УДК 004.75, 004.056.52, 004.056.53

Г.А. Абрамов

Россия, г. Самара, АО «Самарский электромеханический завод»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

В данной работе описываются основные проблемы, с которыми сталкиваются специалисты службы защиты информации на 5нновационнях, а также рассмотрены возможные варианты решения с учетом актуальных нормативно-методических рекомендаций. Результатам работы служит практическая оптимизация затрат ресурсов на обеспечения информационной безопасности предприятий и закрытие возможных каналов утечки информации.

Введение

Компьютерные системы переживают революцию. До 80-ых годов прошлого века компьютеры были огромными и дорогими. Даже миникомпьютеры могли стоили многие сотни тысяч долларов. Как результате большинство компаний могли приобрести в лучшем случае лишь несколько компьютеров, и все равно способы их объединить в сеть не было, данные ЭВМ функционировали самостоятельно друг от друга.

Развитие информационных технологий, наблюдавшаяся в последние полвека, действительно поражают. Главным двигателем прогресса было изобретение высокоскоростных компьютерных сетей.

Локальные вычислительные сети (ЛВС) соединяют множество компьютеров, таким образом, что машины способны передавать огромные объемы информации за доли секунд.

Прогресс в технологиях локальных сетей и падение себестоимости комплектующий, входящих в состав АРМ, позволяет создавать сложные вычислительные системы для решения различных задач предприятий.

1. Общие положения

1.1. Определение распределенной системы

Распределенная система – это комплекс технических и программных решений, представляющийся их пользователям единой объединенной системой. В этом определении оговариваются два момента. Первый относится к аппаратуре: все машины автономны. Второй касается программного обеспечения: пользователи думают, что имеют дело с единой системой[1]. Важны оба момента.

На рисунке 1 представлена типовая модель распределенной системы.

Рисунок 1 – Типовая схема сети

1.2. Задачи распределенных систем

Основная задача распределенных систем — предоставить пользователям рабочих мест доступ ко всем ресурсам в сети и обеспечить их взаимное использование, контролируя этот процесс. Ресурсы могут быть виртуальными, но чаще всего в них входят принтеры, устройства хранения данных, компьютеры, файлы. Есть множество потребностей в совместном использовании ресурсов. Одна из очевидных – это экономичность. Например, гораздо дешевле разрешить совместную работу с принтером нескольких пользователей, чем покупать и обслуживать отдельный принтер для каждого пользователя. Точно

так же имеет смысл совместно использовать дорогие ресурсы, такие как суперкомпьютеры или высокопроизводительные хранилища данных.

2. Вопросы безопасности

2.1. Основные положения безопасности

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает разделение информации на категории свободного и ограниченного доступа (право на тайну). В свою очередь информация ограниченного доступа подразделяется на информацию, отнесённую к государственной тайне и конфиденциальную[2] (Рисунок 2).

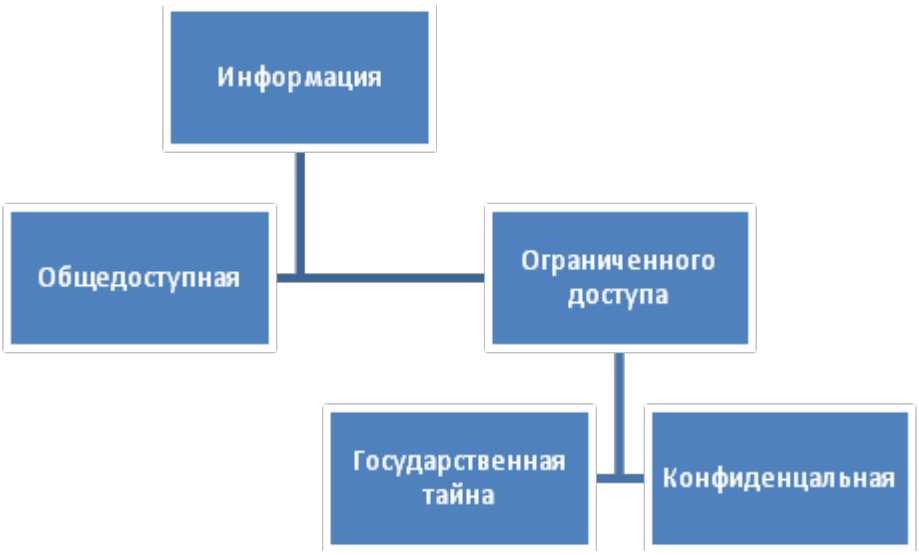

Рисунок 2 – Классификация информации

Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне». Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за её разглашение устанавливаются федеральными законами [3].

2.2. Векторы атаки

Основными векторами атаки являются:

– отказ в обслуживании (англ. *Denial of Service, DoS*) – атака на информационную систему с целью довести её до отказа, то есть создание таких условий, при которых зарегистрированные пользователи системы не могут полу-

чить доступ к предоставляемым системным ресурсам (узлам сети), либо этот доступ затруднён;

– атака посредника или атака «человек посередине» (англ. *Man in the middle (MITM)*) – вид атаки, когда злоумышленник перехватывает и 8нновацией сообщения, которыми обмениваются контрагенты, причём ни один из последних не догадывается о его присутствии в канале, метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию;

– эксплойт (англ. *exploit*) – атака, использующая фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении, целью атаки может быть, как захват контроля над системой (повышение привилегий), так и нарушение её функционирования.

Векторы атаки постоянно меняются и развиваются, злоумышленники не сидят на месте. В обязанности каждого специалиста по информационной безопасности входит постоянный мониторинг актуальных уязвимостей и векторов атак.

2.3. Методы защиты

Безопасность информации при их обработке в информационных системах обеспечивается с помощью системы защиты, включающей 8нновационнонные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и НСД к информации используются следующие основные методы защиты (защитные механизмы):

– идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы;

– разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;

– регистрация и оперативное оповещение о событиях, происходящих в системе;

– криптографическое закрытие (шифрование) хранимых и передаваемых по каналам связи данных;

– контроль целостности и аутентичности (подлинности и авторства) данных;

– резервирование и резервное копирование;

– фильтрация трафика и трансляция адресов;

– обнаружение вторжений (атак);

– выявление и нейтрализация действий компьютерных вирусов;

– затирание остаточной информации на носителях;

– выявление уязвимостей (слабых мест) системы;

– использование технических средств защиты информации.

Перечисленные механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты.

Литература

1. Tanenbaum. A., Steen M., Distributed systems. Principles and paradigms ISBN 0-13-088893-1 // prentice Hall PTR, New Jersey.

2. »Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27 июля 2006 года.

3. »О государственной тайне» Закон РФ №5485-1 от 21 июля 1993 года.