

УДК 621.618

Н.Н. Петрушенко¹, Э.А. Плешко², С.Н. Шолохов³¹Главная инспекция Министерства обороны Украины, Киев²Воинская часть А 30800, Винница³Центральный 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 защиты 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 определенной 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 несанк-

ционированного 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, устанавливающих 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:

- реєстри границь пам'яті, установлюючі нижній і верхній адреси оперативної пам'яті для програми, виконуваної в даний момент часу;

- "замки" захисту блоків пам'яті фіксованого розміру в оперативній пам'яті. Виконувана програма заносить свій "ключ" в спеціальний реєстр. Кожна вибірка і запис в оперативну пам'ять контролюється апаратними засобами на підтвердження того, що ключ відповідає замку;

- сегментація пам'яті, що представляє використання дескрипторів для опису одиниць даних в оперативній пам'яті. Кожен дескриптор містить початковий адрес сегмента, його довжину і вказівники, що визначають тип доступу до даних цього сегмента;

- сторінкова організація пам'яті, в якій кожній програмі користувача ставиться в відповідності таблиця - сторінок, що відображає віртуальні адреси в фізичні. Звичайно захист сторінкової організації пам'яті реалізується через сегментацію;

- ієрархічні кільця безпеки, які забезпечують апаратну ізоляцію даних і програм, що належать до різних кіл.

Термінали звичайно містять замки для запобігання несанкціонованого входу, а також блокувальні пристрої. Блокувальні пристрої можуть містити пристрої встановлення автентичності користувача по жетону, відбиткам пальців. Для систем з високими вимогами до забезпечення безпеки даних термінали оснащуються вбудованими схемами шифрування даних, ідентифікації терміналу.

Пристрої введення-виводу для вирішення завдань захисту можуть містити:

- реєстри адресів і ідентифікаторів;
- реєстри границь виділеної пристрою пам'яті, схеми перевірки каналу введення-виводу;
- реєстри контролю рівня секретності каналу зв'язку;
- схеми контролю номера каналу.

Канали зв'язку, як зазначено в [2], захищаються, в основному, криптографічними засобами.

Апаратні засоби захисту включають і допоміжні пристрої, які забезпечують функціонування ТС. Такими пристроями є, наприклад, пристрої знищення інформації на магнітних носіях, пристрої сигналізації про порушення реєстрів границь пам'яті.

В свою чергу фізична безпека означає збереження комп'ютера і інформації в ньому від небезпек фізичного характеру з допомогою замків на входах в приміщення, де він знаходиться, будівництва огорожі навколо будівлі і розміщення охорони навколо приміщення. Але фізична безпека зараз змінилася через сучасну комп'ютерну середовище - середовище, яке часто представляє собою офіс з великою кількістю персональних ЕВМ або терміналів. Фізична безпека пов'язана з впровадженням заходів захисту, які захищають від стихійних лих (пожег, повеней, і землетрусів), а також всіх випадкових інцидентів. Методи фізичної безпеки визначають, який буде навколишній середовище комп'ютера, вносимі дані, і результати обробки інформації.

Вывод

Таким чином, в даний час основні методи і засоби забезпечення безпеки ТС можуть бути розділені на формальні і неформальні. Найбільш поширеними в даний час серед формальних методів і засобів є фізичні, апаратні і програмні.

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. Petrusenko, 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 back-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.