Мусуралиева М.М., Исмаилова Р.

К ВОПРОСУ О СОДЕРЖАНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мусуралиева М.М., Исмаилова Р.

МААЛЫМАТТЫК КООПСУЗДУКТУН МАЗМУНУ ЖӨНҮНДӨГҮ СУРООГО

M.M. Musuralieva, R. Ismailova

ON THE CONTENT OF INFORMATION SECURITY

УДК: 323.5:27

Содержание информационной безопасности в контексте системного анализа представляет собой комплекс взаимосвязанных структурных элементов. Исследование информационной безопасности с позиций системного подхода позволяет увидеть, сколь сильно отличается научное, пусть и предварительное, понимание этой безопасности от обыденного.

Ключевые слова: *информационная безопасность, угрозы, информационная война, информационно-психологический мониторинг, компьютерная преступность, субъекты и объекты информационной безопасности.*

Тутумдук анализ контекстинде маалыматтык коопсуздуктун мазмуну өз ара байланышкан структуралык элементтердин комплексин түзөт. Маалыматтык коопсуздуктун тутумдук анализ позициясы менен изилденүсү, анын илимий түшүнүгү, мейли алдын ала болжолгон болсо да, бул коопсуздуктун күндөлүк түшүнүгүнөн бир топ айырмаланып турганын көргөнгө мүмкүнчүлүк берет.

Негизги сөздөр: *маалыматтык коопсуздук, коркунучтар, маалыматтык согуш, маалымат-психологиялык мониторинги, компьютердик кылмыш, маалыматтык коопсуздуктун субъекттери жана объекттери*

The content of information security in the context of systems analysis is defined as a set of interconnected structural elements. The study of information security as a system shows the huge difference between scientific approach and the regular notion of security.

Key words: *information security, threats, information war, information and psychological monitoring, computer crime, the subjects and objects of information security.*

Введение

Общеизвестная фраза «Кто владеет информацией, тот владеет миром» выдающегося политика 20 века Уинстона Черчилля и сегодня не потеряла актуальности. Более того с бурным развитием информационных технологий, значимость ее возросла многократно.

Сегодня у определенных субъектов (коалиций, государств, организаций, личностей) возникает стремление единолично обладать информационными ресурсами, средствами и технологиями и использовать их для удовлетворения своих интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. Информация и информационные технологии при этом начинают выступать в качестве объектов угроз, что порождает проблему информационной безопасности.

Под предметом информационной безопасности в научной литературе часто понимается область защиты информации, а именно - обеспечение конфиденциальности, целостности и доступности информации. Указывая на ошибочность такой интерпретации, Г.В. Иващенко пишет: «…значительная часть современных публикаций в области теории безопасности описывает свой предмет бессистемно и на уровне поверхности» [1]. Разделяя эту точку зрения, М.А. Стюгин указывает, что предмет информационной безопасности значительно шире исходя из анализа нормативных правовых документов. В качестве примера автор приводит определение понятия «безопасность» в Доктрине информационной безопасности Российской Федерации, которое вытекает из определения в федеральном законе «О безопасности» от 5 марта 1992 года: «*Информационная безопасность РФ - состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства*» [2]. При этом указывается, что определять «безопасность» через «защищенность» является не корректным, поскольку эти слова синонимы, а поэтому данные определения являются тавтологиями. Безопасность есть некоторое состояние объекта, которое можно определить, выделив соответствующие качественные характеристики. В [3] информационная безопасность рассматривается с точки зрения человеческого фактора, а именно – в совокупности “технический фактор – люди, обслуживающие систему – нормативно-правовые акты обеспечения информационной безопасности”. Резюмируя свой обзор, приходим к выводу, что сводить предмет исследования информационной безопасости только к целостности, конфиденциальности и доступности информации нельзя, во-первых, из определения в доктрине, во-вторых, из необходимости обоснования безопасности информации в целевых функциях более общих систем.

На наш взгляд, предмет информационной безопасности образует совокупность общественных отношений, возникающие и развивающиеся в информационной сфере между субъектами информационного взаимодействия в процессе реализации их прав на целостность, конфиденциальность и защищенность интересов, гарантированных и обеспеченных соответствующими социальными регуляторами. В предлагаемой трактовке предмета отличительным признаком является динамика, в то время как в указанной выше трактовке акцент ставится на неком статическом состоянии объекта информационного воздействия.

В теории информационной безопасности ключевую роль играют понятия объекта и субъекта. К *объектам информационной безопасности* относятся:

Права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности; информационные ресурсы; информационные технологии; информационная инфраструктура.

Следующим структурным элементом информационной безопасности являются субъекты, представляющие собой органы и структуры, которые в той или иной мере занимаются обеспечением информационной безопасности. На государственном уровне ими могут быть органы не только исполнительной, но и законодательной, судебной властей.

Угрозы информационной безопасности.

Активная позиция субъекта, оказывающего прямое или косвенное воздействие на определенную группу информационных отношений, ведет к возникновению ситуации, когда присутствует угроза целостности, конфиденциальности и/или защищенности интересов объекта. При этом угрозы информационной безопасности или источники информационных опасностей - это фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды. Согласно [4], источники угроз информационной безопасности разделяются на две основные группы:

1. Естественные, которые не зависят от чьей-либо воли, носят случайный характер.
2. Искусственные (человеческий фактор), которые являются результатом умышленной деятельности одного человека, какой-либо социальной группы или государства.

Естественные угрозы существуют изначально в природе или возникают в результате случайных факторов, таких как стихийные бедствия и катастрофы, непреднамеренные ошибки персонала информационных систем, отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах и многое другое.

К искусственным угрозам информационной безопасности государства относятся недружественная политика иностранных государств; деятельность иностранных разведывательных и специальных служб; деятельность иностранных политических и экономических структур, направленная против интересов государства в области формирования, распространения и использования информации; противоправные действия со стороны как организованных преступных групп, так и отдельных лиц; неправомерные действия государственных структур, нарушающие законные права граждан и организаций в информационной сфере и многое другое. Представляется, что всю совокупность угроз этой группы можно классифицировать на следующие виды:

- информационная война;
- информационно-психологический мониторинг;
- правонарушения, связанные с использованием средств компьютерной техники.

Сам термин “*информационная война*” появился приблизительно в середине 70-х гг. XX века. На Западе основоположником данного термина принято считать ученого- физика Томаса Рона, который в разгар “холодной войны” (1976 г.) назвал информацию самым слабым звеном вооруженных сил и обороны. Термин “информационная война” является сложной структурой, в которой слово “война”, по мнению И.В. Свиридова, “выступает в роли порождающего понятия, несущего основную смысловую нагрузку, а слово “информационная” – его качественной характеристики” [5]. Информационная война представляет собой комплекс действий, предпринимаемых для достижения информационного превосходства путем активного воздействия на информационные органы и структуры противника, на процессы его информационного обеспечения, компьютерные сети при одновременной защите, обеспечении устойчивости и безопасности собственной информации и ее структур; преднамеренные и систематические атаки на критическую информационную деятельность с целью перехвата информации, ее изменения, дезинформации и нарушения информационного обеспечения [6].

Информационно-психологический мониторинг как угроза информационной безопасности представляет не меньшую опасность, чем информационная война. Однако в отличие от последней, информационно-психологический мониторинг предполагает установление тотального контроля над жизнью человека, общества и государства в процессе информатизации.

Последним из названных видов угроз информационной безопасности являются правонарушения, связанные с использованием средств компьютерной техники, совокупность которых объединена общим понятием -*компьютерная преступность*. Возникшая в процессе информатизации общества, данная форма преступности представляет непосредственную опасность субъектам информационного взаимодействия. Впервые термин «компьютерная преступность» появился в начале 60-х гг. Несмотря на имевшие место случаи компьютерных правонарушений, законодательство стран вплоть до 70-х гг. не содержало специальных норм, предусматривающих юридическую ответственность за правонарушения, связанные с использованием информационной технологии. Реализация необходимости совершенствования законодательства, особенно уголовного, во многих развитых странах возникла с резким увеличением числа правонарушений, вызванного массовым производством персональной компьютерной техники и развитием компьютерных сетей [7].

Методы обеспечения информационной безопасности.

Всю совокупность факторов, влияющих на обеспечение информационной безопасности можно раз-

делить на политические, экономические и организационно-технические [8].

В условиях научно-технического прогресса взаимозависимость и уязвимость субъектов информационной безопасности увеличивается пропорционально процессу развития национальной информационной инфраструктуры. В то же время, основным субъектом, определяющим приоритетность программ и направлений информатизации, является государство, которое под условием обеспечения безопасности национальных интересов целенаправленно принимает меры для соблюдения конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных теле-коммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Для реализации государственной политики обеспечения информационной безопасности необходимо в первую очередю разработать и внедрить механизмы реализации правовых норм, ре гулирующих отношения в информационной сфере, подготовить концепции правового обеспечения информационной безопасности, разработать и реализовать механизмы повышения эффективности го сударственного руководства деятельностью государственных средств массовой информации, осуществление государственной информационной политики и т.д. [9]

Частным примером является проблема, связанная с криптографическими методами защиты информации. Высокая степень защиты и практическое отсутствие возможности дешифрования информации, обеспечиваемые современными криптосистемами, в настоящее время вызывают беспокойство со стороны силовых структур государств. С одной стороны, возникла угроза потери установившейся в некоторых странах монополии этих структур в области разработки криптографических методов защиты, а, с другой, утраты контроля над информационным пространством страны. Последнее означает, что многие из успешно осуществляемых сегодня оперативно-розыскных мероприятий в целях предупреждения угроз национальной безопасности, в частности, прослушивание переговоров, перехват сообщений или снятие информации с каналов связи, в ближайшем будущем станут нереализуемы.

Проблема борьбы с компьютерной преступностью в Кыргызской Республике в том, что в развитых странах уголовный кодекс касательно киберпреступлений развивался непосредственно по мере развития информационных технологий, и соответственно – информационных угроз. В то время как рост киберпреступности в развитых странах был пропорционален развитию информационных технологий, в Кыргызской Республике, а также во многих других странах с аналогичной историей, мы столкнулись со сформировавшейся угрозой. Ни интернет-пользователи, ни государство не были готовы к преступлениям, которые были привнесены глобальной сетью. В уголовном кодексе Кыргызской Республики предусмотрена только одна статья о преступлении в сфере компьютерной информации – статья 290.

Заключение

Сегодня технологически развитые державы занимают ключевые позиции в экономической и научно-технической информатике. Передача государствам с развивающейся экономикой информационной технологии неизбежно ведет и к передаче соответствующих административных процедур, форм учета, методов управления и контроля. Постепенно передаваемая информационная технология превращается в политический и идеологический фактор, в фактор распространения культуры, языка, других духовных ценностей, а также соответствующих экономических, производственных отношений, в фактор давления на экономику развивающихся стран, в средство эксплуатации их информационного, интеллектуального потенциала. В процессе формирования Глобального информационного общества сотрудничество государства означает равноправие и независимость во всем международном информационном обмене, то есть в обмене экономической, научно-технической, политической, культурной и пропагандистской (идеологической) информацией. С этой точки зрения, актуальным и необходимым является участие КР в международно-правовых механизмах создания системы мер доверия и гарантийных мер безопасности в контексте развития нового мирового информационного порядка.

Литература:

1. Иващенко Г.В. (2000). Доктрина информационной безопасности и методические проблемы теории безопасности. Материалы круглого стола «Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества», МГУ, с. 48-63
2. Стюгин М.А. Информационная безопасность «по существу» // http://psyfactor.org/lib/styugin6.htm
3. Whitman M., Mattord H. (2011). Principles of information security. Cengage Learning.P.20
4. Peltier T.R. (2005). Information security risk analysis. CRC press. P.12
5. Свиридов И.В. Информационная война: определения, подходы, взгляды // Безопасность информационных технологий, 1998. - № 4. С. 25
6. Цыбмал Ы.И. (1995). О концепции информационной войны. Информационный сборник “Безопасность”, N9. С.35
7. Зинина У.В. (2007). Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Москва.С.56
8. Родичев Ю.А., Родичев Ю.А. (2008). Информационная безопасность: нормативно-правовые аспекты: [по специальности 090102 Компьютер. безопасность, 090105 Комплекс. обеспечение информ. безопасности автоматизир. систем]. Издательский дом " Питер". С.78
9. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. (2006). Основы информационной безопасности. Горячая линия – Телеком. М. С.34

Рецензент: к.филос.н., доцент Арзыматов Дж.С.