БЕЗОПАСНОСТЬ ТРАНСПОРТНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ КАК ОСНОВА УСТОЙЧИВОСТИ СИСТЕМЫ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Федоренко В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Утин Л.Л. – канд. тех. наук

Аннотация. Ведущие развитые страны активно развивают сети связи специального назначения, функционирующие в интересах органов государственной власти, безопасности государства и обеспечения правопорядка. Основными мировыми тенденциями развития этих сетей является использование в них ресурсов сетей электросвязи общего пользования, а также коммерческих протоколов связи.

В настоящее время информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Республики Беларусь, обеспечение устойчивого и бесперебойного функционирования ее информационной инфраструктуры, в первую очередь критической, является важнейшей государственной задачей.

Появление и стремительный рост новых вызовов и угроз в информационной сфере обусловливают необходимость повышения защищенности транспортной телекоммуникационной сети, и как следствие, всей системы связи Вооруженных Сил. В качестве телекоммуникационной основы системы связи Вооруженных Сил Республики Беларусь в настоящее время используются ресурсы сети электросвязи общего пользования (далее – СЭОП).

СЭОП представляет собой комплекс взаимодействующих сетей электросвязи различных операторов связи, характеризуется широкой географической разветвленностью, способностью предоставления самого широкого спектра услуг связи. При этом СЭОП имеет подсоединение к сетям связи общего пользования иностранных государств и фактически является частью глобальной мировой телекоммуникационной системы.

Широкое использование в СЭОП иностранного телекоммуникационного оборудования и программного обеспечения, содержащего уязвимости и недекларированные возможности, создает потенциальную угрозу внешнего вмешательства в функционирование сети, в том числе:

– нарушение штатного функционирования средств сети электросвязи;
– изменение маршрута сообщения, заданного в нем или в системе коммутации сети связи;
– смещение по времени, переупорядочение сообщений при их обработке, хранении и передаче;
– повтор передачи (в том числе множественный) уже переданного сообщения;
– изменение контента сообщений;
– блокировку передачи, уничтожение сообщения;
– передачу копий сообщений в пункты сбора информации спецслужб иностранных государств;
– вскрытие архитектуры и топологии сети, характеристик ее компонентов;
– вмешательство в работу средств защиты информации, вплоть до их полного выключения;
– внедрение вредоносных программ и создание уязвимостей;
– изменение и создание ложных конфигураций и состояний сети связи;
– проведение сетевых компьютерных атак.

При этом непосредственными объектами, подверженными влиянию активных и пассивных деструктивных воздействий, являются сетевые механизмы, протоколы и интерфейсы, алгоритмы функционирования активного телекоммуникационного оборудования.

Таким образом, телекоммуникационные ресурсы СЭОП в настоящее время являются существенным и одновременно наиболее уязвимым объектом системы связи Вооруженных Сил Республики Беларусь, функционирование которой в любое время может быть дезорганизовано действиями иностранных государств.

Список использованных источников:

1. Макаренко С. И., Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. №2. С. 113-164.

2. Старовойтов А. В., Безопасность телекоммуникационной инфраструктуры как основа устойчивости критической информационной инфраструктуры России // Информационные технологии и цифровая экономика. 2015. № 3. С. 77-79.