Стандарты ИБ: ищем ошибки в новом ГОСТе

Храмцовская Н.А.[1]

Осенью 2006 года наконец был опубликована новая версия ГОСТа, посвященного практическим правилам управления ИБ. Этого давно ждали, но чего же дождались? Во-первых, специалисты получили лишь перевод устаревшей версии 2000 года, а во-вторых, качество этого перевода оставляет желать много лучшего.

ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология - Практические правила управления информационной безопасностью", подготовленный Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России"), был опубликован осенью 2006 года.

Специалисты в области информационной безопасности и ряда смежных отраслей уже давно ждали принятия этого ключевого стандарта в качестве национального. Несколько огорчает то, что был получен перевод версии 2000 года, а не существенно более современной и детальной версии 2005 года. Обе версии, как известно, были переведены и прошли публичное обсуждение. Возможно, комитет-разработчик стандарта предпочел не спешить и как следует доработать по итогам обсуждения перевод стандарта ИСО 17799:2005 и "парного" к нему сертификационного стандарта ИСО 27001:2005, - а пока опубликовать лучше "отлаженный" перевод версии 2000 года.

Обеспечение непрерывности работы компании в случае непредвиденных обстоятельств вынесено в отдельный раздел нового стандарта

Основные принципы СУИБ

ГОСТ Р ИСО/МЭК 17799-2005 представляет собой перечень мер, необходимых для обеспечения информационной безопасности организации, включая действия по созданию и внедрению системы управления информационной безопасности (СУИБ), которая строится таким же образом и на тех же принципах, что и система менеджмента качества, и совместима с ней. Это - не единственный документ такого рода, однако именно в стандарте ИСО 17799 (и в его предшественнике – британском стандарте BS 7799-1) впервые предпринята попытка охватить весь комплекс проблем, связанных с информационной безопасностью. Наиболее важными являются следующие особенности этого документа.

---

[1] Храмцовская Наталья Александровна - ведущий эксперт по управлению документацией компании «Электронные Офисные Системы», член Гильдии Управляющих Документацией и ARMA International.

Информационная безопасность не сводится только к компьютерной. Стандарт говорит не только о защите компьютерных систем, сетей и носителей информации, но и о других активах организации: об информации и документах на "традиционных" носителях (бумага, микропленка), а также об информации, хранящейся в головах сотрудников организации. При этом обеспечить защиту необходимо на всех стадиях обработки информации, таких как копирование, хранение, передача и уничтожение.

Обеспечение информационной безопасности не сводится к защите от действий криминального характера. Самое серьезное внимание уделено обеспечению наличия и доступности информации и документов, необходимых организации для деловой деятельности и для защиты своих прав и интересов, а также защите целостности и аутентичности этих документов в ходе нормальной деловой деятельности.

В отдельные разделы выделены **вопросы обеспечения соответствия организации законодательно-нормативным требованиям**, а также обеспечение непрерывности деловой деятельности в случае непредвиденных обстоятельств и ее восстановления после катастроф.

Учитывая важность этого стандарта, а также его использование в процессе сертификации СУИБ, хочется надеяться на то, что его разработчики впредь постараются не повторять печальный опыт перевода стандартов ИСО серии 9000 по системе менеджмента качества. Допущенные тогда многочисленные грубые ошибки до сих пор дают о себе знать, а в последнее время привели к "обострению отношений" между специалистами по качеству и по документационному обеспечению управления.

Особенности перевода

Знакомство с текстом стандарта оставляет двоякое впечатление. С одной стороны, переводчики сумели правильно отразить все основные идеи, и данный ГОСТ, безо всякого сомнения, будет очень полезен для широкого круга заинтересованных лиц.

С другой стороны, данному документу присущи все те недостатки, которые, к сожалению, стали типичными для "переводных" национальных стандартов. Качество русского текста оставляет желать лучшего. Создается впечатление, что при подготовке стандарта сэкономили на редакционной литературной правке, и в результате то и дело попадаются выражения типа "обеспечение уверенности в том-то" вместо "обеспечения того-то" (а ведь информационная безопасность – это не психотерапия!).

Проведенная сверка текста стандарта с англоязычным оригиналом выявила многочисленные (хотя и относительно мелкие) погрешности перевода и допущенные переводчиками вольности – например, сплошь и рядом условные конструкции преобразуются в безусловные; к месту и не к месту вставляется уточнение "… информационной безопасности", в отдельных случаях искажающее смысл оригинального текста.

Например, в п.7.1.2 (второй подпункт перечисления) фраза "An audit trail of all access should be securely maintained" (т.е. требование протоколировать все случаи доступа в защищенном журнале) переведена следующим образом: "Необходимо также надежным образом проводить аудит журналов регистрации доступа".

В подпункте c) (в переводе – в)) п.7.2.1 в оригинале написано "Items requiring special protection should be isolated to reduce the general level of protection required" т.е. "отдельные элементы оборудования, требующие специальной защиты, должны быть изолированы, с

тем, чтобы можно было понизить требуемый общий уровень защиты". В стандарте читаем прямо противоположное: "отдельные элементы оборудования, требующие социальной защиты, необходимо изолировать, чтобы повысить общий уровень необходимой защиты".

Подпункт e) (в переводе – д)) того же пункта: "An organization should consider its policy towards eating, drinking and smoking on in proximity to information processing facilities" т.е. "организации следует определить свою политику по отношению к приему пищи и напитков и к курению вблизи средств обработки информации" переведен так: "в организации необходимо определить порядок приема пищи, напитков и курения вблизи средств обработки информации". И если оригинал прозрачно намекает на необходимость запрета, то в ГОСТе речь идет о том, как правильно организовать питание и места для курения!

Там же, в подпункте h) (в переводе – з)): "The impact of a disaster happening in nearby premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street should be considered." т.е. "Следует принять во внимание возможный ущерб вследствие бедствия, которое может произойти в близлежащих помещениях, - например, вследствие пожара в соседнем здании, вследствие протечки воды через крышу или в подвальных помещениях, или вследствие взрыва на улице". В ГОСТе читаем: "необходимо разработать меры по ликвидации (!) последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице".

При переводе последнего абзаца п.8.6.2 переводчики "потеряли" часть предложения, и вместо "собранное вместе большое количество несекретной информации может стать более конфиденциальным, чем небольшое количество секретной информации" получилось "большой объем открытой информации может сделать ее более важной".

В п.8.7.3 переводчики решили "доработать" стандарт, и дописали следующую фразу: "Для обеспечения безопасности электронной торговли необходимо проанализировать степень достоверности и обоснованности предлагаемых поставщиками мер обеспечения информационной безопасности" (интересно, что в этом пункте о поставщиках вообще речи не идет!).

В п.8.7.5 читаем: "Необходимо учитывать последствия для информационной безопасности и бизнес-процессов от взаимодействия вышеуказанных средств, в частности:… - идентификацию статуса пользователей, например служащих организации или подрядчиков, в отдельных директориях, для удобства других пользователей". Правильнее было бы перевести, например, так: "Рассматривая деловые последствия и последствия в области безопасности вследствие взаимодействия этих систем, следует подумать о следующем: … - об указании в справочниках статуса пользователей (например, "сотрудник организации", "представитель подрядчика") для удобства других пользователей".

В п.8.7.7 c) (в переводе – в)): фраза "not leaving messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling" т.е. "не оставлять сообщений на автоответчиках, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами, могут быть сохранены в общедоступных системах либо неправильно сохранены вследствие неверного набора номера", переведена так: "не оставлять сообщения на автоответчиках, переадресация на которые произошла вследствие ошибки соединения, или автоответчиках операторов связи, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами".

Согласно новой версии стандарта, "в организации необходимо определить порядок приема пищи, напитков и курения вблизи средств обработки информации"

Из п.9.2.3 можно узнать, что, согласно ГОСТу, "пароли являются наиболее распространенными средствами подтверждения идентификатора пользователя" - а вовсе не его личности, как это записано в оригинале.

В п.9.4.2 встречаем более серьезную терминологическую ошибку, когда вместо "принудительно устанавливаемого маршрута" (enforced path) вдруг начинает использоваться термин "оптимальный маршрут".

В п.9.5 a) фраза "identifying and verifying the identity, and if necessary the terminal or location of each authorized user" т.е. "идентификация и проверка личности, а при необходимости – терминала и местоположения каждого авторизованного пользователя" переведена так: "идентификацию и верификацию компьютера пользователя и, если необходимо, терминала и местоположение каждого авторизованного пользователя".

Серьезная ошибка допущена в п. 10.2.1 "Подтверждение корректности ввода данных", подпункт a). Перевод "Для этого целесообразно применение … a) проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок" полностью искажает смысл данного пункта, который как раз рекомендует двойной ввод как меру обеспечения правильности исходных данных.

Особенно много мелких и не очень мелких неточностей в переводе главы 12, где часто встречаются термины, относящиеся к юриспруденции и делопроизводству. Следуя печальной традиции, заложенной еще при переводе стандартов ИСО серий 9000 и 14000, термин records как только ни переводился, однако ни разу не было использовано его правильное значение - "документы", и это существенно повлияло на смысл получившегося текста.

Можно было бы еще долго перечислять аналогичные примеры. Ошибки подобного рода вполне терпимы там, где данный ГОСТ будет применяться для общего ознакомления с мерами, обеспечивающими информационную безопасность. Однако его вряд ли можно рекомендовать для использования в тех случаях, когда каждое слово может иметь значение – т.е. в случае сертификации СМИБ по стандартам ISO 27001 или BS 7799-2. Обидно,

что всех этих "накладок" вполне можно было бы избежать, если бы "публичное" обсуждение данной версии стандарта в 2005 году было действительно публичным, - ведь именно в области информационной безопасности мы располагаем большим количеством высококвалифицированных специалистов, многие из которых к тому же прекрасно владеют английским языком.

Полезный инструмент

Несмотря на многочисленные погрешности различного характера, широкая трактовка информационной безопасности делает стандарт полезным инструментом не только для специалистов в области информационных технологий и информационной безопасности, но и для представителей кадровой, юридической служб и службы документационного обеспечения управления (ДОУ). Так, например, специалисты ДОУ могут использовать ГОСТ Р ИСО/МЭК 17799-2005 совместно со стандартом ISO 15489:2001 по управлению документами. ГОСТ Р ИСО/МЭК 17799-2005 подробно раскрывает многие вопросы, лишь схематично обрисованные в ISO 15489.

Также стандарт можно и нужно использовать в практической работе служб делопроизводства даже с перечисленными выше недочетами. Большое значение имеет то, что, хотя документ подготовлен для специалистов совершенно другого направления, он постоянно затрагивает вопросы организации работы с документами на всех видах носителей – причем в качестве одного из основных элементов деятельности по обеспечению информационной безопасности организации.

Стандарт дает возможность поднять престиж работы с документами в глазах высшего руководства организации и влиятельных служб ИТ и информационной безопасности. Многие специалисты ДОУ порой затрудняются четко и обоснованно ответить на часто задаваемый вопрос: "А зачем нужно хорошо налаженное и организованное делопроизводство?". ГОСТ Р ИСО/МЭК 17799 говорит: деятельность службы ДОУ, прежде всего, направлена на обеспечение информационной безопасности организации.

В частности, специалисты по управлению документацией могут использовать в своей работе нижеперечисленные положения.

Так, в п.8.6.2. рассматривается вопрос об "утилизации носителей информации". В нем перечислены основные носители информации, которые использует в своей работе организации, и первыми в списке идут бумажные документы. Организация работы по уничтожению документов на всех видах носителей по истечении установленных сроков хранения является одной их основных обязанностей службы делопроизводства.

В п.8.4, посвященном вопросам безопасности, связанным с использованием электронной почты, предусматривается решение вопроса о хранения сообщений электронной почты. Сообщения должны сохраняться таким образом, чтобы их можно было использовать в случае судебных разбирательств. Это возможно только тогда, когда обеспечивается целостность и аутентичность электронных сообщений. Как показывает опыт, выполнить эту работу в организации без участия службы ДОУ весьма затруднительно.

Особое внимание рекомендуется обратить на раздел 12, который скромно назван "Соответствие требованиям". В первую очередь, речь идет о необходимости обеспечить соответствие деятельности организации законодательно–нормативным требованиям. Практика работы показывает, что специалисты ДОУ, наравне с юристами, отвечают за это направ-

ление деятельности, особенно тогда, когда необходимо выполнять требования, непосредственно связанные с документированием деятельности организации.

Пункт 12.1.3 (содержание которого было бы яснее и понятнее, если бы вместо "записей" был использован термин "документ") полностью посвящен вопросам защиты документов организации и их хранению. Специалистам ДОУ стоит обратить внимание на то, что в стандарте рекомендуется с этой целью разработать "руководство в отношении сроков хранения, порядка хранения и утилизации данных и меры для защиты важной информации от потери, разрушения и фальсификации" (иными словами, инструкцию по делопроизводству); а также "опись источников ключевой информации и график хранения наиболее важных данных" (т.е. номенклатуру дел).

Добиваясь поддержки высшим руководством разработки инструкции по делопроизводству и номенклатуры дел, можно ссылаться на эти требования, содержатся в уважаемом во всем мире стандарте, регламентирующем такой ответственный вид деятельности, как обеспечение информационной безопасности.

В целом, нужно отметить, что хотя версия ISO 17799 2000 года, на основе которой разработан ГОСТ Р ИСО/МЭК 17799-2005 в целом несколько устарела, некоторые вопросы обеспечения информационной безопасности освещены в ней лучше – например, более подробно говорится об обеспечении безопасности при использовании электронной почты, что весьма актуально для России.

Подводя итог, хотелось бы поставить оценку "хорошо" переводчикам, которые подготовили вполне добротный "продукт", - и "двойку" организации-разработчику и техническому комитету ТК 362, которые не смогли организовать проверку точности перевода и литературное редактирование документа, чтобы его качество действительно соответствовало высокому званию "национального стандарта Российской Федерации".

Опубликовано: CNews, 10 января 2007 года,
http://www.cnews.ru/reviews/index.shtml?2007/01/10/230553_2