ИНФОРМАЦИЯ — очень дорогой ресурс

Александр Васильевич Мигутский, генеральный директор ЗАО «БЕЛТИМ СБ»

Уважаемые коллеги, каждый из нас знает, что информацию нужно оберегать, хранить, защищать, но не всегда мы придаем этому значение и знаем, как это делать. В связи с этим мы хотим еще раз напомнить, насколько важно руководителям и первым лицам органов государственного управления и субъектов хозяйствования ориентироваться в вопросах обеспечения безопасности и защиты информации. Наша компания на этом рынке уже одиннадцать лет позиционирует себя как системный интегратор. Мы имеем богатый опыт маркетинговой работы и при продвижении своих услуг стремимся к прямым контактам с первыми лицами потенциальных заказчиков.

Как практикующий субъект хозяйствования некоторые актуальные вопросы и аспекты данной деятельности планируем изложить на страницах данного журнала.

Оставим на потом техническое обеспечение, конкретные решения и предложения, а сегодня поговорим о главной проблеме, которая стоит перед нашими менеджерами на протяжении всего этого времени. Дело в том, что большинство из читающих сейчас эту статью не всегда в достаточной мере сознают и оценивают значение и стоимость (реальную цену) информационного ресурса, а он во многом является главным во всем управленческом процессе. Иногда об этом просто некогда подумать.

Информация — это основа всех управленческих решений и действий, это экономика, финансы, ноу-хау, технологии, схемы взаимодействия с партнерами и т.д. Ее содержание, состояние (безопасность, защищенность, доступность) влияют на положение дел руководимых вами объектов и отраслей и, в конце концов, и на вашу личную безопасность.

В нашей практической работе и организации маркетинга самое сложное — это дойти до первых лиц, от которых зависит принятие управленческих решений в указанной области. Как правило, обращения, информационные материалы и т.д. передаются для рассмотрения и подготовки предложений в службу безопасности или IT-специалистам. Чаще всего ни те, ни другие нашими союзниками на объекте на этом этапе не становятся. В привлечении сторонних специалистов к решению специфических и часто весьма конфиденциальных задач они видят угрозу своему имиджу и авторитету. Чаще всего такую позицию занимают системные администраторы. Но как только первое лицо понимает суть наших предложений, степень вероятных угроз и рисков, связанных с утечкой информации (хищение, незаконное изменение (искажение), утрата и т.д.), вопрос сразу переходит в другую плоскость. Для нас это самая трудная стадия проекта. Технические, организационные и финансовые вопросы решаются специалистами в штатном режиме и достаточно просто.

Символом нашей компании — в грустном смысле — является «жареный петух», потому что пока он не клюнет, директора и другие руководители за помощью к нам обращаются редко.

Мы достаточно часто сталкиваемся со случаями, когда пренебрежение информационной безопасностью приводило к большим проблемам, финансовым потерям, другим издержкам, вплоть до проблем личного характера руководителей предприятия или организации.

Например, к нам обратилось руководство достаточно крупного предприятия с просьбой о создании системы защиты информации всего объекта. В то время решался вопрос об акционировании данного объекта, и на него имело виды несколько недобросовестных российских покупателей. В процессе нашей работы было установлено, что конкуренты незаконным путем организовали технические каналы утечки информации и, имея об объекте сугубо конфиденциальную и реальную информацию, планировали при покупке снизить цену.

На другом объекте конкурирующая фирма, естественно, незаконным путем, заполучила информацию, содержащую конструкторскую документацию на новое изделие, на разработку которого были затрачены очень большие средства. Изделие было представлено на рынке под маркой конкурента до того, как сам разработчик смог развернуть производство.

А вот недавний случай, который получил огласку. На одной из фабрик, подлежащих продаже (акционированию), мы проводили проверку служебных помещений, где обсуждались конфиденциальные вопросы финансового положения, перспективы акционирования, и выявили подслушивающее устройство достаточно высокого качества. Впоследствии выяснилось, что «жучок» установили т.н. «черные риэлторы», которые стремились в несколько раз снизить продажную цену, обанкротить, а затем купить за бесценок эту фабрику.

В нашем архиве имеется ряд других примеров, однако, как правило, факты реализованных посягательств на информационный ресурс, который выражается в самых различных формах — от сведений о личности руководителя, его доходах, личных качествах и заканчивая коммерческой тайной, — должностные лица стараются не предавать огласке. Причины самые разные. Руководители иногда не придают значения данным фактам, считая, что информационная безопасность здесь вовсе не при чем: люди, дескать, плохие, стечение обстоятельств, техника подвела и т.д. Или не хотят привлекать внимание многочисленных проверяющих и контролирующих органов, а заинтересованные службы не

Справка «ТБ»

Мигутский Александр ВАСИЛЬЕВИЧ. *Родился в 1947 году. Окончил среднюю школу в г. Марьина Горка Минской обл. в 1966 г.; Минский радиотехнический институт в 1974 г.; Высшую школу КГБ СССР в 1985 г.; Академию управления при Президенте Республики Беларусь в 1997 г.*

Служил в органах государственной безопасности, работал в Институте национальной безопасности Республики Беларусь. С 1999 г. работал в ООО «БелТим», с 2004 г. является ген. директором ЗАО «БЕЛТИМ СБ», вопросами защиты информации, информационной и общей безопасности занимается более 30 лет.

Опубликованы два учебных пособия в Институте национальной безопасности по специальным дисциплинам.

хотят «выносить сор из избы», терять свой имидж и авторитет внутри предприятия.

Государство озабочено проблемами информационной безопасности, и Совет Министров Республики Беларусь издал Постановление N 675 от 26 мая 2009 г. «О некоторых вопросах защиты информации». Оно определяет «порядок защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено», и требует от руководителей субъектов хозяйствования и госуправления принятия действенных мер по ее защите. Компания «БЕЛТИМ СБ» предлагает свои услуги и готова участвовать в реализации требований данного Постановления и других нормативных актов в интересах любого заказчика независимо от формы собственности.

В этом материале мы не касаемся защиты информации, содержащей государственные секреты. В этой области процессы в определенной степени урегулированы нормативными документами. А вот на вопросы создания **режима «коммерческой тайны»** стоит обратить внимание. Актуальность этой темы возрастает в условиях экономического и финансового кризиса. Сегодня обострилась конкурентная борьба за рынки сбыта, используются некорректные, а то и незаконные средства и методы при реализации процессов приватизации (акционирования). При этом информация является главным объектом устремлений недобросовестных, в первую очередь иностранных, оппонентов. Под угрозой экономическая и энергетическая безопасность. И везде информация играет ведущую, если не сказать — главную, роль. Вместе с тем решение поднимаемых нами вопросов в лучшем случае отодвигается на второй план, в худшем случае они вообще не рассматриваются и не решаются.

Мы считаем, что приоритет информационной безопасности на каждом объекте должен быть однозначным.

Нашей компанией в процессе длительной работы с предприятиями и организациями определены следующие основные проблемы в области информационной безопасности:

- недооценка значения защиты информации;
- отсутствие комплексного подхода в обеспечении информационной безопасности;
- отсутствие системы управления информационной безопасностью; существующие службы безопасности наделены в основном охранными функциями;
- не определены цели и задачи защиты информации, не определены и не оценены критичные ресурсы;
- не определены и не оценены угрозы, уязвимости, риски критичных ресурсов;
- отсутствие системы взаимосвязанных организационных документов по обеспечению информационной безопасности;
- не сформирована среда безопасности;

внедрение компьютерной техники и программного обеспечения, модернизация автоматизированных систем производится без учета вопросов информационной безопасности;

- отсутствие контроля состояния безопасности (экспертной оценки или периодического аудита).

Комплексный подход — вот оптимальный путь к сохранению ресурсов, сокращению затрат на борьбу с различными угрозами. Мы предлагаем объединять в интегрированные системы безопасности все имеющиеся на предприятии силы и средства. Такой подход исключит дублирование при закупках оборудования, облегчит обслуживание, повысит оперативность соответствующих служб. Мы ратуем за создание объединенных служб безопасности, которые руководили бы и организовывали взаимодействие различных служб, подразделений и отдельных сотрудников в целях защиты информационных ресурсов.

Получить максимальную отдачу от всех мер и средств защиты, избежать неразумной избыточности в защите и, соответственно, излишних финансовых затрат позволит системное согласование всех мер защиты между собой и объединения их в комплексную систему безопасности. Хотелось бы, чтобы такой подход находил поддержку у тех из вас, кто действительно заинтересован в делах своей организации, обеспокоен состоянием информации и общей безопасности.

Специалисты компании «БЕЛТИМ СБ» готовы участвовать в любых мероприятиях по защите вашей личной и служебной информации — начиная от проверки помещений на наличие «жучков» и других каналов утечки, поставки различных средств защиты до реализации комплексных технических и программных проектов информационной и общей безопасности. ■

**Республика Беларусь,
220002, г. Минск,
пр-т Машерова, 25, офис 434,
Тел/факс.: (017)334-99-11,
334-95-12,
e-mail: migutsky@beltim.by,
www.beltim.by
УНП: 190527159**

УНП: 100972915