БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ КАК ОСНОВА УСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИИ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР МЕЖДУНАРОДНОГО ЦЕНТРА ПО ИНФОРМАТИКЕ И ЭЛЕКТРОНИКЕ (ИНТЕРЭВМ), ПРЕЗИДЕНТ ФГАНУ ЦИТиС
Александр Владимирович Старовойтов

В условиях формирования современного информационного общества, перехода к цифровой экономике, когда информационные технологии становятся неотъемлемой частью всех сфер деятельности личности, общества и государства, а информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации, обеспечение устойчивого и бесперебойного функционирования ее информационной инфраструктуры, в первую очередь критической, является важнейшей государственной задачей.

Немаловажным фактором, требующим принятия безотлагательных мер по обеспечению устойчивости функционирования информационной инфраструктуры Российской Федерации, является разворачивающаяся в настоящее время против России гибридная война, характеризующаяся целенаправленностью и высокой динамикой перехода гибридных угроз из категории потенциальных в реально действующие, проявляющиеся в виде усиления глобального информационного противоборства, совершенствования форм противоправной деятельности в высокотехнологичной кибернетической сфере.

Появление и стремительный рост новых вызовов и угроз в информационной сфере обусловливают необходимость повышения защищенности информационной инфраструктуры Российской Федерации. При этом одной из самых серьезных угроз безопасности Российской Федерации являются активизация деятельности иностранных технических разведок, а также создание ведущими западными странами средств ведения наступательных операций в информационном пространстве и готовность к их применению.

В соответствии с Федеральным законом от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» критическая информационная инфраструктура Российской Федерации включает информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления объектов критической информационной инфраструктуры, в том числе функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, в банковской сфере и иных сферах финансового рынка, топливно-энергетическом комплексе, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

В качестве телекоммуникационной основы критической информационной инфраструктуры Российской Федерации в настоящее время используют ресурсы сети связи общего пользования Российской Федерации (далее – ССОП).

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

Особенность конфигурации ССОП, а именно наличие магистральных линий и сетевых узлов, расположенных за границей Российской Федерации (Амстердам, Лондон, Стокгольм, Франкфурт-на-Майне, Гонконг, Тбилиси и др.), с учетом использования современных протоколов

и технологий маршрутизации информационного трафика, основанных на анализе загруженности тех или иных направлений связи в ССОП, создает потенциальные условия для перенаправления российского внутреннего трафика на зарубежные сетевые узлы – «ловушки» с имитируемым высоким качеством обслуживания.

Широкое использование в ССОП иностранного телекоммуникационного оборудования и программного обеспечения, содержащего уязвимости и недекларированные возможности, создает потенциальную угрозу внешнего вмешательства в функционирование сети. Ситуация усугубляется тем, что операторы ССОП широко используют практику аутсорсинга эксплуатации своих сетей, передавая управление сетями компаниям (в том числе и зарубежным), тесно связанным с иностранными производителями телекоммуникационного оборудования.

Использование на транспортном уровне и уровне доступа ССОП активного телекоммуникационного оборудования и программных средств иностранного производства, не прошедших специальные исследования и специальные проверки, предоставляет техническим разведкам иностранных государств, имеющим доступ к заложенным скрытым каналам управления и мониторинга аппаратуры, возможность осуществлять различные виды деструктивных воздействий, 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 ССОП в настоящее время являются существенным и одновременно наиболее уязвимым объектом критической информационной инфраструктуры Российской Федерации, функционирование которой в любое время может быть дезорганизовано действиями иностранных государств.

Значительную часть вышеперечисленных проблем позволяет решить создание выделенной телекоммуникационной основы, в качестве которой выступает создаваемая в соответствии с решениями Президента Российской Федерации, Правительства Российской Федерации интегрированная сеть связи для нужд обороны страны, безопасности государств и обеспечения правопорядка (далее – ИСС).

Устранение проблем будет достигаться принципиальными системно-техническими решениями по созданию ИСС, обеспечивающими гарантированную защиту трафика спецпользователей от информационно-технологических воздействий в трактах передачи информации ИСС. Важнейшими из них являются:

- физическая изолированность телекоммуникационной инфраструктуры ИСС от инфраструктуры ССОП;
- применение телекоммуникационного оборудования отечественного производства, сертифицированного по требованиям ФСБ России;
- оригинальная архитектура, функциональность и защищенность подсистемы централизованного управления сетью как системное решение обеспечения информационной безопасности технологических процессов управления;
- комплексные решения по обеспечению информационной безопасности ИСС (включая обнаружение, предупреждение и ликвидацию последствий компьютерных атак на ИСС), логично встроенные в замысел построения сети.

В инфраструктурном и системном отношении ИСС должна стать телекоммуникационной основой практически всех существующих и перспективных систем управления обороной и безопасностью государства, без создания которой невозможно их эффективное функционирование в условиях нарастающего информационного противоборства.

Масштабы ИСС, применяемые телекоммуникационные технологии и технологии информационной безопасности, приоритетная нацеленность на поддержку решения государственных и оборонных задач позволяют рассматривать ИСС как проект, обеспечивающий выход на новый уровень системы государственного и военного управления в мирное время и в условиях чрезвычайных ситуаций.

Создание ИСС как высокозащищенной телекоммуникационной платформы, в частности в интересах критической информационной инфраструктуры Российской Федерации, устойчивой к широкому классу деструктивных информационно-технологических воздействий и поражающих факторов высокоточного оружия, должно входить в число высших государственных приоритетов и является первым шагом на пути создания и развития национальной защищенной инфокоммуникационной инфраструктуры Российской Федерации как важнейшего элемента системы стратегического поддержания паритетов безопасности.

Функциональную основу системы может составить защищенная информационно-телекоммуникационная система поддержки государственного и военного управления,

объединяющая ведомственные специальные сети связи, информационные системы и ресурсы, базы данных экономического, военного, финансового характера, ситуационные центры в единое инфокоммуникационное пространство Российской Федерации на основе интегрированной сети связи, единых принципов защиты и управления и дальнейшего развития безбумажных технологий.

Отдельно следует отметить, что взятый руководством страны курс на развитие цифровой экономики Российской Федерации, нацеленной на повышение ее конкурентоспособности, качества жизни граждан, обеспечение экономического роста и национального суверенитета, делает это направление одним из важных объектов для спецслужб иностранных государств в рамках ведения гибридной войны против Российской Федерации.

В этой связи программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 года №1632-р, уделяет особое внимание информационной инфраструктуре цифровой экономики и ее информационной безопасности по следующим направлениям:

– развитие сетей связи, которые обеспечивают потребности экономики по сбору и передаче данных государства, бизнеса и граждан с учетом технических требований, предъявляемых цифровыми технологиями;
– развитие системы российских центров обработки данных, которая обеспечивает предоставление государству, бизнесу и гражданам доступных, устойчивых, безопасных и экономически эффективных услуг по хранению и обработке данных и позволяет, в частности, экспортировать услуги по их хранению и обработке;
– внедрение цифровых платформ работы с данными для обеспечения потребностей власти, бизнеса и граждан;
– создание эффективной системы сбора, обработки, хранения и предоставления потребителям пространственных данных, обеспечивающей потребности государства, бизнеса и граждан в актуальной и достоверной информации о пространственных объектах.

В этом контексте главной задачей является обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства.

Таким образом, можно констатировать, что создаваемая ИСС, обеспечивающая безопасность решения вышеперечисленных функциональных задач цифровой экономики, должна стать безальтернативной технологической платформой единого инфокоммуникационного пространства Российской Федерации.