УДК 621.391.7

Ю.Е. Яремчук,
кандидат технических наук, доцент
Е.А. Кулагин

ВОЗМОЖНОСТЬ ПОСТРОЕНИЯ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрена возможность построения скрытого канала передачи данных в системах технической защиты информации, структура системы защиты и его элементы, формализация объекта методами системного анализа, а также угрозы и целевые ограничения скрытой передачи информации.

Ключевые слова: *системы защиты информации, сокрытие информации, скрытый канал передачи данных, системный анализ.*

Розглянуто можливість побудови прихованого каналу передавання даних у системах технічного захисту інформації, структуру системи захисту та його елементи, формалізацію об'єкта методами системного аналізу, а також загрози та цільові обмеження прихованого передавання інформації.

Ключові слова: *системи захисту інформації, приховування інформації, прихований канал передавання даних, системний аналіз.*

We consider the possibility of building a hidden channel for data transmission in the systems of technical protection of information, the protection of the system structure and its elements, formalization of the objects of the methods of a system analysis, as well as the threats and restrictions of a hidden data transmission.

Keywords: *information security systems, information hiding, hidden data channel, system analysis.*

До сих пор не существует формальных методов решения всего спектра задач при создании систем технической защиты информации (ТЗИ), поэтому часто используются неформальные, эмпирические методы. Поскольку требования к ТЗИ велики, а возможности по их реализации ограничены, эффективными оказались методы системного анализа, при которых объекты рассматриваются как системы с межэлементными связями, элементы которых также являются системами. Системный анализ более полувека используется во многих отраслях военного строительства, планирования и разработок, а также во многих гражданских отраслях. Наиболее эффективные методики системного анализа относятся к области выявления, прогнозирования и решения проблем.

Кратко очертим основные положения теории системного анализа.

Согласно теории системного анализа, в изложении Оптнера [1], проблема – это ситуация, которая характеризуется различием между требуемым и существующим выходом системы. Актуальность проблемы определяется состоянием системы при нерешенной проблеме и определяет необходимость ее решения. Система, которая решает задачу преобразования существующего выхода системы к требуемому

значению, является объектом конструирования и называется решением проблемы. Методология системного анализа основывается на количественном сравнении альтернатив. Альтернативой является система, которая решает проблему. Критерием принадлежности элемента к конкретной альтернативе служит его участие в процессе преобразования входа системы в ее выход. Процесс является центральным понятием системного анализа.

Система определяется системными объектами, свойствами и связями. К ним относятся: вход, процесс, выход, обратная связь, ограничение.

Ограничение состоит из цели системы, которая задается потребителем, и принуждающих связей (качеств).

Связи – это порядок следования процессов, т.е. соединение выходов одних процессов с входами других.

Всякая система состоит из подсистем. Всякая система является подсистемой некоторой системы. Граница системы определяется совокупностью входов от окружающей среды. Окружающая среда – это совокупность систем, для которых данная система является подсистемой.

В самом общем виде методология решения проблем состоит из выявления проблемы, конструирования решения проблемы, и реализации этого решения.

Определим входы, выходы, процессы и ограничения системы. Они заданы окружающей средой системы, т.е. системами, для которых исследуемая система является подсистемой, в том числе и системой нормативных документов. В нашем случае объект исследования находится на стыке двух систем: системы обеспечения информационной безопасности и системы передачи информации. Рассмотрим подробнее, какие цели, задачи и ограничения они имеют.

Целью обеспечения информационной безопасности является обеспечение безопасности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение вреда, в частности, через несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации [2]. Одним из путей обеспечения информационной безопасности является выявление, оценка и прогнозирование угроз информационной безопасности, и предупреждение этих угроз. Для решения этих задач создаются системы защиты информации.

Одним из путей решения задач защиты информация является техническая защита информации. Согласно ДСТУ 3396.2-97, ТЗИ – это деятельность, направленная на предотвращение нарушения целостности, блокирования и (или) утечки информации по техническим каналам [2]. Для реализации целей ТЗИ создаются системы ТЗИ, одной из составляющих которых являются инженерно-технические мероприятия (ИТМ). Под ИТМ будем понимать совокупность специальных технических средств (СТС) и их использование для защиты информации. В данном случае СТС понимаются шире, чем только средства негласного съема информации с каналов связи и негласного получения информации.

Нашей задачей является защита скрытого канала передачи информации. Поэтому мы будем рассматривать создание скрытых каналов связи как основные технические мероприятия, т.е. мероприятия с использованием средств ТЗИ.

Согласно ДСТУ 3396.0-96, ИТМ проводятся на этапе реализации плана защиты информации [3]. Еще до начала ИТМ, на этапе разработки системы защиты информации (СЗИ), на основании результатов определения и анализа угроз

создаются СТС и планы проведения ИТМ. Контроль эффективности проведения ИТМ осуществляется на этапе контроля функционирования и управления СЗИ.

Исходя из цели защиты информации, очевидно, что защищенная система передачи информации как ИТМ включает в себя следующие процессы:

– процессы передачи информации;
– процессы защиты конфиденциальности;
– процессы защиты целостности и доступности.

Объектом ТЗИ является информация, которая составляет государственную или другую, предусмотренную законами тайну, а также конфиденциальная информация, которая является государственной собственностью или передана государству. Такую информацию принято называть информацией с ограниченным доступом (ИОД) [3]. Очевидно, что СЗИ обеспечивает существование информации как ИОД.

При нарушении СЗИ информация с ограниченным доступом либо повреждается, либо превращается в информацию без ограниченного доступа. Поэтому можно утверждать, что одним из входов ИТМ как системы, при построении СЗИ, является информация, а выходом – ИОД. Другим входом ИТМ является задание, в соответствии с планом защиты информации.

Определим ограничения системы ИТМ исходя из требований нормативных документов [3]. Таковыми ограничениями являются:

– соответствие угрозам;
– обеспечение заданной эффективности;
– соответствие законам и нормативным документам.

На рис. 1 изображена структура системы защищенной передачи информации.

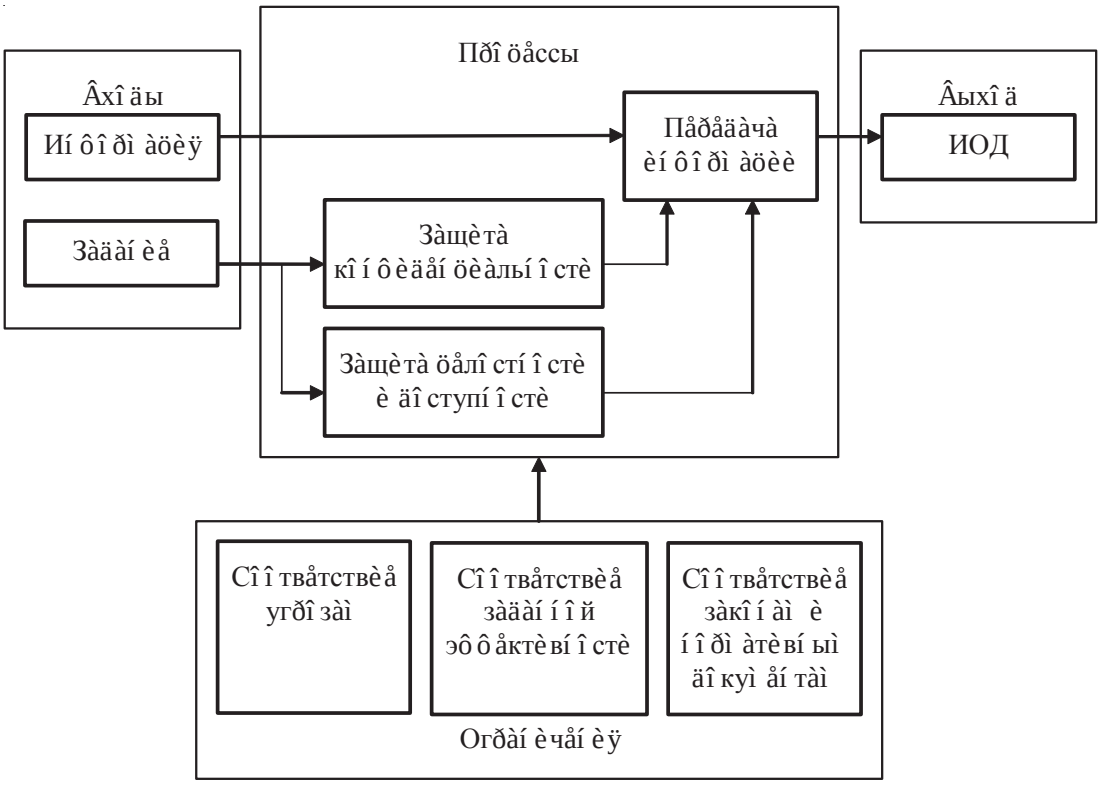

Рис. 1. Структура системы защищенной передачи информации

Отметим, что эта структура соответствует именно ИТМ и является только подструктурой СЗИ, т.к. СЗИ имеет еще процессы оценки угроз, разработки СТС и анализа эффективности, а также обратные связи.

Теперь рассмотрим систему передачи информации. В структуре ИТМ (рис. 1), она включена в процесс “Передача информации”.

Из теории связи [4] известно, что любая система связи состоит из пяти основных объектов:

– источника информации;
– передатчика;
– канала;
– приемника;
– потребителя информации.

Входом системы передачи является сообщение, испускаемое источником информации.

Передатчик преобразует входной сигнал в форму, пригодную для передачи по линии связи. В передатчике электрические сигналы подвергаются различным преобразованиям. Основными из них являются: кодирование, модуляция и согласование с линией по мощности и по спектру.

Канал является средой, в которой осуществляется передача информации. Сам по себе канал является системой, в которой входной сигнал преобразуется в выходной, представляющий собой смесь полезного сигнала и помех. Помехи могут быть двух видов:

– мультипликативные;
– аддитивные.

Мультипликативные помехи представляют собой искажения параметров сигнала, вызванные перемножением входного сигнала и помехи. Они вызывают различные сдвиги параметров в частотной или временной области. Аддитивные помехи представляют собой результат суммирования входного сигнала и шума. Помехи могут быть непреднамеренными и преднамеренными, созданными с целью противодействия средствам связи.

Приемник выполняет задачу, обратную задаче передатчика – восстанавливает исходное сообщение.

Передатчик, канал передачи и приемник могут быть источниками утечки информации:

– через визуальный канал;
– через электромагнитные излучения;
– через электрические сигналы.

Уточним ограничения, связанные с возможными угрозами скрытому каналу. Сразу же выделим два вида угроз. Первый – это угрозы пассивные, не связанные с вмешательством в процесс передачи информации. Такими угрозами являются угрозы конфиденциальности. Второй вид угроз – это активные угрозы, связанные с каким-либо видом нарушения канала. Такими угрозами являются угрозы целостности и доступности информации, т.е. уничтожение информации или ее модификация.

К пассивным угрозам в первую очередь относится угроза несанкционированного доступа к информации, или утечка информации. Учитывая, что при защите информации используются методы сокрытия факта передачи информации, факты обнаружения (идентификации) сигналов скрытого канала или обнаружения

каналообразующей аппаратуры (идентификация СТС) являются также угрозой конфиденциальности. Как сказано выше, эти угрозы могут осуществляться через визуальный, электромагнитный и электрический каналы. Через визуальный канал можно непосредственно увидеть и идентифицировать СТС. Это позволяет нарушителю с большой вероятностью сделать вывод о наличии скрытого канала. Через электромагнитный канал можно обнаружить саму аппаратуру по паразитным излучениям или имеющимся в ней нелинейностям (нелинейная локация); можно обнаружить сигналы скрытого канала, излучаемые участком линии связи и сделать вывод о наличии скрытого канала; можно перехватить и записать излучаемый сигнал для дальнейшей обработки и получения несанкционированного доступа. Через электрический канал можно обнаружить факт подключения к линии дополнительного оборудования; можно обнаружить сигнал скрытого канала; можно перехватить передаваемую информацию скрытого канала.

Активные угрозы связаны с помехами передачи информации и с подменой передаваемого сообщения. Непреднамеренные помехи могут привести к уничтожению всей информации или ее части, сделать ее недоступной. Преднамеренные помехи могут уничтожить или изменить информацию. При подмене сообщения нарушитель имитирует сигналы скрытого канала, модифицируя при этом содержимое информации, например с целью дезинформации.

Требования по противодействию указанным угрозам составляют первую группу ограничений системы передачи информации, другую группу ограничений составляют требования, связанные с целевым назначением системы.

Целевое назначение системы передачи определяется задачами ИТМ, наиболее востребованными являются [5, 6]:

– защита речевой информации;

– защита визуальной информации;

– защита информации, циркулирующей в технических средствах обработки, хранения и передачи информации (ТСПИ).

После физического преобразователя, информация представлена в виде электрических сигналов, которые поступают в канал передачи информации. Перед каналом передачи стоит задача доставить эти сигналы в заданную точку. Характер передаваемой информации определяет:

– требуемый объем передаваемой информации или скорость передачи;

– режимы работы канала передачи;

– методы преобразования сигналов в процессе передачи.

Тактические задачи, решаемые при проведении ИТМ, определяют:

– участки линии связи, на которых организован канал передачи;

– особенности структуры системы передачи информации;

– взаимодействие системы передачи с другими системами, задействованными в СЗИ.

Выводы

Структура системы технической защиты информации скрытого канала передачи данных строится как структура системы, являющейся подсистемой защиты информации и передачи данных. Системный подход при построении и анализе данной структуры позволяет выявить и систематизировать основные угрозы и целевые ограничения скрытых каналов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Оптнер С.Л.* Системный анализ для решения деловых и промышленных проблем / С.Л. Оптнер. – М., 1969.

2. ДСТУ 3396.2-97. Технічний захист інформації. Терміни та визначення.

3. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення.

4. *Шеннон К.* Работы по теории информации и кибернетики / К. Шеннон; пер. с англ. – М. : Иностранная литература, 1963.

5. *Абалмазов Э.И.* Методы и инженерно-технические средства противодействия информационным угрозам / Э.И. Абалмазов. – М. : Гротек, 1997.

6. *Хореев А.А.* Защита информации от утечки по техническим каналам : учеб. пос. / А.А. Хореев. – М. : Государственная техническая комиссия Российской Федерации, 1998.

Отримано 21.02.2013