РЕФЕРАТ

по дисциплине «Информатика»

по теме: «Защита информации»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. Информационная безопасность и мероприятия по ее технической защите

2. Методы опознания и разграничения информации

ЗАКЛЮЧЕНИЕ

ЛИТЕРАТУРА

ВВЕДЕНИЕ

В современном мире платой за всеобщее пользование Интернетом является всеобщее снижение информационной безопасности. Интернет и информационная безопасность несовместимы по самой природе Интернет. «Всемирная паутина» – Интернет родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Интернет со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Для предотвращения несанкционированного доступа к своим компьютерам необходимы средства, направленные на опознание и разграничение доступа к информации.

1. Информационная безопасность и мероприятия по ее технической защите

Информация представляет собой результат отражения движения объектов материального мира в системах живой природы.

Информация обращается в коллективе однотипных организмов в форме сведений и сообщений. Сведения образуются в результате отражения организмами объектов материального мира, в том числе сообщений. Сообщения образуются организмами для передачи сведений другим организмам, содержат совокупность передаваемых сведений, и представляют собой набор знаков, с помощью которого сведения могут быть переданы другому организму и восприняты им.

Преобразование сведений в сообщения и сообщений в сведения осуществляется человеком с использованием алгоритмов кодирования и декодирования поступившего набора знаков в элементы его «информационной» модели мира.

Важное событие последнего десятилетия в области технической защиты информации – это появление и развитие концепции аппаратной защиты. Основные идеи аппаратной защиты состоят в следующем:

- признании мультипликативной парадигмы защиты, и, как следствие, равное внимание реализации контрольных процедур на всех этапах работы информационной системы (защищенность системы не выше защищенности самого слабого звена);
- материалистическом решении «основного вопроса» информационной безопасности: «Что первично – hard или soft?»;
- последовательном отказе от программных методов контроля, как очевидно ненадежных (попытка с помощью программных средств проконтролировать правильность других программных средств эквивалентна попытке решения неразрешимой задачи о самоприменимости) и перенос наиболее критичных контрольных процедур на аппаратный уровень;

- максимально возможном разделении условно-постоянных (программы) и условно-переменных (данные) элементов контрольных операций.

Необходимость защиты информационных технологий была осознана лишь в последнее время.

В процессе информационного взаимодействия на разных его этапах заняты люди (операторы, пользователи) и используются средства информатизации – технические (ПЭВМ, ЛВС) и программные (ОС, ППО). Сведения порождаются людьми, затем преобразовываются в данные и представляются в автоматизированные системы в виде электронных документов, объединенных в информационные ресурсы. Данные между компьютерами передаются по каналам связи. В процессе работы автоматизированной системы данные преобразовываются в соответствии с реализуемой информационной технологией. В соответствии с этим, в мероприятиях по технической защите можно выделить:

1. аутентификацию участников информационного взаимодействия;
2. защиту технических средств от несанкционированного доступа;
3. разграничение доступа к документам, ресурсам ПЭВМ и сети;
4. защиту электронных документов;
5. защиту данных в каналах связи;
6. защиту информационных технологий;
7. разграничение доступа к потокам данных.

Информационную систему собирают из готовых элементов, разрабатывая, как правило, лишь небольшую прикладную составляющую (естественно, важнейшую, так как ею определяется функциональность системы). Здесь уместно вспомнить мультипликативную парадигму защиты, а именно – уровень информационной безопасности не выше обеспечиваемой самым слабым звеном. Для нас это означает, что в случае использования готовых «блоков» их нужно выбирать так, чтобы уровень защиты каждого из них был не ниже того, который требуется для системы в целом, включая и

защиту информационных технологий, и защиту электронных документов. Незащищенность как одного, так и другого, сводит на нет усилия в остальных направлениях.

В следующем разделе будут рассмотрены виды мероприятий по опознанию и разграничению информации применительно к нашей теме.

2. Методы опознания и разграничения информации

Идентификация/аутентификация (ИА) участников информационного взаимодействия должна выполняться аппаратно до этапа загрузки ОС. Базы данных ИА должны храниться в энергонезависимой памяти СЗИ, организованной так, чтобы доступ к ней средствами ПЭВМ был невозможен, т.е. энергонезависимая память должна быть размещена вне адресного пространства ПЭВМ. Программное обеспечение контроллера должно храниться в памяти контроллера, защищенной от несанкционированных модификаций. Целостность ПО контроллера должна обеспечиваться технологией изготовления контроллера СЗИ. Идентификация должна осуществляться с применением отчуждаемого носителя информации.

Для ИА удаленных пользователей также необходима аппаратная реализация. Аутентификация возможна различными способами, включая электронно-цифровую подпись (ЭЦП). Обязательным становится требование «усиленной аутентификации», т.е. периодического повторения процедуры в процессе работы через интервалы времени, достаточно малые для того, чтобы при преодолении защиты злоумышленник не мог нанести ощутимого ущерба.

Современные операционные системы все чаще содержат встроенные средства разграничения доступа. Как правило, эти средства используют особенности конкретной файловой системы (ФС) и основаны на атрибутах, сильно связанных с одним из уровней API операционной системы. При этом неизбежно возникают проблемы, по крайней мере, следующие.

- Привязка к особенностям файловой системы.

В современных операционных системах, как правило, используются не одна, а несколько ФС – как новые, так и устаревшие. При этом обычно на новой ФС встроенное в ОС работает, а на старой – может и не работать, так как встроенное разграничение доступа использует существенные отличия новой ФС. Это обстоятельство обычно прямо не оговаривается в сертификате, что может ввести пользователя в заблуждение. И действительно, представим, что на компьютере с новой ОС эксплуатируется программное обеспечение, разработанное для предыдущей версии, ориентированное на особенности прежней ФС. Пользователь вправе полагать, что установленные защитные механизмы, сертифицированные и предназначенные именно для используемой ОС, будут выполнять свои функции, тогда как в действительности они будут отключены. В реальной жизни такие случаи могут встречаться довольно часто – зачем переписывать прикладную задачу, сменив ОС? Более того – именно с целью обеспечения совместимости старые ФС и включаются в состав новых ОС.

- Привязка к API операционной системы.

Как правило, операционные системы меняются сейчас очень быстро – раз в год – полтора. Не исключено, что будут меняться еще чаще. Некоторые такие смены связаны с изменениями в том числе и API – например, смена Win9x на WinNT. Если при этом атрибуты разграничения доступа отражают состав API – с переходом на современную версию ОС будет необходимо переделывать настройки системы безопасности, проводить переобучение персонала и т.д. и т.п.

Таким образом, можно сформулировать общее требование – подсистема разграничения доступа должна быть наложенной на операционную систему, и тем самым, быть независимой от файловой системы. Разумеется, состав атрибутов должен быть достаточен для целей описания политики безопасности, причем описание должно осуществляться

не в терминах API ОС, а в терминах, в которых привычно работать администраторам безопасности.

Рассмотрим теперь конкретный комплекс мер программно-технического уровня, направленных на обеспечение информационной безопасности информационных систем. Здесь можно выделить следующие группы:

- средства универсальных ОС;
- межсетевые экраны.

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС – это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений (как и врач, не ведающий всех побочных воздействий рекомендуемых лекарств). Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.).

Как указывалось выше, единственный перспективный путь связан с разработкой специализированных защитных средств, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран – это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и

контролирует все информационные потоки во внутреннюю сеть и из нее (рис. 1). Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

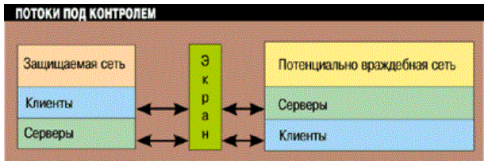

Рис.1 Межсетевой экран как средство контроля информационных потоков

Целесообразно разделить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, мы будет говорить о внешнем и внутреннем межсетевых экранах.

Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее, здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность. Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования (рис. 2). В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно

считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

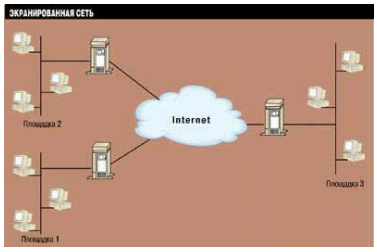

Рис.2 Экранирование корпоративной сети, состоящей из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования.

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по тому, на каком уровне производится фильтрация – канальном, сетевом, транспортном или прикладном. Соответственно, можно говорить об экранирующих концентраторах (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

В данной работе мы не будем рассматривать экранирующие концентраторы, поскольку концептуально они мало отличаются от экранирующих маршрутизаторов.

При принятии решения «пропустить/не пропустить», межсетевые экраны могут использовать не только информацию, содержащуюся в фильтруемых потоках, но и данные, полученные из окружения, например текущее время.

Таким образом, возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах

фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован. В то же время фильтрация на каждом из перечисленных выше уровней обладает своими достоинствами, такими как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также некоторых других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны. Наиболее типичным является сочетание экранирующих маршрутизаторов и прикладного экрана (рис. 3).

Приведенная конфигурация называется экранирующей подсетью. Как правило, сервисы, которые организация предоставляет для внешнего применения (например «представительский» Web-сервер), целесообразно выносить как раз в экранирующую подсеть.

Помимо выразительных возможностей и допустимого количества правил качество межсетевого экрана определяется еще двумя очень важными характеристиками – простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует еще позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.

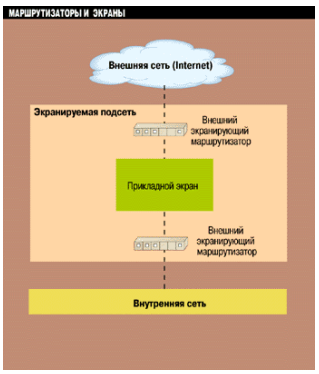

Рис.3 Сочетание экранирующих маршрутизаторов и прикладного экрана.

Природа экранирования (фильтрации), как механизма безопасности, очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной экран может осуществлять действия от имени субъектов внутренней сети, в результате чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном (рис. 4). При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

Рис.9 Истинные и кажущиеся информационные потоки.

Более общим методом сокрытия информации о топологии защищаемой сети является трансляция «внутренних» сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации. Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать,

особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый видит лишь то, что ему положено. Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, в частности таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация баз данных.

ЗАКЛЮЧЕНИЕ

В области защиты компьютерной информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

Выполнение перечисленных выше требований обеспечивает достаточный уровень защищенности сообщений, обрабатываемых в информационных системах.

В современных условиях, для целей разграничения доступа к потокам данных используются, как правило, маршрутизаторы с функцией «VPN – построителя». Надежно эта функция может быть реализована только с помощью криптографических средств. Как всегда в таких случаях – особое внимание должно уделяться ключевой системе и надежности хранения ключей. Естественно, что требования к политике доступа при разграничении потоков совершенно отличаются от таковых при разграничении доступа к файлам и каталогам. Здесь возможен только простейший механизм – доступ пользователю разрешен или запрещен.

ЛИТЕРАТУРА

1. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. – М.: «МЦНМО», 2002.

2. Гадасин В.А., Конявский В.А. От документа – к электронному документу. Системные основы. – М.: РФК-Имидж Лаб, 2001.

3. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: «Радио и связь», 1999.