ОТЗЫВ

официального оппонента на диссертацию

Новикова Сергея Николаевича

МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕТЕВОГО УРОВНЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

представленную на соискание ученой степени доктора технических наук по специальности 05.13.19 – «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи»

1. *Актуальность избранной темы.*

До недавнего времени услуги передачи информации строились на различных технологиях коммутации. Т.е., создавались отдельные сети, оплачивалась аренда каналов связи и для каждой сети могли использоваться свои организационно-технические методы защиты конфиденциальной информации. Развитие Интернет привело к новым технологическим и программным решениям в области передачи информации, на базе которых развиваются *мультисервисные сети связи* (МСС). Сеть ММС является единой телекоммуникационной структурой, способной одновременно передавать разнородную информацию (электронные документы, e-mail, речь, видео/мультимедиа), обеспечивая при этом заказанный пользователем объем и качество услуг (QoS). Мультисервисные сети базируются на Интернет технологиях, включающих в себя протокол IP и технологию MPLS. Принципиально важно отметить высокие риски, связанные с переводом телекоммуникационной индустрии на достаточно уязвимый протокол IP и разнородные среды доступа. Следовательно, вопросам, связанным с безопасностью МСС следует уделять пристальное внимание, поскольку здесь потенциальные нарушители получают новые возможности для мошенничества по сравнению, например, с обычными телефонными или IP сетями. Поэтому совершенствование научно-методологического аппарата защиты информации в МСС является актуальной задачей.

2. *Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации.*

Диссертационная работа Новикова С.Н. посвящена созданию методологической основы, алгоритмов и технологий для защиты конфиденциальности, целостности и доступности информации с использованием технологий сетевого уровня МСС.

В главе 1 выполнен анализ современного состояния обеспечения конфиденциальности, целостности и доступности информации в МСС. Выявлены проблемы применения традиционных подходов к защите информации в МСС, связанные с увеличением времени задержки передачи информации. Показано, что технологически эти проблемы можно решить за счет привлечения криптографических, канальных и других ресурсов мультисервисной сети связи по заявке пользователей на передачу защищенной информации.

В главе 2 исследуется многократное асимметричное шифрование и разрабатывается метод обеспечения целостности информации на сетевом уровне. Получена теоретическая оценка вероятности целостности информации, которая подтверждается результатами имитационного моделирования. Разработан критерий выбора ресурсов мультисервисных сетей связи для обеспечения целостности и доступности информации. Показано, что процедуры, участвующие в мониторинге инфраструктуры мультисервисной сети связи при выборе оптимального маршрута и установлении соединений, позволяют обеспечить не только должный уровень качества предоставляемого сервиса, но и требуемый уровень информационной безопасности.

В главе 3 разрабатываются методы маршрутизации в МСС. Автор представляет обобщенную функциональную модель маршрутизации в мультисервисных сетях связи и классификацию методов маршрутизации: «Локально-волновой» и «Гибридный» методы маршрутизации.

В главе 4 разрабатываются модели маршрутизации в мультисервисной сети связи в условиях внешних деструктивных воздействий. Поскольку для IP сетей маршрутизация является ключевой технологией, то здесь используется весь спектр методов выбора оптимального пути - начиная с теории графов и заканчивая сетями Петри и технологиями искусственного интеллекта. Автором предложена математическая модель оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов, модель для исследования маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи, а также методика определения плана распределения информации на однородной ячеистой сети связи большой размерности.

В главе 5 приводится анализ результатов моделирования технологий маршрутизации в условиях внешних деструктивных воздействий на элементы мультисервисной сети связи. При этом под деструктивными воздействиями понимается выход из строя маршрутизаторов. С помощью эмулятора строятся модели сетей для анализа различных технологий маршрутизации с учетом деструктивных воздействий.

В главе 6 приведены авторские методики защиты информации за счет привлечения территориально-распределенных ресурсов в мультисервисных сетях связи (каналов связи, криптографических программно-аппаратных комплексов, баз данных). Методики позволяют предложить пользователю тарифный план, зависящий не только от типа и качества сервиса (передача данных, видеоконференции, мультимедиа и т. п.), но и от степени защищенности (конфиденциальности, целостности и доступности) передаваемой информации.

В заключении представлены основные результаты работы. Все выводы, сделанные соискателем, в этой части работы можно найти в наиболее точном и сжатом виде.

Таким образом, можно заключить, что анализ предметной области, постановка проблемы исследования, выбор подходов и методов ее решения обеспечивают должный уровень обоснованности положений и результатов работы, которые соответствуют поставленной цели исследования, а итоги - положениям, выносимым на защиту.

3. *Достоверность и новизна полученных результатов, выводов и рекомендаций, сформулированных в диссертации.*

Диссертация С.Н. Новикова является комплексным исследованием. Соискателем сделан качественный анализ научных публикаций по тематике исследования, касающегося технологий предоставления, распространения и защиты информации в современных телекоммуникационных системах связи. На основании анализа сформулирована цель исследования - создание методологических основ и инструментария для реализации защиты информации с использованием технологий сетевого уровня мультисервисных сетей связи, что позволяет автору, используя МСС, обеспечить достижение необходимого уровня конфиденциальности, целостности и доступности передаваемой информации с помощью пользовательских сервисов сетевого уровня связанных, в том числе, с качеством обслуживания (QoS).

Характеризуя *научную новизну* работы следует отметить новые *методики, модели, критерии и алгоритмы выбора сетевых параллельных маршрутов,* позволяющие на базе протоколов сетевого уровня мультисервисных сетей связи *обеспечить защиту конфиденциальности, целостности и доступности информации* при минимальной стоимости и без потери качества.

Автор адекватно использует математические модели, а корректное сравнение выводов, полученных в результате моделирования, с экспериментальными данными подтверждает достоверность положений и результатов работы. Все основные результаты, представленные в работе

опубликованы в достаточном количестве научных статей и прошли должную апробацию.

4. *Значимость для науки и практики полученных автором результатов.*

Разработана методология, позволяющая реализовать защиту информации на базе протоколов сетевого уровня мультисервисных сетей связи

Разработан и реализован новый эффективный алгоритм проверки графа сети на связность.

Разработана математическая модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи.

Практическая значимость работы заключается в определении факторов, влияющих на уменьшение вероятности отказа в обслуживании заявок за счет применения параллельных методов маршрутизации в условиях внешних деструктивных воздействий на элементы МСС, и разработке технологий, позволяющих обеспечить необходимый уровень конфиденциальности, целостности и доступности передаваемой информации с должным качеством обслуживания без увеличения стоимости услуг.

5. *Рекомендации по использованию результатов и выводов диссертации.*

Материалы диссертационного исследования уже внедрены в ряде организаций, связанных с защитой информации, а также используются в учебном процессе на специальностях, направлениях укрупненной группы «Информационная безопасность».

Замечания:

1. Список сокращений было бы уместно привести не на стр. 174, а во введении.

2. Имеются опечатки, в частности (стр. 49), незаконченное предложение «*Для обеспечения доступности либо целостности информации за счет организации параллельных независимых соединений между УИ и УП необходимо выбирать те соединения, у которых отношение».*
3. Попытка на одной странице (стр.89) представить в виде схемы «Концепцию математической модели маршрутизации в МСС» не является удачной. Обилие переменных с индексами и стрелок скорее усложняет понимание концепции.
4. Выводы к главе 1 (стр. 31) «Для обеспечения конфиденциальности, доступности и целостности информации ***пользователи*** мультисервисной сети связи *должны иметь в своем распоряжении специализированное актуальное (постоянно обновляемое) программно-аппаратное обеспечение и обладать знаниями в области защиты информации»* вызывают вопрос, поскольку непонятно, кто, с точки зрения автора, является ***конечным пользователем*** МСС. А без четкой конкретизации пользователей трудно установить, какую информацию следует защищать.
5. Табл. 2.1 (стр.34), судя по библиографической ссылке, взята из работы Б.Шнайера, изданной на русском языке в 2002 году, а на английском - в 1994 году. За прошедшие два десятилетия многочисленные работы по теории чисел и криптоанализу изменили представление о криптостойкости асимметричных шифров. *Традиционные асимметричные криптосистемы теперь требуют больших размеров ключей чем указанные в таблице, при той же стойкости относительно симметричных ключей.* По нашему мнению в таблице следует также учесть использование алгоритмов на эллиптических кривых, к каковым, например, относятся современные стандарты на

цифровую подпись ГОСТ Р 34.10-2012 и ECDSA, и которые обеспечивают более высокую криптостойкость при меньших ключах, нежели традиционные асимметричные криптосистемы, какие рассматривались в работе Б.Шнайера.

6. На рис.2.3. (стр 38) приведены данные эксперимента "*шифрования алгоритмом RSA блока данных объемом 1 кБ при изменении длины ключа от 256 бит до 2048 бит и использовании составного 256-битного ключа (многократное асимметричное шифрование).*" Как следует из описания эксперимента, здесь под размером ключа, подвергающегося разбиению, понимается именно *показатель степени* в которую возводится текст *(а не размер модуля, как это предусмотрено формулой 1.1, на основании которой производятся теоретические выкладки 2.1-2.3)*, Эти результаты плохо согласуются с тем, что можно получить при использовании быстрого (дихотомического) алгоритма возведения в степень по модулю.
7. В главе 3 рассматриваются методы построения таблиц маршрутизации, но не упоминаются современные подходы, когда создается Forwarding Information Base (FIB) - таблица, содержащая маршрут, исходящий интерфейс и L2 destination. FIB хранится в быстрой памяти, а работа с этой базой может осуществляться на уровне микросхем, т.е. как при коммутации, что существенно уменьшает время на выбор маршрута, компенсируя время, затраченное на создание таблицы маршрутизации.
8. В главе 5 выполнено сравнение сходимости IP протокола маршрутизации OSPF и протокола MPLS на программном эмуляторе для сетевой инфраструктуры. Автору требуется более четко объяснить суть эксперимента, поскольку в реальных сетях протокол MPLS не создает таблиц

маршрутизации, а для создания своих меток использует уже созданные таблицы маршрутизации IP протоколов (OSPF, IS-IS, но чаще BGP, который в связке с MPLS настраивается только на пограничных маршрутизаторах AS клиентов и/или других провайдеров). Для таких экспериментов в лабораторных условиях больше подходит сеть на базе виртуальных машин, на которых поднимаются реальные операционные системы сетевых устройств и, естественно, работают отладчики, с помощью которых можно лучше понять причины тех или иных эффектов.

Ряд сделанных замечаний носит в определенной мере дискуссионный характер и не снижает общую положительную оценку результатов проведенного исследования.

Заключение

Диссертационная работа Новикова Сергея Николаевича «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи» представленная на соискание ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность по объему представленного материала, степени достоверности результатов исследования и научной новизне представляет собой самостоятельное, завершенное научное исследование, выполненное на актуальную тему и имеющая теоретическую и практическую значимость. Автор продемонстрировал умение решать научные и прикладные задачи на современном уровне.

Автореферат и опубликованные работы достаточно полно отражают содержание диссертации.

Результаты диссертационного исследования соответствует пунктам 1, 5, 6, 8, 13 паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Работа «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи» соответствует требованиям сформулированным в п. 9-10 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства РФ от 24.09.2013 № 842, предъявляемым к докторским диссертациям, а ее автор Новиков Сергей Николаевич, заслуживает присуждения искомой ученой степени доктора технических наук технических наук по специальности – 05.13.19 - Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Доктор технических наук, профессор,
заведующий кафедрой информационной безопасности
Института математики и компьютерных наук,
ФГАОУ ВО «Тюменский государственный
университет»

Александр Анатольевич Захаров

ПОДПИСЬ ЗАВЕРЯЮ:
Ученый секретарь Ученого совета
Э.М. Лимонова
21.10.2016

625003, г. Тюмень, ул.Семакова,10
Тел. +7(3452) 46-83-43
e-mail: azaharov@utmn.ru