СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ

Анфиса НАШИНЕЦ-НАУМОВА,
кандидат юридических наук,
Национальный технический университет Украины «Киевский политехнический институт»

Summary

In a scientific article examines the system to ensure information security. Contributed by various scientific approaches to the definition of individual elements in the system to ensure information security. A comparative analysis set forth in the provisions of Ukrainian legislation and regulations relating to the individual elements of the system, such as an object, the subjects, the main characteristics, the levels of information security and the list of threats. The author's definition of the notion of information security system of the state.

Key words: information security, information security threats.

Аннотация

В научной статье исследуется система обеспечения информационной безопасности государства. Предоставлены различные научные подходы к определению отдельных элементов в системе обеспечения информационной безопасности государства. Проводится сравнительный анализ закрепленных в украинском законодательстве положений и норм, касающихся отдельных элементов системы, таких как объект, субъекты, основные характеристики, уровни информационной безопасности и перечень угроз. Сформулировано авторское определение понятия «система обеспечения информационной безопасности государства».

Ключевые слова: информационная безопасность, уровни информационной безопасности, угрозы.

Постановка проблемы. Очевидно, что залогом создания надежной системы охраны информации сегодня может быть только укрепление самого украинского государства и государственных органов, ответственных за обеспечение информационной безопасности в стране. В связи с этим стоят масштабные задачи, связанные с выработкой системы обеспечения информационной безопасности, поиска принципиально новых, нестандартных форм организации, взаимодействия, координации деятельности, совершенствование всех средств, направленных на обеспечение процесса управления угрозами и опасностями. Для комплексного определения системы обеспечения информационной безопасности проанализируем теоретические положения, которые предусматривают наличие соответствующих структур регламентированного процесса принятия и реализации управленческих решений в сфере управления информационной безопасностью. Подтверждением **актуальности исследования** является то, что 1 мая 2014 г. исполняющий обязанности Президента Украины, председатель Верховной Рады Украины Александр Турчинов подписал Указ № 449/2014 о решении СНБО от 28 апреля 2014 г. «О мерах по совершенствованию формирования и реализации государственной политики в сфере информационной безопасности Украины». Исходя из необходимости совершенствования нормативно-правового обеспечения, предупреждения и нейтрализации потенциальных и реальных угроз информационной безопасности, Совет национальной безопасности и обороны Украины поручил Кабинету Министров Украины в месячный срок разработать и внести на рассмотрение Верховной Рады Украины законопроекты о внесении изменений в некоторые законы Украины относительно противодействия информационной агрессии иностранных государств. Следовательно, важным моментом является то, что Украина должна сформировать такую систему обеспечения информационной безопасности, которая позволит гарантированно обеспечить национальные интересы при любых условиях.

Цели и задачи статьи. В настоящее время проблематика информационной безопасности государства исследуется в работах многих украинских ученых, таких как В. Копылов [1], Б. Кормич [2], В. Липкан [3], А. Марущак [4], В. Цымбалюк [5], Ю. Шемчушенко [6] и других. Однако указанные исследования и научные труды касались только национальной безопасности в информационной сфере. Концептуальные же основы системы обеспечения информационной безопасности государства в настоящее время остаются недостаточно изученными, что и является целью статья.

Изложение основного материала. Необходимость обеспечения информационной безопасности государства очевидна. Потребность в защите в равной мере касается как информации, содержащейся во всех информационных системах и передающейся сетью, так и той, что находится «за кадром». Информация многообразна: от материалов обсуждений в залах сессионных заседаний и кабинетах комитетов и комиссий (в том числе таких, которые происходят за закрытыми дверями) до личной переписки, данных отдела кадров и другой деликатной информации, поэтому обеспечение безопасности всегда является актуальной темой. Ежедневно появляются новые сообщения о злоупотреблениях и взломах. Вместе со сложными проблемами, связанными с социотехникой, проблемы защиты информации требуют от ее владельцев постоянного пребывания настороже. Вторжение, атаки, направленные на срыв обслуживания пользователей, незаконное разглашение информации – «вечные» угрозы, противостоять которым должны тщательно продуманные программы защиты данных для всех аспектов деятельности законодательного органа. Речь идет как о внутренних системах и процедурах, так и о тех, которые освещаются в Интернете.

Большинство государственных органов придерживаются лишь базовых принципов обеспечения информационной безопасности:

– использование информации в соответствии с законодательством и исключительно с той целью, с которой она предоставляется;

– сведения объемов информации до необходимого минимума;

– уважение прав граждан или организаций, к которым относятся данные;

– своевременное обновление, обеспечение актуальности и достоверности информации;

– хранение информации только до тех пор, пока она нужна;

– поддержание безопасности информационной среды;

– предоставление информации другим организациям только после поступления соответствующих запросов и осуществления защитных мероприятий.

Таким образом, определение данного понятия имеет не только чисто теоретический, но и практический интерес, связанный с необходимостью формирования системы органов государственного управления информационной безопасностью государства.

Анализ научной литературы свидетельствует, что вопросы системы обеспечения информационной безопасности недостаточно исследованы. В. Липкан, Ю. Максименко, В. Желиховский [7, с. 158] рассматривают систему обеспечения информационной безопасности как систему информационно-аналитических, теоретико-методологических, административно-правовых, организационно-управленческих, специальных и других мероприятий, направленных на обеспечение устойчивого развития объектов информационной безопасности, а также инфраструктуры ее обеспечения. Как видим, авторы в громоздком определении сочетают субъективный и нормативный подходы, не указав элементов системы. Другой подход демонстрирует А. Стрельцов и к системе информационной безопасности относит следующие элементы: субъекты информационных процессов; информация, предназначенная для использования субъектами информационного общества; информационная инфраструктура; общественные отношения, которые складываются в связи с созданием, хранением, передачей и распространением информации [8, с. 15–21]. Но ученый, на наш взгляд, рассматривает механизм обеспечения информационной безопасности, а не ее систему. Очевидно, что система обеспечения информационной безопасности является совокупностью отдельных элементов, которыми, как правило, является объект, субъекты и виды. В то же время отдельными ее составляющими являются основные характеристики, уровни информационной безопасности и перечень угроз.

Таким образом, система обеспечения информационной безопасности – это внутренняя структура, систематизированная совокупность, единство, взаимосвязь и дифференциация отдельных ее элементов (объект, субъекты, основные характеристики, уровни информационной безопасности и перечень угроз).

В вопросе об объекте информационной безопасности обращаем внимание, что законодатель дает перечень объектов национальной безопасности: человек и гражданин – их конституционные права и свободы; общество – его духовные, морально-этические, культурные, исторические, интеллектуальные и материальные ценности; информационная и окружающая природная среда и природные ресурсы; государство – его конституционный строй, суверенитет, территориальная целостность и неприкосновенность [9]. Как уточняют авторы учебника «Курс административного права Украины», основными объектами безопасности являются следующие: лицо – его права и свободы; общество – материальные и духовные ценности; государство – конституционный строй, суверенитет и территориальная целостность [10, с. 34–35]. Итак, очевидна необходимость дополнения этого перечня (на примере информационной безопасности) таким объектом, как информация, информационная деятельность. Законодательство не содержит четкого перечня субъектов информационной безопасности, а в Законе Украины «Об основах национальной безопасности Украины» [11] представлена только система субъектов обеспечения национальной безопасности. Однако в Законе Украины «Об информации» [12] субъектами определены физические лица, юридические лица, объединения граждан и субъекты властных полномочий. Другой перечень мы можем просмотреть в Законе Украины «О доступе к публичной информации» [13], где субъектами признаны запрашивающие информацию (физические, юридические лица, объединения граждан без статуса юридического лица, кроме субъектов властных полномочий); распорядители информации; структурные подразделения или ответственные лица по вопросам запросов на информацию распорядителей информации. Необходимо уточнить, что до распорядителей информации законодатель отнес немалый перечень, а именно: субъекты властных полномочий (органы государственной власти, иные государственные органы, органы местного самоуправления, другие субъекты, осуществляющие властные управленческие функции в соответствии с законодательством и решения которых обязательны для исполнения); юридические лица, финансируемые из государственного, местных бюджетов, – относительно информации относительно использования бюджетных средств; лица, если они выполняют делегированные полномочия субъектов властных полномочий по закону или договору, включая предоставление образовательных, оздоровительных, социальных или других государственных услуг, – в отношении информации, связанной с выполнением их обязанностей; субъекты хозяйствования, которые занимают доминирующее положение на рынке или наделены специальными или исключительными правами, или являются естественными монополиями, – относительно информации относительно условий поставки товаров, услуг и цен на них. Считаем, что указанный перечень неполный, поскольку, по нашему убеждению, субъектом информационной безопасности является, с одной стороны, Украина как государство в целом, другие государства и международные организации, а с другой – юридические и физические лица (потребители информации, производители информации, эксперты по квалификации и специалисты по сертификации).

Прежде всего в системе обеспечения информационной безопасности рассмотрим ее основные характеристики. Информационная безопасность выступает как характеристика стабиль-

ного, устойчивого состояния системы, которая при воздействии внутренних и внешних угроз и опасностей сохраняет важные характеристики для собственного существования. Так, Ю. Гатчина, В. Сухостат выделяют следующие основные характеристики информационной безопасности: доступность, целостность и конфиденциальность [14, с. 45]. С. Арбуз, В. Носов, А. Манжай основными характеристиками информационной безопасности называют критерии конфиденциальности, критерии целостности, критерии доступности, критерии наблюдаемости [15, с. 16]. Авторский коллектив под редакцией В. Кононовича объединяет основные характеристики информационной безопасности в деятельность собственника информации или уполномоченного им лица с обеспечения своих прав на владение, распоряжение и управление защищенной информации; предотвращения утечки и потери информации; сохранение полноты, достоверности, целостности защищенной информации, ее массивов и программ обработки; конфиденциальности или секретности защищенной информации, в соответствии с правилами, установленными законодательными и другими нормативными актами [16, с. 9]. Но их объединения по различным критериям (субъекты и сфера информационной деятельности) является спорным. Внимание заслуживает мнение, что информационная безопасность государства имеет динамический характер. В каждый конкретный отрезок времени состояние защищенности может иметь разный уровень, определяется остротой внутренних и внешних угроз и характером реагирования на них управленческого аппарата открытой социальной системы [17]. Уместно, по нашему мнению, отнести к характеристике информационной безопасности содержательные ее показатели, которые проявляются по-особенному на каждом из уровней государственного управления, в частности на стратегическом – Кабинет Министров Украины; тактическом – центральные органы исполнительной власти; оперативном – местные органы исполнительной власти, ведущее место среди которых занимают местные государственные администрации. Приведенное позволяет определить основными характеристиками системы обеспечения информационной безопасности: доступность, целостность и конфиденциальность. В системе обеспечения информационной безопасности основными элементами считаем перечень ее уровней. Анализ источников показывает, что ученые предлагают рассматривать следующие уровни информационной безопасности: нормативно-правовой уровень – законы, нормативно-правовые акты и т. д.; административный уровень – действия общего характера, предпринимаемые органами государственного управления; процедурный уровень – конкретные процедуры обеспечения информационной безопасности; программно-технический уровень – конкретные технические меры обеспечения информационной безопасности. Так, В. Липкан предлагает рассматривать следующие уровни информационной безопасности: стратегический уровень – Совет национальной безопасности и обороны Украины и Кабинет Министров Украины; тактический уровень – центральные органы исполнительной власти; оперативный уровень – местные органы исполнительной власти [18, с. 20]. Однако в учебном пособии «Информационная безопасность Украины в условиях евроинтеграции» В. Липкана, Ю. Максименка, В. Желиховского [7, с. 158] находим другой перечень уровней информационной безопасности: физический, программно-технический, управленческий, технологический, уровень пользователя, сетевой, процедурный. Рассмотрим несколько подробнее каждый из этих уровней. На физическом уровне осуществляется организация и физическая защита информационных ресурсов и информационных технологий. На программно-техническом уровне осуществляется идентификации и проверка подлинности пользователей, управления доступом, протоколирование и аудит, криптография, экранирование, обеспечение высокой доступности. На уровне управления осуществляется управление, координация и контроль организационных, технологических и технических мероприятий на всех уровнях управления со стороны единой системы обеспечения информационной безопасности органов государственного управления. На технологическом уровне осуществляется реализации политики информационной безопасности за счет применения комплекса современных автоматизированных информационных технологий. На уровне пользователя реализация политики информационной безопасности направлена на уменьшение рефлексивного воздействия на субъекты государственного управления, предотвращения информационного воздействия со стороны социального среды. На уровне сети данная политика реализуется в формате координации действий органов государственного управления, которые связаны между собой одной целью. На процедурном уровне принимаются меры, реализуемые людьми.

Среди них можно выделить следующие группы процедурных мероприятий: управление персоналом, физическая защита, поддержание работоспособности, реагирования на нарушения режима безопасности, планирование реанимационных работ. С. Макаренко для защиты интересов субъектов информационных отношений предлагает сочетать следующие уровни обеспечения информационной безопасности: законодательные, административные (приказы и другие действия руководства, которые связаны с защитой информационных систем), процедурные, программно-технические [19, с. 62]. Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, а так же потому, что так поступать не принято. На законодательном уровне различают две группы мероприятий:

– меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);

– направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры творческой направленности).

Наиболее важное на законодательном уровне – создать механизм, позво-

ляющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности. К административному уровню информационной безопасности относятся действия общего характера. Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и определена стратегия защиты, составляется программа обеспечения информационной безопасности. «Политика безопасности» (не совсем точный перевод английского словосочетания «security policy») имеет в виду не отдельные правила или их наборы, а стратегию организации в области информационной безопасности. Политика безопасности – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов. Процедурный уровень, ориентированный на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания. Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Акцент следует делать не на военной или уголовной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных. Программно-технический уровень, то есть уровень, направленный на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Подчеркиваем, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги – некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Уместно отнести к уровням обеспечения информационной безопасности те, которые предлагает рассматривать В. Цымбалюк. За основу разделения он определяет такие критерии, как среда, в которой находится информация: а) социальная среда (отдельный человек, сообщества людей, государство); б) инженерно-технологическая (машинная, аппаратно-программная, автоматическая, телекоммуникационная) среда; в) социотехническая (человеко-машинная) среда. Каждый указанный уровень относительно среды объективно дополняет и взаимообуславливает другие уровни, в основе образуя триединую гиперсистему – систему обеспечения информационной безопасности [20, с. 32]. Итак, перечисленные уровни обеспечения информационной безопасности подчеркивают важность комплексного подхода к их внедрению. Среди составных частей системы информационной безопасности важное место занимает перечень ее угроз. Так, уже в упомянутом Законе Украины «Об основах национальной безопасности» все виды безопасности, в том числе и информационные, связываются с состоянием защищенности жизненно важных интересов ее объектов. Анализ источников показывает, что некоторые ученые ставят знак равенства между понятиями «угрозы информационной безопасности» и «угрозы национальной безопасности и национальным интересам», с чем мы не согласны, потому что имеет место общее явление и частное. Другие ученые понимают угрозы как совокупность условий, процессов и факторов, препятствующих реализации национальных интересов или создающих им опасность [21, с. 145]. Есть мнения, что угрозы – это конкретные и непосредственные формы опасности или совокупность негативных факторов или условий [22, с. 38]; совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере [23, с. 123]; явные или потенциальные действия, которые затрудняют или делают невозможным реализацию национальных интересов в информационной сфере и создают опасность для системы государственного управления, жизнеобеспечения ее системообразующих элементов [7, с. 97].

Следует согласиться с теми исследователями, которые считают угрозы совокупностью негативных факторов или условий. Г. Емельянова и А. Стрельцова в определении их роли одним из источников угроз интересам общества в информационной сфере называют непрерывное усложнение информационных систем и сетей связи, критически важных инфраструктур обеспечения жизни общества [24, с. 15–17]. Итак, угрозы информационной безопасности представляют собой совокупность негативных факторов (условий), которые затрудняют реализацию информационных интересов личности, общества и государства.

Выводы. Учитывая изложенное, следует отметить, что при анализе информационной безопасности необходимо различать систему информационной безопасности и систему обеспечения информационной безопасности. Первая – это функциональная система, отражающая процессы взаимодействия интересов и угроз, а вторая – это организационная система органов, сил, средств, различных организаций, призванных решать задачи по обеспечению информационной безопасности. Причем без понимания сущности первой невозможно понимание принципов функционирования второй. Таким образом, система обеспечения информационной безопасности – это внутренняя структура, систематизированная совокупность, единство, взаимосвязь и дифференциация отдельных ее элементов (объект, субъекты, основные характеристики, уровни информационной безопасности и перечень угроз).

Высказанные положения являются результатом творческого поиска. Они, безусловно, дискуссионные и требуют дальнейшего теоретического исследования.

Список использованной литературы:

1. Копылов В.А. Информационное право : [учебник] / В.А. Копылов. – 2-е изд., перераб. и доп. – М., 2003. – 512 с.
2. Кормич Б.А. Организационно-правовые основы политики информационной безопасности Украины : [монография] / Б.А. Кормич. – О. : Юридическая литература, 2003. – 472 с.
3. Липкан В.А. Теоретические основы и элементы национальной безопасности Украины : [монография] / В.А. Липкан. – К. : Текст, 2003. – 600 с.
4. Марущак А.И. Информационное право: регулирование информационной деятельности : [учебное пособие] / А.И. Марущак. – К. : Издательский дом «Скиф», КНТ, 2008. – 344 с.
5. Цымбалюк В.С. Основы информационного права Украины : [учебное пособие] / В.С. Цымбалюк. – К. : Знание, 2004. – 274 с.
6. Шемчушенко Ю.С. Правовое обеспечение информационной деятельности в Украине / Ю.С. Шемчушенко. – К. : Юридическая мысль, 2006. – 384 с.
7. Липкан В.А. Информационная безопасность Украины в условиях евроинтеграции : [учебное пособие] / В.А. Липкан, Ю.Е. Максименко, В.М. Желиховский. – К. : КНТ, 2006. – 280 с.
8. Стрельцов А.А. Направление совершенствования правового обеспечения информационной безопасности Российской Федерации / А.А. Стрельцов // Информационное общество. – 1999. – № 6. – С. 15–21.
9. Об основах национальной безопасности Украины : Закон Украины от 19 июня 2003 г. № 964-IV // Ведомости Верховной Рады Украины. – 2003. – № 39. – Ст. 352.
10. Курс административного права Украины : [учебник] / [В.К. Колпаков, А.В. Кузьменко, И.Д. Пастух, В.Д. Сущенко и др.] ; под ред. В.В. Коваленко. – К. : Юринком Интер, 2012. – 564 с.
11. Об основах национальной безопасности Украины : Закон Украины // Правительственный курьер. – 2003. – 30 июля.
12. Об информации : Закон Украины от 2 октября 1992 г. // Ведомости Верховной Рады Украины. – 1992. – № 48. – Ст.650.
13. О доступе к публичной информации : Закон Украины // Ведомости Верховной Рады Украины. – 2011. – № 32. – Ст. 314.
14. Гатчина Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчина, В.В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.
15. Арбуз С.В. Информационная безопасность : [учебное пособие] : в 2-х ч. / С.В. Арбуз, В.В. Носов, А.В. Манжай. – Х. : Вид ХНЭУ, 2008. – Ч. 2. – 196 с.
16. Обеспечение информационной безопасности цифровых программно-управляемых АТС : [учебное пособие] / [В.Г. Кононович, С.В. Стайкуца, Т.М. Тардаскина, Т.М. Шинкарчук] ; под ред. чл.-корр. МАЗ В.Г. Кононовича. – О. : ОНАС им. А.С. Попова, 2010. – 168 с.
17. Сащук А.В. Информационная безопасность в системе обеспечения национальной безопасности / А.В. Сащук [Электронный ресурс]. – Режим доступа : journ.univ.kiev.ua/trk/.../Satshuk_publ.php.
18. Липкан В.А. Административно-правовые основы обеспечения национальной безопасности Украины : автореф. дис. ... докт. юрид. наук : спец. 12.00.07 / В.А. Липкан ; Киев. нац. ун-т внутр. дел. – К., 2008. – 34 с.
19. Макаренко С.И. Информационная безопасность : [учебник для вузов] / С.И. Макаренко. – Ставрополь : СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.
20. Цымбалюк В.С. Отдельные вопросы определения категории «информационная безопасность» в нормативно-правовом аспекте / В.С. Цымбалюк // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – 2004. – Вып. 8. – С. 32.
21. Липкан В.А. Национальная и международная безопасность в определениях и понятиях / В.А. Липан, О.С. Липкан, А.А. Яковенко. – К. : Текст, 2006. – 256 с.
22. Нижник Н.Р. Национальная безопасность Украины (методологические аспекты, состояние и тенденции развития) : [учебное пособие] / Н.Р.Нижник;подобщ.ред.П.В.Мельника, Н.Р. Нижник. – Ирпень, 2000. – 304 с.
23. Тарасенко Р.Б. Информационное право : [учебно-методическое пособие] / Р.Б. Тарсенко ; МВД Украины, Луган. гос. ун-т внутр. дел им. Е.О. Дидоренко. – М. : РИО ЛГУВД им. Е.О. Дидоренко, 2010. – 512 с.
24. Емельянов Г.В. Проблемы обеспечения безопасности информационного общества / Г.В. Емельянов, А.А. Стрельцов // Информационное общество. – 1999. – Вып. 2. – С. 15–17.