Информационная безопасность — новые вызовы

О.О. ГРОМОВА, руководитель проекта НИО НИИПС — филиала ФГУП ГЦСС

В феврале в Москве традиционно прошел ряд форумов по информационной безопасности, в том числе Инфофорум-2017, ТБ-форум, Cyber Security Forum 2017. В связи с изменившимися политическими и экономическими условиями теме информационной безопасности сегодня придается особое значение как на уровне выработки стратегических государственных документов и концепций, так и на уровне законодательного регулирования Рунета. На форумах представители государственных структур, интернет-бизнеса, компаний-разработчиков и общественных организаций активно обсуждали актуальные вопросы и методы защиты от киберугроз.

Инфофорум-2017

Проведение Инфофорума в этом году имело особое значение, так как мероприятие проходило после утверждения Президентом России обновленной Доктрины информационной безопасности Российской Федерации (указ подписан 5 декабря 2016 г.; действовавший вариант Доктрины, принятый 16 лет назад, утратил силу). Как следует из документа, Доктрина представляет собой “систему официальных взглядов на обеспечение национальной безопасности страны в информационной сфере”. По этой причине основное внимание участников Инфофорума было направлено на обсуждение стратегических задач государственной политики в области обеспечения инфобезопасности РФ и было посвящено вопросам противодействия новым вызовам и угрозам в информационной среде.

Рост кибератак

Эксперты прогнозируют, что в будущем году ожидается серьезное увеличение роста компьютерных атак, в том числе на объекты критической информационной инфраструктуры (КИИ) — объекты промышленности, предприятия ТЭК, финансовый сектор и пр.

Николай Мурашов, заместитель начальника Центра информационной безопасности ФСБ России, сообщил, что ряд зарубежных стран наращивают возможности воздействия на информационную инфраструктуру в политических и экономических целях. Состояние информационной безопасности характеризуется на сегодняшний день постоянным повышением сложности, увеличением масштабности и ростом координации компьютерных атак на объекты КИИ.

При этом практически равную опасность представляют компьютерные атаки, совершаемые в преступных, террористических и разведывательных целях, со стороны отдельных лиц, сообществ, иностранных спецслужб и организаций. Террористическими и экстремистскими организациями активно создаются и совершенствуются средства воздействия на интернет.

По данным за последние годы, исходя из различных методик оценки, ущерб от вредоносных программ в мире составил от 300 млрд. до 1 трлн. долл. — от 0,4 до 1,5 % общемирового ВВП. В минувшем году была парализована работа нескольких крупных финансовых учреждений в Южной Корее, нарушена работа доменной печи в Германии (кибератака на металлургический завод), атакована телекоммуникационная компания “Дойче Телеком”.

По данным ФСБ, на информационную структуру России в 2016 г. произошло свыше 70 млн. кибератак, и эти показатели имеют тенденцию к росту.

Алексей Мошков, начальник Бюро специальных технических мероприятий МВД России, отметил, что за последние полтора года сотрудники управления “К” МВД РФ предотвратили хищение из российских банков на общую сумму более 3 млрд. руб., а также пресекли деятельность двух преступных групп, атаковавших учреждения кредитно-финансовой сферы. Произведены аресты и возбуждены уголовные дела. Одна из групп использовала методы социальной инженерии для введения в заблуждение лиц, которые выдавали злоумышленникам сведения, необходимые для дистанционного управления банковским счетом. Другая группа специализировалась на хищении средств, собранных для лечения онкологических больных. Действия фигурантов привели к смерти нескольких человек, не дождавшихся лечения.