ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕАЛИЗАЦИИ НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
Владимир Викторович Селин

По событиям, происходящим в мире и в нашей стране, мы видим, что планета охвачена информационной революцией, которая стала локомотивом глобализации. За последнее десятилетие отрасль информационных технологий получила существенное развитие.

Результаты исследований отечественных и зарубежных аналитиков показывают, что объем глобального рынка информационных технологий ежегодно растет.

С учетом стремительного процесса интернетизации планеты эксперты предсказывают, что в течение ближайших 15 лет роль Интернета в мире будет критически важной. Конкуренция в сфере интернет-услуг приведет к появлению огромного числа новых технологий.

В нашей стране в соответствии с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденной распоряжением Правительства Российской Федерации от 17 ноября 2008 года №1662-р, в качестве одной из целей государственной политики определено создание информационного общества, которое характеризуется высоким уровнем информационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти.

В соответствии со Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 года (№Пр-212), наша страна уже в ближайшей перспективе должна войти в число 20 ведущих стран мира в области развития информационного общества и занять ведущее место в международных рейтингах по уровню доступности национальной информационной и телекоммуникационной инфраструктуры.

Для достижения этих целей постановлением Правительства Российской Федерации от 15 апреля 2014 года №313 утверждена государственная программа Российской Федерации «Информационное общество (2011–2020 годы)», итоговым результатом которой станет появление ши-

рокого спектра возможностей использования информационных технологий в производственной, научной, образовательной и социальной сфере.

Однако наряду с очевидными положительными эффектами развитие информационных технологий несет в себе принципиально новые глобальные вызовы и угрозы.

В условиях развития информационного общества с точки зрения информационного пространства понятия «граница» и «территория государства» теряют смысл, так как становятся легко проницаемы для современных информационных технологий, а усиление значимости информационных ресурсов в политике, экономике и конкурентной борьбе обусловливает возникновение новых рисков.

В этих условиях актуальным становится предотвращение использования информационных технологий для решения задач, противоречащих интересам обеспечения мира и стабильности, суверенитета и безопасности государства.

В соответствии со Стратегией национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12 мая 2009 года №537, одним из основных источников угроз национальной безопасности является разведывательная и иная деятельность специальных служб и организаций иностранных государств, а также отдельных лиц или группы лиц, направленная на нанесение ущерба Российской Федерации.

Анализ и прогнозирование развития разведывательных средств и систем спецслужб иностранных государств показывают, что их активность, направленная в том числе на оказание воздействия на информационное пространство России, не снижается. Эти службы продолжают наращивать и совершенствовать средства разведки, методы и способы добывания информации. Отдельные разведывательные средства объединяются в глобальные системы, способные обеспечивать тотальный контроль по всему миру за обрабатываемой и передаваемой информацией.

Необходимо отметить, что интенсивное развитие информационного общества и значительное расширение областей использования информационных технологий в России вывели компьютерную разведку на одно из первых мест по значимости и объемам добываемой информации.

Основным устремлением компьютерной разведки являются информационные системы, обрабатывающие информацию ограниченного доступа, открытые информационные системы и информационно-телекоммуникационные сети.

В этих условиях важнейшей составляющей деятельности органов государственной власти и организаций по предотвращению угроз национальной безопасности, определенных Стратегией национальной безопасности Российской Федерации до 2020 года, является защита информации.

Основными направлениями деятельности ФСТЭК России в этой области являются:

– защита информации, составляющей государственную тайну;
– защита информации конфиденциального характера в государственных информационных системах;
– обеспечение безопасности информации в ключевых системах информационной инфраструктуры критически важных объектов.

Обработка информации, составляющей государственную тайну, с использованием средств вычислительной техники осуществляется практически во всех органах государственной власти и в организациях, выполняющих государственный оборонный заказ.

Практический опыт реализации мер по защите такой информации формировался более 20 лет. Сегодня можно однозначно сказать, что для решения этой задачи в нашей стране разработаны необходимые нормативные правовые акты и методические документы, имеются необходимые сертифицированные средства защиты.

В условиях стремительного роста государственных информационных систем и их интеграции в единое информационное пространство важным направлением является обеспечение эффективной защиты информации конфиденциального характера.

В базах данных государственных информационных систем, развернутых в настоящее время, хранятся и обрабатываются колоссальные объемы данных о гражданах, сведения об экономической, социальной, политической, правоохранительной и других областях деятельности реги-

онов России. Около 90% систем взаимодействуют с сетью Интернет и используют общедоступные интернет-сервисы.

Разработанные ФСТЭК России и ФСБ России нормативные правовые акты и методические документы, а также созданные и сертифицированные средства позволяют проводить весь необходимый комплекс работ.

В частности, в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» приказом ФСТЭК России от 11 февраля 2013 года №17 утверждены Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Указанным нормативным правовым актом устанавливаются требования к обеспечению защиты информации конфиденциального характера от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Кроме того, во исполнение Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» утверждены состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК России от 18 февраля 2013 года №21). Документ определяет необходимый набор защитных мер, принятие которых позволит обеспечить необходимый уровень защищенности персональных данных, обрабатываемых в информационных системах персональных данных.

Помимо нормативных правовых актов, устанавливающих требования в области защиты информации конфиденциального характера, ФСТЭК России разработала и утвердила значительное количество методических документов, целью которых является формирование единого методического подхода при обеспечении безопасности информации.

Особое значение имеет задача защиты информации в ключевых системах информационной инфраструктуры, срыв функционирования которых может привести к гибели людей, экологическим и техногенным катастрофам, нарушению государственного управления, жизнедеятельности населенных пунктов и социальной стабильности в стране и другим чрезвычайным ситуациям. К таким системам относятся в первую очередь автоматизированные системы управления технологическими процессами критически важных и потенциально опасных объектов атомной и гидроэнергетики, управления добычей и транспортировкой нефти и газа, управления транспортом, системы кредитно-финансовой сферы.

По оценкам экспертов, предотвращение угроз безопасному функционированию автоматизированных систем управления критически важных объектов является стратегическим направлением деятельности всех развитых стран.

Компьютерные атаки на такие системы способны вывести из строя критически важные объекты. Один из ярких примеров такой угрозы – информационное воздействие на системы управления иранских ядерных объектов, в результате которого были выведены из строя центрифуги на заводе по обогащению урана. Иранские власти официально признали, что системы управления ядерными объектами в Натанзе и Бушере подверглись информационной атаке.

В Российской Федерации, так же как и во всем мире, вопросам обеспечения безопасности автоматизированных систем управления на критически важных объектах уделяется особое внимание. Указанные вопросы неоднократно были рассмотрены в Совете Безопасности Российской Федерации.

В феврале 2012 года Президентом Российской Федерации подписаны Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.

В целях реализации положений этого документа и в соответствии с поручением Президента Российской Федерации приказом ФСТЭК России от 14 марта 2014 года №31 утверждены Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально

опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Для разработки указанных требований в ФСТЭК России была создана рабочая группа, в состав которой вошли представители ФСБ России, Минпромторга России, Минтранса России, Минэнерго России, Роскосмоса, Госкорпорации «Росатом», а также государственных и частных компаний, в ведении которых имеются критически важные объекты. Всего в работе приняли участие более 20 специалистов.

При разработке документа был учтен опыт не только российских компаний, но и иностранных государств.

Реализация требований защиты информации в автоматизированных системах управления позволит обеспечить, в первую очередь, целостность и доступность информации, обрабатываемой в автоматизированных системах управления технологическими процессами, а также непрерывность технологических процессов, задействованных в управлении критически важными и потенциально опасными процессами.

Благодаря этой работе обеспечение безопасности систем управления критически важных объектов имеет положительные тенденции.

Еще одним направлением деятельности ФСТЭК России является обеспечение функционирования системы сертификации средств защиты информации по требованиям безопасности информации.

В соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 года (№Пр-1895), система сертификации средств защиты информации является одним из элементов системы информационной безопасности Российской Федерации.

Основной целью сертификации является подтверждение соответствия средств защиты информации установленным требованиям безопасности.

Система сертификации ФСТЭК России создана в начале 1990-х годов в целях реализации Закона Российской Федерации от 21 июля 1993 года №5485-1 «О государственной тайне» и постановления Правительства Российской Федерации от 26 июня 1995 года №608 «О сертификации средств защиты информации».

23 декабря 1993 года был выдан первый сертификат соответствия на средство защиты информации от несанкционированного доступа «Снег 1.0».

На начальном этапе система сертификации ФСТЭК России была направлена только на оценку соответствия средств, предназначенных для защиты информации, составляющей государственную тайну. Однако по мере внедрения информационных технологий и роста угроз безопасности информации возникла потребность в применении сертифицированных средств для защиты информации конфиденциального характера.

Сегодня в соответствии с законодательством Российской Федерации сертифицированные средства применяются для защиты информации, составляющей государственную тайну, а также для всех государственных информационных ресурсов.

В целях организации сертификации средств защиты информации создана необходимая система нормативных и методических документов, устанавливающая порядок сертификации, требования к средствам защиты информации, правила аккредитации испытательных лабораторий и органов по сертификации.

Систему сертификации ФСТЭК России образуют органы по сертификации, испытательные лаборатории, разработчики и производители средств защиты информации, а также органы по аттестации объектов информатизации.

За последние 3 года количество участников системы сертификации ФСТЭК России увеличилось на 25%.

С момента выдачи первого сертификата в 1993 году в системе сертификации ФСТЭК России сертифицировано более 3 тыс. средств защиты информации различных типов. Объемы производства и количество применяемых сертифицированных средств ежегодно растут.

За последние 10 лет произведено и поставлено производителями в органы государственной власти и организации около 8,5 млн сертифицированных ФСТЭК России средств защиты. Ожидается, что этот показатель и дальше будет расти не менее чем на 5–7% в год.

Приведенные цифры показывают, что с развитием информационных технологий, количественным и качественным ростом угроз безопасности информации растет понимание органами государственной власти и организациями важности решения задач защиты информации.

Растет количество средств защиты, разрабатываемых и производимых российскими организациями. Сегодня количество сертифицированных средств защиты конфиденциальной информации отечественного производства составляет около 50% от общего количества сертифицированных средств. Так, если в 2009 году на рынке было представлено только 56 типов средств защиты информации, то в 2013 году их количество составило уже 121.

Интенсивно развивается разработка и производство отечественных средств защиты информации от несанкционированного доступа. На сегодняшний день в Российской Федерации разрабатываются и производятся средства защиты информации практически всех требуемых классов.

Помимо средств защиты информации общего применения, в системе ФСТЭК России проходят сертификацию средства, специально предназначенные для применения в определенных областях деятельности или решения важнейших задач. В первую очередь это средства защиты, предназначенные для применения в автоматизированных системах управления критически важных объектов, системах управления оборонно-промышленного комплекса, системах управления транспортом.

В целом, подводя итог, можно отметить, что сегодня вопросам обеспечения защиты информационных ресурсов Российской Федерации уделяется значительное внимание как со стороны государства, так и со стороны бизнес-сообщества. Однако только скоординированные усилия общества, бизнеса и государства позволят эффективно противостоять возрастающим угрозам и рискам в информационной сфере.