Потенциальные угрозы для сетей специального назначения

Б.С. ГОЛЬДШТЕЙН, зав. кафедрой СПбГУТ, доктор технических наук, профессор,
Н.А. СОКОЛОВ, главный научный сотрудник ЛО ЦНИИС, доктор технических наук

Исторически сложившимся научным центром по проблематики безопасности сетей связи всегда был и остается С.-Петербург с его научными центрами — СПбГУТ им. проф. М.А. Бонч-Бруевича, ЛОНИИС, "Красная заря", НИИДС и др. Эта работа проводилась сначала для ОГСТфС (Общегосударственной сети телефонной связи), потом для ЕАСС (Единой автоматизированной сети связи), ВСС (Взаимоувязанной сети связи), ЕСЭ (Единой сети электросвязи). Сегодня, по известным причинам, проблематике безопасности ЕСЭ РФ и построенных на ее основе сетей специального назначения связисты уделяют особое внимание. Поэтому редакция посчитала интересным попросить высказаться на эту тему своих постоянных авторов, участвовавших в системных проектах всех вышеупомянутых поколений отечественных сетей связи и в исследовании сетевых аспектов построения перспективных сетей связи различного назначения.

Введение

Термины "угроза", "безопасность" и им подобные все чаще встречаются в публикациях отечественных и зарубежных специалистов. Возникающие риски проявляются практически во всех сферах жизни современного общества, но особо критичны они для безопасности государства [1], под которой обычно понимается уровень его защищенности от внешних и внутренних угроз. С этой точки зрения актуальными становятся задачи устойчивого и безопасного функционирования современных сетей специального назначения (ССН). Для сетей подобного рода потенциальные угрозы уместно классифицировать по виду основных источников преднамеренного воздействия:

пользователи сети, включая эксплуатационный персонал;

программное обеспечение (ПО);

аппаратные средства (АС).

Для большинства ССН хорошо разработаны механизмы практического исключения (теоретически — радикальной минимизации) влияния источников первого вида. По этой причине ниже рассматриваются потенциальные угрозы, обусловленные преднамеренными воздействиями через программные продукты и аппаратные средства.

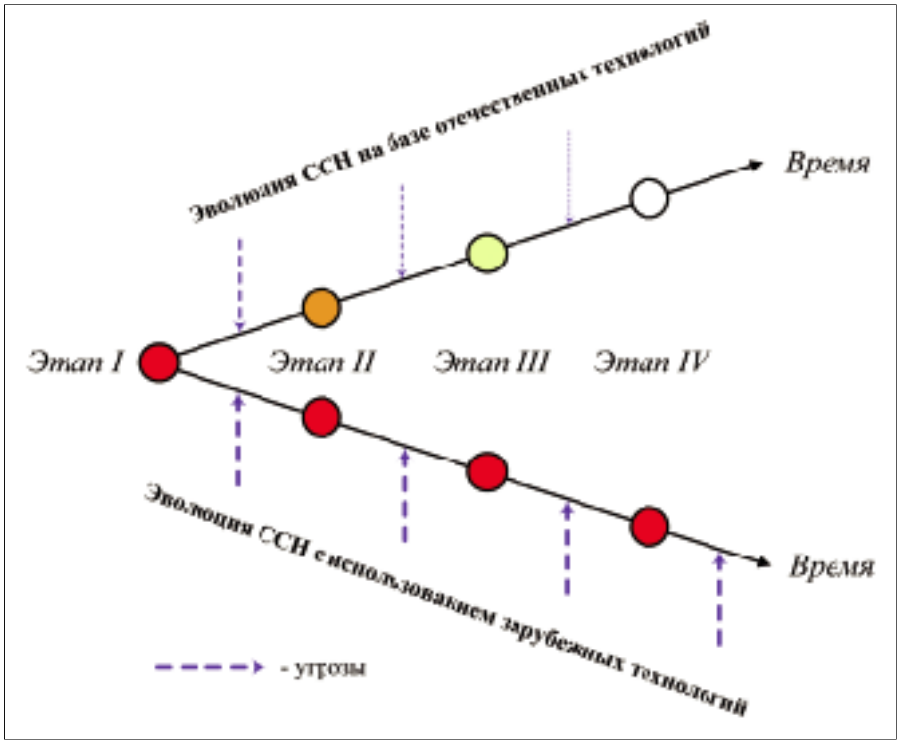

Рис. 1. Два основных сценария развития ССН

Сценарии создания и развития ССН

Создание и поэтапная эволюция ССН могут осуществляться по двум базовым сценариям. Эти сценарии иллюстрирует рис. 1 для четырех этапов эволюции ССН. Первый сценарий подразумевает эволюцию ССН с использованием зарубежных технологий и, как правило, технических средств. Второй сценарий основан на дальнейшем развитии ССН с поэтапным переходом на отечественные технологии, что подразумевает постепенное замещение импортного оборудования передачи, коммутации и обработки информации. Предложенную иллюстрацию следует рассматривать как формализованную схему развития ССН. Тем не менее, она позволяет изложить основные соображения, которым посвящена данная статья.

Динамика первого сценария в чем-то похожа на движение по дороге с заминированными участками. С ростом времени сложность мин замедленного действия (например, закладок в составе ПО) повышается. Их обнаружение носит вероятностный характер. В некоторых случаях принципы обнаружения мин определенного типа (как и ранее — закладок в составе ПО) могут быть разработаны после первого взрыва (проявление действия закладки). Поскольку технология минирования (скрытости закладок) постоянно совершенствуется, на всех этапах