КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ КОНФЛИКТУЮЩИХ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

***Паршуткин Андрей Викторович**, доктор технических наук, доцент, г.Санкт-Петербург*

Статья посвящена анализу и обобщению известной эталонной модели взаимодействия открытых систем для ее применения к ситуации взаимодействия конфликтующих информационных и телекоммуникационных систем. Предложена концептуальная модель взаимодействия конфликтующих систем. Показана возможность применения данной модели как для определения методов создания радиоэлектронных информационных воздействий на телекоммуникационные и информационные системы, так и для обоснования мер защиты от таких воздействий.

***Ключевые слова**: информационный конфликт, модель конфликта, информационные системы, телекоммуникационные системы, радиоэлектронные информационные воздействия, защита информации.*

CONCEPTUAL INTERCONNECTION MODEL OF CONFLICT INFORMATION AND TELECOMMUNICATION SYSTEMS

***Andrey Parshutkin** , Sc. Dr., Associate Professor, St. Petersburg*

Article is devoted to the analysis and generalization of known reference model of open systems interaction for its application to a situation of cashing information and telecommunication systems interaction. Conceptual conflict systems interconnection model is offered. Possibility for this model application is shown as for definition of radio-electronic information impacts creation methods on telecommunication systems, and for justification of protection from such influences.

***Keywords**: Information Conflict, Conflict Model, Information Systems, Telecommunication Systems, Radio-electronic Information Action, Information Protection*

Введение

Основу сетевой структуры современных систем управления различного назначения составляют информационно-телекоммуникационные системы (ИТКС), включающие взаимосвязанные комплексы и средства передачи, обработки, хранения и отображения целевой информации. Рост количества информационных и телекоммуникационных систем (ИТКС), в том числе и в государственных структурах различного уровня, требует активизации усилий по обеспечению их защиты от воздействий со стороны различных нарушителей [1-7]. Развитие техники и технологий информационно-технических воздействий, обуславливают необходимость принятия адекватных мер и проведения работ в направлении создания средств защиты сетей и систем управления наиболее важных государственных и ведомственных объектов. При большом числе прикладных работ в области компьютерной безопасности, до сих пор отсутствует обобщенная модель взаимодействия потенциального нарушителя с защищаемой сетью, в условиях отсутствия у него доступа к терминалам сети. Поэтому актуальна разработка концептуальной модели взаимодействия конфликтующих информационных и телекоммуникационных систем, пригодной как для определения основных методов воздействия на телекоммуникационные и информационные системы, так и для обоснования мер защиты от таких воздействий.

Обобщенные модели взаимодействия открытых и конфликтующих систем

Для вербальной формулировки концепции применения РЭИВ, отметим, что объектом воздействия является группировка информационно-телекоммуникационных средств, соединенных в сеть [1]. Для осуществления взаимодействия элементов ИТКС друг с другом в такой сети устанавливаются правила коммуникаций описывае-

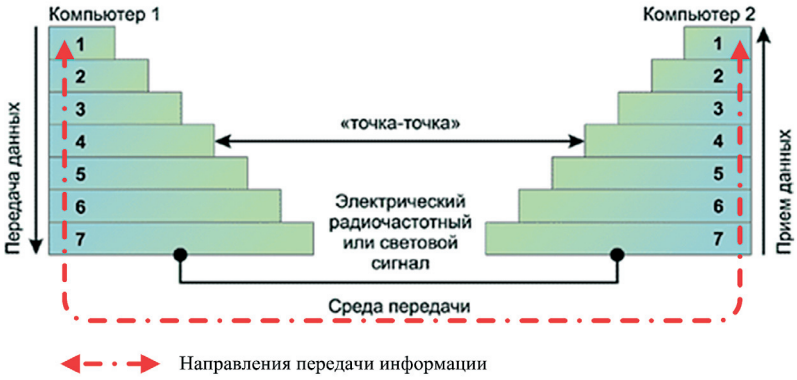

***Рис. 1**. Модель OSI взаимодействия двух сетевых компьютеров*

мые в самом общем случае эталонной моделью взаимодействия открытых систем (Open System Interconnection Reference Model), часто называемой моделью OSI (рис. 1).

Эта модель разработана Международной организацией по стандартизации (International Organization for Standardization, ISO). Модель OSI описывает схему взаимодействия сетевых объектов, определяет перечень задач и правила передачи данных. Она включает в себя семь уровней: физический (Physical — 1), канальный (Data-Link — 2), сетевой (Network — 3), транспортный (Transport — 4), сеансовый (Session — 5), представления данных (Presentation — 6) и прикладной (Application — 7). Считается, что два элемента системы (компьютера) могут взаимодействовать друг с другом на конкретном уровне модели OSI, если их программное обеспечение, реализующее сетевые функции этого уровня, одинаково интерпретирует одни и те же данные. В этом случае устанавливается прямое взаимодействие между двумя элементами сети, называемое "точка-точка".

Реализации модели OSI протоколами называются стеками (наборами) протоколов. В рамках одного конкретного протокола невозможно реализовать все функции модели OSI. Обычно задачи конкретного уровня реализуются одним или несколькими протоколами. На одном компьютере должны работать протоколы из одного стека. При этом компьютер одновременно может использовать несколько стеков протоколов. Модель OSI систематизирует представление об организации сетей и разбивает задачи коммуникаций на более мелкие фрагменты (подзадачи) реализуемые протоколами различных уровней. Конкретные протоколы и стеки протоколов выполняют подзадачи определенных уровней модели OSI.

Модель OSI описывает взаимодействие отдельных компьютеров только в рамках отдельной ИТКС – объекта воздействия. Данная модель не применима для описания взаимодействия средств воздействия и объекта воздействия. В отличие от сетевых структур общего (открытого) доступа, ИТКС органов государственной власти и силовых ведомств являются закрытыми и включают в свой состав неизвестные нарушителю до начала конфликта программные и аппаратные средства и средства защиты информации. В связи с этим существует необходимость создания новой концептуальной модели взаимодействия конфликтующих систем (Conflict System Interconnection Model) которую обозначим CSI. Такая модель должна в самом общем виде описывать две конфликтующие ИТКС и общую физическую среду, через который обеспечивается их взаимодействие (рис. 2). При этом одна ИТКС может рассматриваться как объект воздействия, а другая как создающая воздействия.

Предлагаемая модель CSI базируется на анализе научной и методической литературы по данному вопросу и позволяет обобщить известные модели программно-технических и радиоэлектронных воздействий на различные элементы современных информационных и телекоммуникационных систем.

В ИТКС выступающей в роли объекта воздействия необходимо рассматривать следующие составные части:

- подсистему взаимодействия элементов ИТКС, построенную на некотором стеке протоколов, и в достаточно общем виде представляемую, моделью OSI;
- подсистему защиты информации;
- подсистему управления и решения целевых задач ИТКС.

Фактическая работа объекта воздействия осуществляется для нарушителя априорно неизвестным программным и аппаратным обеспечением.

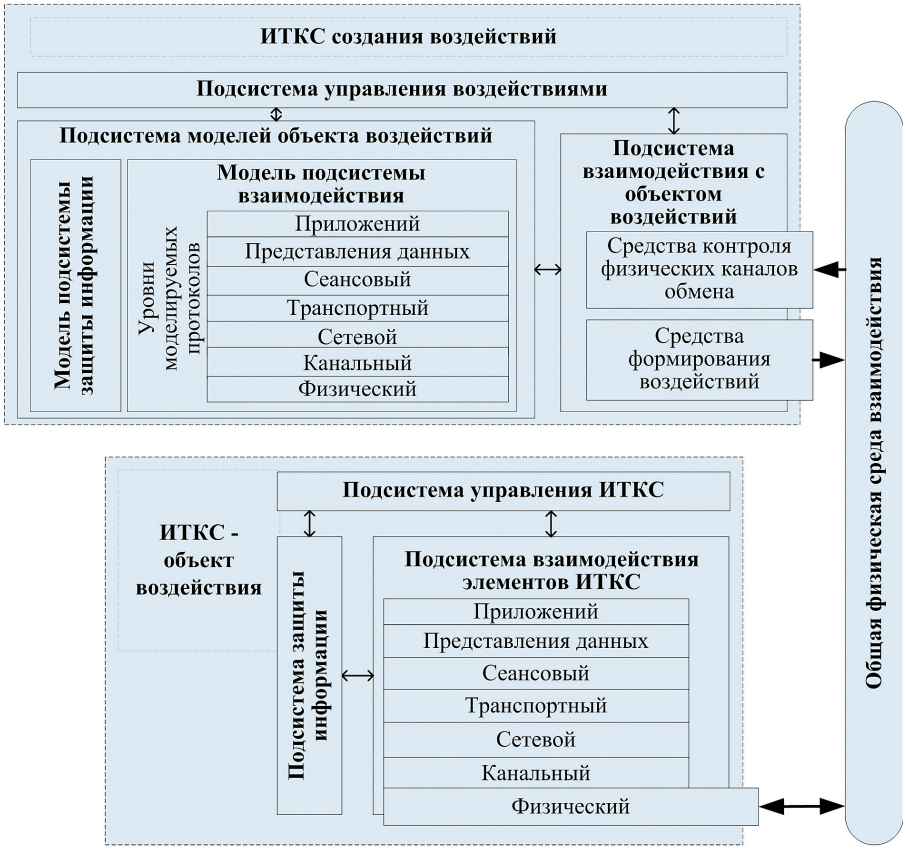

***Рис. 2**. Обобщенная модель взаимодействия конфликтующих систем – CSI*

При этом основные протоколы обмена информацией в сетях достаточно полно описаны. Поэтому в процессе подготовки воздействия нарушителю достаточно решать задачи идентификации реализованных в ИТКС стеков протоколов. Соответственно ИТКС, формирующая воздействия и выступающая в роли нарушителя, должна содержать:

- подсистему управления воздействиями;
- подсистему взаимодействия с объектом воздействий;
- подсистему моделей объекта воздействий, включающую подмодели подсистем взаимодействия и защиты информации.

Специфика данной модели заключается в том, что чем более высокого уровня протоколы удается идентифицировать или смоделировать нарушителю, тем более опасные виды воздействий могут создаваться. В самом опасном случае нарушитель может вскрыть все уровни протоколов обмена информацией и конфигурацию системы защиты информации в объекте воздействия. При этом нарушитель может создать виртуальный элемент сети, имитирующий работу легитимного пользователя или узла сети и получить полный доступ к защищаемой системе.

Радиоэлектронные информационные воздействия

Отдельные структурные элементы ИТКС должны быть связаны каналами передачи данных. Для мобильных объектов каналы передачи данных создаются преимущественно с использованием радиосредств. Радиоэлектронная структура ИТКС часто является основным источником сведений при доразведке нарушителем защищенных ИТКС, изолированных от общедоступных сетей. Поэтому в условиях ограниченных возможностей непосредственного доступа нарушителей к объектам в составе ИТКС и ее сетевой инфраструктуре, следует ожидать от нарушителей реализации сравнительно нового вида воздействия на ИТКС в целях прекращения доступа к обрабатываемой информации или ее целенаправленного искажения (подмены) т.е. радиоэлектронного информационного воздействия (РЭИВ).

РЭИВ можно определить следующим образом: – это совокупность согласованных мероприятий (действий) специальных комплексов и средств по добыванию информации о состоянии и порядке функционирования ИТКС – объекте воздействия, и специальным радиоэлектронным воздействиям

на элементы ИТКС и ее информационные ресурсы через каналы радиосвязи и передачи данных с целью нарушения ее функционирования.

Таким образом, РЭИВ по сути является разновидностью радиоэлектронного подавления, однако отличается от последнего следующими основными чертами:

1) объектом воздействия является не приемное устройство конкретного РЭС, а информационная система, использующая данное РЭС в контуре обработки или передачи информации;

2) потенциальный масштаб воздействия не ограничивается локальным (в зоне действия помех) и кратковременным (на время действия помехи) нарушением функционирования РЭС, а ориентируется на нарушение процесса функционирования всей информационной системы в целом;

3) нестрогим совпадением или возможным несовпадением места и времени воздействия с временем и местом его проявления в виде нарушений процесса функционирования информационной системы (например, при реализации отложенных воздействий);

4) бескомпроматностью воздействия на информационную систему (т.е. скрытностью воздействия, которое в ряде случаев достигается имитацией непреднамеренных мешающих помех, избирательным точечным воздействием на устройства выделения и обработки информации в приемниках, оставаясь за рамками возможностей систем контроля электромагнитной обстановки, имитацией функционирования отдельных подсистем и элементов в ИТКС с целью целенаправленного дезорганизующего воздействия на их функционирование и т. д.).

Основные направления разработок в области РЭИВ могут быть связаны с разработкой методов нарушения синхронизации легитимных узлов сети и внедрения ложной информации (дезинформации) от нелигитимных виртуальных элементов ИТКС. Возможные эффекты от применения нарушителем РЭИВ – сбои в протоколах обмена, создание виртуальных элементов ИТКС, внедрение в ИТКС программных закладок. Например, в работах [4-6] рассматриваются эффекты воздействия преднамеренных деструктивных воздействий на элементы ИТКС на канальном, сетевом и транспортном уровнях модели OSI.

РЭИВ для своей успешной реализации требует проведения ряда предварительных действий направленных на контроль радиоканалов в ИТКС-объекте воздействия:

- обнаружение потенциальных объектов информационного воздействия (сигналов в радиоэфире и пространственного положения РЭС);
- вскрытие вида и параметров модуляции сигналов в канале;
- вскрытие процедур вхождения в связь и ее окончания, алгоритмов синхронизации и управления потоками данных;
- вскрытие правил и параметров помехоустойчивого кодирования сигналов, методов и ключей шифрования передаваемой информации (для каналов связи и передачи данных), протоколов канального, сетевого, транспортного и сеансового уровней (для систем связи и передачи данных);
- вскрытие способов многостанционного доступа к общему ограниченному аппаратному ресурсу (например к ретранслятору сигналов);
- вскрытие содержания информации передаваемой в канале связи;
- вскрытие сетевой структуры и используемой конфигурации системы защиты информации.

В зависимости от степени успешности проведения контроля и моделирования протоколов обмена на всех уровнях модели OSI объекта подавления действий на подготовительном этапе реализуются различные по содержанию и эффективности способы РЭИВ. Перечень способов РЭИВ может включать различные по задачам воздействия на ИТКС:

- имитация непреднамеренных мешающих воздействий;
- ретрансляция сигналов с задержкой (ретранслированная помеха);
- имитационная по виду и параметрам сигнала (сигналоподобная) помеха;
- помеха имитирующая вхождения в связь с целью перегрузки диспетчера очередей или сигнал окончания связи для досрочного обрыва связи;
- дезинформирующая помеха (сигналоподобная помеха с ложным информационным сообщением);
- помеха содержащая вредоносный программный агент;
- создание виртуального элемента сети, имитирующего работу легитимного пользователя или узла сети.

Основными направлениями защиты ИТКС от РЭИВ должны быть методы направленные с одной стороны на предотвращение успешного проведения контроля и идентификации протоколов обмена, а с другой стороны на повышение защищенности от уже формируемых нарушителем РЭИВ. Для противодействия контролю со стороны нару-

шителя могут использоваться методы повышения скрытности радиосистем и протоколов передачи данных. Для снижения эффективности уже формируемых нарушителем РЭИВ необходимо обеспечивать помехоустойчивость каналов передачи данных и имитостойкость протоколов обмена данными в стеках протоколов всех уровней. Особенно опасны РЭИВ при наличии в защищаемой ИТКС мобильных сегментов сетей со средствами беспроводного доступа.

Заключение

Таким образом, предложена концептуальная модель взаимодействия конфликтующих систем. Показана возможность применения данной модели как для определения методов создания радиоэлектронных информационных воздействий на ИТКС, так и для обоснования мер защиты от таких воздействий.

Предложенная концептуальная модель может использоваться в учебном процессе при подготовке специалистов в области информационной безопасности. Кроме того, предлагаемый в статье материал может быть полезен при решении задач систематизации разнородных фактов информационных атак на сети и проектировании систем защиты информации для перспективных информационных и телекоммуникационных систем.

Литература

1. Максимов Ю. Н., Паршуткин А. В., Еремеев М. А. и др. Технические методы и средства защиты информации. СПб: Полигон, 2000. –320 с.
2. Паршуткин А. В. Основы оптимизации стохастических воздействий на каналы утечки информации//Проблемы информационной безопасности. Компьютерные системы, - СПб: ГТУ, 1999. № 2. С. 17-24.
3. Паршуткин А. В. Топологический подход к формализации задачи защиты информации в стратегическом управлении //Проблемы информационной безопасности. Компьютерные системы, - СПб: ГТУ, 2001 № 4. С. 28-31.
4. Макаренко С. И. Проблемы и перспективы применения кибернети-ческого оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47.
5. Макаренко С. И., Михайлов Р. Л. Модель функционирования мар-шрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. Т. 12. № 2. 2014. С. 44–49.
6. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. № 3(4). 2014. С. 7-13.
7. Мальцев Г. Н., Вознюк В. В., Туктамышев М. Р. Моделирование конфликта сложных радиотехнических систем методом параллельных развивающихся стохастических процессов // Информационно-управляющие системы, 2013. № 5. С. 26-33.

References

1. Maksimov Y. N., Parshutkin A. V., Eremeev M. A. etc. Tehnicheskie metody i sredstva zashity informacii [Technical Methods and Means of Information Protection]. Saint-Petersburg, Publ.Poligon, 2000. –320 p. (In Russian).
2. Parshutkin A. V. Bases of optimization of stochastic impacts on information leakage channels. Problemy informasionnoy bezopastnosty. Komputernye sistemu, -Saint-Petersburg, GTU, 1999. № 2. C. 17-24. (In Russian).
3. Parshutkin A. V. Topological approach to formalization of a problem of information security in strategic management. Problemy informasionnoy bezopastnosty. Komputernye sistemu, -Saint-Petersburg, GTU, 2001 № 4. C. 28-31. (In Russian).
4. Makarenko S. I. The problems and outlook for the cybernetic weapon employment in the net-centric war. Spectehnika i sviaz, 2011, no. 3, pp. 41-47. (In Russian).
5. Makarenko S. I., Mikhaylov R. L. The model of functioning of the router in the case of limited reliability of communication canals. Infocommunikacionie tehnologii, 2014. no. 2. pp. 44-49. (In Russian).
6. Makarenko S. I. Premeditated formation of the traffic of difficult structure due to implementation in the communication system of additional imitative traffic. Voprosy kiberbezopasnosti, 2014, no. 3(4), pp. 7-13. (In Russian).
7. Maltsev G. N., Voznyuk V. V., Tuktamyshev M.R. Modeling the Conflict of Complex Radio Engineering Systems by the Method of Parallel Developing Stochastic Processes. Informatsionno-upravliaiushchie sistemy, 2013. N 5. P. 26-33.