На правах рукописи

Груздева Людмила Михайловна

# МОДЕЛИ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 05.12. 13 – Системы, сети и устройства телекоммуникаций

**А в т о р е ф е р а т**
диссертации на соискание ученой степени
кандидата технических наук

Владимир - 2011

Работа выполнена на кафедре «Информатика и защита информации» Владимирского государственного университета

Научный руководитель: доктор технических наук, профессор Монахов Михаил Юрьевич

Официальные оппоненты: доктор технических наук, профессор Полушин Петр Алексеевич,
кандидат технических наук, доцент Дерябин Вячеслав Михайлович

Ведущая организация: ОАО «Владимирское конструкторское бюро Радиосвязи»

Защита состоится «27» апреля 2011 г. в «$14^{00}$» час в ауд. 301-3 на заседании диссертационного Совета Владимирского государственного университета по адресу: 600000, Владимир, ул. Горького, 87, ВлГУ, ФРЭМТ.

С диссертацией можно ознакомиться в библиотеке ВлГУ.

Автореферат разослан «___» _____ 2011г.

Ученый секретарь
диссертационного Совета,
доктор технических наук, профессор Самойлов А.Г.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

***Актуальность темы.*** Проблема повышения производительности корпоративных телекоммуникационных сетей (КТКС) в последние годы существенно обострилась как в отечественной науке и промышленности, так и за рубежом. Это обусловлено рядом причин, среди которых выделим две основные:

- постоянно возрастающая структурная сложность и размерность современных КТКС, характеризующихся множественными изменяющимися во времени информационными связями;

- постоянно возрастающие потребности практики в увеличении уровня информационной безопасности (ИБ) КТКС, особенно предназначенных для работ на опасных промышленных объектах.

Анализ современных КТКС показывает, что существенное снижение производительности сети происходит из-за угроз ИБ, реализация которых способна полностью блокировать работу КТКС. Для эффективного проектирования и эксплуатации КТКС, функционирующих в условиях воздействия угроз ИБ, необходимо располагать моделями и алгоритмами, позволяющими оценивать, прогнозировать и обеспечивать требуемый уровень производительности, как одного из основных показателей-индикаторов эффективности КТКС и качества обслуживания абонентов.

Известные сетевые модели с использованием аппарата теории массового обслуживания, предложенные В.М. Вишневским, А.И. Герасимовым, Б.В.Гнеденко, П.П. Бочаровым, Л. Клейнроком не учитывают параметры угроз ИБ и систем защиты (СЗИ). Подходы к обеспечению ИБ в телекоммуникационных сетях, предложенные в трудах российских ученых В.А. Герасименко, С.П. Расторгуева, П.Д. Зегжды, В.И. Завгороднего, А.А. Малюка, А.А. Грушо, В.В.Домарева, зарубежных исследователей Р. Брэтта, К. Касперски, С. Норкатта, В. Столингса, хоть и обеспечивают существенное повышение защищенности КТКС, но не используют в качестве критерия эффективности производительность.

Таким образом, исследования, направленные на разработку моделей повышения производительности КТКС, функционирующей в условиях воздействия угроз ИБ, актуальны и имеют теоретическое и практическое значение при моделировании, проектировании и эффективной эксплуатации телекоммуникационных сетей.

**Объект исследования** - корпоративная телекоммуникационная сеть.

**Цель работы** – решение научно-технической задачи разработки новых моделей и процедур управления, направленных на повышение производительности корпоративной телекоммуникационной сети в условиях воздействия угроз информационной безопасности.

Для достижения поставленной цели в работе решены следующие **задачи**:

1. Выявление угроз ИБ, вызывающих существенное снижение производительности КТКС.

2. Синтез аналитических моделей оценки производительности КТКС в условиях воздействия угроз ИБ.

3. Разработка алгоритмов достоверного обнаружения реализации угроз ИБ в КТКС за ограниченное время.

4. Разработка модели распределенной системы противодействия угрозам информационной безопасности в КТКС.

5. Разработка средств экспериментального исследования характеристик производительности КТКС с учетом воздействия и противодействия угрозам ИБ.

В ходе решения перечисленных задач использовались следующие ***методы исследования:*** анализ структур и процессов функционирования КТКС, моделирование и синтез оптимальных процедур управления и обработки информации. Научные положения, выводы и рекомендации, сформулированные в диссертации, теоретически обосновываются с помощью аппарата теории вероятностей, теории очередей.

***Научные результаты, выносимые на защиту***:

– аналитические модели оценки производительности КТКС в условиях воздействия угроз информационной безопасности;

– алгоритмы достоверного обнаружения реализации угроз ИБ в КТКС за ограниченное время;

– модель распределенной системы противодействия угрозам ИБ.

***Научная новизна работы***:

1. Разработано семейство аналитических моделей оценки производительности КТКС в условиях воздействия угроз ИБ, отличающихся тем, что они учитывают параметры угроз ИБ и систем защиты информации.

2. Предложена методика повышения производительности КТКС в условиях воздействия угроз ИБ, включающая:

– алгоритмы обнаружения угроз ИБ за ограниченное время;

– модель противодействия угрозам ИБ, обеспечивающая максимальную производительность КТКС;

– средства и механизмы, позволяющие автоматизировать процессы определения характеристик производительности КТКС в условиях воздействия угроз ИБ.

**Практическая ценность работы** заключается в следующем:

1. Разработанные инструментальные средства в среде Adobe Flash CS3 Professional, позволяют: моделировать воздействие угроз ИБ и СЗИ на производительность замкнутой и разомкнутой систем, определять характеристики производительности по аналитическим алгоритмам.

2. Предложенные имитационные модели КТКС в среде GPSS World, позволяют количественно оценить характеристики производительности в условиях воздействия угроз ИБ и снять ограничения, накладываемые аналитическими моделями.

3. Разработанные инструментальные средства подсистемы раннего обнаружения информационных атак, позволяют снижать время обнаруже-

ния минимум на 20% по сравнению со стандартной системой обнаружения вторжений, что при оперативном инициировании средства противодействия угрозам ИБ в наиболее уязвимых узлах КТКС позволяет повысить производительность не менее чем в 2 раза.

**Реализация и внедрение результатов работы**. Исследования и практические разработки, выполненные в диссертационной работе, являются частью научно-исследовательских работ, выполненных Владимирским государственным университетом: г/б НИР 396/03 «Исследование и разработка методов повышения эффективности распределенных управляющих систем»; х/д НИР №3701/08, № 3744/08 «Разработка ведомственных информационных систем администрации Владимирской области»; № ДУ55/08 «Развитие сети передачи данных администрации Владимирской области».

Результаты исследований были внедрены в корпоративной телекоммуникационной сети ОАО «Завод «Электроприбор»» г. Владимир, КТКС ООО «Гранит» г. Владимир, Администрации Владимирской области, а также были использованы при разработке учебных курсов во Владимирском государственном университете.

**Достоверность** полученных результатов подтверждается полнотой и корректностью теоретических обоснований и результатами экспериментов, проведенных с помощью разработанных в диссертации программ.

**Апробация работы.** Основные положения диссертационной работы докладывались на: Международной научно-технической конференции «Автоматизированная подготовка машиностроительного производства, технология и надежность машин, приборов и оборудования» (Вологда, 2005); III Всероссийской научно-технической конференции «Образовательная среда сегодня и завтра» (Москва, 2006); XIX, XX, XXI, XXII, XXIII Международных научных конференциях «Математические методы в технике и технологиях» (Воронеж, 2006, Ярославль, 2007, Саратов, 2008, Иваново, 2009, Саратов, 2010); XXVI Международной научно-технической конференции «Проблемы эффективности безопасности функционирования сложных технических и информационных систем» (Серпухов, 2007); IV Всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика» (Санкт-Петербург, 2009).

**Публикации.** Основные положения диссертационной работы отражены в 24 публикациях, включая в рекомендуемых ВАК изданиях.

**Структура и объем диссертационной работы.** Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы из 170 наименований, приложений и содержит 120 страниц основного текста, иллюстрированного 22 рисунком.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обосновывается актуальность темы диссертации. Формируется цель и задачи исследований.

**В главе 1** рассматривается структура КТКС, анализируются показате-

ли производительности, выявляются существенные угрозы ИБ, вызывающие снижение ее производительности, анализируются современные методы и средства обнаружения информационных атак, как реализации угроз ИБ, степень их влияния на производительность КТКС.

Снижение производительности КТКС связано с недостаточной защищенностью по причинам: широкого использования слабозащищенных протоколов HTTP, SNMP, FTP, TCP/IP; участия в процессе обработки информации пользователей различных категорий, их непосредственного и одновременного доступа к системным ресурсам и процессам [1, 11, 12]. Современная СЗИ, включающая системы предотвращения и обнаружения вторжений IPS/IDS не могут гарантировать даже 70% детектирования информационной атаки, что периодически приводит к значительному возрастанию вредоносного трафика (ВТ) в КТКС [5, 10]. Одной из актуальных задач является и, очевидно, будет оставаться перспективной на ближайшее время – задача повышения достоверности обнаружения информационных атак, их идентификация, а также разработка методов и средств снижения их влияния на производительность КТКС.

Постановка задачи [5]. Дано:

1. Множество объектов КТКС $O = \{O_1, O_2, ..., O_{NS}\}$. Линии связи надежны, помехоустойчивы и состоят из дуплексного канала; маршрутизаторы сегментов имеют бесконечную память; трафик состоит из пакетов одинакового приоритета и образует пуассоновский поток; длительность обработки пакетов определяется экспоненциальным законом распределения.

2. СЗИ включает модули защиты (МЗ), в состав которых входит средство обнаружения (СО) угроз ИБ из $SO = \{SO_1, SO_2, ..., SO_N\}$ и средство противодействия (СП) угроз ИБ из $SP = \{SP_1, SP_2, ..., SP_M\}$.

3. Характеристики СО: $p_i(t)\left(i = \overline{1, N}\right)$ – вероятность обнаружения угроз ИБ; $\overline{p_i(t)}\ \left(i = \overline{1, N}\right)$ – вероятность возникновения «ложной тревоги»; $t_i^{\text{ОБ}}\left(i = \overline{1, N}\right)$ – время обнаружения угроз ИБ, за которое достигается максимальное значение вероятности обнаружения угроз ИБ, т.е. $p_i^{\max} = \lim\limits_{t \to t_i^{\text{ОБ}}} p_i(t)$.

4. Характеристики СП: $q_j(t)\left(j = \overline{1, M}\right)$ – вероятность противодействия угроз ИБ; $t_j^{\text{ПР}}\left(j = \overline{1, M}\right)$ – время противодействия угрозам ИБ, за которое достигается максимальное значение вероятности противодействия угрозам ИБ, т.е. $q_j^{\max} = \lim\limits_{t \to t_j^{\text{ПР}}} q_j(t)$.

Требуется обеспечить максимально возможную производительность КТКС при достоверном обнаружении и максимально эффективном противодействии угрозам ИБ:

$$\begin{cases} \Phi(\Pi) \to \max; \\ P_{\text{ОБ}}(t) \to \max;\ \ \overline{P_{ЛТ}}(t) \to \min;\ Q_{\text{ПР}} \to \max; \\ T^{\text{ОБ}} + T^{\text{ПР}} \le T^{Д}. \end{cases}$$

где $\Phi(\Pi)$ – производительность КТКС; $P_{ОБ}(t) = \varphi_1(p_1(t),\ p_2(t),..., p_N(t))$ – вероятность обнаружения угроз ИБ; $\overline{P_{ЛТ}}(t) = \varphi_2\left(\overline{p_1}(t),\ \overline{p_2}(t),..., \overline{p_N}(t)\right)$ – вероятность возникновения «ложной тревоги»; $Q_{ПР}(t) = \varphi_3(q_1(t),\ q_2(t),..., q_M(t))$ – вероятность противодействия угрозам ИБ; $T^{\text{ОБ}} = \varphi_4\left(t_1^{\text{ОБ}}, t_2^{\text{ОБ}},..., t_N^{\text{ОБ}}\right)$ – время обнаружения угроз ИБ; $T^{\text{ПР}} = \varphi_5\left(t_1^{\text{ПР}}, t_2^{\text{ПР}},..., t_M^{\text{ПР}}\right)$ – время противодействия угрозам ИБ; $T^{Д}$ – допустимые временные затраты на обеспечение защиты ($\varphi_1, \varphi_2, \varphi_3, \varphi_4$ – виды соответствующих функциональных зависимостей).

Решение задачи предложено искать в следующем порядке: (1) выявить целевые характеристики производительности КТКС; разработать (2) аналитические модели оценки производительности КТКС в условиях воздействия угроз ИБ; (3) алгоритмы достоверного обнаружения угроз ИБ; (4) модель распределенной системы противодействия угрозам ИБ.

**Глава 2** посвящена исследованию и разработке аналитических моделей оценки производительности КТКС в условиях воздействия угроз ИБ [4-7, 14, 24].

1. Моделью КТКС является замкнутая сеть из $K$ СМО. Циркулирует фиксированное число пакетов. Сеть массового обслуживания (СеМО) задается стохастической маршрутной матрицей: $P_R = \|p_{ij}\|$, где $p_{ij}$ – вероятность пересылки пакета из $i$-го узла в $j$-й узел, причём $\sum_{j=1}^{K} p_{ij} = 1\ \ \forall i = \overline{1, K}$.

Воздействия угроз ИБ, как вредоносный поток (ВП), создаваемый атакующим средством, оценим интенсивностью потока пакетов, поступающих в $i$-й узел: $\lambda_i = e_i \Lambda$, где $e_i$ – передаточные коэффициенты, $\Lambda$ – интегральный сетевой трафик. Описывая $\lambda_i$ пуассоновским процессом с экспоненциальным распределением времени их передачи, учитывая независимость данного потока, положим, что $\lambda_i = \lambda_i^0 + \lambda_i^{ВП}$, где $\lambda_i^0$ - интенсивность «полезного» потока, $\lambda_i^{ВП}$ - интенсивность ВП, получим

$$\lambda_j = \sum_{i=1}^{K} (\lambda_i^0 + \lambda_i^{ВП}) p_{ij} = \sum_{j=1}^{K} (e_j^0 \Lambda^0 + e_j^{ВП} \Lambda^{ВП}) p_{ij}. \qquad (1)$$

$\lambda_i^{ВП}$ зависит от характеристик угроз ИБ. Для угроз ИБ – «вредоносная программа» (ВПр), введем классификацию: «слабая» ВПр (алгоритм сканирования перебором, опрос путём ICMP, одномодульная (сканер уязвимостей, механизм распространения, а также механизм реализации сосредоточены в одном программном модуле)); «сильная» ВПр (усовершенствованные алгоритмы сканирования сетевых адресов, опрос с использованием

полуоткрытого TCP-соединения, многомодульная, использование технологий, затрудняющих ее обнаружение).

Будем считать $\Lambda^{ВП} = \xi\Lambda^0, \xi < 1$, где коэффициент $\xi$ представляет ВП как часть от полезного. Таким образом,

$$\lambda_j = \sum_{i=1}^{K}(\lambda_i^0 + \lambda_i^{ВП})p_{ij} = \Lambda^0(1+\xi)\sum_{j=1}^{K}(e_j^0 + e_j^{ВП})p_{ij}. \quad (2)$$

Интенсивность обработки пакетов в *i*-м узле: $\mu_i = 1/\tau_i$, где $\tau_i$ – среднее время обработки пакета в *i*-м узле, распределённое по экспоненциальному закону. $\tau_i$ зависит от длительности непосредственной обработки пакета в узле ($\tau_i^0$ – расшифровка пакета, формирование запроса к БД и т.п.), от длительности функционирования угроз ИБ ($\tau_i^{ВП}$ – запуск кода ВПр, «пустое» или «разрушающее» использование ресурсов узла и т.п.) и от длительности функционирования МЗ (например, для антивирусных средств $\tau_i^{МЗ}$ – поиск ВПр, уничтожение, обновление и т.п.)

$$\tau_i = \Phi(\tau_i^0, \tau_i^{ВП}, \tau_i^{МЗ}). \quad (3)$$

Экспериментальные исследования [18, 19, 20-22] показали, что $\tau_i$ пропорциональна $\tau_i^0$ и имеет тенденцию к увеличению при возрастании $\tau_i^{ВП}$. К увеличению длительности обработки в узле ведет и величина $\tau_i^{МЗ}$, которая зависит от $\lambda_i^{ВП}$ и от характеристик СЗИ, определяемых отсутствием и/или неправильным функционированием межсетевых экранов и IPS/IDS, отсутствием средств реструктуризации топологии КТКС, отсутствием или недостаточной оперативностью обеспечения МЗ обновлениями («слабая» СЗИ), или наличием комплексной СЗИ, включающей механизмы управления безопасностью («сильная» СЗИ).

Расчет характеристик производительности КТКС, как замкнутой сети, предлагается выполнять в соответствии с известными методиками.

2. Моделью КТКС является разомкнутая СеМО, состоящая из источника пакетов (узел 0) и $K$ СМО. СеМО задается матрицей: $P_R = \|p_{ij}\|$, где $p_{ij}$ – вероятность пересылки пакета из *i*-го узла в *j*-й узел, причём $\sum_{j=0}^{K} p_{ij} = 1$ $\forall i = \overline{0, K}$. Интенсивность потока пакетов, поступающих в *i*-й узел: $\lambda_i = e_i\lambda_0$, где $\lambda_0$ – интенсивность входящего в сеть потока пакетов. Учет влияния угроз ИБ и СЗИ, ведется в соответствии с (1) - (3).

Алгоритм расчета средней задержки пакетов в разомкнутой КТКС

Шаг 1. Задать начальные условия: $K$, $\lambda_0$, $P_R$, $m_i$, $\tau_i$ $\left(\forall i = \overline{1, K}\right)$.

Шаг 2. Получить систему уравнений

$$\begin{cases} -(e_0^0 + e_0^{ВП}) + p_{10}(e_1^0 + e_1^{ВП}) + \ldots + p_{K0}(e_K^0 + e_K^{ВП}) = 0 \\ p_{01}(e_0^0 + e_0^{ВП}) + (p_{11} - 1)(e_1^0 + e_1^{ВП}) + \ldots + p_{K1}(e_K^0 + e_K^{ВП}) = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_{0K}(e_0^0 + e_0^{ВП}) + p_{1K}(e_1^0 + e_1^{ВП}) + \ldots + (p_{KK} - 1)(e_K^0 + e_K^{ВП}) = 0 \end{cases}.$$

Найти передаточные коэффициенты $e_0, e_1, e_3, \ldots, e_K$.

Шаг 3. Найти интенсивности потока пакетов: $\lambda_i = e_i \lambda_0 \quad \forall i = \overline{1, K}$.

Шаг 4. Найти загруженность узлов сети: $\chi_i = \frac{\lambda_i}{m\mu_i} \quad \forall i = \overline{1, K}$.

Шаг 5. Рассчитать вероятности состояний: $P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0) \quad \forall i = \overline{1, K}$,

где $P_i(0) = \left( \sum_{n=0}^{m} \frac{\rho_i^n}{n!} + \frac{\rho_i^{m+1}}{m! m(1-\chi_i)} \right)^{-1}$, $\rho_i = \frac{\lambda_i}{\mu_i}$ и $\beta_i(n) = \begin{cases} n!, n \le m \\ m! m^{n-m}, n > m \end{cases}$, $m$ – число каналов в $i$-м узле, $n$ – число пакетов $i$-м узле.

Шаг 6. Найти: загруженность узла $\chi_i = \frac{\lambda_i}{m\mu_i}$; среднюю длину очереди в узле $r_i = P_i(0) \frac{\rho_i^{m+1}}{m! m(1-\chi_i)^2}$; $k_i = \rho_i$; среднее число пакетов в узле $L_i = k_i + r_i$; среднее время пребывания пакета в узле: $T_i = L_i / \lambda_i \quad \forall i = \overline{1, K}$.

Шаг 7. Рассчитать среднюю задержку пакетов в сети: $T = \sum_{i=1}^{K} L_i / \sum_{i=1}^{K} \lambda_i$.

Конец алгоритма.

Для проверки адекватности моделей были проведены расчеты характеристик производительности КТКС в среде Adobe Flash CS3 Professional, а также выполнено их имитационное моделирование [23]. Кроме того, фиксировались данные исследуемых характеристик на экспериментальной установке (рис. 3). В ходе исследований сопоставлялись предсказанные и экспериментальные данные (табл.1).

Таблица 1 - Относительная погрешность предсказания средней задержки пакетов в КТКС

| Метод / Угроза ИБ | Аналитический метод | | Имитационный метод | |
|---|---|---|---|---|
| | «Слабая» СЗИ | «Сильная» СЗИ | «Слабая» СЗИ | «Сильная» СЗИ |
| «Слабая» ВПр | 2,33% | 1,28% | 2,79% | 4,80% |
| «Сильная» ВПр | 2,80% | 0,84% | 7,33% | 6,20% |

Экспериментальные данные в целом подтвердили адекватность моделей. Наибольшие расхождения (до 7,33% для имитационных и до 2,80% для аналитических моделей) наблюдаются при высокой интенсивности ВП («сильной» ВПр) и недостаточной («слабой») СЗИ, что можно объяснить тем, что в моделях практически невозможно учесть ограничения, обусловленные задержками сканирующих подключений в ОС, ограничения на ко-

личество полуоткрытых исходящих соединений, интервал времени, в течение которого подключение находится в режиме ожидания, ограничение на общее число одновременно открытых подключений.

***Глава 3*** посвящена разработке моделей повышения производительности КТКС в условиях воздействия угроз ИБ. На рис. 1 представлена структурная модель обнаружения и противодействия угрозам ИБ [3]. Уровень обнаружения – совокупность СО. На выходе СО формируется сигнал $X_i(t)$ $\left(i=\overline{1,N}\right)$, принимающий либо 1 (угроза ИБ обнаружена), либо 0 (угроза ИБ не обнаружена). $X_i(t)$ характеризуется плотностями распределения вероятностей его появления – $f_y(X_i(t))$ (угроза ИБ есть) и $f_n(X_i(t))$ (угрозы ИБ нет):

$$f_y(X_i(t))=\begin{cases} p_i(t) & при\ \ X_j(t)=1 \\ 1-p_i(t) & при\ \ X_j(t)=0 \end{cases},\quad f_n(X_i(t))=\begin{cases} \overline{p_i}(t) & при\ \ X_i(t)=1 \\ 1-\overline{p_i}(t) & при\ \ X_i(t)=0 \end{cases}.$$

Уровень противодействия – совокупность СП, каждое из которых может быть инициировано при обнаружении угрозы ИБ. Решающий модуль реализует следующий алгоритм: на основании показаний СП $(X_1(t),\ X_2(t),...,X_N(t))$ принимается решение о наличии или отсутствии угроз ИБ: $Z=\begin{cases}1, & \text{если угроза ИБ обнаружена}\\ 0 & \text{в противном случаи}\end{cases}$. Если $Z=1$, то вырабатывается управляющее воздействие $(y_1,\ y_2,...,y_M)$, иначе конец алгоритма.

На рис. 2 представлена модель организации защитных механизмов в КТКС [2, 13]. Вершины графа – объекты и модули защиты. Дуги (связи) графа – возможные пути распространения угроз ИБ в КТКС.

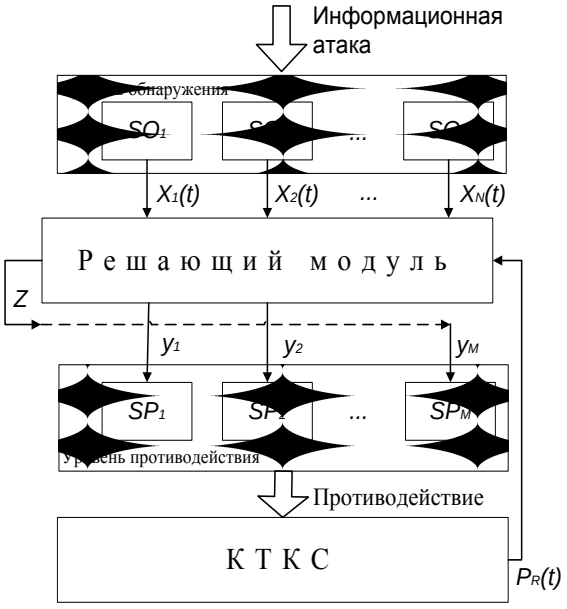


Рисунок 1 - Структурная модель обнаружения и противодействия угрозам ИБ

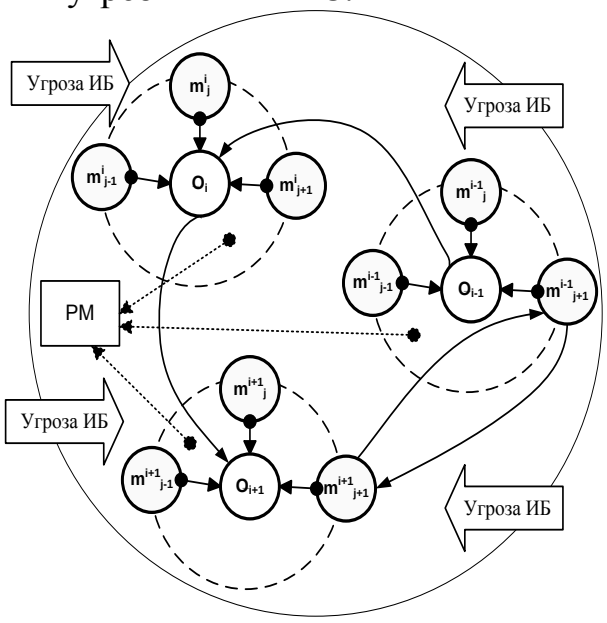


Рисунок 2 – Модель организации защитных механизмов в КТКС

Кольцо защиты (КЗ) - совокупность МЗ, количество и состав, которых

зависит от характеристик объекта защиты. Для каждого КЗ выбирается алгоритм обнаружения угроз ИБ. Сигналы от КЗ обрабатываются общим РМ.

В процессе формирования кольца должны выполняться следующие условия: (1) возможность совместной работы объединяемых СО; (2) обеспечение оптимального времени работы КЗ по обнаружению и противодействию угрозам ИБ; (3) обеспечение заданной вероятности обнаружения угроз ИБ; (4) снижение средней частоты «ложных тревог» [8, 15].

Алгоритм обнаружения угроз ИБ основанный на понятии критической области угроз:

Шаг 1. Снятие показаний, генерируемых СО $x = (X_1(t),\ X_2(t),..., X_N(t))$.

Шаг 2. Если $x \in S^*$ ($S^*$ - критической области угроз (КОУ)), то принимается решение о наличии угрозы ИБ. При этом время обнаружения $T^{\text{ОБ}}$ зависит только от характеристик выбранных СО. Конец алгоритма.

Формирование КОУ [2, 9] - $S^*$. Необходимые вероятностные характеристики для формирования КОУ могут быть представлены разработчиками СО или получены экспериментально. Пусть имеется случайная величина (СВ) $X_0$, которая принимает значение 1, если угроза ИБ есть и 0 в противном случае. Экспериментатор, проводя моделирование, изменяет значение $X_0$. СО вырабатывают сигнал $X_i \left(i = \overline{1, N}\right)$ о наличие угроз ИБ. Предметом исследования является распределение многомерной СВ $(X_0,\ X_1,..., X_N)$. Введем следующие обозначения: $x_0$ – показатель, принимающий значения 0 или 1 (реализация $X_0$); $x = (x_1, x_2,..., x_N)$ – система показателей, где $x_i \ \left(i = \overline{1, N}\right)$ так же принимает одно из двух значений; $S$ – множество всех наборов $x$, состоящее из $K = 2^N$ элементов; $S^*$ – КОУ $\left(S^* \subset S\right)$. Функция $p(x_0, x_1, ..., x_N)$, где $p$ – относительные частоты кода, позволяет определить КОУ. Выборочный закон распределения $X_0$: значению $X_0 = 0$ соответствует вероятность $q_0$, значению $X_0 = 1$ – вероятность $p_0$, где $p_0 = \sum_{x \in S} p(1; x);\ q_0 = 1 - p_0$.

Пусть гипотеза $H_0$ - угрозы ИБ нет $(X_0 = 0)$, $H_1$ – альтернативная $(X_0 = 1)$. Тогда если $x \in S^*$, то гипотеза $H_0$ отвергается. Ошибка I рода $\alpha = \frac{1}{q_0} \sum_{x \in S^*} p(0; x)$. Ошибка II рода $\beta = 1 - \frac{1}{p_0} \sum_{x \in S^*} p(1; x)$. Величина $\alpha q_0$ - вероятность «ложной тревоги», $\beta p_0$ – вероятность «необнаруженной угрозы». Задача построения КОУ состоит в том, чтобы при фиксированном уровне значимости $\alpha$ за счет выбора $S^*$ минимизировать $\beta$.

Алгоритм построения КОУ по экспериментальным данным [16]

Шаг 1. Пронумеровать элементы множества $S$ так, чтобы величины $p(1; x_a) / p(0; x_a)$ не возрастали, где $a = \overline{1, K}$.

Шаг 2. Построить последовательность расширяющихся подмножеств $S_a^* \subset S$: $S_0^* = \varnothing$, $S_1^* = \{x_1\}$, $S_2^* = \{x_1, x_2\}$ и т.д. Если найдутся наборы элементов $x$ с частотой $p(0;x) = 0$, то такие наборы $x$ включаются в $S_0^*$.

Шаг 3. Рассчитать последовательности: $0 = \alpha_0 \le \alpha_1 \le ... \le \alpha_{K'} = 1$, $\beta_0 \ge \beta_1 \ge ... \ge \beta_{K'} = 0$, где $K' \le K$, $\alpha_a = \frac{1}{q_0} \sum_{x \in S^*_a} p(0;x)$, $\beta_a = 1 - \frac{1}{p_0} \sum_{x \in S^*_a} p(1;x)$.

Шаг 4. Вычислить суммы: $\alpha_0 + \beta_0$, $\alpha_1 + \beta_1$ и т.д. Определить номер $a$, которому соответствует наименьшее из полученных значений. Подмножество $S_a^*$ будет являться КОУ. Конец алгоритма.

Алгоритм инициирования уровня противодействия [3]

Шаг 1. Для каждого варианта инициирования уровня противодействия вычисляется вероятность $Q_{ПР}(t)$ и производительность КТКС - $\Phi(П)$.

Шаг 2. Выбирается вариант инициирования СП, которому соответствует максимально возможная вероятность $Q_{ПР}(t)$ при $\Phi(П) \to \max$. Конец алгоритма.

Выбор варианта инициирования уровня противодействия в КТКС – разомкнутой СеМО. Определим, для конкретности, $K$-ый узел, как защищаемый ресурс СеМО. В каждом $i$-м узле $(i = \overline{1, K-1})$ может быть инициировано СП, способное с вероятностью $u_i$ противодействовать угрозам ИБ. Под противодействием будем понимать выброс вредоносного пакета в $(K+1)$-ый узел, который имеет связь только с узлами, в которых инициируются СП. В системе всего $2^{(K-1)} - 1$ варианта инициирования СП, его номер численно равен двоичному числу $j = (x_1\ x_2\ ...\ x_{M-1})_2$, где $x_i = \begin{cases} 1, \text{ если СП инициируется в i}-\text{ом узле} \\ 0 \text{ в противном случаи} \end{cases}$ $(i = \overline{1, K-1})$.

Алгоритм вычисления вероятности противодействия угрозам ИБ

Шаг 1. Построить матрицу $Q$ из матрицы $P_R(t)$:

$$Q = \begin{pmatrix} 0 & p_{01} & p_{02} & ... & p_{0K} \\ p_{10} & p_{11} & p_{12} & ... & p_{1K} \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 \end{pmatrix}.$$

Шаг 2. Если в системе нет СП, то перейти на шаг 3. В противном случае по номеру $j$ ввести в $Q$ противодействие угрозам ИБ:

$$Q = \begin{pmatrix} 0 & p_{01} & ... & p_{0K} & 0 \\ p_{10} & p_{11} & ... & p_{1K} & 0 \\ \hline (1-u_i)\cdot p_{i0} & (1-u_i)\cdot p_{i1} & ... & (1-u_i)\cdot p_{iK} & u_i \\ \hline 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix}.$$

Шаг 3. Задать вектор распределения вероятностей на нулевом шаге:

$e = (1, 0, 0, ..., 0)$.

Шаг 4. Найти распределение вероятностей состояний на $n$-ом шаге: $q(n) = e \cdot Q^n$. Будем считать процесс распространения угроз ИБ завершенным на шаге $n$, если $p_1(n) = p_2(n) = ... = p_{K-1}(n) = 0$. Вероятности поражения ресурса $p_K(n)$, противодействия $Q_{ПР}(t) = p_{K+1}(n)$. Конец алгоритма.

***Глава 4*** посвящена экспериментальному исследованию характеристик производительности КТКС, характеризующейся передачей больших объемов трафика и в условиях воздействия угроз ИБ [1]. Схема экспериментальной установки (аналог фрагмента СПД Администрации Владимирской области) представлена на рис. 3. Приведены результаты 4 экспериментов.

Первый эксперимент проведен для получения динамической характеристики вероятности выявления угроз ИБ средствами обнаружения при различной степени нагрузки на сеть [17, 22]. Результаты эксперимента представлены на рис. 4, где СН - средняя, НН – низкая, ВН – высокая нагрузка на сеть. Характеристики СО сильно зависят от загруженности сети. Время достоверного обнаружения («вероятность обнаружения» / «вероятность «ложной тревоги»» ≥ 9) изменялось от 12 с (СН) до 25 с (ВН).

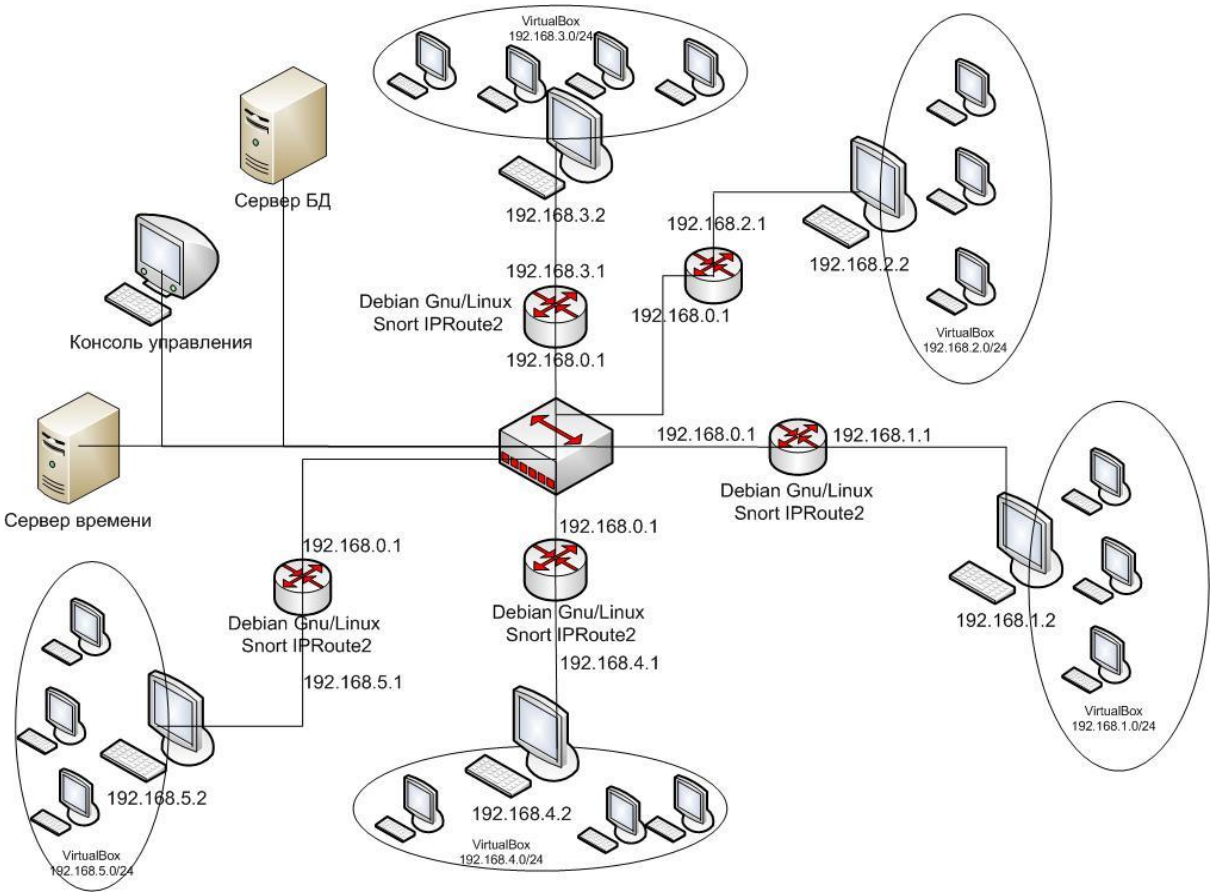


Рисунок 3 – Схема экспериментальной установки

Второй эксперимент предназначен для сравнения вероятностных и

временных характеристик работы кольца защиты, работающего по различным схемам обработки сигналов сенсоров IDS. Анализ результатов исследования показывает выигрыш алгоритма КОУ при различной загруженности сети. Значения относительного уменьшения времени обнаружения ВТ алгоритмом КОУ по отношению к другим алгоритмам обнаружения, рассчитанные по формуле $\left(t_{обн}^{КОУ} - t_{обн}^{алг}\right)/t_{обн}$ при $p_{обн} = 0{,}75$, сведены в таблицу на рис. 5.

Третий эксперимент позволил оценить производительность сети при разной нагрузке в наличии/отсутствии СЗИ. При включении СЗИ производительность сети падает. На снижение производительности влияет величина входящего трафика, так и параметры СЗИ.

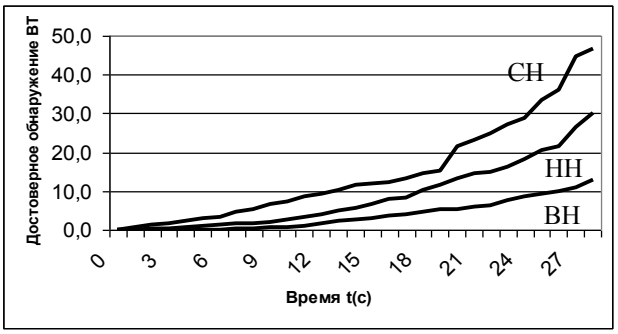


Рисунок 4 – Относительное снижение времени обнаружения вредоносного тра-

| Схема / Нагрузка | «2 из 5» | «3 из 5» | «4 из 5» | «И» | «ИЛИ» |
|---|---|---|---|---|---|
| Низкая | 0,07 | 0,14 | 0,17 | 0,31 | 0,36 |
| Средняя | 0,06 | 0,09 | 0,14 | 0,24 | 0,29 |
| Высокая | 0,05 | 0,07 | 0,17 | 0,21 | 0,23 |

Рисунок 5 - Относительное уменьшение времени обнаружения ВТ в КТКС

В четвертом эксперименте проведена оптимизация СЗИ в экспериментальной сети (рис. 3). График изменения производительности в условиях воздействия ВТ и динамического построения адаптивной СЗИ представлен на рис. 6. Вредоносный трафик в систему стал поступать с 10 с. Производительность сети с этого момента стала подать.

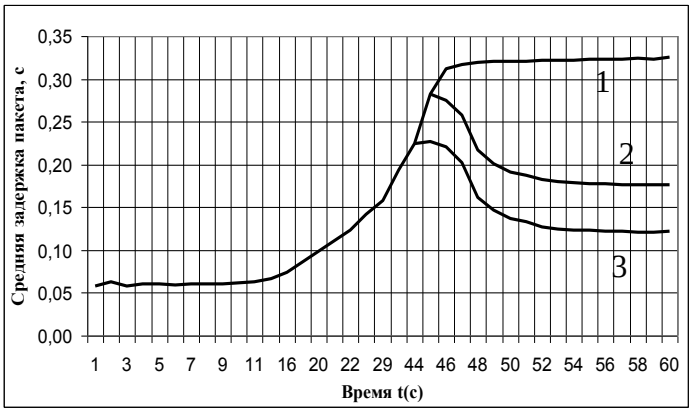


Рисунок 6 – Изменение производительности в экспериментальной сети

В условиях отсутствия СЗИ (1) производительность упала в ≈ 6 раз за 40 с. В условиях типовой СЗИ (2) производительность по сравнению с исходным вариантом уменьшилась в ≈ 3 раза, что может обеспечить нормальное функционирование КТКС. Наилучший вариант, приводящий к снижению производительности всего лишь в 2 раза (3 – оптимальная СЗИ), обеспечивается следующими механизмами: за счет использования алгоритма КОУ снижается время обнаружения ВТ (на 20-25%), с помощью алгоритма расстановки СЗИ в узлах сети в

максимальный режим включается лишь часть СП узлов (3 из 5).

**В заключении** перечисляются **основные выводы и результаты диссертационной работы**:

1. Анализ работ в области исследования КТКС и опыт практических работ позволяют констатировать резкое снижение производительности в условиях воздействия угроз ИБ (до 80%). Современные СЗИ решают данную проблему за счет частичного блокирования вредоносного потока, но обеспечение высокой вероятности обнаружения и задержки, связанные с противодействием ведут к значительному расходованию ресурсов КТКС, что в конечном итоге сопровождается дополнительным снижением системной производительности.

2. Показано, что задача повышения производительности КТКС в условиях воздействия угроз ИБ может быть формализована как задача построения системы защиты, которая смогла бы обеспечить максимально возможный уровень производительности КТКС при достоверном обнаружении и максимально эффективном противодействии угроз ИБ. Для решения поставленной задачи разработаны: аналитические модели оценки производительности КТКС в условиях воздействия угроз ИБ; модели и алгоритмы его достоверного обнаружения за ограниченное время; модель распределенной системы защиты.

3. Предложено семейство аналитических моделей оценки производительности КТКС в условиях воздействия угроз ИБ, отличающихся тем, что они учитывают интенсивность вредоносного потока, длительность функционирования угроз ИБ и средств противодействия. Экспериментально показана их эффективность.

4. Синтезирован алгоритм достоверного обнаружения угроз ИБ за ограниченное время, основанный на понятии «критическая область угроз». Экспериментальные исследования подтвердили уменьшение времени обнаружения на 20-25% по сравнению с традиционными логическими алгоритмами («вероятность обнаружения»/«вероятность «ложной тревоги»$\geq$9).

5. Выработаны научно-технические предложения по реализации модели распределенной системы противодействия угроз ИБ, позволяющие обеспечивать максимально возможный уровень производительности КТКС при эффективном противодействии угроз ИБ (вероятность противодействия, как показатель защищенности, не хуже 0,85).

6. Примеры эффективного апробирования механизмов и средств повышения производительности КТКС в условиях воздействия угроз ИБ дают основание констатировать адекватность и функциональность основных теоретических построений и разработанных на их основе алгоритмических и инструментальных средств. Раннее обнаружение угроз ИБ позволяло оперативно инициировать средства противодействия угроз ИБ в наиболее уязвимых узлах КТКС. В результате производительность КТКС в условиях

воздействия угроз ИБ удалось повысить не менее чем в 2 раза.

**Основные публикации по теме диссертации**

Статьи в изданиях, рекомендуемых ВАК

1. Груздева, Л.М. Экспериментальное исследование производительности корпоративной телекоммуникационной сети [Текст] / Л.М. Груздева, Ю.М. Монахов, М.Ю. Монахов // Проектирование и технология электронных средств. – 2009. – №4. – С. 21-24 (соискатель – 50%).

2. Монахов, М.Ю. Алгоритм раннего обнаружения атак на информационные ресурсы АСУП [Текст] / М.Ю. Монахов, Л.М. Груздева // Автоматизация в промышленности. – 2008. – №3. – С.12-14 (соискатель – 75%).

3. Груздева, Л.М. Алгоритм оптимизации функционирования распределенной системы защиты [Текст] / Л.М. Груздева, М.Ю. Монахов // Системный анализ. Теория и практика. – 2008. – №2. – С. 80-82 (соискатель – 75%).

Учебные пособия с грифом УМО

4. Монахов, Ю.М. Вредоносные программы в компьютерных сетях: учеб. пособие / Ю.М.Монахов, Л.М.Груздева, М.Ю.Монахов; Владим. гос.ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2010. – 72 с. – ISBN 978-5-9984-0087-2 (соискатель – 40%).

5. Груздева, Л.М. Оценка сетевых характеристики компьютерных сетей в условиях информационного вредоносного воздействия: учеб. пособие / Л.М.Груздева, Ю.М.Монахов, М.Ю.Монахов; Владим. гос.ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2010. – 71 с. – ISBN 978-5-9984-0089-6 (соискатель – 40%).

Учебные пособия

6. Устинов, В.Н. Теория вероятностей и моделирование вероятностных процессов в информационной безопасности: учеб. пособие / В.Н.Устинов, Л.М.Груздева и др.; Владим. гос.ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2005. – 92 с. – ISBN 5-89368-623-3 (соискатель – 40%).

7. Груздева, Л.М. Модели объектов информатизации: учебное пособие / Л.М. Груздева, В.Н.Устинов; Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2008. – 76 с. – ISBN 978-5-89368-884-9 (соискатель – 40%).

Статьи

8. Груздева, Л.М. Типовые алгоритмы работы комплекса средств обнаружения угроз информационной безопасности [Текст] / Л.М. Груздева, М.Ю. Монахов // Комплексная защита объектов информатизации. Материалы научно-технического семинара. ВлГУ. – 2005. – С. 58-60 (соискатель – 50%).

9. Груздева, Л.М. Пример формирования критической области в задачи достоверного обнаружения угроз информационной безопасности

[Текст] / Л.М. Груздева, А.Ю. Казарин // Комплексная защита объектов информатизации. Материалы научно-технического семинара. ВлГУ. – 2005. – С. 91-92 (соискатель – 75%).

10. Груздева, Л.М. К вопросу оценки эффективности систем информационной защиты предприятия [Текст] / Л.М. Груздева // Системы и методы обработки и анализа информации: сборник научных статей. – М.: Горячая линия – Телеком. – 2005. – С. 285-293.

11. Груздева, Л.М. Проблема защиты информации в АСУП [Текст] / Л.М. Груздева // Краеведение и регионоведение: межвузовский сборник научных трудов. Выпуск 2 – ВЗФИ. – 2006. – С. 142-143.

12. Груздева, Л.М. Подход к обеспечению надежности работы АСУП [Текст] / Л.М. Груздева, М.Ю. Звягин, А.Ю. Казарин, М.Ю. Монахов // Краеведение и регионоведение: Межвузовский сборник научных трудов. Выпуск 2 – ВЗФИ. – 2006. – С. 144-148 (соискатель – 25%).

13. Груздева, Л.М. Модель распределенной антивирусной защиты информационной системы предприятия [Текст] / Л.М. Груздева // Современные проблемы экономики и новые технологии исследований: межвуз. сб. науч. трудов. ВЗФИ. – 2006. – С.157-158.

14. Груздева, Л.М. Определение среднего времени распространения угроз в распределенной информационно-вычислительной системе АСУП [Текст] / Л.М. Груздева, М.Ю. Монахов // Информационно-телекоммуникационные технологии и электроника. Труды Владимирского государственного университета. Выпуск 1. – Владимир: ВлГУ. – 2006. – С. 77-81 (соискатель – 75%).

Опубликованные доклады и тезисы

15. Груздева, Л.М.Алгоритмы обнаружения угрозы информационной безопасности [Текст] / Л.М. Груздева, М.Ю. Звягин, А.Ю. Казарин, М.Ю. Монахов // Автоматизированная подготовка машиностроительного производства, технология и надежность машин, приборов и оборудования: материалы Международной научно-технической конференции. – Вологда: ВоГТУ. – 2005. С. 153-156 (соискатель – 25%).

16. Груздева, Л.М. О задаче построения критической области угроз информационной безопасности [Текст] / Л.М. Груздева, М.Ю. Звягин, М.Ю. Монахов // Математические методы в технике и технологиях. Сборник трудов XIX Международной научной конференции. – ВГТА г.Воронеж. – 2006. – С.194-196 (соискатель – 30%).

17. Груздева, Л.М. Экспериментальное исследование антивирусных программ в распределенных информационных системах [Текст] / Л.М. Груздева // Образовательная среда сегодня и завтра: Материалы III Всероссийской научно-технической конференции. – М.: Рособразование. – 2006. – С. 168-169.

18. Груздева, Л.М. Решение жестких задач динамики распростране-

ния вредоносных программ / Л.М. Груздева // Математические методы в технике и технологиях – ММТТ-20. [Текст]: сб. трудов XX междунар. науч. конф. Т. 6. – Ярославль: Изд-во Ярос. гос. техн. ун-та. – 2007. – С. 63-65.

19. Груздева, Л.М. Об одной математической модели динамики распространения вредоносных программ / Л.М.Груздева, Ю.М.Монахов // Математические методы в технике и технологиях – ММТТ-20. [Текст]: сб. трудов XX междунар. науч. конф. Т. 6. – Ярославль: Изд-во Ярос. гос. техн. ун-та. – 2007. – С. 65-66 (соискатель – 75%).

20. Груздева, Л.М. Анализ вероятностных характеристик распространения вируса в компьютерной системе [Текст] / Л.М. Груздева, М.Ю. Монахов // Проблемы эффективности безопасности функционирования сложных технических и информационных систем. Сборник №2. Труды XXVI Международной научно-технической конференции. – Серпухов, Серпуховской ВИ РВ. – 2007. – С. 44-47 (соискатель – 75%).

21. Груздева, Л.М. Исследование SIR-модели динамики распространения вредоносных программ / Л.М. Груздева // Математические методы в технике и технологиях – ММТТ-21. [Текст]: сб. трудов XXI междунар. науч. конф. Т. 5. - Саратов: Сарат. гос. техн. ун-т. – 2008. – С. 242-244.

22. Груздева, Л.М. Исследование влияния вредоносных и антивирусных программ на характеристики открытой компьютерной сети / Л.М. Груздева // Математические методы в технике и технологиях – ММТТ-22. [Текст]: сб. трудов XXII междунар. науч. конф. - Иваново: издательство ИГХТУ. – 2009. – С. 208-210.

23. Груздева, Л.М. Имитационное моделирование корпоративной сети в условиях вредоносного информационного воздействия [Текст] / Л.М. Груздева // Имитационное моделирование. Теория и практика / Сборник докладов четвертой всероссийской научно-практической конференции. Т. 2. – Санкт-Петербург. – 2009. – С. 60-64.

24. Груздева, Л.М. Модель оценки трудоемкости обнаружения вредоносных программ в компьютерных системах / Л.М. Груздева // Математические методы в технике и технологиях – ММТТ-23. [Текст]: сб. трудов XXIII междунар. науч. конф. Т. 9. – Саратов: Сарат. гос. техн.ун-т . – 2010. – С. 160-162.

Подписано в печать
Формат 60×84/16. Усл. печ. л. 1,16. Тираж 100.
Заказ
Издательство
Владимирского государственного университета
600000, Владимир, ул. Горького, 87