Уважаемые председатель и члены комиссии!

Вашему вниманию предлагается дипломный проект на тему «Однонаправленная ведомственная сеть».

Проблема хранения конфиденциальных данных возникает в любой организации, работающей с информацией, потеря, утечка или искажение которой может привести к значительным последствиям.

В настоящее время передовые методы защиты данных подразумевают возможность компрометации любого участка защищенной системы. Несмотря на технический прогресс в области защиты информации и сетевых технологий, даже новейшая инфраструктура нуждается в регулярных обновлениях программно-технического комплекса и отслеживания новых методик противодействия атакам.

Наиболее эффективным методом предотвращения утечек является полная изоляция сети.

К сожалению, даже полностью изолированная система нуждается в доступе во внешний мир для выполнения своих функций. Данную проблему можно решить посредством физических накопителей или использованием программного подхода ограничения прав доступа или использованием межсетевых экранов, однако подобный подход не может гарантировать, что пользователь.

Для решения проблемы невозможности работы полностью изолированной сети используют методы однонаправленной передачи данных. Диод данных, это комплекс, который позволяет передачу данных только в одном направлении, предотвращая передачу в обратном направлении. Таким образом, даже в случае полной компрометации внутренней сети, передать данные во внешний мир не представляется возможным, предотвращая возможную утечку данных.

Областями применения однонаправленных сетей являются приватные сети ведомств, репликация данных, защита критических источников данных.

Однако при передаче данных через однонаправленных шлюз отсутствует обратная связь. По этой причине, классические методы передачи данных и файлов во внутреннюю сеть не могут быть применены.

Однонаправленная сеть реализована на базе двух серверов, одного расположенного в публичной сети, и одного расположенного в приватной сети. Серверы соединены между друг-другом однонаправленным шлюзом. Передача данных производится посредством протокола UDP.

Программно передача данных происходит посредством клиент-серверного приложения. На публичном сервере расположена программа передачи данных. При запуске программы, она считывает конфигурацию (плакат конфигурации), и приступает к отслеживанию рабочего каталога.

Рассмотрим передачи файла.

Перед началом работы, передающая сторона, считывает файл конфигурации и загружает сохраненное состояние каталога. Далее через интервал, заданный в файле конфигурации, происходит проверка отслеживаемого каталога на наличие изменений, изменения добавляются в очередь, после чего начинается процесс передачи файла.

Файл разделяется на фрагменты, которые вместе с заголовками, отправляются по однонаправленной сети посредством протокола UDP.

На приемной стороне происходит ряд проверок, в числе которых:

– проверка источника пакета

– проверка на наличие пакета в кэше обработанных пакетов

– проверка контрольных сумм данных

– проверка целевого состояния каталога, для случаев, когда пришедший пакет описывает создание уже существующего файла.

После прохождения проверок, идентификатор пакета добавляется в кэш обработанных пакетов и происходит обработка фрагмента в зависимости от типа изменения.

Для изменения типа создать или изменить в случае прихода первого пакета для файла происходит проверка на наличие файла с тем же именем в рабочем каталоге. В случае если файл с тем же именем существует, он переносится в каталог Old.

Далее в каталоге Downloading создается файл с размером целевого файла и заполняется нулями. Данное действие необходимо для корректного размещения данных в файле, так как пакеты могут приходить в произвольном порядке.

После инициализации загрузки в первый раз, файл заполняется данными из пришедшего и последующих пакетов.

По завершению загрузки, сверяется контрольная сумма файла и происходит его перенос в рабочий каталог.

Состояние каталога в кэше обновляется, это нужно для корректной проверки целевого состояния каталога и происходят сервисные очистки файлов Old и Downloading от устаревших записей.

В случае удаления файл просто переносится из рабочего каталога в каталог Old.

В случае наличия логических ошибок, вроде создание уже существующего файла, или модификация не существующего файла происходит событие, заданное в файле конфигурации.

На чертеже 1 представлена схема разработанной ведомственной сети, состоящая из публичной и приватной части, они соединены однонаправленным шлюзом, а передача информации на публичный сервер, может происходить любым удобным для пользователей образом. Доступ в приватной сети, также осуществляется любым удобным для пользователей образом.

На чертеже 2 представлен алгоритм подпрограммы инициализации клиент-серверного приложения синхронизации каталогов.

На чертеже 3, 4 представлен алгоритм передачи данных, на чертеже 5 представлен алгоритм приема данных.

В дипломном проекте была проведена реализация клиент-серверного приложения, технико-экономическое обоснование проектируемой системы.

Доклад окончен.