УДК 621.96: 004.056

С.Л. Емельянов

Одесская национальная юридическая академия, Одесса

ТЕХНИЧЕСКАЯ РАЗВЕДКА И ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Показана взаимосвязь системы технической разведки и возможных технических каналов утечки информации с типового объекта информатизации. Рассмотрена роль и место компьютерной разведки в системе технической разведки.

Ключевые слова: *технические средства разведки, компьютерная разведка, технические каналы утечки информации, объект информатизации.*

Введение

Постановка проблемы. Среди многочисленных информационных угроз объекту информатизации (ОИ) лидирующее положение по данным многочисленных статистических исследований [1] занимают угрозы конфиденциальности информации, при реализации которых информация с ограниченным доступом (ИсОД) становится известной лицам, не имеющим права доступа к ней, т.е. происходит утечка защищаемой информации с ОИ.

Источниками (носителями) ИсОД на типовом ОИ [2] в общем случае являются: люди (персонал); основные и вспомогательные технические средства передачи информации (ТСПИ); документы (в том числе публикации) как в электронном, так и в бумажном виде; продукция (материальные и информационные ресурсы); отходы производственной деятельности; физические поля, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов [3, 4].

В решении актуальной проблемы защиты информации от утечки важное место занимают исследования возможных способов и средств ведения разведки и путей (каналов) утечки информации.

Анализ публикаций. Анализ последних исследований и публикаций показывает, что для стратегических ОИ, где циркулирует секретная (сведения, составляющие государственную или военную тайну) или конфиденциальная информация, являющаяся собственностью государства, основный упор в этих исследованиях делается на анализе принципов построения, функционирования и возможностей системы иностранной технической разведки (ИТР) по добыванию охраняемых сведений на основе выявления и анализа демаскирующих ОИ признаков [5].

Для ОИ, где циркулирует конфиденциальная информация, являющаяся собственностью юридических или физических лиц, основное внимание уделяется анализу возможных физических путей неконтролируемого распространения информации от указанных источников к злоумышленнику (технических каналов утечки информации). Причем в качестве элементов технических каналов утечки информации (ТКУИ) рассматриваются, в основном, портативные технические средства разведки (ТСР) (радиомикрофоны, сетевые закладки, диктофоны, специальные приемники и т.д.) [6].

Однако в [3] отмечается, что по мере ослабления противостояния между Востоком и Западом промышленный шпионаж в работе многих разведок становится приоритетным направлением наряду с политической и военной разведкой, что создает объективные предпосылки для сближения указанных выше направлений исследований. Поэтому в ряде фундаментальных работ, посвященных проблеме защиты информации от утечки [7, 8], авторы сначала рассматривают систему построения и возможности ИТР, а затем проводят анализ возможных ТКУИ, как правило, без учета их взаимосвязи.

Целью статьи является анализ взаимосвязи между системой технической разведки (ТР) и ТКУИ с типового ОИ, а также определение роли и места компьютерной разведки в системе ТР.

Основной материал

Под ТР в общем случае понимается несанкционированное получение охраняемых сведений путем сбора информации техническими средствами и ее анализа [9]. Доля ТСР в общей системе добывания защищаемой информации достаточно велика и, по некоторым оценкам [5], может составлять до 50% и более. Причем дальнейшее развитие науки и техники объективно приводит к повышению роли и значимости ТР [8].

При анализе ТСР используют различные классифицирующие признаки. Например, по месту их размещения выделяют космическую, воздушную, наземную и морскую ТР. Более интересной представляется классификация ТСР по физическому принципу построения ее аппаратуры, в соответствии с которым выделяют следующие виды ТР [5, 7]:

- оптическую;
- оптикоэлектронную;
- радиоэлектронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;
- магнитометрическую.

Сущность и характеристика указанных видов ТР, а также их дальнейшая классификация по подвидам приведена в [5, 7] и показана на рис. 1. Применение тех или иных видов ТСР, их комплексирование и тип возможного носителя зависят от многих случайных факторов: характера, ценности и формы представления разведываемой информации (речевая, видовая, сигнальная и др.), характеристик сопутствующих физических полей и сред, степени защищенности ОИ, его размещения на местности (вблизи государственных границ и иностранных посольств или в глубине страны) и др.

Известно также, что ТКУИ представляет собой совокупность источника (носителя) информации, среды распространения информационных сигналов и технического средства разведки [3, 4, 6 – 9]. В зависимости от физической природы информационных сигналов, а также среды их распространения и способов перехвата все ТКУИ можно классифицировать на [8]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (опасные напряжения и токи в токопроводящих коммуникациях);
- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы, выбросы и т.д.).

Так как ТСР, по определению, является оконечным элементом ТКУИ, то рассмотренные классификации ТСР и ТКУИ по физическим принципам, лежащим в их основе, являются жесткокоррелированными. Иначе говоря, каждому виду ТР соответствует один или несколько ТКУИ, и наоборот (рис. 1). Например, радиоэлектронная разведка может добывать информацию по радиоканалу и электрическому каналу утечки информации. Акустический канал утечки информации используется акустической и гидроакустической разведками и т.д.

Заметим, что в последнее время на многих ОИ для обработки ИсОД широкое применение находят компьютерные системы и сети (КСС). В связи с этим приобрела широкий размах и деятельность по гласному и негласному добыванию информации из открытых и закрытых КСС, баз и банков данных, контролю за сообщениями, передаваемыми в вычислительных сетях, получению персональных данных пользователей КСС и другой ценной компьютерной информации. Для характеристики подобной деятельности стали широко использоваться термины: «компьютерный шпионаж», «компьютерная разведка», «информационно-аналитическая работа в Интернет», «аналитическая разведка» и др.

Большинство авторов [5, 7], опираясь на определение технической разведки как способа добывания информации с помощью технических средств, небезосновательно относят КР к одному из видов технической разведки. В нормативном документе РФ [2] КР также рассматривается как один из методов доступа к защищаемой информации с применением технических средств разведки.

Следуя изложенному выше подходу, можно предположить, что КР должна иметь собственный (отдельный) ТКУИ. Поэтому, например, в работе [10] автор трактует КР как метод добывания информации путем перехвата и анализа побочных электромагнитных излучений и наводок (ПЭМИН) средств ЭВТ, т.е. рассматривает ее как разновидность радиоэлектронной разведки, которая, в свою очередь, является одним из видов ТР.

Если исходить из классического определения канала утечки, как канала передачи информации в виде: **источник→физическая среда→получатель** [6 – 9], то технический канал утечки компьютерной информации формально может рассматриваться как самостоятельный канал утечки, поскольку он имеет все указанные элементы. Источник информации здесь КСС, среда (тракт) распространения – телекоммуникационные линии связи (нижние физический и канальный уровни модели открытых систем OSI [11]), получатель информации – другие государства, отдельные юридические или физические лица, добывающие ИсОД с объекта информатизации путем бесконтактного проникновения в КСС.

Однако, существует и другое мнение [8] о нецелесообразности выделения явлений, приводящих к утечке информации из КСС, в отдельную группу, образующую самостоятельный технический канал утечки информации, поскольку многие из них при более детальном рассмотрении могут быть приведены к одному из описанных ТКУИ, например, электромагнитному или материально-вещественному.

На наш взгляд, сущность КР заключается в добывании [12]:

– компьютерной информации, обрабатываемой, хранимой и передаваемой в КСС;

– данных и сведений о характеристиках (параметрах) программных, аппаратных и программно-аппаратных комплексов, применяемых в КСС;

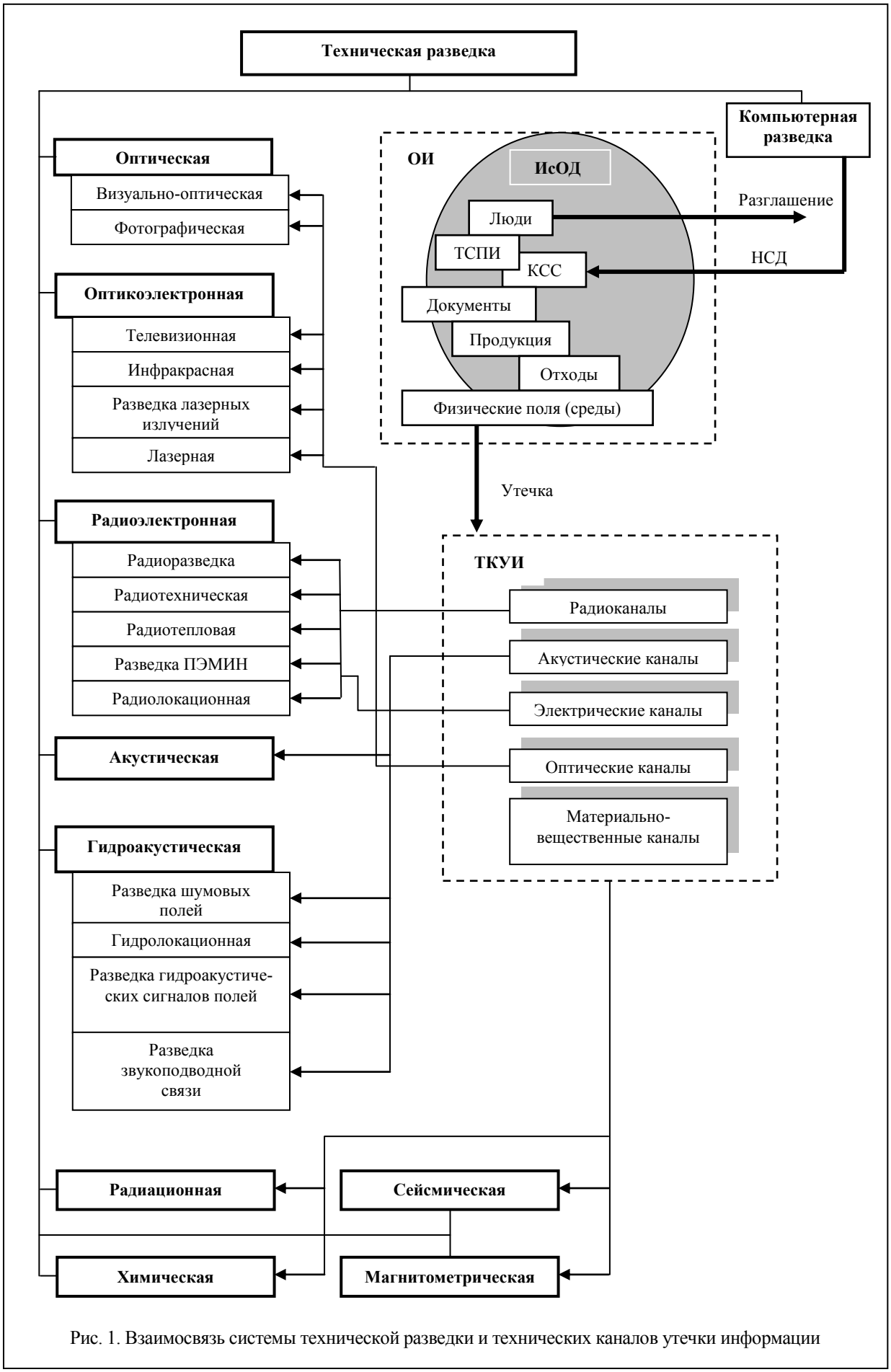

Рис. 1. Взаимосвязь системы технической разведки и технических каналов утечки информации

– данных и сведений о применяемых в КСС методах, способах и механизмах защиты информации;

– персональной информации о пользователях КСС.

Исходя из сущности КР, следует, что она не привязывается к физическим полям и сигналам (не является видовой или сигнальной) в отличие от других способов ведения технической разведки.

Основным методом ведения КР является несанкционированный доступ (НСД) к компьютерной информации, циркулирующей в КСС. Способы бесконтактного НСД в КСС основаны на использовании недостатков языков программирования, наличии уязвимостей (брешей, «люков», «дыр» и т.д.) в штатном программном обеспечении (ПО) КСС и применении специального ПО, называемого атакующим [13]. Его применение, как правило, предполагает работу на более высоких уровнях упомянутой модели OSI (транспортном и сетевом, сеансовом и представительском, прикладном).

Выводы

1. Техническая разведка и технические каналы утечки информации жестко взаимосвязаны по физическим принципам, лежащим в их основе.

2. Компьютерная разведка является относительно новым и самостоятельным видом технической разведки, добывающим компьютерную информацию на основе бесконтактного НСД к КСС.

3. Предложенный подход согласуется с известными путями утечки информации с типового объекта информатизации [3, 4, 8, 9] за счет: разглашения информации персоналом; технических каналов утечки информации; НСД к источникам (носителям) информации.

Список литературы

1. Скиба В.Ю. Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.А Курбатов.– СПб.: Питер, 2008. – 320 с.

2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р51275-99. – [Действительный от 01.01.2000]. – (Государственный стандарт России).

3. Защита информации. Основные термины и определения: ГОСТ Р50922-96. – [Действительный от 01.01.1997]. – (Государственный стандарт России).

4. Ярочкин В. И. Информационная безопасность: учебник для студентов вузов / В. Ярочкин. – 2 -е изд. – М.: Академический Проект, Гаудеамус, 2004. – 544 с.

5. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки / Ю.К. Меньшаков. – М.: Российск. гос. гуманит. ун-т, 2002. – 399 с.

6. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие / А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

7. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

8. Хорошко В.А. Методы и средства защиты информации / В.А Хорошко, А.А. Чекатков. – Юниор, 2003. – 504 с.

9. Защита информации. Техническая защита информации. Термины и определения. (ДСТУ 3396.2-97) .– [Действительный от 01.07.1997]. – (Национальный стандарт Украины).

10. Ржавский В.К. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: учебное пособие / В.К. Ржавский. – Волгоград: ВолГУ, 2002. – 122 с.

11. Протоколы информационно-вычислительных сетей: справочник / Под общ. ред. И. А. Мизина, А.П. Кулешова. – М.: Радио и связь,1990. – 504 с.

12. Емельянов С.Л. Компьютерная разведка как способ несанкционированного доступа к компьютерной информации / С.Л. Емельянов // Збірник тез V Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології-COMINFO'2009», 05 – 09 жовтня 2009 р. – К.: ДУІКТ. – С. 190-191.

13. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2000. – 384 с.

Поступила в редколлегию 23.03.2010

Рецензент: д-р техн. наук, проф. В.А. Лужецкий, Винницкий национальный технический университет, Винница.

ТЕХНІЧНА РОЗВІДКА ТА ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

С.Л. Ємельянов

Показано взаємозв'язок системи технічної розвідки та можливих технічних каналів витоку інформації з типового об'єкту інформатизації. Розглянуто роль та місце комп'ютерної розвідки в системі технічної розвідки.

Ключові слова: *Технічні засоби розвідки, комп'ютерна розвідка, технічні канали витоку інформації, об'єкт інформатизації.*

TECHNICAL INTELLIGENCE AND TECHNICAL CHANNELS OF LEAK INFORMATION

S.L. Emelyanov

Intercommunication of the technical intelligence service system and possible technical channels of leak information from the typical object of informatization is shown. The role and place of computer intelligence service is considered in the system of technical secret service.

Keywords: *technical intelligence hardware, computer intelligence service, technical channels of leak information, object of informatization.*