ПОД ФЛАГОМ обновленной доктрины

Л.Павлова

DOI: 10.22184/2070-8963.2017.63.2.40.41

"Инфофорум-2017", проведенный практически сразу после утверждения Президентом РФ обновленной Доктрины информационной безопасности Российской Федерации, сосредоточился на стратегических задачах государственной политики в данной области, развитии международного сотрудничества, вопросах противодействия новым вызовам и угрозам в информационной среде.

Новая Доктрина информационной безопасности Российской Федерации, утвержденная 5 декабря 2016 года, пришла на смену одноименному документу, действовавшему с сентября 2000-го. Этот стратегический документ представляет собой систему официальных взглядов на обеспечение национальной безопасности страны в информационной сфере. Его основные положения прокомментировал Дмитрий Грибков, референт аппарата Совета Безопасности РФ. Он отметил, что в документе четко разделены технологический и психологический аспекты деятельности в информационной сфере, а поскольку он разработан на базе Стратегии национальной безопасности Российской Федерации, принятой в декабре 2015 года, именно на обозначенные в ней стратегические национальные интересы ориентированы и основные положения доктрины.

К национальным интересам отнесены: обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации; обеспечение безопасности критической информационной инфраструктуры, устойчивого и бесперебойного функционирования единой сети электросвязи РФ; развитие в России отрасли ИТ и электронной промышленности; продвижение достоверной информации о государственной политике России и ее официальной позиции по социально значимым событиям в стране и мире; содействие формированию системы международной информационной безопасности.

В информационно-технологическом и информационно-психологическом аспектах изложены и основные угрозы: наращивание возможности воздействия со стороны ряда западных стран на информационную инфраструктуру в военных целях; попытки иностранных спецслужб дестабилизировать посредством использования ИТ внутриполитическую и социальную ситуацию в различных регионах мира; рост в зарубежных СМИ объема материалов, содержащих предвзятую оценку государственной политики России; откровенная дискриминация российских СМИ за рубежом; увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере; рост числа преступлений, связанных с нарушением конституционных прав и свобод человека; рост количества и усложнение компьютерных атак на объекты критической информационной инфраструктуры; высокий уровень зависимости отечественной промышленности от зарубежных ИТ и др.

Соответственно угрозам определены и стратегические цели – в военной политике, в области государственной и общественной безопасности, в экономике, в науке и образовании, в международных отношениях. Следует отметить, что в январе нынешнего года Государственная дума приняла в первом чтении пакет законопроектов, устанавливающих организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Законопроекты также ужесточают уголовную ответственность за создание программ, предназначенных для хакерских атак на такие объекты. При этом, как подчеркнул в своем выступлении заместитель начальника Центра ФСБ России Николай Мурашов, российский бизнес, владеющий объектами критической информационной инфраструктуры, должен взять на себя часть ответственности за их кибербезопасность, поскольку, как показывает мировая практика,

обеспечить ее исключительно силами и средствами государства невозможно.

Что касается растущей киберпреступности, то, как сообщил начальник Бюро специальных технических мероприятий МВД России Алексей Мошков, в 2016 году в России было возбуждено почти 6 тыс. уголовных дел по преступлениям в сфере ИТ, причем 38% из них – по факту совершения мошеннических действий. Только за последние полтора года МВД России предотвратило ущерб от кибератак более чем на 3 млрд руб. и ведет постоянную разъяснительную работу среди потенциальных кибержертв. Со своей стороны в этом направлении действуют и кредитно-финансовые структуры. Так, замначальника Главного управления безопасности и защиты информации Банка России Артем Сычев заявил, что ЦБ вместе с отраслью готовит проект рекомендаций в области стандартизации квалификационных требований к специалистам ИБ в кредитно-финансовой сфере. Хищения средств у банков в 2016 году показали, насколько важно иметь квалифицированных сотрудников в этой сфере, однако в банках не всегда понимают, что должен знать и уметь такой специалист. По словам А.Сычева, завершение работ по проекту рекомендаций планируется в третьем квартале 2017 года.

Одна из стратегических целей в области международной ИБ – установление правил поведения государств. Как сообщил спецпредставитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности Андрей Крутских, в настоящее время этот вопрос обсуждается в ООН на заседаниях группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций. По словам А.Крутских, Россия рассчитывает, что в июне ООН утвердит правила поведения государств в сфере ИБ либо в виде отдельного документа с поправками в международное право, либо в форме резолюции.

Примечательно, что в новой редакции доктрины участниками системы обеспечения информационной безопасности наряду с органами власти признаются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты; средства массовой информации и массовых коммуникаций; организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка; операторы связи; операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения ИБ, по оказанию услуг в области обеспечения ИБ; организации, осуществляющие образовательную деятельность в данной области. Эти категории были представлены на тематических секциях "Инфофорума-2017". Так, в работе секции "Импортозамещение и безопасность в сфере создания, развития и использования сетей связи", организованной Россвязью, приняли участие представители ОАО "КБ "ИСКРА", ООО "Т8", СПбГУТ, ООО "ОКБ САПР", ФГУП "ЦНИИС" и др.

Как отметил в своем выступлении Игорь Багаев, руководитель проектов ООО "Т8", отечественное магистральное оборудование сетей связи уже представлено на рынке: в компании разработана широкая линейка транспондеров и мукспондеров для скоростей от 10 до 400 Гбит/с и внесена в перечень телекоммуникационного оборудования российского происхождения (ТОРП). В то же время, по словам представителя Россвязи Владимира Арефьева, существующий перечень средств связи, которым может быть присвоен статус ТОРП, на данный момент не покрывает всю номенклатуру производимого телекоммуникационного оборудования, поэтому в перечень нужно включать устройства, подлежащие процедуре подтверждения соответствия в форме декларирования.

Всего в рамках форума состоялось более 100 выступлений и презентаций, посвященных актуальным вопросам обеспечения ИБ в различных сферах. ■