УДК 681.3:519.1

ОБ ОСОБЕННОСТЯХ НЕКОТОРЫХ ОСНОВАНИЙ ПРИ КЛАССИФИКАЦИИ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

С.В. Скрыль, В.С. Зарубин, В.В. Киселев, В.Н. Финько

Обосновывается ряд классификаций угроз нарушения целостности информации в информационно-телекоммуникационных системах (ИТКС) по различным основаниям. Приводится соответствующие классификационные схемы

Ключевые слова: информационно-телекоммуникационные системы, угрозы нарушения целостности информации, классификационные схемы угроз нарушения целостности информации в ИТКС

В соответствии с существующими взглядами на проблемы развития информационных технологий /1 - 3/ одним из важнейших свойств информации при ее обработке и обмене в информационно-телекоммуникационных системах (ИТКС) является свойство целостности. Согласно /4/ «Целостность информации - это свойство информационной технологии обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок».

Практика эксплуатации современных ИТКС убедительно доказывает, что нарушение свойства целостности информации в этих системах приводит к их неработоспособности /5/. Отсюда весьма актуальной становится проблема классификации угроз нарушения целостности информации в ИТКС с целью выработки эффективных мер противодействия подобного рода нарушениям.

Угрозы нарушения целостности информации в ИТКС принято делить на случайные (непреднамеренные) и умышленные (преднамеренные). Источником первых могут быть ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей или администрации сети и т.п. Умышленные угрозы, в отличие от случайных, преследуют цель нанесения ущерба пользователям (абонентам) ИТКС. В отличие от широко распространенных угроз информационной безопасности – угроз нарушения конфиденциальности информации, которые бывают как активными, так и пассивными угрозы нарушения целостности информации в ИТКС только активны и имеют цель нарушения нормального процесса их функционирования посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. Источниками таких угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п. /6/.

В зависимости от местонахождения источника угрозы нарушения целостности информации в ИТКС делятся на две группы: внешние и внутренние. К внешним угрозам относятся:

- деятельность иностранных разведывательных и специальных служб;
- деятельность конкурирующих иностранных экономических структур;
- деятельность политических и экономических структур, преступных групп и формирований, а также отдельных лиц внутри страны, направленная против интересов граждан, государства и общества в целом и проявляющаяся в виде воздействий на ИТКС;
- стихийные бедствия и катастрофы.

Скрыль Сергей Васильевич – МГТУ им. Н.Э. Баумана, профессор кафедры ИУ-10, д-р техн. наук, профессор тел. (495) 632-22-47

Зарубин Владимир Сергеевич - Воронежский институт МВД России, начальник кафедры технических систем безопасности и связи, канд. техн. наук, доцент, тел. 89102473470

Киселев Вадим Вячеславович – Воронежский институт МВД России, канд. техн. наук, кафедра технических систем безопасности и связи, старший преподаватель, тел. 70-63-76

Финько Владимир Николаевич - Воронежский институт МВД России, канд. техн. наук, соискатель, тел. 70-63-76

К внутренним угрозам ИБ относятся:

- нарушения установленных требований по информационной безопасности (непреднамеренные либо преднамеренные) допускаемые обслуживающим персоналом и пользователями ИТКС;

- отказы и неисправности технических средств обработки, хранения и передачи сообщений (данных), средств защиты и средств контроля эффективности принятых мер по защите, сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности принятия мер по защите.

По способу реализации угрозы нарушения целостности информации в ИТКС подразделяются на следующие виды:

- организационные;
- программно-математические;
- физические;
- радиоэлектронные.

К *организационным* угрозам относятся:

- нарушения установленных требований по информационной безопасности, допускаемые обслуживающим персоналом и пользователями ИТКС;

- несанкционированный доступ обслуживающего персонала и пользователей ИТКС к информационным ресурсам;

- манипулирование информацией (дезинформация, скрытие или искажение информации);

- уничтожение или модификация данных в ИТКС.

К *программно-математическим* угрозам относятся:

- внедрение программ-вирусов;

- применение программных закладок.

К *физическим* угрозам относятся:

- уничтожение, разрушение средств сбора, обработки, передачи защиты информации, целенаправленное внесение в них неисправностей;

- уничтожение или разрушение машинных носителей информации;

- воздействие на обслуживающий персонал и пользователей ИТКС с целью реализации физических, программно-математических или организационных угроз.

К *радиоэлектронным* угрозам относятся:

- навязывание ложной информации в сетях передачи данных и линиях связи;

- радиоэлектронное подавление линии связи, дезорганизация систем управления ИТКС.

На рис. 1 представлены наиболее часто встречаемые угрозы воздействия на канал связи.

Взаимосвязь различных видов угроз безопасности информации с видами нарушений и последствий, к которым они приводят, представлены на рис. 2.

То обстоятельство, что ИТКС строятся на технологической платформе компьютерных сетей обусловливает необходимость рассмотрения информационных процессов в этих системах с учетом взаимосвязи отдельных элементов. Инструментом описания таких взаимосвязей является эталонная модель взаимосвязи открытых систем (ЭМ ВОС), в соответствии с которой взаимодействие элементов ИТКС представляются на физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном уровнях /5/.

Поэтому важна классификация угроз нарушения целостности информации в ИТКС и в рамках указанной архитектуры.

В таблице 1 показано, на какие уровни эталонной модели взаимосвязи открытых систем воздействуют основные угрозы нарушения целостности информации в ИТКС (1 - физический, 2 - канальный, 3 - сетевой, 4 - транспортный, 5 - сеансовый, 6 - представительный, 7 - прикладном). Рассмотренные классификации позволяют выявить причинно-следственные связи между факторами, возникновения и реализации угроз нарушения целостности информации в ИТКС и позволяют корректно обосновать способы противодействия подобного рода угрозам.

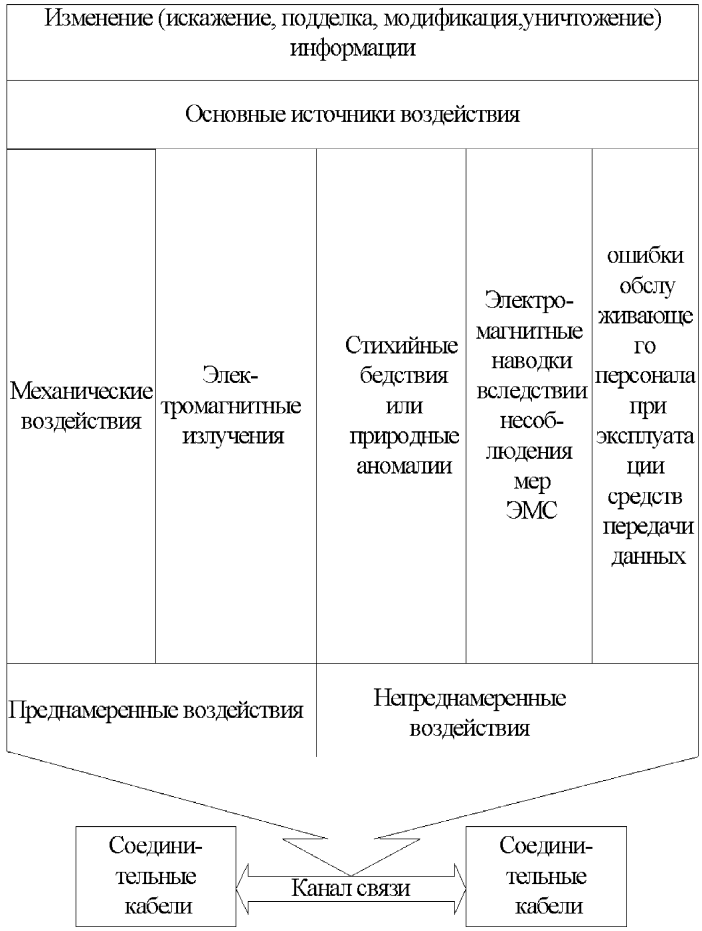

Рис. 1.

Факторы негативного влияния на информацию			
Внешние		Внутренние	
Искусственные			
Преднамеренные		Непреднамеренные	
Вредоносное программное обеспечение	Вложенные дефекты программного и аппаратного обеспечения	Неправомерные действия	Ошибки в работе
Разрушение информации		Искажение информации	
Несанкционированный доступ			
Нарушение целостности информации			
Нарушение безопасности информации			
Потеря работоспособности ИТКС			

Рис. 2

Таблица 1

Угрозы безопасности информации	Уровни ЭМ ВОС						
	1	2	3	4	5	6	7
стихийные бедствия	+	+	+	+	+	+	+
электромагнитные бури	+	+	+	+	+	+	+
радиоподавление линий связи	+	+					
компьютерные вирусы					+	+	+
специальные программно-технические воздействия			+	+	+	+	+
встроенные дефекты			+				
разрушение	+	+	+	+	+	+	+
подделка			+				+
неправомерные действия					+	+	+
ошибки в работе							+
задержки информации	+	+	+	+	+		
информационное подавление						+	+
ПЭМИН	+	+				+	

ЛИТЕРАТУРА

1. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. – М.: Издательский дом «Парад», 2005. – 392 с.

2. Информатика: учебник для высших учебных заведений МВД России. Том 1. Информатика: Концептуальные основы / С.В. Скрыль [и др.]. - М.: Маросейка, 2008. – 464 с.

3. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты): монография / С.В. Скрыль [и др.]. – Орел: Орловский юридический институт МВД России, 2005. – 192 с.

4. Основы информационной безопасности: учебник для высших учебных заведений МВД России / Под ред. В.А. Минаева и С.В. Скрыля – Воронеж: Воронежский институт МВД России, 2001. – 464 с.

5. Информационная безопасность телекоммуникационных систем (технические вопросы): Учебное пособие для системы высшего профессионального образования России / И.В. Новокшанов, С.В. Скрыль [и др.]. – М.: Радио и связь, 2004. – 388 с.

6. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.].. – М.: Горячая линия-Телеком, 2006. – 536 с.

Московский государственный технический университет им. Н.Э. Баумана
The Moscow State Technical University n. N.E. Bauman

ABOUT FEATURES OF SOME BASIS AT CLASSIFICATION OF THREATS OF VIOLATION OF INFORMATION INTEGRITY IN INFORMATION-TELECOMMUNICATION SYSTEMS

S.V. Skryl', V.S. Zarubin, V.V. Kiselev, V.N. Finko

A number of classifications of threats of infringement of integrity of the information in informational -telecommunication systems on the various bases is proved. It is resulted corresponding classification circuits

Key words: informational-telecommunication systems, threats of infringement of integrity of the information, classification circuits of threats of infringement of integrity of the information in informational-telecommunication systems