МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ ЗАЩИТЫ ИНФОРМАЦИИ: ОТДЕЛЬНЫЕ АСПЕКТЫ

Наталья ЖМУР,
соискатель Юридического института
Национального авиационного университета

Summary

Determined that the transnational nature of information threats led to the need for international cooperation in the field of information security. The purpose of the work is to determine the international legal standards in the field of information security. In this connection describes the main types of international legal standards for the protection of the information, outlined prospects of international legal standards into national legislation. It is concluded about the necessity to take into account in developing of information protection systems a large number of international legal standards that had been tested already.

Key words: international standards, a system of information protection, information security management, international standards of information security.

Аннотация

Определено, что транснациональный характер информационных угроз обусловил необходимость международного сотрудничества в сфере защиты информации. Целью работы является определение международно-правовых стандартов в сфере защиты информации. В статье определены основные виды международно-правовых стандартов в сфере защиты информации; охарактеризованы основные виды международно-правовых стандартов в сфере защиты информации; определены перспективы внедрения международно-правовых стандартов в национальное законодательство. Сделан вывод о необходимости брать во внимание при разработке системы защиты информации апробированные большим количеством стран международно-правовые стандарты.

Ключевые слова: международные стандарты, система защиты информации, управление информационной безопасностью, международные стандарты защиты информации.

Постановка проблемы. Конец XX – начало XXI веков ознаменовался широким развитием и массовым внедрением информационных технологий в деятельность органов государственной власти. При этом техническая защита информации и информационной инфраструктуры осуществляется на основании нормативно-правовых документов, большинство из которых были приняты в 90-х годах XX века. Ни один из них не содержит положения о необходимости управления защитой информации, управления информационной безопасностью. Работа над разработкой новых и современных национальных стандартов по управлению информационной безопасностью ведется очень медленно, в отличие от внедрения в украинское законодательство таких стандартов, как «Системы управления качеством», «Системы управления окружающей средой» и «Системы управления безопасностью пищевых продуктов».

Актуальность темы. Глобальная компьютеризация через Internet вызвала необходимость поиска средств и методов гармонизации национальных правовых систем в сфере международных информационных отношений, соотношение этих систем на уровне коллизионного и материального международного права [1]. Выходом из данной ситуации стала стандартизация мер защиты информации, что и обусловливает актуальность данной научной статьи.

Целью работы является определение международно-правовых стандартов в сфере защиты информации.

Для этого автором поставлены следующие **задачи**:

– определить основные виды международно-правовых стандартов в сфере защиты информации;

– охарактеризовать основные виды международно-правовых стандартов в сфере защиты информации;

– определить перспективы внедрения международно-правовых стандартов в национальное законодательство.

Изложение основного материала исследования. Понимание того, что стандарты необходимы для развития сотрудничества и разработки совместных подходов, способствовало осознанию ведущими специалистами в области информационных технологий необходимости разработки системного подхода к построению системы защиты информации и внедрению соответствующих стандартов.

Так, появились такие известные проекты и объединения, как ARIADNE, LTSC, IMS, ADL и др. В настоящее время действуют следующие международные организации по стандартизации качества и сертификации: Международная организация по стандартизации (ISO), Международная электротехническая комиссия (МЭК), Международный союз телекоммуникаций, Европейская организация по качеству, Европейская организация по испытаниям и сертификации, Международный совет по стандартизации, метрологии и сертификации, Международная ассоциация качества, Украинский международный фонд качества и т.п. [2, с. 81]. Однако безусловное лидерство в сфере стандартизации досталось ISO [3, с. 45].

ISO (International Organization for Standartization – Международная организация по стандартизации) – крупнейший в мире разработчик добровольных международных стандартов. Международные стандарты дают современные спецификации для продукции, услуг и, согласно мировой практике, способствуют развитию стандартизации в мировом масштабе для облегчения международного товарообмена и взаимопомощи, а также для расширения

сотрудничества в области интеллектуальной, научной, технической и экономической деятельности.

Для достижения этой общей цели ISO действует в следующих направлениях:

• разработка и публикация международных стандартов во всех областях технической и экономической деятельности, за исключением электротехники и электроники, относящихся к сфере компетенции Международной электротехнической комиссии (МЭК);

• разработка и распространение документов по методам, правилам и процедурам, ориентированным на содействие и облегчение гармонизации стандартов различных национальных систем стандартизации;

• организация обмена информацией о работе своих центральных и технических органов, а также членов ISO;

• сотрудничество с другими международными органами и организациями в смежных сферах деятельности.

Большое внимание при этом уделяется таким проблемам:

1) управление окружающей средой с целью обеспечения его качества;

2) разработка системы международных стандартов по безопасности и деятельности по унификации методов определения требований безопасности в стандартах ISO на продукцию, процессы и услуги;

3) разработка международных стандартов в области систем качества [2, с . 86].

История ISO началась в 1946 году, когда делегаты из 25 стран встретились в Institute of Civil Engineers в Лондоне и решили создать новую международную организацию «для содействия международной координации и унификации промышленных стандартов». ISO официально начала свою деятельность в феврале 1947 года.

С тех пор было опубликовано более 19 500 международных стандартов, охватывающих почти все области технологий и производства. На сегодняшний день членами ISO являются 169 стран и 3368 технических органов, занимающихся разработкой стандартов. Более 150 человек работают на постоянной основе в Центральном секретариате ISO в Женеве, Швейцария [4]. После обретения независимости Украина осуществляет активную политику интеграции в международные и европейские структуры, сотрудничая также со странами СНГ. 1 января 1993 Украина принята в члены Международной организации ISO, а 14 февраля 1993 г. – Международной электротехнической комиссии (IEC), что дает ей право наравне с другими 90 странами мира участвовать в деятельности более 1000 международных рабочих органов, технических комитетов по стандартизации, и использовать в своей работе более 12 тыс. международных стандартов.

К международным стандартам по управлению информационной безопасностью относятся стандарты, такие как ISO/IEC 27001:2005, ISO/IEC 27002:2007, ISO/IEC 15408, ISO/IEC 17799 [5].

Стандарт ISO 15408. В 1990 году Международной Организацией по Стандартизации была начата работа по созданию международных критериев оценки безопасности компьютерных систем. Результатом явился стандарт «Общие критерии безопасности информационных технологий», который на данный момент признается одним из самых функциональных стандартов, ставшие основой для развития стандартизации в сфере информационной безопасности.

ISO 15408 разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей продуктов информационных технологий. Этот стандарт полезен в качестве руководства при разработке функций безопасности, а также в приобретении коммерческих продуктов с подобными свойствами. Основное направление оценки – это угрозы, появляющиеся при преступных действиях пользователя информационных технологий, но стандарт также использовать и при оценке угроз, вызванных другими факторами.

Стандарт ISO 15408 состоит из трех частей: часть 1 – «Введение и общая модель», часть 2 – «Функциональные требования безопасности», часть 3 – «Гарантийные требования безопасности». Стандарт предусматривает наличие двух типов требований безопасности: функциональных и гарантированности. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д. Требования гарантированности относятся к технологии разработки, тестирования, анализа уязвимостей, поставки, сопровождения, эксплуатационной документации.

Основные структуры безопасности согласно стандарту – это «Профиль защиты» и «Проект защиты». По определению стандарта ISO 15408 «Профиль защиты» – независимые от реализации, требования безопасности для некоторой категории объектов оценки, которые отвечают определенным потребностям потребителей. Профиль состоит из компонентов или пакетов функциональных требований и одного из уровней гарантированности.

«Профиль защиты» служит основой для создания «Проекта защиты», который является техническим проектом для разработки объекта оценки. В отличие от «Профиля», «Проект защиты» описывает уровень функциональных возможностей средств и механизмов защиты, реализованных в объекте оценки, и приводит обоснование степени их адекватности. В процессе исследования строятся модели угроз.

В стандарте определяются понятие «потенциал нападения» и его состав. Также стандарт определяет функцию безопасности информации, его критерии с подробной структурой, схему вычисления «потенциала нападения». Внедрение стандарта за границей происходило путём разработки новой архитектуры, которая должна обеспечить информационную безопасность вычислительных систем. Другими словами, создавались технические и программные средства, которые отвечали стандарту. Например, международная организация «Open Group» выпустила новую архитектуру безопасности информации для коммер-

ческих автоматизированных систем с учетом указанных критериев.

Стандарт ISO/IEC 17799. Имеет на сегодняшний день мировое признание и статус международного стандарта ISO. В сентябре 2005 г. основные положения ISO/IEC 17799 были пересмотрены и дополнены с учетом развития современных информационных технологий и требований к организации режима ISO.

Стандарт регламентирует общие принципы, которые предлагается конкретизировать применительно к исследуемым информационным технологиям. Также внимание уделено сертификации информационной системы на соответствие. Стандарт содержит систематический, универсальный перечень регуляторов безопасности, полезен для организации практически любой независимо от размера, структуры и сферы деятельности. Предназначен для использования в качестве справочного документа руководителями и рядовыми сотрудниками, ответственными за планирование, реализацию и поддержание внутренней системы информационной безопасности.

Согласно стандарту, цель информационной безопасности – обеспечить бесперебойную работу организации, по возможности предотвратить и минимизировать ущерб от нарушений безопасности [6, с. 122]. Предлагаемые в первой части стандарта регуляторы безопасности разбиты на десять групп:

– политика безопасности;

– общеорганизационные аспекты защиты;

– классификация активов и управления ими;

– безопасность персонала;

– физической безопасности и безопасности окружающей среды;

– администрирование систем и сетей;

– управление доступом к системам и сетям;

– разработка и сопровождение информационных систем;

– управление бесперебойной работой организации;

– контроль соответствия требованиям.

Во второй части стандарта ISO/IEC 17799 «Системы управления информационной безопасностью – спецификация с руководством по использованию» предметом рассмотрения является система управления информационной безопасностью.

В основу процесса управления положена четырехфазная модель, которая используется в современном ISO 27001, что включает: планирование, реализацию, оценку, корректировку.

Стандарты 2700х серии:

1) *ISO/IEC 27001:2005 – Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.* Предоставляет модель для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения Системы Менеджмента Защиты Информации (СМЗИ). Рекомендуется, чтобы принятие СМЗИ было стратегическим решением для организации. На проектирование и реализацию СМЗИ организации влияют ее потребности и цели, требования защиты, применяемые процессы, а также размер и структура организации. Ожидается, что все эти элементы, а также их вспомогательные системы, будут со временем меняться. Ожидается, что реализация СМЗИ будет масштабироваться в соответствии с потребностями организации, например, простая ситуация требует простого решения СМЗИ. Этот международный стандарт можно использовать для оценки соответствия заинтересованными внутренними и внешними сторонами.

2) ISO/IEC 27002:2005 – Информационные технологии. Методы защиты. Кодекс практики для управления информационной безопасностью. Этот международный стандарт устанавливает руководящие и общие принципы начинания, реализации, поддержания в рабочем состоянии и улучшения управления защитой информации в организации. Цели, указанные этим международным стандартом, дают общие руководящие принципы по целям управления защитой информации, обычно принимаются. Цели и средства управления настоящего стандарта разработаны для реализации, осуществляемой с целью выполнить требования, выявленные оценке рисков. Этот международный стандарт может служить в качестве практического руководства по разработке организационных стандартов защиты и практик эффективного управления защитой, а также для того, чтобы помочь создать доверие в между организационных деятельности.

3) ISO / IEC 27003:2010 – Информационные технологии. Методы защиты. Руководство по применению системы менеджмента защиты информации. В данном международном стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2005. В нем описывается процесс определения и разработки СМИБ, от запуска к составлению планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СМИБ, определяется проект внедрения СМИБ (упоминается в данном международном стандарте, как проект СМИБ), и представлены рекомендации по планированию проекта СМИБ, в результате которого получается конечный план внедрения СМИБ. Данный международный стандарт предназначен для использования организациями, применяющими СМИБ. Он применяется ко всем типам организаций (например, коммерческим предприятиям, правительственным органам, некоммерческим организациям) любых размеров.

4) ISO/IEC 27004:2009 – Информационные технологии. Методы защиты. Измерения. Этот стандарт содержит рекомендации по разработке и использованию измерений и мер измерения для проведения оценки эффективности реализованной системы менеджмента информационной безопасности (СМИБ), а также мер и средств контроля и управления или их групп по ISO/IEC 27001.

Процесс измерений затрагивает политику, менеджмент риска информационной безопасности, меры и средства контроля и управления и цели их применения, процессы и процедуры, а также поддерживает процесс проверки СМИБ, помогая

определить, нужно ли менять или совершенствовать какие-либо из процессов или мероприятий и средств контроля и управления СМИБ. Следует помнить, что никакие измерения мер и средств контроля и управления не могут обеспечить полной безопасности.

Процесс измерений реализуется в виде программы измерений, связанных с информационной безопасностью (далее – программа измерений). Программа измерений предназначена для оказания помощи руководству организации в выявлении и оценке неподходящих требованиям и неэффективных процессов, мероприятий, средств контроля и управления СМИБ, а также в определении приоритетов действий, направленных на усовершенствование или изменение этих процессов и (или) мер и средств контроля и управления.

Программа измерений также может помочь организации в демонстрации соответствия СМИБ требованиям ISO/IEC 27001 и создании дополнительного основания для проведения руководством организации проверки процессов менеджмента риска информационной безопасности.

5) ISO/IEC 27005:2008 – Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. Этот интернациональный стандарт обеспечивает рекомендации для менеджмента рисков информационной безопасности в организации, особенно поддерживая требования СМИБ согласно ISO/IEC 27001. Однако этот интернациональный стандарт не обеспечивает определенной методологии для менеджмента рисков информационной безопасности. Он предназначен для определения в организации подхода к менеджменту рисков в зависимости, например, от области действия СМИБ, области применения менеджмента рисков или сектора промышленности. Чтобы осуществить требования СМИБ, многие существующие методологии могут воспользоваться структурой, описанной в этом интернациональном стандарте. Этот интернациональный стандарт относится к менеджерам и сотрудникам, которые заинтересованы в менеджменте риска информационной безопасности в пределах организации, и где есть соответствующие внешние стороны, поддерживающие такие действия.

6) ISO/IEC 27006:2007 – Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента информационной безопасности. Цель настоящего стандарта – дать возможность органам аккредитации более эффективно применять стандарты, по которым они обязаны оценивать органы сертификации. В этом контексте любое отклонение органа сертификации от руководства является исключением. Такие отклонения будут разрешены только на основе рассмотрения каждого случая отдельно после того, как орган сертификации докажет органам аккредитации, это исключение удовлетворяет эквивалентным образом соответствующему пункту требований ISO/IEC 17021, ISO/IEC 27001 и настоящего стандарта.

Выводы. Учитывая вышесказанное, считаем необходимым брать во внимание при разработке системы защиты информации апробированые большим количеством стран международно-правовые стандарты.

Список использованной литературы:

1. Основи інформаційного права України : [Навч. посіб.] / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін. ; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К. : Знання, 2004. – 274 с.

2. Болотніков А.О. Стандартизація та сертифікація товарів і послуг : [Навч. посіб. для студ. вищ. навч. закл.] – К. : МАУП, 2005. – 144 с.

3. Запорожченко Ю.Г. Міжнародні стандарти в сфері інформаційно-комунікаційних засобів // Актуальні проблеми соціології, психології, педагогіки: Збірник наукових праць. – К. : Логос, 2011. – 251 с.

4. International Organization for Standartization [Електронний ресурс]. – Режим доступу : http://www.iso.org/iso/about.htm/.

5. Богданов О.М., Бакалинський О.О. «Адаптація міжнародного стандарту управління інформаційною безпекою ISO/IEC 27001: 2005 у структурах державного управління України» // Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ») [Електронний ресурс]. – Режим доступу : http://nc.nusta.com.ua/Kyrsi%202009/tezi/images_tezi/S_6_Bogdanov_Bakalynsky_1.htm.

6. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. – М. : Компания АйТи; ДМК Пресс, 2004. – 384 с.