УДК 338.24:351.862.4

О.С. МОРОЗ (кандидат экономических наук, доцент кафедры менеджмента организаций)

Запорожская государственная инженерная академия, Запорожье

E – mail: oleg.moroz.55@mail.ru

Е.О. МОРОЗ (магистр права, юрисконсульт 1категории)

Открытое акционерное общество "Металлургический комбинат «Запорожсталь»", Запорожье

E–mail: moroz_eo@zaporizhstal.com

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ КОРПОРАТИВНОЮ БЕЗПЕКОЮ

Аналізуються проблеми, що виникають при створенні корпоративної служби безпеки та її інтеграції в загальну систему менеджменту в організації. В першу чергу подаються аналізу проблеми, що пов'язані з недостатньою правовою забезпеченістю процесу створення та функціонування служб безпеки в організаціях (особливо недержавної форми власності). В зв'язку з тим, що діяльність служб безпеки корпоративних структур, теоретично недостатньо досліджена й законодавчо в єдиному державному нормативно-правовому акті не врегульована, наводяться пропозиції по документарному оформленню при формуванні системи управління корпоративною безпекою та її інтеграції в існуючу систему менеджменту підприємства.

Ключові слова: *корпоративна безпека, інформація, нормативно – правовий акт, регламент системи безпеки, меморандум по забезпеченню безпеки*

Постановка проблемы

Обеспечение безопасности бизнеса — это одна из важнейших функций любой организации и предпринимателя. Развитие экономической конкуренции, необходимость достижения преимущества на рынке выдвигают перед субъектами хозяйствования задачи по созданию системы управления корпоративной безопасностью. Учитывая, что функции государства законодательно и административно увеличиваются, в процессе делегирования, при помощи законов и подзаконных актов, ряда существенных полномочий по обеспечению безопасности непосредственно юридическим и физическим лицам проблемы реализации корпоративной безопасности *наиболее актуализируются.* При этом, отношения, возникающие между предприятиями в связи деятельностью служб безопасности, *теоретически мало изучены и законодательно в едином нормативно-правовом акте не урегулированы*, что вызывает настоятельную необходимость не только создания системы управления корпоративной безопасностью, но и интеграцию её в общую корпоративную систему управления.

Исследования проблемы и нерешённые аспекты

В реалии существующего корпоративного регулирования неизбежно сталкиваются с потенциальными и насущными проблемами внедрения системы безопасности менеджмента на предприятии, к которым можно

отнести, в том числе, следующие [1]: декларативность норм Конституции в части обеспечения прав и свобод гражданина, безопасности бизнеса; коррумпированность органов власти и управления государства, командно-административные методы управления ведомствами; криминализация существующего порядка управления, рейдерство; правовой вакуум в сфере законодательства, призванного регулировать вопрос безопасности предпринимательской деятельности. Сегодня сотрудник службы, обеспечивающей корпоративную безопасность — это все чаще не человек с ружьем, а управленец, аналитик, менеджер. Это вызвано тем, что в последние годы наблюдается смена видения роли и сущности системы безопасности бизнеса, которая становится составной частью общей системы управления рисками организации (“*general risk management”*) [2].

Целью создания системы корпоративной безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее организации: успешно функционировать в нестабильных условиях внешней и внутренней среды; предотвращать угрозы собственной безопасности; защищать свои законные интересы от противоправных посягательств; охранять жизнь и здоровья персонала; не допускать хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации. Достижение этой цели требует решения таких следующих задач, как: выявления угроз стабильности работы предприятия и его развитию и выработка мер противодействия; обеспечения защиты технологических процессов; реализации мер противодействия всем видам шпионажа (промышленного, научно-технического, экономического и т.д.); своевременного информирования руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия; предупреждения переманивания сотрудников предприятия, обладающих конфиденциальной информацией; всестороннего изучения деловых партнеров; своевременного выявления и адекватного реагирования на дезинформационные мероприятия; разработки и совершенствования правовых актов предприятия, направленных на обеспечение его безопасности; реализации мер по защите коммерческой и иной информации; организации мероприятий по противодействию недобросовестной конкуренции; обеспечения защиты всех видов ресурсов предприятия; реализации мер по защите интеллектуальной собственности; организации и проведения мер по предотвращению чрезвычайных ситуаций;

выявления негативных тенденций среди персонала предприятия, информирования о них руководства предприятия и разработки соответствующих рекомендаций; организации взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;

разработки и реализации мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу; возмещения материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц. Результатом деятельности по обеспечению комплексной безопасности предприятия являются: стабильность (надежность) его функционирования и финансово-экономического состояния, личная безопасность персонала.

Цели статьи

Целью настоящей статьи является исследование регуляторных функций субъекта хозяйствования по формированию системы корпоративной безопасности и разработка предложений по её интеграции в общую корпоративную систему управления организации.

Результаты исследования

Объектом защиты корпоративной системы безопасности являются ресурсы в самом широком смысле: информация, интеллектуальная собственность, активы, имущество, клиенты, персонал, технологии и так далее. Сама система управления предприятием также является определенным ресурсом и требует защиты. Система безопасности предприятия может состоять из ряда подсистем, которые должны быть интегрированы в общую систему менеджмента (управления) предприятия. К таким подсистемам отдельные авторы относят [3]: собственно экономическая безопасность; информационная безопасность; техногенная безопасность; экологическая безопасность; психологическая безопасность; физическая безопасность; пожарная безопасность; научно-техническая безопасность. Управление организацией должно быть построено так, чтобы система безопасности не замыкалась только в отдельной структуре. Обеспечение безопасности — это забота не только службы безопасности, но и всего менеджмента компании. Система должна охватывать всех сотрудников, начиная с первого руководителя организации и заканчивая техническим персоналом. Когда же рынок динамично развивается, нужна гибкая система, поэтому и управление безопасностью необходимо рассматривать как развивающийся процесс. В процессе реализации управления безопасностью в организации, каждая компания выбирает свои приоритеты в развитии указанных направлений обеспечения безопасности. Практической схемы построения универсальной системы безопасности не существует. Каждая система корпоративной безопасности — это «уникальный продукт». Ее нужно строить, исходя из сущностных связей и действующих корпоративных нормативно – правовых актов (документации) и каждого конкретного предприятия, так как промышленное предприятие, торговая фирма и финансовая компания очень отличаются друг от друга. Кроме того, необходимо учитывать, что построение системы безопасности в организации неизбежно сталкивается с возникновением различных противовесов, которые необходимо урегулировать в установленном в организации порядке с учётом норм действующего законодательства.

Существуют типовые алгоритмы локализации угроз и этапы

формирования системы безопасности, которые применимы при создании любой системы безопасности. Так, например, целостная система безопасности должна предусматривать как профилактическую работу, так и внутреннюю оперативную работу. Профилактическая работа допускает использование технических методов и способов контроля, однако возможность их проведения в отношении сотрудников должна быть, в обязательно порядке, закреплена письменным согласием самого работника – иначе следует нарушение закона. Внутренняя оперативная работа, представляющая собой процесс выявления информации опасного (сигнального) характера, а также постановки конкретных задач сотрудниками безопасности по контролю исполнения тех или иных режимных мер также должна базироваться на внутренних нормативных документах, утверждённых в установленном порядке.

К основным этапам формирования системы корпоративной безопасности организации можно отнести следующие: идентификация источников угроз и рисков для бизнеса; оценка степени серьезности угрозы (уровень ресурсов источника угрозы и его цели — возможного ущерба ресурсам предприятия); выделение групп источников угроз по целям, ресурсам, интересам; оптимальное выделение ресурсов, выбор и применение оптимального алгоритма локализации угроз (построение системы защиты) с учетом выделенного на это бюджета. При построении любой системы корпоративной безопасности организации имеет смысл руководствоваться универсальным и давно проверенным правилом: “предвидеть опасность, по возможности избегать ее, при необходимости – действовать”. [4] Таким образом, создание эффективной системы менеджмента предприятия, включая систему управления его безопасностью, подразумевает: формирование ее концепции в общей структуре бизнеса; интеграцию системы безопасности в производственную и организационную структуры предприятия; интеграцию системы безопасности в существующую документацию предприятия (разработка регламентирующих документов (положений, инструкций, порядков взаимодействия и других процедур - «процессуальных кодексов»); учет специфики коммерческой деятельности предприятия, его информационных и других коммуникационных связей.

В регламентирующих документах не только профильной службы, но и параллельных подразделений должны быть прописаны направления сопряженной безопасности, формы взаимодействия и обязанности специалистов-партнеров. Для создания эффективной системы взаимосвязей необходима программа по формированию наполняемости работы системы безопасности предприятия, ее оценки и поиска «узких мест». Особое внимание должно быть обращено на то, что перед тем, как строить и интегрировать систему безопасности в общую систему менеджмента, действующую на комбинате, необходимо определить: что необходимо обеспечить защитой; кто этим будет заниматься; каким образом будет осуществляться деятельность по обеспечению безопасности. Таким образом, одним из видов отношений субъектов хозяйствования, нуждающихся в

правовом регулировании, является отношения по *закреплению и интеграции созданной системы корпоративной безопасности организации в действующую документацию предприятия.* К примеру, в действующих нормативных актах дается легальное определение понятия коммерческой тайны, определяется перечень сведений, которые не могут составлять коммерческую тайну [5]: *государственная тайна* - вид секретной информации, охватывающий сведения в сфере обороны, экономики, науки и техники, внешних отношений, государственной безопасности и охраны правопорядка, разглашение которых может привести к негативным последствиям государственного суверенитета Украины (ст. 1 ЗУ «О Государственной тайне»); *коммерческая информация* – информация, которая является секретной в том понимании, что она (в целом либо в определенной форме и совокупности ее составных) неизвестна и/или не является легкодоступной для лиц, которые обычно имеют дело с видом информации;

информация с ограниченным доступом – по своему правовому режиму разделяют на: *а) конфиденциальную информацию*- сведения, находящиеся во владении, пользовании либо распоряжении отдельных физических или юридических лиц и распространяются по их желанию в соответствии с предусмотренными ними условиями; б) *тайную информацию* - информацию, содержащую сведения, являющиеся государственной либо другой тайной, разглашение которой наносит урон физическому лицу, обществу и государству. Коммерческая информация – информация, имеющая коммерческую ценность для лица, которому она принадлежит и в связи с этим является предметом адекватных соответствующим обстоятельствам мер по сохранению ее секретности, принятых лицом, законно контролирующим эту информацию (ст. 505 Гражданского Кодекса Украины). Состав и объем сведений, составляющих коммерческую тайну, способ их защиты определяются субъектом хозяйствования в соответствие с действующим законодательством (ст. 36 Хозяйственного Кодекса Украины). Защита информации с ограниченным доступом регулируется Законом Украины «Об информации» (ст. 30). Так как к информации с ограниченным доступом относится также банковская тайна (информация, относительно деятельности и финансового положения клиента, которая стала известна банку в процессе обслуживания клиента и взаимоотношений с ним или третьими лицами при предоставлении услуг банка и разглашение, которой может привести к причинению материального или морального вреда клиенту), то она также регулируется Законом Украины «О банках и банковской деятельности» (ст. 60).

Вместе с тем, для обеспечения права предприятия на коммерческую тайну, норм, содержащихся в государственных нормативно-правовых актах, недостаточно. Поэтому субъекты хозяйствования сами регулируют, среди прочего, отношения по определению и охране коммерческой тайне путем принятия соответствующих локальных документов. Следовательно, правовое регулирование деятельности службы по обеспечению

корпоративной безопасности необходимо не только на уровне нормативно-правовых актов, но и на локальном уровне – в виде корпоративных актов управления предприятия. По мнению отдельных исследователей, на уровне локального корпоративных нормативного акта хозяйствующего субъекта необходимо определять не только конкретный перечень сведений, относимых к коммерческой тайне, но и мероприятия, определяющие порядок обращения с ней и направленные на ее защиту, сроки, в течение которых сведения, по мнению их обладателя, составляют коммерческую тайну, а также максимальные пределы ее стоимостной оценки на момент введения ограничения по ее распространению [6].

Таким образом, базой для работы по формированию системы управления корпоративной безопасностью и интеграции её в существующую систему менеджмента предприятия должно стать *принятие корпоративных нормативных документов регламентирующих этот процесс*. То есть создать своеобразную «*оболочку по обеспечению интеграции*». В то же время, речь должна идти не об одном локальном акте, а о нескольких корпоративных актах. Причем одни локальные акты предприятия будут являться общими, поскольку будут включать в себя все положения и функции по обеспечению корпоративной безопасности, а другие - специальными, регулирующими отдельные структурные элементы корпоративной системы безопасности и возможность её интеграции в существующую систему менеджмента. На основании изложенного, предлагается предусмотреть при создании системы управления корпоративной безопасностью оформление в установленном в организации порядке общего Регламента системы безопасности организации, включающего в себя:

- Положение об управлении безопасностью в организации;
- Порядок взаимодействия служб, отделов и других подразделений существующей системы управления организации при осуществлении деятельности по обеспечению корпоративной безопасности;
- Порядок взаимодействия службы безопасности со сторонними организациями, предоставляющими услуги (работы) для организации;
- Положение о коммерческой тайне в организации;
- Примеры типовых договоров о соблюдении коммерческой тайны (с нерезидентами, юридическими лицами, физическими лицами). Учитывая требования действующего законодательства, для обеспечения действенности документов, предусмотренных Регламентом системы безопасности организации, представляется целесообразным создание корпоративного Меморандума по обеспечению безопасности в организации, который должен быть доведен до сведения и соответствующим образом акцептирован (по подобию правил охраны труда) каждым сотрудником предприятия. Ответственность работника за соблюдение правил корпоративной безопасности, в первую очередь должна быть отражена во внутренней документации предприятия, может быть предусмотрена как в общих локальных документах, так и в тексте контракта заключаемом

работником с собственником предприятия, а также в коллективном договоре, правилах внутреннего трудового распорядка. В таком случае обеспечиваются вопросы по осуществлению деятельности контролирующими службами и соотношение такой деятельности с конституционными правами граждан на защиту сведений о личности и неприкосновенность частной собственности (ст. 29, 31, 34, 60, 64 Конституции Украины – фотографирование, видеонаблюдение и аудиозапись, надзор, превентивные меры обеспечения безопасности, по подобию применяемые правоохранительными органами при осуществлении функций согласно действующему законодательству).

Такую точку зрения разделяет ряд авторов, занимающихся исследованием данной проблемы [7]. Так, например, Е. Кибенко считает, что ответственность за разглашение конфиденциальной информации может устанавливаться не только действующим законодательством, но и специальными нормативными актами организации с которыми ознакомлены и согласны её работники, в том числе Положение о коммерческой тайне, Положение об ответственности должностных лиц общества и т.п. [8]. Таким образом, предлагается в Меморандуме по обеспечению безопасности предусмотреть следующие взаимоотношения между организацией и её работниками на основе *ознакомления работников под роспись о его согласии с:* доступом к информации, составляющей коммерческую тайну, необходимым для выполнения им своих трудовых обязанностей; перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты; установленным в организации режимом коммерческой тайны и мерами ответственности за его нарушение; перечнем и объемом личной информации, разрешенной к хранению и использованию рабочем месте, компьютере и т.п.; методами и способами осуществления деятельности службой безопасности (видеонаблюдение, аудиозапись, фотографирование, досмотр рабочего места и личных вещей в случае выявления противоправных деяний либо наличия аргументированных подозрений и т.п.); возможностью составления, перечнем и результатом применения документов реагирования службой безопасности (Акты, протоколы, предписания); порядком возмещения причиненного ущерба вследствие нарушения требований о конфиденциальности.

В Меморандуме по обеспечению безопасности необходимо детально очертить и регламентировать случаи применения методов по управлению безопасностью, а также возможности реагирования и объем применяемых при этом средств, а также создание работнику необходимых условий для соблюдения, им установленного в организации режима управления безопасностью. При этом, режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Выводы и предложения

На основании исследования закрепления права организации на обеспечение корпоративной безопасности при формировании системы управления безопасностью и интеграции её в существующую систему менеджмента предприятия, помимо использования типовых алгоритмов локализации угроз и этапов формирования системы безопасности, целесообразно: регулирование деятельности службы безопасности организации осуществлять на основании сочетания государственного нормативно - правового регулирования и корпоративного (локального, негосударственного) регулирования, осуществляемого в организации. На практике отношения по регулированию такой деятельности в большей степени осуществляются локальными корпоративными актами и в меньшей степени – общими нормативно - правовыми актами, принятыми государством; право службы безопасности организации на осуществление деятельности по обеспечению корпоративной безопасности, закреплённое в локальных актах, необходимо систематизировать в своде таких актов в виде Регламента системы безопасности организации; обязательства и права работников организации по обеспечению корпоративной безопасности, а также цели, принципы и меры регуляторной деятельности, осуществляемой организацией в этом направлении, необходимо закрепить принятием Меморандума по обеспечению безопасности между собственником организации (уполномоченным лицом) и её работником; интеграция системы управления корпоративной безопасностью в существующую систему менеджмента организации обеспечивается путём учета действующих в организации стандартов, правил и Положений при разработке корпоративных локальных актов нормативно - правового регулирования, входящих в состав Регламента системы безопасности организации и Меморандума по обеспечению безопасности.

Список использованных источников:

1. Ершова И.В. Предпринимательское право. – М.: Наука, 2003. – С.54;
2. Соловьев И.Н. Информационная и правовая составляющая безопасности предпринимательской деятельности //Налоговый вестник, №10,11 август, сентябрь 2011г.- С.19-20;
3. Ростова Н. Безопасность бизнеса // Консультант, №9, май 2005 г.- С.8;
4. Методика выделения сведений, составляющий коммерческую тайну // Электронный ресурс. Режим доступа: www. Kiev-security.org.ua;
5. Кузнецов И. Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. М.: Изд-во Яуза, 2001.- С.28-30;
6. Янина Е.В. Актуальные вопросы информационной безопасности: защита коммерческой тайны хозяйствующего субъекта в рамках локального нормативного акта //Актуальные проблемы современной науки. – 2003. - №2. – С. 109-111;
7. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Кондор, 2000.- С.43-44;
8. Кибенко Е.Р. Корпоративное право Украины. – К. : Професіонал, 2009. – С. 88-89.

REFERENCES (TRANSLATEO & TRANSLITERATED):

1. Ershov I.V. Business law. - Moscow: Nauka, 2003. - P. 54;

2. Solovyov I.N/ Information and legal component Business Security // Tax Bulletin, № 10,11 August and September 2011. - P.19-20;

3. Rostova H. Safety Business / / Consultant, № 9, May 2005 - P. 8;

4. Method for detecting the information constitutes a trade secret // Electronic resource. Mode of access: www. Kiev-security.org.ua;

5. Kuznetsov H. Information: collection, protection, analysis. Tutorial for information and analysis. Moscow: Jauza in 2001. - Pp. 28-30;

6. Yanina E.V. Actual questions information security: protection trade secrets business entity within the local regulatory act // Actual problems of modern science. - 2003. - № 2. - Pp. 109-111;

7. Androschuk G.A., Krainev P.P. The economic security of the enterprise: the protection of trade secrets. - K.: Condor, 2000. - Pp. 43-44;

8. Kibenko E.R. Corporate law Ukraine. - K.: Profesional, 2009. - Pp. 88-89.

О. С. МОРОЗ
Запорожская Государственная Инженерная Академия, Запорожье
E – mail: oleg.moroz.55@mail.ru
Е. О. МОРОЗ
ОАО “Металлургический комбинат «Запорожсталь»”, Запорожье
E – mail: moroz_eo@zaporizhstal.com

ФОРМИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ БЕЗОПАСНОСТЬЮ

Анализируются проблемы, которые возникают при создании корпоративной службы безопасности и ее интеграции в общую систему менеджмента в организации. В связи с тем, что деятельность служб безопасности корпоративных структур, теоретически недостаточно исследована и законодательно в едином государственном нормативно-правовом акте не урегулирована, приводятся предложения по документарному оформлению при формировании системы управления корпоративной безопасностью и ее интеграции в существующую систему менеджмента предприятия.

Ключевые слова: корпоративная безопасность, информация, нормативно – правовой акт, регламент системы безопасности, меморандум по обеспечению безопасности

O. MOROZ
Zaporozhye State Engineering Academy, Zaporozhye
E – mail: oleg.moroz.55@mail.ru
E. MOROZ
OJSC "Metallurgical plant" Zaporizhstal "", Zaporozhye
E – mail: moroz_eo@zaporizhstal.com

FORMATION OF CONTROL SYSTEM BY CORPORATE SAFETY

Analyze the problems that arise when creating a corporate security and its integration into the overall management of the organization. Due to the fact that the security services of corporate structures, insufficiently studied theoretically and legally in the single state legal act is not regulated, provides suggestions for documentary design in forming corporate security management system and its integration into existing enterprise management.

Keywords: corporate safety information, normative - legal act, the rules security systems, the memorandum on security

Стаття надійшла до редколегії 21.02.13
Прийнята до друку 26.02.13
Рецензент: д.філософ.н., проф. Попов С.М.