На правах рукописи

Рудина Екатерина Александровна

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СРЕДСТВ СЕТЕВОЙ ЗАЩИТЫ НА ОСНОВЕ МЕТОДА СИНТАКСИЧЕСКОГО АНАЛИЗА ТРАФИКА

Специальность 05.13.19

Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет».

Научный руководитель: Зегжда Дмитрий Петрович
доктор технических наук, профессор

Официальные оппоненты: Макаров Сергей Борисович,
доктор технических наук, профессор,
заведующий кафедрой
ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Томилин Василий Николаевич,
кандидат технических наук,
системный инженер ООО "Сиско Системс"

Ведущая организация: ФГБОУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Защита состоится « » декабря 2012 г. в часов на заседании диссертационного совета Д212.229.27 при ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет» (по адресу 195251, Санкт-Петербург, ул. Политехническая, д.29/1 ауд. 175 главного здания.)

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан « » ноября 2012 г.

Ученый секретарь
диссертационного совета

Платонов Владимир Владимирович

Общая характеристика работы

Актуальность темы исследования

Неуклонное развитие сетевых технологий, стандартов и протоколов, в совокупности с разнообразием и многочисленностью функционирующих в глобальной сети Интернет систем и сервисов порождает сложную и динамичную среду сетевого взаимодействия, в которой реализуются современные угрозы безопасности. Противодействие нарушителя средствам сетевой защиты носит характер постоянной борьбы, методы которой непрерывно совершенствуются – средства защиты стремятся полностью контролировать сетевые потоки, а нарушители задействуют все новые способы обхода этого контроля.

Обход сетевой защиты признается серьезной проблемой как работающими в этой области учеными, так и экспертами из ведущих ИТ компаний и разработчиками средств защиты. Сложные методы обхода сетевого контроля и противодействие им обсуждаются на авторитетных отечественных и международных форумах по информационной безопасности. В настоящее время, согласно исследованиям компании Stonesoft, известно не менее двух сотен различных методов для обхода средств сетевой защиты, и это число продолжает расти.

Другая наблюдаемая в последние годы тенденция состоит в значительном смещении вектора сетевых атак в направлении пользователей Интернет-сервисов, в то время как раньше атакам в большей мере подвергались сами сервисы. При этом конечной целью атаки может быть как включение пользовательской системы в состав бот-сети, так и распространение вторжения в локальной подсети. Таким образом, успешная атака, проведенная в обход сетевой защиты, влияет не только на безопасность атакованной системы, но и на безопасность всей сети в целом.

Наиболее часто применяемым методом обхода средств сетевой защиты является туннелирование протоколов, представляющее собой инкапсуляцию сообщений протокола некоторого уровня модели OSI в сообщения протокола того же уровня или более высокого. При этом средства защиты обрабатывают только внешний протокол, игнорируя вложенный, что приводит к потере эффективности средств защиты.

Следовательно, задача повышения эффективности средств сетевой защиты за счет предотвращения туннелирования протоколов является актуальной.

Степень разработанности темы исследования

Основанием для диссертации служат исследования в области обеспечения сетевой безопасности отечественных и зарубежных ученых В.А.Галатенко, В.И.Городецкого, П.Д.Зегжды, И.В.Котенко, И.Б.Саенко, M.Baldi, V.Paxson, F.Risso, V.Skormin, в работах которых описываются основы обеспечения сетевой безопасности, но не в полной мере раскрыты методы фильтрации трафика и обнаружения атак в условиях использования нарушителем инкапсуляции протоколов.

Представленная работа посвящена повышению эффективности существующих методов защиты от сетевых атак путем обнаружения туннелирования потенциально опасного трафика с помощью методов синтаксического анализа, не зависящих от типов протоколов, используемых при построении туннелей.

Целью диссертационной работы является повышение эффективности существующих средств сетевой защиты посредством применения метода синтаксического анализа трафика с использованием контекстно-свободных грамматик.

В соответствии с поставленной целью сформулированы основные задачи:

1. Исследование методов обхода средств сетевой защиты путем туннелирования прикладных протоколов и разработка подхода к оценке повышения эффективности средств сетевой защиты.
2. Создание универсальной лексикографической модели Интернет-протоколов.
3. Создание аналитической модели и распознающей грамматики сетевого взаимодействия.
4. Разработка специализированного языка описания сетевого взаимодействия.
5. Разработка алгоритма синтаксического анализа трафика на основе описания взаимодействия с использованием специализированного языка и создание методики повышения эффективности средств сетевой защиты с применением этого алгоритма.
6. Разработка прототипа программного средства, реализующего синтаксический анализ трафика с целью повышения эффективности средств сетевой защиты.

Научная новизна диссертационной работы заключается в следующем:

1. Предложена универсальная лексикографическая модель Интернет-протоколов, описывающая параметры отдельных сообщений и сеансов взаимодействия в целом и определяющая алфавит языка взаимодействия по Интернет-протоколам.
2. Создана аналитическая модель сетевого взаимодействия и эквивалентная контекстно-свободная грамматика, позволяющая распознавать взаимодействие по Интернет-протоколам в сетевом трафике.
3. Разработан специализированный контекстно-свободный язык описания взаимодействия по сетевым протоколам.
4. Предложен алгоритм синтаксического анализа трафика, основанный на аналитической модели и использующий описания взаимодействия по протоколам на специализированном языке.

Теоретическую значимость работы составляет разработка аналитической модели, применимой для синтаксического распознавания сетевого взаимодействия по протоколам, описанным с использованием специализированного формального языка.

Практическую ценность работы составляет созданное программное средство синтаксического анализа трафика, интегрируемое с межсетевым экраном (МЭ) для распространения функций МЭ на взаимодействие по туннелированным протоколам.

Методы и методология исследования. Для исследования предметной области проведен анализ основанных на туннелировании протоколов способов обхода средств сетевой защиты. При решении поставленной задачи использовался аппарат аналитических грамматик теории формальных языков. Предлагаемый в работе метод анализа трафика обоснован с использованием элементов теории автоматов, языков и вычислений, а повышение эффективности средств сетевой защиты с применением этого метода подтверждено проведенными экспериментами.

Основные положения, выносимые на защиту:

1. Универсальная лексикографическая модель, определяющая параметры протоколов, анализируемые средствами защиты в Интернет.
2. Аналитическая модель сетевого взаимодействия, применяемая для обнаружения туннелирования протоколов.
3. Специализированный контекстно-свободный язык формального описания взаимодействия по сетевым протоколам.
4. Алгоритм синтаксического анализа сетевого трафика согласно описаниям на специализированном языке, и методика распознавания туннелирования протоколов с целью повышения эффективности средств защиты.

Степень достоверности и апробация результатов

Основные теоретические и практические результаты работы обсуждались на XVII общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2008), на четвертой общероссийской конференции «Математика и безопасность информационных технологий» (МаБИТ, Москва, 2008) и на Международной молодежной конференции «Информационные системы и технологии» (Москва, 2012).

Достоверность работы подтверждается публикацией ее результатов в рецензируемых научных изданиях. По теме диссертации опубликовано 9 работ, в их числе 3 научные статьи, из них в изданиях, входящих в перечень утвержденных ВАК РФ – 3, 1 учебно-методическое пособие, 5 докладов на конференциях.

Метод синтаксического анализа сетевого трафика был применен в НИР «Разработка методики идентификации прикладных Интернет протоколов на основе вариативно-сигнатурного анализа взаимодействия клиент-серверных компонент» (шифр 2011-1.4-514-065-025) по государственному контракту № 07.514.11.4107 от 26.10.2011.

Результаты работы применены в части обеспечения защиты информации от Интернет-угроз, связанных с туннелированием протоколов, на малом

инновационном предприятии ООО "Инфоком"; а также в части подготовки специалистов, обучающихся по специальности 090105.65 на кафедре Информационная безопасность компьютерных систем ФГБОУ СПбГПУ, при проведении практических занятий по дисциплине «Безопасность вычислительных сетей», что подтверждается соответствующими Актами об использовании.

Структура работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 88 наименований.

Основное содержание работы

Первая глава содержит описание способов обхода средств сетевой защиты путем туннелирования протоколов, причин сопутствующего снижения эффективности этих средств, а также подхода к оценке повышения эффективности средств сетевой защиты при обнаружении туннелирования.

Основным средством сетевой защиты от удаленных атак является межсетевой экран, осуществляющий контроль и фильтрацию трафика в соответствии с заданными правилами.

Однако реализуемый МЭ контроль взаимодействия может быть обойден за счет применения разрешенных правилами МЭ протоколов для организации туннелей, внутри которых используются запрещенные протоколы. Туннелирование протоколов может осуществляться сетевыми сервисами-посредниками (например, GNUhttptunnel, iodine) или непосредственно протоколом сервиса, к которому обращается пользователь (например, BOSH); при этом атака через туннель не будет отражена МЭ (см. рисунок 1).

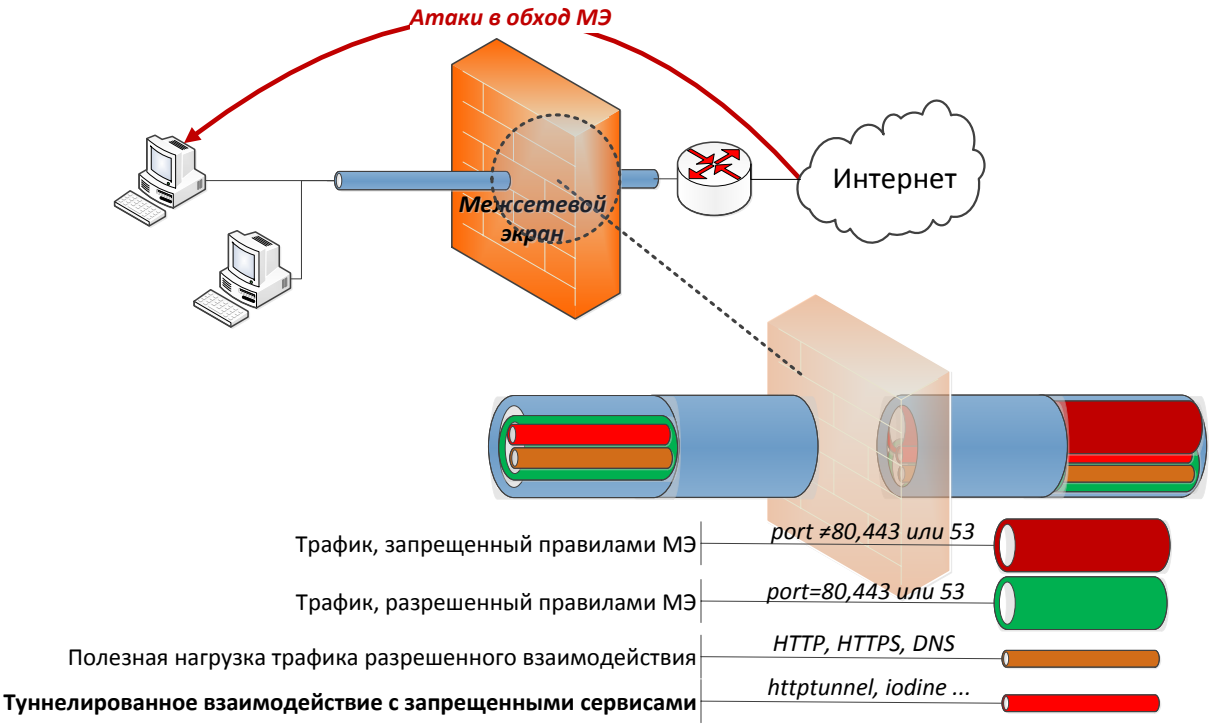

Рисунок 1 – Обход средств защиты при помощи туннелирования протоколов

Эффективность МЭ принимается равной 100%, если фильтрация трафика согласно правилам МЭ позволяет отразить сетевые атаки при использовании запрещенных этими правилами протоколов или Интернет-сервисов. Туннелирование протоколов приводит к снижению эффективности МЭ вследствие несрабатывания правил. Для повышения эффективности МЭ необходимо обнаруживать туннелирование и применять правила фильтрации к инкапсулированным протоколам. Полученное за счет этого повышение эффективности работы МЭ ΔE оценивается через отношение доли отраженных атак по туннелируемым протоколам к общей доле отражаемых МЭ атак (без учета инкапсулированных протоколов):

$$\Delta E = \frac{\sum_{i \in 1:n} k_i^D}{K} * 100\%, \text{ где}$$

- K – общее количество атак, отражаемых МЭ;
- n – количество запрещенных протоколов или Интернет-сервисов, используемых посредством туннелирования;
- $k_i^D, i \in 1:n$ – число известных атак по каждому из протоколов, которые могут быть подвергнуты туннелированию.

Задачу настоящей работы составляет обнаружение скрытых с использованием техники туннелирования протоколов путем синтаксического анализа сетевого трафика на основе грамматик протоколов взаимодействия. Протокол сетевого взаимодействия $\mathcal{P}$ рассматривается как грамматика $G_{\mathcal{P}}$ языка взаимодействия сетевых компонент, продукционные цепочки (фразы) этого языка представлены сетевым трафиком в каналах связи. Решение задачи

синтаксического распознавания продукционных цепочек с помощью двойственной $G_{\mathcal{P}}$ аналитической грамматики $G_{\mathcal{A}}$ (или эквивалентной $G_{\mathcal{A}}$ аналитической модели $\mathcal{A}$) дает решение задачи идентификации протокола $\mathcal{P}$ в трафике. Для описания грамматики протокола, используемой при синтаксическом анализе трафика, необходим специализированныйязык описания протоколов.

Сравнительный анализ распространенных языков и способов формального описания сетевых протоколов не выявил существующей нотации, которая могла бы быть эффективно применена для спецификации сетевого протокола с целью синтаксического анализа трафика.

Вторая глава посвящена разработке формальных моделей, применяемых в решении поставленной задачи.

Целью лексикографической модели протокола сетевого взаимодействия является формальное описание параметров протокола на основе его функциональной спецификации.

Лексикографическая модель протокола сетевого взаимодействия описывается кортежем $M = (P, A, C, NC)$, в котором:

- $P = \{prop\}$ – множество параметров сообщения, (значения которых из множества $V = \{V_i | V_i = \{v_{x_i}\}_{x_i \in 1:k_i}\}_{i \in 1:|P|}$ определяются только текущим сообщением в сеансе взаимодействия);
- $A = \{aprop\}$, $A \subseteq P$ – подмножество атомарных параметров (значения которых вычисляются непосредственно из сообщения);
- $C = \{ctx\}$ – множество параметров контекста;
- $U = \{U_j | U_j = \{u_{y_j}\}_{y_j \in 1:l_j}\}_{j \in 1:|C|}$ – множество значений параметров контекста;
- $NC \subseteq C$ – подмножество параметров контекста, от текущих значений которых зависят значения других параметров.

Множества V и Uпредставляют лексемы языка взаимодействия.

Экземпляр контекста, описывающий состояние взаимодействия

$$Cur = \{cur\_ctx_j\}_{1:|C|}, \forall j \in 1:|C|\ cur\_ctx_j \in U_j$$

задается множеством значений параметров контекста в каждый момент времени для каждого текущего сеанса взаимодействия.

Для каждого протокола необходимо определить набор функций со следующими прототипами:

- $get(x), x \in P \cup C$ – функция получения текущего значения параметра или параметра контекста;
- $calc(x), x \in P \cup C$ – функция вычисления параметра сообщения (параметра контекста) с учетом текущих значений прочих параметров;
- $init\_ctx(z, init\_val), z \in C$ – функция инициализации текущего значения параметра контекста;

– $update\_ctx(z), z \in C$ – функция обновления текущего значения параметра контекста.

Эти функции задают отношение $Dep\_prop(x, y)$ зависимости параметров сообщения и отношение $Dep\_ctx(x, y)$ зависимости параметров контекста:

$$Dep\_prop: (P \backslash A) \times (P \cup C) \to \{true, false\}$$
$$Dep\_ctx: C \times (P \cup C) \to \{true, false\}$$

В свою очередь, отношения зависимости определяют множество $A \subseteq P$ атомарных параметров сообщения и множество $NC \subseteq C$ параметров контекста, требующих инициализации перед созданием сеанса.

Целью аналитической модели сетевого взаимодействия является распознавание значений параметров протокола (заданных лексикографической моделью) в сетевом трафике при таком взаимодействии.

Аналитическая модель сетевого взаимодействия построена на базе лексикографической модели протокола с добавлением обобщенного алгоритма сетевого взаимодействия и описана в виде

$$\mathcal{A} = (M_i, I, F, C_i, T), \text{ где}$$

– M_i – описание протокола, уточняющее лексикографическую модель;
– $I = \{init\_val_z\}_{z \in NC}$ – множество начальных значений параметров контекстаNC при создании сеанса взаимодействия;
– $F \subset U$ – множество значений, при достижении которых заданным параметром контекста z_f взаимодействие завершается;
– $C_i = \{Calc\}$ – множество функций, реализующих вычисление параметров сообщений и параметров контекста исходя из значений полей сетевых сообщений и текущих значений параметров контекста;
– $T = xchg\_trigger$ – триггер цикла обработки, представляющий собой логическое выражение, при выполнении которого обновляются параметры контекста. Триггер цикла обработки включается при поступлении нового сетевого пакета, если соблюдаются ограничения на параметры сообщения и параметры контекста сеанса взаимодействия.

Обобщенный алгоритм сетевого взаимодействия с использованием псевдокода можно описать следующим образом:

begin
  foreach $z \in NC$ $init\_ctx(z, init\_val_z)$
  while $get(z_f) \notin F$
    if $xchg\_trigger$
    foreach $z \in C$ $update\_ctx(z)$
  end while
end

Для оценки универсальности аналитической модели доказана следующая теорема.

Теорема 1 Аналитическая модель сетевого взаимодействия на базе лексикографической модели протокола обладает, по крайней мере, такой же выразительной мощностью, какой обладает линейно-ограниченный автомат (ЛОА).

Доказательство теоремы выполняется путем интерпретации аппарата ЛОА с помощью предложенного обобщенного алгоритма сетевого взаимодействия.

На основании теоремы 1 предложенная аналитическая модель применима для анализа произвольного останавливающегося протокола сетевого взаимодействия.

В работе описана аналитическая грамматика языка сетевого взаимодействия, эквивалентная созданной аналитической модели. Недостаток это грамматики состоит в том, что она является контекстно-зависимой. Для этого типа грамматик не существует простых алгоритмов распознавания, а известные алгоритмы очень медленны. Для использования лишенной данного недостатка контекстно-свободной грамматики доказана теорема 2.

Теорема 2. Грамматика, формируемая аналитической моделью сетевого взаимодействия на базе лексикографической модели, может быть преобразована к контекстно-свободной грамматике при выполнении следующих ограничений на лексикографическую модель протокола сетевого взаимодействия:

1) *отсутствуют циклические зависимости между параметрами сообщений*
$$\forall x, y \in P \backslash A: Dep^T(x, y) = true => Dep^T(y, x) = false;$$
2) *параметры сообщения (ациклически) зависят только от других параметров сообщения и параметров контекста из множества* NC
$$\forall p \in P \backslash A: y \in C, Dep\_prop(p, y) = true \Rightarrow y \in NC.$$

Доказательство теоремы выполняется для каждого правила контекстно-зависимой грамматики путем индукционного преобразования его во множество правил, в левой части которых стоит нетерминальный символ.

Следствие из теоремы 2: при выполнении условий теоремы синтаксический анализ сетевого трафика на основе грамматик протоколов взаимодействия имеет сложность не выше полиномиальной.

Третья глава посвящена реализации синтаксического анализа сетевого трафика на основе созданной аналитической модели.

Специализированный язык описания сетевого взаимодействия по протоколу реализует основные концепции лексикографической модели протоколов и аналитической модели сетевого взаимодействия. Параметры сообщения и параметры контекста задаются как типизированные переменные. Формат сетевого сообщения задается в виде декларативного описания альтернативных последовательностей полей, транслируемого в бинарную структуру данных (дерево анализа сообщения). Взаимодействие по протоколу задается правилами инициализации/обновления и предикатами.

Правила описывают:

- инициализацию параметров контекста при создании сеанса взаимодействия(*Init*);
- обновление параметров контекста при обработке каждого последующего сообщения (*Renew*).

Предикаты, определенные на параметрах сообщения и параметрах контекста, описывают условия:

- отнесения сообщения к некоторому сеансу взаимодействия (*This*);
- корректности сообщения в сеансе взаимодействияпо значениям параметров (*Proper*);
- готовности данных для передачи инкапсулируемым протоколам (*Ready*);
- закрытия сеанса взаимодействия, после чего экземпляр контекста уничтожается (*Destructible*).

Алгоритм синтаксического анализа сетевого трафика осуществляет распознавание значений параметров используемого протокола, путем последовательно применяемых к сообщению синтаксического разбора и обработки контекста.

Алгоритм синтаксического разбора сообщения, основан на применении бинарной структуры данных – дерева анализа сообщения (ДАС), представляющего собой иерархическое описание формата сообщения сетевого протокола. Рекурсивный алгоритм, показанный на рисунке 2, выполняет обход дерева с тремя типами вершин (последовательность, альтернатива и атом) в двух режимах – обычном (позволяющем выделить поля с фиксированной длиной) и режиме «плавающего начала» (для выделения полей, ограниченных служебными полями или разделителями).

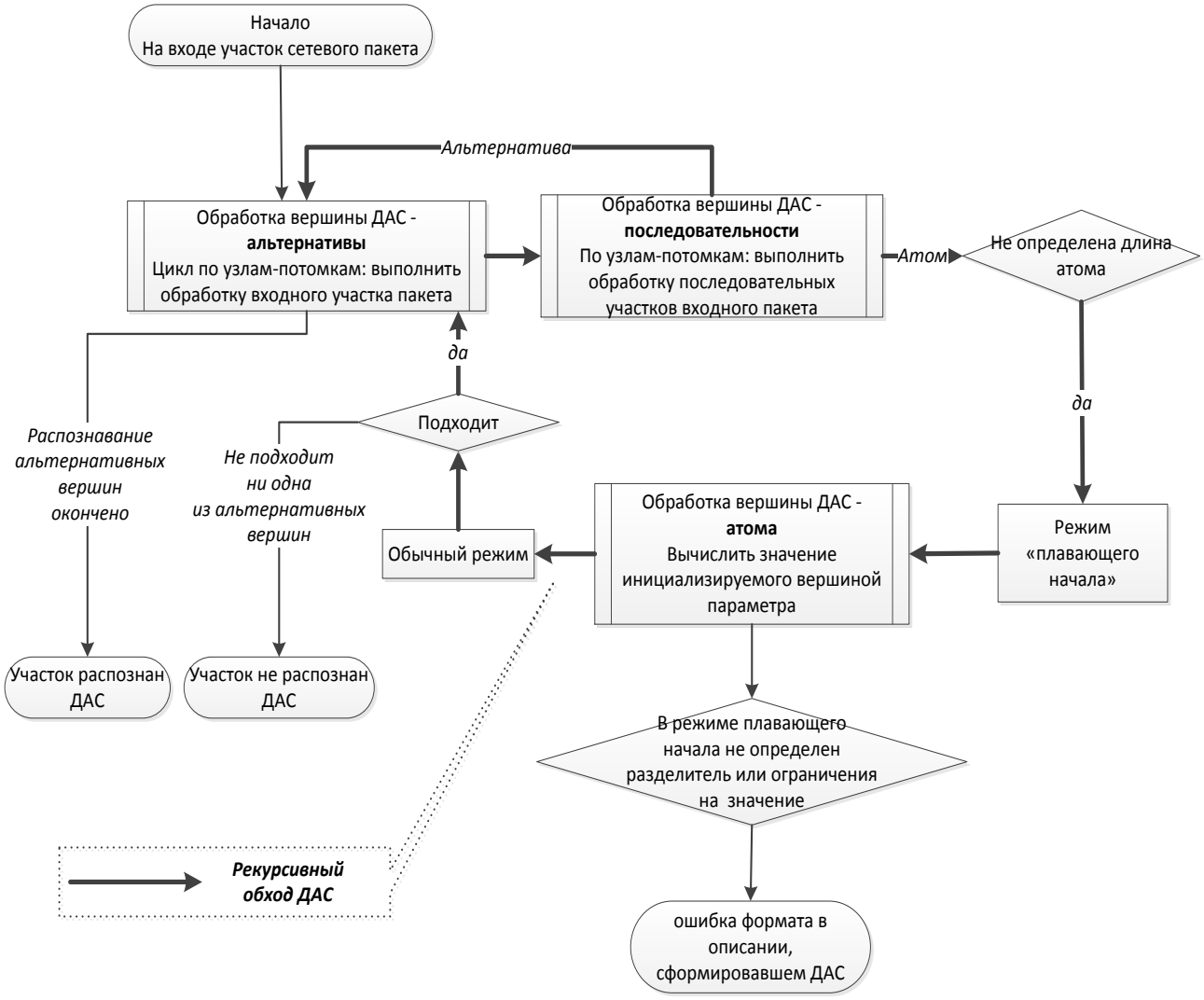

Рисунок 2 – Алгоритм синтаксического разбора сообщения

В работе описаны также вспомогательные алгоритмы, связанные с представлением формата сообщения в виде ДАС: алгоритм трансляции описания в ДАС и алгоритм нормализации ДАС для ускорения анализа трафика.

Алгоритм обработки контекста на основе декларативно заданных правил инициализации/обновления и предикатов, регулирующих условные переходы обобщенного алгоритма на каждой итерации обработки сообщений (рисунок 3). Кроме того, реализация алгоритма предусматривает возможность введения дополнительных правил и предикатов для упрощения подаваемой на вход спецификации протокола.

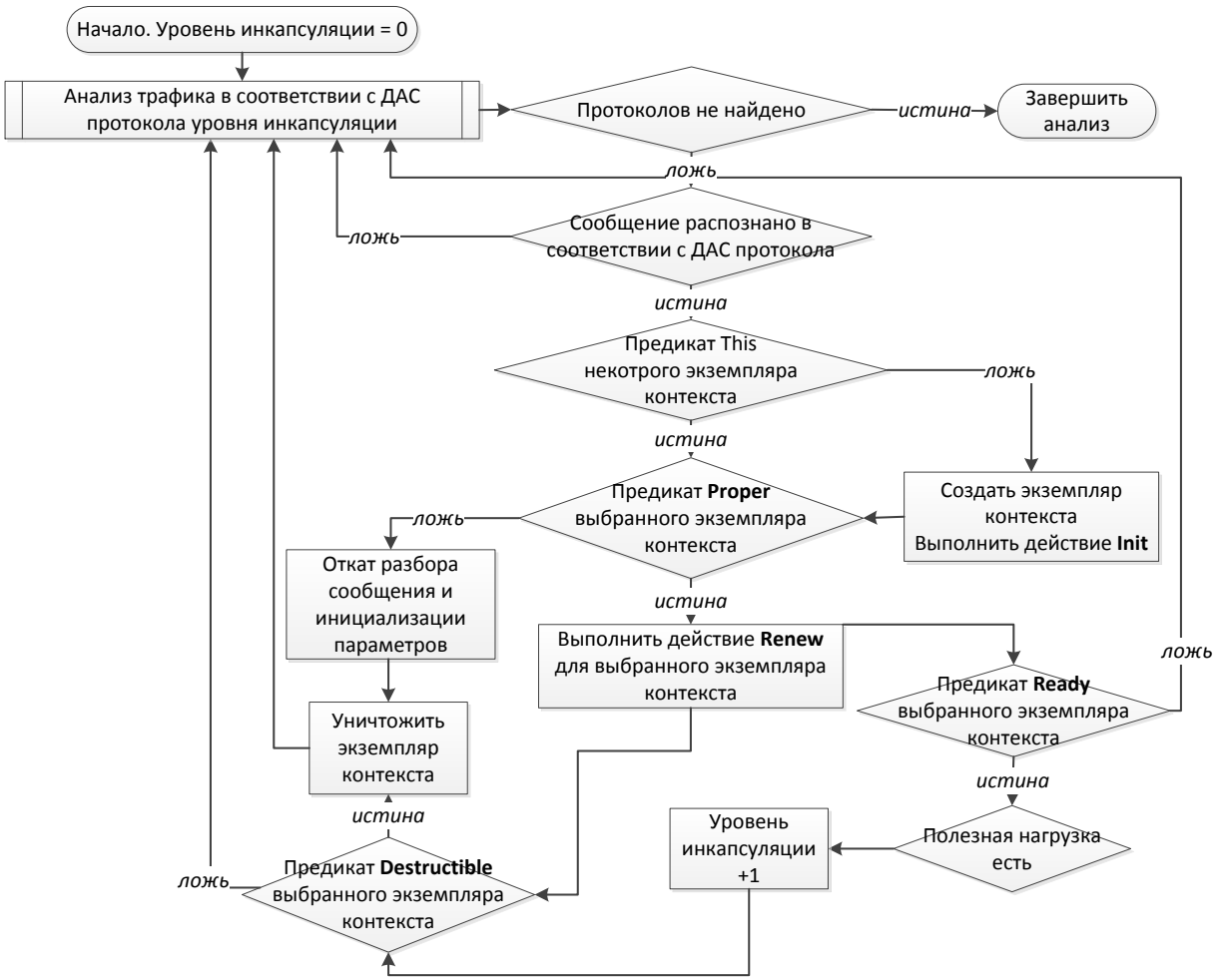

Рисунок 3 – Алгоритм обработки контекста

Четвертая глава диссертационной работы содержит методику повышения эффективности средств сетевой защиты с применением синтаксического анализа трафика, описание разработанного прототипа программного средства и результаты проведенного экспериментального исследования.

Методика повышения эффективности средств защиты содержит рекомендации по использованию синтаксического анализа трафика для распознавания и блокировки туннелированного взаимодействия. Для реализации этих возможностей следует осуществить действия:

1. Организовать перенаправление потоков сетевого трафика на вход синтаксического анализатора туннелированных протоколов.
2. Настроить синтаксический анализатор туннелированных протоколов.
   2.1. Специфицировать типовые виды туннелей с использованием языка описания протоколов.
   2.2. Специфицировать протоколы, которые могут быть использованы как несущие протоколы туннелей (для обнаружения нетиповых туннелей).
   2.3. Специфицировать протоколы, запрещенные на МЭ.
3. Настроить МЭ для блокировки туннелированного трафика.

3.1. Блокировать взаимодействие при синтаксическом распознавании типовых туннелей в сетевом трафике.

3.2. Блокировать взаимодействие при синтаксическом распознавании запрещенных протоколов, инкапсулированных в туннели.

Предложенная методика реализована с использованием разработанного прототипа программного средства синтаксического анализа трафика.

Разработанный прототип программного средства обеспечивает интерактивное взаимодействие с пользователем, в том числе в части составления описания протоколов, проверки этого описания и трансляции в бинарное представление. Сбор, синтаксический анализ и перенаправление сетевого трафика осуществляются до выполнения его фильтрации на МЭ. Правила МЭ корректируются в соответствии с результатами обнаружения туннелирования протоколов на основе синтаксического анализа трафика. Это позволяет интегрировать разработанный прототип с МЭ для повышения эффективности МЭ при отражении сетевых атак в условиях туннелирования протоколов (рисунок 4).

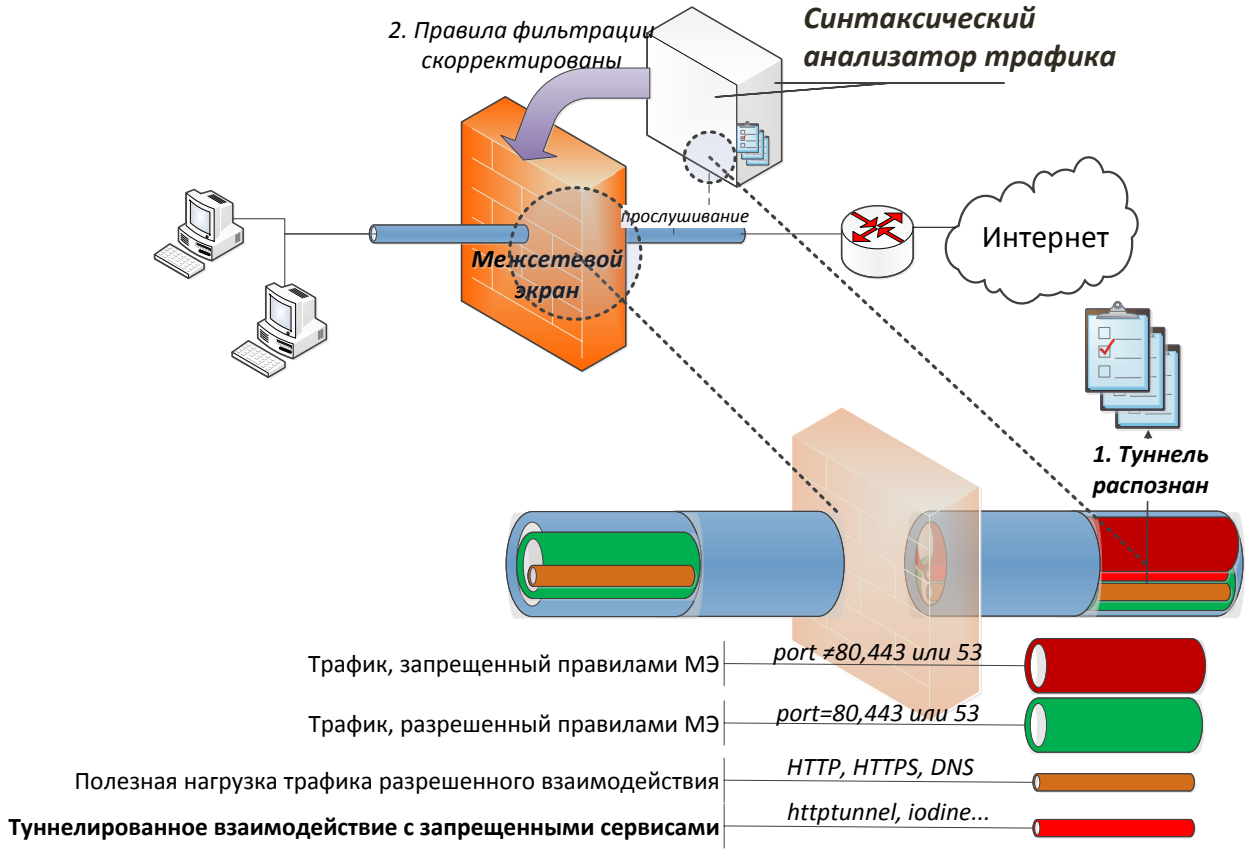

Рисунок 4 – Интеграция синтаксического анализатора трафика с межсетевым экраном для повышения эффективности защиты

Проведен ряд экспериментов по обнаружению туннелирования с использованием разработанного средства синтаксического анализа для протоколов HTTP, FTP, Telnet, SMTP, POP3 и др., сервисов AIM, ICQ (протокол OSCAR) и оценке повышения эффективности МЭ за счет применения этого средства.

Например, при разрешенном МЭ использовании Интернет сервисов по протоколам HTTP, HTTPS, DNS с помощью ПО туннелирования взаимодействия в сообщения протокола HTTP был организован сеанс FTP в обход ограничений МЭ.

При этом перед передачей трафика на МЭ с помощью разработанного средства был выполнен синтаксический анализ трафика, распознавший передаваемые на прикладном уровне сообщения как фразы, соответствующие языковой спецификации сеанса взаимодействия по протоколу HTTP. Для этого выполнен разбор фрагментов трафика путем рекурсивного разбиения каждого фрагмента на составные блоки (соответствующие узлам дерева синтаксического анализа сообщения) и установления соответствия этих блоков лексическим конструкциям протокола HTTP (методам запроса, идентификаторам ресурсов и пр.), описанным в его спецификации. По значениям лексических параметров в соответствии с алгоритмом обработки контекста восстановлен сеанс взаимодействия и передаваемые по протоколу объекты полезной нагрузки (обычно – файлы HTML, графические файлы и т.п.). К объектам, выделенным при анализе взаимодействия по HTTP, был рекурсивным образом применен синтаксический анализ, распознавший в них языковые конструкции протокола FTP (команды входа, просмотра каталога, передачи файлов и т.д.). Результаты анализа были переданы на МЭ, где было принято решение о запрете этого трафика.

Для оценки повышения эффективности МЭ в приведенном примере использовались данные о числе сетевых атак по каждому протоколу в действующей базе правил системы обнаружения сетевых атак Snort.

Рассчитано повышение эффективности МЭ при обнаружении и предотвращении взаимодействия с использованием туннелирования протоколов для описанного примера:

$$\Delta E = \frac{k_{FTP} + k_{Telnet} + k_{POP3} + k_{SMTP} + k_{OSCAR}}{K} * 100\% \simeq 9{,}5\%$$

где k_i – количество атак по протоколу i, K – общее число отражаемых МЭ атак.

Оценка повышения эффективности МЭ при предотвращении HTTP-туннелирования каждого из рассмотренных протоколов приведена на рисунке 5.

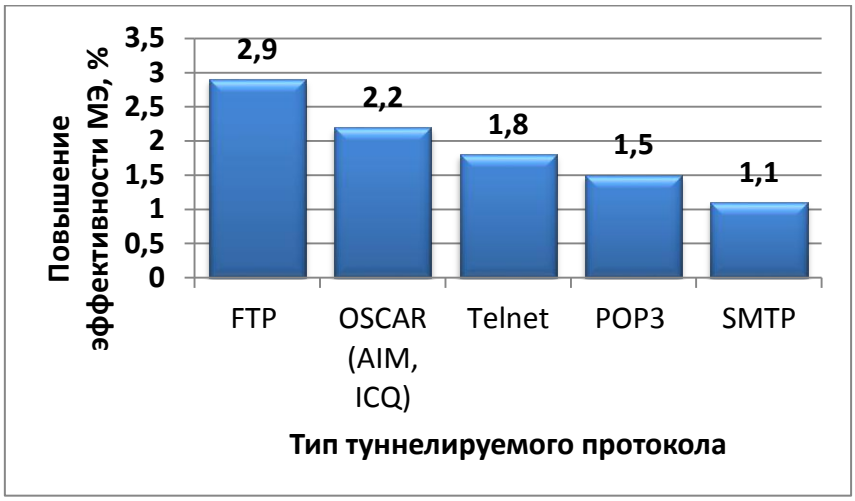

Рисунок 5 – Оценка повышения эффективности МЭ при обнаружении и предотвращении HTTP-туннелирования различных протоколов

Представленный пример характеризует типичную ситуацию применения туннелирования для обхода МЭ, разрешающего HTTP, когда HTTP-туннелирование используется для доступа к почтовым службам, сервисам мгновенных сообщений и т.д. При запрете протокола HTTP для организации туннеля может использоваться другой протокол. Чем слабее ограничения МЭ, тем разнообразнее могут быть туннели и больше повышение эффективности МЭ при применении методов обнаружения скрытого использования протоколов. Эта зависимость представлена на рисунке 6.

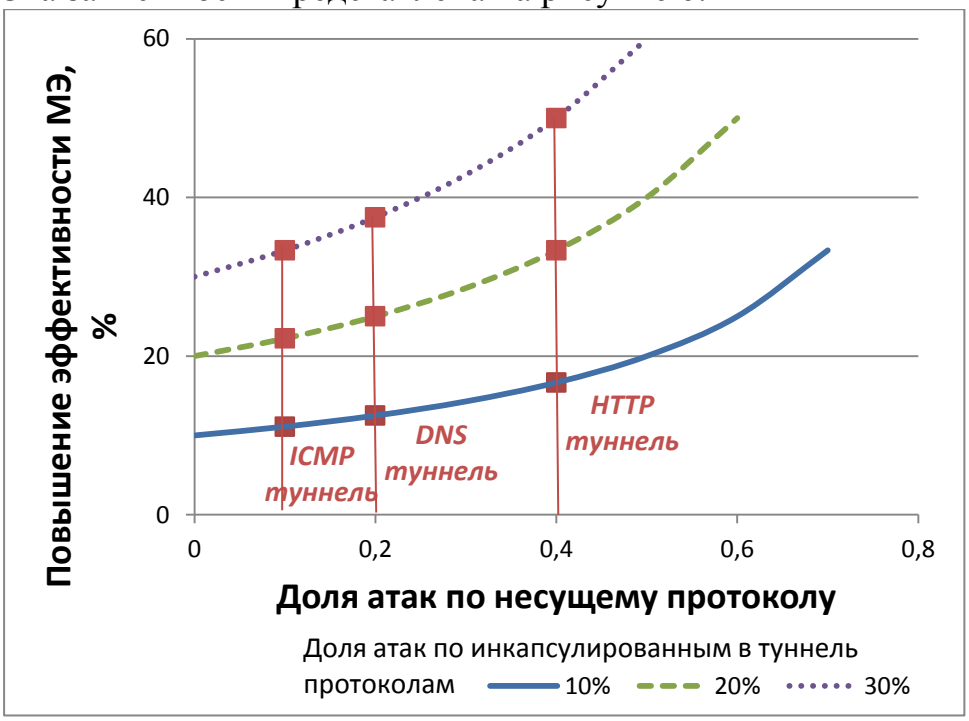

Рисунок 6 – Зависимость повышения эффективности МЭ от вида туннелирования

Полученные результаты свидетельствуют о повышении эффективности средств сетевой защиты при применении для выявления туннелирования протоколов предложенного в работе метода синтаксического анализа трафика.

Заключение

Итоги диссертационного исследования

1. Исследованы методы обхода средств сетевой защиты, основанные на туннелировании протоколов; предложен подход к оценке повышения эффективности средств сетевой защиты при обнаружении туннелирования.

2. Создана универсальная лексикографическая модель, определяющая параметры Интернет-протоколов, анализируемые средствами защиты в компьютерных сетях.

3. Создана аналитическая модель сетевого взаимодействия и эквивалентная контекстно-свободная грамматика, предназначенная для обнаружения туннелирования протоколов.

4. Разработан специализированный контекстно-свободный язык описания взаимодействия по сетевым протоколам, предназначенный для параметризации аналитической модели.

5. Предложен алгоритм синтаксического анализа трафика согласно описаниям протоколов на специализированном языке и методика повышения эффективности средств сетевой защиты с применением этого алгоритма.

6. Разработан прототип программного средства, реализующего синтаксический анализ трафика для распознавания туннелирования протоколов, и проведены экспериментальные исследования, подтверждающие повышение эффективности средств сетевой защиты при его использовании.

Рекомендации и перспективы дальнейшей разработки темы

Перспективы дальнейшей разработки темы лежат в области разработки методов анализа протоколов взаимодействия на предмет их корректности и безопасности. Поскольку предложенный язык описания взаимодействия является декларативным, он может быть использован для автоматизации разработки спецификаций Интернет-протоколов.

Список работ, опубликованных автором по теме диссертации

1. Рудина Е.А. Спецификация сетевых протоколов с использованием декларативного языка описания / Е.А.Рудина // журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехн. ун-та, 2012 г. – № 2, С.69-75.

2. Рудина Е.А. Подход к анализу клиент-серверного взаимодействия на основе декларативного описания сетевого протокола / С.С.Корт, Е.А.Рудина // журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехн. ун-та, 2011 г., – № 4, С.27-39.

3. Рудина Е.А. Обобщенное представление сетевых протоколов / Е.А.Рудина // журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехн. ун-та, 2008 г. – № 4, С.56-60.

4. Рудина Е.А. Контекстно-детерминированная идентификация прикладных протоколов в дампах сетевого трафика / Е.А.Рудина // Сб.материалов Международной молодежной конференции «Информационные системы и технологии». – М., 2012. – С.94-96.

5. Рудина Е.А. Вычислительные сети: лабораторный практикум / С.С. Корт, Е.А. Рудина. – СПб.: Изд-во Политехн. ун-та, 2011. – 188 с.

6. РудинаЕ.А. Формальное представление сетевого протокола / П.Д.Зегжда, Е.А.Рудина // Материалы Седьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008). – М., Издательство МЦНМО, 2009. – Т.2, с. 232-241.

7. Рудина Е.А. Поиск вариаций в полях сетевых пакетов по декларативному описанию протоколов / А.В. Шумов,Е.А.Рудина // Сб.Материалов «XXXVIII Недели науки СПбГПУ», СПб.: Изд-во Политехн. ун-та, 2009 г. – С.171-172.

8. Рудина Е.А. Подход к решению задачи восстановления значений параметров сообщений произвольных сетевых протоколов / Е.А.Рудина // СПб: Сб.Материалов XI международной конференции «Региональная информатика-2008 (РИ-2008)». – СПб.: Изд-во СПИИРАН, 2008 г.

9. Рудина Е.А. Обобщенное представление сетевых протоколов / Е.А.Рудина // Сб.Материалов XVII общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». – СПб.: Изд-во Политехн. ун-та, 2008 г. – С.108.