпочтений. При этом сама значительная функциональная операция должна занять первое место, а самая малозначимая – последнее. После каждого тура опроса экспертов знакомили с результатами. Это позволяло каждому эксперту более объективно пройти к решению задачи и при необходимости изменить свое решение.

Обработка результатов каждого тура опроса осуществлялась следующим образом:

- ранжирование каждого эксперта представлялось в виде матрицы упорядочения в канонической форме;
- определялась мера близости (расстояние) Кемени между всеми ранжированиями;
- рассчитывалась матрица рассогласования мнений экспертов;
- выделялись согласованные группы экспертов на основе графа взаимосвязи.

Фрагмент перечня функциональных операций представлен в таблице 3.

Таблица 3 – Фрагмент перечня функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами

№	ЦЕНТР УПРАВЛЕНИЯ	Вес*
1	Создание, перемещение и удаление группы	0,09915
2	Создание структуры групп администрирования	0,09786
3	Структура групп на основе Active Directory	0,09645
4	Структура групп на основе содержимого текстового файла	0,09633
5	Просмотр информации о группе	0,09583
…	…	…
124	Реестр программ	0,00014
	МЕХАНИЗМЫ ЗАЩИТЫ	
125	Использование эвристического анализа	0,09844
126	Проверка составных файлов	0,09760
127	Проверка составных файлов большого размера	0,09742
128	Изменение режима проверки	0,09726
129	Приостановка работы компонента: формирование расписания	0,09663
…	**...**	…
295	Удаление статистической информации для отчетов	0,00008

***** Примечание: весовой коэффициент показывают степень важности той или иной функциональной операции и изменяется от 0 до 1.

Во второй главе «Сравнительный анализ потребительского качества иммунных механизмов защиты распределенных информационных систем» предложен метод, базирующийся на основе алгоритма формальных процедур анализа предметной области, позволяющий на основании списка выделенных ранее характеристик осуществлять сравнительную оценку ряда систем защиты с шаблоном системы защиты от программных кодов деструктивного воздействия, полученным на основе первой главы, и определять количественный показатель соответствия сравниваемых систем заданным характеристикам. В случае отсутствия удовлетворительного результата после использования описанного выше метода целесообразным является построение гетерогенных систем защиты методом сравнительной оценки программных средств защиты для каждого класса защищаемых объектов. Для сравнительно анализа используется методика сравнения сложных программных систем по критерию функциональной полноты[2].

В первом случае для сравнения системы защиты от программных кодов деструктивного воздействия определяется соответствие исследуемой системы шаблону объекта (заданным характеристикам функционирования системы защиты), что выражается количественно при помощи меры подобия Жаккарда.

2 Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (Software & Systems). – 1998. – № 2. – С. 6–9.

Во втором случае следует произвести сравнительный анализ программных средств защиты для каждого класса защищаемых объектов информационной системы (защита рабочих станций, мобильных устройств, файл-серверов, интернет шлюзов и т.д.).

Для анализа использовалось программное обеспечение известных производителей:

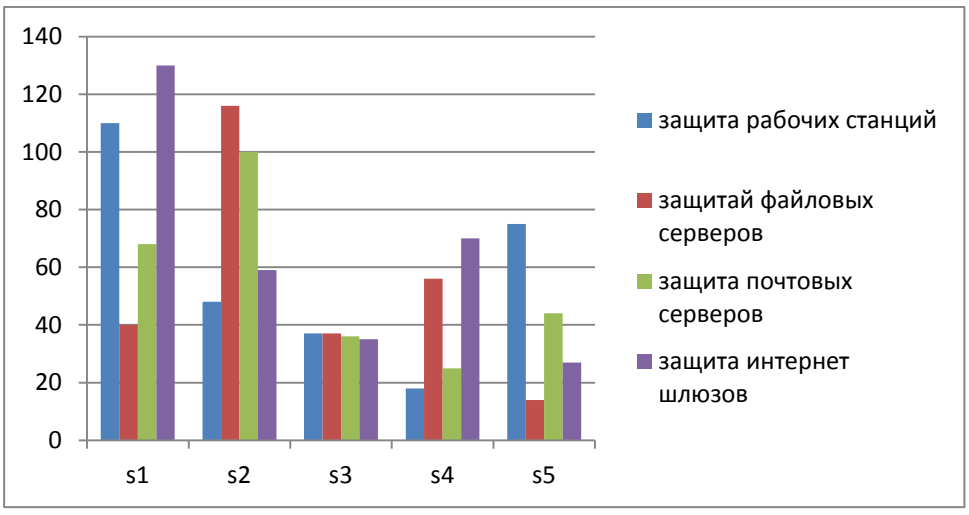
- S1- «Лаборатория Касперского»;
- S2 -ESET NOD32;
- S3- Dr. Web;
- S4- Symantec;
- S5- McAfee.

Для оценки степени поглощения тем или иным программным средством защиты соответствующих функциональных операций рассчитывается значение функционального веса (таблица 4).

График весовых коэффициентов, приведенный на рисунке 3, демонстрирует, какие программные средства защиты наиболее оптимальны для построения комплексной системы защиты от программных кодов деструктивного воздействия для следующих объектов защиты:

- Рабочих станций;
- Файловых серверов;
- Почтовых серверов;
- Интернет шлюзов.

В данном примере система S1 является наиболее функциональной для защиты рабочих станций и интернет шлюзов, а система S2 наиболее функциональна для защиты почтовых и файловых серверов.



Источник: авторский.

Рисунок 3 – График весовых коэффициентов

Таблица 4 – Фрагмент значения функционального веса

Система	Весовой коэффициент
	Защита рабочих станций
S1	110
S2	48
S3	37
S4	18
S5	75
	Защита файловых серверов
S1	40
S2	116
S3	37
S4	56
S5	14
	Защита почтовых серверов
S1	68
S2	100
S3	36
S4	25
S5	44
	Защита интернет шлюзов
S1	130
S2	59
S3	35
S4	70
S5	27
…	…

Источник: авторский

Однако на практике необходимо проводить оценку систем защиты не только с точки зрения набора выполняемых функций и качества функциональных возможностей, но и с точки зрения возможности своевременного обнаружения и нейтрализации угроз от программных кодов деструктивного воздействия. Для этого был составлен перечень базовых операций, совершаемых программными кодами деструктивного воздействия. Основой для составления такого перечня послужила информация из научных изданий с учетом мнения экспертов.

Экспериментальным путем методом атаки на информационную систему на программном стенде в виртуальной среде (VMware vSphere), моделирующей информационную систему, с использованием специальных программ (Netstat, Process Monitor, HTTP Analizer, WireShark) были определены временные характеристики блокировки системой защиты операций, выполняемых программными кодами деструктивного воздействия.

Фрагмент перечня функциональных операций приведен в таблице 5.

Таблица 5 – Фрагмент перечень функциональных операций и время их блокировки

№	Операция	t min(сек)	t max(сек)	t вероятное (сек)
1	чтение данных файлов	0,70	5,58	1,87
2	чтение данных папок	0,70	8,58	1,78
3	запись данных в файлы	1,35	6,29	2,47
4	чтение атрибутов файлов	0,50	1,76	1,01
5	чтение атрибутов папок	0,33	1,68	0,84
6	запись атрибутов файлов	0,50	2,10	1,01
7	запись атрибутов папок	0,52	2,35	1,04
8	чтение дополнительных атрибутов файлов	0,39	2,68	1,04
9	чтение дополнительных атрибутов папок	0,40	2,68	1,21
10	запись дополнительных атрибутов файлов	0,50	3,93	1,49
…	…	…	…	…

Источник: авторский

Конкретный алгоритм атаки программного кода деструктивного воздействия представляет собой определенную последовательность базовых операций.

Например, вредоносная программа Worm.Win32.Zomque.bj имеет следующую последовательность базовых операций: 46,10,39,7,37,56,32,54,40, 24,40,14,8,28,76,8,49,44,63,38,44,40,63,14,6,26,69,21,24,31,32,27,56,1,25,4,8,58, 51,16,27,44,53,35,58,44,25,53,76,22,2,64,71,3,63,41,45,60,26,38,73,53,49,24,4,7, 13,78,35,28,12,66,37,70,76,8,54,43,48,13,65,48,44,80,79,86,31,61,26,50,48,26,12, 61,73,23,73,29,60,77,85,20,54,29,65,10,21,52,8,32,20,14,56,61,17,16,44,34,37,75, 63,70,29,18,73,17,62,47,65,68,72,60,57,37,65,56,73,45,75,7,55,37,64,24,37,32,46, 36,30,64,41,36,7,69,37,76,59,55,69,34,49,55,37,39,73,69,51,30,62,9,56,9,47,2,12, 48,71,20,15,29.

На основании алгоритма возможно определение вероятности преодоления системы защиты за определенный промежуток времени.

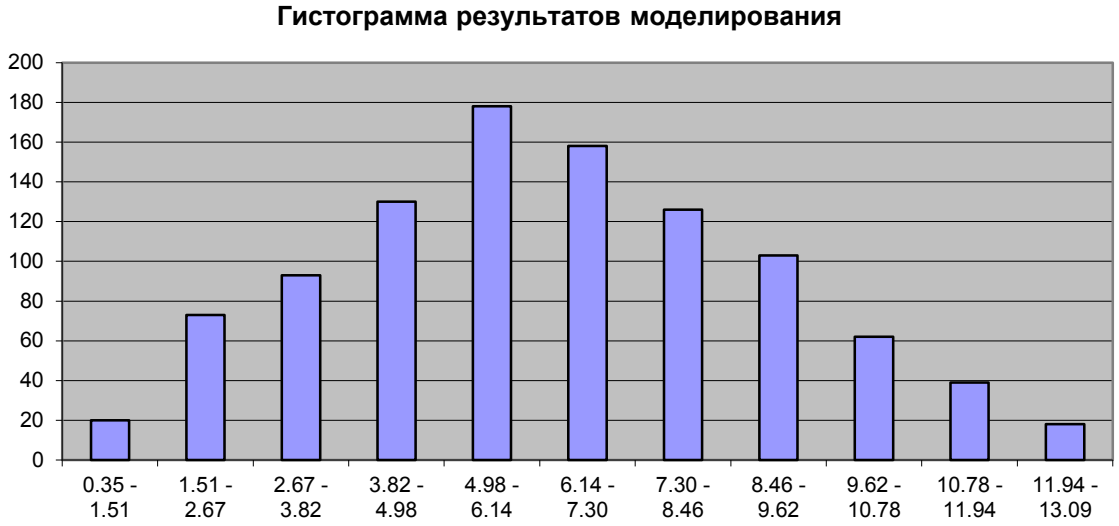
Для этого нами были определенны параметры закона распределения базовых операций.

Результаты имитационного моделирования действия вредоносной программы Worm.Win32.Zomque.bj представлены на рисунке 4.

Для набора базовых операций (113), используемого в эксперименте, закон распределения является нормальным, что позволяет применить функцию Лапласа для расчета вероятностей.

Параметрами нормального распределения послужили статистические характеристики, полученные экспериментально.

Для группы операций, выполняемых программными кодами деструктивного воздействия, была рассчитана функция распределения и получена вероятность блокировки системой защиты таких операций за определенный промежуток времени.



Параметр	Значение
Среднее	6.339
Дисперсия	6.954
Среднеквадратическое отклонение	2.637
Коэффициент вариации	0.416
Асимметрия	0.173
Эксцесс	-0.510
Минимум	0.348
Максимум	13.094

Источник: отчет программы имитационного моделирования «СИМ-UML»

Рисунок 4 – Результаты имитационного моделирования

Расчет показал, что система защиты с вероятностью 70% блокирует вирусную атаку за промежуток времени от 290 до 318 секунд.

Также с помощью формулы обратного нормального распределения было рассчитано необходимое время для блокировки атаки программными кодами деструктивного воздействия на информационную систему по заданной вероятности.

Расчет показал, что система защиты с вероятностью 98% блокирует атаку за промежуток времени от 273,23 до 336,51 секунд.

Предложенная методика позволяет оценить вероятность преодоления иммунной системы защиты программными кодами деструктивного воздействия.

В третьей главе «Совершенствование структуры распределенной системы управления иммунными механизмами защиты» определено, что совершенствование структуры распределенной системы управления иммунными механизмами защиты может быть основано на оценке функциональности основного элемента системы управления – центра управления, ответственного за выполнение следующих операций:

- удаленное управление программным средством защиты;
- предоставление отчетов и уведомлений;

- обновление программных средств защиты;
- управление лицензиями;
- управление хранилищем зараженных объектов.

Для этого нами была предложена методика определения вероятности реализации атаки с учетом такого параметра как удаленность центра управления от базовых защитных механизмов.

Процесс атаки программных кодов деструктивного воздействия на информационную систему может развиваться по следующему сценарию. Атака осуществляется на информацию в защищенном сегменте информационной системы. Сообщение от программных средств защиты того или иного уровня о попытке атаки в реальном масштабе времени поступает в центр управления. Центр управления автоматически или по командам администратора безопасности реагирует тем или иным образом на попытку атаки. При этом возможна реализация двух альтернативных ситуаций:

- атака осуществлена;
- попытка атаки блокирована.

Обозначим вероятность второго события как вероятность пресечения $P_{пр}$. Тогда задача определения вероятности $P_{пр}$ может быть сформулирована следующим образом.

Введем следующие ограничения:

- Сигнал от программных средств защиты поступает в центр управления в реальном масштабе времени.
- Система защиты с центром управления периодически проверяется и диагностируется, чем обеспечивается высокая степень эксплуатационной надежности.
- Контроль и блокировка атаки осуществляется только в пределах защищенного сегмента системы защиты.

Блокировка атаки программных кодов деструктивного воздействия будет возможна только при обнаружении двух независимых условий:

- Факт атаки будет зафиксирован системой защиты определенного уровня.
- Центр управления в автоматизированном или управляемом администратором безопасности режиме будет иметь соответствующие алгоритмы блокировки и успеет осуществить данную блокировку атаки программных кодов деструктивного воздействия.

Таким образом, получим:

$$P_{пр} = P_{обн} P_k,$$

где $P_{обн}$ - вероятность обнаружения атаки;

$P_к$ - вероятность срабатывания механизма блокировки атаки вовремя.

В свою очередь вероятность обнаружения складывается из двух составляющих:

- вероятности обнаружения атаки конкретной системой защиты, зависящей от его эксплуатационных характеристик и количества контролируемых методов атаки программных кодов деструктивного воздействия;
- вероятности обхода механизма системы защиты.

Вероятность обнаружения атаки конкретным программным средством защиты зависит от количества механизмов защиты, контролирующих те или иные алгоритмы атаки. Наличие вероятности обхода механизма защиты обусловлено тем, что программный код деструктивного воздействия может использовать методы атаки, неизвестные средствам защиты.

В общем случае вероятность обнаружения попытки атаки программных кодов деструктивного воздействия каждым механизмом можно оценить по формуле:

$$P_j = P_j^{пд} P_j^{н},$$

где $P_j^{пд}$ - вероятность выдачи j-м механизмом защиты сообщения центру управления о попытке атаки;

$P_j^{н}$ - надежность j-го механизма защиты.

Возможность соответствующего по времени реагирования на атаку программных кодов деструктивного воздействия защитного механизма центра управления обусловлена вероятностью того, что он сумеет определить тип и направление атаки за определенный промежуток времени.

Выражение для определения данной вероятности может быть получено с помощью следующих составляющих:

- время определения типа и направления атаки;
- эффективное количество закрываемых методов атаки (оптимальное для адекватного времени поиска и реагирования);
- диапазон закрываемых методов атаки;
- производительность определения типа и направления атаки;
- количество распределенных баз вирусных сигнатур с параллельным поиском.

Производительность поиска определяется из эффективного количества закрываемых методов и средней скорости поиска в базах данных уязвимостей.

Время поиска ограничено средним временем реализации атаки на информацию в пределах защищаемого сегмента. Время вирусной атаки складывается из времени инициализации алгоритма атаки, времени обхода стандартных средств разграничения доступа на уровне операционной системы и времени атаки, необходимого для воздействия на защищаемую информацию.

Принимая во внимание тот факт, что сообщение об атаке от программных средств защиты определенного уровня поступает в центр

управления практически мгновенно, считаем началом отсчета времени момент контакта алгоритма программного кода деструктивного воздействия с защитным механизмом. Однако в случае значительной удаленности центра управления от защищаемого сегмента значение времени типа и направления атаки уменьшается на время, необходимое центру управления для реакции на попытку атаки.

На программном стенде в виртуальной среде на смоделированную защищенную информационную систему была произведена атака с применением программных кодов деструктивного воздействия. Данные, необходимые для расчета, были получены экспериментальным путем.

Расчеты по приведенной выше методике позволили получить следующее значение вероятности блокирования атаки программных кодов деструктивного воздействия на информацию: $P_{пр} = 0{,}674$.

Одним из методов повышения надежности управления системой защиты от программных кодов деструктивного воздействия является использование метода кластеризации узлов сети, на базе которых сформирован центр управления. Архитектура отказоустойчивого кластера центров управления системой защиты представлена на рисунке 5.

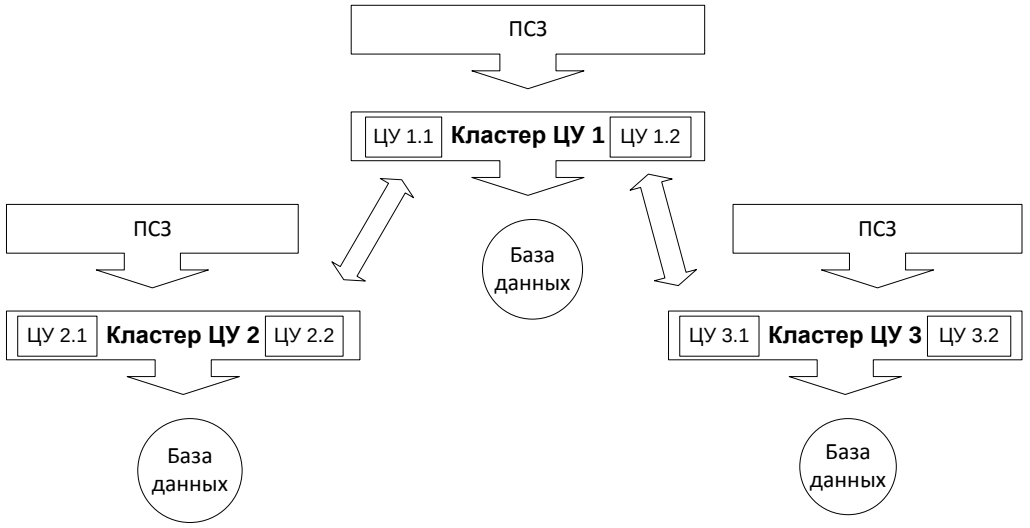


Рисунок 5 – Архитектура отказоустойчивого кластера центра управления системой защиты

Предложен метод, позволяющий оценить вероятность отказа кластера центра управления системой защиты от программных кодов деструктивного воздействия и, соответственно, вероятность безотказной работы.

Вероятность отказа всего кластера центра управления системой защиты определяется следующим образом:

$$F(t) = f_1(t) * f_2(t) * \ldots * f_N(t) = \prod_{i=1}^{N} f_i(t) = \prod_{i=1}^{N} (1 - p_i(t)),$$

где $f_i(t)$ – вероятность отказа i-го узла, $p(t)$ – вероятность безотказной работы i-го узла.

Тогда вероятность безотказной работы можно рассчитать по формуле:

$$P(t) = 1 - F(t) = 1 - \prod_{i=1}^{N}(1 - p_i(t)).$$

Для того, чтобы получить численное значение вероятности безотказной работы, достаточно обратиться к журналу регистрации технических сбоев, который ведется на каждом предприятии.

Анализ предприятия в рамках научно-исследовательской работы (№1293/11 от 01.10.2011) показал, что использование кластера центра управления в значительной степени уменьшает риск потери управления над сегментом системы защиты, что повышает надежность как показатель потребительского качества таких систем.

Вероятность безотказной работы для узлов центра управления составила 0,57 и 0,72.

$$P(t) = 1 - (1 - 0{,}57) * (1 - 0{,}72) = 0{,}8796.$$

Вероятность безотказной работы для центра управления состоящего из 2-х узлов, составила 88%.

Экономическая оценка применения таких систем не является целью диссертационного исследования, однако в ходе выполнения хоздоговорной работы нами были проведены подсчеты, показывающие выгоду применения кластерных систем на практике. Стоимость дополнительного узла сети, как элемента кластеризации центра управления, для выше упомянутого предприятия составляет около 15000 рублей. Заявленная руководством предприятия стоимость убытков от нарушения функционирования информационной системы вследствие вирусной атаки составляет около 80000 рублей в час. В данном конкретном случае применение кластеризации центра управления экономически выгодно.

Случайная и многократная повторяющаяся природа событий, происходящих в системах защиты от программных кодов деструктивного воздействия, позволяет использовать для ее анализа теорию массового обслуживания. На основании систем массового обслуживания (СМО) с отказами и СМО с ожиданием становится возможным получить характеристики качества ее работы (пропускную способность, среднее время пребывания заявки в системе, среднюю длину очереди, среднее время ожидания в очереди и т.д.).

Объектом исследования выступило предприятие, где в рамках хоздоговорной работы была построена система защиты от программных кодов деструктивного воздействия высокой готовности, состоящая из двух центров управления. Среднее время выполнения функциональной операции, связанной с центром управления, равняется 10,5 сек.

Собранные в течение недели данные позволили рассчитать, что в среднем в сеть поступает 15 запросов на обслуживание в течение минуты. Потребовалось определить показатели эффективности и качества системы защиты от программных кодов деструктивного воздействия, а также определить минимальное количество узлов, достаточное для того, чтобы не менее 95% всех запросов на обслуживание были приняты и обработаны.

Расчет показал, что СМО с ожиданием позволяет, изменяя размер очереди и количество узлов в системе, решить проблему низкой пропускной способности и достигнуть баланса между затратами на расширение центра управления системой защиты и увеличением длины очереди, что сказывается на качестве функционирования комплексной системы защиты от программных кодов деструктивного воздействия.

В ходе диссертационного исследования было проанализировано множество систем защиты от программных кодов деструктивного воздействия. Однако, в связи с несовместимостью различных программных продуктов, создание гетерогенной комплексной системы защиты от программных кодов деструктивного воздействия с единым центром управления представляется достаточно сложным. Именно поэтому было принято решение о разработке собственного программного продукта, позволяющего осуществлять систематизированный сбор статистической отчетности на главном центре управления.

Для решения поставленной задачи был создан программный продукт «Antivir Remote Control», позволяющий осуществлять централизованный сбор отчетов о работе программных средств защиты разных фирм-производителей.

Фрагмент работы программы «Antivir Remote Control» представлен на рисунке 6.

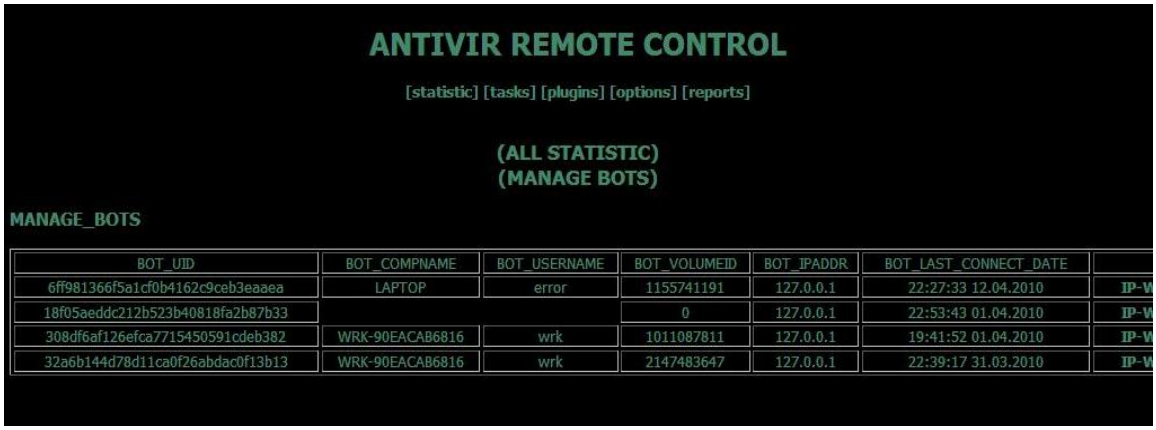


Рисунок 6 – Фрагмент работы программы «Antivir Remote Control»

В заключении диссертационной работы приведены основные выводы по результатам проведенного исследования.

По теме диссертации автором опубликованы следующие работы.

Статьи в периодических научных изданиях, рекомендуемых ВАК для публикации научных работ, отражающих основное научное содержание диссертаций:

1. Строкань, Д.А. Количественная оценка параметров кластеризации центра управления иммунностойкой экономической информационной

системой /Д.А. Строкань // Вестник РГЭУ (РИНХ), 2011. – №3(35). – С. 107-111.- 0,19 п.л.

2. Строкань, Д.А. Оценка защищенности распределенных информационных систем от программ деструктивного характера / Д.А. Строкань, Т.Н. Шарыпова // Вестник РГЭУ (РИНХ), 2011. – №2(34). – С. 109-113.- 0,2 п.л. (лично автора 0,13 п.л.).

3. Строкань, Д.А. Сравнительный анализ систем антивирусной защиты при построении гетерогенных систем / Д.А. Строкань // Экономические науки, 2011. – №5(78). – С. 371-374. - 0,23 п.л.

Статьи в журналах, сборниках научных трудов и сборниках материалов докладов конференций:

4. Строкань, Д.А. Вероятность блокировки вирусной атаки в распределенной системе антивирусной защиты с единым центром управления / Д.А. Строкань //Проблемы информационной безопасности: материалы всероссийской научно-практической Интернет-конференции / РГЭУ «РИНХ». - Ростов н/Д, 2009. – С. 254-257.- 0,3 п.л.

5. Строкань, Д.А. Оценка вероятности вирусной атаки в распределенной экономической информационной системе с централизованным управлением антивирусной защитой / Д.А. Строкань // Вопросы экономики и права. Сборник статей аспирантов и соискателей ученой степени кандидата наук. Выпуск 8.- Ростов н/Д: Рост.гос.эконом. ун-т(РИНХ), 2010. – С. 191-195.- 0,5 п.л.

6. Строкань, Д.А. Расчет отказоустойчивости работы кластера центров управления антивирусной защитой / Д.А. Строкань //Проблемы создания и использования информационных систем и технологий: материалы IV межригеон. науч.-практ. конф. / Рост. гос. эконом. ун-т. (РИНХ). –Ростов н/Д, 2011. – С. 101-103.- 0,2 п.л.

7. Строкань, Д.А. Сравнительный анализ программных средств администрирования комплексных антивирусных систем / Д.А. Строкань // Экономические информационные системы и их безопасность : разработка, применение, сопровождение: материалы регион. науч.-практ. конф. профес.-преподват. состава, молодых ученых, аспирантов и студентов (п. Архыз, 1-5 октября 2009 г.) / Рост. гос. эконом. ун-т (РИНХ).-Ростов н/Д, 2010. – С. 39-43.- 0,25 п.л.

8. Строкань, Д.А. Разработка методики создания системы антивирусной защиты с единым центром управления на предприятиях различных форм собственности / Д.А. Строкань, Е.Ю. Федорова //Проблемы создания и использования информационных систем и технологий: материалы III межригеон. науч.-практ. конф. / Рост. гос. эконом. ун-т. (РИНХ). –Ростов н/Д, 2010. – С. 60-66.- 0,7 п.л. (лично автора 0,4 п.л.).

Печать цифровая. Бумага офсетная. Гарнитура «Таймс».
Формат 60х84/16. Объем 1,0 уч.-изд.-л.
Заказ № 2581 Тираж 120 экз.
Отпечатано в КМЦ «КОП***И***ЦЕНТР»
344006, г. Ростов-на-Дону, ул. Суворова, 19, тел. 247-34-88