УДК

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И ПРОБЛЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ

Портнова Д.В., Антоненко В.Н.,
Портнова Г.А.

Донецкий национальный технический университет

г. Донецк, Украина

В настоящее время, в эпоху появления и развития информационного общества, современные информационные технологии проникают во все сферы деятельности человечества, что, в принципе, является вполне закономерным и объективным процессом. Более того, это напрямую связано с эволюционным развитием современного общества, в котором информационные технологии являются неотъемлемым и обязательным элементом прогресса. Информатизация всех общественных процессов является объективно необходимой для самых различных пользователей и потребителей информации: граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений и других [7].

Данный путь развития мировой цивилизации затрагивает все без исключения государства и направления их деятельности. В Украине в настоящее время такое информационное пространство активно формируется, что объясняется современными реалиями и актуальными потребностями этого времени. По этой причине вопросы, связанные с формированием современного информационного пространства, и задачи по созданию современного информационного общества, являются в значительной степени важными и актуальными для всех государств, в том числе и для Украины.

В обобщенном значении, информация – это данные, представленные в том или ином виде, пригодные для хранения обработки и (или) передачи.

Из всех видов используемой в настоящее время информации, по нашему мнению, наиболее востребованной является экономическая информация, под которой понимается совокупность сведений, отражающих состояние или определяющих изменение и развитие экономики и всех ее элементов.

Вместе с тем, к основным изменениям, характеризующим современную экономику, относятся:

- глобализация (конкуренция на мировых рынках, глобальные группы производителей, глобальные системы поставки);
- переход от индустриальной экономики к экономике, основанной на знаниях, к информационному обществу;
- перестройка предприятия (отсутствие жесткой иерархии, децентрализация, гибкость, независимость от местоположения, низкие транзакционные издержки, совместная работа) [7].

Нужно сказать, что авторы приведенного выше перечня особенностей современной экономики, хотя и указали на основные моменты современности, но при этом не вполне обоснованно его (перечень) сформировали, либо во многом его сузили. Экономика как отдельный предмет исследования, является значительно многообразнее и включает гораздо большее количество важных аспектов своего проявления, даже с учетом рассматриваемого информационного контекста ее изучения.

Хотя приведенное выше определение экономической информации является вполне адекватным, но, как нам представляется, относится в большей степени к глобальным макроэкономическим процессам в обществе, и гораздо в меньшей степени учитывает специфические экономические проблемы и тенденции современных предприятий, работающих в этих глобальных информационных условиях.

Тем не менее, в условиях рыночного хозяйствования образовалась и функционирует масса самых различных экономических (хозяйствующих) субъектов, имеющих вполне четкие собственные экономические интересы, отличные от макроэкономических интересов. А у любого, отдельно взятого и работающего на свой собственный экономический интерес, предприятия, естественно, возникают, и свое внутреннее информационное обеспечение его деятельности, и некоторое внешнее информационное окружение.

К сожалению, практика такова, что отдельно функционирующие предприятия зачастую лишены реальной возможности иметь доступ и эффективно использовать необходимые им информационные ресурсы. В Украине, например, нет ни одного государственного или публичного органа, который бы обеспечивал предприятия информацией, необходимой им для принятия управленческих решений.

Поэтому рассмотрение вопросов, связанных с информационным обеспечением хозяйствующих субъектов, должно стать одним из приоритетных направлений научных исследований и практически направленных поисков их применения.

Это касается изучения всех вопросов, связанных, во-первых, с информационными технологиями, и, во-вторых, с формированием и внедрением на предприятиях систем эффективного менеджмента. По нашему мнению, такое системное объединение вопросов информационного обеспечения и менеджмента предприятий даст им (предприятиям) желаемый положительный эффект синергии.

Кстати, именно в этом направлении совпадают научные и практические цели и задачи соответствующих специалистов: специализирующихся на разработках информационных технологий, и специалистов – экономистов.

Объясняется это тем, что в рыночных условиях хозяйствования именно интересы различных экономических субъектов являются своеобразным стимулом для получения и использования той информации, которая может обеспечить им получение желаемой прибыли и улучшение их рыночных позиций. Поэтому было бы логичным уточнить определение экономической информации применительно к отдельным обособленным хозяйствующим субъектам. Исходя из их экономических интересов, связанных с получением прибыли, улучшением конкурентных позиций на рынке и т.п., к такой микроэкономической информации следует относить совокупность специфических сведений, создающих условия и возможности при их эффективном использовании обеспечивать указанным хозяйствующим субъектам экономические выгоды.

В довольно сложных и противоречивых условиях формирования на постсоветском пространстве рыночного хозяйствования интерес к экономической информации, приносящей экономическую выгоду, крайне высок.

Однако проблема усугубляется тем, что формирование этих условий происходит на фоне постоянных экономических противоречий, обусловленных, как объективными, так и субъективными, причинами. К таким причинам, в частности, можно отнести:

- последствия используемой в советский период неэффективной модели экономического развития;

- неспособность некоторых менеджеров рационально использовать имеющуюся у них информацию;

- недостоверность и необъективность самой экономической информации;

- постоянная (можно сказать хроническая) и необоснованная изменяемость данной информации, которая делает ее непригодной для принятия соответствующих управленческих решений;

- коррумпированность многих властных структур, что, в свою очередь, изменяет приоритеты менеджеров предприятий в поиске нужной информации.

Эти и некоторые подобные свойства информационного экономического пространства в Украине (впрочем, как и в других постсоветских государствах) негативно влияют, и на развитие экономики этих стран, и на формирование указанного информационного пространства.

Безусловно, затронутая проблема относительно информационного обеспечения предприятий – в настоящее время является своевременной, важной и многоплановой, но при этом – крайне недостаточно исследованной и поэтому требующей дальнейшей разработки.

Рассматривая основные, наиболее важные, вопросы указанной проблемы, целесообразно, на наш взгляд, выделить первоочередные из них:

- определение и обоснование роли и места информационного обеспечения в системе эффективного менеджмента предприятий (ЭМП);

- формулирование и обоснование требований к информационному обеспечению с позиций ЭМП;

- формирование принципов создания информационного обеспечения в системе ЭМП;

- постановка задач для разработчиков информационного обеспечения в системе ЭМП;

- определение состава и структуры информационного обеспечения ЭМП;

- адаптация и внедрение разработанного информационного обеспечения в действующую систему менеджмента предприятия;

- создание эффективно действующей системы сбора, накопления, передачи, хранения, обработки и использования экономической информации в системе ЭМП;

- своевременное регулирование состава и структуры информационного обеспечения ЭМП;

- создание и внедрение подсистемы активно действующей защиты экономической информации от любых на нее посяганий со стороны любых заинтересованных лиц;

- оценка качества и эффективности использования информационного обеспечения в системе ЭМП.

Все перечисленные выше аспекты создания информационного обеспечения системы ЭМП должны быть разработаны и внедрены на предприятиях комплексно, с учетом их системной взаимосвязи и объективной необходимости.

Однако следует подчеркнуть, что из всего перечисленного комплекса создания системы информационного обеспечения ЭМП в настоящее время, самым отстающим элементом

и потому тормозящим внедрение всей указанной системы, является создание и внедрение подсистемы активно действующей защиты экономической информации. И это при том, что экономическая информация, как было сказано, создает условия для получения прибыли и улучшения рыночных позиций предприятий. А утечка или любое несанкционированное использование информации конкурентами или другими экономически заинтересованными субъектами объективно создает им такие выгодные экономические условия, лишая при этом предприятия их экономических перспектив.

В связи с этим такая экономическая информация представляет особый (экономический) интерес для указанных выше субъектов, посягающих на чужую экономическую выгоду. Для удержания собственной коммерческой выгоды предприятиям необходимо такую информацию защищать, для чего она приобретает правовой статус коммерческой тайны.

На сегодняшний день в Украине усиливается практический интерес к коммерческой тайне и другим связанным с ней понятиям, как одной из наиболее эффективных мер информационной безопасности [1].

Коммерческая тайна выполняет важную функцию в обеспечении конкурентоспособной деятельности. Поэтому правообладатель, безусловно, имеет право на защиту ее от неправомерного использования. Но, несмотря на высокую и непрерывно растущую значимость этого объекта интеллектуальной собственности, до сих пор отсутствует его прямая правовая охрана.

Целью данной статьи является освещение некоторых теоретических и практических аспектов по определению коммерческой тайны и защиты права на нее.

Термин “коммерческая тайна” означает разновидность информации с особым (коммерческим) статусом. Согласно Закону Украины “Об информации” [4], информация, в зависимости от режима доступа к ней, подразделяется на открытую и ограниченную. Исходя из этого определения, коммерческая информация, которая требует защиты от неправомерного ее использования другими лицами, не может принадлежать к информации, доступ к которой свободен. Статья 30 этого Закона [4] разделяет информацию с ограниченным доступом на конфиденциальную и секретную. Указанные в Законе сведения не дают нам достаточно оснований отнести коммерческую тайну к одному из видов информации с ограниченным доступом. Поэтому при определении правовой природы коммерческой тайны целесообразно отметить, что она является разновидностью информации с ограниченным доступом.

Коммерческая информация имеет особый статус, обусловленный наличием ряда признаков, присущих только коммерческой тайне, которые отличают ее от других видов информации. К основным признакам коммерческой информации относятся:

1) коммерческая ценность – этот признак является достаточно относительным, однако его существование обусловлено тем, что коммерческая ценность одной и той же информации в разных случаях может быть разной. А потому довольно затруднительно выявить определенную точку отсчета для установления ценности информации;

2) ограниченность – информация, составляющая коммерческую тайну, должна быть неизвестной для третьих лиц, иначе она просто потеряет свою ценность;

3) защищенность – субъект, который владеет информацией, составляющей коммерческую тайну, должен принимать меры для ограничения свободного доступа к этой информации. Этот признак является также относительным, поскольку трудно определить тот уровень необходимости и целесообразности принимаемых мер для сохранения ограниченности информации, составляющей коммерческую тайну;

4) законность – информация, составляющая коммерческую тайну, должна быть полученной ее собственником на законных основаниях [3].

Каждый признак коммерческой тайны играет важную роль, поскольку, согласно ст. 508 Гражданского кодекса Украины [4], срок действия права интеллектуальной собственности на коммерческую тайну ограничивается сроком существования совокупности указанных признаков коммерческой тайны. Следовательно, коммерческая тайна – это разновидность информации с ограниченным доступом, что имеет коммерческую ценность в связи с тем, что она неизвестна третьим лицам и к ней нет свободного доступа других лиц на законных основаниях, а ее владелец принимает соответствующие меры для сохранения ее конфиденциальности.

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются:

- массовое распространение средств электронной вычислительной техники (ЭВТ);
- постоянное и объективное усложнение шифровальных технологий;

- необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой;

- расширяющиеся возможности любых нежелательных несанкционированных действий с информацией.

Конечно, защита любой тайны, в том числе и коммерческой, всегда связана с наличием и носителем какой-либо угрозы по поводу утечки или несанкционированного использования такой информации.

Анализ имеющихся актуальных угроз конфиденциальной информации, на основе которого строится система информационной безопасности предприятия, начинается с понимания и классификации этих угроз.

В настоящее время теория информационной безопасности рассматривает несколько классификаций информационных рисков и угроз защиты информации. Мы остановимся на генерализированном разделении угроз информационной безопасности интеллектуальной собственности организации на две категории – внешние и внутренние угрозы.

Данная классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать, как удаленно, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, так и посредством доступа к внутренним ресурсам IT-инфраструктуры объекта.

Носителей угроз при этом, с учетом структуры системы менеджмента предприятий, было бы интересно разделить та внешних и внутренних. Они в принципе имеют разный доступ и по-разному сталкиваются с коммерческой информацией, но, и те, и другие, могут нанести умышленный (осознанный) либо неумышленный (неосознанный) ущерб предприятию.

В случае внешних атак носитель угрозы (преступник) ищет уязвимость в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д.

Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации. Рассмотрим эти категории рисков информационной безопасности подробнее.

Вначале уделим внимание внешним угрозам, так как, без сомнения, они представляют значительно больший интерес в свете рассматриваемой проблемы.

Доклад Всемирного экономического форума “Глобальные риски 2012” (“Global Risks 2012”) рассматривает кибератаки как одну из основных угроз мировой экономике. По вероятности наступления, кибератаки входят в пятерку наиболее вероятных глобальных угроз за 2012 год. Такое заключение Всемирного экономического форума свидетельствует о высокой актуальности и значительной опасности электронной преступности. В документе приводится также график роста официально признанных инцидентов киберпреступности с указанием значительного увеличения потерь от таких преступлений на примере США.

Кибератаки сегодня – давно не голливудский миф, это реальная и серьезная опасность информационной инфраструктуре, интеллектуальной и физической собственности государственных и коммерческих объектов.

Наиболее распространенной в настоящее время и разнообразной по методам исполнения формой киберпреступности является использование вредоносного программного обеспечения. Такие угрозы представляют прямую опасность конфиденциальности и целостности информационных ресурсов организации. В атаках с использованием вредоносных кодов и приложений используются уязвимости информационных систем для осуществления несанкционированного доступа к базам данных, файловой системе локальной корпоративной сети, информации на рабочих компьютерах сотрудников. Спектр угроз информационной безопасности, вызванных использованием вредоносного программного обеспечения чрезвычайно широк. Вот некоторые примеры таких угроз защиты информации:

- внедрение вирусов и других разрушающих программных воздействий;

- анализ и модификация/уничтожение установленного программного обеспечения;

- внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений;

- использование различных уязвимостей программного обеспечения для взлома программной защиты с целью получения несанкционированных прав чтения, копирования, модификации или уничтожения информационных ресурсов, а также нарушения их доступности;

- раскрытие, перехват и хищение секретных кодов и паролей;

- чтение остаточной информации в памяти компьютеров и на внешних носителях;

- блокирование работы пользователей системы программными средствами;

и т.д.

Внутренние угрозы также имеют большое значение, если при этом учесть желания внешних носителей угроз любыми методами привлечь или использовать сотрудников предприятия к получению ими (конкурентами и другими заинтересованными лицами) коммерческой информации.

Большинство имеющих место на практике инцидентов информационной безопасности связано с воздействием внутренних угроз – утечки и кражи информации, утечки коммерческой тайны и персональных данных клиентов организации, ущерб информационной системе связаны, как правило, с действиями сотрудников этой организации. В классификации внутренних угроз в первую очередь можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности.

Преступления или любые неправомерные действия сотрудников, способных причинить вред сохранности интеллектуальной и коммерческой собственности организации (их принято называть “инсайдерами”), можно разделить на категории злонамеренного и непредумышленного инсайда.

Злоумышленным инсайдером могут стать:

- сотрудники, затаившие обиду или злобу на компанию-работодателя (“обиженные”). Такие инсайдеры действуют исходя из мотивов личной мести, причин для которой может быть масса – от увольнения/понижения в должности до отказа компании предоставить статусные атрибуты, например, ноутбук или социальный пакет;

- нечистые на руку сотрудники, стремящиеся подзаработать за счёт компании-работодателя. Такими инсайдерами становятся сотрудники, использующие секретные информационные ресурсы компании для собственной выгоды. Базы данных клиентов, интеллектуальная собственность компании, состав коммерческой тайны – такая информация может использоваться инсайдером в личных интересах, либо продаваться конкурентам;

- внедренные и завербованные инсайдеры, – самый опасный из всех и при этом самый трудно идентифицируемый тип внутренних злоумышленников. Как правило, они являются звеном преступной цепочки или членом организованной преступной группы. Такие сотрудники имеют достаточно высокий уровень доступа к конфиденциальной информации, ущерб от их действий может стать фатальным для компании.

Злонамеренные инсайдеры представляют определённую опасность для информационной системы и конфиденциальных данных, однако их вероятность злоумышленных инцидентов ничтожно мала по сравнению с утечками информации, совершаемыми по неосторожности или вследствие технической безграмотности сотрудников. Увы, львиная доля всех инцидентов информационной безопасности на объекте любой сложности является следствием непредумышленных действий сотрудников. Возможностей для таких утечек информации множество: от ошибок ввода данных при работе с локальными сетями или интернетом до утери носителя информации (ноутбук, USB-накопитель, оптический диск); от пересылки данных по незащищённым каналам связи до непредумышленной загрузки вирусов с развлекательных веб-сайтов.

Безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе. Критериями информационной безопасности являются конфиденциальность, целостность и будущая доступность информации. При этом под конфиденциальностью понимается свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц. Целостность – это свойство информационных ресурсов, в том числе информации, определяющее их точность и полноту. В свою очередь доступность информации – это свойство, определяющее возможность получения и использования информации по требованию уполномоченных лиц.

Следует подчеркнуть, что темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы, руководящих документов. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии напрямую связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Современные методы управления рисками позволяют решить ряд задач перспективного стратегического развития предприятия. Во-

первых, количественно оценить текущий уровень информационной безопасности предприятия, что потребует выявления рисков на правовом, организационно-управленческом, технологическом и техническом уровнях обеспечения защиты информации. Во-вторых, в систему риск-менеджмента на предприятии может быть включена политика безопасности и планы совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании.

С этой целью рекомендуется осуществить расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, произвести соотношение расходов на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения. Необходимо также выявлять и проводить первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на наиболее уязвимые ресурсы.

Следует определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия, а также разработать необходимый пакет организационно-распорядительной или другой используемой на предприятии документации. Одновременно необходимо осуществлять разработку и согласование со службами предприятия, надзорными органами проекта внедрения необходимого комплекса защиты, учитывающего современный уровень и тенденции развития информационных технологий.

Кроме того, важным мероприятием поддержки системы безопасности информации является обеспечение поддержания внедренного комплекса защиты в соответствии с изменяющимися условиями работы предприятия, регулярными доработками и целенаправленным совершенствованием организационно-распорядительной и другой документации, модификацией технологических процессов и модернизацией технических средств защиты.

Система защиты информации на предприятии преследует такие цели как предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Помимо этого, система информационной безопасности нацелена на обеспечение устойчивого функционирования объекта: предотвращение угроз его безопасности, защиту законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом.

Обязательным условием эффективной реализации вышеупомянутых целей является действенный и комплексный контроль качества предоставляемых услуг и обеспечение гарантий безопасности имущественных прав и интересов клиентов.

В связи с этим, система информационной безопасности должна базироваться на следующих принципах:

- прогнозирование и своевременное выявление угроз безопасности информационных ресурсов, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц и, тем самым, ослабление возможного негативного влияния последствий нарушения информационной безопасности.

При разработке политики безопасности рекомендуется использовать модель, основанную на адаптации общих критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель отвечает требованиям специальных нормативных документов по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 “Информационная технология – методы защиты – критерии оценки информационной безопасности”, стандарту ISO/IEC 17799 “Управление информационной безопасностью”.

Поэтому, возвращаясь к вопросу обеспечения информационной защищенности украинских предприятий, необходимо подчеркнуть, что для них также, как и для российских, должна быть разработана и

внедрена аналогичная модель информационной безопасности.

Комплексная система защиты информации (КСЗИ) – это совокупность соответствующих организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Организационные мероприятия являются обязательной составляющей построения любой КСЗИ. Инженерно-технические мероприятия осуществляются по мере необходимости.

Организационные мероприятия включают в себя создание концепции информационной безопасности, а также:

- составление должностных инструкций для пользователей и обслуживающего персонала;
- создание правил администрирования составляющих информационной системы, учета, хранения, размножения, уничтожения носителей информации, идентификации пользователей;
- разработка планов действий в случае выявления попыток несанкционированного доступа к информационным ресурсам системы, выхода из строя средств защиты, возникновения чрезвычайной ситуации;
- обучение правилам информационной безопасности всех пользователей.

В случае необходимости, в рамках проведения организационных мероприятий, может быть создана служба информационной безопасности, проведена реорганизация системы делопроизводства и хранения документов.

Инженерно-технические мероприятия – совокупность специальных технических средств и их использование для защиты информации. Выбор инженерно-технических мероприятий зависит от уровня защищенности информации, который необходимо обеспечить.

Инженерно-технические мероприятия, проводимые для защиты информационной инфраструктуры организации, могут включать использование защищенных подключений, межсетевых экранов, разграничение потоков информации между сегментами сети, использование средств шифрования и защиты от несанкционированного доступа.

В случае необходимости, при проведении инженерно-технических мероприятий, может осуществляться установка в помещениях систем охранно-пожарной сигнализации, систем контроля и управления доступом. Отдельные помещения могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

Кроме рассмотренных элементов системы КСЗИ, важным представляется также идентификация субъектов и объектов этой системы.

Субъекты КСЗИ – это уполномоченные лица, которые осуществляют специфические функции по созданию и функционированию КСЗИ.

В процесс создания КСЗИ вовлекаются следующие стороны:

- организация, для которой осуществляется построение КСЗИ (заказчик);
- организация, которая реализует и осуществляет мероприятия по построению КСЗИ (исполнитель);
- Государственная служба специальной связи и защиты информации Украины (ГСССЗИУ) (контролирующий орган);
- организация, которая уполномочена и осуществляет государственную экспертизу КСЗИ (организатор экспертизы);
- организация, в случае необходимости привлекаемая заказчиком или исполнителем для выполнения некоторых работ по созданию КСЗИ (подрядчик).

Объектами защиты КСЗИ является информация, в любом ее виде и форме представления.

Материальными носителями информации являются сигналы. По своей физической природе информационные сигналы можно разделить на следующие виды: электрические, электромагнитные, акустические, а также их комбинации.

Сигналы могут быть представлены в форме электромагнитных, механических и других видах колебаний, причем информация, которая подлежит защите, содержится в их изменяющихся параметрах.

В зависимости от природы, информационные сигналы распространяются в определенных физических средах. Среды могут быть газовыми, жидкостными и твердыми. Например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и другие.

В зависимости от вида и формы представления информационных сигналов, которые циркулируют в информационно-телекоммуникационной системе (ИТС), в том числе и в автоматизированных системах, при построении КСЗИ могут использоваться различные средства защиты.

Как видно из проведенного изложения некоторых аспектов исследуемой темы, последняя является комплексной и в значительной степени структурированной, поэтому ее практическая реализация сопряжена с многочисленными трудностями и вызывает необходимость ее адекватного научного обоснования. На наш взгляд, вопросы,

затронутые в изложенной статье, должны привлечь внимание специалистов в области информационной защиты коммерческой тайны, а также менеджеров-практиков.

Список литературы

1. Шевелева Т. Правовые аспекты регулирования отношений, связанных с коммерческой тайной, в проекте Закона Украины “Об охране прав на коммерческую тайну” // Интеллектуальная собственность. – 2008, №7. – С.9-15.

2. Закон Украины “Об информации”. – Ведомости Верховной Рады Украины (ВВР), 1992, №48 (с изменениями и дополнениями) / www.rada.gov.ua.

3. Сляднева А. Определение понятия коммерческой тайны субъекта хозяйствования // Предпринимательство, хозяйство и право. – 2007, №9. – С.40-43.

4. Гражданский кодекс Украины. – Ведомости Верховной Рады Украины (ВВР), 2003, №№40-44 / www.rada.gov.ua.

5. Конституция Украины. – Ведомости Верховной Рады Украины (ВВР), 1996, №30 / www.rada.gov.ua.

6. Шулика С. Глобальные риски – 2012. [Электронный ресурс]. Код доступа: http://economics.lb.ua/world/2012/01/20/132846_globalnie_riski-2012.html.

7. Архипова З.В., Пархомов В.А. Информационные технологии в экономике: Учеб. пособие. Иркутск: Изд-во БГУЭП, 2003, 184 с. [Электронный ресурс]. Код доступа: http://ecsocman.hse.ru/text/19185598/.