УДК 681.324

Н.И. АЛИШОВ, В.А. МАРЧЕНКО

ТЕХНОЛОГИЯ ИНТЕГРАЦИИ СРЕДСТВ ЗАЩИТЫ СЕТЕВОГО ПЕРИМЕТРА

Abstract: *In article the new approach in technology of integration of means of protection of network perimeter of information system is considered. Formalization of technology of the organization of protection of network perimeter is adduced and its brief description is given. Results of experimental modelling of the offered technology in the environment of discrete modelling OMNET ++ are described*
Key words: *network perimeter, means of protection, security, technology of integration, information security.*

Анотація: *У статті розглядається новий підхід в технології інтеграції захисту мережевого периметра інформаційної системи. Подається формалізація технології організації захисту мережевого периметра і дається її короткий опис. Описуються результати експериментального моделювання запропонованої технології в середовищі дискретного моделювання OMNET++.*
Ключові слова: *мережевий периметр, засоби захисту, безпека, технологія інтеграції, інформаційна безпека.*

Аннотация: *В статье рассматривается новый подход в технологии интеграции средств защиты сетевого периметра информационной системы. Приводится формализация технологии организации защиты сетевого периметра и даётся её краткое описание. Описываются результаты экспериментального моделирования предложенной технологии в среде дискретного моделирования OMNET++*
Ключевые слова: *сетевой периметр, средства защиты, безопасность, технология интеграции, информационная безопасность*.

1. Введение

Информационная безопасность (ИБ) – одно из наиболее бурно развивающихся направлений в современной IT индустрии. Появляется очень много новых продуктов и технологий для организации безопасности информационных ресурсов. Соответственно все понятия и установившиеся подходы в обеспечении защиты информации приобретают новый смысл и содержание.

Одним из основных понятий в ИБ является понятие сетевого периметра. В современном контексте сетевой периметр определяется не только как граница между внутренней и внешней сетями, но и есть граница критической инфраструктуры для жизнедеятельности организации. К таким критическим элементам относятся почтовые серверы, серверы баз данных, внешние носители информации внутренних систем и т.д.

В свете такого подхода защита по сетевому периметру ведётся как от внешнего проникновения, так и от внутренних угроз. В ответ на эти требования IT-индустрия выпускает всё новые и новые средства для решения подобных задач. Причём эти средства зачастую не имеют как обратной совместимости, так и несовместимы между собой. При этом разные средства дублируют функции других, а некоторые из них бывают невостребованными данной информационной средой.

2. Постановка задачи

Одним из направлений развития средств защиты является попытка объединения разрозненных элементов защиты сетевого периметра в единую интегрированную систему с центральным управлением. Такие возможности существуют у всех ведущих поставщиков, присутствующих на рынке, но качество взаимодействия этих средств внутри системы очень разное и не всегда является оптимальным с точки зрения как выполнения требуемых функций, так и набора составляющих данной системы. Кроме того, большую проблему составляет трудность интеграции продуктов разных производителей в единую систему. Для чего требуется реализовать дополнительные компоненты-

прослойки. Поэтому в данной статье рассматриваются концепция и технологические особенности реализации метода интеграции средств защиты сетевого периметра путем взаимной адаптации базовых функций безопасности информационных ресурсов корпоративной системы.

3. Состояние проблемы

Почти каждый продукт защиты сетевого периметра представляет собой сложный комплекс разнообразных компонентов, выполняющих разные задачи. И зачастую востребованными у конечного пользователя остаются в лучшем случае только некоторые из этих компонентов. Примерами таких устройств может служить Cisco Secure PIX Firewall 525 [1] и Check Point Firewall-1 [2]. Это брандмауэры корпоративного уровня, сочетающие в себе не только сам межсетевой экран, но и функции VPN сервера и системы обнаружения вторжений, не считая поддержки специфических протоколов и технологий. Соответственно и цена на такие устройства очень высока и не всегда соответствует используемым возможностям. При этом для реализации одних и тех же функций используются разные средства. Каждое из этих устройств использует свою внутреннюю операционную систему со своим языком программирования. Отчеты, предоставляемые для пользователя, имеют разный формат и для их объединения нужно использовать дополнительное программное обеспечение [3].

4. Метод решения поставленной задачи

В качестве решения вышеизложенных задач предлагается использовать модульный принцип защиты сетевого периметра [4]. В основе этого принципа лежит идея создания фиксированного набора простых программно-аппаратных модулей, каждый из которых реализует определенную функцию защиты [4]. Такой – набор состоит из нескольких групп модулей:

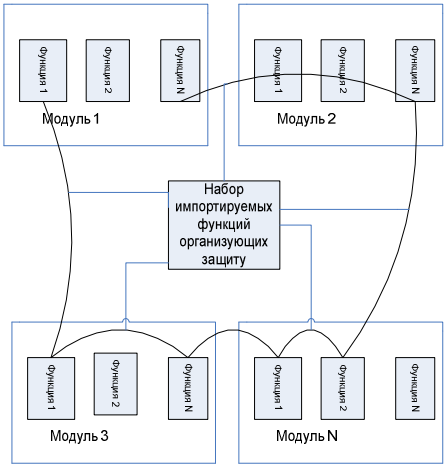

Рис. 1. Организация защиты сетевого периметра при помощи модулей защиты

– контроля доступа и управления информационной средой;

– управления информационными потоками;

– криптографического обеспечения.

Все эти группы модулей выполняют определённый круг задач для построения интегрированной системы защиты сетевого периметра. Такой подход даёт возможность унифицировать современные средства защиты информации. При этом определённый профиль защиты может быть образован путем интеграции используемых модулей в конкретной информационной системе. В данной работе интеграция средств представляется как агрегация реализуемых функций разных модулей для целей защиты информационной среды (рис. 1).

Для взаимодействия между модулями в рамках единой информационной среды используется специализированный протокол обмена сообщениями. Функциями такого протокола являются:

– определение конфигурации окружающей среды;

– поддержание заданной конфигурации среды;

– утилизация текущей конфигурации среды;

– распределение и агрегация функций конкретных модулей на основе заданного профиля защиты;

– контроль, идентификация, аутентификация, шифрование сообщений.

Ниже рассматриваются основные функциональные возможности базовых групп модулей, которые являются определяющими сущности технологии интеграции защиты сетевого периметра.

1. Группа модулей контроля доступа и управления информационной средой. Модули, принадлежащие к группе контроля доступа и управления информационной средой, выполняют функции контроля доступа пользователя к информационной среде, организовывают и контролируют взаимодействие между остальными модулями в данной информационной среде, а также реализуют оповещение конечных пользователей и сбор статистических данных всей информационной системы. К таким модулям относятся:

– контроль доступа;

– управление конфигурацией;

– оповещение.

Модуль контроля доступа. Этот модуль управляет доступом субъектов информационной системы к её объектам. При этом для контроля доступа могут быть подключены другие модули, в частности, модуль аутентификации. Это позволяет гибко изменять и настраивать текущую конфигурацию всей информационной среды. Предлагаемая структура организации модуля имеет следующий состав:

– метод доступа на основе временных ограничений;

– метод доступа на основе места расположения субъекта;

– модуль аутентификации на основе:

- o парольных фраз;
- o цифрового сертификата;
- o электронных ключей;
- o биометрических методов;
- o комбинированных методов.

Следует отметить, что сопутствующие функции импортируются с других соответствующих модулей (шифрование, цифровая подпись, хеширование и т.д.). Это позволяет максимально упростить архитектуру модулей, а также повысить их надёжность.

Модуль управления конфигурацией. Этот модуль реализует функции создания, управления, контроля и утилизации всей конфигурации информационной среды. И поэтому он должен реализовывать следующие функции:

– менеджмент на основе заданных профилей безопасности;

– менеджмент на основе динамических профилей безопасности;

– менеджмент множеством конфигураций;

– проверка целостности конфигураций;

– анализ качества и эффективности профилей безопасности;

– масштабирование системы;

– определение вышедших из строя модулей;

– «горячая» реконфигурация системы.

Эти обобщенные функции требуют дальнейшего уточнения и детализации, но они обеспечивают минимально необходимую функциональную полноту.

Модуль оповещения предоставляет услуги «пассивного» и «активного» оповещения.

Под «пассивным» оповещением следует понимать извещение о событии контролирующего субъекта системы и сохранение данных о событии в определённом хранилище. Под «активным» оповещением следует понимать возможность самостоятельного принятия решения или использования сторонней экспертной системы для изменения текущей конфигурации сетевой среды. При этом возможна реализация разных сценариев протекания процесса реконфигурации. Базовыми функциями, которые должны быть реализованы модулем оповещения, являются:

– визуальное оповещение;

– отправка сообщения на E-mail;

– оповещение на пейджер или телефон;

– выдача звукового сигнала;

– отправка SNMP-сообщения;

– регистрация в системном журнале (Syslog);

– реконфигурация сетевой среды.

Перечисленные функции выбраны, исходя из пользовательских возможностей модуля оповещения, реализованных в современных средствах защиты информации, и поэтому являются наиболее оптимальными с точки зрения частоты использования и востребованности.

Безусловно, данный перечень может быть расширен. Выбор конкретных функций определяется политикой безопасности в реальных информационных системах.

2. Группа модулей управления информационными потоками. Группа модулей управления информационными потоками занимается непосредственной обработкой информационных потоков. Набор этих модулей является результатом декомпозиции на составляющие современных средств защиты информации (СЗИ), и поэтому они максимально упрощены. При этом следует понимать, что некоторые современные средства не реализуются каким-то одним определённым модулем, а синтезируются с помощью нескольких экспортируемых функций от разных модулей. И поэтому нет смысла выделять их в отдельный модуль. Минимальный состав этой группы складывается из следующего множества модулей:

– Фильтрация пакетов.

– Экспертный уровень.

– Прокси-сервер.

– Обнаружение атак на основе сигнатур.

– Обнаружение атак на основе статистических показателей.

– Фильтрация контента.

– Обнаружения атак на основе анализа логфайлов.

– Обнаружение атак на основе проверки целостности файловой системы.

– Антивирусная защита.

Модуль фильтрации пакетов. Функции и возможности данного модуля полностью соответствуют классическому фильтрирующему брандмауэру. Соответственно и требования, выдвигаемые к этому модулю, соответствуют аналогичным требованиям к фильтрирующим системам в части реализации конкретных функций [4]. А все остальные функции (управление доступом, оповещение о нарушении и т.д.) реализуют другие модули группы управления информационной средой. Такое разделение функций присуще всем модулям данной группы.

Модуль экспертного уровня. Минимально необходимым набором, реализуемым данным модулем, представляет собой следующий кортеж функций:

– фильтрация по состоянию флагов пакета;

– фильтрация нестандартных наборов флагов;

– фильтрация сообщений ICMP;

– динамическое отслеживание состояния соединения разных протоколов без установления соединения.

Модуль прокси-сервера. К данному модулю выдвигается только несколько требований:

– максимальный набор доступных прокси-серверов;

– полнота соответствия спецификациям реализуемых протоколов.

Все остальные функции данный модуль агрегирует у других модулей и поэтому не нуждается в повторной реализации.

Модуль обнаружения атак на основе сигнатур. Это модуль, лежащий в основе любой классической сетевой системы обнаружения вторжений, и поэтому требования к его организации и реализации давно устоялись. К организационным требованиям следует отнести:

– периодичность обновления сигнатур;

– открытость создания сигнатур;

– простоту создания сигнатур;

– гибкость сигнатур.

В качестве прототипа реализации можно предложить хорошо зарекомендовавшую себя открытую IDS “Snort”, обладающую необходимыми характеристиками [5].

Модуль обнаружения атак на основе статистических показателей. Этот модуль является основой многих современных систем обнаружения разнообразного назначения. К ним относятся сетевые системы обнаружения вторжения, хостовые системы обнаружения вторжений, системы обнаружения нарушителя.

В основе этого модуля лежит некая математическая модель анализа показателей информационной среды. Наиболее распространенными являются следующие математические модели.

Операционная модель основывается на том, что каждое новое наблюдение переменной должно укладываться в некоторых границах. Если этого не происходит, то мы имеем дело с отклонением. Допустимые границы определяются на основании анализа предыдущих значений переменной. Данная модель может использоваться, если некоторое значение метрики можно аргумен-

тированно связать с попыткой вторжения (например, количество попыток ввода пароля более 10) [6].

Модель среднего значения и среднеквадратичного отклонения базируется на том, что для всех значений, известных из предыдущих наблюдений некоторой величины $(x_1,...,x_n)$ их среднее значение $(m = \overset{\circ}{a}\, x_i / n)$, а среднеквадратичное отклонение $s = \sqrt{\frac{x_1^2 + ... + x_n^2}{n-1} - m^2}$. Тогда новое наблюдение является анормальным, если оно не укладывается в границах доверительного интервала $m + d \cdot s$. Модель применима для измерения счетчиков событий, временных интервалов и используемых ресурсов. Преимуществом модели по сравнению с *операционной* является независимость оценки анормальности поведения от априорных знаний. Кроме того, необходимо отметить, что анормальность поведения зависит от значения доверительного интервала и, как следствие, понятие анормальности для пользователей системы может отличаться [7].

Многовариационная модель аналогична модели среднего значения и среднеквадратичного отклонения, но учитывает корреляцию между двумя или большим количеством метрик (использование ЦПУ и количество операций ввода-вывода, количество выполненных процедур входа в систему и время сессии) [8].

Модель Марковского процесса применима только к счетчикам событий, она рассматривает каждый тип событий как переменную состояния и использует матрицу переходов для характеристики частоты переходов между состояниями. Наблюдение является анормальным, если вероятность перехода, определенная предыдущим состоянием и матрицей перехода, очень мала. Модель применима в том случае, если рассматривается множество команд, последовательность которых важна [9].

Модель временных серий использует временные периоды вместе со счетчиками событий и измерениями ресурса, учитывает как значения наблюдений $x_1,...,x_n$, так и временные интервалы между ними. Новое наблюдение является анормальным, если вероятность его появления с учетом времени низка. Преимуществом данной модели является учет временного сдвига между событиями, а недостатком – накладные расходы по вычислению по сравнению с моделью среднего значения и среднеквадратичного отклонения [10].

Модуль фильтрации контента. Этот модуль является основой современных систем фильтрации разнообразного контента. Хотя данные системы и очень похожи на сигнатурные системы обнаружения вторжений, они имеют свои особенности, позволяющие выделить их в отдельный модуль. К таким особенностям относятся:

– проверка адресов Интернет-ресурсов;

– анализ текстов в передаваемом потоке на наличие запрещенного содержимого (по возможности, с извлечением текста из файлов разных форматов, таких, как Microsoft Word/Excel и т.п.);

– анализ типов передаваемых данных;

– проверка объема передаваемых данных/предоставление квот на загрузку;

– проверка присвоенной сайту категории;

– проверка сайта на соответствие определенному рейтингу;

– поддержка фильтрации HTTPS-трафика;

– модификация или замена передаваемых данных.

При фильтрации используются специализированные базы сигнатур. Для организации таких баз выдвигаются идентичные организационные требования, как и для баз сигнатур систем обнаружения вторжения [11].

Модуль обнаружения атак на основе анализа лог-файлов является одним из наиболее трудно реализуемых универсальных модулей. Главными причинами такой трудности является нестандартизированность форматов журналов регистрации разных операционных систем и разных сетевых устройств. Соответственно для анализа регистрационного файла любого сетевого объекта требуется наличие особенных баз сигнатур, написанных и обновляемых специально для этого объекта. Поэтому для полной функциональной реализации данного модуля необходимо сначала свести отчёты разных сетевых объектов к единому представлению и способу описания события [11].

Модуль обнаружения атак на основе проверки целостности файловой системы предназначен для сравнения фактических значений хеш-функций со значениями, находящимися во внешней базе данных эталонных функций. Минимальный набор требований, предъявляемых к данному модулю, включает:

– расширенный набор поддерживаемых хеш-алгоритмов;

– возможность настройки временных параметров проверки;

– возможность хранения базы данных хешей как на локальных носителях, так и на удалённых системах;

– настройку частоты обновления базы хешей.

При этом следует учитывать, что сами хеш-алгоритмы реализуются модулем управления хеш-функциями.

Модуль антивирусной защиты. Этот модуль реализует классический антивирус. Соответственно и требования к данному модулю совпадают с требованиями к обычному антивирусу. При этом нужно учитывать тот факт, что функция сканирования объекта является экспортируемой данным модулем и поэтому должна иметь специальный интерфейс [12].

3. Группа модулей криптографического обеспечения. Группа модулей криптографического обеспечения реализует все функции, связанные с криптографией, а также сопутствующие технологии, такие как хеширование, цифровая подпись, верификация подписанных данных, сообщений и т.д. В состав этой группы входят модули:

– поддержки VPN;

– шифрования симметричными ключами;

– шифрования не симметричными ключами;

– управления хеш-функциями;

– управления цифровыми сертификатами;

– утилизации данных криптографическими методами;

– управления защищёнными хранилищами.

Модуль поддержки VPN. Этот модуль служит для организации VPN-соединений между разными системами. Этим модулем должны поддерживаться следующие варианты построения VPN:

– Intranet VPN;

– Remote Access VPN;

– Client/Server VPN;

– Extranet VPN.

В качестве протоколов инкапсуляции должны поддерживаться:

– L2F;

– L2TP;

– MPLS;

– GRE;

– PPTP;

– IPSEC.

Соответственно должны поддерживаться разнообразные их возможные комбинации, а также инкапсуляция одного протокола в другой.

Модули шифрования симметричными и асимметричными ключами, а также модуль управления хеш-функциями, поддерживают максимальное количество алгоритмов, основанных на симметричных ключах шифрования. Для возможности добавления новых алгоритмов предусматривается контейнерная архитектура модулей.

Модуль управления цифровыми сертификатами. Этот модуль организовывает работу по управлению цифровыми сертификатами. К функциям данного модуля относятся:

– создание цифрового сертификата;

– удостоверение сертификата;

– валидация сертификата;

– поддержка разнообразных алгоритмов обмена сертификатов;

– управление сторонними сертификатами;

– уничтожение сертификата;

– отзыв сертификата.

При этом нужно учитывать, что сами сертификаты хранятся в защищённом хранилище, реализованном другим модулем.

Модуль утилизации данных криптографическими методами. Современные требования к защищённым системам требуют гарантированного уничтожения любой информации, подлежащей удалению [13]. При этом данные могут уничтожаться как в памяти компьютера, так и на разнообразных носителях.

Модуль управления защищёнными хранилищами предназначен для построения и управления защищенными хранилищами (криптоконтейнеры). К реализуемым функциям данного модуля относятся:

– создание криптоконтейнера;

– уничтожение криптоконтейнера;

– загрузка информации в криптоконтейнер;

– выгрузка информации из криптоконтейнера.

Функции разграничения доступа и управления доступом реализуются импортируемым модулем.

Многоуровневая формализация метода. Согласно теории иерархических систем, любой объект можно представить в виде детерминированного набора составных элементов с внутренними связями между ними: $M = A \bigcup B$, где M – результирующий объект; $A = \{a_0, a_1, ..., a_n\}$ – множество составных элементов объекта; $B = \{b_0, b_1, ..., b_n\} \subset C \bigcup D$ – множество связей между составными элементами объекта; $C = \{c_0, c_1, ..., c_n\}$ множество неизменяемых во времени связей; $D = \{d_0, d_1, ..., d_n\}$ – множество изменяемых во времени связей. При этом следует учитывать, что a_n, в свою очередь, является объектом, состоящим из детерминированного набора элементов и связей $a_n = A^{'} \bigcup B^{'}$ и $b_n = C' \bigcup D'$, где $M_n = A_n^k \bigcup B_n^k$, где n – индекс конкретной выборки из множества $0 < n < \infty$, k – индекс уровня иерархии $0 < k \le n$.

Объект защиты M имеет несколько вложенных уровней декомпозиции и наиболее низкий зависит от области применения и характера самой системы. Исходя из этого, любую информационную систему, подлежащую защите, можно представить в виде схемы, показанной на рис. 2.

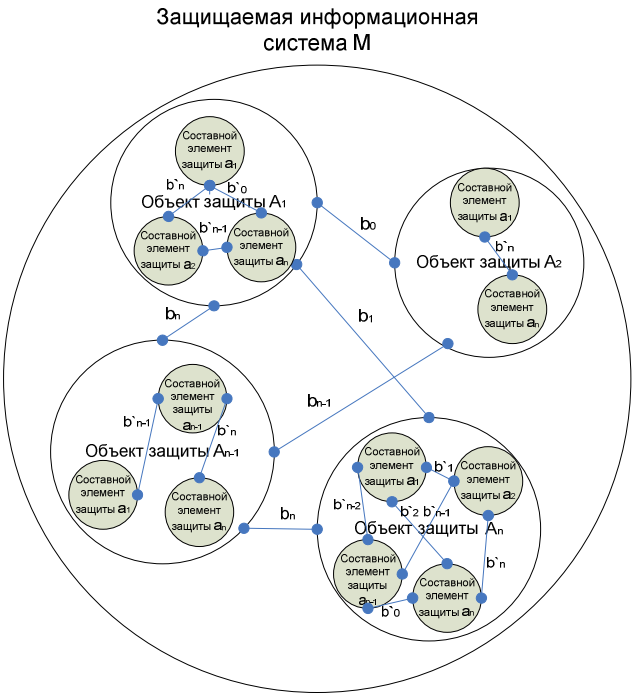

Рис. 2. Графическая интерпретация формальной модели

Любой элемент $a_n \in A$ обладает набором функций $f_n = \{f_n^1, f_n^2 ... f_n^n\}$, которые и определяют его как таковой. Набор элементов a_n конечен для конкретного уровня декомпозиции. И поэтому может быть использован для построения систем любой сложности, стоящих на более высоком уровне иерархии.

Для систем, применяемых в области защиты информации, минимально декомпозированным можно считать *объект, который модифицирует или верифицирует* каким-либо образом информацию на определённом уровне модели OSI. Результирующим объектом верхнего уровня иерархии является система, удовлетворяющая требованиям текущей политики безопасности организации. Особенностью такой организации является изменяемость результирующей информационной системы, включающей объекты типа M защиты сетевого периметра во времени и пространстве, но при этом неизменным является исходный набор составных элементов защиты a_n.

При этом полученная цепочка иерархии объектов реализует принцип эшелонированной защиты, которая характеризируется защитой, циркулируемой в информационной системе информации на всех уровнях модели OSI. А объединение объектов защиты A_n с помощью связей B_n реализует профиль защиты информационной системы на базе объектов M_n. Для систем, обеспечивающих сетевую безопасность, обрабатываемая информация должна относиться к 2 – 7 уровню этой модели.

Представленная формализованная модель позволяет синтезировать различные профили систем защиты сетевого периметра на основе рекуррентных процедур, минимизирующих на каждом уровне иерархии типы объектов защиты. Тем самым достигается возможность унифицировать уровневые объекты защиты и обеспечивать функциональные полноты группы модулей.

5. Реализация технологии

Для разработки имитационной модели предлагаемой системы используется среда для дискретного моделирования OMNET++ [14]. OMNeT++ разработана с использованием следующего подхода: языковая среда, "упрятанная" в гибридной оболочке из быстроисполняемых низкоуровневых конструкций и "медленного" интерпретирующего графического интерфейса. В OMNeT++ основным примитивом является модуль, принципиально способный "общаться" с другими модулями. Модули OMNeT++ могут группироваться, образовывая макромодули, могут соединяться между собой. Реализация модуля – сопрограмма, написанная на языке C++ и использующая специальную библиотеку, поддерживающую псевдопараллельное исполнение модулей.

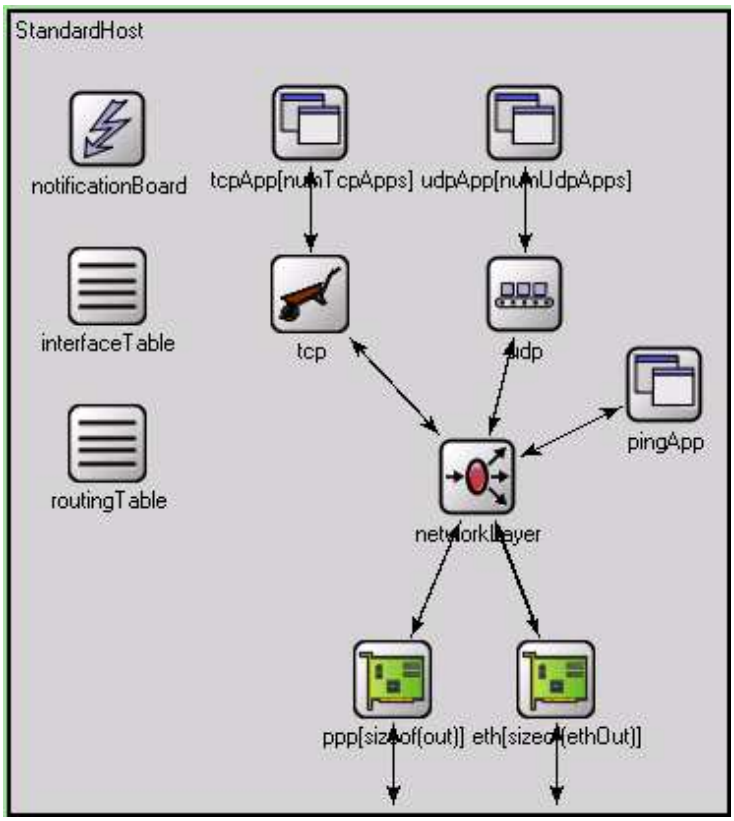

Рис. 3. Графическое представление модели хоста

Иерархический характер модели OMNeT++ обеспечивается не только вложенностью модулей, но и понятиями "портов" (gates) и связей. Порты-интерфейсы модулей, обеспечивающие взаимодействие элементов модели, и связи между портами описываются на одном уровне иерархии. Фактически это означает возможность построения и повторного использования макромоделей из уже существующих моделей. Такая особенность, дополненная открытым характером модульной модели (пользователь OMNeT++ всегда может расширить набор модулей собственными низкоуровневыми реализациями) и исполняемым принципом, позволяет применять OMNeT++ для моделирования действительно

больших и сложных систем [15]. Кроме того, модули-сопрограммы OMNeT++ основаны на так называемых "нитях" (threads), что обеспечивает адекватный прирост производительности на мультипроцессорных машинах.

В основе всей программной конструкции лежит высокоуровневый специализированный язык NED. Это язык описания топологии модели (или проще – язык описания соединения модулей). Процесс написания NED-программ происходит за удобным графическим интерфейсом, с помощью которого пользователь оперирует графическим представлением модулей (пиктограммами) и их иерархий, а NED-программы генерируются автоматически. OMNeT++ – модель позволяет оценить и поведение будущей системы в худших случаях, и ее статистические характеристики.

Вышеописанная среда была принята для разработки предлагаемой технологии интеграции средств защиты сетевого периметра. Для моделирования функционирования сетевой среды применяется стандартный модуль INET framework. Этот модуль полностью моделирует стек протокола TCP/IP и поэтому не нуждается в дополнительной доработке. В данном модуле хост представляется в виде следующей графически интерпретированной модели (рис. 3).

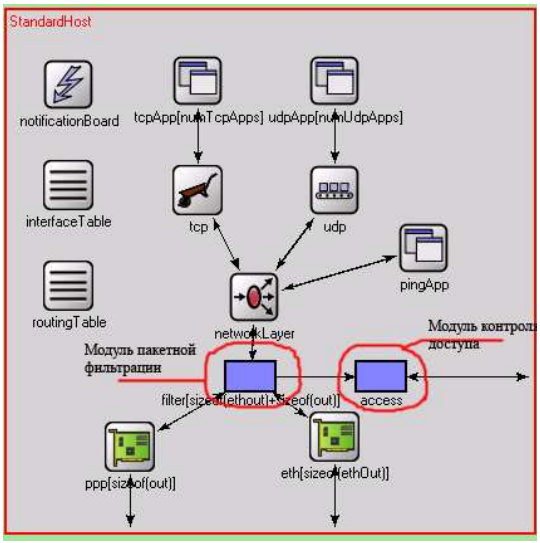

Рис. 4. Модель с интегрированными модулями защиты

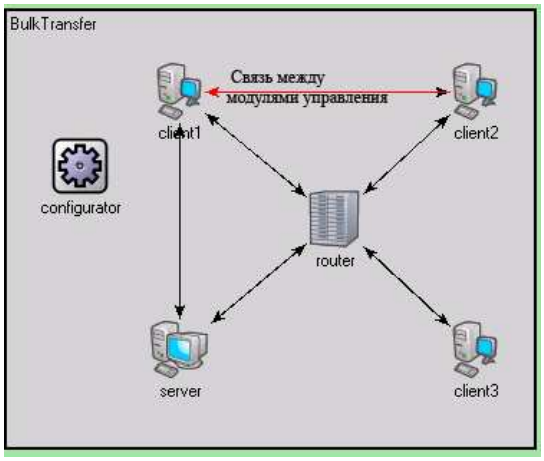

Рис. 5. Организация сети управления модулями

В этой модели приложения, выполняемые на компьютере, представлены в виде седьмого уровня модели OSI. Соответственно моделирование приложений, выполняемых на хостах, сводится к заданию специфических параметров для приложений. К этим параметрам относятся IP-адрес назначения, порт источника, порт адресата и специфический протокол взаимодействия данных приложений. При разработке предлагаемой модели защиты сетевого периметра каждый разрабатываемый модуль из группы модулей управления информационными потоками интегрируется в определённый уровень модели OSI. Примером такой интеграции служит модель, отдельно представленная на рис. 4. Здесь на сетевой уровень интегрируется модуль пакетной фильтрации. Он абсолютно прозрачный для выше и ниже лежащих уровней и реализует полный набор функций пакетной фильтрации. Управление этим модулем производится модулем контроля доступа.

Следует отметить, что группа модулей контроля доступа и управления информационной средой не принадлежит какому-то определённому уровню и взаимодействует только с другими модулями. Модули управления могут создавать сети

управления для объединения нескольких разрозненных модулей, расположенных на хостах, в единую систему защиты сетевого периметра. Такая конфигурация представлена на рис. 5.

6. Заключение

Предложенные технология и методы создания современных средств защиты сетевого периметра на базе типизации и унификации уровневых объектов обеспечивают функциональную полноту для реализации конкретных профилей безопасности информационных ресурсов в корпоративных информационных системах. При этом достигается возможность синтеза базовых объектов защиты информации на различных уровнях семиуровневой модели взаимодействия открытых систем с возможностью интеграции для реализации требуемой политики защиты сетевого периметра от внешних и внутренних угроз. Подобная технология унификации гарантирует возможность минимизации сетевого трафика служебной и управляющей информации.

СПИСОК ЛИТЕРАТУРЫ

1. Описание межсетевых экранов CISCO. – http://www.cisco.com.
2. Описание межсетевых экранов Check Point Firewall-1. – http:// www.checkpoint.com.
3. Алишов Н.И. Распределенная система организации безопасности информационных ресурсов // Труды IV-й Международной научно-практической конференции ”Современные информационные и электронные технологии”. – Одесса, 2003. – С.123.
4. Норткатт С., Зелстер Л., Винтерс С. и др. Защита сетевого периметра: Пер. с англ. – К.: «ООО ТИД ДС», 2004. – 672 с.
5. Описание IDS “Snort”. – http://www.snort.org.
6. Biswanath Mukherjee, Todd Heberlein L. and Levitt Karl N. Network intrusion detection // IEEE Network. – 1994. – N 8(3). – P. 26–41.
7. Bace R., Mell P. Special Publication on Intrusion Detection Systems, Tech. Report SP 800-31. – Gaithersburg: National Institute of Standards and Technology. – 2001. – November. – P. 54– 63.
8. Advanced Authentication Technology: CSL Bulletin.- National Institute of Standards and Technology. – 1991. – November. – 15 p.
9. Бусленко Н.П. Моделирование систем. – М.: Наука, 1978. – 400 с.
10. Снапелев Ю.М., Старосельский В.А. Моделирование и управление в сложных системах. – М.: Советское радио, 1974. – 354 с.
11. Stephen Northcutt.IDS Signatures and Analysis, Parts 1 & 2. – Baltimore, Maryland: SANS, 2001.– May. – 459 p.
12. Описание и сравнительный анализ современных антивирусов. – http://www.virusbtn.com.
13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – 1999. – 59 с.
14. Описание, документация, исходники системы дискретного моделирования OMNET++. – http://www.omnetpp.org.
15. Котенко И.В. Многоагентные модели противоборства злоумышленников и систем защиты в сети Интернет // Третья Общероссийская конференция «Математика и безопасность информационных технологий» (МаБИТ-04). – М.: МГУ, 2004. – 234 с.