УДК 34.03:004.056 + 002:004.056 Вестник УрФО № 3(21) / 2016, с. 56–61

Куц Д. В., Виноградова Н. С., Третьяк Н. В.

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА И ОСНОВНЫЕ НАПРАВЛЕНИЯ ЕЕ ОБЕСПЕЧЕНИЯ

Информационная безопасность сегодня является составной частью политической, экономической, военной, правоохранительной и других составляющих национальной безопасности нашей страны, потому что угрозы национальной безопасности осуществляются и через информационную среду. В данной статье рассматриваются понятие информационной безопасности государства и основные направления ее обеспечения. Также сформулированы методы и средства обеспечения информационной безопасности государства в нормативно-правовой, организационной и инженерно-технической сферах. Все это заставляет с особым вниманием отнестись и к угрозам, осуществляемым в информационной сфере, и соответственно к проблемам обеспечения безопасности.

Ключевые слова: *информационная безопасность государства, направления обеспечения информационной безопасности страны.*

Kuts D. V., Vinogradova N. S., Tretyak N. V.

CONCEPTION OF THE NATIONAL SECURITY AND DIRECTIONS OF ITS MAINTENANCE

Nowadays information security is an important component of political, economic, military, law enforcement and other aspects of the national security of our country, because the national security threats are carried out through the IT environment. In this article we consider the conception of the national security and the main directions of its maintenance. Also there are couched approaches and tools of maintenance of the national security in legal and regulatory, organizational and engineering and technical spheres. All of this makes us pay attention to either the threats which are carried out in the information sphere, and accordingly to that to problems of security assurance.

Keywords: *national security, national security maintenance directions*

Интерес к безопасности (защищенность от различных опасностей и угроз), к обеспечению ее необходимого уровня проявляется на протяжении практически всей истории человеческой цивилизации. Явление безопасности изучается и переосмысливается заново на каждом этапе развития общества. Исследование проблем безопасности человеческой цивилизации позволяет характеризовать безопасность как широкое явление. В современных условиях, когда во всех сферах жизни цивилизованного государства используются и продолжают внедряться информационные технологии, в том числе и новые технологии, функционирующие в режиме реального времени, повышается ценность информации, информация становится средством воздействия, безопасность общества зависит от безопасности используемых информационных технологий и существующей инфраструктуры. «Информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики»[1].

Информация превратилась в один из основных ресурсов развития общества. В связи с этим вопросы обеспечения информационной безопасности (ИБ) государства приобрели первостепенное значение.

Информационная безопасность представляет собой сложное социальное явление, состоящее из системы положений для защиты интересов субъектов информационных отношений и процесса использования ресурсов и возможностей общества, обеспечивающих сохранение и совершенствование системы защиты. Сущность ИБ как социального явления заключается в сложившихся реальных социальных отношениях в обществе, которые обеспечивают гарантии безопасности в информационной сфере и позволяют государству прогнозировать, выявлять, устранять и предупреждать реальные и потенциальные опасности и угрозы. «Возникновение ряда глобальных проблем современного общества требует разработки новых технологий их решения с привлечением все более многочисленных групп специалистов. Сегодня мировой опыт свидетельствует о том, что при помощи социальных технологий (информационных, …, политических, управленческих и др.) можно своевременно разрешать социальные конфликты, снимать социальное напряжение, предотвращать катастрофы, блокировать рискованные ситуации, принимать и выполнять оптимальные управленческие решения и др.» [2].

Развитие информационных технологий, превращение информации в стратегический ресурс, переход проблемы информационной безопасности из узко технологической категории в категорию управления общественными процессами, признание проблемы ИБ на международном уровне обосновывают актуальность темы.

Под информационной безопасностью понимается «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства»[3].

Информационная безопасность в начале третьего тысячелетия выходит на первое место в системе национальной безопасности, и, соответственно, формирование и проведение единой государственной политики в этой сфере требует приоритетного рассмотрения. Понятие информационной безопасности в разных доктринальных документах государств (в РФ – Доктрина информационной безопасности РФ, в США – Национальная стратегия достижения безопасности в киберпространстве и др.), в разных контекстах может иметь различный смысл, содержание и задачи.

Для ряда понятий на сегодняшний день нет терминов, однозначно признанных в мировом сообществе. В рамках Двустороннего проекта Россия-США проводилась работа по согласованию терминов кибер- и информационной безопасности. В проекте принимали участие Институт проблем информационной безопасности Московского Государственного университета имени М. В. Ломоносова (ИПИБ МГУ) и Институт Восток-Запад со стороны США. В апреле 2011 г. были приняты «Основы критически важной терминологии»[4] и согласованы 20 терминов, касающихся определения кибербезопасности. Работа над следующими 20 терминами, касающимися более широкого понятия информационной безопасности продолжается.

Разногласия по поводу терминологии кибер- и информационной безопасности за-

ключаются в том, что имеются две точки зрения на эту проблему. Наметились две группы государств, имеющие серьезные разногласия по поводу развития информационной цивилизации и будущего всемирной компьютерной сети. В одну группу входят Россия, Китай, Казахстан, Белоруссия, Армения, Таджикистан и ряд других стран, а в другую – США и их союзники по НАТО. Информационная безопасность – это более широкое понятие, чем кибербезопасность. В рамках понятия информационной безопасности рассматриваются не только технические стороны защиты информации, но и факторы, воздействующие на человека, общество и государство. Кибербезопасность же не рассматривает вопросы, связанные с воздействием вредоносного контента и использованием информационно-коммуникационных технологий на общественное сознание.

Успешные решения в системе ИБ обеспечиваются применением комплексного подхода к проблеме, учитывающего организационно-правовые, физические, социальные, духовные, информационные, программно-математические и технические методы, мероприятия и средства, обеспечивающие нормальное функционирование государства, его структур, различных организаций как на его территории и в его пространстве, так и в межгосударственных отношениях.

Решение проблем противодействия конкретным угрозам и опасностям в информационных системах, защиты интересов субъектов информационных отношений определяет основные направления государственной политики информационной безопасности.

Ключевым компонентом системы ИБ можно считать информацию в связи с тем, что информация с одной стороны легко уязвима, а с другой стороны информация может быть источником разнообразных угроз. Соответственно можно назвать защиту информации и защиту от информации составляющими общей проблемы информационной безопасности, автоматически добавляется и защита инфраструктуры.

Защите подлежит только та информация, которая зафиксирована на материальном носителе с реквизитами, позволяющими ее идентифицировать. Информация в качестве информационного ресурса принадлежит собственнику, находится в ведении соответствующих органов и организаций, подлежит учету и защите. Основные способы защиты информации связаны с такими аспектами, как доступность, целостность и конфиденциальность информации.

Под доступностью следует понимать возможность за приемлемое время получить требуемую информационную услугу. Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Конфиденциальность информации подразумевает защиту от несанкционированного доступа к информации [5].

В связи с многообразием информационных угроз, воздействие которых не всегда очевидно, проблема защиты от информации более сложна и требует технических, организационно-правовых и политических решений на внутригосударственном и международном уровнях.

Защита людей от информации носит преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем, так же как и по защите информации, носят технический характер и поддаются систематизации и математическому описанию.

В сфере информационной безопасности можно выделить следующие основные направления развития:

- нормативно-правовое;
- организационное;
- инженерно-техническое.

Каждое из этих основных направлений имеет свои составляющие, для которых определены конкретные способы, средства и мероприятия обеспечения ИБ.

Нормативно-правовое направление в системе обеспечения информационной безопасности государства связано с правовым регулированием отношений, обеспечением и защитой интересов личности, общества и государства в информационной сфере, и базируется на конкретных правовых актах, законах, в том числе и гражданского, административного, уголовного права, нормативных и ведомственных методических документах, стандартах. К вопросам нормативно-правового регулирования относятся :

- информационная безопасность на государственном и международном уровне;
- правовое регулирование в сфере обращения информации;
- правонарушения и ответственность в сфере обращения информации;

- правовое регулирование в сфере криптографической защиты информации;
- защита авторских и патентных прав;
- компетенции СМИ.

В рамках организационного направления формируется и регламентируется деятельность и взаимоотношения в информационной сфере на основе имеющейся нормативно-правовой базы [6].

Организационное направление системы обеспечения ИБ государства включает:

- регламентацию деятельности органов государственной власти и других государственных органов, ответственных за обеспечение ИБ;
- взаимодействие с другими государствами в рамках международного сотрудничества в сфере ИБ;
- разработку и совершенствование нормативно-правовой базы в области обеспечения ИБ;
- комплекс фундаментальных и прикладных научных исследований в области ИБ, анализ функционирования системы ИБ с целью оценки возможностей системы по выявлению внутренних и внешних угроз, по их предотвращению и нейтрализации;
- подготовка кадров для сферы ИБ;
- формирование программы функционирования ИБ на основе единой государственной политики безопасности, отражающей подход государства к защите граждан, общества и информационных ресурсов;
- создание надежной системы обеспечения ИБ государства, защищающей в первую очередь государственные информационные ресурсы в государственных органах, в оборонной (военной) сфере и других отраслях, имеющих государственное значение;
- сертификация средств защиты информации, телекоммуникационного оборудования и программного обеспечения, лицензирование деятельности в области защиты государственной тайны;
- развитие информационной инфраструктуры и технологий, а также индустрии производства информационных и телекоммуникационных средств, программных продуктов;
- управление персоналом, физическую защиту, поддержание работоспособности системы защиты (непрерывность защиты в пространстве и времени), реагирование на нарушение режима безопасности (локализация инцидента, выявление нарушителя, предупреждение повторного нарушения), планирование восстановительных работ (знание критически важных функций системы, учет приоритетов, наличие плана восстановительных работ).

В рамках организационного направления решаются вопросы по координации и планированию использования финансовых, материальных, кадровых и других ресурсов, обеспечивающих функционирование системы обеспечения ИБ.

Экономическая составляющая организационного направления в области ИБ включает определение порядка финансирования программ обеспечения информационной безопасности, совершенствование системы финансирование работ, связанных с реализацией основных направлений обеспечения безопасности в сфере ИБ, создание системы страхования информационных рисков физических и юридических лиц.

Инженерно-техническое направление обеспечения ИБ является одним из важнейших в перечне мероприятий ИБ и включает следующие составляющие:

- физическую защиту объектов (техническая укрепленность зданий и сооружений; защита периметра);
- комплекс технических средств охраны (охранная сигнализация; пожарная сигнализация; охранное телевидение; система контроля управления доступом; охранное освещение, связь и пр.);
- технические средства защиты информации от утечки по техническим каналам (средства активной защиты (акустические и электромагнитные); средства пассивной защиты; средства контроля);
- программно-аппаратные средства защиты (средства криптографический защиты информации; средства сетевой защиты информации; средства защиты информации от НСД).

Элементы защиты информации предоставляют следующие сервисы:

- идентификация и аутентификация (криптографические методы аутентификации, реализуемые посредством программного или аппаратно-программного способа; парольная защита; биометрические методы защиты);

- управление доступом (доверенный доступ);
- протоколирование и аудит (многоуровневость; фильтрация данных при переходе на более высокий уровень; применение средств активного аудита);
- шифрование (применение криптографического программного ПО и аппаратных средств);
- контроль целостности (использование криптографических методов и запоминающих устройств);
- программное экранирование (межсетевые экраны; виртуальные частные сети; ограничивающие интерфейсы);
- анализ защищенности (инструмент поддержки безопасности, обеспечивающий обновление системы и контролирующий выход новых продуктов);
- обеспечение отказоустойчивости (вопрос архитектуры информационной системы, касающийся как аппаратной составляющей, так и программной);
- обеспечение безопасного восстановления системы.

Управление инфраструктурой включает в себя:

- продуманность архитектуры безопасности информационной системы (непрерывность защиты в пространстве и времени, иерархическая организация ИС, устойчивость);
- соответствие стандартам, использование апробированных решений.

Сервисы безопасности должны функционировать в открытой сетевой среде с разнородными компонентами, быть устойчивыми к угрозам, но и удобными для пользователей [7].

Каждое по отдельности из рассмотренных направлений в обеспечении информационной безопасности государства не обеспечит комплексной и эффективной защиты. Надежная защита возможна при совокупном использовании всех методов и средств, присущих рассмотренным выше направлениям развития ИБ.

Соблюдение режима безопасности затрудняет постоянная модернизация ИС и программных продуктов, внедрение новых программных продуктов и информационных устройств. Основной угрозой нарушений в системе ИБ является внутренняя сложность информационных систем, затем идут непреднамеренные ошибки обслуживающего персонала и пользователей, следующей категорией угроз являются кражи и подлоги, в отдельную категорию можно выделить пожары, стихийные бедствия, аварии, нарушающие работу поддерживающей инфраструктуры. В общем числе нарушений растет доля внешних атак.

Информационная безопасность является социальным явлением, сущность которого заключается в сложившихся реальных социальных отношениях в обществе, которые обеспечивают гарантии безопасности в информационной сфере и позволяют государству прогнозировать, своевременно выявлять, предупреждать и устранять реальные и потенциальные опасности и угрозы. Формирование политики в любой сфере деятельности, проводимой государством, возможно только на основе применения стратегических технологий (методов) с максимально эффективным и целесообразным использованием ресурсов и средств. В связи с применением сегодня социальных технологий (совокупность методов и инструментов для достижения желаемого результата) во всех сферах деятельности современного человека и общества можно утверждать, что применение стратегических технологий (методов) в управлении обеспечением информационной безопасности государства является определяющим фактором и обеспечивает максимальный эффект при использовании этих ресурсов и средств.

Примечания

1. Окинавская хартия глобального информационного общества : принята 22 июля 2000 г. [Электронный ресурс] / Электронный фонд правовой и нормативно-технической документации. Консорциум Кодекс. – Поисковая прогр. – URL: http://docs.cntd.ru/document/901770887 (дата обращения: 30.04.2016).

2. Технологии социальной работы: учебник / под общ. ред. проф. Е. И. Холостовой. – М. : ИНФРА-М, 2001. – С.13.

3. Белов Е. Б., Лось В. П. и др. Основы информационной безопасности : учебное пособие для вузов. – М.: Горячая линия-Телеком, 2006. – С. 459.

4. Двусторонний проект: Основы критически важной терминологии [Электронный ресурс] / ИПИБ МГУ – URL: http://www.iisi.msu.ru/articles/article31/ (дата обращения: 30.04.2016).

5. См.: Галатенко В. А. Основы информационной безопасности: учебное пособие. – М.: Интернет-Университет Информационных Технологий, 2006. – С.13.

6. См.: Ярочкин В. И. Информационная безопасность: учебник для студентов вузов. – М.: Академический проект. Гаудеамус, 2004. – С.51.

7. См.: Галатенко В. А. Основы информационной безопасности: учебное пособие. – М.: Интернет-Университет Информационных Технологий, 2006. – С.196–199.

Куц Дмитрий Владимирович, старший преподаватель кафедры теоретических основ радиотехники, Института радиоэлектроники и информационных технологий – РтФ, Уральский федеральный университет имени первого Президента России Б. Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail:d.v.kutc@urfu.ru

Виноградова Нина Сергеевна, старший преподаватель кафедры теоретических основ радиотехники, Института радиоэлектроники и информационных технологий – РтФ, Уральский федеральный университет имени первого Президента России Б. Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: n.s.vinogradova@urfu.ru

Третьяк Наталия Вадимовна, сотрудник Уральского федерального университета имени первого Президента России Б. Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: n.v.tretiak@urfu.ru

Kuts Dmitry Vladimirovich, senior teacher of the "Basic Theory of Radio Engineering" department, Institute of Radioelectronics and Information Technologies, Ural Federal University named after the first President of Russia B. N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: d.v.kutc@urfu.ru

Nina Sergeevna Vinogradova, senior teacher of the "Basic Theory of Radio Engineering" department, Institute of Radioelectronics and Information Technologies, Ural Federal University named after the first President of Russia B. N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: n.s.vinogradova@urfu.ru

Tretyak Nataliya Vadimovna, employee of Ural Federal University named after the first President of Russia B. N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: n.v.tretiak@urfu.ru