На правах рукописи

СИЛИНЕНКО Александр Витальевич

РАЗГРАНИЧЕНИЕ ДОСТУПА В IP-СЕТЯХ НА ОСНОВЕ МОДЕЛЕЙ СОСТОЯНИЯ ВИРТУАЛЬНЫХ СОЕДИНЕНИЙ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2010

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:

доктор технических наук, профессор	Заборовский Владимир Сергеевич

Официальные оппоненты:

доктор технических наук, профессор	Оков Игорь Николаевич
кандидат технических наук, доцент	Шишкин Владимир Михайлович

Ведущая организация:

Институт проблем информационной безопасности Московского государственного университета имени М.В.Ломоносова

Защита состоится 4 марта 2010 г. в 16 часов на заседании диссертационного совета Д 212.229.27 при ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу 195251, Санкт-Петербург, ул. Политехническая, 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Автореферат разослан 3 февраля 2010 г.

Ученый секретарь диссертационного совета Платонов В.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящее время информация является главным стратегическим и тактическим ресурсом для многих сфер человеческой деятельности. По этой причине особое внимание уделяется вопросам обеспечения информационной безопасности (ИБ) объектов различной природы, и, в частности, – противодействию реализациям угроз сетевого характера, обусловленных удалёнными деструктивными воздействиями на программно-аппаратные средства обработки, хранения и передачи данных. Наиболее подверженными такого сорта воздействиям являются информационно-вычислительные и коммуникационные ресурсы (далее именуемые сетевыми) распределённых автоматизированных систем (АС), построенных с использованием компьютерных сетей на базе стека протоколов TCP/IP (далее – IP-сети). Среди причин такого положения дел – существенная неадекватность встроенных механизмов обеспечения ИБ базовых протоколов IP-сетей современному уровню развития средств реализации угроз, наиболее распространёнными среди которых являются попытки несанкционированного обращения к сетевым ресурсам, атаки на отказ в обслуживании, а также сетевая активность вирусов и «ботнетов».

Одним из основных методов защиты сетевых ресурсов АС от распределённых деструктивных воздействий в IP-сетях является разграничение доступа (РД). Согласно принятой политике ИБ этот метод реализуется на основе идентификации, аутентификации и моделей логического разграничения доступа пользователей или процессов, действующих от их имени, к сетевым ресурсам. Попытки несанкционированного обращения при этом блокируются средствами, реализующими указанные сервисы ИБ. Как правило, такими средствами являются программные или программно-аппаратные средства межсетевого экранирования и фильтрации трафика. Наряду с разграничением доступа пользователей к сетевым ресурсам межсетевые экраны (МЭ) обеспечивают выполнение ряда важных сервисов и функций ИБ, включая криптографическую защиту данных, сокрытие структуры защищаемой сети, мониторинг трафика и обнаружение некоторых видов сетевых атак.

Используемые в настоящее время подходы к реализации РД в IP-сетях основаны на анализе сетевого трафика на предмет соответствия политике доступа, выраженной в виде совокупности правил фильтрации. При этом следует подчеркнуть, что возможности такого анализа не позволяют обеспечить защиту от всего существующего многообразия вредоносных

сетевых воздействий. Это обусловлено постоянным совершенствованием методов и средств реализации сетевых угроз через разрешённые политикой доступа виртуальные соединения (ВС). С точки зрения задачи РД под ВС понимается информационное взаимодействие сетевых приложений, выполняющихся на различных узлах сети, посредством формирования одно- или двунаправленного потока IP-пакетов, а также логическая организация сетевых ресурсов, необходимых для обеспечения такого взаимодействия.

Важной особенностью, которую необходимо учитывать при обеспечении ИБ объектов АС, распределённых на IP-сетях, является возможность ситуации, при которой в момент установления ВС соответствует требованиям политики доступа, а во время обмена данными – перестаёт им соответствовать. Необходимо отметить также, что сетевые средства защиты информации сами могут оказаться объектом деструктивных воздействий, что, при успешном проведении атаки, влечёт за собой серьёзные нарушения политики ИБ, которую такие средства призваны обеспечивать.

С учётом изложенного актуальной научно-технической задачей является разработка и совершенствование методов и средств РД в IP-сетях на основе выявления и блокирования ВС, представляющих угрозу ИБ сетевых ресурсов распределённых АС. При этом создаваемые средства должны надёжно парировать направленные на них уделённые деструктивные воздействия.

В диссертационной работе предлагается подход к решению задачи РД в IP-сетях, основанный на представлении каждого виртуального соединения в виде модели состояния. Эта модель включает в себя, как детерминированные параметры сетевого, транспортного и прикладного уровней межсетевого взаимодействия, так и статистические характеристики потока IP-пакетов. Анализ параметров модели производится межсетевым экраном, функционирующим в скрытном режиме. Скрытность МЭ обеспечивается за счёт прозрачности этого устройства для безопасных ВС и отсутствию логических и физических адресов на его фильтрующих интерфейсах.

Диссертационная работа опирается на исследования таких российских и зарубежных учёных, как В.А. Васенин, В.А. Галатенко, П.Н. Девянин, Д. фон Биддер-Сенн и других.

Целью исследования является разработка подхода к решению задачи разграничения доступа в IP-сетях на основе моделей состояния виртуальных соединений.

Для достижения поставленной цели в диссертационной работе были сформулированы и решены следующие задачи.

1. Разработать теоретико-множественную модель описания виртуального соединения для её использования при решении задачи разграничения доступа в IP-сетях.
2. Предложить формальное описание политики доступа к сетевым ресурсам на основе множества правил фильтрации.
3. Разработать модели состояния виртуальных соединений, учитывающие особенности используемых протоколов транспортного уровня в различных фазах межсетевого взаимодействия.
4. Сформировать методику выявления атак типа «затопление» на основе анализа статистических характеристик виртуальных соединений.
5. Разработать архитектуру системы разграничения доступа в IP-сетях, которая обеспечивает скрытную фильтрацию трафика на основе предложенных моделей состояния виртуальных соединений.

Объектом исследования являются виртуальные соединения, организуемые в IP-сетях для обеспечения информационного взаимодействия сетевых приложений. **Предметом** исследования являются модели виртуальных соединений и их использование для решения задачи разграничения доступа в IP-сетях.

Методы исследований. Для решения сформулированных задач использовался аппарат теории множеств, теории алгоритмов, основ теории защиты информации, а также методы статистической обработки данных, процедурного и объектно-ориентированного программирования.

Научные результаты и их новизна

1. Предложена теоретико-множественная модель виртуального соединения, которая является универсальным способом описания информационного потока, возникающего при доступе пользователя к сетевому ресурсу. Такая модель может применяться при решении различных задач по обработке трафика в IP-сетях, включая разграничение доступа, маршрутизацию, биллинг, мониторинг и анализ сетевых протоколов.
2. Впервые предложена алгебра правил фильтрации, формально описывающая политику доступа к сетевым ресурсам. Алгебра позволяет в автоматическом режиме производить оптимизацию набора правил, определять его полноту и непротиворечивость.
3. Разработаны модели состояния виртуальных соединений, позволяющие контролировать корректность использования транспортных протоколов в различных фазах межсетевого взаимодействия. Модели состояния

предназначены для реализации в межсетевых экранах, которые функционируют в скрытном режиме и не разрывают транспортные соединения между взаимодействующими приложениями в IP-сетях.

4. Сформирована методика выявления межсетевыми экранами атак типа «затопление», основанная на анализе статистических характеристик виртуальных соединений. Предложенная методика позволяет идентифицировать атаку для заданных значений вероятностей ошибок 1-го и 2-го рода и минимальном в среднем объёме выборки.
5. Предложена архитектура системы разграничения доступа в IP-сетях, основанная на использовании разработанных моделей состояния виртуальных соединений.

Положения, выносимые на защиту.

1. Теоретико-множественная модель описания виртуального соединения как последовательности IP-пакетов, формируемых в рамках взаимодействия пользователя и сетевого ресурса.
2. Алгебра правил фильтрации для формального описания политики доступа к сетевым ресурсам.
3. Модели состояния виртуальных соединений на основе конечных автоматов, учитывающих параметры протоколов сетевого, транспортного и прикладного уровней в различных фазах межсетевого взаимодействия.
4. Методика выявления межсетевыми экранами атак типа «затопление» на основе анализа статистических параметров моделей состояния виртуальных соединений.
5. Архитектура и программная реализация системы разграничения доступа в IP-сетях, обеспечивающей скрытную фильтрацию трафика на основе моделей состояния виртуальных соединений и подходов к определению их безопасности.

Обоснованность и достоверность представленных в диссертационной работе научных положений подтверждается согласованностью теоретических результатов с результатами, полученными при реализации, а также апробацией основных теоретических положений в печатных трудах и докладах на научных конференциях.

Практическая ценность работы. Разработанные модели, подходы и архитектура системы фильтрации могут быть использованы для создания средств защиты сетевых ресурсов АС, позволяющих производить многоуровневый контроль трафика и разграничение доступа путём

блокирования виртуальных соединений, признанных опасными. В основу диссертационной работы положены результаты, полученные автором в период с 2004 по 2009 год в ходе выполнения НИР и ОКР в ЦНИИ РТК, а также на кафедре «Телематика» ГОУ ВПО «СПбГПУ».

Внедрение результатов. Результаты проведённых исследований нашли практическое применение в перечисленных далее разработках, в которых автор принимал личное участие.

1. Разработанное программное обеспечение вошло в состав межсетевого экрана ССПТ-2, сертифицированного на соответствие требованиям руководящих документов ФСБ и ФСТЭК РФ по 3 классу защищённости. В составе систем защиты информации ССПТ-2 внедрён в эксплуатацию в сетях Федеральной таможенной службы РФ, ФГУ ГНИИ ИТТ «Информика», ОАО «ТГК-1», ЦНИИ РТК, правительства Ленинградской области и в других учреждениях.
2. Модели и алгоритмы, полученные в результате работы, используются в учебном процессе при проведении лабораторных работ по курсам «Методы и средства защиты компьютерной информации», «Сети ЭВМ и телекоммуникации», а также в студенческих НИР на кафедре «Телематика» ГОУ ВПО «СПбГПУ».
3. Программная реализация алгоритмов и подходов, полученная в работе, применяется в составе системы защиты информации, используемой при проведении космического эксперимента «Контур» по управлению роботом-манипулятором, находящимся на борту Международной космической станции, через Интернет.

Апробация и публикация результатов работы. Результаты, полученные в ходе работы над диссертацией, докладывались на всероссийских и межвузовских научно-технических конференциях. По теме диссертации опубликовано 14 статей, в том числе – 3 в изданиях, публикации в которых рекомендуются Высшей аттестационной комиссией Министерства образования и науки Российской Федерации.

Результаты диссертационной работы получены в ходе научно-исследовательских работ, выполненных при поддержке Комитета по науке и высшей школе Правительства Санкт-Петербурга на средства грантов в сфере научной и научно-технической деятельности за 2008 и 2009 годы.

Структура и объем диссертации. Диссертационная работа общим объемом 128 страниц состоит из введения, четырех глав, заключения, списка литературы из 101 наименования, включает 37 рисунков и 8 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении приводится обоснование актуальности темы диссертации, сформулированы цель и задачи исследований, перечислены основные научные результаты и положения, выносимые на защиту. Представлены сведения о внедрении результатов работы, их апробации, о публикациях, а также дана краткая характеристика содержания диссертации.

В первой главе рассмотрены актуальные аспекты обеспечения ИБ сетевых ресурсов АС, распределённых на IP-сетях. Дан краткий обзор основных понятий, протоколов и технологий, которые применяются при построении и эксплуатации таких АС. Предложена классификация сетевых ресурсов, как объектов защиты в распределённых АС, по способу использования, назначению, архитектуре и происхождению.

В главе рассмотрены причины возникновения угроз ИБ сетевых ресурсов распределённых АС. Основными среди этих причин признаны уязвимости базовых протоколов IP-сетей, а также большая размерность и динамичность множества сетевых ресурсов. Проведён анализ актуальных в настоящее время технических способов реализации таких угроз, а также методов и средств, применяемых при построении защищённых систем хранения, обработки и передачи информации.

Показано, что одним из эффективных методов защиты информации является разграничение доступа. В сетевой среде РД реализуется с помощью межсетевых экранов, которые устанавливаются на границе сегментов сети и контролируют информационные потоки, передаваемые из одного сегмента в другой. Приведена классификация и обзор существующих МЭ, выделены общие функциональные особенности. Показано, что большинство современных МЭ обеспечивают РД в IP-сетях на основе многоуровневого анализа информационных потоков, возникающих при доступе пользователей к сетевым ресурсам. Так, на сетевом и транспортном уровне используется пакетная фильтрация, проверка корректности реализации протоколов обеспечивается путём контроля (инспекции) их состояний, а на прикладном уровне применяется контентная фильтрация. Выявлены сильные и слабые стороны используемых подходов.

Отмечены преимущества скрытного режима функционирования МЭ. В таком режиме устройство прозрачно для трафика, соответствующего требованиям реализованной политики доступа к ресурсам. Прозрачность подразумевает отсутствие логических и физических адресов на сетевых интерфейсах, а также сохранение целостности заголовков и данных в

обрабатываемых сетевых пакетах. Преимуществом скрытного режима является принципиальная невозможность удалённого доступа к операционной системе МЭ, что делает его устойчивым к атакам, связанным со взломом программных компонентов средств защиты информации. Определено понятие полной скрытности устройств защиты, включающее свойство статистической инвариантности, при котором МЭ сохраняет статистические характеристики обрабатываемых информационных потоков.

Сформулировано обоснование актуальности темы исследования, выполнена постановка задачи.

Во второй главе представлена теоретико-множественная модель ВС, обоснован переход от такой модели к вектору состояния для решения задачи РД. Изложен способ формального описания политики доступа к сетевым ресурсам на основе алгебры правил фильтрации, приведены примеры использования разработанной алгебры.

Показано, что для межсетевого экрана любое ВС однозначно определяется последовательностью IP-пакетов, формируемых сетевыми приложениями для информационного обмена. В этом случае ВС *v* представимо в виде счётного подмножества декартова произведения конечного множества IP-пакетов *P* и счётного (в случае дискретного времени) множества временны*х* меток *T*: $v = \{p_{t_i}\}, i = \overline{1, N}, N \in [1, \infty) \subset P \times T$. Решение задачи РД в IP-сетях на основе данной теоретико-множественной модели представляется затруднительным в силу отсутствия в ней таких понятий, как субъект и объект взаимодействия. По этой причине предложено описание ВС в виде вектора состояния:

$$v = \{p_{t_i}\}, i = \overline{1, N}, N \in [1, \infty) \rightarrow v' = \{y_k\}, k = \overline{1, K}, K < \infty$$

Вектор состояния $Y = \{y_k\}$ ВС объединил параметры y_k, которые идентифицируют субъект, объект и информационный поток, возникающий в IP-сети при осуществлении доступа. К этим параметрам были отнесены IP-адреса субъекта и объекта (далее именуемые клиентом и сервером в соответствии с моделью «клиент-сервер»), порты протоколов TCP и UDP клиента и сервера, протоколы транспортного и прикладного уровней, состояние (фаза соединения) транспортного протокола, доменное имя при обращении к WEB-серверу, имя запрашиваемого файла для обмена по протоколам HTTP и FTP, адреса электронной почты отправителя и получателя для протокола SMTP и ряд других параметров, необходимых для анализа безопасности ВС. Кроме детерминированных параметров в вектор состояния вошли и статистические характеристики потока IP-пакетов,

передаваемых в рамках ВС, в том числе интенсивность потока, а также количество переданных пакетов и байт.

Задача разграничения доступа была сведена к классификации виртуальных соединений на основе анализа параметров их векторов состояния и решалась в следующей постановке. Имеется множество виртуальных соединений $V=\{v_i,\ i=\overline{1,\infty}\}$, каждое из которых описывается вектором состояния $Y_i=\{y_k\}_i, k=\overline{1,K}$. Известно, что множество V является объединением подмножества опасных $V_{\text{о}}$ и безопасных $V_{\text{б}}$ виртуальных соединений. Необходимо определить индикаторную функцию $F(Y_i)$, такую, что

$$F(Y_i)=\begin{cases}1, \text{если } v_i \in V_{\text{о}};\\ 0, \text{если } v_i \notin V_{\text{о}}.\end{cases} \quad (1)$$

Решение задачи в предложенной постановке потребовало конкретизации понятия опасных виртуальных соединений, для чего множество $V_{\text{о}}$ было представлено в виде объединения подмножеств $V_{\text{од}} \cup V_{\text{оп}} \cup V_{\text{оа}}$, где:

- $V_{\text{од}}$ – подмножество ВС, которые используются для межсетевых взаимодействий, запрещённых реализованной политикой доступа;
- $V_{\text{оп}}$ – подмножество ВС, использующих сетевые протоколы в порядке, не предусмотренном их спецификациями;
- $V_{\text{оа}}$ – подмножество ВС, представляющих собой удалённые деструктивные воздействия через разрешённые реализованной политикой доступа ВС (в работе рассматривались атаки типа «затопление»).

Для решения поставленной задачи произведена декомпозиция функции (1), в результате чего она представлена в виде совокупности следующих функций:

- $F_1(Y_i,\ R)$ определяет соответствие виртуального соединения v_i реализованной политике доступа R;
- $F_2(Y_i,G)$ проверяет виртуальное соединение на предмет корректности использования транспортного протокола, заданного моделью состояния G в виде конечного автомата;
- $F_3(Y_i)$ производит оценку вероятности реализации атаки типа «затопление» через виртуальное соединение v_i.

В соответствии с приведенным разбиением множества $V_{\text{о}}$:

$$F_1(Y_i,R)=\begin{cases}1, \text{если } v_i \in V_{\text{од}};\\ 0, \text{если } v_i \notin V_{\text{од}}.\end{cases}\ F_2(Y_i,G)=\begin{cases}1, \text{если } v_i \in V_{\text{оп}};\\ 0, \text{если } v_i \notin V_{\text{оп}}.\end{cases}\ F_3(Y_i)=\begin{cases}1, \text{если } v_i \in V_{\text{оа}};\\ 0, \text{если } v_i \notin V_{\text{оа}}.\end{cases} \quad (2)$$

Для определения функции $F_1(Y,R)$ (2) в работе введено формальное

описание политики доступа, представляющее собой алгебру правил фильтрации $\mathcal{R} = <R, \Sigma>$, где R – множество правил фильтрации, Σ – множество допустимых над элементами R операций. Множество правил фильтрации $R = \{r_j, j=\overline{1,|R|}\}$ – несущее множество алгебры $\mathcal{R}$, являющееся коммутативным кольцом. Каждое правило $r_j = \{X_1,\ldots,X_N, A_1,\ldots A_M\}_j$ состоит из вектора X_j параметров и вектора A_j атрибутов. Пример элементов вектора параметров правила r_j: X_{j1} – множество IP-адресов клиента, X_{j2} – множество TCP-портов сервера. Атрибуты правила фильтрации определяют действия механизма РД, связанные с обработкой ВС, например A_{j1} – обязательный атрибут, определяющий действие правила фильтрации и заданный на множестве значений {0, 1}, где A_{j1}=0 означает запрет доступа, A_{j1}=1 – разрешение доступа. Области допустимых значений для векторов параметров и атрибутов задаются в виде множеств $DX_1,\ldots,DX_N$ и $DA_1,\ldots,DA_M$ в соответствии с семантикой каждого параметра и атрибута. Множество $\Sigma=\{\varphi_1,\varphi_2\}$ определяет операции, допустимые над правилами фильтрации, где φ_1 – операция сложения, φ_2 – операция умножения.

Операция сложения для правил определяется следующим образом:

$$r_3 = r_1 + r_2 = \{X_{11}, X_{12},...X_{1N}, A_{11}, A_{12},..., A_{1M}\} + \{X_{21}, X_{22},...X_{2N}, A_{21}, A_{22},..., A_{2M}\}$$

$$r_3 = \begin{cases} \{X_{11} \cup X_{21},...X_{1N} \cup X_{2N}, A_{11} \vee A_{21}, A_{12} \cup A_{22},..., A_{1M} \cup A_{2M}\}, \text{где } A_{11} = A_{21}; \\ \{X_{11} \Delta X_{21},...X_{1N} \Delta X_{2N}, A_{11} \wedge A_{21}, A_{12} \Delta A_{22},..., A_{1M} \Delta A_{2M}\}, \text{где } A_{11} \neq A_{21}, \end{cases}$$

где A_{i1} – атрибут действия правила фильтрации; $\cup$ – объединение; Δ – симметричная разность; $\vee$ и $\wedge$ – логические дизъюнкция и конъюнкция.

Операция умножения для правил задаётся следующим образом:

$$r_3 = r_1 * r_2 = \{X_{11}, X_{12},...X_{1N}, A_{11}, A_{12},..., A_{1M}\} * \{X_{21}, X_{22},...X_{2N}, A_{21}, A_{22},..., A_{2M}\}$$

$$r_3 = \{X_{11} \cap X_{21}, X_{12} \cap X_{22},...X_{1N} \cap X_{2N}, A_{11} \wedge A_{21}, A_{12} \cap A_{22},..., A_{1M} \cap A_{2M}\}$$

где $\cap$ – операция пересечения множеств.

Нулевой 0_r, единичный 1_r и противоположный $-r$ элементы множества R:

$0_r = \{\varnothing,...,\varnothing, A_1, \varnothing,...,\varnothing\}$, где $A_1 = 0$

$1_r = \{DX_1, DX_2,..., DX_N, A_1, DA_2,..., DA_M\}$, где $A_1 = 1$

$-r = \{X_1, X_2,..., X_N, \overline{A}_1, A_2,..., A_m\}$, где $\overline{A}_1$ – логическое отрицание A_1

Для несущего множества R, как коммутативного кольца, выполняются необходимые условия коммутативности, ассоциативности и дистрибутивности, а также существование нулевого, единичного, и противоположного элемента.

Возможность доступа субъекта к объекту в рамках ВС, заданного вектором состояния $Y_i=\{y_{ik},k=\overline{1,K}\}$, определяется правилом фильтрации,

соответствующим ВС и содержащим вектор параметров $X_j=\{X_{jn},\ n=\overline{1,N}\}$. Соответствие между Y_i и X_j задаётся следующим образом: правило r_j соответствует ВС v_i в случае, если $\forall y_k \in Y_i \cap X_j$ и $\forall X_n \in Y_i \cap X_j$ выполняется условие $y_{i1} \in X_{j1},\ y_{i2} \in X_{j2},\ \ldots,\ y_{il} \in X_{jl},\ l=\overline{1,|Y_i \cap X_j|}$. Правило r_i считается в большей степени соответствующим ВС v, чем правило r_j, если оба правила r_i и r_j соответствуют ВС v, и при этом выполняется одно из условий: 1) $X_{i1} \subset X_{j1}$; 2) $X_{i1} \subseteq X_{j1} \wedge X_{i2} \subset X_{j2}$; 3) $X_{i1} \subseteq X_{j1} \wedge X_{i2} \subseteq X_{j2} \wedge X_{i3} \subset X_{j3}$; … ; n) $X_{i1} \subseteq X_{j1} \wedge X_{i2} \subseteq X_{j2} \wedge X_{i3} \subseteq X_{j3} \wedge \ldots \wedge X_{iN} \subset X_{jN}$. Под правилом фильтрации, соответствующим ВС v в наибольшей степени понимается правило r_k, вектор параметров X_k которого удовлетворяет условию $X_{k1} \subseteq X_{j1} \wedge X_{k2} \subseteq X_{j2} \wedge X_{k3} \subseteq X_{j3} \wedge \ldots \wedge X_{kN} \subset X_{jN}$, j=1..k-1,k+1,…|R|. Обозначим через r_i* правило фильтрации, соответствующее ВС v_i в наибольшей степени. В этом случае функция РД $F_1(Y,R)$ принимает вид:

$$F_1(Y_i,R)=\begin{cases}1\ для\ r_k^*(k\in\{1..|R|\}),\ если\ A_{k1}=0\ (v_i\in V_{оз})\\ 0\ для\ r_k^*(k\in\{1..|R|\}),\ если\ A_{k1}=1\ (v_i\notin V_{оз}).\end{cases}$$

Вычислимость функции F_1 определяется наличием алгоритма, который производит поиск и применение правила фильтрации, в наибольшей степени соответствующего обрабатываемому виртуальному соединению.

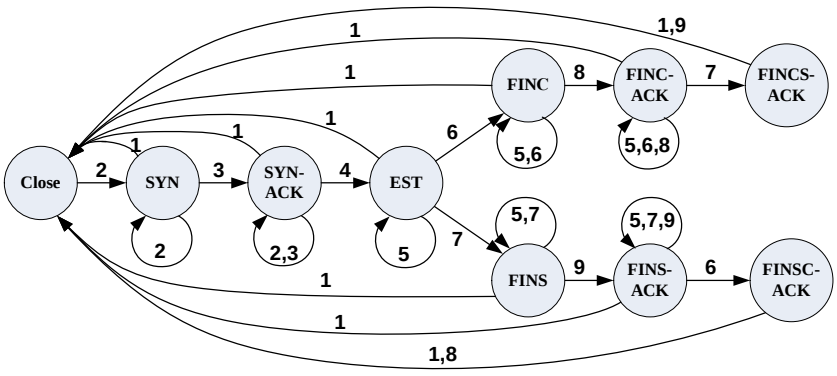
В третьей главе представлены модели состояния виртуальных соединений, изложены результаты исследования сетевого трафика для выявления атак типа «затопление», сформулирована методика обнаружения подобных атак на основе анализа статистических характеристик вектора состояния виртуального соединения.

Определение функции $F_2(Y_i,G)$ (2) связано с анализом корректности используемых в рамках ВС протоколов транспортного уровня стека TCP/IP. С учётом специфики используемых в настоящее время транспортных протоколов было принято решение о разработке двух моделей состояния ВС: конечного автомата G_1 для протокола TCP и конечного автомата G_2 для остальных протоколов, включая UDP, ICMP и других, функционирующих над уровнем IP. При разработке конечных автоматов G_1 и G_2 учитывалось, что их программная реализация будет использоваться межсетевым экраном, работающем в скрытном режиме. На рис.1 представлен конечный автомат G_1, являющийся моделью состояния виртуального соединения, использующего протокол TCP.

Конечные автоматы G_1 и G_2 описывается списком из пяти элементов: (Q, B, δ, ϕ, q_s). В этом списке:

- Q – множество состояний автомата;

- B – входной алфавит автомата (IP-пакеты и события таймера);
- $\delta(q_i, p) = q_k$ – функция переходов автомата;
- $\phi(q, p, Y_i) = \{1,0\}$ – функция контроля соответствия IP-пакета p вектору состояния Y_i виртуального соединения v_i, в состоянии q; отражает требования спецификаций используемого протокола;
- q_s – начальное состояние автомата.



Входной алфавит
(пакеты с флагами TCP *F* и таймаут T):
1. p: RESET ∈ *F* V T
2. p: SYN ∈ *F*
3. p: SYN&ACK ∈ *F*
4. p: ACKS∈ *F* (ACK на SYN)
5. p: ACK∈ *F*
6. p: FIN-C ∈ *F* (FIN от клиента)
7. p: FIN-S ∈ *F* (FIN от сервера)
8. p: ACKS-FC ∈ *F* (ACK от сервера на FIN от клиента)
9. p: ACKC-FS ∈ *F* (ACK от клиента на FIN от сервера)

Состояния:
Close – соединение закрыто
SYN – синхронизация (передан SYN-пакет)
SYN-ACK – подверждение синхронизации (передан SYN&ACK-пакет)
EST – соединение установлено
FINC – запрос на завершение соединение от клиентом
FINS – запрос на завершение соединение от сервера
FINC-ACK – подтверждение завершения соединения сервером
FINS-ACK – подтверждение завершения соединения клиентом
FINCS-ACK – завершения соединения клиентом и запрос на завершение от сервера
FINSC-ACK – завершения соединения сервером и запрос на завершение от клиента

Рис. 1. Модель состояния виртуального соединения по протоколу TCP

Разработанные модели состояния позволяют задать функцию $F_2(Y_i,G)$ контроля корректности используемого протокола следующим образом:

$$F_2(Y_i, G) = \begin{cases} 1, \text{ если } \phi(q, p, Y_i) = 0 \ (IP\text{ - пакет } p \text{ не соответствует состоянию } q,\ v_i \in V_{\text{оп}}), \\ 0 \text{ если } \phi(q, p, Y_i) = 1 \ (IP\text{ - пакет } p \text{ соответствует состоянию } q,\ v_i \notin V_{\text{оп}}). \end{cases}$$

Виртуальные соединения, разрешённые реализованной политикой доступа, могут использоваться для проведения удалённых атак типа «затопление» (flood-атак). Этот класс деструктивных воздействий характеризуются передачей на сетевой объект (хост или сеть) значительного количества IP-пакетов, что в большинстве случаев приводит к недоступности атакуемого объекта. В силу существенных ограничений на вычислительные и временные ресурсы при обработке трафика МЭ для выявления flood-атак, как правило, используются поведенческие модели. В рамках этих моделей для контролируемых параметров трафика определяются пороговые значения, превышение которых означает идентификацию атаки МЭ в текущий момент времени. При этом обычно не учитывается принадлежность IP-пакетов, формирующих flood-атаку, к тому или иному ВС, что при обнаружении атаки

влечёт за собой блокирование, в том числе, и безопасных ВС. С этой точки зрения более предпочтительным является подход, при котором контролируются, как параметры совокупного трафика, так и параметры каждого виртуального соединения в отдельности.

В ходе исследования было установлено, что перспективными с точки зрения выявления flood-атак являются такие параметры вектора состояния ВС, как мгновенная интенсивность (частота поступления) пакетов и межпакетные интервалы. На рис.2 представлены графики, демонстрирующие вариации этих параметров для различных ВС, в том числе и для имитаций некоторых типов flood-атак.

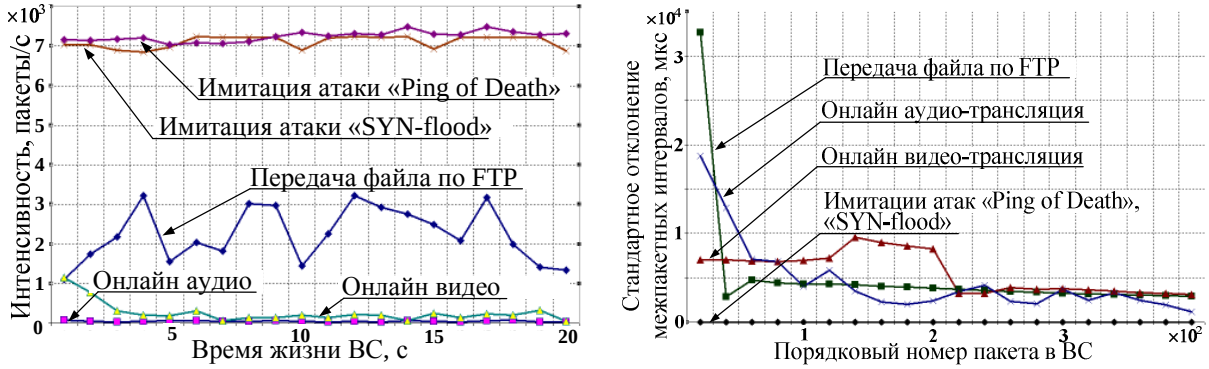


Рис.2. Графики интенсивностей и стандартного отклонения межпакетных интервалов для различных виртуальных соединений

Показано, что одновременный подсчет статистик мгновенной интенсивности и межпакетных интервалов для выявления flood-атак не является целесообразным в силу того, что эти параметры ВС математически связаны между собой. По этой причине предложена методика выявления flood-атаки межсетевым экраном на основе выборки значений мгновенной интенсивности пакетов в рамках ВС, подсчёта статистик для безопасных ВС на этапе обучения и определения аномальных отклонений от полученных значений на этапе обнаружения. При этом мгновенная интенсивность ВС определялась по формуле: $y_{ij} = d / t_i$, где y_{ij} – j-е значение выборки i-го параметра (мгновенной интенсивности) в векторе состояния ВС, d – константа, определяющая количество ожидаемых IP-пакетов (в исследованиях d полагалась равной 10), а t_j – временной интервал, в течение которого было получено d IP-пакетов для вычисления y_{ij}.

В ходе исследования доказано, что мгновенная интенсивность ВС, как случайная величина, при достаточно больших объёмах выборки ($n>10^2$) в соответствии с критерием χ^2 Пирсона на уровне значимости $\alpha=0{,}05$ апроксимируется нормальным законом распределения $N(y_0, \sigma^2)$. Параметры этого закона зависят от текущей загрузки сегментов IP-сети на маршруте

между взаимодействующими сетевыми приложениями, а также от типа этих приложений. Статистическая модель параметра мгновенной интенсивности для безопасных ВС и flood-атак представлена на рис.3 (а). Здесь кривая $\varphi_0(y)$ соответствует распределению $N_0(y_0,\sigma_0^2)$ мгновенных интенсивностей для безопасных ВС, а кривая $\varphi_1(y)$ – распределению $N_1(y_1,\sigma_1^2)$ для flood-атак, то есть опасных виртуальных соединений.

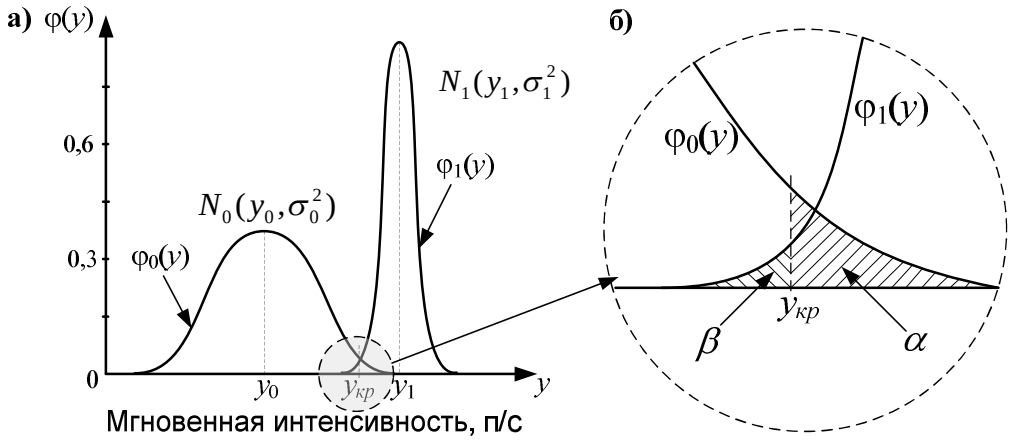


Рис. 3. Кривые распределений мгновенных интенсивностей (а); вероятности ошибок 1-го (α) и 2-го (β) рода при оценке безопасности ВС (б)

Задача классификации ВС в данном случае была сведена к задаче проверки простых статистических гипотез. Основной гипотезой H_0 признано предположение о соответствии математического ожидания выборки $(y_{i1},y_{i2},\ldots,y_{in})$ закону $N_0(y_0,\sigma_0^2)$, альтернативной гипотезой H_1 – предположение о соответствии указанной статистики закону $N_1(y_1,\sigma_1^2)$. В случае подтверждения гипотезы H_0 ВС признавалось безопасным, в случае подтверждения H_1 – опасным. При решении отдавалось предпочтение уменьшению вероятности β ошибки 2-го рода (рис. 3, б), когда принимается основная гипотеза H_0 в то время, как она не верна (пропуск flood-атаки).

Для проверки статистических гипотез был выбран метод последовательного анализа с использованием критерия отношения функций правдоподобия (критерий Вальда):

$$\lambda = \frac{L_1(y_{i1}, y_{i2},..., y_{in})}{L_0(y_{i1}, y_{i2},..., y_{in})},$$

где $L_0(y_{i1},y_{i2},\ldots,y_{in})$ и $L_1(y_{i1},y_{i2},\ldots,y_{in})$ – функции правдоподобия при условии справедливости соответственно гипотезы H_0 и H_1. Эти функции вычисляются по следующим формулам:

$$L_0(y_{i1}, y_{i2},..., y_{in}) = \varphi_0(y_{i1})\varphi_0(y_{i2})...\varphi_0(y_{in})$$
$$L_1(y_{i1}, y_{i2},..., y_{in}) = \varphi_1(y_{i1})\varphi_1(y_{i2})...\varphi_1(y_{in})$$

Таким образом, методика обнаружения flood-атак сводится к определению значения критерия λ каждый раз при вычислении очередного значения y_{ij} мгновенной интенсивности на протяжении всего времени жизни ВС. После этого вычисляется функция $F_3(Y_i)$ (2) по следующей формуле:

$$F_3(Y_i)=\begin{cases} -1, \text{ если } \lambda \le \dfrac{\beta}{1-\alpha} \text{ (принимается гипотеза } H_0,\ v_i \notin V_{\text{оа}}), \\ 0, \text{ если } \dfrac{\beta}{1-\alpha} < \lambda < \dfrac{1-\beta}{\alpha} \text{ (продолжение измерений)} \\ 1 \text{ если } \lambda \ge \dfrac{1-\beta}{\alpha} \text{ (принимается гипотеза } H_1,\ v_i \in V_{\text{оа}}). \end{cases}$$

Если в результате очередного вычисления $F_3(Y_i)$=1 (принимается гипотеза H_1), то это означает, что ВС v_i принадлежит подмножеству $V_{\text{оа}}$ и подлежит блокированию.

Предложенная методика позволяет получить минимальный в среднем объем выборки по сравнению с другими критериями (Байеса, Неймана-Пирсона, максимального правдоподобия), что гарантирует скорейшее принятие решения об опасности ВС. Объём выборки при этом зависит от величин вероятностей ошибок 1-го и 2-го рода.

В четвертой главе представлена архитектура (рис. 4) и результаты разработки системы разграничения доступа в IP-сетях на основе скрытной фильтрации трафика с использованием моделей состояния ВС.

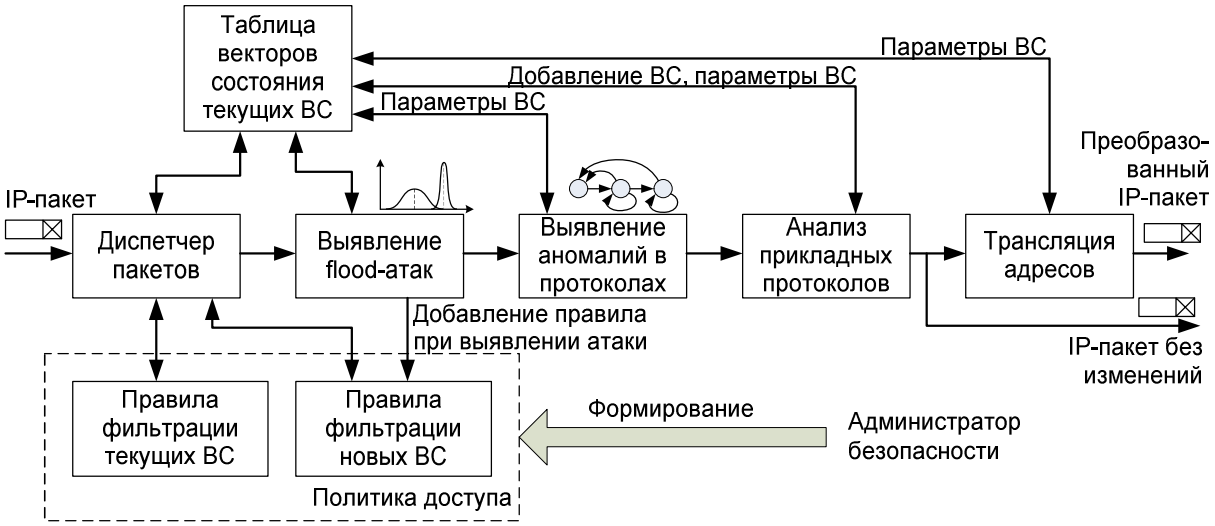


Рис. 4. Архитектура системы разграничения доступа в IP-сетях

Реализованная на основе предложенной архитектуры система разграничения доступа в качестве подсистемы вошла в состав программного обеспечения МЭ ССПТ-2. Данный межсетевой экран может использоваться в локальных вычислительных сетях, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с, поддерживает

одновременную обработку до 50000 ВС, обеспечивает совокупную пропускную способность до 800 Мбит/с и создание до 7000 ВС в секунду.

Программная реализация разработанных моделей явилась основой для внедрения в МЭ ССПТ-2 функций контентной фильтрации данных, передаваемых прикладными протоколами в рамках виртуального соединения.

Отличительной особенностью МЭ ССПТ-2 является постоянный скрытный режим функционирования в сетевой среде. За счёт этого достигается нечувствительность МЭ к широкому классу деструктивных воздействий, направленных на компоненты системы защиты информации, а также универсальность процедуры установки в инфраструктуру эксплуатируемых IP-сетей.

Основные результаты работы

1. Разработана теоретико-множественная модель виртуального соединения, которая является универсальным способом описания информационного потока между взаимодействующими приложениями в IP-сети.
2. Предложено формальное описание политики доступа к сетевым ресурсам на основе алгебры правил фильтрации, которая учитывает параметры сетевых, транспортных и прикладных протоколов виртуального соединения.
3. Разработаны модели состояния виртуальных соединений на основе конечных автоматов, учитывающих особенности различных фаз межсетевого взаимодействия. Данные модели позволяют выявить аномалии, связанные с некорректным использованием сетевых протоколов, а также являются основой для реализации контентной фильтрации трафика.
4. Сформирована методика выявления атак типа «затопление» на основе последовательного анализа статистических параметров моделей состояния виртуальных соединений.
5. Разработана архитектура системы разграничения доступа в IP-сетях на основе предложенных в диссертации моделей и подходов к определению безопасности виртуальных соединений. Реализация системы включена в состав программного обеспечения межсетевого экрана, который осуществляет скрытную многоуровневую фильтрацию трафика и может использоваться, как составная часть комплексной системы защиты информации организации.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Силиненко, А.В. Модели и методы описания политики безопасности для управления доступом в распределённых информационных системах / А.В. Силиненко, А.Н. Титов, В.Ю. Скиба, Ю.Н. Рыжов // Научно-технические ведомости СПбГПУ. – 2009. – №4. – С. 176-182**
2. **Заборовский, В.С. Система семантического управления доступом к сетевым ресурсам / В.С. Заборовский, Ю.Н. Рыжов, А.В. Силиненко // Научно-технические ведомости СПбГПУ. – 2008. – №2. – С. 17-21.**
3. **Силиненко, А.В. Модели и методы скрытной контентной фильтрации прикладных протоколов / А.В. Силиненко // Научно-технические ведомости СПбГПУ. – 2007. – №4. – С. 117-121.**
4. Силиненко, А.В. Логико-динамические аспекты моделирования процессов контентной фильтрации прикладных протоколов / А.В. Силиненко, В.С. Заборовский, // Третья международная научная конференция по проблемам безопасности и противодействия терроризму: докл. конф., Московский государственный университет им. М.В. Ломоносова, 25-27 окт. 2007 г. – М.: МЦНМО, 2008. С. 272-277.
5. Силиненко, А.В. Обеспечение полной скрытной фильтрации сетевыми средствами защиты информации / Силиненко А.В. // XIV конференция представителей региональных научно-образовательных сетей «RELARN-2007»: докл. конф., Н.Новгород, 6-9 июня 2007 г. – Н.Новгород, 2007. – С. 33-34.
6. Силиненко, А.В. Теоретические аспекты использования механизма контроля транспортных соединений в межсетевых экранах / А.В. Силиненко // Шестая Всероссийская научно-техническая конференция «Теоретические и прикладные вопросы современных информационных технологий» : докл. конф, Улан-Удэ, 25-31 июня 2005 г. – Улан-Удэ: Изд-во ВСГТУ, 2005. – С. 57-61.
7. Силиненко, А.В. Средства защиты информации на основе скрытной многоуровневой фильтрации / А.В. Силиненко, В.С. Заборовский, // II Всероссийская научно-практическая конференция «Методы и средства технической защиты конфиденциальной информации» : докл. конф., Обнинск, 7-9 июня 2005 г. – Обнинск, 2005. – С. 78-80.