На правах рукописи

Басыня Евгений Александрович

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНО-АДАПТИВНОГО УПРАВЛЕНИЯ ТРАФИКОМ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Специальность 05.13.01 – Системный анализ, управление и обработка информации (в промышленности)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Новосибирск - 2014

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Новосибирский государственный технический университет»

Научный руководитель:	доктор технических наук, доцент **Французова Галина Александровна**
Официальные оппоненты:	**Мамойленко Сергей Николаевич**, доктор технических наук, доцент, Сибирский государственный университет телекоммуникаций и информатики, заведующий кафедрой вычислительных систем
	Пестунова Тамара Михайловна кандидат технический наук, доцент, Новосибирский государственный университет экономики и управления, заведующая кафедрой информационной безопасности
Ведущая организация:	Конструкторско-технологический институт вычислительной техники Сибирского отделения Российской академии наук

Защита состоится «03» марта 2015 г. в 10.00 часов на заседании диссертационного совета Д 212.173.05 при Новосибирском государственном техническом университете по адресу 630073, г. Новосибирск, пр. К. Маркса, д. 20.

С диссертацией можно ознакомиться в библиотеке Новосибирского государственного технического университета и на сайте http://www.nstu.ru.

Автореферат разослан «23» января 2015 г.

Ученый секретарь
диссертационного совета  Чехонадских Александр Васильевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Информационно-коммуникационные технологии оказывают существенное влияние на уровень экономической конкурентоспособности и национальной безопасности государства. Сетевые инфраструктуры государственных учреждений и частных предприятий в преимущественном большинстве организованы на технологии Ethernet и подключены к глобальной сети Интернет, функционирующей на основе стека протоколов TCP/IP и широко распространенной по всему миру. Однако, данные технологии имеют ряд уязвимостей, обусловленных в первую очередь алгоритмами протоколов различного уровня взаимодействия на базе «жесткой» логики.

Необходимость оптимизации загрузки каналов связи в корпоративных вычислительных сетях (в том числе и географически распределенных) является одной из приоритетных задач современных IT-технологий. Другим немаловажным аспектом является защита процесса передачи данных. Уровень обеспечения информационной безопасности является следствием эффективности методов управления трафиком. Для достижения данных целей разрабатываются специальные методы управления трафиком вычислительных сетей.

Так вопросы управления трафиком корпоративных вычислительных сетей с точки зрения обеспечения надежного функционирования рассмотрены в работах Вишневского В.М., Рыкова В.В., Ивницкого В.А., Вербицкого С.Н., Kelly F.P., Korilis Y.A., Altman E., Turner S.и др. [1-7]. Однако, данные исследования не принимают в расчет человеческий фактор, инсайдерские угрозы, имеющие место в реальных системах.

С 2009 года ключевым трендом развития алгоритмов и методов управления трафиком локальных вычислительных сетей (ЛВС) являются исследования в области технологий обнаружения аномальной активности сетевого трафика по сигнатурным, поведенческим, комбинированным методикам с обеспечением информационной безопасности. Результаты, полученные в этом направлении, опубликованы в работах следующих ученых: Ажмухамедов И.М., Гамаюнов Д.Ю., Качалин А.И., Марьенков, А. Н., Селин Р.Н., P. Lippmann, R. Kwitt, M. Szmit, L. Chang и др. [8-26]. Данные методы функционируют на основе жесткой логики с потребностью в поддержке квалифицированными специалистами. Они не способны адекватно реагировать на новые сетевые угрозы и объективно анализировать полезную часть дейтаграмм.

Вопросы автомодельности сетевого трафика, а также модернизация инструментария накопления статистических данных для проверки и фильтрации сетевых пакетов по их содержимому (англ. *Deep Packet Inspection*, сокр. DPI) представлены в работах Меретукова Ш.Т., Габдрахманова А.А., Скуратова А.К., Тихомирова И.А., Cho Y.H., Wang G., Tao Y., Ansari N.и др. [27-40].

Данные методы не ориентированы на функционирование в реальных системах с криптографическими протоколами и/или элементарным дроблением пакетов для сокрытия их типа (как, например, организовано в Tor-сетях). Эти обстоятельства обуславливают необходимость разработки новых методов интеллектуально-адаптивного управления трафиком вычислительных сетей, которые позволят оптимизировать загрузку каналов связи и повысить уровень обеспечения информационной безопасности (ИБ), в том числе минимизируя человеческий фактор.

Цель работы заключается в разработке нового метода интеллектуально-адаптивного управления трафиком корпоративных вычислительных сетей, обеспечивающего оптимизацию загрузки каналов связи, высокий уровень информационной безопасности и минимизацию человеческого фактора.

Для достижения указанной цели в работе были поставлены и решены следующие **основные задачи**:

1. разработка метода интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей;
2. разработка алгоритма управления информационными потоками корпоративных ЛВС;
3. формирование системы интеллектуально-адаптивного управления трафиком вычислительной сети с коммутацией пакетов (СИАУ);
4. программная реализация предложенной СИАУ;
5. экспериментальное исследование функциональных возможностей разработанного вычислительного комплекса СИАУ, анализ его комплексной эффективности (быстродействия, уровня обеспечения информационной безопасности и др.), сравнение с коммерческими продуктами.

Методы исследований. Для решения поставленных задач использованы методы системного анализа, теории принятия решений, математического и имитационного моделирования, теории вероятностей, математической статистики, аппарат нечеткой логики, методы и модели интеллектуальных и стохастических систем.

Достоверность и обоснованность работы подтверждается корректным использованием математических методов, данными экспериментальных исследований в сравнении с существующими коммерческими решениями, публикациями в центральной печати, докладами на международных и региональных научно-технических конференциях.

Научная новизна работы состоит в следующем:

1. разработан новый метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей с применением модифицированной генетической алгоритмизации и нечеткой логики, позволяющий прогнозировать реакцию хостов на

различные виды сетевых воздействий посредством распределенного анализа на модельных объектах. Отличие от существующих методов заключается в обеспечении минимизации загрузки канала связи выбором оптимальной стратегии управления трафиком при различных типах сетевой активности, а также автоматической идентификацией новых сетевых угроз и выработкой оптимального решения по их устранению;

2. разработан оригинальный алгоритм управления информационными потоками корпоративных вычислительных сетей на базе распределенной обработки данных с фрагментацией пакетов на экземпляры случайной длины, изменением флагов дейтаграмм (в допустимых рамках), привнесением различных задержек на обработку каждого пакета узлом-отправителем и всеми промежуточными звеньями, а также генерацией фальшивого p2p трафика. Как следствие, алгоритм исключает возможность осуществления автоматического и автоматизированного анализа трафика (с пресечением потенциальной возможности корреляции параметров прохождения дейтаграмм и идентификации автомодельности), а также риск прогнозирования продвижения трафика; обеспечивает защиту от инсайдерских атак, сниффинга и дешифровки, тайминг-атак глобальным наблюдателем;

3. реализована система интеллектуально-адаптивного управления трафиком вычислительной сети, обеспечивающая эффективное функционирование в условиях аномальной активности трафика.

Основные положения, выносимые на защиту:

- метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей;
- алгоритм управления информационными потоками корпоративных вычислительных сетей;
- структура системы интеллектуально-адаптивного управления трафиком вычислительной сети с коммутацией пакетов.

Практическая значимость работы. Использование разработанных методов управления трафиком в ЛВС позволяет существенно повысить эффективность управления информационными потоками в вычислительных сетях с коммутацией пакетов. Результаты исследования могут быть использованы как в государственных учреждениях, так и в корпоративном секторе, где возникает необходимость защиты передачи данных в корпоративных вычислительных сетях от несанкционированных воздействий.

Соответствие диссертации паспорту научной специальности. Основным содержанием диссертации является разработка методов и алгоритмов решения задач обработки и управления информацией, а также разработка специального программного обеспечения соответствующих систем.

Таким образом, отраженные в диссертации научные положения соответствуют формуле специальности 05.13.01 «Системный анализ,

управление и обработка данных (в промышленности)», а результаты научного исследования соответствуют п. 4, п. 5, п. 12 паспорта специальности.

Апробация работы. Научные положения и практические рекомендации диссертационной работы в целом, а также отдельные ее разделы докладывались и обсуждались на международных научно-технических конференциях «Global Science and Innovation» (USA-Chicago, 2013 г.), «Перспективное развитие науки, техники и технологий» (г. Курск, 2013 г.), «Современные тенденции в образовании и науке» (г. Тамбов, 2013 г.), «Компьютерные технологии в науке, производстве, социальных и экономических процессах» (г. Новочеркасск, 2013 г.), «Перспективные инновации в науке, образовании, производстве и транспорте» (г. Одесса, 2013 г.), «Нелинейные динамические системы: моделирование и оптимизация управления» (г. Новосибирск, 2012 г.) и всероссийских научно-технических конференциях «Искусственный интеллект: философия, методология, инновации» (г. Москва, 2013 г.), «Наука. Технологии. Инновации» (г. Новосибирск, 2013 г.), «Новые информационные технологии в научных исследованиях» (г. Рязань, 2013 г.), «Актуальные проблемы электронного приборостроения» (г. Новосибирск, 2012 г.), а также на кафедре автоматики НГТУ (2012-2014 гг.).

Внедрение результатов. Результаты диссертационной работы были внедрены в ИКТ-сектор мэрии города Новосибирска, департамент энергетики, жилищного и коммунального хозяйства города, МУП «Энергия» (приложение А) и холдинг ООО ТД «Басон» (приложение Б), а так же в Новосибирском государственном техническом университете при разработке учебно-методического обеспечения дисциплин «Вычислительные машины, системы и сети», «Системное администрирование» и «Безопасность информационных ресурсов» на кафедре автоматики (приложение В).

Публикация результатов работы. Основные результаты диссертации отражены в 16 научных трудах, в том числе 2 публикации в рецензируемых научных журналах. В работах, опубликованных в соавторстве, доля материалов, принадлежащих автору диссертации, составляет не менее 70%. Кроме того, получено свидетельство о государственной регистрации программы для ЭВМ (№ 2014615697 «Self-organizing control system of computer network traffic» в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности, приложение Г).

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав, заключения, списка литературы из 101 наименования и 5 приложений. Общий объем работы - 150 страниц, включая 27 рисунков.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснованы актуальность и практическая значимость работы, сформулированы основные задачи исследования и пути их решения.

В **первой главе** проанализированы основные подходы к управлению трафиком вычислительной сети с коммутацией пакетов (Ethernet) на основе стека протоколов TCP/IP. Исследованы слабые стороны алгоритмов коммутации и протоколов маршрутизации, способов обеспечения качества обслуживания (анализа и управления очередями, кондиционирования трафика, обратной связи, резервирования ресурсов, инжиниринга трафика, профилирования и др.), интеллектуальных функций сетевого оборудования уровней 2-7, а также различных протоколов стека TCP/IP. Рассмотрены основные уязвимости, составляющие угрозу целостности, доступности и конфиденциальности передаваемой по сети информации. Выделены недостатки «жесткой» логики в существующих методиках. Изложены современные тенденции развития алгоритмов и методов управления трафиком ЛВС, выделены основные недостатки и достоинства.

На примерах протоколов различных уровней стека OSI (а также TCP/IP) приведен анализ методов управления трафиком по защищенным каналам. Рассмотрены вопросы аутентификации и авторизации абонентов, шифрования и проверки целостности поступающих сообщений по различным протоколам. Выделены проблемы организации виртуальных частных сетей в срезе коммерческих и бесплатных решений.

Представлены методы управления трафиком в оверлейных сетях (работающих поверх глобальной сети Интернет) в сравнительном анализе по оптимизации пропускной способности канала связи, уровню обеспечения анонимизации и информационной безопасности. Рассмотрены как узкоспециализированные (JAP, Mixminion), гибридные (TOR, Psiphon), так и децентрализованные распределенные анонимные сети (Gnutella2, I2P). Представлена оценка рисков воздействия тайминг атак, идентификаций отпечатков, ассоциации анонимного и псевдонимного трафика, атаки на TCP timestamp и других видов злоумышленных действий, использующих уязвимости алгоритмов управления трафиком.

Сформулированы основные задачи диссертационного исследования.

Во **второй главе** изложена разработка метода интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей (в ряде печатных работ по теме диссертации именован как «метод противодействия сетевым угрозам»). Задача управления трафиком ЛВС (объект исследования) может быть решена различными способами. Критерием оптимальности J в рассматриваемой задаче выбран суммарный критерий минимизации загрузки линии связи J_1 и быстродействия J_2:

$$J = J_1 + J_2 = \min_{u \in \Omega_u} F(u, h, t) + \min_{u \in \Omega_u} T \qquad (1)$$

где u - управляющее воздействие (набор команд модулям системы согласно стратегии реагирования); Ω_u - рабочая область управляющих воздействий; $F(u,h,t)$ - функция загрузки канала, в связи с отсутствием возможности представления в математическом виде, рассматриваемая как нелинейная, псевдослучайная, описывающая изменение пропускной способности ЛВС во времени *t*; *h* - злоумышленные сетевые воздействия, неполадки в работе ЛВС; *T* - время принятия решений по управлению.

Стоит отметить, что внешними возмущениями считаются как аппаратно-программные неполадки, так и злоумышленные воздействия и человеческий фактор. Таким образом, осуществляется выбор оптимальной стратегии реагирования на несанкционированные воздействия с обеспечением информационной безопасности.

Существующие системы используют «жесткую» логику поведения, не проводящую сравнительного анализа и поиска оптимального решения (минимизирующего загрузку канала связи и обеспечивающего более высокий уровень информационной безопасности). Это позволяет хакерам идентифицировать продукт защиты атакуемого объекта посредством сканеров/зондеров и задействовать известные уязвимости. Для устранения этого недостатка следует использовать методы и алгоритмы, обладающие интеллектуально-адаптивными свойствами.

Выбор стохастических методов обусловлен необходимостью динамической автономной оптимизации с низкой потенциальной возможностью прогнозирования «извне». Локально-градиентный метод, векторно-адаптивный методы не применяются в силу проблемы «остановки» в локальных экстремумах. Больцмановское обучение, обратное распространение и адаптация Коши требуют корректировки начальной выборки, близкой к оптимальной, что в рассматриваемой задаче не может быть гарантировано. Ряд других методов не представляется возможным реализовать в связи с вышеупомянутой проблемой составления математической модели трафика вычислительной сети. Отсюда очевидна необходимость применения методов синтеза самоорганизующихся адаптивных систем - по причине невозможности определения даже приблизительного порядка системы. Одной из приемлемых методик является генетическая алгоритмизация (ГА), позволяющая получить устойчивые решения при значительном недостатке априорной информации о структуре системы и характере возмущений [71].

Использование ГА в рамках данной работы обосновывается их преимуществами: гибкостью функционирования, высокой скоростью поиска решений на нелинейных функциях, возможностью эффективного распараллеливания вычислений, возможностью выхода из локальных на глобальные экстремумы и др. Необходимость принятия решений в условиях приближенных рассуждений обуславливает использование нечеткой логики (англ. *fuzzy logic*). Технологии нейронных, гибридных и др. сетей являются избыточным инструментом в срезе исследуемой задачи.

В ходе проведенного сравнительного анализа было принято решение об использовании ГА совместно с нечеткой логикой, что явилось основой разработанного метода управления трафиком.

Поскольку в задаче оптимизации канала связи с обеспечением высокого уровня информационной безопасности некоторые экземпляры решений недопустимы (могут привести к выходу из строя информационной системы), а также необходимо реализовать механизмы подмены и прогнозирования реакций на модельных объектах (МО) СИАУ, то требуется модернизация ГА. Данные вопросы решаются вводом дополнительного фильтра после создания поколений, контура функционирования нечеткой логики и блока прогнозирования (рисунок 1).

С помощью модельных объектов СИАУ возможно прогнозировать реакции системы, по обратной связи корректировать начальную выборку (новые поколения). Идентичная подстройка фильтра с использованием нечеткой логики позволяет выбирать из правильных решений наиболее оптимальные, что приводит к минимизации загрузки канала связи.

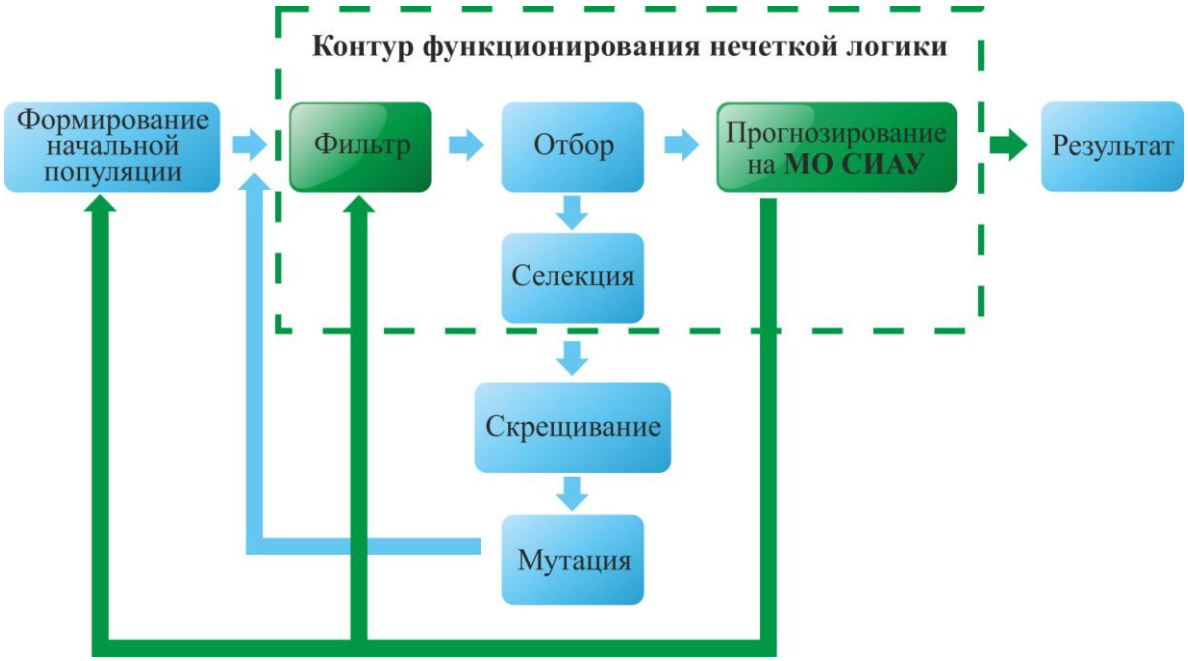

Рисунок 1 - Блок-схема модернизированного генетического алгоритма поиска оптимального решения задачи минимизации загрузки канала связи

Идея генетической алгоритмизации заимствована у природы и заключена в организации эволюционного процесса. Популяцией особей выступает конечное множество альтернативных решений. Хромосомы выражают составляющие действия в решении и являются упорядоченными последовательностями генов, описывающих параметры задачи. В качестве оценки приспособленности предлагается использовать стоимостную функцию

$$\omega(t_i) = N \cdot \overline{traffic} + \frac{\sum_{i \in N}(traffic(t_i) - \overline{traffic})}{2}, \qquad (2)$$

где N - количество измерений нагрузки канала в рассматриваемом интервале времени T; $\overline{traffic}$ - среднее арифметическое значение загрузки канала в этом интервале времени; $traffic(t_i)$ - значения нагрузки канала для каждого отсчета времени t_i, $i \in N$.

С целью улучшения быстродействия системы производится распараллеливание анализа генерируемых решений СИАУ перенаправлением идентичных информационных потоков на модельные объекты, подключенные к альтернативному каналу связи. Для каждого из этих решений на соответствующем МО высчитывается функция приспособленности. Условие остановки алгоритма необходимо рассчитывать в условиях приближенных рассуждений. Поэтому здесь задействуется блок нечеткой логики. Для оценки эффективности решения используется функция приспособленности:

$$F_i = \frac{\Delta\omega(t_i)}{\omega(t_i)} \times 100\% \quad (3)$$

С ее помощью производится подсчет процентного соотношения приращения значения стоимостной функции $\Delta\omega(t_i)$ к значению стоимостной функции в момент до принятия решения $\omega(t_i)$. Данный показатель рассчитывается для каждой изучаемой особи (хромосомы, экземпляра решения, стратегии реагирования) на модельных объектах.

Система анализирует текущие и статистические значения функций приспособленности (F_i) всей популяции особей. Вычисляя средние значения и среднеквадратичные отклонения (СКО) для их множеств, блок нечеткой логики может принять одно из следующих решений (процентные соотношения могут динамически изменяться):

1) если текущее среднее значение лучше статистического более чем на 5%, то выбрать лучшую особь, применить к реальной системе, не останавливать работу генетического алгоритма;
2) если количество итераций < 3; то не останавливать работу ГА;
3) если количество итераций ≥ 3, все решения хуже статистических, то остановить работу генетического алгоритма;
4) если количество итераций ≥ 3, текущее среднее значение лучше статистического не более чем на 5% и СКО ≤ 5%, то выбрать лучшую особь, применить к реальной системе, остановить работу ГА;
5) если количество итераций ≥ 3, значение для лучшей особи превосходит статистическое не более чем на 5% и СКО ≤ 40%, то выбрать лучшую особь, применить к реальной системе, перезапустить работу ГА;
6) если количество итераций ≥ 3, значение для лучшей особи превосходит статистическое не более чем на 5% и СКО > 40%, то выбрать лучшую особь, применить к реальной системе, перезапустить работу генетического алгоритма с дополнительными параметрами фильтра;

С первого по шестой пункты динамически подстраиваются параметры фильтра. В случае идентификации крайне отрицательного решения, подтвержденного статистикой к различным типам атак, особь

исключается из допустимой выборки начальной популяции. Временные интервалы исследования решений и условия выбора корректируются блоком нечеткой логики. В случае отключения информационных потоков, проброшенных на МО (например, оппоненты прекратили взаимодействие), СИАУ перенаправляет очередную порцию клиентов на данный объект. Действие производится для обеспечения равномерного распределения нагрузки на линии связи, предоставляемые модельным объектам.

Блок-схема функционирования информационной системы на основе предлагаемого метода проиллюстрирована на рисунке 2, где пунктиром выделены основные стадии и этапы рабочего процесса.

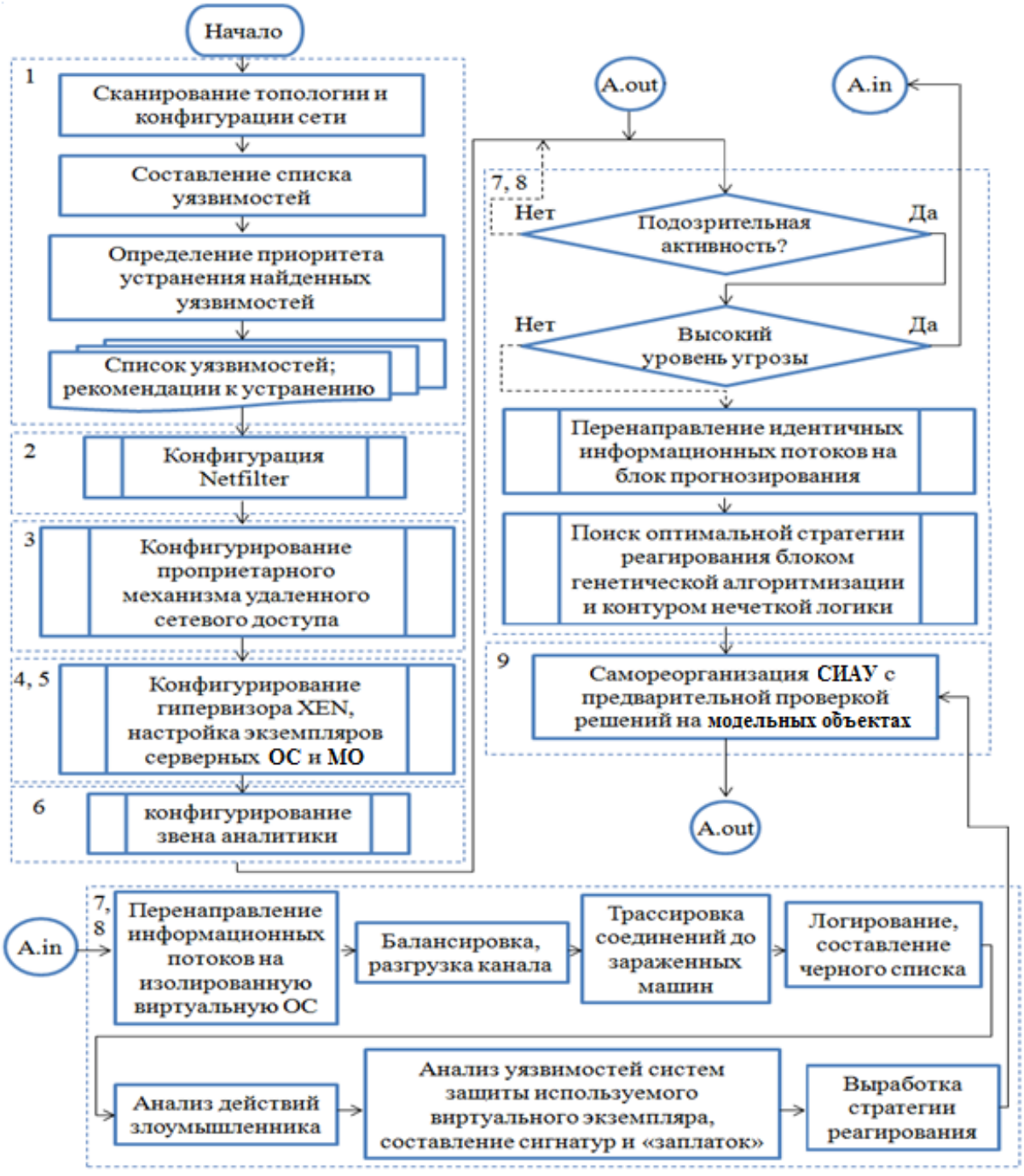

Рисунок 2 - Блок-схема функционирования СИАУ с использованием метода управления трафиком на межсетевых узлах ЛВС

СИАУ содержит звено аналитики, которое ведет статистику по объектам, классам и группам объектов. Разграничиваются угрозы, атаки и решения. Процентное соотношение генетических рулеток адаптивно изменяется в зависимости от статистики звена аналитики. Однако, для повышения эффективности работы ГА элитарное доминирование пресекается нечеткой логикой.

В случае идентификации высокой степени угрозы или попыток сканирования/зондирования системы СИАУ задействует блок фальсификации заранее подготовленных серверных решений. Злоумышленник перенаправляется на изолированный поддельный модельный объект, где пытается осуществить враждебные действия. Система отслеживает поведение, и, в случае успешного взлома/вывода из строя МО, создает детальное описание уязвимости установленной на ней операционной системы. Производится автоматическое генерирование «заплатки», из выборки исключаются решения с данной уязвимостью.

Для усложнения попыток активного и пассивного анализа установленного ПО была разработана библиотека генерации псевдослучайных чисел. На ее основе осуществляется выбор фальсифицированных модельных объектов сервера с предустановленными операционными системами (ОС) для перенаправления на них злоумышленников. Выборка ОС представлена линейкой Windows Server 03-12, Red Hat Enterprise Linux, CentOS, Debian, Ubuntu, Solaris и др.

В дополнение, звено аналитики включает инструментарии для идентификации злоумышленника посредством трассировки соединения, а также дальнейшего составления «черного» списка. Использование теории вероятности и методов статистики в сочетании с выставлением «информационных ловушек» позволяют также установить круг соучастников (или зараженных вредоносным кодом и подчиненных хакеру хостов). Соответственно, СИАУ динамически самообучается и самореорганизуется.

Работа СИАУ предполагает последовательное выполнение операций:

1) первоначальное сканирование топологии и конфигурации сети;
2) конфигурирование базовых правил системы управления трафиком с учетом текущей политики безопасности;
3) конфигурирование механизма удаленного сетевого доступа;
4) формирование блока прогнозирования: установка и синхронизация модельных объектов СИАУ;
5) развертывание блока фальсифицирования: установка и конфигурирование изолированных виртуальных серверов с различными операционными системами и программным обеспечением;
6) конфигурирование звена аналитики;
7) динамический анализ трафика, идентификация попыток сканирования/зондирования/взлома. В случае обнаружения

подозрительной сетевой активности системой производится оценка угрозы и предпринимается, в зависимости от ситуации, следующее действие:

7.1. в случае низкой и средней степени угрозы производится перенаправление идентичных информационных потоков на модельные объекты (п. 4), подключенные к альтернативному каналу связи. Задействуются блок генетической алгоритмизации и контур нечеткой логики, осуществляющие поиск оптимальной стратегии реагирования (минимизирующей загрузку канала связи, обеспечивающей высокий уровень ИБ);

7.2. в случае идентификации высокой степени угрозы или попыток сканирования/зондирования системы задействуется блок фальсификации заранее подготовленных серверных решений (п. 5). Составляются сигнатуры новых уязвимостей, формируются «заплатки»;

8) трассировка и идентификация хостов-злоумышленников и дальнейшее их внесение в черный список с временной блокировкой - действие «юрисдикции» звена аналитики;

9) систематическая самореорганизация системы с предварительной проверкой решений на ее МО.

Спроектированная таким образом система способна автономно видоизменять существующие и создавать новые алгоритмы реагирования, идентифицировать ранее неизвестные уязвимости операционных систем и создавать «заплатки» к ним, производить минимальную идентификацию злоумышленников. Соответственно, СИАУ динамически самообучается и самореорганизуется с предварительной доскональной проверкой решений на собственных модельных объектах.

Таким образом, использование разработанного метода позволяет обеспечить:

- динамическое самообучение и самореорганизацию ИС (с автоматической идентификацией новых сетевых угроз и выработкой оптимальной стратегий по их устранению);
- минимизацию загрузки канала связи (выбор оптимальной стратегии управления трафиком при различных типах сетевой активности);
- минимизацию человеческого фактора (автоматическое функционирование системы с защитой от инсайдерских атак и автономным принятием решений);
- высокий уровень информационной безопасности с невозможностью прогнозирования стратегии реагирования системы как с локальной вычислительной сети предприятия, так и «извне».

Третья глава посвящена проблеме управления трафиком корпоративных вычислительных сетей. Обусловлено это тем, что уровень обеспечения ИБ является следствием эффективности методов управления трафиком. Дополнительно освещена проблематика человеческого фактора и инсайдерских атак.

В целях минимизации рисков по данным угрозам разработан алгоритм управления информационными потоками корпоративных вычислительных сетей, в основу которого заложена распределенная система шифрования. Блок-схема предлагаемого алгоритма представлена на рисунке 3, где пунктиром выделены основные этапы работы.

Данная идея появилась при изучении «луковой маршрутизации» tor-сетей, созданных для анонимизации серфинга в сети интернет. При этом устранены уязвимости оверлейных сетей и технологий, изложенных в первой главе, разработана более надежная программная основа и принцип шифрования реализован более безопасным способом.

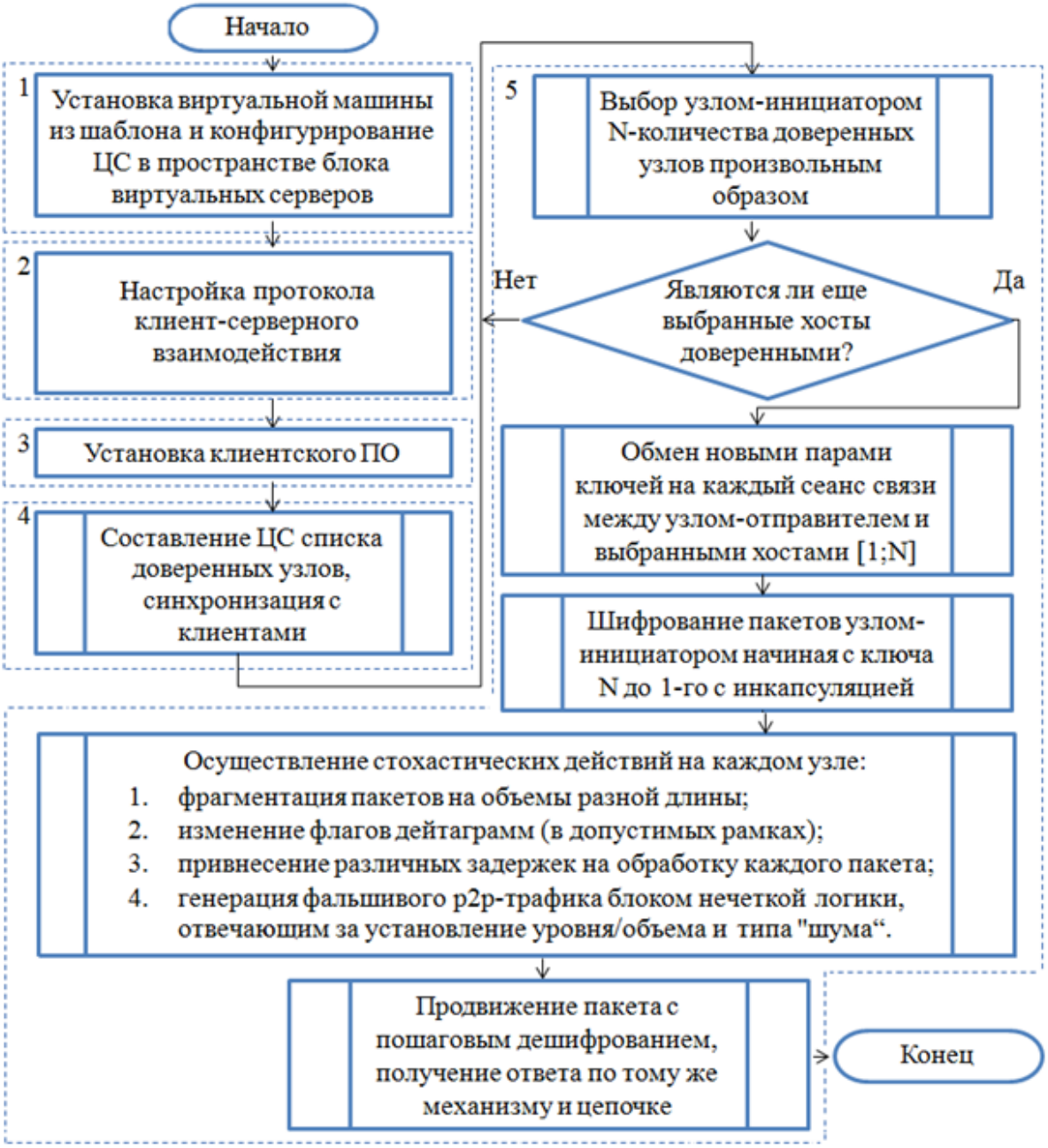

Рисунок 3 - Блок-схема функционирования СИАУ с использованием метода управления информационными потоками корпоративных вычислительных сетей

Разработанный метод (в ряде печатных работ по теме диссертации именован как «метод обеспечения конфиденциальности информационных потоков корпоративной сети») лежит в основе оригинальной системы управления трафиком вычислительной сети и предполагает последовательное выполнение следующих операций:

1) установка и конфигурирование доверенного удостоверяющего центра сертификации корпоративной сети в блоке виртуальных серверов;

2) настройка протокола клиент-серверного взаимодействия. Блок нечеткой логики с использованием различных параметров ИКТ предприятия и привнесением стохастических величин обеспечивает уникальность параметров протокола для каждой компании;

3) установка клиентской части программного обеспечения на рабочих станциях через групповые политики или «вручную»;

4) составление ЦС списка доверенных узлов, синхронизация его с клиентской частью;

5) обмен данными, организованный в следующей последовательности:

5.1. выбор узлом-инициатором N-количества доверенных узлов произвольным образом (благодаря разработанной библиотеке генератора псевдослучайных чисел);

5.2. проверка актуальности информации: являются ли еще выбранные хосты доверенными в рамках данной корпорации (дополнительное согласование по закрытому протоколу с ЦС);

5.3. обмен новыми парами ключей на каждый сеанс связи между узлом-отправителем и хостами [1;N];

5.4. шифрование пакетов узлом-инициатором, начиная с ключа N до 1-го, инкапсулируя содержимое таким образом, чтобы каждый участник взаимодействия мог дешифровать лишь свою часть и просмотреть информацию о следующем адресе пересылки;

5.5. фрагментация пакетов на экземпляры случайной длины, изменение флагов дейтаграмм (в допустимых рамках), привнесение различных задержек на обработку каждого пакета узлом-отправителем и всеми промежуточными звеньями. Приведенные действия производятся со стохастическим подходом, для сокрытия типа содержимого дейтаграмм и усложнения анализа (с пресечением возможности корреляции параметров, идентификации автомодельности и тайминг-атак глобальным наблюдателем). Еще одним инновационным инструментом, усложняющим дешифровку трафика злоумышленнику, является генерация фальшивого p2p трафика клиентским программным обеспечением с блоком нечеткой логики, отвечающим за установление уровня/объема и типа «шума»;

5.6. продвижение пакета с пошаговым дешифрованием и выполнением п. 5.5. Лишь последний узел декапсулирует пакет окончательно и по зашифрованному каналу (например https) передает информацию и прогоняет ответ по той же цепочке.

Этап 5.5 порождает резкое возрастание объема трафика. Для минимизации загрузки линии связи был разработан и включен в систему дополнительный модуль инжиниринга трафика с разработанным новым алгоритмом выбора маршрутов по распределению информационных потоков. Данный алгоритм заключается в рассмотрении хостами упреждающих воздействий с блока прогнозирования СИАУ и анализе состояния коммутационных узлов (в том числе и выбранных в цепочку передачи информации). В совокупности с ранее изложенным методом управления трафиком на межсетевых узлах локальных вычислительных сетей данная методика формирует алгоритм регулирования загрузки канала связи.

Иллюстрация примера работы информационной системы на основе предложенного метода представлена на рисунке 4.

Рисунок 4 - Общая схема шифрования информационных потоков в корпоративной сети с использованием СИАУ

При использовании данного метода попытки дешифровки информационных потоков и деанонимизации источника являются нерентабельной задачей (временные, технические и материальные издержки значительно превышают выгоду от дешифрованного потока информации одного случайного источника за малый период времени).

Применение разработанного алгоритма позволяет обеспечить:

- оптимизацию загрузки канала связи (посредством предложенного инжиниринга генерируемого псевдо-трафика);

- исключение возможности осуществления автоматического и автоматизированного анализа трафика (с пресечением потенциальной возможности корреляции параметров прохождения дейтаграмм и идентификации автомодельности);
- исключение возможности прогнозирования продвижения трафика, как из локальной вычислительной сети предприятия, так и «извне»;
- минимизацию человеческого фактора (автоматическое функционирование системы с защитой от инсайдерских атак);
- высокий уровень информационной безопасности (защита от сниффинга и дешифровки, тайминг-атак глобальным наблюдателем).

Следует отметить, что фрагментация пакетов на экземпляры случайной длины, изменение флагов дейтаграмм (в допустимых рамках), привнесение различных задержек на обработку каждого пакета узлом-отправителем и всеми промежуточными звеньями, а также генерация фальшивого p2p трафика являются оригинальными для систем управления трафиком и позволяют устранять уязвимости оверлейных сетей. Предложенный алгоритм подразумевает возможность функционирования в новой области - корпоративных ЛВС.

В **четвертой главе** изложены требования к системе и узлам ЛВС, выявлены структурообразующие элементы процессов функционирования организации (бизнес-процессы) с рассмотрением их во взаимосвязанном статическом и динамическом представлении, проведено моделирование предметной области. Представлен сравнительный анализ типов СУБД и их программной реализации. На основе продуктов PostgreSQL и MySQL Workbench была спроектирована и реализована база данных СИАУ.

В качестве платформы моделирования серверных решений был выбран гипервизор Xen, архитектура которого решает задачу построения блоков серверов предприятий, фальсифицированных серверных решений и прогнозирования/моделирования.

Проведена настройка веб-сервера, предоставляющего аналитику и статистику функционирования системы. Написан компонент на PHP, HTML, JS + jQuery, CSS.

Итогом данного раздела является реализация (с использованием гибкой методологии XP, языка программирования C++ со сборщиком проектов Cmake), развертывание и автоматическое тестирование системы интеллектуально-адаптивного управления трафиком, основой которого являются разработанные метод управления информационными потоками корпоративных вычислительных сетей и алгоритм управления трафиком на межсетевых узлах ЛВС. В ходе работы использовалось аппаратное обеспечение: выделенный сервер PX60 (Intel® Xeon® E3-1270 v3 Quadcore, 32 GB ECC RAM, 2x2 TB SATA 6 Gb/s 7200 rpm с аппаратным LSI-RAID контролером, 3 сетевые карты 1 Gbit/s) с ОС Linux CentOS 6.5.

В **пятой главе** описаны функциональные возможности СИАУ, отвечающей всем поставленным требованиям, а также проведено тестирование в сравнительном анализе с коммерческими продуктами.

Для анализа эффективности работы системы было проведено более 100 итерации сканирования системы (с установленным параметром реагирования блока фальсификации до 20% на обнаруженные процессы сканирования) посредством программ XSpider, LanGuard, SS-Scanner, X-Scan с использованием в каждой итерации средств зондирования GcodePRO, ZondGuard (результаты представлены на рисунке 5).

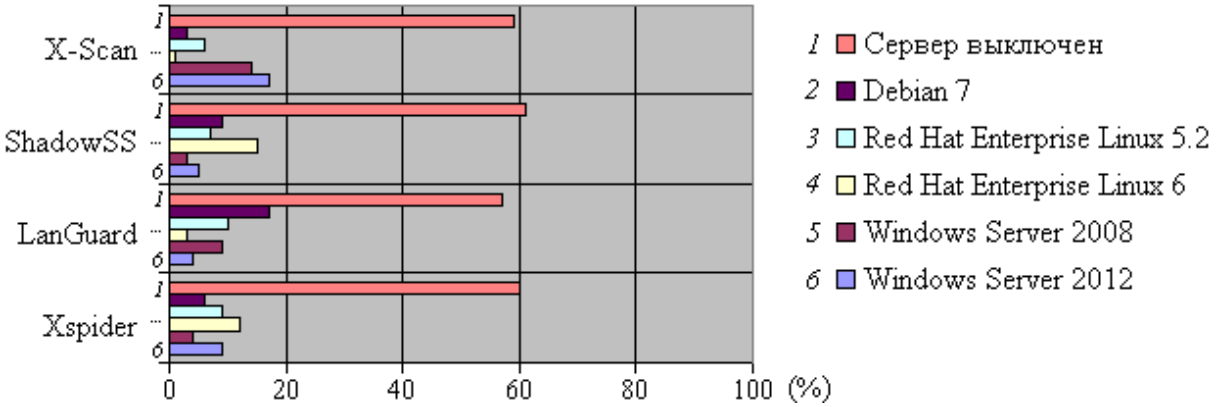

Рисунок 5 - Диаграмма идентификации ОС сервера сканерами/зондерами

Как видно из диаграммы, в ходе эксперимента СИАУ выдержала порог фальсификации серверных решений в 20% (имитируя Windows Server 2012, 2008, Red Hat Enterprise 6, 5.2, Debian 7), в остальных 80% злоумышленного сканирования информационная система представлялась выключенной.

Далее, при проведении 153 распределенных сетевых атак с различными модификациями типов вторжений от 760 узлов (на рисунке 6 временной интервал от 0 до 50 сек), рассматриваемые средства защиты (СИАУ, Kerio Control 8, Outpost NS 3.2, Traffic Inspector 2, запущенные на идентичной аппаратной платформе) показали следующий результат:

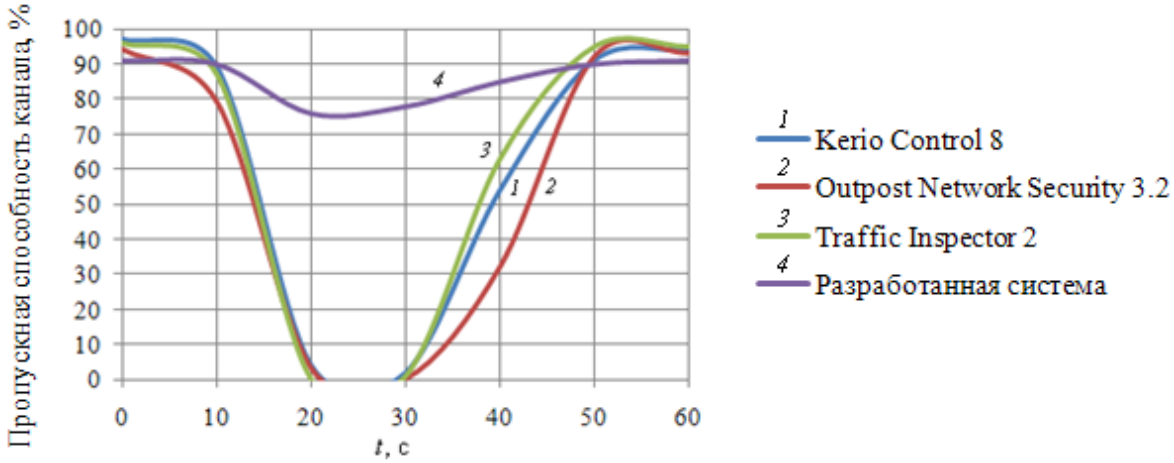

Рисунок 6 - Диаграмма пропускной способности канала связи при распределенных сетевых атаках

Как видно из рисунка 6, разработанная СИАУ сохраняет режим минимальной загрузки канала, не «проседает» в режим недоступности. Данные результаты обусловлены работой метода противодействия сетевым угрозам с фальсификацией серверных решений, выставлением «ловушек» и идентификацией круга зараженных машин.

Впоследствии было проведено более 1300 равнозначных распределенных сетевых атак с различными модификациями типов и параметров вторжений (результаты представлены графиком на рисунке 7).

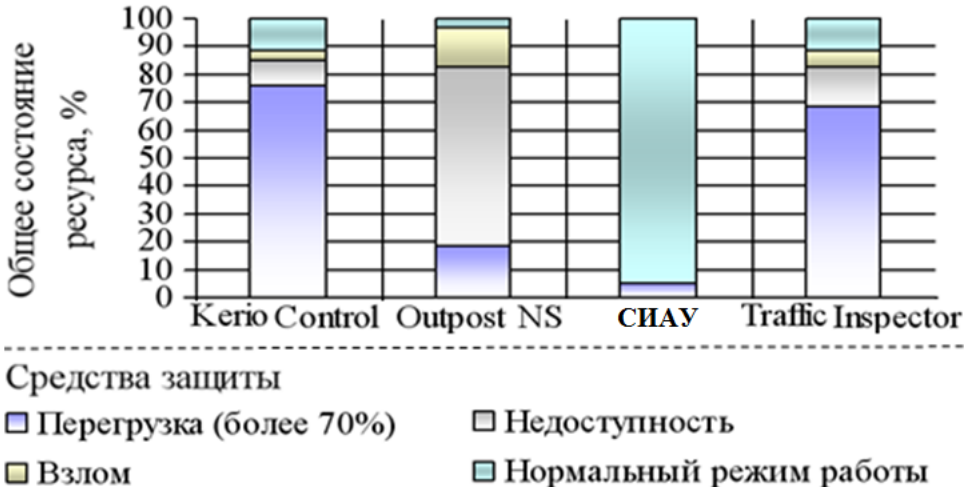

Рисунок 7 - Диаграмма состояния систем защиты при атаках

Согласно результатам проведенного эксперимента (рисунок 7), из рассмотренных продуктов наилучший результат продемонстрировала предлагаемая СИАУ, у которой лишь в 5% случаев загрузка канала составляла 70% ±4. В рамках проведенных экспериментов попытки взлома/вывода из состояния доступности СИАУ были безуспешными.

Для сравнительной оценки разработанного оптимального регулирования пропускной способностью ЛВС разработанной системой было проведено более сотни экспериментов в ВС с пропускной способностью до 10 Мбит/с и 100 хостами (пример на рисунке 8).

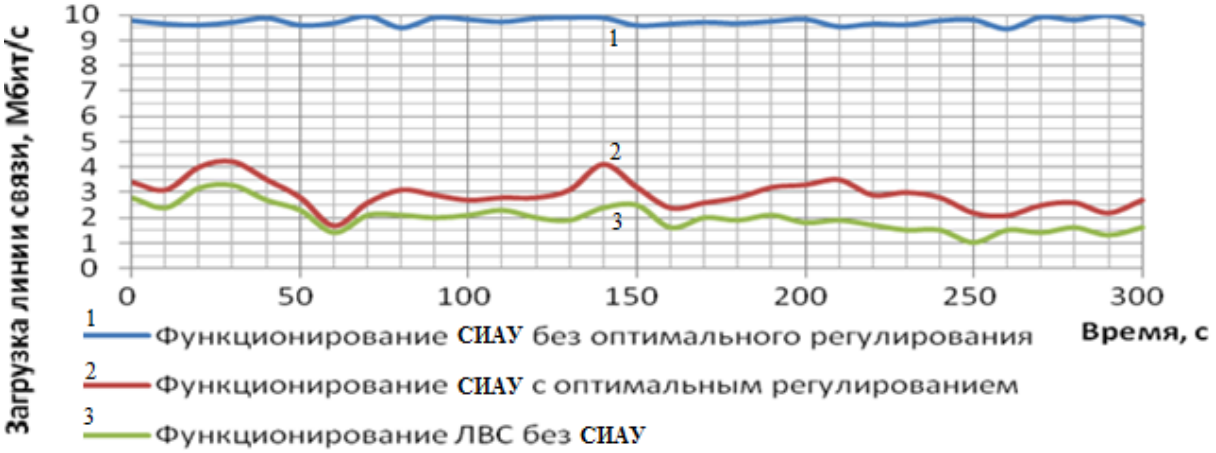

Рисунок 8 - Диаграмма загрузки линии связи

Стандартные методы не справляются с разгрузкой сети при внедренной СИАУ, теряя до 34% пакетов. А разработанный алгоритм

оптимального регулирования (являющийся составной частью метода управления информационными потоками корпоративных ЛВС) хорошо себя зарекомендовал: выдерживает минимум 30% недогруженности линии связи в пиковую загрузку с максимальным порогом превышения лишь «стандартного» режима работы ВС до 15%, что является минимальными издержками в задаче обеспечения высокого уровня ИБ.

Параллельно в течение года проводился эксперимент по расшифровке конфиденциальных данных сети СИАУ путем внедрения снифферов (CommView, IRIS, LanExplorer, Net Analyzer) в каналы связи различных филиалов, а также средствами дешифровки трафика (unMilitaryZ, BDUpro и иными специализированными средствами) на вычислительных кластерах из 15 серверов DELL PowerEdge™ R720 12thG DX290 (Dual Intel® Xeon® E5-2620, 128 GB DDR3, RAID-C Dell H710, SATA 6Gbit/s). Программное обеспечение для распараллеливания вычислений разворачивалось на различных хостах с разными ОС на базе гипервизоров (ESXi) и паравиртуализаторов (XEN). Попытки дешифровки данных в рамках описанного временного интервала оказались безуспешными.

На обзор вынесен широкий спектр работ по тестированию СИАУ, зарекомендовавшей себя надежным, автономным, отказоустойчивым, интеллектуально-адаптивным инструментом, оптимизирующим загрузку канала связи и обеспечивающим высокий уровень ИБ в сравнении с дорогостоящими коммерческими продуктами; СИАУ минимизирует человеческий фактор, исключает возможность прогнозирования стратегии реагирования, а также дешифровки информации в рентабельные сроки.

Минусом системы является требование к значительным вычислительным мощностям: остальным продуктам достаточно CPU 1GHz, RAM 1Gb, HDD 30Gb. Учитывая, что развитие микроэлектроники стремительно набирает обороты, требование обеспечения заявленных вычислительных мощностей не является весомым недостатком.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В **заключении** изложены основные результаты исследования:

1) разработан новый метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей с применением модифицированной генетической алгоритмизации и нечеткой логики, позволяющий прогнозировать реакцию хостов на различные виды сетевых воздействий посредством распределенного анализа на модельных объектах. Отличия от существующих методов заключаются в обеспечении:

- ✓ динамического самообучения и самореорганизации ИС (с автоматической идентификацией новых сетевых угроз и выработкой оптимальной стратегий по их устранению);

- ✓ минимизации загрузки канала связи (выбор оптимальной стратегии управления трафиком при различных типах сетевой активности);
- ✓ минимизации человеческого фактора (автоматическое функционирование системы с защитой от инсайдерских атак и автономным принятием решений);
- ✓ высокого уровня информационной безопасности с невозможностью прогнозирования стратегии реагирования системы как с локальной вычислительной сети предприятия, так и «извне»;

2) разработан оригинальный алгоритм управления информационными потоками корпоративных вычислительных сетей на базе распределенной обработки данных с фрагментацией пакетов на экземпляры случайной длины, изменением флагов дейтаграмм (в допустимых рамках), привнесением различных задержек на обработку каждого пакета узлом-отправителем и всеми промежуточными звеньями, а также генерацией фальшивого p2p трафика. Как следствие, отличительными особенностями алгоритма являются:

- ✓ оптимизация загрузки канала связи (посредством авторского инжиниринга генерируемого псевдо-трафика);
- ✓ исключение возможности осуществления автоматического и автоматизированного анализа трафика (с пресечением потенциальной возможности корреляции параметров прохождения дейтаграмм и идентификации автомодельности);
- ✓ исключение возможности прогнозирования продвижения трафика, как из локальной вычислительной сети предприятия, так и «извне»;
- ✓ минимизация человеческого фактора (автоматическое функционирование системы с защитой от инсайдерских атак);
- ✓ обеспечение высокого уровня информационной безопасности (защита от сниффинга и дешифровки, тайминг-атак глобальным наблюдателем);

3) разработана система интеллектуально-адаптивного управления трафиком вычислительной сети с коммутацией пакетов (СИАУ), в основу которой заложены предложенные методы;

4) реализовано программное обеспечение предложенной системы (с использованием гибкой методологии XP) на базе паравиртуализатора XEN с веб-сервером для предоставления аналитической информации;

5) проведено экспериментальное исследование функциональных возможностей разработанного вычислительного комплекса СИАУ, анализ его комплексной эффективности (быстродействия, уровня обеспечения информационной безопасности, оптимизации загрузки канала связи и др.) в сравнении с существующими решениями. Предложенная система обеспечивает преимущества вышеизложенных методов и зарекомендовала

себя надежным, автономным, отказоустойчивым и более эффективным инструментом в сравнении с дорогостоящими коммерческими продуктами, ориентированными на корпоративный сектор.

В приложениях приведены данные экспериментальных исследований, описание комплекса программ, акты об использовании результатов диссертационной работы.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в журналах, рекомендованных ВАК для публикации результатов диссертаций на соискание ученой степени доктора и кандидата наук:

1. Басыня, Е. А. Самоорганизующаяся система управления трафиком вычислительной сети [Текст] / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 1 (31). – С. 179–184.
2. Французова, Г. А. Самоорганизующаяся система управления трафиком вычислительной сети: метод противодействия сетевым угрозам [Текст] / Г. А. Французова, А. В. Гунько, Е. А. Басыня // Программная инженерия. – 2014. – № 3. – С. 16–20.

Свидетельства о регистрации программ:

3. Свидетельство о государственной регистрации программы для ЭВМ (№ 2014615697 «Self-organizing control system of computer network traffic».

Публикации в журналах и сборниках трудов:

4. Басыня, Е. А. Стохастические методы управления трафиком вычислительной сети с коммутацией пакетов [Текст] / Е. А. Басыня, А. В. Гунько // Нелинейные динамические системы: моделирование и оптимизация управления. (НДС–2012) : сб. тез. докл. междунар. молодеж. конф., Новосибирск, 2–5 окт. 2012. – Новосибирск : Изд-во НГТУ, 2012. – С. 5–7.
5. Гунько, А. В. Стохастические методы обеспечения информационной сетевой безопасности [Текст] / А. В. Гунько, Е. А. Басыня // Актуальные проблемы электронного приборостроения : материалы 11 междунар. конф. В 7 т. – Новосибирск : Изд-во НГТУ, 2012. – Т. 7. – С. 47–49.
6. Басыня, Е. А. О перспективах развития криптографии [Текст] / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Перспективное развитие науки, техники и технологий : материалы 3 междунар. науч.-практ. конф. В 3 т. – Курск : Изд-во ЮЗГУ, 2013. – Т. 1. – С. 199–200.
7. Французова, Г. А. Разработка и исследование самоорганизующейся системы управления трафиком вычислительной сети [Текст] / Г. А. Французова, А. В. Гунько, Е. А. Басыня ; науч. рук. Г. А. Французова // Наука. Технологии. Инновации : материалы Всерос. науч. конф. молодых ученых, Новосибирск, 21–24 нояб. 2013 г. : в 10 ч. – Новосибирск : Изд-во НГТУ, 2013.–Ч.2. – С. 3–7.
8. Французова, Г. А. Обеспечение информационной безопасности внутренних информационных потоков корпоративной сети [Текст] / Г. А. Французова, А. В. Гунько, Е. А. Басыня ; науч. рук. Г. А. Французова // Наука. Технологии. Инновации : материалы Всерос. науч. конф. молодых ученых, Новосибирск, 21–24 нояб. 2013 г. : в 10 ч.–Новосибирск: Изд-во НГТУ,2013.–Ч. 2.–С. 41–43.

9. Басыня, Е. А. Технология управления трафиком вычислительной сети на основе самоорганизующихся систем [Текст] / Е. А. Басыня ; науч. рук. Г. А. Французова ; консультант А. В. Гунько // Новые информационные технологии в научных исследованиях: материалы 18 Всерос. науч.-технич. конф. студентов, молодых ученых.–Рязань: Изд-во РГРТУ,2013.–С. 181–183.
10. Басыня, Е. А. Оптимальное регулирование пропускной способностью вычислительной сети самоорганизующейся системой управления трафиком [Текст] / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Современные тенденции в образовании и науке : сб. науч. тр. по материалам междунар. науч.-практ. конф.,31 окт. 2013 г.: в 26 ч.–Тамбов: Б-Н-О, 2013.–Ч.5.–С. 13–14.
11. Французова, Г. А. Самоорганизующаяся система управления трафиком вычислительной сети: механизмы защиты от сканирования и зондирования [Текст] / Г. А. Французова, А. В. Гунько, Е. А. Басыня // Сборник научных трудов Sworld. – 2013. – Т. 9, вып. 4. – С. 75–78. – Тема вып. Перспективные инновации в науке, образовании, производстве и транспорте –2013.
12. Французова, Г. А. Применение искусственного интеллекта в сфере сетевой информационной безопасности [Текст] / Г. А. Французова, А. В. Гунько, Е. А. Басыня // Искусственный интеллект: философия, методология, инновации : сб. тр. 7 Всерос. конф. студентов, аспирантов и молодых ученых, Москва, 13–15 нояб. 2013 г. – Москва : Радио и Связь, 2013. – Ч. 2, секции 4–6. – С. 110–115.
13. Басыня, Е. А. О шифровании и анонимизации в вопросах обеспечения информационной безопасности [Текст] / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Компьютерные технологии в науке, производстве, социальных и экономических процессах : материалы 14 междунар. науч.-практ. конф., Новочеркасск,12 дек. 2013 г.–Новочеркасск: ЮРГПУ (НПИ),2014.–С.165–168.
14. Basinya, E. A. Methods of self-organization in providing network security [Text] / E. A. Basinya, G. A. Frantsuzova, A. V. Gunko // Global Science and Innovation : materials of the 1 intern. sci. conf., USA, Chicago, 17–18 Dec. 2013. – Chicago : Accent Graphics communications 2013. – Vol. 2. – P. 386–389.
15. Басыня, Е. А. Интелектуально-адаптивные методы обеспечения информационной сетевой безопасности [Текст] / Е. А. Басыня, А. В. Гунько // Автоматика и программная инженерия. – 2013. – № 1 (3). – С. 95–97.
16. Басыня, Е. А. Самоорганизующаяся система управления трафиком сети: удаленный сетевой доступ [Текст] / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Автоматика и программная инженерия. – 2014. – № 1 (7). – С. 9–12.
17. Басыня, Е. А. Вопросы управления трафиком в оверлейных сетях. [Текст] / Е. А. Басыня // Автоматика и программная инженерия. – 2014. – № 3 (9). – С. 29–32.

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20,
тел./факс: (383) 346-08-57
Формат 60 X 84/16. Объём 1.5 п.л. Тираж 100 экз.
Заказ No 111. Подписано в печать 17.12.2014 г.