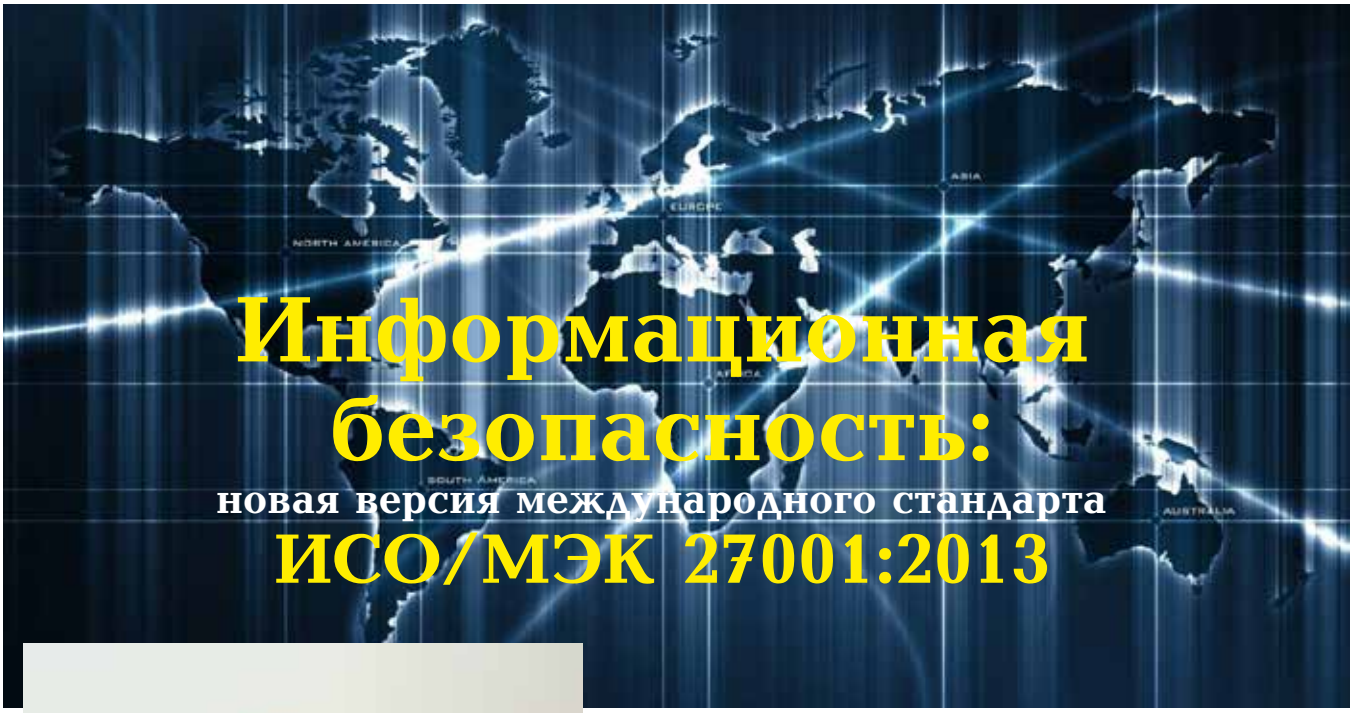


Информационная безопасность:

новая версия международного стандарта ИСО/МЭК 27001:2013

ЕРБОЛ ЕСМУХАНОВ,
кандидат технических наук,
аудитор IRCA

Наш XXI век с самого начала окрестили информационным веком. Значимость информации в нашей работе и повседневной жизни постоянно нарастает. Практически все признают тот факт, что информационные активы – стали наиболее ценными активами организации. Что, 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 ультравысокого разрешения. А мобильная связь, став повсеместной и общедоступной даже для малообеспеченных слоев общества, сегодня превращается в мощный мобильный центр обработки информации. Само понятие телефон изменилось, теперь это чаще смартфон, который все более успешно заменяет такие устройства, как видеокамеры, фотокамеры, диктофоны, справочники, игровые консоли, электронные книги, ноутбуки и собственно телефоны.

Как никогда раньше возможности по обработке информации возросли многократно, но и проблемы, прежде всего информационной безопасности, также выросли. 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, воровство ноу-хау, 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. В результате возможна потеря ценного конкурентного преимущества, утечка информации личного характера, кража клиентской базы данных и прямые финансовые потери. Кроме того, компания теряет свой имидж из-за неспособности защитить конфиденциальную информацию, предоставленную ему клиентом. В наихудшем случае возможна и утечка государственных секретов.

Очевидно, что задача по обеспечению информационной безопасности является одной из приоритетных для современной организации. От успешного решения этой задачи зависит устойчивость и конкурентоспособность организации, а также ее репутация. Необходимо заметить, что обеспечение информационной безопасности не может быть частичной, т.е. оставляющей «дырки» в своей защите. Наличие даже небольшой бреши в защите означает только одно — ее отсутствие. Чтобы реально обеспечить информационную безопасность без брешей в защите, нужен СИСТЕМНЫЙ ПОДХОД. Не только и не столько технологии, а именно комплексный подход, разработка и внедрение результативной системы менеджмента информационной безопасности — СМИБ (ISMS — information security management system) резко снижает риски по инцидентам в области информационной безопасности.

К сожалению, наше мышление больше соответствует мышлению страуса, который зарывает свою голову в песок при виде надвигающейся угрозы. Кажется, что отдаленная или невидимая угроза менее значима, чем очевидная и текущая. Погоня за сегодняшними прибылями приводит бизнес на грань опасной черты. Приведем один лишь всем известный пример: информационная атака на kaspi bank, которая произошла в начале текущего года, могла привести к финансовому коллапсу всей банковской системы страны и экономики в целом. Этот инцидент обнажил всю уязвимость наших организаций перед угрозами извне, причем самых дешевых и простых, как sms рассылка с провокационной информацией. Она показала полную неготовность к таким событиям. Проблема не в наличии или в отсутствии преступников, так как они всегда были и будут, а в отсутствии надлежащей системы информационной безопасности. И это всего лишь верхушка айсберга, которая видна всем, а то, что скрыто под водой и невидимо – колоссально. Реальные потери чрезвычайно высоки. Пора, наконец, строить надежные и эффективные системы менеджмента информационной безопасности.

Системы менеджмента информационной безопасности проще и удобнее начать с внедрения соответствующих международных и национальных стандартов, например, ИСО/МЭК 27001. Этот стандарт в Казахстане внедрили ряд организаций. Что объясняется не столько популярностью стандартов ИСО, сколько насущной потребностью организаций в защите их нематериальных активов. Также важно для организаций участие в тендерах и конкурсах, где обязательным условием является наличие сертифицированной системы менеджмента информационной безопасности.

Недавно было опубликовано второе издание ИСО/МЭК 27001:2013 «Информационные технологии. Системы информационной безопасности. Требования», заменяющее первое издание ИСО/МЭК 27001:2005. Главное отличие нового издания этого стандарта заключается в унифицированной структуре для всех стандартов на системы менеджменты, официально утвержденной в приложении SL от 2012 года. Это дает новые возможности по интеграции с другими стандартами менеджмента, например, со стандартом ИСО 9001 «Системы менеджмента качества. Требования», ИСО 14001 «Системы экологического менеджмента. Требования и руководство по применению» и другими.

Для создания, внедрения и постоянного улучшения СМИБ широко применяется известный цикл PDCA (см. Рисунок 1), где:

Plan — разработайте СМИБ, которую затем установите, например, посредством утверждения и рассылки процедур и планов.

Do — внедрите СМИБ и обеспечьте ее функционирование, например, посредством распределения полномочий и четкой постановки целей и задач.

Check — регулярно проводите мониторинг и анализ СМИБ, например, через плановые и внеплановые аудиты, через анализы со стороны руководства.

Act — при необходимости адаптируйте и улучшайте СМИБ, например, через корректирующие действия.

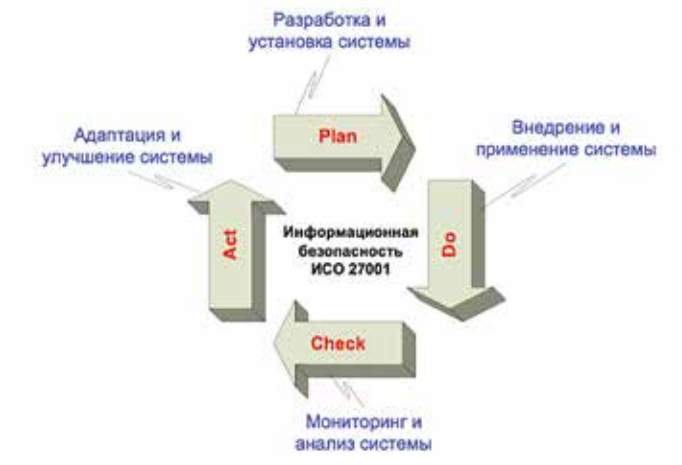


Рисунок 1. Цикл PDCA в ИСО 27001

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.

Часто риски информационной безопасности подсчитываются в денежном эквиваленте. Это позволяет оценить эффективность инвестиций в информационную безопасность организации. Как правило, инвестиции в информационную безопасность окупаются стабильностью или устойчивостью организации, большим доверием клиентов.

ИСО/МЭК 27001 является документом, в котором сконцентрирована лучшая международная практика, достигнутая в области информационной безопасности. Как это принято в ИСО (международная организация по стандартизации) и МЭК (международный электротехнический комитет), в разработку новых международных стандартов привлекается широкий круг заинтересованных организаций и экспертов посредством технических комитетов. Данный стандарт был разработан в ОТК 1 (объединенный технический комитет) «Информационные технологии».

ИСО/МЭК 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, мониторинге, поддержании и постоянном улучшении СМИБ. ИСО/МЭК 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.

Далее, ИСО/МЭК 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 и нормативным требованиям и контрактным требованиям.

Применение стандарта ИСО/МЭК 27001 позволяет получить следующий ряд преимуществ:

— демонстрация посредством сертификации на соответствии ИСО/МЭК 27001 того, что системы и процессы организации в достаточной степени обеспечивают безопасное обращение и пересылку информации;

— обеспечение информационной безопасности для клиентов, что жизненно важно для ведения организацией успешного бизнеса, а в частности, для получения преимуществ в тендерах и конкурсах;

— передача на аутсорсинг процессов без ущерба для информационной безопасности, как организации, так и ее клиентов;

— снижение рисков организации, связанных с вопросами информационной безопасности, что в целом способствует устойчивому развитию.

Организации, прошедшие сертификацию по ИСО/МЭК 27001, прежде всего, видят пользу от этой сертификации в расширении портфеля сертификатов, что непосредственно влияет на имидж организации, как преуспевающей и современной.

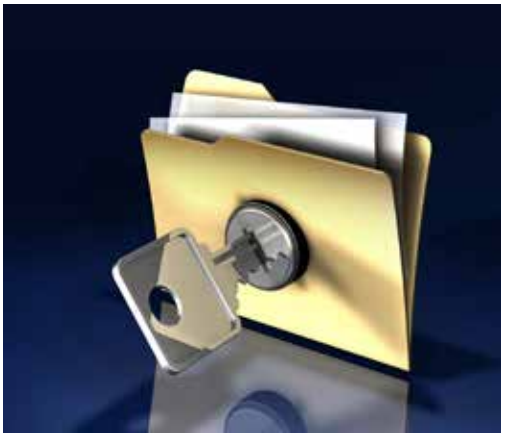
ИСО/МЭК 27001 применим для любых видов деятельностей, для любых типов и размеров организаций. Наибольшей популярностью стандарт ИСО/МЭК 27001 пользуется в следующих отраслях:

— телекоммуникация;
— банковская деятельность и финансы;
— страхование;
— информационные технологии;
— здравоохранение;
— государственные услуги;
— коммунальные услуги;
— розничная торговля;
— образование;
— службы по чрезвычайным ситуациям;
— силовые структуры;
— производство;
— транспортные компании и
— поставщики услуг.

Стандарт ИСО/МЭК 27001 достаточно гибок, чтобы его можно было бы использовать для интеграции СМИБ в существующие системы менеджмента, а также для интеграции в любые существующие методики риск менеджмента.

Как и при применении ИСО 9001, применяя ИСО/МЭК 27001, организация может разработать, внедрить и сертифицировать свою систему менеджмента на соответствие международного стандарта. Общая динамика роста сертификатов по ИСО/МЭК 27001 свидетельствует о том, что данный стандарт является настоящим бестселлером. Несомненно, кроме жизненной необходимости в защите информации, этому способствует все большее преобладание в деятельности нематериальных активов над материальными активами, т.е. информационной над физической составляющей продукции. Последний финансовый кризис еще раз подтвердил значимость информации в наше время и тяжесть последствий от ошибок в области информационной безопасности.

Приступить к внедрению систем информационной безопасности можно, например, воспользовавшись услугами консультантов, обладающих соответствующей подготовкой и знаниями, подтвержденными международными сертификатами. Например, Казахстанская организация качества имеет около 700 успешно внедренных проектов в области систем менеджмента на территории Республики Казахстан.



Если у Вас возникнут вопросы касательно процедур внедрения и сертификации по ИСО 27001 или любых других стандартов на системы менеджмента, то Вы получить ответ на все ваши вопросы по телефонам 8(727)2-60-87-68, 2-60-87-69 или по электронной почте kok@kok.kz.

При выборе органа сертификации, прежде всего, необходимо обратить на наличие у него аккредитации. Например, Ассоциация по сертификации Русский Регистр имеет международную аккредитацию в ANAB.
Телефоны: +7(727)311-12-39, +7(727)311-12-86.