УДК 006.35 (100) ISO; (100) IEC

Польза от внедрения международного стандарта ISO/IEC 27001

Касымбек Айдана Торегелдикызы, магистрант
Казахский Национальный Технический Университет имени К.И. Сатпаева
Институт промышленной инженерии имени А.Буркитбаева

Информация – один из основных ресурсов бизнес процессов, обеспечивающий предприятиям дополнительную стоимость и, соответственно, нуждается в защите. Слабая защита конфиденциальной информации может привести к финансовым потерям, навредить репутации предприятия и принести ущерб коммерческим операциям. Именно поэтому разработка системы управления информационной безопасностью и ее внедрение на предприятии является столь важным [3].

Для защиты информации был разработан специальный стандарт ISO / IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования» для построения на предприятиях системы управления информационной безопасностью в соответствии с разработанными требованиями спецификации. Стандарт ISO/IEC 27001:2005 содержит перечень требований к системе менеджмента информационной безопасности, обязательных для сертификации. Этот стандарт выступает в качестве руководства по внедрению, которое может использоваться при проектировании механизмов контроля, выбираемых организацией для уменьшения рисков информационной безопасности [5].

Стандарт серии ISO/IEC 27001 принадлежит к наиболее известным в мире стандартам ISO. ISO/IEC 27001 — международный стандарт по информационной безопасности, разработанный совместной Международной организацией по стандартизации и Международной электротехнической комиссией. Подготовлен к выпуску подкомитетом SC27 Объединенного технического комитета JTC 1 [2].

Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ) [1].

В стандарте ISO/IEC 27001 (ISO 27001) собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения Системы Менеджмента Информационной Безопасности (СМИБ) [2].

Цель СМИБ - выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон [1].

ISO 27001 подходит малым и крупным предприятиям, занимающихся деятельностью в любых сферах, особенно в тех, где защита информации особенно актуальна, например, в таких отраслях, как здравоохранение, работа с финансами, IT и госучреждения [1].

Стандарт ISO 27001 определяет информационную безопасность как: «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность» [4].

– Конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);

– Целостность – обеспечение точности и полноты информации, а также методов ее обработки;

– Доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Стандарт ISO 27001 гармонизирован со стандартами систем менеджмента качества ISO 9001:2000 и ISO 14001:2004 и базируется на их основных принципах и процессном подходе. Более того, обязательные процедуры стандарта ISO 9001 требуются и стандартом ISO 27001. Структура документации по требованиям ISO 27001 аналогична структуре по требованиям ISO 9001. Большая часть документации, требуемая по ISO 27001, уже могла быть разработана, и могла использоваться в рамках ISO 9001. Таким образом, если организация уже имеет систему менеджмента в соответствии, например, с ISO 9001 или ISO 14001, то предпочтительно обеспечивать выполнение требования стандарта ISO 27001 в рамках уже существующих систем [4].

Преимущества стандарта ISO 27001. Сертификация согласно ISO 27001 имеет много преимуществ:

– Возможность выявления рисков и принятия мер по их оптимизации или устранению;

– Гибкость адаптации инструментов к любым областям вашей деятельности;

– Доверие со стороны заинтересованных лиц и клиентов благодаря защите их данных;

– Соответствие стандартам гарантирует статус привилегированного поставщика;

– Удовлетворение любых ожиданий благодаря соответствию требованиям стандартов [5].

Ядром СМИБ является риск менеджмент. Для банков и организаций в некоторых других отраслях это вполне знакомый термин. Обычно под риск менеджментом понимают управление рисками, включая их определение, оценку и принятие мер для их исключения или снижения до минимума. А собственно говоря, риск – это сочетание вероятности возникновения события (инцидента) и последствия этого. Например, компьютерная система организации может легко быть инфицирована компьютерным вирусом, а последствия этого могут вылиться в остановку бизнес процессов и вытекающие из этого значительные финансовые потери. Поэтому вирусная атака связана с очень высоким риском и обязательно необходима соответствующая защита с помощью организационных, программных и технических средств [1].

ISO/IEC 27001 интегрируют в себе оба метода — PDCA и риск менеджмент. Это позволяет построить максимально результативную систему менеджмента. Методы риск менеджмента непосредственно встроены в цикл PDCA, с целью их применения при разработке, монито-

ринге, поддержании и постоянном улучшении СМИБ. ISO/IEC 27001 предоставляет рабочую структуру для применения лучшей международной практики в области СМИБ, т.е. для понимания того, где те или иные средства по информационной безопасности могут быть применены. Кроме того, руководителям организаций следует признать, что информационная безопасность будет результативной и эффективной при условии вовлечения всех структурных подразделений и всех работников в обеспечение информационной безопасности. Этот подход, основанный на общих организационных рисках, отражен в другом стандарте серии ISO/IEC 27002:2005 «Информационные технологии — Методы обеспечения безопасности — Практические правила управления информационной безопасностью» (прежний шифр ISO/IEC 17799, переименованный в апреле 2007 года). Новейшие принципы безопасности OECD (Организация по экономическому сотрудничеству и развитию) требуют создания «культуры безопасности» внутри организации. Далее, ISO/IEC 27001 предоставляет средства для внедрения результативной СМИБ, соответствующей организационным целям и потребностям бизнеса. Ядро СМИБ должно также соответствовать существующим и потенциальным угрозам безопасности, техническим и технологическим требованиям, возможностям информационных систем и бизнес процессов, законодательным, нормативным и контрактным требованиям [4].

Стандарт ISO/IEC 27001 достаточно гибок, чтобы его можно было использовать для интеграции СМИБ в существующие системы менеджмента, а также для СМК.

Цикл PDCA в ISO 27001 интеграции в любые существующие методики риск менеджмента. Например, уже немало примеров применения СМИБ и стандарта ISO/IEC 27001 (или его предшественника — BS 7799) в рамках предоставления государственных услуг, в частности, при реализации программ электронного правительства (e-government). Как известно, в Казахстане также осуществляются программы электронного правительства, так что, несомненно, применение ISO/IEC 27001 будет интересно и в этом направлении [1].

Как и при применении ISO 9001, применяя ISO/IEC 27001, организация может разработать, внедрить и сертифицировать свою систему менеджмента на соответствие международного стандарта. Согласно официальным данным ISO во всем мире по ISO/IEC 27001 сертифицировались 7 732 организации из 70 стран. Здесь быстрее Казахстана оказались ближайшие соседи — Кыргызстан, Молдавия, Украина и Россия. Абсолютный лидер — Япония, где сертификацию по ISO/IEC 27001 прошли 4 896 организаций, т.е. 63% от общего объема сертификации [6].

К работе по разработке серии стандартов информационной безопасности подключился МСЭ (ITU) — Международный союз электросвязи.

По всей видимости, стандарты серии ISO/IEC 27001 станут не только мощными инструментами, но и будут обладать широкой международной поддержкой авторитетных технических организаций и крупных компаний. Например, Казахстанская организация качества имеет около 500 успешно внедренных проектов в области систем менеджмента на территории РК [6].

Исходя из этого, как мы знаем, принято считать XXI век — информационным веком. Это, прежде всего, связано с революционными изменениями в методах деятельности — в переходе от медленных процессов обработки информации к компьютерам и Интернету. В наше время колоссальный объем информации можно уместить на небольших портативных устройствах, а многоядерные микропроцессоры способны обработать такой ранее немыслимый информационный поток, как видео в формате высокого разрешения. Но, в то же время, вместе с новыми информационными технологиями появились новые проблемы и новые виды преступности, т.е. новые угрозы информационной безопасности. Это компьютерные вирусы, «трояны», хакеры, промышленный шпионаж, кража информации, террор, шантаж и т.п. Источниками этих угроз могут быть информационные сети и системы, сотрудники, поставщики, потребители, финансовые организации и государственные учреждения. Слабая защита также является постоянным источником угроз по безопасности. Сегодня как никогда конкурентоспособность бизнеса любой отрасли зависит от безопасности информационных активов. При этом для эффективного обеспечения информационной безопасности требуются системные решения, основанные на подходах современного риск - менеджмента и интегрируемые в общую систему управления организацией. Управление рисками информационной безопасности - это задача, которую руководители и собственники любой организации, вне зависимости от вида ее деятельности, объемов и местоположения, вынуждены решать ежедневно. Таким образом, для защиты информации был разработан специальный стандарт ISO / IEC 27001:2005 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Этот стандарт выступает в качестве руководства по внедрению, которое может использоваться при проектировании механизмов контроля, выбираемых организацией для уменьшения рисков информационной безопасности.

Ценность сертификации для бизнеса также заключается в упорядоченном подходе, который предполагает разработку процессов управления безопасностью, методологий, инструментов и шаблонов, которые можно многократно использовать во всей компании и для всех операций — планирования безопасности, внедрения, функционирования, мониторинга, отслеживания, подготовки отчетности. Средства отслеживания и отчетности, основанные на отраслевых стандартах, таких как стандарты ISO, упрощает проведение аудита, что ведет к снижению затрат на аудиты и повышению вероятности успешного прохождения аудита.

В целом стандарт система управления информационной безопасностью на основе стандарта ISO 27001 позволяет:

– Сделать большинство информационных активов наиболее понятными для менеджмента компании;
– Выявлять основные угрозы безопасности для существующих бизнес-процессов;
– Рассчитывать риски и принимать решения на основе бизнес-целей компании;
– Обеспечить эффективное управление системой в критичных ситуациях;
– Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности);
– Четко определить личную ответственность;
– Достигнуть снижения и оптимизации стоимости поддержки системы безопасности;
– Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках;

– Подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту.

Таким образом, если организация уже имеет систему менеджмента в соответствии, например, с ISO 9001 или ISO 14001, то предпочтительно обеспечивать выполнение требования стандарта ISO 27001 в рамках уже существующих систем. Внедрение и сертификация по ISO 27001 на базе внедренной системы менеджмента качества по ISO 9001 предполагает значительное снижение внутренних затрат предприятия и стоимости работ по внедрению и сертификации. По стандарту ISO/IEC 27001:2005 проводится официальная сертификация системы управления информационной безопасностью. Сертификация на соответствие стандарту позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании защита информации поставлена на высокий уровень и налажено эффективное управление информационной безопасностью.

Литература:

1. Авторские статьи А. Дмитриева по стандарту ISO 27001.
2. Александр Астахов. История стандартов информационной безопасности. CISA, 2006.
3. Блинов А. М. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебное пособие. Изд-во СПбГУЭФ., 2010.
4. Журнал "Information Security/ Информационная безопасность", 2013.
5. http://www.intercert.kz/index.php?option=com_content&view=article&id=36:iso-27001&catid=8&Itemid=116&lang=ru
6. http://www.zerde.gov.kz/ru/page/informacilnnaya-bezopasnost-na-osnove-mezhdunarodnogo-standarta-iso-27001