значений бит, фазовое кодирование, расширение спектра за счет изменения времени задержки эхо-сигнала, маскирования ЦВЗ.

Из различных возможных методов встраивания информации в видеопоследовательности наибольшее распространение получили следующие три группы методов: встраивание информации на уровне коэффициентов дискретных преобразований, встраивание информации на уровне битовой плоскости и методы дифференциального энергетического встраивания [4]. Следует отдельно отметить последний из них, отличающийся от других лучшей устойчивостью к различным последующим преобразованиям самих видеоданных, таких как сжатие, фильтрование и т. п.

Круг задач защиты авторского права, решаемых с помощью ЦВЗ, постоянно расширяется. Так, появились алгоритмы встраивания ЦВЗ в интернет-радиовещании. Крупнейшие производители программного обеспечения начинают предоставлять свои продукты с возможностями встраивания в аудиофайлы ЦВЗ для решения проблем, связанных с пиратством [5].

При наличии достаточной правовой поддержки цифровые водяные знаки могут стать наиболее эффективным инструментом для защиты авторских прав на аудио- и видеопродукцию.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ларичев В. Д., Трунцевский Ю. В.* Защита авторского права в аудиовизуальной сфере. Уголовно-правовой и криминалистический аспекты. М.: Дело, 2004. — 352 с.
2. *Chun-Shien Lu.* Steganography and digital watermarking techniques for protection of intellectual property. Idea Group Publishing, 2005.
3. *Грибунин В. Г., Оков И. М., Турищев И. В.* Цифровая стеганография. М.: Салон-Пресс, 2002. — 272 с.
4. *Cassuto Y., Lustig M., Mizrachyy S.* Real-time digital watermarking system for audio signals using perceptual masking. Signal and Image Processing Lab, Faculty of EE. URL: http://www-sipl.technion.ac.il/.
5. Digital Audio Watermarking. Technical Pre-release / Prototype Product Overview. Microsoft Corporation, 2006. URL: http://download.microsoft.com/download/d/6/b/d6bde980-5568-4926/_audio_watermark.

М. Н. Даннави
Московский технический университет связи и информатики

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ DOS В СЕТЯХ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Рассматриваются угрозы DoS в ОКС-7, вызванные фальсификацией сообщений обновления маршрутизации, реализация которых может нанести серьезный урон функционированию сетей связи общего пользования.

Вопросы информационной безопасности (ИБ) в сетях связи общего пользования обладают высокой важностью [1]. Фальсификация злоумышленником некоторых сообщений обновления маршрутизации в системе общеканальной сигнализации ОКС-7 может вызвать нарушение функционирования сетей связи общего пользования вплоть до вывода из строя части сети ТфОП, GSM и интеллектуальной сети (IN) [2, 3]. Возможность отсутствия механизмов защиты от таких угроз или несовместимость этих механизмов в ОКС-7 разных производителей показывают

актуальность анализа уязвимостей информационной безопасности. Наибольший ущерб наносит фальсификация следующих сообщений обновления маршрутизации сетевого уровня ОКС-7:

- недоступность подсистемы пользователя «UPU (User Part Unavailable)»;
- запрещение переноса сигнального трафика «TFP (Transfer Prohibited)»;
- доступ к подсистеме запрещен «SSP (Subsystem Prohibited)».

На примере гипотетической схемы ОКС-7 (Рис. 1) приводится описание угроз от фальсификации этих сообщений, включая последствия от их реализации в сетях связи общего пользования. Анализ этих угроз кратко может быть сведен к следующему:

1. Угрозам DoS ОКС-7 потенциально подвержены как абоненты фиксированной сети ТфОП/ISDN, так и пользователи мобильных станций сети GSM.

2. Угрозы DoS ОКС-7 проявляются при фальсификации сообщений обновления маршрутизации подсистемы MTP3 сетевого уровня.

3. Реализация угроз DoS ОКС-7 может иметь место в результате фальсификации сообщений обновления маршрутизации между всеми смежными пунктами сигнализации.

4. Нарушению маршрутизации от воздействия угроз DoS ОКС-7 подвержены пункты сигнализации ОКС-7, смежные с пунктом сигнализации, который является источником фальсифицированных сообщений обновления маршрутизации.

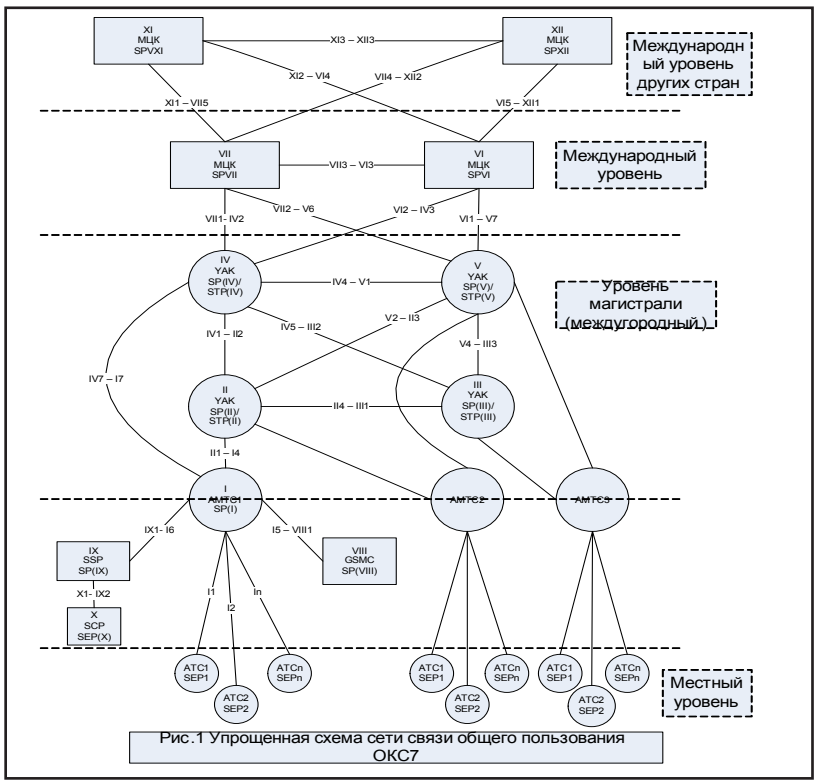

Рис. 1. Гипотетическая схема ОКС-7

Местом локализации при тестировании, а также местом защиты от воздействия угрозы являются эти пункты сигнализации.

5. Нарушению маршрутизации от воздействия фальсифицированных сообщений подвергаются также пункты сигнализации, которые не являются смежными с указанными выше в п. 4 пунктами сигнализации. Однако эти пункты сигнализации не позволяют обеспечить защиту от угроз DoS ОКС-7 пункта сигнализации — источника угроз.

6. Особенностью реализации угроз DoS ОКС-7 в результате фальсификации указанных подсистем MTP3 и SCCP является высокое значение риска, который отражается одновременно

на большом числе пользователей сетями ОП. Под термином «риск» понимается последствие реализуемых угроз ИБ [1, 2].

7. Риск при реализации угроз DoS ОКС-7 в результате фальсификации указанных сообщений подсистем МТР3 отражается на пользователях сетями ОП (ТфОП/ISDN, GSM, IN) в части:

- отказа в установлении соединения;
- отказа в предоставлении всех или определенных услуг интеллектуальной сети;
- ухудшения качества обслуживания.

8. Риск при реализации угроз DoS ОКС-7 может относиться к следующим соединениям:

а) в ТфОП/ISDN — международным, междугородним или местным;

б) в GSM — внутри одного региона страны, между разными регионами страны, между мобильными абонентами разных стран;

в) между абонентами ТфОП/ISDN и абонентами GSM;

г) в сети GSM мобильных абонентов домашней сети и абонентов-роумеров.

9. Заинтересованными в защите от угроз DoS ОКС-7 являются [3]:

- пользователи в отношении доверия к сети и услугам, предоставляемым конкретным оператором/поставщиком услуг;
- операторы сетей и поставщики услуг в обеспечении защиты своих эксплуатационных и коммерческих интересов, в выполнении своих обязательств перед населением;
- органы государственной власти в выполнении директив и законов, с тем чтобы обеспечить готовность предоставления услуг и добросовестную конкуренцию.

СПИСОК ЛИТЕРАТУРЫ:

1. *Драйберг Ли, Хьюитт Джефф.* Система сигнализации № 7 (SS7/ОКС7) протоколы, структура и применение. М.: Вильямс, 2006.
2. *Бельфер Р. А., Горшков Ю. Г.* Система сигнализации ОКС-7. Требования к QoS и организация программного обеспечения сетевого уровня. Учебное пособие МТУСИ. М.: ООО «Информсвязьиздат», 2007.
3. *Бельфер Р. А., Горшков Ю. Г., Даннави М. Н.* Алгоритмы в сетях связи общего пользования России // Электросвязь. 2008. № 8.

Н. В. Дмитриенко, А. И. Труфанов,
Иркутский государственный технический университет,
Р. Е. Лапорт, Ф. Ю. Линькова,
Университет г. Питтсбурга, Пенсильвания, США,
Е. В. Шубников
НИИ терапии, Сибирское отделение Российской Академии медицинских наук, Новосибирск

АРХИТЕКТУРА СВЯЗЕЙ УЧАСТНИКОВ ПРОЕКТА SUPERCOURSE И АНАЛИЗ ЕЕ УЯЗВИМОСТИ

Выполнен анализ связей в рамках интернет-проекта Supercourse. Исследованы топология и динамика сети, определены параметры, важные для понимания развития сети и ее безопасности.