

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

НА ОСНОВЕ МЕЖДУНАРОДНОГО СТАНДАРТА ИСО 27001



Ербол Есмуханов,
кандидат технических
наук, аудитор IRCA,
PrCert, CQI, RR, ГСТР РК,
зарегистрированный
в IRCA международный
тренер

В Казахстане уже несколько организаций внедрили или внедряют систему менеджмента информационной безопасности на основе международного стандарта ИСО 27001. Это объясняется не столько популярностью стандартов ИСО, сколько насущной потребностью организаций в защите их нематериальных активов. 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. А мобильная связь стала повсеместна и общедоступна даже для малообеспеченных слоев общества.



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, 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 неспособ-

ности 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 брешы в защите означает только одно — ее отсутствие. Чтобы реально обеспечить информационную безопасность без брешей в защите, нужен СИСТЕМНЫЙ ПОДХОД.

Прошлогодний скандал, связанный с банком Golden Man Sachs и программистом Сергеем Алейниковым, обвиняемым в краже исходных текстов закрытой банковской программной торговой системы, показателен в том плане, что даже дорогие защитные технологии и высокие заработные платы не являются гарантией от информационных преступлений. Они могут быть совершены сотрудниками той же организации на обычном рабочем месте и обычное время. Поэтому 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, даже в банках второго уровня Казахстана состояние информационной безопасности вызывает тревогу. Бывают случаи, когда информация о вкладчиках одного банка попадает в иной, конкурирующий с ним банк. О том, что такие инциденты имеют место, знают клиенты банка, но никак не руководство этих банков. Соответствующий имидж «болтливости» банка естественно не может вызвать высокое доверие у клиентов. Руководителям многих организаций, не только банков, следует взвесить ценность собственных информационных активов и информации по своим клиентам, а также последствия от их попадания «не в те руки».

К счастью появился стандарт ИСО/МЭК 27001:2005 «Информационные технологии. Системы информационной безопасности. Требования», на основе которого можно создать современную СМИБ. Этот стандарт основан на другом известном стандарте ИСО 9001 «Системы менеджмента качества. Требования», а также по структуре подходит к ИСО 14001 «Системы экологического менеджмента. Требования и руководство по применению». ИСО/МЭК 27001 был разработан на основе пересмотра и адаптации весьма успешного британского стандарта BS 7799, часть 2.

ИСО/МЭК 27001, как и стандарт ИСО 9001, применяет широко известный цикл PDCA (см. Рисунок 1) для постоянного улучшения и адаптации системы менеджмента:

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. ►



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

- демонстрация посредством сертификации на соответствие 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, 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 деятельности, 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.

Act — при необходимости адаптируйте и улучшайте СМИБ, например, через корректирующие и предупреждающие 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. Этот подход, основанный на общих организационных рисках, отражен в другом стандарте серии ИСО/МЭК 27002:2005 «Информационные технологии — Методы обеспечения безопасности — Практические правила управления информационной безопасностью» (прежний шифр ИСО/МЭК 17799, переименованный в апреле 2007 года). Новейшие принципы безопасности OECD (Организация по экономическому сотрудничеству и развитию) требуют создания «культуры безопасности» внутри организации.

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, нормативным и контрактным требованиям.

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

интеграции в любые существующие методики риск менеджмента. Например, уже немало примеров применения СМИБ и стандарта ИСО/МЭК 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 ИСО/МЭК 27001 будет интересно и в этом направлении.

Как и при применении ИСО 9001, применяя ИСО/МЭК 27001, организация может разработать, внедрить и сертифицировать свою систему менеджмента на соответствие международного стандарта. На конец 2007 года согласно официальным данным ИСО (www.ISO.org) во всем мире по ИСО/МЭК 27001 сертифицировались 7 732 организации из 70 стран, но ни одной организации из Казахстана. Здесь быстрее нас оказались ближайшие соседи — Кыргызстан, Молдавия, Украина и Россия. Абсолютный лидер — Япония, где сертификацию по ИСО/МЭК 27001 прошли 4 896 организаций, т.е. 63 % от общего объема сертификации! В этой стране бизнес всегда уделял первостепенное внимание информации и знаниям, считая их основой успеха в международной конкуренции.

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, т.е. информационной над физической составляющей продукции. Текущий финансовый кризис еще раз подтвердил значимость информации в наше время и тяжесть последствий от ошибок в области информационной безопасности. ►



Кроме упомянутых выше стандартов ИСО/МЭК 27001 и ИСО/МЭК 27002 в серию стандартов по информационной безопасности уже вошли следующие стандарты:

ИСО/МЭК 27000:2009 «Информационные технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности — Общие сведения и словарь». Данный стандарт содержит общие сведения и терминологию по информационной безопасности, также как стандарт ИСО 9000 предоставляет общие положения и словарь для системы менеджмента качества.

ИСО/МЭК 27003:2010 «Информационные технологии — Методы обеспечения безопасности — Руководящие указания по внедрению системы менеджмента информационной безопасности». Данный стандарт содержит руководящие указания для внедрения СМИБ на основе стандартов серии ИСО/МЭК 27000.

ИСО/МЭК 27004:2009 «Информационные технологии — Методы обеспечения безопасности — Менеджмент информационной безопасности — Измерения» содержит рекомендации по показателям и измерениям в области информационной безопасности.

ИСО/МЭК 27005:2008 «Информационные технологии — Методы обеспечения безопасности — Управление рисками информационной безопасности». Как было отмечено выше, риск менеджмент является ядром стандартов серии ИСО 27000, и поэтому был опубликован дополнительный стандарт касательно управления рисками безопасности.

ИСО/МЭК 27006:2007 «Информационные технологии — Обеспечение безопасности — Требования к органам, осуществляющим аудит и сертификацию систем информационной безопасности». Данный стандарт необходим аккредитованным органам для предоставления услуг по аудиту и сертификации систем информационной безопасности. Следует также опираться на стандарт ИСО/МЭК 17021:2006 «Оценка соответствия - Общие требования для органов, выполняющих аудит и сертификацию систем менеджмента» и ИСО 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

К работе по разработке серии стандартов информационной безопасности подключился МСЭ (ITU) — Международный союз электросвязи. По всей видимости, стандарты серии ИСО/МЭК 27000 станут не только мощными инструментами, но и будут обладать широкой международной поддержкой авторитетных технических организаций и крупных компаний.

Приступить к внедрению систем информационной безопасности можно, например, воспользовавшись услугами наших консультантов, обладающих соответствующей подготовкой и знаниями, подтвержденными международными сертификатами. Например, Казахстанская организация качества имеет около 500 успешно внедренных проектов в области систем менеджмента на территории РК.

Казахстанская организация качества с 1 сентября 2005 г. является членом EFQM (Европейский фонд управления качеством). Казахстанская организация качества одна из первых казахстанских консалтинговых компаний в 2005 году успешно прошла процедуру международной сертификации системы менеджмента качества на соответствие требованиям международных стандартов ИСО 9001, 14001 и OHSAS 18001 и получила сертификат соответствия единого международного образца IQNet. Кроме того, Казахстанская организация качества разработала десятки СТ РК — стандартов Республики Казахстан, включая стандарты по качеству и безопасности на производстве. Казахстанская организация качества является также членом технического комитета ТК 54 «Системы менеджмента качества».

Казахстанская организация качества организует большое количество бизнес семинаров по системам менеджмента, как для специалистов, так и для высшего руководства. Эти семинары посетили более 25 000 слушателей из всех регионов Казахстана. Темы и программы семинаров постоянно совершенствуются, например, проводятся семинары для организаций, которые уже внедрили и сертифицировали системы менеджмента.

Если у Вас возникнут вопросы касательно процедур внедрения и сертификации по ИСО 27001 или любых других стандартов на системы менеджмента, то мы будем рады ответить на все ваши вопросы по телефонам: +7 (727)2-60-87-68, 2-60-87-69 или по электронной почте kok@kok.kz.



Следующие стандарты информационной безопасности будут полезны применительно к КИС (корпоративным информационным системам):

ИСО/МЭК 27033-1:2009 «Информационные технологии — Методы обеспечения безопасности — Сетевая безопасность — Часть 1: Обзор и концепции».

ИСО 13335-1:2004 «Информационные технологии. Руководство по управлению ИТ безопасностью. Концепции и модели для управления безопасностью информационных и теле-коммуникационных технологий».

ИСО 13335-3:1998 «Информационные технологии. Руководство по управлению ИТ безопасностью. Методы управления ИТ безопасностью».

ИСО 13335-4:2000 «Информационные технологии. Руководство по управлению ИТ безопасностью. Выбор механизмов защиты».

ИСО 13335-5:2001 «Информационные технологии. Руководство по управлению ИТ безопасностью. Руководство по управлению сетевой безопасностью».

ИСО/МЭК 18044:2004 «Информационная технология. Методы и средства обеспечения безопасности. Управление инцидентами информационной безопасности».

ИСО/МЭК 18045:2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ИСО/МЭК 15408-1:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

ИСО/МЭК 15408-2:2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

ИСО/МЭК 15408-3:2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».