20 години катедра "Търговски бизнес"

Стопанска академия „Д. А. Ценов" - Свищов

Факултет „Производствен и търговски бизнес"
Катедра „Търговски бизнес"

Юбилейна научнопрактическа конференция
с международно участие

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС – КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

Том I

12-13 май 2011 г.

Свищов, 2011 г.

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ" СВИЩОВ
ФАКУЛТЕТ „ПРОИЗВОДСТВЕН И ТЪРГОВСКИ БИЗНЕС"
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

ЮБИЛЕЙНА НАУЧНОПРАКТИЧЕСКА КОНФЕРЕНЦИЯ
С МЕЖДУНАРОДНО УЧАСТИЕ

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

12-13 май 2011 г.

Том I

20 ГОДИНИ
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

Академично издателство „Ценов" Свищов
2011 г.

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Председател: Доц. д-р Марияна Божинова

Членове: Доц. д-р Петранка Мидова
Доц. д-р Светослав Илийчовски
Доц. д-р Симеонка Петрова
Доц. д-р Теодора Филипова
Доц. д-р Петя Иванова

Конференцията се посвещава
на 20-годишния юбилей
на катедра „Търговски бизнес"
и на 75-годишнината от създаването
на Стопанска академия „Д. А. Ценов"
Свищов.

Публикуваните доклади не са редактирани и коригирани. Авторите носят пълна отговорност за съдържанието, оригиналността им и за грешки, допуснати по тяхна вина.

ISBN 978-954-23-0592-7

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И СТАНДАРТИЗАЦИЯ ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Проф. к. э. н. Татьяна Мишова
Молдавская Экономическая Академия
Михаил Нищий
ГП „CADASTRU”

В статье на примере автоматизированной информационной системы управления социальным страхованием рассматриваются вопросы внедрения международного стандарта информационной безопасности ISO 27001. Обсуждаются возможные направления стандартизации процессов обработки данных и направления стандартизации как бизнес процессов, так и информационных процессов на базе библиотеки ITIL с точки зрения повышения информационной безопасности системы.

Целью настоящей статьи является обсуждение практических аспектов разработки и внедрения системы управления информационной безопасностью в организации, предоставляющей социальные услуги населению.

Внедрение политики ИБ предполагает разработку совокупности документированных правил, регламентов, процедур, инструкций или руководящих принципов в области информационной безопасности, которыми должны руководствоваться сотрудники организации в своей повседневной деятельности. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей международной и внутригосударственной нормативно-методической базы в области защиты информации. Особое значение этот факт имеет , когда организация внедряет несколько стандартов, как в нашем случае стандарт управления качеством ИСО 9001:2008 и проводит работы по внедрению требований стандарта управления информационной безопасностью ИСО 27001:2005

В работе [1.2] мы определили место системы управления информационной безопасностью ISO 27001 в общей архитектуре менеджмента организации, в условиях внедрения стандарта ISO 9001 управления качеством, а также использования библиотеки ITIL (рис.1). В таблице 1 приведено сопоставление требований регуляторов управления качеством стандарта ИСО 9001 с соответствующими показателями (регуляторами) с стандарта управления информационной безопасностью – ISO 27001 (см. табл.1). Одним из основных условий эффективного функцио-

нирования системы управления ИБ является вовлеченность руководства организации в процесс разработки и внедрения системы управления ИБ.

При этом важно отметить необходимость понимания всеми сотрудниками организации следующих основных моментов:

1) вся деятельность по обеспечению ИБ инициирована руководством организации и обязательна для выполнения всеми сотрудниками компании, 2) руководство компании лично контролирует разработку и функционирование системы управления ИБ, 3) само руководство выполняет те же правила по обеспечению ИБ и требует того же от сотрудников организации.

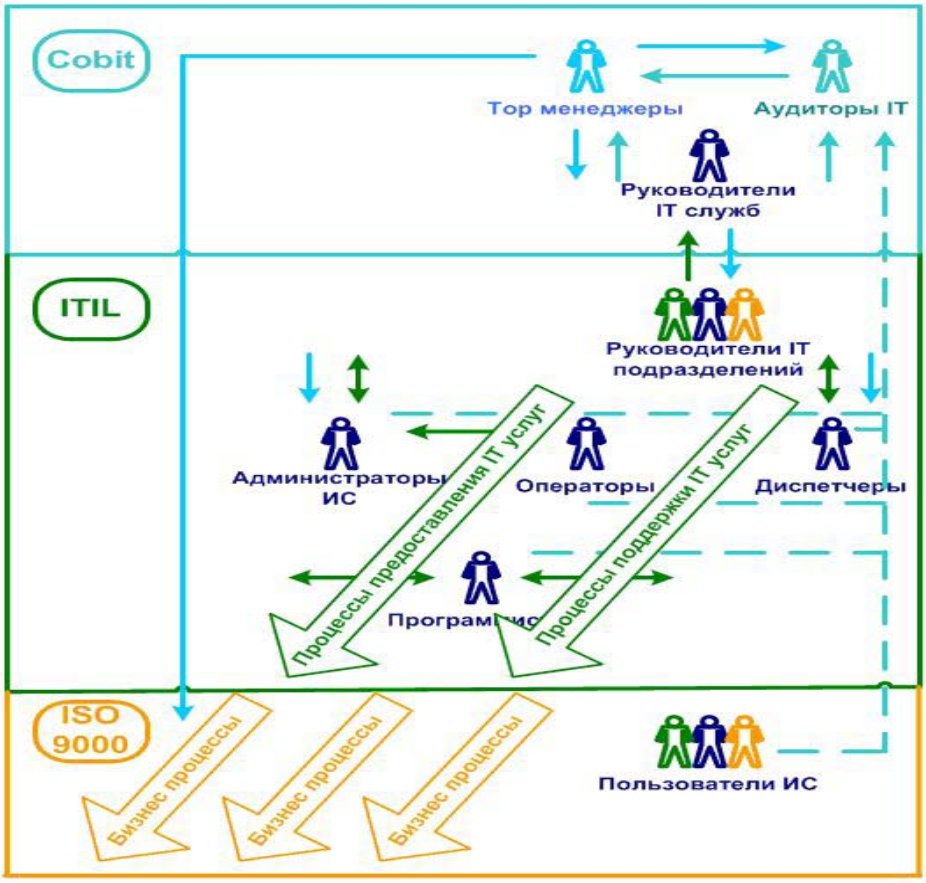

Рисунок 1. Взаимосвязь системы управления ИБ со стандартами управления качеством.

Разработка политики безопасности собственными силами – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области информационной

безопасности. В соответствии с принятой практикой руководством организации было принято решение выбрать внешнюю специализированную компанию для проведения аудита информационной безопасности (ИБ) автоматизированных информационных ресурсов организации и разработки концепции и политики ИБ.

В докладе обсуждаются некоторые практические вопросы выполненного аудита системы управления ИБ организации, полученные результаты и рекомендации, представленные компанией аудитором.

По результатам материалов детального отчета и анализа, проведенного аудита системы управления ИБ и в соответствии с согласованными требованиями в области ИБ, были разработаны основные документы по ИБ, в том числе, Концепция ИБ, Политика ИБ, основные Регламенты и другие организационные и распорядительные документы .

Для внедрения процессов управления ИТ-рисками в организации был разработан Регламент управления рисками, методика инвентаризации, категорирования и оценки рисков информационных ресурсов организации.

Анализ информационных рисков – составная часть процесса управления рисками. При выполнении работ по анализу информационных рисков были оценены уязвимости информационной инфраструктуры организации к угрозам информационной безопасности, их критичность и вероятность ущерба, выработаны контрмеры по уменьшению рисков до приемлемого уровня и предложены методы контроля для защиты информационной инфраструктуры.

Оценивая информационные риски, ИТ-специалисты не ограничились только лишь одними информационными системами, программным, аппаратным и коммуникационным обеспечением, а также были рассмотрены вопросы физической безопасности и учтены и вопросы, связанные с человеческим фактором.

Как показывает практика оценку ИТ-рисков желательно проводить не реже одного раза в год, чтобы можно было гарантировать, что не остались не выявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно. Внутри организации работа по оценке рисков должна быть организована на основании разработанных и утвержденных Регламентов, процедур и инструкций и согласована с риск менеджментом бизнес процессов организации. В целях повышения эффективности и качества работ в данном направлении желательно автоматизировать процессы управления информационными рисками в организации.

Сегодня высшее руководство любой компании по существу имеет дело только с информацией – и на ее основе принимает решения. Понятно, что эту самую информацию готовят множество нижестоящих

слоев достаточно сложной организационной системы, которая называется современным предприятием. И нижние слои этой системы вообще могут не иметь понятия о том, что они производят не только какую-то продукцию или услугу, но и информацию для руководства. Глубинный смысл автоматизации бизнес-процессов заключается как раз в том, чтобы ускорить и упорядочить информационные потоки между функциональными уровнями и слоями этой системы и представить руководству компании лишь самую необходимую, достоверную и структурированную в удобной для принятия решения форме информацию. Критичная для производства и бизнеса информация должна быть ***доступной, целостной и конфиденциальной.*** Отсюда нетрудно сделать вывод, что ключевой бизнес-задачей корпоративной системы ИБ является обеспечение гарантий достоверности информации, или, говоря другими словами, гарантий доверительности информационного сервиса. В соответствии с рекомендациями стандарта по управлению информационной безопасностью ISO 27001:2005, в организации были определены требования к функционированию системы документов информационной безопасности, в том числе, и связи этих документов с документами системы управления качество, которая внедряется в соответствии с требованиями стандарта ИСО 9001:2008.

В процессе внедрения стандартов ИСО 9001 и ИСО 27001 были определены взаимосвязи с документами, которые разрабатываются на предприятии в рамках внедрения стандарта ISO 9001 (рис.1).

Система управления ИБ фактически охватывает три основные области, где действуют следующие стандарты:

а) стандарт ISO 9001 (регламентация и описание бизнес процессов предприятия),

в) описание процессов предоставления ИТ услуг и поддержки ИТ услуг (регламентация и описание осуществляются на основании требований библиотеки ITIL),

с) описание процедур и правил информационной безопасности, основанные на методологии оценки информационных рисков (регламентация и описание на основании требований и рекомендаций международных стандартов типа ISO/IEC 17799:2005 , ISO/IEC 27005, а также стандартов в области управления информационными рисками Cobit).

Одной из важнейших составляющих эффективной системы управления информационной безопасностью является набор работающих политик, регламентов, процедур и инструкций. Указанные документы необходимы, чтобы у всех работников предприятия было одинаковое понимание о том, что, когда, как и кто должен делать для защиты информации.

Ниже приводится таблица возможной классификации документов в области ИБ в соответствии со стандартом ИСО 27001 и связи этих документов со стандартом ИСО 9001.

Таблица 1.

Сравнение содержания стандартов ISO 27001и ISO 9001

Разделы ISO 27001	Разделы ISO 9001, в части ИБ
Введение	*Введение*
1. Границы применимости	*1. Границы применимости*
2. Нормативные ссылки	*2. Нормативные ссылки*
3. Термины и определения	*3. Термины и определения*
3.1. Доступность	
3.2. Конфиденциальность	
3.3. Информационная безопасность	
3.4. Система управления режимом информационной безопасности	
3.5. Целостность	
3.6. Принятие рисков	
3.7. Анализ рисков	
3.8. Оценка рисков	
3.9. Определение рисков	
3.10. Управление рисками	
3.11. Действия по уменьшению рисков	
3.12. Ведомость соответствия	
4. Управление информационной безопасностью	*4. Требования к системе управления качеством (QMS)*
4.1. Общие требования	*4.1. Общие требования*
4.2. Создание и организация системы управления режимом информационной безопасности	
4.2.1. Создание системы управления режимом информационной безопасности	
4.2.2. Средства и действия в рамках системы управления режимом информационной безопасности	
4.2.3. Отслеживание событий в системе управления режимом информационной безопасности	

Разделы ISO 27001	Разделы ISO 9001, в части ИБ
4.2.4. Обслуживание и модернизация системы управления режимом информационной безопасности	
4.3. Документирование требований	*4.2. Документирование требований*
4.3.1. Общие требования	*4.2.1. Общие требования*
4.3.2. Управление документами	*4.2.3. Управление документами*
4.3.3. Управление записями	*4.2.4. Управление записями*
5. Распределение обязанностей персонала	*5. Распределение обязанностей персонала*
5.1. Передача полномочий	*5.1. Передача полномочий*
5.2. Управление ресурсами	*5.2. Управление ресурсами*
6. Управление процедурой пересмотра некоторых положений	*6. Управление процедурой пересмотра некоторых положений*
6.1. Общие положения	*6.1. Общие положения*
6.2. Пересмотр входа	*6.2. Пересмотр входа*
6.3. Пересмотр выхода	*6.3. Пересмотр выхода*
6.4. Внешний аудит	*6.4. Внешний аудит*
7. Модернизация системы управления режимом информационной безопасности	
7.1. Непрерывная модернизация	
7.2. Корректирующие действия	
7.3. Превентивные действия	
Приложение А Цели управления и средства управления	
А1. Введение	
А2. Обзор передового опыта	
А3. Политика безопасности	
А4. Организационные аспекты безопасности	
А5. Классификация ресурсов и управляющих воздействий	
А6. Безопасность персонала	
А7. Безопасность инфраструктуры и физическая безопасность	
А8. Управление коммуникациями и процессами	

Разделы ISO 27001	Разделы ISO 9001, в части ИБ
A9. Управление доступом	
A10. Развитие системы и обслуживание	
A11. Обеспечение бесперебойной работы	
A12. Технические требования	
Приложение B	
Руководство по использованию стандарта	
Приложение C	*Приложение A*
Соответствие между ISO 9001:2000, ISO14001:1996 и BS7799 part 2:2002	*Связь между ISO 14001 и ISO 9001*

Сравнительный анализ показывает, что в обоих стандартах ИСО 9001 и ИСО 27001 прослеживается концептуальное единство регуляторов управления качеством и информационной безопасностью производства и это даёт предпосылки для выстраивания сквозной процедуры аттестации (сертификации) организации одновременно как по показателям качества, так и гарантии обеспечения непрерывности основных бизнес-процессов на основе доверительности информационного сервиса.

Литература

1. Т. Мишова, М. Нищий. Информационный менеджмент и моделирование развития системы социального страхования. Информационно осигурование на бизнеса. Юбилена международна научна конференция. Академично издательство „Цинев”, 7-8 юни, 2006, стр.28-39.

2. М. Нищий. Практические аспекты разработки и внедрения политики информационной безопасности. Securitatea informaţională 2010. Conferinţă ineternaţională (ediţia a VII-a), 15-16 aprilie 2010. pag.108-110.

4. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

5. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.

6. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.