МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27010

Первое издание
2012-04-01

Информационные технологии. Методы обеспечения защиты. Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями

Information technology – Security techniques – Information security management for inter-sectoral and inter-organizational communications

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO/IEC 27010:2012(R)

ДОКУМЕНТ ЗАЩИЩЁН АВТОРСКИМ ПРАВОМ

Бюро ISO по авторским правам:
Case postale 56 • CH-1211 Geneva 20
Тел.: + 41 22 749 01 11
Факс: + 41 22 749 09 47
Эл. почта: copyright@iso.org
Веб-сайт: www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) образуют специализированную организацию по международной стандартизации. Национальные органы стандартизации, являющиеся членами ISO или IEC, участвуют в разработке Международных стандартов через технические комитеты, учреждённые соответствующей организацией для компетентного рассмотрения проблем в конкретных предметных областях. Технические комитеты ISO и IEC сотрудничают в сфере общих интересов. Международные правительственные и неправительственные организации, имеющие связь с ISO и IEC, также принимают участие в этой работе. Применительно к сфере информационных технологий ISO и IEC учредили объединённый технический комитет ISO/IEC JTC 1.

Проекты международных стандартов разрабатываются согласно правилам, приведённым в Директивах ISO/IEC, Часть 2.

Разработка международных стандартов является основной задачей технических комитетов. Проекты международных стандартов, принятые техническими комитетами, рассылаются комитетам-членам на голосование. Для публикации в качестве международного стандарта требуется одобрение не менее 75 % комитетов-членов, принявших участие в голосовании.

Принимается во внимание тот факт, что некоторые из элементов настоящего документа могут быть объектом патентных прав. ISO не принимает на себя обязательств по определению отдельных или всех таких патентных прав.

ISO/IEC 27010 был подготовлен Объединённым техническим комитетом ISO/IEC JTC 1, *Информационные технологии,* Подкомитетом SC 27, *IT Методы обеспечения безопасности.*

Введение

Настоящий международный стандарт дополняет стандарты ISO/IEC 27001:2005 и ISO/IEC 27002:2005, предназначенные для сообществ пользователей, работающих с одной и той же информацией. Содержащиеся в данном стандарте руководящие указания служат дополнением общего руководства, представленного в семействе стандартов ISO/IEC 27000.

Хотя предметом рассмотрения в ISO/IEC 27001:2005 и ISO/IEC 27002:2005 является обмен информацией между организациями, этот обмен описывается в общих чертах. Однако при возникновении необходимости передачи конфиденциальной информации множеству других организаций передающая сторона должна иметь твёрдую уверенность в том, что организации-адресаты обладают адекватными средствами защиты получаемой информации. Подобные средства могут быть реализованы путём образования сообщества пользователей общей информации, в рамках которого каждый его участник доверяет другим участникам защиту совместно используемой информации, даже несмотря на то, что при отсутствии такого сообщества эти организации могли бы быть конкурентами друг друга.

Сообщество пользователей общей информации не может успешно работать при отсутствии доверительных отношений. Пользователи, предоставляющие информацию, должны иметь гарантии того, что её получатели не будут разглашать полученные сведения или воздействовать на полученные данные ненадлежащим образом. В свою очередь, получатели информации должны иметь гарантии её полной достоверности по всем характеристикам, которые отмечены источником. Оба этих аспекта одинаково важны и должны подтверждаться явно видимой эффективной политикой защиты информации и использованием лучших достижений сложившейся практики. Для получения таких результатов члены сообщества пользователей должны иметь на вооружении общую автоматизированную систему, решающую проблемы защиты совместно используемой информации. Правильным техническим решением является внедрение системы обеспечения информационной безопасности (СОИБ).

Совместное использование информации может также осуществляться в рабочей среде информационного обмена между сообществами, среди которых могут быть получатели, не знакомые источнику информации. В такой ситуации эффективная работа возможна только в случае установления адекватных доверительных отношений между всеми сообществами путём заключения соглашений о совместном использовании информации. Это особенно важно при обмене конфиденциальной информацией между сообществами разного профиля: например, между различными отраслями промышленности или разными секторами рынка.

В настоящем международном стандарте представлены руководящие указания и общие принципы обеспечения соответствия организаций установленным требованиям при использовании существующих способов передачи сообщений и других технических методов. Стандарт предназначен для поддержки идеи создания доверительных отношений между сотрудничающими сообществами при информационном обмене конфиденциальной информацией и её совместном использовании, что способствует росту числа таких сообществ в международном масштабе.

Информационные технологии. Методы обеспечения защиты. Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями

1 Область применения

Настоящий международный стандарт содержит руководящие указания, которые дополняют представленное в семействе стандартов ISO/IEC 27000 руководство по реализации системы обеспечения информационной безопасности в рамках сообществ пользователей общей информации.

Дополнительно в стандарте предоставляются средства управления и специальное руководство по вводу в действие, инструментальному оснащению, поддержке и усилению информационной безопасности операций передачи данных между организациями и между различными секторами профессиональной деятельности.

Данный международный стандарт применим ко всем формам информационного обмена и совместного использования конфиденциальной информации, как общедоступной, так и личной; как национальной, так и международной; как в рамках одной и той же отрасли или сектора рынка, так и между отраслями или секторами. В частности, он может применяться к информационным обменам и совместному использованию информации, относящейся к формированию, поддержке и защите необходимой инфраструктуры на организационном или национальном уровне.

2 Нормативные ссылки

Перечисленные ниже ссылочные документы обязательны для применения данного документа. В случае датированных ссылок действующим является только указанное издание. Применительно к недатированным ссылочным документам применяются их самые последние издания (включая все последующие изменения):

ISO/IEC 27000:2009, *Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь*

ISO/IEC 27001:2005, *Информационные технологии. Методы обеспечения защиты. Системы управления информационной безопасностью. Требования*

ISO/IEC 27002:2005, *Информационные технологии. Методы обеспечения защиты. Управление рисками информационной безопасности*

3 Термины и определения

В рамках настоящего документа используются термины и определения ISO/IEC 27000, а также термины и определения, приведённые ниже.

3.1
сообщество пользователей общей информации
information sharing community
группа организаций, совместно использующих информацию по общему согласию

ПРИМЕЧАНИЕ: Организация может быть представлена одним лицом.

3.2
доверенная сторона передачи информации
trusted information communication entity
автономная организация, поддерживающая процесс информационного обмена в рамках сообщества пользователей общей информации

4 Концепции и обоснование

4.1 Общие замечания

Ниже, в разделах с 5-го по 15-й, представлено руководство по системе обеспечения информационной безопасности (СОИБ), относящееся к области информационного обмена как между организациями, так и между различными секторами профессиональной деятельности.

ISO/IEC 27002:2005 определяет средства управления, которые обеспечивают как взаимный информационный обмен между организациями, так и распространение общедоступной открытой информации. Однако в некоторых обстоятельствах возникает потребность в совместном использовании тем или иным сообществом сотрудничающих организаций общей информации конфиденциального характера, которая не может быть доступной ни для кого кроме членов конкретного сообщества. Такая информация часто может делаться доступной только конкретным лицам внутри каждой организации, входящей в сообщество, или связываться требованием её анонимности. Настоящий международный стандарт определяет также возможные дополнительные средства и методы защиты и содержит дополнительные рекомендации по обеспечению их соответствия требованиям ISO/IEC 27001:2005 и ISO/IEC 27002:2005.

4.2 Сообщества пользователей общей информации

Для эффективной работы сообщества пользователей общей информации должны иметь некоторые общие интересы или какие-то определённые отношения, позволяющие определить целесообразные масштабы обмена информацией конфиденциального характера; например, сообщества могут работать с каким-то сектором рынка и состоять только из организаций, связанных с этим конкретным сектором. Конечно, могут существовать и другие сферы общих интересов: например, общее географическое расположение или общая совместная собственность.

4.3 Координация работы сообществ

Сообщества пользователей общей информации должны формироваться из независимых организаций или их подразделений. Поэтому в построенных таким образом сообществах может не быть чётко очерченных или унифицированных организационных структур и управленческих функций, распространяющихся на всех членов сообщества. Что же касается обеспечения эффективной защиты информации, то здесь необходимо формирование координирующего сообщества, а это значит, что должны быть чётко определены организационные структуры и функции управления, касающиеся обеспечения информационной безопасности сообщества.

Должны учитываться также существующие различия между сообществами пользователей общей информации. Эти различия могут состоять в следующем:

— организации-члены сообщества могут уже использовать собственную СОИБ либо не иметь её, и

— организации-члены могут использовать свод правил защиты информационных активов и сохранения конфиденциальности информации или не иметь таких правил.

4.4 Узлы поддержки

Множественные сообщества пользователей общей информации должны создать или определить подразделение централизованной реализации и поддержки соответствующих операций. Такое

подразделение способно обеспечить реализацию многих функций поддержки (например, анонимизации источников и получателей сообщений) намного легче и эффективней, чем это возможно при непосредственном взаимодействии всех участников сообщества.

Существует целый ряд различных организационных моделей, которые могут использоваться для создания узлов поддержки. Две такие обобщённые модели приведены в Приложении D настоящего стандарта; это доверенный узел информационного обмена [Trusted Information Communication Entity (TICE)] и Пункт оповещения, консультативного обслуживания и представления информации [Warning, Advice and Reporting Point (WARP)].

4.5 Межсекторный обмен информацией

Многие сообщества пользователей общей информации, должны принадлежать к тому или иному сектору профессиональной деятельности, поскольку такая принадлежность естественным образом указывает на наличие общего интереса. Однако вполне может существовать и совместно используемая сообществами информация, которая может представлять интерес для других сообществ пользователей общей информации в рамках других секторов. В таких случаях возможно формирование сообществ пользователей общей информации, членами которого являются сообщества пользователей общей информации, объединённые на основе какого-то общего интереса, определяемого, например, конкретным характером совместно используемой информации. Далее такая ситуация рассматривается как информационный обмен между секторами профессиональной деятельности.

Подобный межсекторный обмен информацией существенно упрощается в тех случаях, когда внутри каждого сообщества пользователей общей информации существуют узлы поддержки; в таких ситуациях необходимые соглашения об информационном обмене и требуемых средствах управления могут заключаться между узлами поддержки, а не между всеми членами всех сообществ. Некоторые сообщества в рамках сектора будут требовать при этом анонимизации организации-источника или организаций-получателей сообщений, что может осуществляться также с помощью узлов поддержки.

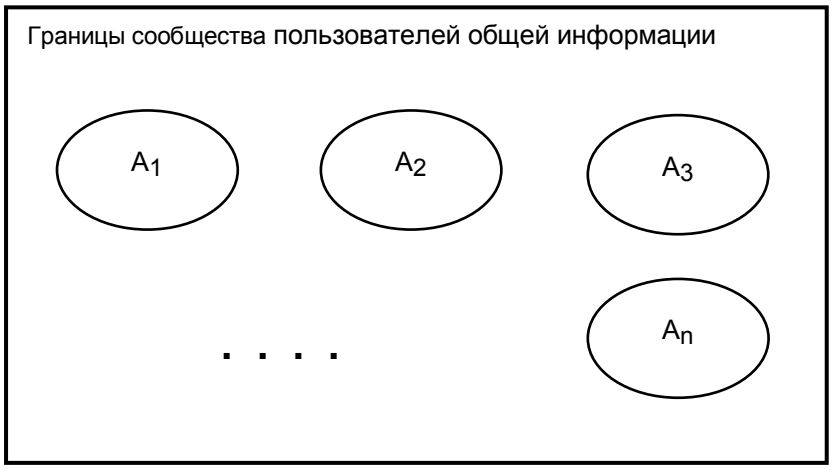
4.6 Обеспечение соответствия требованиям

Любая система обеспечения информационной безопасности (СОИБ), созданная и эксплуатируемая в соответствии с положениями ISO/IEC 27001:2005 и содержащая средства управления, определённые в ISO/IEC 27002:2005, в настоящем международном стандарте и в других первоисточниках, может быть оценена на предмет её соответствия требованиям международного стандарта ISO/IEC 27001:2005 без внесения в него каких-либо изменений или дополнений.

Однако имеется целый ряд сфер применения, в которых положения стандарта ISO/IEC 27001:2005 подлежат отдельному толкованию в отношении сообщества пользователей общей информации (или межсекторного информационного обмена, т.е. в рамках объединения сообществ).

Первое, что требует адекватной интерпретации, это чёткое определение рассматриваемой организации.

Согласно требованиям ISO/IEC 27001:2005, СОИБ создаётся организацией и работает в среде её общей хозяйственной деятельности, подверженной существующим рискам (ISO/IEC 27001:2005, раздел 4.1). В этом контексте релевантной организацией является сообщество, объединённое совместным использованием информации. Однако члены сообщества пользователей общей информации сами должны представлять собой организации (см. Рисунок 1).



Условные обозначения

A_k - это *k*-я организация-член сообщества (где k = 1 ... n), включающая в себя и любой узел поддержки.

Рисунок 1 — Сообщество организаций

Во многих сообществах пользователей общей информации не всем лицам организаций-членов будет разрешён доступ к информации конфиденциального характера. В этом случае одна часть организации-члена сообщества будет находиться в границах действия СОИБ сообщества, а другая – за этими границами. Часть, находящаяся вне границ сообщества, будет иметь доступ только к информации сообщества, помеченной как сведения для более широкого круга пользователей (см. Рисунок 2).

Рисунок 2 — Интерпретация частичного членства в сообществе

Вполне возможно, что организации-члены сообщества пользователей общей информации имеют свои собственные системы обеспечения информационной безопасности; тогда, как следствие, некоторые процессы могут подпадать под действие обеих систем защиты информации одновременно – системы сообщества в целом и системы членов сообщества. В этом случае существует (по крайней мере, теоретически) возможность конфликта между несовместимыми требованиями к таким процессам, и может оказаться оправданным их исключение из области действия СОИБ организации-члена сообщества (см. ISO/IEC 27001:2005, 4.2.1 a).

При определении подходящего метода оценки рисков (ISO/IEC 27001:2005, 4.2.1 c) сообществу пользователей общей информации надо чётко осознавать тот факт, что влияние рисков будет сказываться по-разному на разных членах сообщества. Поэтому сообществу необходимо выбрать такую методологию оценки рисков, которая способна обеспечить учёт неравномерного характера их влияния на сообщество, равно как и на выбор критериев оценивания рисков.

Измерение эффективности выбранных средств управления (ISO/IEC 27001:2005, 4.2.3 c) требует участия в этом процессе всех членов сообщества пользователей общей информации. Необходимо, чтобы все они регулярно предоставляли по каналам обратной связи с источниками и сообществом в целом соответствующие данные, касающиеся эффективности функционирования средств управления в собственной рабочей среде членов сообщества.

4.7 Модель передачи данных

Обмен конфиденциальной информацией, рассматриваемый в настоящем международном стандарте, может происходить в любой форме – письменной, устной или электронной – при условии выполнения установленных требований к этому процессу.

В последующих разделах данного международного стандарта процесс обмена конфиденциальной информацией описывается в предположении наличия следующих его участников:

— *источника* элемента информации, т.е. физического лица или организации, которые являются его создателями; источник не обязательно должен быть членом сообщества;

— *инициатора*, т.е. члена сообщества пользователей общей информации, который первым начинает распространять элемент информации внутри сообщества. Инициатор (отправитель) может распространять информацию непосредственно или переслать её в узел поддержки для последующего распространения. Инициатор не обязательно может быть одновременно и создателем информации; он может также маскировать личность источника. Сообщества могут предоставлять средства, позволяющие члену сообщества скрывать свою личность как инициатора.

— *получателя*, т.е. лица, принимающего информацию, которая распространяется внутри сообщества. Получатели не обязательно должны быть членами сообщества, если получаемая информация идентифицируется как доступная для широкого распространения. Сообщества могут предоставлять средства, позволяющие получателям скрывать свою личность от инициаторов передачи информации.

5 Стратегия защиты

5.1 Политика в области защиты информации

5.1.1 Программный документ в области защиты информации

Описание средства управления в 5.1.1 ISO/IEC 27002:2005 расширяется следующим образом:

Руководство по реализации

Документ, касающийся политики в области защиты информации, должен определять, как и в каком направлении членам сообщества пользователей общей информации надлежит совместно работать над реализацией стратегии обеспечения информационной безопасности. Этот документ должен быть сделан доступным для всех сотрудников, использующих общую информацию в рамках сообщества. Выработанная стратегия может предусматривать наложение ограничений на передачу информации другим членам сообщества.

Документ по информационной безопасности должен определять правила классификации информации и содержать описание политики её распространения в рамках сообщества.