following an earthquake in the nearby of the Indonesian Island of Sumatra, a gigantic *tsunami*-wave was created. The number of fatalities is being estimated at over 300000, wounded at a few million. It was perceived that the environment was friendly, safe.

References:

1. DWORZECKI J.: KOCHAŃCZYK R.: *Współczesne zagrożenia*. Gliwice: GWSP 2010.
2. KORZENIOWSKI L.F. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS 2008. http://www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66
3. LEWIN K.: *Principles of Topological Psychology*. New York: 1936.
4. SZMIT M.: *Informatyka w zarządzaniu*. Warszawa: Difin, 2003.
5. TOMASZEWSKI T.: *Psychologia*. Warszawa: PWN 1977.

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ СТАНДАРТА ISO 27001 В СФЕРЕ PUBLIC RELATIONS (PR)

Анатолий КРАПИВЕНСКИЙ,
ГОУ ДПО «Волгоградский институт молодежной политики и социальной работы» (Российская Федерация)

The process of informational security ensuring in the XXI century is actual practically for all the fields of human activity, especially for such a basic field of social stability as Public Relations (PR). Author investigates an opportunity of application of standard ISO 27001 in the above area.

Процесс связей с общественностью, или Public Relations (PR), вне зависимости от того, на каком уровне он осуществляется (государство-общественность, организация-общественность, политик-общественность и т.д.), по сути представляет собой частный вариант достижения общественного консенсуса, в котором заинтересованы все задействованные в данном процессе социальные акторы – как коллективные, так и индивидуальные.

PR-деятельность представляет собой, с одной стороны, разновидность процесса управления (в данном случае – управления общественным мнением по какому-либо значимому для базисного субъекта вопросу), а с другой стороны – разновидность процесса коммуникации (информационного обмена, инициированного базисным субъектом).

С функциональной точки зрения управление есть "целенаправленное воздействие на сознание и поведение людей, осуществляемое с целью направить их действия на достижение желаемых целей" [1: 4], а в самом общем, схематичном виде - "воздействие субъекта управления на его объект" [2: 33]. В свою очередь,

коммуникация заключается в "информационном воздействии субъекта коммуникации на объект, преследующем цели, заданные субъектом" [3: 40].

По определению Э.А. Сидельник, "в современной литературе сложилось два подхода, определяющие сущность PR: социальный и технологический. Первый подразумевает достижение социального согласия, обеспечение социального взаимодействия… Второй подход обращается к технологиям управления, методам воздействия на людей" [4: 5].

Очевидно, что именно второй подход (технологический) и позволяет говорить о возможности управления уровнем информационной безопасности в данном процессе.

В этой связи вызывает интерес возможность использования стандарта ISO 27001 Международной организации по стандартизации (International Organization of Standardization) применительно к сфере Public Relations.

Указанный стандарт "предназначен для разработки системы управления информационной безопасностью организации вне зависимости от ее сферы деятельности" [5]. Более того, система управления информационной безопасностью (СУИБ) — это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности. Система управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы. Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления» [6].

Российский аналог этого стандарта – ГОСТ Р ИСО/МЭК 27001-2006 указывает, что при разработке системы менеджмента информационной безопасности (СМИБ) необходимо: " a) определить область и границы действия СМИБ с учетом характеристик … организации, в том числе детали и обоснование любых исключений из области ее действия; b) определить политику СМИБ на основе характеристик бизнеса, организации, …которая: 1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере информационной безопасности (ИБ); 2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности; 3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ; 4) устанавливает критерии оценки рисков; 5) утверждается руководством организации; c) определить подход к оценке риска в организации, для чего необходимо: 1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности; 2) разработать критерии принятия риска и определить приемлемые уровни риска. Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты" [7: 3-4].

Следовательно, стандарт ISO 27001 по своим принципиальным положениям, касающимся построения эффективной системы управления информационной безопасностью, вполне может быть применим и к сфере Public Relations.

Здесь хотелось бы уточнить три момента:

1) под риском в PR следует понимать "отказ от предупредительных мер" [8: 157] по пресечению угроз общества в данной сфере деятельности;
2) несмотря на то, что декларируемой целью PR-деятельности в первую очередь является удовлетворение интересов именно ее организатора, что, как уже указывалось выше, происходит при любой коммуникативной интеракции, тем не менее, в рамках PR, безусловно, некорректно рассматривать общественность как жертву базисного субъекта (организатора) PR-акций. Говорить о наличии жертвы в данном случае неуместно, так как цель PR-акции по определению не должна нарушать законодательно закрепленные права общественности, а при отсутствии нарушения прав объекта информационного воздействия, его невозможно рассматривать в качестве жертвы;
3) определять законодательно закрепленные правила ведения коммуникативной деятельности в сфере PR и обеспечивать соблюдение действующего законодательства, является прерогативой государства. В Российской Федерации эта деятельность регулируется, в частности, Доктриной информационной безопасности Российской Федерации (утверждена Президентом РФ 9 сентября 2000 г., № Пр-1895), Законом РФ «О средствах массовой информации» от 27.12. 1991 г. № 2124-1, Федеральным законом «О противодействии экстремистской деятельности» от 25.07.2002 г. №114-ФЗ, Федеральным законом «О рекламе» от 13.03.2006 г. № 38-ФЗ и рядом других нормативно-правовых актов.

Литература:

1. Гулиев М.А., Епифанцев С.Н., Самыгин С.И. Социология и психология управления. – Ростов н/Д: Феникс, 2006.
2. Шепелева Ю.Е. Муниципальное управление: организационно-правовой аспект. М.: АНО РЖ «Социально-гуманитарные знания», 2006.
3. Науменко Т.В. Социология массовых коммуникаций в структуре социологического знания // Социологические исследования. – 2003. - № 10.
4. Сидельник Э.А. PR в современном обществе: сущность и социальное значение. – Таганрог: Изд-во ГОУ ВПО «ТГПИ», 2005.
5. Digital Security: Сертификация по ISO 27001. - http://dsec.ru/consult/cert
6. Понятие системы управления информационной безопасностью / Global Trust Solution Limited - http://www.globaltrust.ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu

7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования / ФГУП «Стандартинформ» . – М.: «Московский печатник», 2008.
8. Луман Н. Понятие риска: Пер. с нем. // THESIS: теория и история экономических и социальных институтов и систем. — 1994. — № 5.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

***Владимир ШКВИР**, Львовская Политехника, (Украина),*
***Анджей АУГУСТЫНЕК**, Научно-технологический Университет, Краков, (Польша)*

В процессе подготовки специалистов по экономическим специальностям (бухгалтерский учет, менеджмент, маркетинг и другие), необходимо должное внимание уделять основам информационной безопасности. Это обусловлено рядом объективных причин, основными из которых являются следующие:

- деятельность экономистов, напрямую связана с формированием информационных ресурсов предприятия, часть которых попадает под действие Закона «О коммерческой тайне»;
- технологические процессы сбора, обработки и хранения информации, выполняемые пользователями, должны быть надежно защищены от несанкционированного доступа и утечки.

Предлагаемые структура и состав средств обеспечения информационной безопасности, используемые пользователями, включает следующие компоненты:

- правовые методы защиты. Пользователи должны обладать глубокими знаниями законодательного обеспечения, которое регулирует отношения в области информационных отношений. В первую очередь, это относится к Закону «О коммерческой тайне», «О персональных данных», «О бухгалтерском учете» и др.;
- организационные средства защиты;
- технические и программные средства.

Пользователи должны понимать и знать основные принципы системы информационной безопасности. Основными из них являются::

- принцип законности – заключается в соответствии принимаемых мер законодательству о защите информации, а при отсутствии соответствующих законов – другими нормативными документами по ее защите;
- принцип комплексности – с позиций предотвращения разноплановых угроз и используемых методов. Имеется в виду полнота защиты по