

Авторы:

Сулипов Шамиль Ломалиевич

студент

Сайдаев Магомед Салуевич

студент

Джамурзаева Хава Зелимхановна

студентка

ФГБОУ ВО «Чеченский государственный

педагогический университет»

г. Грозный, Чеченская Республика

ЗАЩИТА ИНФОРМАЦИИ В ВИРТУАЛЬНОЙ СЕТИ

Аннотация: в данной статье рассматривается вопрос о защите информации в виртуальной сети и ее структуре. Использование интернет-технологии в сети, а также формирование режима информационной безопасности.

Ключевые слова: Интернет, Сеть, архитектура в Сети, интернет-технологии.

Архитектура сети подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов во вне, что предъявляет повышенные требования к защите данных.

В интернет-системах использование подхода клиент-сервер и основная роль на сегодняшний день играет в веб-серверы. Веб-серверы должны поддерживать традиционные меры защиты, такие как проверка подлинности и контроль доступа; кроме того, необходимо обеспечить новые свойства, особенно среды программного обеспечения безопасности и сервера и на стороне клиента.

Это, можно сказать в двух словах, вызовы в области информационной безопасности, которые возникают в связи с переходом на технологии Интернет. Далее рассматриваются возможные подходы к их решению.

Формирование режима информационной безопасности-проблема комплексная.

Меры по ее решению можно разделить на четыре уровня:

- законодательные (законы, нормативные акты, стандарты и др.);
- административный (действия общего характера, предпринимаемые руководством организации);
- процедурные (конкретные меры безопасности, касающиеся людей);
- программное и аппаратное обеспечение (конкретные технические меры).

Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

- 1) ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web;
- 2) заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Internet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов;
- 3) перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Выводы

Проблемы информационной безопасности в Интернете и, с разной степенью эффективности, решается с момента появления сетей на основе протоколов TCP/IP.

В последние годы взрывной рост Интернета и связанных с ним коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в сетях TCP/ИС. И если раньше, до начала 90-х годов, главной целью защиты было сохранение интернет-ресурсов в основном от хакерских атак, то теперь становится актуальной задача защиты коммерческой информации.

Выбор технологии защиты информации для большой открытой системы – сети масштаба Интернете, большой корпоративной сети, поставщик связи должен соответствовать определенным требованиям:

- 1) отсутствие монополии в плане технологических решений;
- 2) широкое масштабирование по техническим и ценовым параметрам;
- 3) универсальность, переносимость, многоплатформенность
- 4) сомастостатин, программное обеспечение, коммуникационные решения;
- 5) обеспечение, при необходимости, ComplexRussia информацию;
- 6) простое управление ключами и безопасная связь для вновь подключенных пользователей.

Список литературы

1. Игер Б. Работа в Internet / Под ред. А. Тихонова; пер. с англ. – М.: Бином, 1996. – 313 с.
2. Фролов А.В. Глобальные сети компьютеров. Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windows Sockets / А.В. Фролов, Г.В. Фролов. – М.: Диалог – МИФИ, 1996. – 283 с.