Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.738.5:004.056.5

На правах рукописи

Игнатович
Юрий Борисович

МЕТОДЫ И СРЕДСТВА АДАПТАЦИИ ПОЛИТИКИ МАРШРУТИЗАЦИИ СЕТЕВОГО ТРАФИКА К ТРЕБОВАНИЯМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-38 80 04 Технология приборостроения

Минск 2019

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **КУНКЕВИЧ Дмитрий Петрович,**
кандидат технических наук, доцент кафедры «Системы автоматизированного проектирования» учреждения образования «Белорусский национальный технический университет»

Рецензент: **РУДИКОВА Лада Владимировна,**
кандидат физико-математических наук, доцент, заведующая кафедрой технологий программирования учреждения образования «Гродненский государственный университет имени Янки Купалы»

Защита диссертации состоится «26» июня 2019 г. года в $9^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Современный мир характеризуется высокими темпами научно-технического прогресса, глобальной автоматизацией и информатизацией человеческой деятельности, повсеместным использованием электронно-вычислительных машин, разнообразных организационно-технических и человеко-машинных систем, применяемых для всестороннего обеспечения существования человеческой цивилизации. Важнейшим классом таких систем являются автоматизированные системы различного назначения, в которых сбор, хранение и обработка данных осуществляется средствами автоматизации и вычислительной техники.

Создание автоматизированных систем и информационно-вычислительных сетей привело к формированию в рамках мировой цивилизации единого международного информационного пространства. Анализ примеров и последствия нарушений безопасности в различных автоматизированных системах, в том числе и критического назначения, позволяет сделать вывод о том, что на фоне стремительного развития информационных технологий наблюдается кризис обеспечения безопасности информации, и об особой роли информационной безопасности в жизни человеческого общества.

Таким образом, можно сделать следующий вывод: большинство нарушений в области информационной безопасности в сетях не могут контролироваться только средствами защиты на основе разграничения и контроля доступа (межсетевые экраны, фильтры, системы разграничения доступа и т.д.), независимо от того, происходят нарушения из-за наличия ошибок в сетевом программном обеспечении или ошибок в настройках системы защиты. Использование информационной сети, подключенной к сети общего доступа, является типовым решением и задача ее защиты – наиболее актуальной среди прочих задач сетевой безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Развитие информационных технологий ставит актуальные задачи повышения надежности функционирования компьютерных сетей. Для решения таких задач необходимы исследования существующих сетевых протоколов, сетевых архитектур, разработка способов повышения безопасности при передаче информационных ресурсов по сети.

Одним из перспективных подходов к построению систем сетевой защиты является адаптация политики динамической маршрутизации сетевого трафика к требованиям по информационной безопасности, который, в отличии от традиционных методов сетевой защиты, позволяет реализовать концепцию упреждающей защиты на основе управления потоками трафика. Сложность современных топологий распределенных сетей передачи данных не позволяет

решать такие задачи методом простого перебора возможных вариантов решения. Поэтому необходимо создание специальных моделей, алгоритмов и методик для автоматизированного решения подобных задач, из чего можно сделать вывод, что разработка методов и методик управления потоками трафика в сети передачи данных при помощи средств динамической маршрутизации на основе требований по информационной безопасности является актуальной.

Степень разработанности проблемы

В настоящее время в учреждении образования Белорусский государственный университет информатики и радиоэлектроники существует единая информационно-вычислительная сеть передачи данных. Для того чтобы любая компьютерная сеть эффективно работала, необходимо использовать одинаковую форму представления информации и использовать политики маршрутизации сетевого трафика. Поэтому существует необходимость разработки основных методов и политик маршрутизации сетевого трафика для обеспечения безопасной передачи данных по компьютерной сети университета.

Цель и задачи исследования

Целью диссертации является повышение безопасности информационно-вычислительных сетей, разработка метода и методики построения адаптируемой политики маршрутизации сетевого трафика для повышения эффективности функционирования корпоративных вычислительных сетей при частичных изменениях структуры сети, возникающих из-за изменения нагрузки и реальной пропускной способности каналов связи и коммутационного оборудования.

Для достижения поставленных целей необходимо было решить **следующие задачи**:

1. Провести обзор и анализ существующих подходов защиты компьютерной сети применяемых в корпоративных вычислительных сетях, для выявления достоинств и области их применения.
2. Проанализировать протоколы для обеспечения безопасной передачи данных по информационной вычислительным сетям.
3. Спроектировать автоматизированную систему управления потоками сетевого трафика с использованием proxy сервера UserGate.

Объектом исследования является сеть передачи данных, построенная на основе маршрутизации третьего уровня модели взаимодействия открытых сетей ISO/OSI.

Предметом исследования выступает безопасность каналов доступа к информации в сети передачи данных в зависимости от структурной схемы потоков трафика и характеристик маршрутов передачи данных.

Область исследования. Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 «Технология приборостроения».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области методов и средств защиты компьютерной сети, политик сетевой безопасности, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в разработке методов и средств адаптации политики маршрутизации сетевого трафика к требованиям по информационной безопасности.

Теоретическая значимость работы заключается в детальном анализе политик и протоколов, используемые для безопасной передачи данных по информационно-вычислительным сетям.

Практическая значимость диссертации состоит в подготовке автоматизированной системе управления потоками сетевого трафика, которая позволит оптимизировать и увеличить безопасность компьютерной сети.

Основные положения, выносимые на защиту

1. Методика оценки защищенности каналов доступа в распределенной сети передачи данных на основе требований по информационной безопасности.
2. Метод и алгоритмы построения адаптируемой политики сетевой безопасности, определенных на базе требований по сетевой безопасности.
3. Система управления потоками сетевого трафика с использованием proxy сервера UserGate.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 55-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Беларусь, 2019 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 5 печатных работах и опубликованы в сборниках материалов научных конференций.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен анализ современных угроз информационной безопасности в сетях передачи данных и рассмотрена современные архитектуры систем защиты корпоративных сетей. Изучены более подробно политики сетевой безопасности на примере учреждения образования Белорусских государственный университет информатики и радиоэлектроники.

Во второй главе рассмотрены протоколы для обеспечения безопасной передачи данных по информационно-вычислительным сетям. Произведен анализ сетевого протокола IPsec, в результате чего выявлены достоинства и область применения протокола.

В третьей главе рассмотрены основные требования к автоматизированной системе и приведена инфраструктура proxy сервера, а также составлена подробная инструкция по настройке сервера на примере UserGate.

В приложении представлены публикации автора.

Общий объем диссертационной работы составляет 105 страницы. Из них 73 страниц основного текста, 31 иллюстрация на 26 страницах, 3 таблицы на 3 страницах, библиографический список из 50 наименований на 4 страницах, список собственных публикаций соискателя из 5 наименований на 1 странице, 4 приложений на 28 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы компьютерных сетей, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы. Обоснована и сформулирована задача разработки автоматизированных средств и методов построения политики маршрутизации сетевого трафика с учетом требований по информационной безопасности.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе приведен анализ современных угроз информационной безопасности в сетях передачи данных и рассмотрены политики сетевой безопасности на основе управления потоками трафика. Рассмотрены и проанализированы основные подходы к построению защищенных информационных сетей, проведен анализ основных этапов реализации информационных угроз в сетях, выявлены недостатки существующих методов

и средств обеспечения сетевой безопасности. На основе проведенного анализа сформулирована задача автоматизированного построения политики маршрутизации с учетом требований по сетевой безопасности. Анализ тенденций правонарушений с использованием компьютерных сетей как средства доступа к информации, позволяет сделать выводы о постоянном росте количества преступлений, совершаемых при помощи сетей.

Подробно рассмотрены и описаны этапы развития сетевой атаки:

– Поиск точек входа в корпоративную сеть: на данном этапе злоумышленник определяет потенциально-уязвимые точки доступа к информационной сети.

– Поиск уязвимостей в системе безопасности найденных точек доступа: на этом этапе злоумышленник определяет, какие уязвимости в найденных точках могут быть использованы для проведения атаки.

– Использование найденных уязвимостей для взлома системы защиты точек доступа: на данном этапе злоумышленник взламывает систему защиты, используя найденные уязвимости.

– Сканирование внутренней корпоративной сети, поиск в ней нужной информации: На этом этапе злоумышленник определяет местоположение интересующей его информации во внутренней сети корпорации.

– Взлом внутренней системы защиты: на данной стадии нарушитель, используя уязвимости внутренней системы защиты, получает доступ к интересующей его информации.

– Работа с интересующей информацией: на данной ' стадии злоумышленник обрабатывает ценную информацию в зависимости от цели атаки (копирует ее на удаленный носитель, удаляет, искажает и т.п.).

– Сокрытие следов преступления: на этом этапе злоумышленник уничтожает следы своего присутствия в системе.

На основе анализа выявлены принципиальные недостатки средств и методов сетевой защиты, не позволяющие эффективно противодействовать сетевым информационным угрозам. Показано, что современные системы защиты, построенные по принципу установки информационных «барьеров» разного типа на пути доступа к информации, не способны отразить атаки, эксплуатирующие уязвимости и ошибки в настройках программного обеспечения.

Как решение вышеозначенных проблем, предлагается упреждающая стратегия защиты сети на основе построения политики маршрутизации сетевого трафика с учетом требований по информационной безопасности. Методика построения политики управления трафиком позволяет предотвратить развитие сетевых атак, эксплуатирующих уязвимости открытых информационных сервисов. Схема потоков сетевого трафика строится таким образом, что потенциально уязвимые информационные сервисы становятся недоступны злоумышленникам через сеть.

Во второй главе рассмотрены основные протоколы защиты информационной-вычислительной сети.

В качестве средства обеспечения безопасного сетевого взаимодействия рабочих станций в составе субоперационной системы защиты может быть использован протокол IPsec. Протокол IPsec обеспечивает защиту всего трафика рабочей станции, имеет собственную политику безопасности и обладает широкими возможностями по настройке в зависимости от специфики вычислительной системы - то есть отвечает всем требованиям, предъявляемым к системе обеспечения безопасного взаимодействия рабочих станций по открытым информационно-вычислительным сетям.

Для внедрения протокола IPsec в состав субоперационной системы защиты в стек сетевых протоколов операционных систем должны быть включены модули перехвата сетевого трафика, передающие его на обработку протоколу IPsec. В операционных системах семейства Windows данная задача может быть решена посредством реализации дополнительного сетевого модуля спецификации NDIS.

В ходе решения задачи обеспечения безопасного взаимодействия рабочих станций по открытым информационно-вычислительным сетям были исследованы современные протоколы сетевой безопасности и средства установления защищенных информационных каналов между рабочими станциями. Наиболее эффективными протоколами сетевой безопасности, ставшими общепринятыми стандартами, являются протоколы SSL (Secure Socket Layer) и его развитие TLS (Transport Layer Security), обеспечивающие безопасность на транспортном уровне, и протокол IPsec (IP Security Protocol), обеспечивающий безопасность на сетевом уровне архитектуры TCP/IP, применяющейся для обеспечения сетевого взаимодействия рабочих станций.

Для построения защищенного канала передачи данных на канальном уровне в университете используют различные протоколы. Одним из которых является PPTP (Point to Point Tunneling Protocol). Протокол PPTP позволяет инкапсулировать пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и Интернет). PTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу университета путем создания в сети TCP/IP частной виртуальной сети.

MS-CHAPv2 обеспечивает двустороннюю проверку подлинности, называемую также взаимной проверкой подлинности. Пользователь удаленного доступа получает подтверждение, что сервер удаленного доступа, к которому он пытается подключиться, имеет доступ к паролю пользователя. Ключ шифрования всегда основан на пароле пользователя и произвольной строке запроса. Каждый раз, когда пользователь подключается с одним и тем же паролем, создаются разные ключи шифрования. При использовании протокола MS-CHAP v2 создаются отдельные ключи шифрования для приёма и передачи данных.

IPsec обеспечивает аутентификацию абонентов и управление удаленным доступом, аутентификацию, конфиденциальность и целостность данных, защиту от анализа и воспроизведения трафика. IPsec может быть применен для создания сквозных защищенных каналов между произвольными IP-хостами

и/или группами хостов (т.н. транспортный режим), защищенных каналов между шлюзами отдельных подсетей (туннельный режим) и виртуальных закрытых сетей (Virtual Private Network, VPN), обеспечивающих безопасность и конфиденциальность взаимодействия отдельных фрагментов или подсетей территориально распределенной VPN, связанных между собой не напрямую, а через другие сети.

Архитектура и спецификации протокола IPsec описаны в документах тематической группы IETF по безопасности IP. Основными составляющими IPsec, согласно, являются протокол аутентификации AH (Authentication Header) и протокол инкапсулирующей защиты данных ESP (Encapsulating Security Payload). Эти протоколы составляют так сказать «видимую», интерфейсную часть IPsec.

Для внедрения протокола IPsec в состав субоперационной системы защиты в стек сетевых протоколов операционных систем должны быть включены модули перехвата сетевого трафика, передающие его на обработку протоколу IPsec.

В третьей главе рассматриваются основные требования к автоматизированная система управления потоками сетевого трафика.

Построение политики управления трафиком с учетом требований по информационной безопасности при условии существенных масштабов сети затруднительно без определенной автоматизации процесса. Если корпоративная сеть насчитывает несколько десятков сетевых узлов, участвующих в процессе обработки защищаемой информации, то задача оценки безопасности и построения политики маршрутизации такой сети без помощи некоторой автоматизированной системы становится очень трудоемкой. Поэтому возникает практическая задача реализации системы, позволяющей на основе требований по сетевой безопасности автоматически строить политику маршрутизации.

Одним из основных требований к автоматизированной системе построения политики маршрутизации является требование по скорости обработки данных в системе и скорости применения сгенерированной политики в рамках одного домена маршрутизации.

Еще одним важным требованием к системам управления трафиком является требование масштабируемости системы в рамках распределенной сетевой среды. Во избежание не надежных архитектурных решений, когда существует единая точка сбоя в общем административном центре, предполагается распределение функциональной нагрузки на ряд независимых подсистем.

Большинство компьютеров в университете подключены в сеть по технологии Ethernet со скоростью доступа 1 Гбит/с. Доступ в Интернет осуществляется через прокси: proxy1.bsuir.by, порт 8080, разрешен для сотрудников и студентов или proxy2.bsuir.by для работников ректората, порт 8080 и требует специального разрешения. Основной работой proxy-сервера является предоставление защищенного доступ в сеть интернет, информация, проходящая через него, сжимается на сервере, приводя к экономии трафика, а

также скрывает IP-адрес компьютера пользователя, обеспечивая анонимность в сети.

Зачастую Proxy сервер выполняет несколько функций одновременно, к примеру, Proxy сервер может предоставлять возможности кеширования и аутентификации в дополнение к основной функции обеспечения сетевого посредничества для приложений. Однако более правильно трактовать различные возможности Proxy сервера как отдельные типы Proxy серверов. На сегодня можно классифицировать следующие типы proxy серверов:

– пересылающий Proxy сервер (forward proxies);
– прозрачный Proxy сервер (transparent proxies);
– кэширующий Proxy сервер (caching proxies);
– proxy сервер обеспечения безопасности (security proxies);
– обратный Proxy сервер (reverse proxies).

Proxy – сервер UserGate – это полнофункциональное решение, позволяющее администратору организовать работу пользователей локальной сети в Интернет, а также централизованно управлять Интернет-подключениями с помощью гибкой системы правил. Позволяет осуществлять кэширование сетевых ресурсов, имеет встроенную биллинговую систему, а также систему статистики. С помощью гибкой системы правил администратор сети может блокировать доступ пользователей к определенным ресурсам, регулировать скорость соединения, задавать расписание работы различных пользователей. Программа предоставляет возможность детального мониторинга активных Интернет – сессий пользователя в реальном времени – IP адрес, имя пользователя, точное количество переданного и полученного трафика, а также посещенные URL.

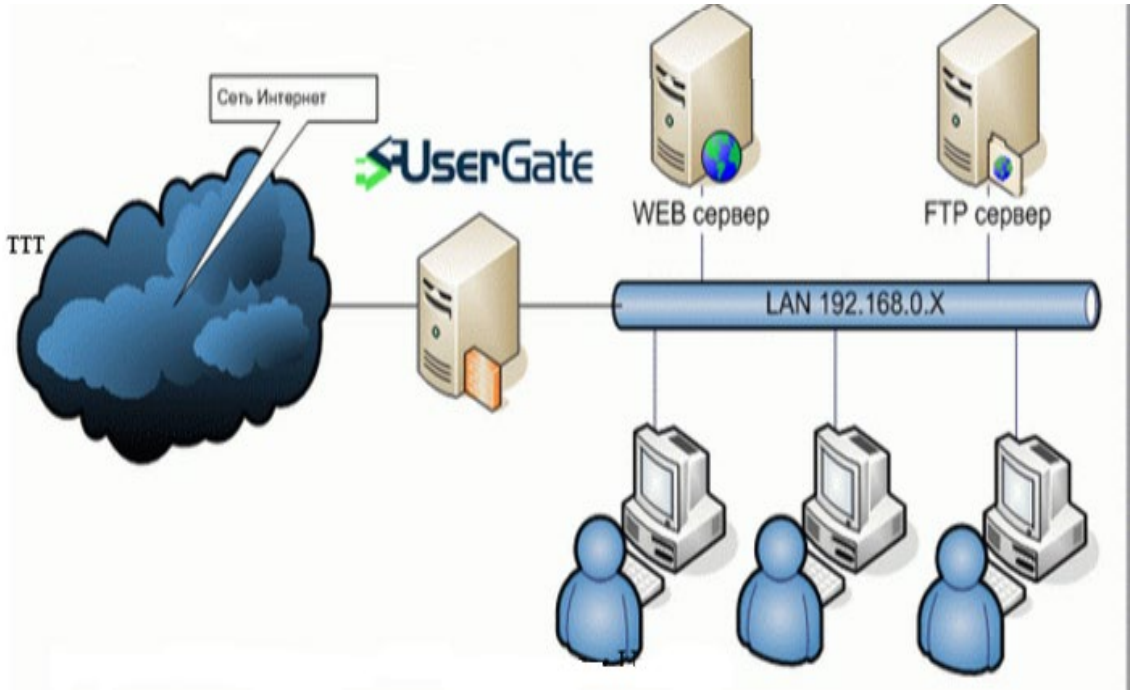

Рисунок 1 – Пример сети с Proxy сервером UserGate

UserGate это Proxy сервер, ориентированный на работу под управлением операционной системы Windows. Компьютер с установленным UserGate должен прямой доступ в сеть Интернет. Остальные компьютеры пользователей должны иметь связь с сервером UserGate (быть в одном адресном пространстве).

Рисунок 2 – Укрупненная схема компьютерной сети БГУИР

В состав UserGate входит модуль статистики, позволяющий составлять различные статистические о т четы. В числе других особенностей программы – различные методы авторизации пользователей; фильтры URL, позволяющие запретить доступ к нежелательным ресурсам; назначение портов для переадресации трафика с одного порта на другой; публикация ресурсов (доступ к внутренним ресурсам сети из Интернета); встроенный файервол; кэширование HTTP ресурсов; автодозвон до провайдера; возможность удаленного администрирования.

UserGate состоит из нескольких модулей:

– UserGate Server – непосредственно сам сервер. Он устанавливается на компьютере, напрямую подключенном к Интернету. Сервер реализует доступ пользователей в Интернет, осуществляет подсчет трафика, ведет статистику работы, осуществляет антивирусную проверку и т. п.

– UserGate Administrator – модуль предназначен для администрирования системы. С его помощью можно осуществить настройку функций Proxy-сервера. Данный модуль не обязательно должен размещаться на сервере, возможно удаленное управление UserGate;

– UserGate Statistics – предназначен для просмотра статистики использования Интернета и построения отчетов на ее основе;

– UGClient – предназначен для обеспечения возможности авторизации пользователей через Active Directory.

Кроме выше рассмотренных возможностей Proxy сервер UserGate предоставляет возможность кеширования трафика. Кроме того данный сервер имеет встроенный модуль файервола и модуль трансляции сетевых адресов, чтопозволяет гибко настраивать различные политики безопасности для различных пользователей, групп пользователей и ресурсов. Также в данном сервере реализованавозможность проверки трафика внешним антивирусом.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведенный анализ современного уровня развития технологий обеспечения сетевой безопасности показал, что традиционные методы обеспечения сетевой безопасности не всегда эффективно справляются с поставленными задачами. Одним из перспективных направлений развития средств и методов сетевой защиты является разработка систем сетевой безопасности на основе управления потоками трафика. Поэтому задача создания методических, алгоритмических и программных средств для управления потоками сетевого трафика является актуальной.
2. Описаны общие принципы и структурная схема построения политики маршрутизации сетевого трафика в распределенной сети.
3. В результате разработан набор требований к реализации автоматизированной системы построения политик маршрутизации на основе требований по информационной безопасности. Определены структурные требования к такой системе, требования к программному обеспечению и средствам реализации данной системы.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирвоания информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Компьютерные сети в электронных системах безопасности».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых журналах

1. Протоколы защиты компьютерных сетей на базе учреждения образования Белорусский государственный университет информатики и радиоэлектроники / Игнатович Ю.Б., Игнатович Р.О., Марков А.Н., Мигалевич С.А // Электронный научный журнал «Вестник современных исследований».

– Омск: Научный центр «Орка», выпуск №3-18 от 27 марта 2019 с.39 ISSN 2541-8300.

2. Организация политики сетевой информационной безопасности в учреждении образования на примере Белорусского государственного университета информатики и радиоэлектроники / Игнатович Ю.Б., Игнатович Р.О., Марков А.Н., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка», выпуск №12-10 от 19 декабря 2018 с.187 ISSN 2541-8300.

3. Проблемы интеграции облачных вычислений в учебный процесс / Игнатович Р.О., Игнатович Ю.Б., Марков А.Н., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка», выпуск №12-10 от 19 декабря 2018 с.185 ISSN 2541-8300.

Тезисы конференций

4. Выбор протокола маршрутизации сетевого трафика / Игнатович Ю. Б., Игнатович Р. О., Марков А. Н., Мигалевич С. А. // Центр молодежных инноваций «Минский городской технопарк» – Минск: 2018, с.69.

5. Игнатович Ю.Б., Игольник А.А. «Адаптация политики маршрутизации сетевого трафика». // материалы 55−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 22-26 апреля 2019 г. / УО «БГУИР». – Минск, 2019.

РЭЗЮМЭ

Ігнатовіч Юрый Барысавіч

Метады і сродкі адаптацыі палітыкі маршрутызацыі сеткавага трафіку да патрабаванняў па інфармацыйнай бяспекі

Ключавыя словы: кампутарная сетка, палітыкі маршрутызацыі, пратакол.

Мэта працы: Мэтай дысертацыі з'яўляецца павышэнне бяспекі інфармацыйна-вылічальных сетак, распрацоўка метаду і методыкі пабудовы адаптуецца палітыкі маршрутызацыі сеткавага трафіку для павышэння эфектыўнасці функцыянавання карпаратыўных вылічальных сетак пры частковых зменах структуры сеткі, якія ўзнікаюць з-за змены нагрузкі і рэальнай прапускной здольнасці каналаў сувязі і камутацыйнага абсталявання.

Атрыманыя вынікі і іх навізна: прапанаваныя ў диссерта-цыі метад і методыка пабудовы палітыкі маршрутызацыі з'яўляецца вос-новай для пабудовы аўтаматызаваных сістэм кіравання патокамі сеткавага трафіку на базе патрабаванняў па інфармацыйнай бяспекі. Значнасць атрыманых вынікаў работы заключаецца ў распрацоўцы метадаў і сродкаў адаптацыі палітыкі маршрутызацыі сеткавага трафіку да патрабаванняў па інфармацыйнай бяспекі.

Мадэль і метад кіравання струменямі трафіку, прапанаваныя ў ра-боце, ўяўляюць сабой тэарэтычную і метадычную базу пры проектировании тапалогіі абароненых сетак перадачы дадзеных і распрацоўцы палітыкі маршрутызацыі сеткавага трафіку.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» у навучальны курс «Кампутарныя сеткі ў электронных сістэмах бяспекі».

Вобласць ужывання: паўправадніковая прамысловасць, микропро-цессорные сістэмы.

РЕЗЮМЕ

Игнатович Юрий Борисович

Методы и средства адаптации политики маршрутизации сетевого трафика к требованиям по информационной безопасности

***Ключевые слова*:** компьютерная сеть, политики маршрутизации, протокол.

***Цель работы*:** Целью диссертации является повышение безопасности информационно-вычислительных сетей, разработка метода и методики построения адаптируемой политики маршрутизации сетевого трафика для повышения эффективности функционирования корпоративных вычислительных сетей при частичных изменениях структуры сети, возникающих из-за изменения нагрузки и реальной пропускной способности каналов связи и коммутационного оборудования.

***Полученные результаты и их новизна*:** предложенные в диссертации метод и методика построения политики маршрутизации является основой для построения автоматизированных систем управления потоками сетевого трафика на базе требований по информационной безопасности. Значимость полученных результатов работы заключается в разработке методов и средств адаптации политики маршрутизации сетевого трафика к требованиям по информационной безопасности.

Модель и метод управления потоками трафика, предложенные в работе, представляют собой теоретическую и методическую базу при проектировании топологии защищенных сетей передачи данных и разработке политики маршрутизации сетевого трафика.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Компьютерные сети в электронных системах безопасности».

***Область применения*:** компьютерные сети предприятий.

SUMMARY

Ignatovich Yury Borisovich

Methods and means of adapting the routing policy of network traffic to information security requirements

***Keywords*:** computer network, routing policies, protocol.

***The object of study*:** The purpose of the thesis is to improve the security of information and computer networks, to develop a method and methodology for constructing an adaptable policy for routing network traffic to improve the efficiency of corporate computer networks with partial changes in the network structure arising from changes in load and actual throughput of communication channels and switching equipment.

***The results and novelty*:** the method and methodology of building a routing policy proposed in the thesis is the basis for building automated systems for managing network traffic flows based on information security requirements. The significance of the results obtained is the development of methods and means of adapting the routing policy of network traffic to information security requirements.

The model and method for managing traffic flows, proposed in the paper, provide a theoretical and methodological basis for designing a topology of secure data networks and developing a policy for routing network traffic.

***Degree of use*:** the results were introduced into the educational process at the department of design of information and computer systems of the educational institution "Belarusian State University of Informatics and Radioelectronics" in the training course "Computer networks in electronic security systems".

Sphere of application: computer networks of enterprises.