ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ КОМПЬЮТЕРНЫХ АТАК

О.Г. Смирнова, кандидат юридических наук, доцент;
С.Б. Хитов.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрена актуальность проблемы защиты информационных систем Российской Федерации от компьютерных атак, основные нормативно-правовые акты, регулирующие порядок создания и функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Ключевые слова: информационные системы, информационная безопасность, компьютерная атака, нормативно-правовой акт, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

LEGAL BASES OF PROTECTION OF INFORMATION SYSTEMS OF RUSSIAN FEDERATION AGAINST COMPUTER ATTACKS

O.G. Smirnova; S.B. Khitov. Saint-Petersburg university of State fire service of EMERCOM of Russia

Article is dedicated relevance of a problem of protection of information systems of Russian Federation against computer attacks, main normative legal acts regulating an order of creation and functioning or the state system of detection, prevention and elimination of consequences of computer attacks.

Keywords: information systems, information security, computer attack, normative legal act, state system of detection, prevention and elimination of consequences of computer attacks

Современный этап развития Российской Федерации, характеризующейся повышением уровня информатизации в органах государственной власти, связанным с увеличением числа создаваемых и внедряемых информационных и телекоммуникационных систем, совершенствованием информационных технологий (ИТ), являющихся основой разработки подобных систем, ведет к росту актуальности проблемы обеспечения информационной безопасности.

Еще пятнадцать лет назад отмечалась [1], существенная зависимость национальной безопасности Российской Федерации от обеспечения информационной безопасности, а также возрастание этой зависимости в ходе технического прогресса. Одной из составляющих национальных интересов Российской Федерации в информационной сфере выделялась защита информационных ресурсов, обеспечение безопасности информационных и телекоммуникационных систем, разворачиваемых и создаваемых в нашей стране. К общим методам обеспечения информационной безопасности были отнесены правовые, организационно-технические и экономические.

К настоящему времени в Российской Федерации разработана и продолжает совершенствоваться достаточно эффективная система правовых методов обеспечения информационной безопасности [2].

С обострением международной обстановки, ростом глобального информационного противоборства, активностью террористических группировок особую остроту приобретает

реализация угроз информационной безопасности посредством проведения компьютерных атак на государственные информационные системы и ресурсы. Значительное увеличение числа компьютерных атак международными террористическими организациями на органы государственной власти и бизнес-структуры во всех регионах мира подчеркнуто на заседании Совета Безопасности Российской Федерации, посвященном оценке состояния информационной безопасности в России в 2015 г. и состоявшемся 14 декабря 2015 г.

Под компьютерной атакой понимается целенаправленное несанкционированное воздействие
на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или аппаратно-программных средств [3].

Данное положение дел привело к необходимости разработки и принятия на государственном уровне комплекса мер, включая нормативно-правовые по противодействию компьютерным атакам.

В основе формирования нормативных правовых актов Российской Федерации, регулирующих вопросы защиты информационных систем от компьютерных атак, лежат положения Конституции Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные законы, регулирующие отношения в информационной сфере, Доктрина информационной безопасности страны, Стратегия национальной безопасности до 2020 г.

В рамках реализации положений Стратегии [4] в 2012 г. Президентом Российской Федерации утверждены Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления (АСУ) производственными и технологическими процессами критически важных объектов (КВО) инфраструктуры Российской Федерации, определяющие целью снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства [5].

Документ оперирует такими понятиями как компьютерная атака, силы обнаружения и предупреждения компьютерных атак и предусматривает создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

Поэтапная реализация Основных направлений предусматривает (в 2014–2016 гг.), в том числе разработку ряда нормативных правовых актов, определяющих:

– порядок получения федеральным органом исполнительной власти в области обеспечения безопасности информации об АСУ КВО и иных объектах критической информационной инфраструктуры;

– права и обязанности собственников АСУ КВО и иных объектов критической информационной инфраструктуры, а также эксплуатирующих их организаций в области обеспечения их безопасности;

– порядок разработки, ввода в действие, эксплуатации и модернизации АСУ КВО;

– регламент функционирования единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки защищенности ее элементов;

– порядок ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

– действия должностных лиц, персонала и владельцев АСУ КВО и иных объектов критической информационной инфраструктуры при обнаружении несанкционированного доступа к обрабатываемой информации и иных компьютерных инцидентах;

– ответственность за нарушение установленного порядка разработки, ввода в действие, эксплуатации и модернизации АСУ КВО и иных объектов критической информационной инфраструктуры;

– правовые основания и порядок применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до полного его прекращения;

К 2020 г. предусматривается реализация комплекса организационных, правовых, экономических и научно-технических мер, определяемых Основными направлениями и ввод в эксплуатацию в целом единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

В январе 2013 г. Президентом Российской Федерации был подписан Указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) на информационные ресурсы Российской Федерации», определяющий в качестве объекта защиты от компьютерных атак информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории страны, а также в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом [6].

Полномочия по созданию ГосСОПКА возлагаются на ФСБ России, которая помимо организации и проведения работ по созданию системы, осуществлении контроля за исполнением этих работ и обеспечения во взаимодействии с государственными органами функционирования ее элементов, разрабатывает ряд нормативных методических документов:

– методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети;

– методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

Реализация упомянутого выше указа привела к появлению в декабре 2014 г. утвержденной Президентом Российской Федерации Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяющей назначение, функции и принципы создания системы, а также виды обеспечения, необходимые для ее создания и функционирования [7].

ГосСОПКА представляет собой единый централизованный территориально-распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган власти, уполномоченный в области обеспечения безопасности критической инфраструктуры Российской Федерации и орган власти, уполномоченный в области создания и обеспечения функционирования системы.

Основной организационно-технической составляющей ГосСОПКА являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак (Центры), организованные по ведомственному и территориальному принципам.

В структуре ГосСОПКА выделяются:

– главный центр (ФСБ России);

– региональные центры (ФСБ России);

– территориальные центры (ФСБ России);

– ведомственные центры (центры органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации);

– корпоративные центры (центры, создаваемы государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации).

– национальный координационный центр по компьютерным инцидентам (ФСБ России).

Основными функциями системы, является выявление признаков проведения компьютерных атак, определение их источников и другой связанной информации, прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации, сбор и анализ информации о компьютерных атаках в отношении информационных ресурсов, Российской Федерации осуществление мероприятии по оперативному реагированию на атаки и ликвидации их последствий и др.

Нормативно-правовое обеспечение создания и функционирования системы включает:

– создание законодательной базы Российской Федерации;

– определение порядка фиксации и обмена информацией между субъектами о компьютерных атаках на информационные ресурсы Российской Федерации; и вызванных ими компьютерных инцидентах;

– определение порядка осуществления деятельности субъектов ГосСОПКА в области обнаружения, предупреждения и ликвидации последствий компьютерных атак;

– определение порядка и периодичности проведения мероприятий по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

– определение порядка обмена информацией между органами государственной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах.

В соответствии с Указом [6] четыре последних составляющих нормативно-правового обеспечения ГосСОПКА отнесены к компетенции ФСБ России.

Подводя итог, можно отметить, что законодательная и нормативная база ГосСОПКА разрабатывается и развивается.

Первым ведомством в России, которое взялось за создание своего сегмента ГосСОПКА стало Министерству экономического развития Российской. Министерство уже провело тендер на научно-исследовательские работы по созданию этой системы, который выиграла IT-компания PositiveTechnologies. Проект обойдется Министерству экономического развития Российской Федерации в 1,5 млн рублей [8].

В перспективе вероятно создание сегментов системы и в других, в том числе силовых министерствах и ведомствах Российской Федерации.

В МЧС России создание ведомственных центров обнаружения, предупреждения и ликвидации последствий компьютерных атак, по мнению авторов статьи, вероятнее всего будет осуществляться на базе возможностей системы распределенных ситуационных центров, объединяющих НЦУКС – ЦУКС региональных центров, ЦУКС главных управлений по субъектам Российской Федерации.

Литература

1. Доктрина информационной безопасности Российской Федерации // В.И. Рохлин, А.Д. Баконин. Закон и средства массовой информации. СПб.: Издательский дом «Нева», 2004. 576 с.

2. Хитов С.Б. Правовые основы защиты информации, обрабатываемой в государственных информационных системах Российской Федерации // Educatio. Ежемес. науч. журнал.2015. № 2 (9). С. 69–73.

3. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275. 2006, М.: ФГУП «Стандартинформ», 2007.

4. Стратегия национальной безопасности до 2020 г.: Указ Президента Рос. Федерации от 12 мая 2009 г. № 537 // Рос. газ. 2009. 12 мая. № 4912.

5. Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ. Утв. Президентом Рос. Федерации 3 февр. 2012 г. № 803. URL: http://www.scrf.gov.ru/documents/6/131.html (Дата обращения: 14.12.2015).

6. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ: Указ Президента Рос. Федерации
от 15 янв. 2013 г. № 31с. URL: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html (Дата обращения: 15.12.2015).

7. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Утв. Президентом
Рос. Федерации 12 дек. 2014 г. № К 1274. URL: http://www.scrf.gov.ru/documents/6/131.html. (Дата обращения: 16.12.2015).

8. Минэкономразвития создает систему защиты от хакеров ГосСОПКА. URL: http://izvestia.ru/news/597713. (Дата обращения: 17.12.2015).