5.4 Перестановка Pr

На вход Pr поступает вектор R длины b бит, каждые 64 бита которого разбиваются на s фрагментов. Если $64 \vdots s$, то длина каждого фрагмента равна 64/s, иначе каждый 64 битный блок разбивается на s-1 фрагментов длины $\lfloor 64/s \rfloor$ бит и один неполный фрагмент длины $64-(s-1)\bullet\lfloor 64/s \rfloor$ бит. Далее к полученной последовательности $r_{1,1}, r_{1,2}, ..., r_{1,s}, r_{2,1}, r_{2,2}, ..., r_{2,s}, ..., r_{s,1}, r_{s,2}, ..., r_{s,s}$ применяется перестановка, как показано на рис. 2, по соотношению: $r'_{i,j} = r_{(i+j-2) \bmod s+1, j}$ для $\forall i, j = \overline{1,s}$. В результате получаем последовательность 64-битных блоков, каждый из которых зависит от каждого 64-битного блока, полученного на вход Pr.

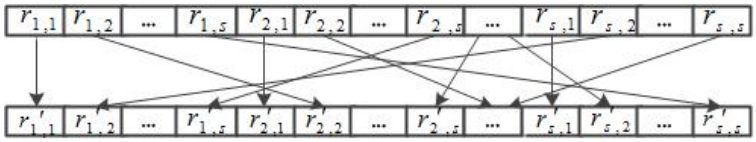


Рис. 2. **Перестановка Pr**

ОБЕСПЕЧЕНИЕ СТАНДАРТИЗАЦИИ БИЗНЕС ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ВНЕДРЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил НИЩИЙ,
Эксперт (Республика Молдова)

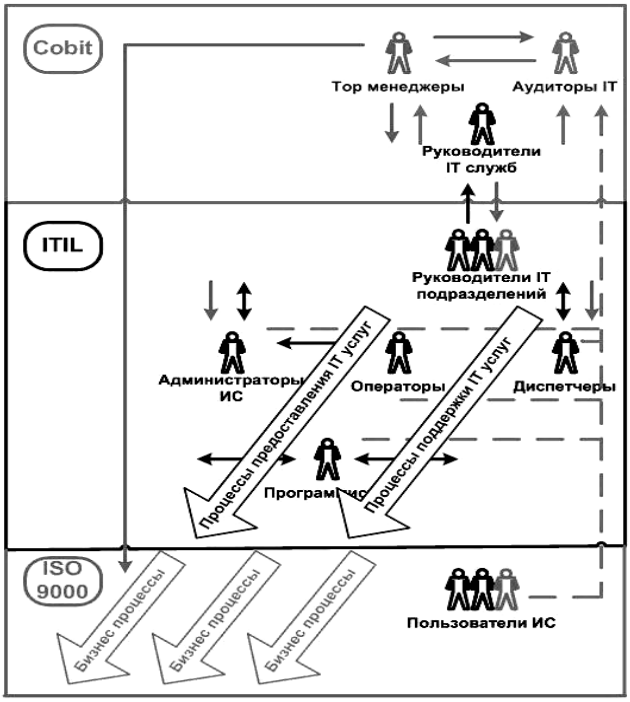
The purpose of this article is to discuss practical aspects of possible directions for standardization of data processing and business processes based on international standards ISO 27001, ISO 9001 and ITIL library in terms of improving information security systems.

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 функционирования 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.

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.

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.

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.

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.

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

Выводы:

1. 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.

2. Внедрение политики ИБ требует регламентации практически всех процессов обработки, хранения, передачи и обмена информации, разработки документированных процедур и инструкций. В этой связи целесообразно использовать имеющиеся стандартные методологии для повышения качества подготавливаемых документов (например, библиотека ITIL, методология Microsoft MOF и т.д.).

3. Как показывает практика, организационные меры играют очень важную роль во внедрении мероприятий политики ИБ в организации, поэтому необходимо организовать непрерывное повышение осведомленности, повышения квалификации и обучения сотрудников организации в области ИБ.

Список литературы:

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 informațională 2010. Conferință ineternațională (ediția 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 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.

EFICIENTIZAREA SERVICIILOR PUBLICE PRIN GUVERNARE ELECTRONICĂ ÎN REPUBLICA MOLDOVA

Vitalie SPÎNACHI,
Academia de Studii Economice din Moldova

Dificultățile şi barierele în obținerea serviciilor publice

Fiind o țară în curs de dezvoltare, R. Moldova este sortită, într-o măsură mai mare, să aibă un decalaj accentuat între nivelul de servire a clienților, în instituțiile publice, față de serviciile oferite de sfera privată. Nivelul necompetitiv de servire a clienților în sfera publică constituie o parte din moștenirea transmisă societății la destrămarea URSS. Conform unui sondaj de opinie (organizat de Magenta Consulting, la inițiativa Institutului de Politici Publice, în iulie 2010), de cele mai dese ori, în obținerea serviciilor publice cetățenii se confruntă cu durata mare de așteptare, indiferență din partea personalului, dezorganizare, corupție, calitate proastă a deservirii, incompetența personalului ș.a.

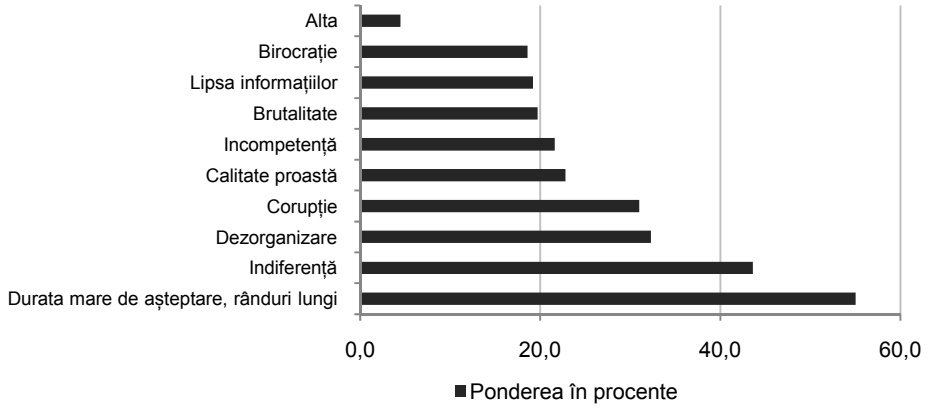


Figura 1. **Dificultățile şi barierele cu care se confruntă cetățenii în obținerea serviciilor publice**

Una din soluțiile referitoare la îmbunătățirea calității serviciilor publice, care se implementează, mai mult sau mai puțin cu succes, constă în guvernarea electronică. Această sarcină este înscrisă în agenda Departamentului Tehnologiilor Informaționale, încă din anul 2005, când a fost adoptată Strategia Națională de edificare a societății