УДК 341.238

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ

Статья посвящена проблеме обеспечения информационной безопасности предприятия как субъекта информационного права и информационных правоотношений. Под информационной безопасностью предприятия понимается сохранение в тайне коммерчески важной информации, позволяющей успешно конкурировать на рынке товаров и услуг.

Ключевые слова: информация, информационная безопасность предприятия.

Нашинец-Наумова Анфиса Юрьевна,

кандидат юридических наук, доцент кафедры конституционного и административного права Юридического института Национального авиационного университета

Предприятие – это инструмент удовлетворения потребностей и достижения определенных целей общества, социальных групп и индивидов. Эффективная деятельность предприятия предполагает, что она обеспечивает безопасность своих членов, выступает средством выживаемости человека, действующего в ее рамках. В тоже время само предприятие подвергается разнообразным опасностям, угрожающим ее существованию и целостности. Это обусловливает необходимость обеспечения деятельности по повышению защищенности жизненно важных интересов предприятия и её членов.

Проблема информационной безопасности предприятия, являясь проблематикой, как общей теории организации, так и информационного права, сегодня приобретает новые аспекты. Их появление предопределяется в первую очередь качественными изменениями самого социума и его внешней среды.

Человек в стремлении повысить степень своей защищенности от негативного воздействия природных сил так изменил условия своего существования, что они сами стали источником опасностей. Развитие общества, научно-технического прогресса со всей ясностью показывает, что среда обитания человека отнюдь не обладает такими качествами, как прозрачность, определенность, стабильность, что характерно для состояния безопасности в целом и информационной

безопасности в частности. Наоборот, сегодня ей присущи противоположные по своему содержанию характеристики, что спровоцировало новый виток в деятельности по обеспечению безопасности. Это предполагает новый уровень в разработке как теоретических вопросов информационной безопасности, так и практических мер по ее обеспечению.

Сегодня наблюдается повышенное внимание представителей всех социальных наук к тематике информационной безопасности. Необходимо отметить работы А. Баранова, К. Белякова, В. Брижко, И. Гаврилова, М. Гуцалюка, Л. Задорожной, А. Зинченко, Г. Лазарева, Д. Ловцова, А. Марущака, А. Новицкого, Р. Северин, В. Цымбалюка, Н. Швеца и др. Последнее время подготовлен ряд диссертационных исследований, посвященных вопросам информационной безопасности, при этом следует отметить, что большинство этих работ связано с вопросом информационной безопасности государства или обеспечения безопасности информационных систем. Однако проблема информационной безопасности предприятия остается недостаточно исследованной. Это связано в частности с тем, что авторы больше внимания уделяют обеспечению информационной безопасности государства, а также с отсутствием целенаправленного подхода к проблеме в целом у тех ученых, которые затрагивали роль информации в деятельности предприятия. Поэтому автор в данной работе пытается проанализировать вопросы обеспечения информационной безопасности предприятия как субъекта информационного права и информационных правоотношений. Основной целью данной статьи является изучение основных требований по обеспечению информационной безопасности предприятия.

В системе обеспечения безопасности все большее значение приобретает обеспечение информационной безопасности предприятия. Это связано с растущим объемом информации, с необходимостью ее хранения, передачи и обработки. Перевод значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

Необходимо отметить, что в научной литературе отсутствует единый взгляд на содержание понятий «информационная безопасность» и «информационная безопасность предприятия». Так, В. Цымбалюк характеризует информационную безопасность в условиях формирования информационного общества как защиту информации в автоматизированных компьютерных системах [5, с. 3], В. Фурашев считает, что информационная безопасность – это вид общественных информационных правоотношений по созданию, поддержке, охране и защите желательных для человека, общества и государства безопасных условий жизнедеятельности [6, с. 48], С. Гуцу предлагает рассматривать информационную безопасность как состояние защищенности потребностей в информации физических лиц, общества и государства, при котором обеспечивается их существования и прогрессивное развитие

независимо от наличия внутренних и внешних информационных угроз [7, с. 35], А. Литвиненко под информационной безопасностью понимает единство трех составляющих (обеспечение защиты информации, защиту и контроль национального информационного пространства, обеспечение надлежащего уровня информационной защиты) [8, с. 9]. Интересным и одновременно дискуссионным является определение, в котором Б. Кормич отмечает, что информационная безопасность – это защита установленных законом правил, по которым осуществляются информационные процессы в государстве, обеспечивающие гарантированные Конституцией условия существования и развития человека, всего общества и государства [9, с. 241]. Л. Харченко, В. Липкан, А. Логинов определили, что информационная безопасность – это составляющая национальной безопасности, процесс управления угрозами и опасностями государственными и негосударственными учреждениями, отдельными гражданами, при котором обеспечивается информационный суверенитет Украины [10, с. 32].

Таким образом, информационную безопасность следует рассматривать как обеспечение реализации национальных интересов с помощью разнообразных средств, имеющихся в ее распоряжении.

Относительно понятия «информационная безопасность предприятия» необходимо отметить, что оно является чрезвычайно актуальным на современном этапе развития информационных технологий, который сопровождается введением информационных систем во все сферы деятельности человека. Так, А. Сороковская определяет информационную безопасность предприятия как общественные отношения по созданию и поддержанию на должном уровне жизнедеятельности информационной системы субъекта хозяйственной деятельности [11], М. Танцюра характеризует информационную безопасность предприятия как сохранение конфиденциальности, целостности и доступности информации (доступность – это свойство быть достижимым и пригодным к использованию в информационной среде; целостность – свойство защищенности точности и полноты данных; конфиденциальность – свойство защищенности информации от несанкционированного использования) [12, с. 160].

Учитывая данные определения, мы согласны с А. Марущаком, что информационная безопасность предприятия – это целенаправленная деятельность его органов и должностных лиц с использованием разрешенных методов и средств по достижению состояния защищенности информационной среды предприятия и обеспечению его нормального функционирования и динамичного развития [13, с. 94].

Итак, суммируя вышесказанное, считаем необходимым подчеркнуть, что приоритетным направлением в процессе обеспечения информационной безопасности предприятия является сохранение в тайне коммерчески важной информации, позволяющей успешно конкурировать на рынке товаров и услуг.

Опыт показывает, что для борьбы с правонарушениями в сфере обращения информации на предприятии необходима целенаправленная организация процесса защиты информационных ресурсов. Источник этого вида угроз может быть внутренним (собственные работники), внешним (например, конкуренты) и смешанным (заказчики – внешние, а исполнитель – работник фирмы). Как показывает практика, подавляющее большинство таких правонарушений осуществляются самими работниками предприятия [14, с. 20].

Что же является непосредственным объектом правонарушений в сфере оборота информации? Прежде всего – это информация (данные). Правонарушитель получает доступ к информации, которая охраняется, без разрешения ее владельца или с нарушением установленного порядка доступа. Способы такого неправомерного доступа к компьютерной информации могут быть разными – кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, предоставление фиктивных документов на право доступа к информации, установка аппаратуры записи, подключаемой к каналам передачи данных. Причем доступ может быть осуществлен на территории предприятия, где хранятся носители, с компьютера на рабочем месте, с локальной сети, глобальной сети. Все угрозы объектам информационной безопасности по способу воздействия могут быть объединены в пять групп [15, с. 172]: информационные, физические, организационно-правовые, программно-математические, радиоэлектронные. Последствия совершенных противоправных действий могут быть различными: а) копирование информации (оригинал при этом сохраняется); б) изменение содержания информации по сравнению с той, которая была раньше; в) блокирование информации – невозможность ее использования при сохранении информации; г) уничтожение информации без возможности ее восстановления; д) нарушение работы компьютерной техники, системы или сети.

Проблемы, связанные с информационной безопасностью на предприятиях, могут быть решены только с помощью систематического и комплексного подхода. С методологической точки зрения, подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов.

В обеспечении информационной безопасности нуждаются разные субъекты информационных отношений:

– государство в целом или отдельные его органы и организации;

– общественные или коммерческие организации (объединения), предприятия (юридические лица);

– отдельные граждане (физические лица).

Весь спектр интересов субъектов, связанных с использованием информации, можно разделить на такие категории: обеспечение доступности, целостности и конфиденциальности ресурсов информационной среды [16, с. 13].

Иногда в ряд основных составляющих информационной безопасности включают защиту от несанкционированного копирования информации, но как нам видится, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это очевидно наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, принято выделять ее как важнейший элемент информационной безопасности [16, с. 17].

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Средства контроля динамической целостности применяются в частности при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. Но практическая реализация мер по обеспечению конфиденциальности современных информационных систем имеет в Украине серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми. Большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы [16, с. 41].

Значение каждой из составляющих информационной безопасности для разных категорий субъектов информационных отношений различно.

В случае государственных организаций во главу ставится конфиденциальность, поэтому скорее будет допущена возможность повреждения или уничтожения информации, чем ее разглашение. Также для государственных структур особую значимость имеет целостность информации. Доступность, как одна из составляющих информационной безопасности, по отношению к двум другим составляющим имеет наименьшее значение.

Для коммерческих организаций ведущую роль играет доступность информации. Особенно ярко это проявляется в разных системах управления – производством, транспортом и т. п. Внешне менее драматичные, но также весьма неприятные последствия –

и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.). Примером может быть и поставщик интернет-услуг (бесплатный почтовый сервер). Обычно для такого учреждения очень важно обеспечить возможность постоянного доступа пользователей к сервису (скорость Интернета для пользователей так же важна).

Целостность – также важнейший аспект информационной безопасности коммерческих структур. Набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Если в качестве объекта выступает, например, значение суммы финансовых средств на счету клиента (остаток), то главная задача банка – обеспечить невозможность ее несанкционированного изменения (целостность). При этом в экстраординарных ситуациях можно пойти на временное отсутствие доступа к счету или разглашение данных. В то же время конфиденциальность в случае коммерческой информации играет заметно меньшую роль [16, с. 43].

Целостность информации тесно связана с понятием надежности как технических, так и программных средств, реализующих процессы накопления, хранения и обработки информации. Из анализа угроз безопасности информации, целей и задач ее защиты следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты. Комплексность является одним из принципов, которые должны быть положены в основу разработки, как концепции защиты информации, так и конкретных систем защиты [17, с. 145]. Цели защиты информации на объектах защиты могут быть достигнуты при проведении работ по таким направлениям:

• определение охраняемых сведений об объектах защиты;

• оценка возможностей и степени опасности технических средств разведки;

• выявление возможных технических каналов утечки информации;

• анализ возможностей и опасности несанкционированного доступа к информационным объектам;

• анализ опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;

• разработка и реализация организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;

• создание комплексной системы защиты;

• организация и проведение контроля состояния и эффективности системы защиты информации;

• обеспечение устойчивого управления процессом функционирования системы защиты информации.

Процесс комплексной защиты информации должен осуществляться

непрерывно на всех этапах. Реализация непрерывного процесса защиты информации возможна только на основе систем концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации.

Для граждан на первое место можно поставить целостность и доступность информации, обладание которой необходимо для осуществления нормальной жизнедеятельности. Например, в случаях искажения информации во время выборов конфиденциальность не играет ключевой роли, хотя отметим, что физические лица сегодня являются самыми незащищенными субъектами информационных отношений.

Итак, на основании проведенного исследования можно отметить, что предприятия рассматриваются как субъекты информационного права, а потому мы должны изучать информационные правоотношения, в которые они практически вступают, реализуя полномочия, регулируемые нормами различных отраслей права.

При этом одним из важных аспектов, на котором должно быть сосредоточено внимание, является вопрос обеспечения информационной безопасности предприятия. Если процедуры создания, получения специальных статусов и разрешений, прекращения деятельности и надзора за такой деятельностью в большей степени относятся к предмету других отраслей права, то обеспечение информационной безопасности, потребность в котором, как автор пытался показать, проявляется в течение всего времени существования предприятия и его взаимодействия с другими субъектами, практически полностью относится к предмету информационного права. В то же время как невозможно в полной мере выделить информационную составляющую в деятельности предприятия, так очень сложно разграничить правовое регулирование этой сферы различными отраслями права.

Список использованных источников:

1. Танцюра М. Ю. Обеспечение эффективности системы информационной безопасности предприятия (на примере туристических предприятий АР Крым): автореф. дисс. на соискание науч. степени канд. экон. наук : спец. 08.00.04 «Экономика и управление предприятиями» / М. Ю. Танцюра. – Симферополь, 2012. – 19 с.

2. Об основных принципах информационного общества в Украине на 2007–2015 годы : Закон Украины от 9 января 2007 г. // Официальный вестник Украины. – 2007. – № 8. – Ст. 273.

3. Бачило И. Л. Гражданское общество и право / И. Л. Бачило // Информационные ресурсы России. – 2005. – № 3. – С. 10–15.

4. Сергиенко Л. А. Культура и гражданское общество / Л. А. Сергиенко // Информационные Ресурсы России. – 2007. – № 6. – С. 1–6.

5. 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. – № 8. – С. 30–33.

6. Фурашев В. М. Вопросы законодательного определения понятийно-категориального аппарата в сфере информационной безопасности / В. Н. Фурашев // Информация и право : научный журнал. – 2012. – № 1(4). – С. 46–56.

7. Гуцу С. Ф. Правовые основы информационной деятельности: учебное пособие / С. Ф. Гуцу. – М., 2009. – 48 с.

8. Литвиненко А. В. Проблемы обеспечения информационной безопасности в постсоветских странах (на примере Украины и России): автореф. дис. на соискание науч. степени канд. полит. наук : спец. 23.00.04 «Политические проблемы международных отношений, глобального и регионального развития» / А. В. Литвиненко. – М., 1997. – 18 с.

9. Кормич Б. А. Организационно-правовые основы политики информационной безопасности Украины : монография / Б. А. Кормич. – Одесса : Юридическая литература, 2003. – 472 с.

10. Харченко Л. С. Информационная безопасность Украины : Глоссарий / Л. С. Харченко, В. А. Липкан, А. В. Логинов. – К. : Текст, 2004. – 136 с.

11. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы [Электронный ресурс]. – Режим доступа : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

12. Танцюра М. Ю. Система управления информационной безопасностью предприятия / М. Ю. Танцюра // Развитие инновационной культуры общества : проблемы и перспективы: материалы науч.-практ. конф. (Симферополь, 2007 г.)/ Крымский институт бизнеса. – Симферополь: «Азгол-Пресс», 2007. – С. 159–161.

13. Марущак А. И. Информационно-правовые направления исследования проблем информационной безопасности // Государственная безопасность Украины / А. И. Марущак. – 2011. – № 21. – С. 92–95.

14. Северин Р. В. Сущность убытков в информационной сфере предприятия / Р. В. Северин // Информационное право. – № 1 (32) . – 2013. – С. 18–21

15. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – Н. : Новый юрист. – 2012. – 256 с.

16. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.

17. Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.

Нашинець-Наумова А. Ю. Інформаційна безпека підприємства: теоретико-методологічні основи правового забезпечення.

Статтю присвячено проблемі забезпечення інформаційної безпеки підприємства як суб'єкта інформаційного права та інформаційних правовідносин. Під інформаційною безпекою підприємства розуміється збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку товарів і послуг.

Ключові слова: інформація, інформаційна безпека підприємства.

Nashynets-Naumova A. Yu. Informational Security of an Enterprise: Theoretical and Methodological Grounds of Legal Support.

The article deals with the problem of informational security of the enterprise as a subject of the information law and information relationships. The term "informational security of the enterprise" means the ensuring of the confidentiality of the important commercial information, which allows competing in the market of goods and services.

Keywords: information, information security of the enterprise.

Стаття надійшла до редакції 12.12.2013