УДК 621.618

Н.Н. Петрушенко[1], Э.А. Плешко[2], С.Н. Шолохов[3]

[1]*Главная инспекция Министерства обороны Украины, Киев*
[2]*Воинская часть А 30800, Винница*
[3]*Центральный НИИ Вооруженных Сил Украины, Киев*

К ВОПРОСУ О ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В статье проведена классификация и рассмотрены методы и средства реализации информационной безопасности в телекоммуникационных системах. Обосновано, что в настоящее время известны методы и средства обеспечения безопасности в телекоммуникационных системах могут быть представлены в виде формальных и неформальных. К формальным методам и средствам предложено отнести физические аппаратные и программные методы и средства. С позиции практической реализации детально рассмотрены формальные методы информационной безопасности телекоммуникационных систем.

Ключевые слова: *электромагнитная совместимость, компьютерная безопасность, сетевые атаки.*

Введение

Постановка проблемы. При рассмотрении вопросов, связанных с безопасностью телекоммуникационных сетей принимают во внимание угрозы, уязвимости и атаки. Как известно [1], угроза безопасности телекоммуникационной системы (ТС) - это потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Уязвимость телекоммуникационной системы - это некая ее характеристика, которая делает возможным возникновение угрозы. Практически все характеристики электромагнитной совместимости (ЭМС) определяют уязвимость системы. Атака - это реализация угрозы. Часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система зашиты должна адекватно реагировать на любое из них [2]. Обычно выделяют три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании. В соответствии с [2] угроза раскрытия заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Угроза целостности как следует из [2] включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие.

Угроза отказа в обслуживании возникает [1, 2] всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан. Характеристики ЭМС в большей мере соответствуют угрозам целостности и отказов. Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений, реализованных в виде структурированных кабельных систем (СКС) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные передаются по сетевым соединениям в виде пакетов обмена. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности ТС с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных ТС состоит в том, что если в локальных ТС наиболее частыми были угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании. Если основные виды угроз безопасности в телекоммуникационных системах достаточно подробно рассмотрены в известной литературе, то рассмотрению методов и средств обеспечения безопасности, а тем более связанных с классификацией их, в известной литературе уделено не достаточное внимание.

Цель статьи. Проведение классификации и рассмотрение методов и средств реализации информационной безопасности в телекоммуникационных системах.

Основная часть

Результаты анализа процесса обеспечения информационной безопасности в каналах телекоммуникации [1, 2] позволяют классифицировать методы и средства его реализации. Как следует из [2], методы обеспечения безопасности в каналах телекоммуникаций реализуются на практике применением различных средств защиты, таких как технические, программные, организационные, законодательные и морально-этические. Рассмотрим их подробнее. В соответствии с [2] технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на:

• аппаратные - устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти по ключу;

• физические - реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации;

• технические - создание препятствий для электромагнитной или кондуктивной утечки или нарушения целостности информации. Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации. Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. Сопоставление существующих методов и средств защиты и эволюции технологии обеспечения безопасности связи в каналах телекоммуникаций показывает, что на первой фазе развития этой технологии преимущественное развитие имели программные средства, вторая фаза характеризовалась интенсивным развитием всех основных методов и средств защиты, на третьей фазе развития все определенней вырисовываются следующие тенденции:

• аппаратная реализация основных функций защиты;

• создание комплексных средств защиты, выполняющих несколько защитных функций;

• унификация и стандартизация алгоритмов и технических средств.

Совершенно очевидно, что для успешной защиты своей информации пользователь должен иметь абсолютно ясную картину о возможных каналах утечки информации, чтобы соответствующим образом принять контрмеры по пресечению несанкционированного доступа (усилить программную защиту, использовать антивирусные программы, усилить пароли, применить экранирование помещения и т. д.). С этой целью перечислим основные пути несанкционированного электромагнитного доступа к закрытой информации:

• перехват электронных излучений; восстановление текста принтера;

• подключение к аппаратуре и линиям связи;

• злоумышленный вывод из строя механизмов защиты путем электромагнитного воздействия (электромагнитный терроризм). Особое место среди средств защиты занимают аппаратные средства. При этом под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения ТС и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами. Аппаратные средства защиты данных можно условно разбить на группы согласно типам аппаратуры, в которых они используются. В качестве таких групп рассмотрим следующие:

• средства защиты процессора;

• средства защиты памяти;

• средства защиты терминалов;

• средства защиты устройств ввода-вывода;

• средства защиты каналов связи.

Не останавливаясь на технических деталях, кратко рассмотрим содержание средств защиты перечисленных групп аппаратуры. Рассмотрим средства защиты процессора оперативной системы. Отметим, что одним из главных условий обеспечения безопасности обрабатываемых данных является обеспечение невозможности одной программы влиять на процесс выполнения другой программы и, особенно, на выполнение программ операционной системы (ОС). Обычно это реализуется введением так называемого привилегированного состояния процессора (в некоторых системах - режима супервизора), характеризуемого специальными привилегированными командами. Для выполнения функций защиты в состав процессора включаются:

• программно-читаемые часы;

• команды очистки блоков памяти;

• программно-читаемые идентификаторы процессора и других технических устройств;

• специальные биты секретности в каждом машинном слове;

• средства контроля регистров, устанавливают их границы памяти.

Отметим, что многие ЭВМ и устройства, входящие в состав ТС, содержат различные механизмы защиты памяти для предотвращения чтения и модификации данных различными пользователями. Для защиты памяти обычно используются следующие средства и механизмы:

• регистры границ памяти, устанавливающие нижний и верхний адреса оперативной памяти для программы, выполняемой в данный момент времени;

• "замки" защиты блоков памяти фиксированного размера в оперативной памяти. Выполняемая программа заносит свой "ключ" в специальный регистр. Каждая выборка и запись в оперативную память контролируется аппаратными средствами на подтверждение того, что ключ соответствует замку;

• сегментация памяти, представляющая использование дескрипторов для описания единиц данных в оперативной памяти. Каждый дескриптор содержит начальный адрес сегмента, его длину и указатели, определяющие вид доступа к данным этого сегмента;

• страничная организация памяти, в которой каждой программе пользователя ставится в соответствие таблица - страниц, отображающая виртуальные адреса в физические. Обычно защита страничной организации памяти реализуется через сегментацию;

• иерархические кольца безопасности, которые обеспечивают аппаратную изоляцию данных и программ, относящихся к различным кольцам.

Терминалы обычно содержат замки для предотвращения несанкционированного включения, а также блокираторы. Блокираторы могут содержать устройства установления подлинности пользователя по жетону, отпечаткам пальцев. Для систем с высокими требованиями к обеспечению безопасности данных терминалы снабжаются встроенными схемами шифрования данных, идентификации терминала.

Устройства ввода-вывода для решения задач защиты могут содержать:

• регистры адресов и идентификаторов;

• регистры границ выделенной устройству памяти, схемы проверки канала ввода-вывода;

• регистры контроля уровня секретности канала связи;

• схемы контроля номера канала.

Каналы связи, как следует из [2], защищаются, в основном, криптографическими средствами.

Аппаратные средства защиты включают и вспомогательные устройства, которые обеспечивают функционирование ТС. Такими устройствами являются, например, устройства уничтожения информации на магнитных носителях, устройства сигнализации о нарушении регистров границ памяти.

В свою очередь физическая безопасность означает содержание компьютера и информации в нем в безопасности от физических опасностей с помощью замков на входах в помещение, где он находится, строительства ограждения вокруг зданий и размещения охраны вокруг помещения. Но физическая безопасность сейчас изменилась из-за современной компьютерной среды - среды, которая часто представляет собой офис с большим числом персональных ЭВМ или терминалов. Физическая безопасность связана с внедрением мер защиты, которые защищают от стихийных бедствий (пожаров, наводнений, и землетрясений), а также всяких случайных инцидентов. Меры физической безопасности определяют, каким будет окружение компьютера, вводимые данные, и результаты обработки информации.

Вывод

Таким образом, в настоящее время основные методы и средства обеспечения безопасности ТС могут быть разделены на формальные и неформальные. Наиболее распространенными в настоящее время среди формальных методов и средств являются физические, аппаратные и программные.

Список литературы

1. Петраков А.В. Основы практической защиты информации / А.В. Петраков. – М: Радио и связь, 2000. – 368 с.

2. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.

Поступила в редколлегию 14.04.2014

Рецензент: д-р техн. наук проф. Л.Ф. Купченко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ДО ПИТАННЯ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

М.М. Петрушенко, Е.А. Плешко, С.М. Шолохов

У статті проведена класифікація і розглянуті методи і засоби реалізації інформаційної безпеки в телекомунікаційних системах. Обґрунтовано, що нині відомі методи і засоби забезпечення безпеки в телекомунікаційних системах можуть бути представлені у вигляді формальних і неформальних. До формальних методів і засобів запропоновано віднести фізичні апаратні і програмні методи і засоби. З позиції практичної реалізації детально розглянуті формальні методи інформаційної безпеки телекомунікаційних систем.

Ключові слова: *електромагнітна сумісність, комп'ютерна безпека, мережеві атаки.*

TO QUESTION ABOUT INFORMATIVE SAFETY IN TELECOMMUNICATION SYSTEMS

M.M. Petrushenko, E.A. Pleshko, S.M. Sholohov

In the article classification is conducted and methods and facilities of realization of informative safety are considered in the telecommunication systems. It is reasonable, that methods and backer-ups of safety are presently known in the telecommunication systems can be presented as formal and informal. To the formal methods and facilities it is suggested to take physical vehicle and programmatic methods and facilities. From position of practical realization the formal methods of informative safety of the telecommunication systems are considered in detail.

Keywords: *electromagnetic compatibility, computer safety, network attacks.*