ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58545— 2019

МЕНЕДЖМЕНТ ЗНАНИЙ

Руководящие указания по сбору, классификации, маркировке и обработке информации

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «НИИ экономики связи и информатики «Интерэкомс» (ООО «НИИ «Интерэкомс») совместно с Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 100 «Стратегический и инновационный менеджмент»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 сентября 2019 г. № 733-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В настоящее время практически во всех сферах бизнеса уже существуют организации, внедрившие у себя качественно новые принципы и процедуры работы с информацией, а именно процессы идентификации, сбора, классификации (назначения категории секретности) и обработки информации, а также процессы ее получения и передачи посредством информационно-телекоммуникационных технологий по регламентированным правилам организации. При этом стало возможным ориентировать сотрудников и партнеров организации на принятие предварительно согласованных мер по использованию, защите и обмену информацией с учетом ее ценности.

Тем не менее эквивалентность процессов классификации, маркировки и обработки информации, согласованная между организациями частного сектора (B2B), организациями государственного сектора (G2G), а также между организациями частного и государственного секторов (B2G) отсутствует, несмотря на существующие попытки создать унифицированные форматы и правила передачи информации между организациями B2B, G2G и B2G. Последнее приводит к возникновению противоречий в способах распределения информации как между организациями в целом, так и ее структурными подразделениями.

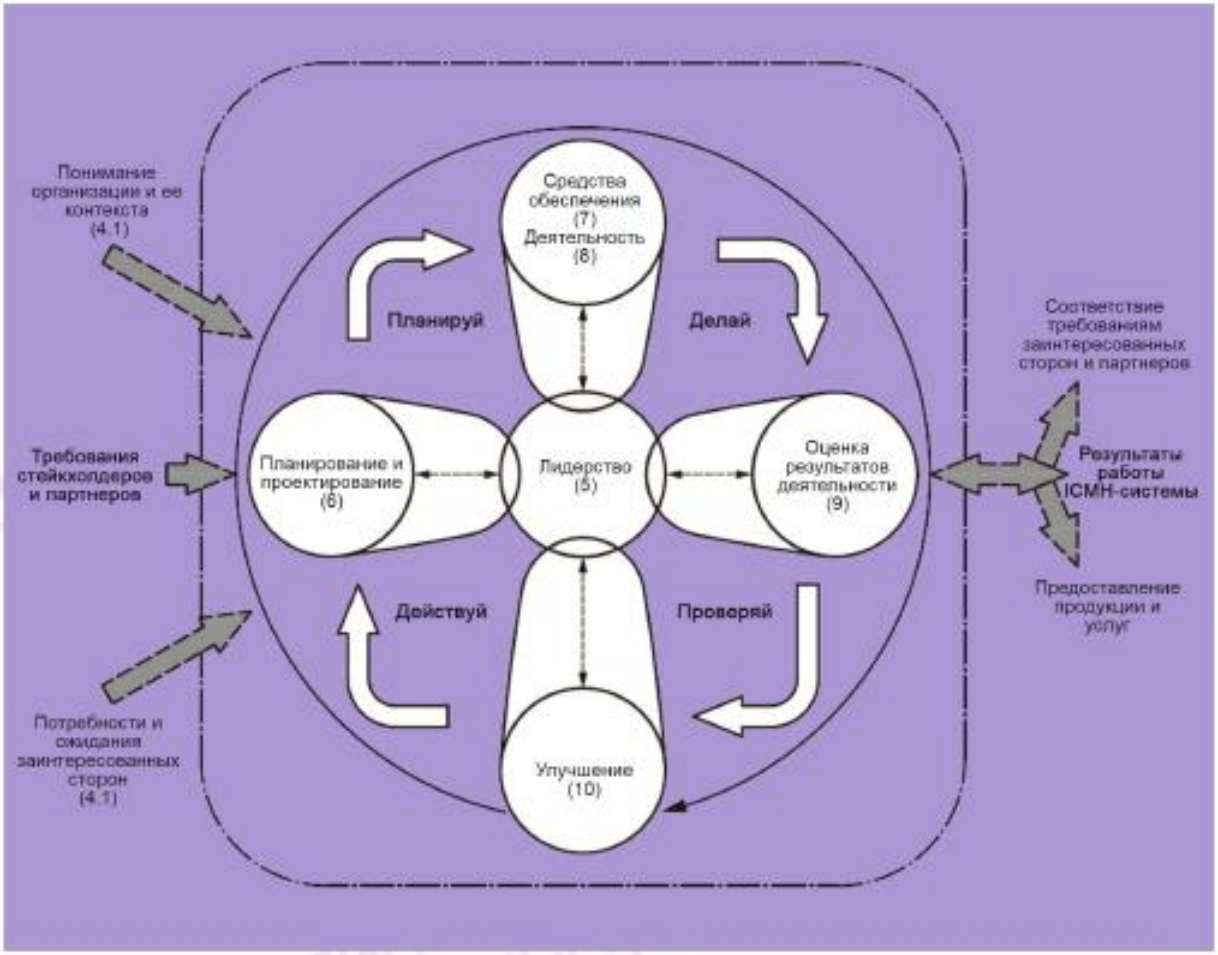
Настоящий стандарт предназначен для стимулирования организаций любого типа и размера к использованию контролируемого и более логичного подхода к обработке информационных активов, основанного на принципах классификации и маркировки, что позволит повысить пользователям настоящего стандарта качество контроля конфиденциальной информации как в рамках собственной организации, так и при совместном использовании и обмене информацией между организациями. Настоящий стандарт также может способствовать защите инвестиций, доходов, репутации и развития любой организации, например ИТ-компаний, занимающихся созданием новой информации или программного обеспечения, внедривших и использующих в своих решениях принципы настоящего стандарта, а также создающих автоматизированные средства обработки документации (включая системы мониторинга), способные обнаруживать и работать с ней при передаче классифицированных и маркированных информационных активов.

Настоящий стандарт предназначен для поддержки организаций в части:

- решения ими своих стратегических задач, выполнения обязательств по управлению рисками на предприятии;
- соблюдения ими юридических, нормативно-правовых и технических обязательств, например по защите данных (см. ГОСТ Р ИСО/МЭК 27001);
- надлежащей защиты и обмена конфиденциальной информацией и
- повышения степени восприятия пользователями ценности и значимости информационных активов и ознакомления с методами их обработки.

Классификация, маркировка и обработка информации (ICMH) требуют системного подхода, который соответствует циклу PDCA («планируй — делай — проверяй — действуй»), приведенному в ГОСТ Р ИСО 9001. На рисунке 1 показано, как пункты 4—10 настоящего стандарта связаны с PDCA-циклом.

Терминология, используемая в настоящем стандарте, соответствует терминологии, установленной в ГОСТ Р 53894, а общий подход, в рамках которого рассматривается внедрение системы менеджмента знаний на малых и средних предприятиях, соответствует ГОСТ Р 57127, ГОСТ Р 57133 и ГОСТ Р 54877.



Примечание 1 — Рисунок заимствован из ГОСТ Р ИСО 9001 (рисунок 2).

Примечание 2 — Цифры в скобках на рисунке относятся к разделам настоящего стандарта.

Рисунок 1 — Связь между ICMH-подходом и PDCA-циклом

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ЗНАНИЙ

Руководящие указания по сбору, классификации, маркировке и обработке информации

Knowledge management.
Guide for information collection, classification, marking and handling

Дата введения — 2020—01—01

1 Область применения

В настоящем стандарте определены требования к созданию, внедрению, оценке и доработке систем, применяемых для сбора, классификации, маркировки и обработки информации (ICMH-систем), а также установлены требования к процессу классификации информации, правам и правилам доступа к информации как для внутренних, так и внешних пользователей.

Пользователями настоящего стандарта могут быть (но не ограничиваться перечисленными ниже):

а) организации любого типа и размера (юридические лица), которые создают, хранят, обрабатывают и/или обмениваются информацией;

б) физические лица, которые создают, хранят, обрабатывают и/или обмениваются информацией;

в) физические лица, ответственные за учет документации, управление системой документационного обеспечения, управление информацией, защиту информации/данных и/или за их конфиденциальность, и

г) организации, которые создают, предоставляют или поддерживают инструментальные и программные средства, позволяющие реализовывать перечисленное в а)—в).

В настоящем стандарте предполагается, что информация рассматривается в форме, понятной для пользователей и допускающей обмен между ними. Далее по тексту аналогичная информация будет именоваться «информационным активом (ресурсом)» независимо от ее носителя или формата.

Примечание — Информационные активы могут содержать как структурированную, так и неструктурированную информацию, тексты, изображения и аудиозаписи, т. е. все то, что может содержать какую-либо информацию.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 53894 Менеджмент знаний. Термины и определения

ГОСТ Р 57133 Менеджмент организационной культуры и знания. Руководство по наилучшей практике

ГОСТ Р 54877 Менеджмент знаний. Руководство для персонала при работе со знаниями. Измерение знаний

ГОСТ Р 57127 Менеджмент знаний. Руководство по наилучшей практике

ГОСТ Р ИСО 9000 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

ГОСТ Р ИСО 15489-1 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Издание официальное

ГОСТ Р ИСО/МЭК 27038 Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 53894, а также следующие термины с соответствующими определениями.

3.1

классификация (classification): Систематическая идентификация и упорядочение деловой деятельности и (или) документов по категориям в соответствии с логически структурированными условиями, методами и процедурными правилами, представленными в классификационной системе.

[ГОСТ Р ИСО 15489-1—2007, пункт 3.6]

Примечание — В этих категориях во внимание принимаются такие факторы, как чувствительность информационных активов к потере или повреждению информации, т. е. к ее конфиденциальности, целостности и доступности.

3.2 **средства хранения информации** (storage media): Устройства, предназначенные для хранения цифровой информации.

3.3

отбор и передача (disposition): Процессы реализации управленческих решений, зафиксированных в перечнях документов или других инструментах управления документами и касающихся уничтожения документов или передачи их на последующее хранение.

[ГОСТ Р ИСО 15489-1—2007, пункт 3.13]

3.4

документ (document): Зафиксированная на материальном носителе идентифицируемая информация, созданная, полученная и сохраняемая организацией или физическим лицом в качестве доказательства при подтверждении правовых обязательств или деловой деятельности.

[ГОСТ Р ИСО 15489-1—2007, пункт 3.3]

Примечание — В качестве документа может рассматриваться материал, представленный в письменной, печатной, устной и визуальной формах, способный формировать, хранить, передавать или совместно использовать информацию.

3.5 **обработка** (handling): Операции, требующиеся для работы с информационными активами, которые промаркированы и обладают определенной классификацией.

3.6 **ICMH-система** (ICMH System): Совокупность взаимосвязанных и взаимодействующих элементов организации для установления политики и целей организации в отношении классификации, маркировки и обработки информации, а также процессов для их достижения.

3.7

информация (information): Значимые данные.

[ГОСТ Р ИСО 9000—2015, статья 3.8.2]

Примечание — Данные можно считать не содержащими собственного контекста, необходимого для интерпретации его смысла. Информация является точными, своевременными, конкретными и сформированными для определенной цели данными, представленными в контексте, который придает им смысл и актуальность, и может приводить к повышению степени их восприятия и снижению неопределенности этих данных. Информация обладает собственной ценностью, поскольку она может влиять на взаимоотношения, решения или результаты.

3.8 **информационные активы** (information asset): Совокупность информации, которая может разделяться и сохраняться в любой форме, например, в аналоговой или цифровой.

3.9 **жизненный цикл информации** (information lifecycle): Последовательность событий, которые отмечают этапы развития и использования информационных активов.

Примечание — Информационные активы в настоящем стандарте также называют информационными ресурсами.

3.10 **маркировка** (marking): Процесс, с помощью которого осуществляется регистрация и индикация классификации информационных активов (обычно — в самом информационном активе).

3.11 **материальные носители информации** (physical storage media): Реальное устройство (или средства), предназначенные для хранения информации.

Примечание — Информация может регистрироваться не в цифровой форме, например в виде печатного документа на бумажном носителе.

3.12 **запись** (record): Информация, сформированная, полученная и поддерживаемая в качестве доказательства и рассматриваемая организацией или физическим лицом как информационный актив в соответствии с юридическими обязательствами или при заключении сделок.

Примечания

1 Важной характеристикой записи является невозможность ее изменения.

2 Термин «доказательство» не ограничивается юридическим смыслом.

3 Записи могут существовать в разных формах и храниться на различных носителях (включая бумагу, диск, устройство хранения данных со съемным носителем/USB, CD, DVD, магнитную ленту для цифровой или аналоговой записи), включая документы и сообщения по электронной почте (тексты, приложения к электронным письмам), видео- и аудио-записи, изображения.

3.13

цензурирование (redaction): Необратимое удаление информации из документа.
[ГОСТ Р ИСО/МЭК 27038—2016, пункт 2.4]

3.14 **отображение (визуализация)** (render): Операция по преобразованию ресурса в легко воспринимаемую пользователем форму.

3.15 **репликация (мультиплицирование)** (replication): Цифровое дублирование информации при отсутствии внесения в нее изменений.

3.16 **схема** (scheme): Соответствующие конкретные требования и договоренности относительно отдельных видов работ по классификации, маркировке или обработке информации.

3.17

высшее руководство (top management): Лицо или группа людей, осуществляющих руководство и управление организацией на высшем уровне.
[ГОСТ Р ИСО 9000—2015, статья 3.1.1]

Примечание — Если сфера функционирования ICMH-системы охватывает только несколько подразделений организации, то руководители высшего звена будут управлять и контролировать только эту часть организации.

3.18 **работник** (worker): Сотрудник, находящийся под контролем организации, включая штатных и временных сотрудников, подрядчиков и консультантов.

4 Контекст организации

4.1 Понимание организации и ее контекста

Для разработки ICMH-системы организация должна определить контекст (организационную среду) и условия операционной деятельности (текущее состояние), которые должны быть задокументированы и официально утверждены руководством организации.

Примечание — При этом необходимо, как минимум, обозначить следующие аспекты:

а) цели и стратегии организации, а также ее ценности, видение себя и своей репутации, которые она стремится защищать и/или усиливать;

б) бизнес-функции и характер основной деятельности организации;

в) способ применения бизнес-функций, их виды и места осуществления своей деятельности;

г) ограничения процессов/методов (внешние и внутренние);

д) технологии, используемые и планируемые в краткосрочной перспективе; технологии, используемые для поддержки и реализации процессов/методов, и

е) заинтересованные стороны, с которыми организация взаимодействует и/или обменивается информацией.

Организация должна гарантировать, что ее профиль и организационная структура утверждены высшим руководством и могут быть использованы для валидации планируемой к разработке ICMH-системы (см. 5.2).

4.2 Межорганизационная координация работы ICMH-системы

В процессе изучения своего контекста организация должна разработать план взаимодействия с другими организациями, с которыми она планирует обмениваться информацией, и в особенности — изучить подходы этих организаций к оценке своих бизнес-рисков, которые могут отличаться от собственных рисков организации.

Организация должна учитывать требования к ICMH-системе (и к связанным с ней системам) тех организаций, с которыми она предполагает обмениваться информацией.

5 Лидерство

5.1 Ответственность сотрудников организации за результат

Руководство организации должно определить сотрудника, который в конечном итоге будет нести ответственность за проектирование, разработку и эксплуатацию ICMH-системы.

5.2 Определение направлений работ

Руководство организации должно четко определить и задокументировать свои ожидания в отношении работы ICMH-системы, например, с точки зрения предоставления отчетности, исходя из контекста организации (см. 4.1), потребности в координации работ со сторонними организациями (см. 4.2) и определения тех структурных подразделений, которые будут взаимодействовать с ICMH-системой.

5.3 Лидерство и ответственность руководства организации

Руководство организации должно продемонстрировать свои лидерские качества и возможности при работе с ICMH-системой.

Примечания

1 Это может осуществляться, например, на любом из первых этапов развертывания ICMH-системы или достигаться привлечением руководства организации к выполнению им на этом этапе определенных обязанностей.

2 Признавая острую реакцию сотрудников организации на действия своего руководства, отстранение руководства от выполнения работ, связанных с ICMH-системой, будет фактически подрывать обязательства руководства по отношению к самой ICMH-системе.

5.4 ICMH-концепция

Руководство организации должно обеспечивать разработку ICMH-концепции в соответствии с принципами, изложенными в 6.2, которая впоследствии должна быть официально утверждена, реализована и распространена (частично — для демонстрации возможности лидерства и обязательств руководства организации (см. 5.3), и частично — для содействия успешной реализации ICMH-системы); при этом руководство организации должно кратко изложить основные положения ICMH-концепции.

Примечание — Концепцию следует сделать доступной для широкого круга сотрудников и организаций, с которыми она предполагает в дальнейшем поддерживать информационный обмен.

5.5 Полномочия

Руководство организации должно четко распределить полномочия по управлению ICMH-системой между ее сотрудниками.

Примечания

1 Как правило, этими сотрудниками должны быть топ-менеджер или подразделение (функция) организации, которые уже обладают достаточными и связанными с ICMH-системой полномочиями для их использования в определенной сфере деятельности и анализа любых проблем или противоречий, выявляемых по результатам эксплуатации ICMH-системы.

2 В небольшой организации этими полномочиями должен обладать владелец или руководитель организации, а в более крупных организациях необходимо выбирать собственную структуру управления, в которой полномочия будут четко распределяться или закрепляться за ответственными сотрудниками, например, за директором по юридическим вопросам, специалистом отдела корпоративного контроля, руководителем службы информационной безопасности или за директором по управлению рисками.

Для выполнения роли координатора и консультанта организация должна назначить по крайней мере одного ответственного.

Примечания

1 Организация должна принять решение о том, будет ли эта роль ограничиваться лишь выдачей рекомендаций/указаний, или назначенный сотрудник будет обладать более широкими полномочиями в части, касающейся обучения персонала или классификации информации.

2 В тех случаях, когда эту роль будут выполнять несколько сотрудников, организация должна обеспечить регулярное проведение их встреч и обмен информацией между ними. Подобные встречи следует планировать, например, в виде форума или аналогичного мероприятия.

3 Конкретные роли могут исполнять сотрудники, ответственные за защиту данных и конфиденциальности информации, а также сотрудники службы безопасности, представители юридических лиц или физические лица, ответственные за информацию.

6 Планирование и проектирование ICMH-системы

6.1 Область применения ICMH-системы

Организация должна четко определить и задокументировать область применения разрабатываемой ICMH-системы с учетом определенных контекста (см. 4.1) и направлений деятельности организации (см. 5.2).

Примечания

1 В области применения ICMH-системы требуется отразить каждый элемент контекста организации для уточнения того, какой из этих элементов попадает/не попадает в область применения.

2 Возможно, будет существовать и перспективная область применения, которую также необходимо прояснить.

3 Если область применения системы достаточно ясна или проста для определения, то ее можно отразить в ICMH-концепции (см. 5.4).

6.2 Принципы создания ICMH-системы

Организация должна определить и задокументировать процесс создания системы для обработки информации способом, приемлемым для ее классификации. Классификация информации должна передаваться посредством ее маркировки.

Организация должна гарантировать, что ее ICMH-система:

а) является максимально простой, насколько это позволяют обстоятельства.

Примечание — Чрезмерно сложный процесс создания системы может оказаться затруднительным для ее применения в небольшой компании, а чрезмерно упрощенный процесс может не соответствовать сложности задач, решаемых в крупной организации;

б) отражает разумные ожидания своих сотрудников с целью достижения надлежащего баланса между тем, что должно, необходимо и будет сделано качественно;

в) способна давать достоверные результаты, не зависящие от пользователя, при многократном использовании информации;

г) пригодна для контроля и верификации;

д) может использоваться сотрудниками организации и автоматическими системами;

е) может использоваться для чисто ручных процессов (например, основанных на технологии регистрации информации на бумажных носителях), а также для полностью или частично автоматизированных процессов;

ж) учитывает все существующие атрибуты безопасности (секретности);

и) способна управлять ICMH-системами предыдущих поколений;

к) поддерживает соответствие между внутренними и внешними требованиями;

л) устойчива к изменениям под действием различных обстоятельств и технологий.

Примечание — При изменении функций или области применения ICMH-системы организациям может потребоваться введение дополнений в первоначальный вариант ICMH-системы (например, дополнительных дескрипторов);

м) учитывает все изменения, касающиеся содержания и ценности информации с течением времени, и

н) применима на протяжении всего срока службы ICMH-системы и жизненного цикла информационных активов.

Организация должна обеспечивать соответствие ICMH-системы разработанной концепции и процедурам управления документооборотом, а также соответствие юридическим и нормативно-правовым требованиям.

Примечание — Пользователям настоящего стандарта также рекомендуется учитывать возможность использования стандартов ГОСТ Р ИСО 15489-1, ГОСТ Р 55.0.01, ГОСТ Р ИСО 9001 и ГОСТ Р ИСО 30301.

Организация должна установить и задокументировать факт интеграции применяемых в организации методов обработки информации в систему менеджмента информационной безопасности (ISMS), если таковая имеется в организации. При отсутствии подобной системы интеграция должна осуществляться в соответствии с принятой в данной организации политикой информационной безопасности.

Организация должна принимать во внимание все имеющиеся у нее возможности по повышению эффективности обработки информации, в том числе с помощью средств информационно-телекоммуникационных технологий.

Примечание — Требования по обязательной поддержке методов управления могут варьироваться от обязательного использования стойких чернил для маркировки бумажных документов и до использования цифровых шаблонов, которые не могут изменяться пользователями.

6.3 Разработка системы классификации

6.3.1 Критерии классификации

Организация должна задокументировать схему (систему) классификации, в которой необходимо подробно описать методы классификации и указать разработчика системы, а также тех сотрудников организации, которые обладают доступом к информации и знакомы с механизмами ее маркировки и обработки.

Информацию необходимо классифицировать в соответствии со следующими критериями:

а) оценка прямой и косвенной ценности информации для соответствующей организации (организаций);

б) риск нарушения конфиденциальности информации, ее повреждения, потери или утраты доступа к информационным активам, а также возможность организации принять такой риск (риски);

в) связанные с классификацией затраты организации на выявление риска (критических событий) и оценка его негативных последствий, например нанесения вреда обществу, ущерба репутации организации, затраты на исправление и смягчение последствий этих событий и т. п.

г) ожидания заинтересованных сторон, которые могут не быть непосредственно связанны с информационными активами, но тем не менее имеют право предъявлять, например, требования юридического и нормативно-правового характера;

д) необходимость контроля уровня доступа к информационным активам на протяжении их жизненного цикла;

е) возможность обеспечения согласованности и сопоставимости уровней классификации и рисков, которые учитываются организацией при менеджменте рисков;

ж) объем оцениваемых усилий по защите информационных активов;

и) ожидания других организаций, с которыми ведется обмен информационными активами;

к) ожидания других заинтересованных сторон, например, представителей общественности и журналистов и т. п., даже в тех случаях, когда обмена информацией не происходит;

Организация должна определять и документировать перечень действий, которые должны выполнять ее сотрудники в тех случаях, когда они:

- не могут проводить оценку классификации или
- посчитают, что классификация, присвоенная информационному активу и промаркированная в нем, неверна.

Организация должна определить и задокументировать свое решение относительно влияния изменений классификации на достоверность и/или целостность информации.

Организация должна определить и задокументировать:

- процедуры, призванные снижать влияние изменений классификации на достоверность и/или целостность информации, и
- допустимые объем и степень изменения классификации, которые могут выполнять сотрудники организации для каждого класса информационных активов на протяжении всего их жизненного цикла.

Обоснования схемы классификации необходимо регистрировать и непрерывно контролировать.

Примечание — В приложении А приведен пример классификации, маркировки и обработки информации, а в приложении В — примеры и подробные рекомендации по применению ICMH-системы к информационным активам, представляемым в различных форматах и/или на различных носителях.

6.3.2 Иерархия информации

Информация должна классифицироваться в соответствии с установленной иерархией. При этом количество уровней иерархии должна определять сама организация.

Примечания

1 Как правило, иерархия ограничений доступа варьируется от ограниченного доступа к неограниченному. Краткий пример иерархии приведен в таблице 1; более подробный пример приведен в приложении А.

2 Организация должна принимать во внимание удобство пользования выбранной иерархией. В общем случае небольшое количество классов будет упрощать использование иерархии и обеспечивать ее надлежащее использование.

Наименования классов в той или иной иерархии должна задавать организация.

Примечания

1 Примером иерархии информации является: высокая степень конфиденциальности; нормальная степень конфиденциальности; отсутствие конфиденциальности и возможность обнародования информации.

2 Наименования классов должны быть наглядными; например, определение ограничений доступа по иерархии от «не конфиденциальный» до «высоко конфиденциальный», скорее всего, будет более наглядным, чем определение подобной иерархии в виде цифр от «1» до «5».

3 Если всю информацию классифицировать на максимально высоком уровне, то экономическая эффективность организации может оказаться заниженной; если же всю информацию необходимо классифицировать по критерию отсутствия ограничений доступа, то, вероятно, это может нанести ущерб организации.

Таблица 1 — Краткий справочный пример иерархии конфиденциальности информации

Класс информации	Описание
Высококонфиденциальная информация	Эта информация является наиболее конфиденциальной, поэтому следует проявлять чрезвычайно большую осторожность при предоставлении ненадлежащего доступа к ней (ограниченного доступа, поскольку совместное использование этой информации подразумевает возможность причинения вреда и большого ущерба организации)
Конфиденциальная информация	Эта информация менее конфиденциальна, однако при несанкционированном доступе к ней организации также может быть нанесен значительный ущерб
Внутренняя информация в организации	Эта информация является конфиденциальной в пределах организации, однако несанкционированный доступ к ней вряд ли сможет нанести ей значительный ущерб
Общедоступная информация	Эта информация предназначена для широкого распространения
Неклассифицированная информация	Вся другая информация или информационные активы не будут классифицироваться, поскольку эта информация будет тривиальной, а доступ к ней не будет представлять опасности для организации

4 Более подробный пример иерархии приведен в таблице А.1.

6.3.3 Эквивалентность схем классификации

Требования к эквивалентности должны устанавливаться в тех случаях, когда организация обменивается информацией или совместно использует информацию с другими организациями. При этом организация должна:

а) объяснить сторонним организациям основные положения функционирования своей ICMH-системы, чтобы они понимали эффективность этой системы, связанных с ней схем и требований к классификации, независимо от того, имеют ли сторонние организации свои схемы классификации;

б) согласовывать и документировать, когда это возможно, эквивалентность схем сторонних организаций и

в) определять и документировать способы информационного обмена, ее совместного использования или классификации и, следовательно, маркировки и обработки в сторонних организациях.

В случае создания или обновления схемы классификации организация должна задокументировать эквивалентность своих ICMH-схем схемам сторонних организаций, с которыми она обменивается информацией или совместно использует ее.

Примечание — Следует рассмотреть возможность использования такой технологии, которая способна обеспечивать надежное и согласованное сопоставления этих схем и применение правил контроля.

6.3.4 Жизненный цикл информационных активов

Схему классификации необходимо применять на протяжении всего жизненного цикла информационного актива — от момента его создания (или получения) и до его окончательного удаления (что может происходить через много лет).

Примечания

1 Несмотря на то, что термин «управление жизненным циклом» здесь напрямую не используется, его концепция подробно рассматривается в ГОСТ Р ИСО 15489-1, в котором управление учетными записями бизнес-деятельности сводится к «принятию надлежащих мер по защите их достоверности, аутентичности, целостности и удобства применения, поскольку бизнес-контекст и требования к их управлению со временем могут изменяться».

2 Нередко могут происходить изменения классификации конкретной информации и, следовательно, ее маркировки и обработки на протяжении всего жизненного цикла этой информации в организации (например, изменение с высокого уровня контроля доступа на более низкий, менее строгий уровень контроля доступа).

В тех случаях, когда изменение классификации запланировано заранее, организация должна задокументировать соответствующие причины (указать инициирующий фактор), процедуры и правила внесения изменений и обеспечить связь информации с этими причинами, процедурами и правилами.

Примечание — Изменения классификации могут предварительно планироваться или быть непредвиденными. Для заранее спланированных изменений классификации инициирующим фактором обычно бывает дата, период или какое-либо конкретное событие.

Организация должна определить и задокументировать основания, которые должны сохраняться для внесения запланированных или незапланированных изменений в классификацию информационных активов.

Примечание — Ниже приведен пример информации, которая может заноситься в журнал регистрации при внесении изменений в классификацию информационных активов.

Новая классификация:

- дата и время классификации/внесения изменений в классификацию;
- классификация информационных активов;
- полномочия, которые необходимы для внесения изменений в классификацию;
- время классификации, дата и любое обоснование, связанное с каким-либо событием (необязательно);
- ожидаемая в перспективе классификация (необязательно).

Предшествующая классификация (классификации) (для каждой предыдущей классификации):

- дата и время внесения изменений в классификацию;
- полномочия, которые необходимы для внесения изменений в классификацию;
- предшествующая классификация информации;
- срок действия (истечения действия) текущей классификации.

Для любой последующей предусмотренной классификации:

- инициирующий фактор, влияющий на изменение классификации (например, время, дата, событие и т. п.);

- возможная классификация информации (по категориям и т. п.);
- полномочия, которые необходимы для внесения изменений в классификацию;
- валидность (пригодность применения) классификации (необязательно).

Информацию в перечне изменений необходимо сделать доступной для того, чтобы предшествующие и последующие классификации можно было анализировать вместе с существующей классификацией и чтобы она служила основанием для изменения уровня классификации.

6.3.5 Стандартные классификации

Организация должна рассмотреть вопрос о том, следует ли создавать и использовать стандартную классификацию и документировать принятые решения.

Примечания

1 При создании или использовании схемы классификации организациям целесообразно вводить стандартную классификацию, которая будет приемлемой для общего, наиболее часто используемого подхода к конфиденциальности информации, поскольку эта классификация обычно облегчает классификацию информации, т. е. нестандартная классификация обеспечивает только индивидуальную маркировку информации. Стандартная классификация может применяться только к информации, которая не может классифицироваться иначе на всем ее жизненном цикле.

2 Даже в одной организации или в ее конкретных подразделениях может существовать несколько стандартных классификаций информации, например стандартная классификация информации в отделе маркетинга может отличаться от таковой в отделе кадров, где большая часть информации является персональной и более конфиденциальной, чем большая часть информации в отделе маркетинга.

3 Стандартная классификация информации по-прежнему должна обеспечивать ее соответствующую маркировку и обработку.

В организации, создающей или использующей стандартную классификацию, ее следует непосредственно включать в задокументированную схему классификации.

Примечание — При утверждении стандартной классификации следует принимать во внимание баланс между удобством ее применения пользователем и информированностью/подотчетностью пользователей, который подведет их к правильному выбору классификации.

6.3.6 Немаркированные информационные активы

В тех случаях, когда организация принимает решение не маркировать информационные активы и не подвергать их специальной классификации, она должна определить и задокументировать наиболее подходящую схему классификации и связанный с ней метод обработки информационных активов.

Примечания

1 Для этих целей часто используется стандартная классификация.

2 Альтернативой стандартной классификации обычно является «общедоступная» (не конфиденциальная) классификация (или аналогичная ей).

3 Указанное требование к маркировке вместе с требованием к обучению (см. 7.4) имеет важное значение, поскольку получатели немаркированной информации могут предполагать, что с ней вообще не связаны никакие ограничения на ее обработку и отсутствует необходимость в каком-либо ограничении доступа к ней.

6.3.7 Дескрипторы и взаимозависимости

Организация должна определить необходимость введения дескрипторов в их схему классификации и, в случае необходимости, введение дескрипторов в схему маркировки информации.

Примечания

1 В некоторых случаях, чтобы дать возможность любому пользователю, занимающемуся ее обработкой, понять сущность классификации информации и каким образом она выполнена, целесообразно применять дескриптор.

2 Ниже приведены примеры возможных дескрипторов:

а) информация, обеспечивающая идентификацию личности (PII);

б) правовая информация;

в) стратегическая информация;

г) структурная информация.

Организация должна определять необходимость введения или рассмотрения взаимозависимостей в ее схему классификации и, в случае необходимости, введение этих взаимозависимостей в схему маркировки.

Примечания

1 Решение об этом должно основываться на возможности существования этих взаимозависимостей.

2 Примеры типичных взаимозависимостей:

а) географические взаимозависимости: информация может иметь различный юридический статус, ценность или требования к безопасности в разных географических регионах; любая информация, доступная в Интернете, не может иметь никаких географических взаимозависимостей, если она каким-либо образом не ограничена;

б) временные взаимозависимости: информация может иметь различный статус или свою значимость в зависимости от времени и даты;

в) событийные взаимозависимости: конкретное событие, например раскрытие информации в соответствии с запросом типа «Свобода распространения информации», которое изменяет классификацию;

г) агрегационные взаимозависимости: информация может получать другой юридический статус или значимость, если она агрегирована или способна объединяться с другой информацией/данными;

д) подтверждающие взаимосвязи: информация и ее классификация могут потребовать дополнительной оценки или отклонения другой стороной.

3 Организация должна принимать в расчет нужное ей число дескрипторов и взаимозависимостей (если таковые имеются) и учитывать отрицательное влияние на ее работу большого числа дескрипторов/взаимозависимостей.

6.4 Разработка схемы маркировки

6.4.1 Критерии разработки схемы маркировки

Пользователь должен применять маркировку для конкретной классификации информации, т. е. классификация должна индицироваться определенным знаком.

Знак маркировки должен быть заметным для пользователя и оставаться заметным даже при копировании информации, обмене ею со сторонними организациями или преобразовании ее формата.

Знак должен быть заметен при использовании любого метода просмотра или доступа к информации.

Примечание — Например, верхние и нижние колонтитулы в электронных документах могут по умолчанию скрываться во многих программах при чтении или редактировании этих документов. Схема маркировки, использующая только верхние и нижние колонтитулы, может быть не всегда заметной. Знак маркировки, который может зависеть от конкретной программы, способен существенно повышать вероятность «потери» метки классификации при изменении формата.

В тех случаях, когда введение видимого знака маркировки неприемлемо, этот факт должен быть четко определен и задокументирован в организации.

Примечания

1 За исключением тех случаев, когда информационный актив предназначен для общественного пользования, отсутствие знака маркировки не должно обесценивать информацию.

2 Термин «видимый» здесь используется в смысле немедленного восприятия информации в соответствии с ее форматом; при прослушивании звукового файла, считывании шрифта Брайля или отображении информации на экране или в документе.

Знак маркировки (метку) необходимо проверять каждый раз при пересмотре классификации. Если организация примет решение не пересматривать все ранее промаркированные информационные активы при изменении схемы, то организация должна задокументировать это решение и сформулировать требования к обработке этих активов, классифицированных по прежней схеме (после реализации новой схемы маркировки).

Метаданные не следует использовать в качестве эквивалента знака маркировки, но в тех случаях, когда они предназначены для целей классификации, эти метаданные должны соответствовать видимому знаку маркировки.

Примечание — Метаданные — это информация, содержащая несколько файлов, которые описывают информационный актив. ICMH-технологии и инструментальные средства обычно используют метаданные для регистрации и передачи методов классификации. Без использования указанных технологий метаданные могут быть не сразу заметны и не передаваться автоматически при изменении формата представления информации.

6.4.2 Расположение и стиль маркировки

Организация должна определить и задокументировать стиль, расположение и схему маркировки, которые будут использоваться для маркировки информационных активов.

Примечания

1 Стиль, расположение и схема маркировки должны применяться систематически и быть пригодными для маркировки различных носителей информации или форматов.

2 Настоящий стандарт не регламентирует способы расположения и место расположения знака маркировки на видео-, аудио- или любом другом виде информации.

Знак маркировки должен быть виден при доступе к информационному активу. Если идентификационная маркировка невозможна, то этот факт в организации необходимо зафиксировать и задокументировать.

Примечания

1 Не вся информация может быть напрямую доступной (например, через веб-сайты). В тех случаях, когда информацию получают подобным способом, следует принимать меры по обеспечению наглядности информации при сохранении простого доступа к ней.

2 Схема маркировки может зависеть от уровней классификации. Информация на минимально конфиденциальном уровне классификации должна требовать наименьших усилий при маркировке, тогда как на максимально высоком уровне конфиденциальности следует прикладывать значительные усилия. Например, в последнем случае информация может получить преимущества от непрерывности маркировки, которые всегда будут заметны при просмотре, прослушивании или ощущении. Маркировка может наноситься в виде водяных знаков на документы, надписей на видеоматериалах или непрерывного тона на аудиоматериалах. Маркировка также будет гарантировать сохранение маркировки даже при частичном просмотре информации, например, одной страницы печатного документа. Информация с низким уровнем конфиденциальности не должна требовать достаточно сложной маркировки, которую авторам/редакторам даже не следует пытаться реализовать.

Организация должна (по возможности) автоматизировать приложение и предотвращать несанкционированное удаление или изменение маркировки информации.

6.5 Разработка схемы обработки

6.5.1 Критерии разработки схемы обработки

Организация должна определить конкретные меры контроля для каждой классификации, которая будет передаваться с помощью конкретного знака маркировки.

Схема классификации должна обеспечивать обработку информационных активов способами, обладающими определенной классификацией (при наличии предварительно созданных условий).

Примечания

1 Таким образом, классификация будет способствовать созданию метода изменения правил, связанных с тем, когда и кому разрешается доступ к информационным активам (или к специализированным способам обработки информации для того или иного бизнес-партнера).

2 Например, организация сделала вывод о необходимости шифрования информации для определенных классификаций и меток, что в дальнейшем в обязательном порядке должно быть доведено до специалистов, занимающихся обработкой информации.

Схема управления в организации должна четко определять, какие ее сотрудники способны обрабатывать информацию и какими методами.

Примечания

1 Определение того, какие сотрудники организации имеют право обрабатывать информацию, может зависеть от их ролей, уровней или от индивидуального выбора, как того потребуют обстоятельства или предпочтения руководства организации.

2 При необходимости, пригодность конкретных сотрудников организации к обработке информации необходимо проверять методами и процедурами, в соответствии с кадровой политикой организации. Соответствующая информация приведена в приложение А к ГОСТ Р ИСО/МЭК 27001.

Организация должна определить и задокументировать:

а) какая автоматическая обработка информации допускается для промаркированных информационных активов;

б) какие классификации информации могут формироваться и на каких платформах;

в) когда рабочие версии информационных активов должны сохраняться, в какой форме и на какой срок;

г) процесс фиксации и реагирования на известные случаи ненадлежащей обработки информации с точки зрения ее классификации, совместимой с системой управления записями в организации.

6.5.2 Обработка информации в процессе ее первоначального формирования и сбора

Организация должна четко указывать, кем и какую информацию можно формировать и/или принимать и какие разрешения для этого необходимы и от кого.

Организация должна обеспечивать возможность классификации информации по месту ее формирования и в соответствии с используемой схемой классификации (см. 6.3).

Организация должна определять спецификации (технические характеристики) на все используемые классификации.

Примечания

1 Например, если информационный актив представляет собой документ, то эти спецификации, как минимум, должны содержать форматы страниц и их разбивку, нумерацию страниц, стиль этой нумерации, способ нумерации копий, места размещения знаков нумерации и способ обработки пустых страниц. В тех случаях, когда информационный актив не является документом, например аудио- или видеофайлом, следует применять другие спецификации.

2 Необходимость нумерации копий может потребовать отслеживания их получателя. В подобных случаях данная информации была бы разумной мерой для ее регистрации (помимо информационных активов).

Если это необходимо для любой заданной классификации (классификаций) и, кроме того, для высококонфиденциальных информационных активов, организация должна вести журнал регистрации классификации, маркировки и обработки информации на протяжении всего жизненного цикла информационных активов.

Примечание — По этой причине ведение подобного журнала должно инициироваться при формировании первого информационного актива, т. е. факт его регистрации будет самой первой записью в этом журнале.

После того как будет решено, что формирование информационного актива уже закончено, его разработчик должен повторно оценить его классификацию и, при необходимости, изменить его прежнюю маркировку и способ обработки.

6.5.3 Многократное использование информации в других информационных активах

Организация должна создать и задокументировать процесс управления многократным использованием информационного актива, его отдельных фрагментов или применением в других информационных активах. При этом следует уточнить следующие вопросы:

а) какие на это потребуются разрешения и согласования;

б) как информация после этого будет классифицироваться, маркироваться и обрабатываться.

6.5.4 Редактирование и внесение изменений в информационный актив

При редактировании или внесении существенных изменений в информационный актив его классификация должна подвергаться повторной оценке, с определением необходимости или способа изменения соответствующей маркировки и обработки информации.

В ICMH-системе необходимо определить термин «существенное изменение».

Примечание — Существенные изменения должны включать в себя редакционные изменения, дополнения, поправки, замещение или удаление какой-либо части (или всей) информации, содержащейся в информационном активе.

6.5.5 Агрегирование информации

Организация должна определить и задокументировать способ классификации, маркировки и обработки той информации, которая предварительно была агрегирована или получена из другого информационного актива.

Примечания

1 Объединение информации из нескольких источников может приводить к генерации информации, требующей уже другой классификации. То же самое относится и к случаю дезагрегации (разукрупнения) информации. Можно привести простой пример того, как объединение информации из разных источников будет изменять классификацию и тем самым влиять на связанную с этим объединением маркировку и обработку информации, например объединение перечня проданных продуктов с перечнем имен покупателей. Кроме того, организации должны принимать во внимание тот факт, что в эпоху «больших данных» (big data) объединение информации от различных источников может приводить к формированию (иногда случайному) «персональной информации», которой необходимо обеспечивать дополнительную специализированную защиту. Пример подобной ситуации приведен в В.10.4.

2 Агрегирование информации, обладающей различными уровнями классификации, может приводить к тому, что агрегированный информационный актив получит наиболее критичную из всех источников информации маркировку.

6.5.6 Доступ к информации

На основе принятой классификации организация должна устанавливать и давать полномочия/возможности для логического и физического доступа к информации. Организация также должна определять и документировать способ предоставления и контроля доступа.

Примечание — Разрешение на доступ может потребовать использования паролей и аутентификации пользователя, например правил дистанционного доступа (был ли он разрешен и как был получен), использования информации о помещениях и физических ограничений (или любых других возможных), например по размещению информации.

Организация должна определять, когда, при каких обстоятельствах и каким образом информационный актив под контролем организации может передаваться из его фактического, географического местонахождения, между различными регионами, возможно, с различными правовыми юрисдикциями.

В случае внесения изменений в схему классификации или в саму классификацию (и маркировку), связанную с конкретным информационным активом, права доступа сотрудника организации к этому активу должны быть пересмотрены, а внесенные изменения — задокументированы.

В тех случаях, когда этого в организации требует ICMH-система (и в особенности ее схемы классификации и обработки информации), она должна обеспечивать введение и реализацию прав доступа к информационным активам и любых ограничений, установленных исходя из соответствующих принципов.

6.5.7 Хранение информации

Организация должна определить и задокументировать правила хранения промаркированных информационных активов.

Примечания

1 Правила хранения могут быть связаны с типами, правами собственности, безопасностью, возможностью объединения и расположением операционных систем в устройствах, которые можно использовать для хранения информации с определенной классификацией. Например, один информационный ресурс может храниться на ноутбуке с криптографической защитой (но не на USB-накопителе), другой информационный актив — только на серверах, находящихся в определенном месте, а третий информационный актив — на общедоступном «облаке» или на других платформах совместного пользования.

2 Например, в то время как процедура маркировки электронного документа относительно проста, получение аудио- или видеоинформации с наложенными на нее маркировкой или тоном (которые впоследствии невозможно удалять или изменять) может оказаться дорогостоящим.

Системы, предназначенные для хранения и отображения информации в безопасном режиме, могут по умолчанию рассматриваться как отвечающие требованиям защиты информации. В этом случае организация должна документировать информацию с указанием того, что ее можно считать промаркированной и защищенной. Информацию в таких системах необходимо защищать от извлечения или совместного использования и подвергать маркировке.

Примечание — Примером может служить аудиозапись беседы, содержащей конфиденциальную информацию, но ставшей доступной во внутрикорпоративной сети компании. На экране может отображаться необходимая информация о маркировке, тогда как в самом аудиофайле аудиоинформация о маркировке будет отсутствовать. При удалении одной и той же информации из исходной системы и передаче ее в другое место сам аудиофайл должен содержать информацию, относящуюся к ее безопасности.

6.5.8 Репликация и отображение информации

Организация должна определить и задокументировать приемлемое для нее время копирования, репликации, отображения или любого иного способа преобразования информационного актива в новую форму (когда это возможно). Даже при репликации или отображении информационного актива в другом формате (или на другом носителе) правила классификации должны оставаться неизменными.

Правила маркировки и обработки реплицированных или отображаемых информационных активов должны соответствовать формату или носителю информации в ICMH-системе, которые могут отличаться от прежних правил.

Примечание — Примером может служить электронный информационный актив, который преобразуется, например, из текстового формата в PDF-формат, или который становится доступным уже не в электронной форме.

Если операции репликации или отображения информации приводят к ее преобразованию в новую форму, то правила обработки этого информационного актива должны отражаться на схеме обработки информации.

В тех случаях, когда подобная репликация осуществляется аппаратно, например при распечатке, отправке факсов или копировании, организация должна определить и задокументировать приемлемые правила обработки, в том числе возможность репликации информации на автоматизированном рабочем месте.

Примечание — Например, когда репликация информации осуществляется на удаленном рабочем месте, с помощью аппарата факсимильной связи или сетевого принтера, ответственный за репликацию сотрудник организации должен информировать сотрудника, работающего на этом удаленном рабочем месте, о необходимости его присутствия вблизи этих приемных устройств и реальной защите поступающей информации.

Для любой заданной классификации (классификаций) организация должна определить и задокументировать необходимость в любой реплицированной информации и информацию о самой репликации.

Примечание — Информация о репликации может содержать сведения о содержании реплицируемой информации, исполнителе, причине, времени, месте и используемом средстве репликации.

После репликации информационного актива в его реплицируемой версии необходимо сохранять исходную классификацию и маркировку.

В тех случаях, когда информационный актив реплицируется в любой иной форме, необходимо использовать стиль маркировки, предусмотренный для новой формы.

Примечание — Пример — распечатка информационного актива в онлайн-режиме.

При репликации организация должна определить и задокументировать те экземпляры (при их наличии), в которых классифицированный и маркированный информационный актив может воспроизводиться без классификации.

Примечание — Например, маркетинговый документ в процессе его оформления может классифицироваться и маркироваться как «общедоступный», однако после официальной публикации маркировка будет удаляться, хотя характер обработки будет оставаться неизменным.

6.5.9 Пересмотр информации

При пересмотре информационного актива его классификация должна подвергаться переоценке и, следовательно, определению необходимости и/или способа внесения изменений в соответствующую маркировку и обработку информации.

Примечание — Некоторые информационные активы, обладающие соответствующей классификацией, могут содержать информацию, которая не должна раскрываться некоторым сообществам, однако после соответствующей обработки исходной информации ее измененные версии (но с измененной классификацией, маркировкой и обработкой информации) все же могут предоставляться этим сообществам. Подобная обработка может, при необходимости, включать в себя удаление каких-либо разделов, абзацев или предложений (с упоминанием об их удалении). Этот процесс называется «пересмотром/редактированием информационного актива».

Организация должна обрабатывать измененную версию исходного информационного актива как новый информационный актив.

Примечание — Пересмотр/редактирование информации также может сопровождаться удалением метаданных информационного актива или конкретной информации (например, изображений).

В тех случаях, когда информационный актив необходимо подвергать цифровой обработке, используемые процессы/процедуры должны обеспечивать невозможность восстановления отредактированной или удаленной информации из отредактированного информационного актива.

Примечания

1 При использовании многих серийно выпускаемых цифровых устройств информация может просто «скрываться» в неотображаемых частях информационного актива, а затем восстанавливаться, что может сводить на нет результаты редактирования и последующей классификации информационного актива.

2 В ГОСТ Р ИСО/МЭК 27038 приведены более подробные сведения о методах цифровой обработки информации.

6.5.10 Распространение, совместное использование и обмен информацией

Организация должна четко определить возможность распространения или совместного использования информационного актива, обладающего определенной классификацией и при наличии такой возможности указать конечных адресатов, а также каким образом и при каких обстоятельствах это допускается. Правила совместного использования должны принимать во внимание права и обязанности получателей информационного актива.

Примечания

1 Права получателей информационного актива на его обработку должны включать право на его дальнейшее распространение и возможность использования функции «переадресовать», существующей в большинстве систем обмена электронной корреспонденцией.

2 Существуют такие средства управления, например, защищенные корпоративные платформы, которые способны поддерживать стандартизованный TLP- протокол.

Организация должна определить тип носителя (носителей) информации (например, USB-накопители, «облачные» службы обмена информацией, мгновенные чаты и платформы обмена сообщениями), которые способны обеспечивать распространение или совместное использование информации.

В тех случаях, когда использование корпоративных платформ не утверждено, организация должна запретить их использование, и либо предоставить эквивалентные утвержденные, надежные средства, либо указать утвержденные, альтернативные методики.

Организация должна определить и задокументировать типы каналов распространения информации, например, почту и электронную почту, которые допустимы для каждой классификации.

Организация должна определить и задокументировать условия и приоритетность схем обработки по сравнению с любой формальной схемой совместного использования или раскрытия информации, в которой они взаимодействуют.

6.5.11 Архивирование и удаление информационных активов

Организация должна определить и задокументировать перечни версий сохраняемых информационных активов, формы и сроки их хранения способом, совместимым с общими методиками и процедурами управления информацией и документооборотом, а также с соблюдением юридических и нормативно-правовых требований.

Организация должна обладать методиками и процедурами отслеживания, сбора и удаления всех копий или версий информационных активов.

Организация должна определить, каким образом информационные активы с различными классификациями и на различных носителях могут храниться, удаляться, стираться или уничтожаться.

Примечание — Эти процедуры должны использоваться в таких организациях, которые наделены полномочиями по архивированию/удалению информации, и организациями, которые могут выполнять эти операции. Например, существует большое количество сторонних организаций, предлагающих свои услуги по измельчению и удалению документации, которые могут считаться достаточно безопасными для данных классификаций.

Организация должна определить и задокументировать способы сохранения дежурных журналов или любой другой документации, содержащей фактическую информацию относительно жизненного цикла информационных активов, времени и способа их удаления.

Примечание — В ГОСТ Р ИСО 15489-1 приведены полезные рекомендации по архивированию и безопасному уничтожению информационных активов.

6.5.12 Обеспечение информационной безопасности

Организация должна определить и задокументировать правила обеспечения информационной безопасности, связанные с каждой классификацией для используемой схемы обработки информации.

Примечание — Все эти правила могут включать шифрование информации при хранении (или при передаче информации), управление цифровыми правами, предотвращение потери данных или безопасное хранение, пакетирование и правила передачи информации.

Организация должна определить и задокументировать правила обработки, связанные с каждой классификацией, с целью удаления информации с аналоговых и цифровых носителей.

Примечание — Например, жесткий диск ноутбука может содержать информацию, доступ к которой имеет только директор по управлению персоналом. Если ноутбук затем будет использовать какой-либо другой пользователь, то следует определить и реализовать правила, связанные с удалением этой информации с ноутбука.

В рамках собственной схемы обработки информации организация также должна определить и задокументировать правила шифрования, которые должны быть связаны с каждой классификацией (в т. ч. в процессе передачи информации).

Примечание — Например, может потребоваться шифрование персональной информации при ее поступлении в офис или хранении на определенных устройствах (например, на USB-накопителях).

7 Средства обеспечения ICMH-системы

7.1 Ресурсы для ICMH-системы

Для успешного функционирования ICMH-системы организация должна выделить достаточное количество ресурсов, необходимых для покрытия всех рабочих аспектов системы.

Для контроля и оценки эффективности использования выделенных ресурсов организация должна проводить анализ работы ICMH-системы в рамках ее основного (не второстепенного) вида деятельности.

7.2 Роли и обязанности сотрудников

Организация должна обеспечивать четкую формулировку и обмен информацией относительно ролей и обязанностей сотрудников организации и связанных с ними прав доступа к ICMH-системе и ограничений (см. 7.3).

Организация должна определить и задокументировать компетенции ICMH-системы, необходимые для каждой роли, закрепленной за определенным сотрудником организации.

Организация должна обеспечивать соответствие прав доступа к этим системам ролям и обязанностям, возлагаемым на сотрудников организации (в тех случаях, когда для поддержки ICMH-системы используются любые системы автоматизации).

Организация должна определить, задокументировать и предоставлять сведения о последствиях, связанных с неисправностями системы, а также активно и должным образом применять ICMH-систему.

7.3 Распространение информации

ICMH-система должна обмениваться информацией с внутренними подразделениями организации, а также с теми организациями, с кем система осуществляет информационный обмен (на протяжении срока валидности информации и до даты ее пересмотра).

Примечание — Помимо проведения для сотрудников организации соответствующего обучения (см. 7.4), характерные особенности ICMH-системы часто целесообразно представлять в виде таблицы, которая затем может изображаться в виде простой настольной контрольной диаграммы, постера и т. п.

7.4 Обучение и информирование сотрудников

Организация должна обеспечивать всем сотрудникам организации надлежащую и адекватную подготовку по вопросам классификации, маркировки и обработки информации.

Примечание — Предлагаемая профессиональная подготовка персонала должна охватывать все используемые методики и технологии, а также подчеркивать важность непрерывности процесса обработки информации на протяжении всего ее жизненного цикла.

Организация должна обеспечивать предоставление соответствующей информации всем своим сотрудникам для надлежащего выполнения работ и совершенствования функционирования ICMH-системы в организации, независимо от того, будет ли это происходить в процессе обучения/информирования персонала или распространения информации (см. 7.3).

7.5 Практические занятия и тестирование

Организация должна определять, когда потребуется тестирование ICMH-методик и практические занятия по их применению, и если они необходимы, то в каких формах.

Примечание — Все это может оказаться целесообразным в процессе первичного развертывания ICMH-системы, в особенности — при выполнении сотрудниками организации наиболее сложных ролей и обязанностей в рамках системы (см. 7.2), а не в процессе их непрерывного обучения и повышения информированности (см. 7.4) или при выполнении ими менее сложных функций.

8 Деятельность организации

Организация должна планировать, осуществлять и контролировать процессы, необходимые для выполнения вышеуказанных требований, а также выполнять операции, указанные в разделе 6, а также определенные меры по совершенствованию ICMH-системы (см. 9 и 10) путем:

а) формулирования критериев оценки процессов относительно:

1) применимости (области применения) системы (см. 6.1);

2) разработки схемы классификации (см. 6.3), т. е.:
   - критериев классификации (см. 6.3.1),
   - иерархии (см. 6.3.2),
   - эквивалентности схем (см. 6.3.3),
   - жизненного цикла информационных активов (см. 6.3.4),
   - стандартной классификации (классификаций) (см. 6.3.5),
   - немаркированных информационных активов (см. 6.3.6),
   - дескрипторов и взаимозависимостей (см. 6.3.7);
3) разработки схемы маркировки (см. 6.4), т. е.:
   - критериев разработки схемы маркировки (см. 6.4.1),
   - расположения и стиля маркировки (см. 6.4.2);
4) разработки схемы обработки информации (см. 6.5), т. е.:
   - критерии разработки схемы обработки (см. 6.5.1),
   - обработка информации в процессе ее первоначального формирования и сбора (см. 6.5.2),
   - многократное использование информации в других информационных активах (см. 6.5.3),
   - редактирование и внесение изменений в информационный актив (см. 6.5.4),
   - агрегирование информации (см. 6.5.5),
   - доступ к информации (см. 6.5.6),
   - хранение информации (см. 6.5.7),
   - репликация и отображение информации (см. 6.5.8),
   - редактирование информации (см. 6.5.9),
   - распространение, совместное использование и обмен информацией (см. 6.5.10),
   - архивирование и удаление информации (см. 6.5.11),
   - обеспечение информационной безопасности (см. 6.5.12),
   - анализ и классификация немаркированной информации (см. 6.3.6),
   - анализ и повторная классификация информации с ненадлежащей классификацией (см. 6.3.1);

б) осуществления контроля за процессами в соответствии с установленными критериями;

в) ведения задокументированной информации в той степени, в которой это необходимо для получения уверенности и обоснованности спланированных и выполненных операций;

г) мониторинга и интерпретации проблем, возникающих при использовании подхода, описанного в разделе 6.

9 Оценка результатов

9.1 Общие положения

Организация должна определить действующую программу оценки эффективности своей деятельности, которую необходимо выполнять сразу же после первого применения ICMH-системы.

Программа оценки должна обеспечивать:

а) использование схем классификации, маркировки и обработки информации, которые могут контролироваться всеми создателями информации в рамках области применения, установленной организацией;

б) использование ICMH-системы, которое будет соответствовать методикам и процедурам, принятым в организации, т. е. чтобы ICMH-система выполняла их надлежащим образом; и

в) сбор соответствующей информации для выявления недостатков и стимулирования повышения эффективности функционирования организации (см. раздел 10).

9.2 Мониторинг и тестирование ICMH-системы

Организация должна определить и задокументировать критерии, с помощью которых следует оценивать степень применимости и эффективности ICMH-системы.

Организация должна сформулировать критерии для обеспечения и оценки совместимости и взаимодействия различных ICMH-систем.

Организация должна определить и задокументировать мероприятия, которые предпринимались для мониторинга и/или проверки работы ICMH-системы.

Примечание — Организация должна поддерживать согласованную оценку уровня развития (зрелости) своей ICMH-системы (систем). Подобная оценка должна принимать в расчет такие факторы, как:

а) степень охвата информационных активов областью применения ICMH-системы;

б) восприятие персоналом информационных активов и его стремление к работе в ICMH-системе в рамках области ее применения;

в) полнота и правильность функционирования ICMH-системы;

г) степень, в которой используемая технология позволяет или препятствует достижению целей, поставленных перед ICMH-системой;

д) эффективность ICMH-устройств при обмене информационными активами.

9.3 Проведение аудита и достоверность результатов

Организация должна определить и задокументировать необходимость в независимой оценке эффективности, если таковая требуется. Оценку следует принимать во внимание наряду с оценкой собственной эффективности, выполняемой теми сотрудниками организации, которые связаны с выполнением функций и обязанностей по управлению ICMH-системой.

Примечание — Аудит должен охватить все аспекты работы ICMH-системы, включая ее применение к информационным активам организации, а также сведения, содержащиеся в различных рабочих журналах.

9.4 Измерение показателей ICMH-системы

Организация должна определить и задокументировать номенклатуру показателей, которые необходимо учитывать, а также ее пользователей (их активность в системе) и временные интервалы ее функционирования.

Примечание — Возможно, что результаты подобных измерений будут приводить к появлению новых требований к предоставлению эксплуатационной информации, вводимой в существующие правила отчетности.

9.5 Управление инцидентами и их расследование

Для поддержания систем управления информацией в надлежащем состоянии и стимулирования их постоянного совершенствования организация должна специально анализировать и сообщать обо всех событиях ICMH-системы, связанных с нарушением информационной безопасности.

9.6 Предоставление отчетности и анализ накопленного опыта

Организация должна периодически предоставлять эффективную отчетность (в первую очередь своим топ-менеджерам) в части степени пригодности ICMH-системы и эффективности ее функционирования.

По результатам рассмотрения представленной отчетности организация должна извлекать уроки и формулировать требования к совершенствованию ICMH-системы в отношении как минимум регистрации причин наступивших инцидентов и выявленных недостатков в работе системы.

Примечание — Подобная отчетность должна относиться к пунктам 9.2—9.5 и предназначаться для стимулирования постоянного совершенствования ICMH-системы (см. раздел 10).

10 Улучшение ICMH-системы

10.1 Анализ управленческой деятельности

Организация должна проводить анализ управленческой деятельности с заданной периодичностью. Все сотрудники организации, выполняющие основные управленческие функции в ICMH-системе, а также исполнители по направлениям деятельности организации, должны вносить свой вклад в проводимый анализ.

Организация в процессе подобного анализа должна решить, какие изменения необходимо внести в ICMH-систему (при необходимости).

Примечание — Примерами тем, которые подлежат рассмотрению при анализе управленческой деятельности, являются:

а) характер возможных изменений основных направлений деятельности организации;

б) характер возможных изменений целей, приоритетов и видов деятельности организации;

в) результаты оценки эффективности деятельности организации (см. раздел 9);

г) рассмотрение существующих схем и информационных активов в части возможности внесения в них изменений (см. 10.3).

10.2 Доработка системы

По итогам анализа управленческой деятельности (см. 10.1) организация должна обеспечить устранение всех выявленных недостатков в соответствующих ICMH-схемах и внесение в них изменений, которые должны выполняться в кратчайшие сроки, в полном соответствии с характеристиками ICMH-системы.

Примечание — Для доработки системы организация должна обеспечивать постоянный мониторинг и поддержание эксплуатационной документации (см. 4.1) для выявления любых существенных изменений.

10.3 Внесение изменений в ICMH-схемы

По итогам анализа управленческой деятельности (см. 10.1) организация должна устранить все выявленные в соответствующих ICMH-схемах недостатки и в кратчайшие сроки в полном соответствии с требованиями к ICMH-системе внести соответствующие изменения. При этом организация также оставляет за собой право на оперативное внесение изменений в ICMH-схемы (при необходимости).

Примечание — Например, внесение изменений, обусловленных изменениями законодательных или нормативно-правовых требований.

В случае изменения общей классификации информации также необходимо регистрировать и изменения классификации, связанные с определенным информационным активом или правами доступа к этому активу.

10.4 Управление изменениями/постоянное совершенствование ICMH-системы

Организация должна предоставлять ICMH-системе достаточные ресурсы (см. 7.1), распределять роли и обязанности среди сотрудников организации (см. 7.2), что необходимо для поддержания управления изменениями в ICMH-системе и/или в подчиненных схемах.

Организация должна выделять на ICMH-систему достаточное количество ресурсов (см. 7.1), распределять роли и обязанности среди сотрудников организации (см. 7.2), что является обязательным условием непрерывного совершенствования ICMH-системы.

10.5 Поэтапное расширение области применения ICMH-системы

В тех случаях, когда ICMH-система первоначально применялась только в некоторых подразделениях организации и/или к некоторым, но не ко всем видам информационного обмена, организация должна предусмотреть возможность разработки, документирования и реализации перспективного плана развития (или аналогичного документа) для поэтапного расширения области применения ICMH-системы.

Примечание — В организации могут существовать подразделения, которые, возможно, не будут нуждаться в использовании ICMH-системы. Стратегический план развития можно использовать для определения и регистрации подобных подразделений. Тем не менее, следует предположить, что всем сферам деятельности организации будет соответствовать, как минимум, наиниший уровень требований к ICMH-системе (с использованием стандартной классификации, без маркировки и т. п.), чтобы она попадала в сферу деятельности организации и была развернута в ней раньше, чем в более сложной сфере деятельности.

10.6 Поэтапная интеграция ICMH-системы в организацию

Организация должна сосредоточить свою деятельность на поэтапной интеграции с ICMH-системой.

Примечание — Например:

а) новые информационные системы могут планироваться к приобретению (если они будут выбраны, имея в виду область применения ICMH-системы) при условии выполнения требований по эффективному применению этой системы;

б) для более эффективной поддержки ICMH-системы могут разрабатываться новые рабочие процессы.

10.7 Поэтапная интеграция ICMH-системы в систему менеджмента организации

Организация должна рассмотреть вопрос о необходимости интеграции своей ICMH-системы и соответствующих схем в другие системы менеджмента организации.

Примечания

1 Подобная интеграция должна способствовать повышению общей экономической эффективности и результативности деятельности организации.

2 Многие системы менеджмента (например, системы менеджмента информационной безопасности, конфиденциальности, управления безопасностью, непрерывности бизнеса и качества) неразрывно связаны с ICMH-системой, вследствие чего на начальных этапах ее проектирования система будет находиться под сильным воздействием этих систем.

3 Эта взаимозависимость, вероятно, потребует предоставления отчетной информации для ICMH-системы (см. 9.6).

4 ГОСТ Р 53893 — это стандарт на интегрированные системы менеджмента, который будет способствовать организации в создании единой структуры управления всеми ее системами менеджмента.

Приложение А
(справочное)

Примеры схем классификации, маркировки и обработки информации

Схемы, рассмотренные в таблицах А.1 и А.2, приведены в настоящем стандарте исключительно в качестве примеров применения положений настоящего стандарта, и не рекомендуются для непосредственного применения на практике, хотя они могут стать основой и внести полезный вклад в решение рассматриваемой задачи по разработке и внедрению ICMH-системы.

Следует отметить, что несмотря на использование в данном примере пяти уровней классификации, это число ни в коей мере не является обязательным и в ряде случае может оказаться избыточным.

В нижеприведенном примере рассматривается организация, которая уделяет повышенное внимание конфиденциальности, доступности и целостности информации. Если бы другие аспекты, связанные с информацией, обладали более высокими приоритетами, ICMH-схемы, безусловно, выглядели бы иначе.

Таблица А.1 использовалась организацией в качестве «памятки на рабочем месте» (в виде коврика для мыши или плаката).

В таблице А.2 представлена подробная схема обработки информации в организации, которая расширяет схему в таблице А.1, одновременно иллюстрируя все положения настоящего стандарта и его взаимосвязь с TLP-протоколом (Traffic Light Protocol).

Подход, принятый при составлении таблицы А.2, заключается в акцентировании внимания исключительно на существующих требованиях. Например, информация, классифицированная, маркированная и обрабатываемая как «общедоступная», может физически уничтожаться и удаляться любым удобным способом, т. е. не устанавливаются обязательные требования, касающиеся измельчения документов, разрезки или немеханического уничтожения документов. Оба эти способа считаются экономически неоправданными из-за высокой стоимости оборудования и большого числа необходимых устройств уничтожения информации.

Таблица А.1 — Пример схемы классификации и маркировки информации

Классификация	Соответствующий уровень риска	Соответствующая маркировка	Описание воздействия	Примеры	Сущность правил по совместному использованию и обработке информации
Высококонфиденциальная информация	Очень высокий	Высококонфиденциальная	Сильное влияние на финансовый сектор и/или на экономику или на ее политический курс. Многомиллионный ущерб и серьезные затруднения, которые вызывают отрицательную реакцию общества. Жизнеспособность организации и ее партнеров ставится под угрозу.	Стратегические планы. Пароли. Конфигурация системы безопасности и другие конфигурации. Кредитные ограничения. Данные о мошенничестве в бизнес-сфере. Коммерческая информация. Документы, связанные с корпоративной политикой.	Регистрация всех изменений, внесенных в информационный контент, классификацию, маркировку и обработку информации. Не для совместного использования информации, если она перед выпуском не была отредактирована по типу «вниз». Информация обычно не отправляется по электронной почте, но может безопасно загружаться на все носители информации, кроме мобильных. Информация хранится в зашифрованном виде. Безопасная печать документов, которая может изыматься только пользователем. Предполагается, что информация требует архивирования/длительного хранения.
Конфиденциальная информация	Высокий	Конфиденциальная	Умеренное влияние на финансовый сектор и затруднения для партнеров. Официальные проверки и меры принудительного характера со стороны контрольно-надзорных органов	Правила обработки информации Документирование процессов Подробные проектные решения Интеллектуальная собственность Отчеты и анализ	Крайне ограниченный доступ к информации минимального числа выделенных сотрудников организации, с передачей этой информации по безопасным каналам для ее ограниченного пользования. Перечни для рассылки всех помеченных страниц. Применяется для всей информации о персонале организации. Дескрипторы, используемые для маркировки основного назначения цели, например, «альфа-проект». Безопасное удаление информации и очистка от нее мобильных носителей
Ограниченная информация	Средний	Ограниченная	Вред и ущерб организации. Воздействие может сказываться на обществе. Продолжительность любого нарушения, которое может быть ограничено по времени и влиянию, зависит только от самой организации	Регистр рисков и планы. Структурная схема организации. Персональная идентификационная информация. Протоколы совещаний. Проекты общедоступных материалов	Обмен информацией между группами по определенным критериям, с подтверждением типа «необходимо знать». Всю информацию, поступающую от партнеров организации, необходимо классифицировать на данном или на более высоком уровне. Документы, помеченные на главной странице Договорное или выполняемое соглашение для всех сотрудников группы. Безопасное физическое хранение информации. Контролируемое уничтожение документации

Окончание таблицы А.1

Классификация	Соответствующий уровень риска	Соответствующая маркировка	Описание воздействия	Примеры	Сущность правил по совместному использованию и обработке информации
Внутренняя информация организации	Низкий	Отсутствие маркировки	Незначительный вред и ущерб для организации, если они выявлены, без какого-либо значимого дискомфорта и при незначительных затратах на восстановление	Справочники, информационные бюллетени. Методики и стандарты. Каталоги. Повестки совещаний	Информация предназначена для общего пользования в организации — отправителе информации. Всю немаркированную и не общедоступную информацию необходимо классифицировать и обрабатывать на данном уровне. Использование информации только на контролируемых рабочих местах. Информация не предназначена для хранения на индивидуальных накопителях. Установка сложных паролей на индивидуальных накопителях
Общедоступная информация	Отсутствует	Отсутствие маркировки	Отсутствие вреда	Маркетинговые материалы. Рекламные объявления. Публичные заявления. Веб-сайты. Публикации	Отсутствие ограничений на совместное использование информации, но может быть или не предназначаться для определенной цели. Информация все еще должна храниться в корпоративных системах и иметь резервные копии. Отсутствие ограничений на передачу информации или других особых требований

Таблица А.2 — Пример схемы обработки информации

Уровень	Высококонфиденциальный	Конфиденциальный	Ограниченный	Внутренний	Общедоступный
Маркировка пресс-релиза для общественности в процессе проектирования					Да
Маркировка при распространении информации				Да	
Маркировка на главной странице			Да		
Маркировка на всех страницах	Да	Да			
Нумерация страниц			Да	Да	Да
Указание текущей страницы из N-страниц	Да	Да			
Нумерация копий и указание их числа	Да	Да			
Официальная регистрация информации	Да				
Степень согласования информации с авторами и пользователями	Высокая	Средняя	Средняя	Низкая	Отсутствует
Разрешение на простое редактирование информации		Да	Да	Да	
Разрешение на редактирование информации только специалистами	Да				
Получение разрешения от первого автора на повторное использование информации	Да	Да			
Маркировка оборудования, используемого для обработки и отображения информации	Да	Да			
Использование сложных паролей	Да	Да	Да	Да	
Использование двухуровневой авторизации для удаленного доступа		Да	Да	Да	
Использование двухуровневой авторизации для полного доступа	Да				
Использование персональных устройств			Да	Да	Да
Использование только корпоративных устройств	Да	Да			
Шифрование данных в состоянии покоя	Да				
Определение местоположения данных с контролем доступа к рабочей площадке и зданию			Да	Да	
Определение местоположения данных с контролем доступа к помещению	Да	Да			
Доступ к данным из заранее согласованных мест	Да	Да			
Безопасное предоставление и хранение данных	Да	Да			

Продолжение таблицы А.2

Уровень	Высококонфиденциальный	Конфиденциальный	Ограниченный	Внутренний	Общедоступный
Отсутствие возможности использования мобильного устройства хранения данных/их носителя	Да				
Определение кодекса взаимоотношений между взаимодействующими сторонами	Да	Да	Да		
Служебная необходимость доступа к информации			Да	Да	
Формальное определение совместного использования информации (кто использует ее и почему)	Да	Да			
Определение уровня протокола совместного использования информации	Нет	Красный	Зеленый	Зеленый	Белый
Распространение информации только по внутренней электронной почте	Да	Да			
Распространение информации по внешней электронной почте			Да	Да	Да
Распространение информации по электронной почте (без возможности ее пересылки)			Да		
Распространение информации с помощью средств оперативной пересылки сообщений и социальных сетевых сервисов					Да
Загрузка информации только из пунктов обмена и др.	Да	Да			
Регистрация цепочки обеспечения сохранности информации	Да				
Использование для обмена информацией предварительно согласованных платформ		Да			
Использование общедоступных платформ для обмена информацией (например, платформы DropBox)			Да	Да	Да
Отсутствие обмена информации в стандартном режиме	Да				
Шифрование информации в процессе ее пересылки	Да				
Использование информационной технологии, непосредственно принадлежащей ее владельцу (или специально выделенной технологии)	Да	Да	Да	Да	
Распечатка информации с выемкой или под контролем оператора	Да	Да			

Окончание таблицы А.2

Уровень	Высококонфиденциальный	Конфиденциальный	Ограниченный	Внутренний	Общедоступный
Информация, распространяемая по факсу и предназначенная для гибкого производственного модуля, который работает по безлюдной технологии					Да
Информация (с известным числом страниц), распространяемая по факсу и предназначенная для оборудования, которое работает под управлением оператора		Да	Да	Да	
Информация, не распространяемая по факсу	Да				
Информация, распространяемая в виде почтовых сообщений			Да	Да	Да
Информация, распространяемая надежным курьером	Да	Да			
Удаление информации, предварительно согласованной с ее владельцем	Да	Да			
Проверка информации для ее архивирования и хранения	Да				
Простое, но контролируемое измельчение документации			Да	Да	
Разрезка/немеханическое измельчение документации	Да	Да			
Периодическая проверка и очистка хранилища информации		Да	Да	Да	Да
Регулярная очистка IT-хранилища	Да				
Стирание информации с ее носителей				Да	Да
Стирание/размагничивание конфиденциальной информации, хранящейся на носителях		Да	Да		
Механическое уничтожение носителей информации	Да				

Приложение Б
(справочное)

Примеры и рекомендации по применению ICMH-системы к информационным ресурсам, представляемым в различных форматах и/или на различных носителях

В.1 Введение

В настоящем приложении приведены примеры и рекомендации по решению конкретных проблем, которые могут возникать при создании информации, последующем ее хранении и использовании в различных форматах и/или на различных носителях:

- использование информационных активов на бумажных носителях;
- электронных документов и цифровых файлов;
- информационных активов, хранящихся на фотопленке и магнитофонной ленте;
- аудио-информационных активов;
- информационных видео-активов;
- просмотр информационных активов на мобильных устройствах;
- использование вспомогательных технологий;
- корпоративных платформ;
- инструментальных средств для работы с базами данных;
- веб-сайтов, сетей Internet и Intranet;
- социальных сетевых сервисов.

В.2 Информационные активы на бумажных носителях

Информационные активы на бумажных носителях необходимо рассматривать с той же точки зрения, что и цифровые активы. Появление методов электронной обработки информации не снижает степень конфиденциальности и/или ценности информации, представляемой на бумажных носителях.

В.2.1 Формирование информационных активов на бумажных носителях

Примечание — Создание нового информационного актива на бумажных носителях обычно требует использования чистых листов, однако допускается и использование листов (или сброшюрованных страниц), уже содержащих какую-либо информацию.

При создании и обработке информационных активов на бумажных носителях следует учитывать:

а) необходимость в классификации и маркировке всех листов с записанной на них информацией (за исключением случаев, когда ICMH-система не допускает применения стандартной классификации и/или немаркированных активов (см. 6.3.5 и 6.3.6);

б) возможность неоднократного формирования и изменения информации относительно исходного листа с соответствующими изменениями уровней конфиденциальности информации; необходимо следить за тем, чтобы любые копии, классифицированные как нуждающиеся в защите, надежно обрабатывались в соответствии с требованиями, предъявляемыми к классификации и маркировке подобных копий (см. 6.5);

в) возможность введения новой информации в документ (который ранее не считался нуждающимся в какой-либо специальной защите), способной приводить к появлению документа, нуждающегося в защите, что потребует его соответствующей классификации, маркировки и обработки.

Примечание — Например, повестка дня совещания может обладать низкой классификационной маркировкой, однако при введении в нее примечаний эта повестка будет изменяться или расширяться, становясь информационным активом, которому потребуется дополнительная защита при обработке, отмечаемая маркировкой более высокого уровня;

г) если для записи документа на бумажном носителе используется ручка или карандаш, то, возможно, отпечаток документа (фактически — его копия) может оставаться на любых нижних и/или верхних бумажных листах, что потребует их соответствующей обработки.

Организация могла бы рассмотреть вопрос о предоставлении своим сотрудникам блокнотов и т. п. с предварительно промаркированными классификациями, чтобы акцентировать внимание этих работников на требуемых аспектах обращения, однако организации следует рассмотреть и практические аспекты этого предложения, чтобы выгоды можно было сопоставлять с эксплуатационными расходами.

Примечание — Например, ношение нескольких блокнотов может оказаться неудобным и обременительным, особенно в тех случаях, когда связанную с конкретными проектами информацию необходимо документировать по отдельности (что может маркироваться соответствующим дескриптором или взаимозависимостью (см. 6.3.7)) и в дальнейшем осложнять процедуру обработки этих блокнотов за счет необходимости их сбора и хранения.

В.2.2 Копирование и воспроизведение информационных активов

Документы на бумажных носителях можно копировать несколькими способами. При этом необходимо учитывать возможность:

а) того, что фотографии документов могут делать либо лица, работающие над этими документами (которые, возможно, желают получить неофициальную копию), либо лица (например, журналисты), которые могут быть заинтересованы в содержании этого документа;

б) использования частных ручных сканирующих устройств, которые способны сканировать текстовые документы как изображения или (при наличии программного обеспечения для оптического распознавания символов) как текста, воспринимаемого текстовым процессором;

в) использования копировальных аппаратов, когда:

- документы могут копироваться не полностью, например, без копируемых классификационных знаков или с исключением определенных страниц,
- копируемые страницы документа могут застревать в копировальном аппарате и неосмотрительно отбрасываться,
- используются устройства с функциями хранения документов, когда их получатель может не знать об отправке документа, в результате чего он будет оставаться в этих устройствах;

г) использования принтеров, которые могут находиться в незащищенных местах, например, в домах сотрудников организации или в государственных центрах оказания печатных услуг, где могут отсутствовать необходимые технологии уничтожения документации.

В.2.3 Использование, обмен и передача информационных активов, выполненных на бумажных носителях

Вопрос наличия важной информации на видных местах бумажных носителей, например, на рабочем столе (в особенности — в тех случаях, когда ими активно не пользуются), должен решаться организацией, создающей и использующей эти активы (в рамках собственной ICMH-системы).

Схема обработки информации в организации должна охватывать все состояния и этапы жизненного цикла информационного актива на бумажных носителях (см., в частности, 6.5.7, 6.5.10—6.5.12).

В.3 Электронные документы и цифровые файлы

В.3.1 Формирование цифровых информационных активов

Практически во всех случаях процесс создания цифрового информационного актива начинается с выбора конкретного программного обеспечения. На каком-либо этапе этого процесса необходимо создавать и сохранять новый файл, соответствующий ICMH-системе (см. 6.5.2—6.5.5).

В.3.2 Использование цифровых информационных активов

На опыт пользователя цифровых информационных активов влияет использование им определенных устройств и программного обеспечения (например, размер экрана дисплея или тип/разрешение веб-браузера, которые влияют на условия наблюдения пользователя). По этой причине организация должна проанализировать, будет ли выбранный дизайн маркировки адекватным при любых обстоятельствах. В частности, организации следует позаботиться о том, чтобы:

а) пользователи, которые получают доступ к цифровым файлам с помощью небольших экранов (например, на мобильных телефонах), смогли видеть маркировку соответствующего информационного актива;

б) пользователи, которые предпочитают использовать общепринятые приемы повышения наглядности информации (например, изменение размера/цвета шрифта или размера изображения), всегда смогли бы видеть классификационную маркировку, не прибегая, например, к прокрутке экрана;

в) в тех случаях, когда имеется возможность изменять параметры настройки, пользователи не смогли бы отказаться от отображения меток.

Поскольку цифровыми файлами часто легко манипулировать (и, следовательно, существует опасность удаления маркировки, незаметного изменения информации или способа обращения к ней с помощью классификации, маркировки и обработки), следует рассмотреть следующие моменты:

1) Некоторые форматы файлов (например, PDF-файлы) можно использовать для сохранения информации в требуемой форме. Многие типы файлов могут предохраняться от несанкционированного редактирования текста.

2) Цифровые файлы могут легко и незаметно изменяться (что невозможно с документами на бумажных носителях), например, легко могут изменяться даты, отправитель или содержимое электронного письма; по этой причине может стать важным архивирование информации с надлежащей защитой исходного документа от несанкционированного доступа (см. 6.5.8, 6.5.9 и 6.5.11 и 6.5.12).

3) Часто можно «вырезать и вставлять» контент из документа, даже если он был защищен от редактирования; при определенных обстоятельствах может становиться целесообразным рассмотрение вопроса о дополнительной маркировке конфиденциального контента (см. 6.4.2 и 6.5.3—6.5.5).

4) Размещение меток на верхних и нижних колонтитулах (при использовании стандартных форматов файлов, таких как Word и PowerPoint), является потенциально проблематичным, поскольку изменение шаблона может приводить к потере этих колонтитулов.

5) Знаки маркировки, помещенные в метаданные, скорее всего не будут заметны для пользователей соответствующего документа.

В.4 Информационные активы на фотопленке и магнитофонной ленте

В.4.1 Формирование аудио- и видеоинформационных активов

Примечание — Большинство цифровых информационных активов представляют собой документы, имеющие свое начало и окончание (т. е. имеющие конечный объем контента), которые в большинстве случаев можно обрабатывать так же, как и документы на бумажных носителях — т. е. с аналогичной маркировкой и в соответствии с принятыми правилами маркировки (см. 6.4.1). Тем не менее, не все цифровые файлы можно представлять в постраничном формате, поскольку часть из этих форматов представляют собой аудио-, видео- или 3D-файлы.

Аудио- и видеоинформационные активы (как оцифрованные, так и зарегистрированные на магнитофонной ленте или фотопленке) обычно относительно легко поддаются классификации по темам/информационному контенту, а также по пользователям, однако, как правило, за ними сложнее закрепить маркировку.

В дополнение к требованиям, указанным в 6.4, организация в своей ICMH-системе может использовать следующие методы маркировки аудио- и видеозаписей:

а) маркировка носителей информации или контента информационного актива.

Примечание — Можно, например, применять маркировку кассеты, содержащей магнитофонную ленту или фотопленку;

б) введение маркировки перед началом записи, чтобы перед использованием информационного актива ее можно было бы прослушивать или просматривать;

в) введение маркировки в конце записи;

г) для информационных аудиоактивов — введение во время их записи определенного звукового сигнала (уникального в принятой классификации), хотя это, возможно, способно повлиять на четкость восприятия звуков и распознавании всех их нюансов. Последнее означает, что после записи клипа информация о классификации все еще будет оставаться доступной для всех тех, кто понимает назначение этого звукового сигнала, пройдя обучение и получив соответствующую информацию (см. 7.4);

д) для информационных видеоактивов — использование заголовков, содержащих маркировку по всему этому активу, хотя следует позаботиться и о том, чтобы этот заголовок не мешал другой содержащейся в заголовках информации, например, закадровым титрам;

е) использование стандартной классификации (см. 6.3.5), без маркировки отдельного информационного ресурса (см. 6.3.6).

Примечание — Например, все записи телефонных звонков, поступающих в тот или иной кол-центр, будут иметь одну и ту же классификацию и соответствующие процедуры обработки;

ж) маркировка информационного актива в метаданных, связанных с этим активом, хотя после введения маркировки следует быть осторожным, поскольку она может быть приемлемой только тогда, когда воспроизведение аудио-информации будет находиться в контролируемой системе, способной распознавать и воспринимать эти метаданные.

Примечание — Некоторые видеоактивы, такие как, например, магнитофонные записи, полученные с помощью ведомственных систем скрытого видеонаблюдения, скорее всего, будут подпадать под законодательство о защите конфиденциальности данных и, следовательно, потребуют соответствующего уровня классификации данных.

В.4.2 Совместное использование и передача информационных активов, содержащихся на магнитофонных лентах и фотопленках

В своей ICMH-системе организации могут выбирать для информационных активов, хранящихся на магнитофонных лентах и фотопленках и классифицированной на определенных уровнях, конкретные процедуры обработки, которые затем будут заспециализированы для определенных типов носителей информации (см. 6.5.10) и учитывать их физические характеристики. Как и в случае любых других информационных активов, организации должны принимать решение о том, должны ли те подобные информационные активы выходить за пределы организаций.

В.4.3 Хранение информационных активов, содержащихся на магнитофонных лентах и фотопленках

Требования к хранению информационных активов, хранящихся на магнитофонных лентах и фотопленках, должны быть аналогичны предъявляемым к информационным активам на бумажных носителях (см. 6.5.7).

В.5 Речевые информационные активы

В.5.1 Непосредственное речевое общение

Информацию, которую можно классифицировать как конфиденциальную (т. е. содержащую важные сведения), необходимо защищать, когда и где бы она ни подвергалась опасности, в том числе — при ее оглашении (в особенности, в сфере государственной деятельности). Любого, обсуждающего конфиденциальную информацию в общественном месте, можно прослушивать, записывать или даже воспринимать его речь по артикуляции губ.

Организации должны включать в свою схему обработки информации способ классификации речевой информации при обмене ей между участниками обмена, а также возможные ограничения на использование этой совместно используемой информации. Сотрудники организации должны предупреждаться о рисках подслушивания конфиденциальной информации.

В.5.2 Коммуникационные услуги

Речевое общение, не происходящее при личном контакте и использующее телекоммуникационные технологии, подвержено дополнительным рискам. Разговоры по стационарным и мобильным телефонам могут перехватываться и записываться. Аналогично, могут оказаться незащищенными и IP-телефония (VOIP), Skype и веб-конференц-связь. Для речевого общения на определенных уровнях классификации организации могут устанавливать в качестве обязательных средства защищенной телефонии.

Организации должны решать эти проблемы особым образом посредством схемы обработки информации (см. 6.5) и проводить специальную подготовку для тех своих сотрудников, чьи функциональные обязанности наиболее подвержены данным рискам (см. 7.4).

В.6 Информационные видеоактивы

Многие из аспектов, которые обсуждались в отношении регистрации информации на бумажных и цифровых носителях, а также на магнитофонных лентах и фотопленках, в равной степени относятся и к информационным видео-активам.

Организация должна обеспечить четкое определение правил первоначального формирования изображений в схеме обработки информации, которые должны охватывать такие аспекты, как разрешающая способность, форматы, исходные атрибуты (дата, время и т. п.) и носители информации, на которых изображения могут храниться.

Кроме того, если изображения поступают от сторонних организаций, то необходимо обеспечивать как контроль достоверности источников, правомочных передавать эти изображения, так и контроль достоверности самих изображений (отсутствие их редактирования/манипулирования), а также наиболее приемлемые для организации изображения по их назначению и качеству.

Использование изображений также требует контроля неизменности их атрибутов. Организация должна обеспечивать наличие правил репликации изображений в схеме обработки информации, например, соблюдение производственных стандартов/форматов классификаций и предотвращение паразитных искажений или неправильного обращения.

Примечание — Организации также может потребоваться предоставление доказательств подлинности этих атрибутов, например, даты и времени их первоначального выбора.

При обработке изображений, например, отдельно от документа, в котором оно содержится, схема обработки информации в организации должна определять наличие на ней маркировки, например, водяных знаков.

В.7 Просмотр информационных активов на мобильных устройствах

ICMH-система должна обеспечивать просмотр информационных активов, хранящихся на мобильных устройствах, и определять требования к размерам используемого экрана и возможности просмотра веб-сайтов при отображении или репликации информации (см. 6.5.8). Организация может устанавливать (в рамках собственной схемы обработки информационных активов) в качестве обязательных требований к этим классифицированным на определенных уровнях активам запрет на их хранение или просмотр на мобильных устройствах из-за невозможности отображения их классификационной маркировки.

В.8 Использование вспомогательных технологий

Организация должна устанавливать оптимальный баланс между требованиями к ее ICMH-системе и потенциально противоречивыми требованиями к поддержке сотрудников организации и защите информации.

Программное обеспечение, осуществляющее надежный синтез контента информационного актива, должно содержать описание его классификации и маркировки.

Представление информации в виде шрифта Брайля также должно осуществляться аналогичным образом, а увеличение размеров экрана и/или символов не должно происходить за счет отображения маркировки информационных активов.

В.9 Использование корпоративных платформ

ICMH-система должна определять, какие корпоративные платформы организации можно считать государственными, а какие платформы - частными, а также какие из платформ можно считать безопасными, например, с точки зрения обладания правами доступа к ним (см. 6.5.6, 6.5.10 и 6.5.12).

Если корпоративная платформа является частной, то возможность ее использования в ICMH-системе должна быть четко оговорена, однако если эта платформа считается общедоступной, то следует принимать в расчет ограничения по ее применению, связанные с использованием социальных сетевых сервисов (см. В.12). Очевидно, что корпоративные платформы, предназначенные для безопасного обмена информацией, должны конфигурироваться с учетом ограничений, установленных в ICMH-системе для обеспечения их эквивалентности с таковыми для выявленных сторонних организаций (см. 6.3.3).

В тех случаях, когда эти платформы допускают совместное редактирование информационных активов, ICMH-система должна определить, какой сотрудник организации правомочен изменять классификацию (см. 6.5.2—6.5.5).

Примечание — Например, для эффективного редактирования информационных активов этот пересмотр/изменение может выполнять последний из сотрудников организации, получивший доступ к ним в процессе их совместного редактирования, или же любой владелец этих активов сразу же после завершения процедуры редактирования. В любом случае владелец информационных активов будет нести ответственность за выполнение поставленной задачи.

В.10 Средства для работы с базами данных

В.10.1 Доступ к базам данных и их использование

Настоящий стандарт рассматривает информационные активы как «данные, обладающие определенным содержанием (смыслом)», и поэтому не принимает во внимание те данные, которые хранятся в базе данных перед их последующей обработкой и формированием информации, которую следует затем подвергать обработке или совместному использованию. Следовательно, данный пункт стандарта относится к информации, извлекаемой из базы данных для создания информационных активов.

Для наиболее эффективного использования ICMH-системы необходимо принять конкретные решения относительно баз данных в процессе:

а) доступа к стандартной базе данных;

б) извлечения информации из специальной базы данных;

в) работы с базами данных.

В.10.2 Доступ к стандартным базам данных

Большинство систем хранения данных работают на программном обеспечении под конкретные операционные системы, которые организация использует для обеспечения своей деятельности, например, поддержки пакетов программ бухгалтерского учета, системы управления взаимоотношениями с клиентами (CRM) и т. п. Эти системы обычно обладают элементами управления доступом пользователей (см. 6.5.6). В тех случаях, когда существует возможность доступа к основной системе баз данных, она также должна увязываться с контролем доступа.

Обычно пользователи взаимодействуют с этими системами с помощью предварительно заданных экранов или отчетной документации, которые являются частью этих систем (в особенности, если они являются частью имеющихся на рынке продуктов), и вряд ли будут содержать по умолчанию схемы классификации, маркировки и обработки информации, определенные в ICMH-системе. Всегда, когда это возможно, эти экраны и документацию необходимо корректировать с учетом характеристик ICMH-системы; когда же это невозможно, ICMH-систему следует информировать об альтернативных мерах, которые пользователи должны предпринять для управления связанными с ними рисками (см. 7.3).

В.10.3 Извлечение информации из специализированной базы данных

Ситуация, описанная в В.10.2, может еще более усложняться в тех случаях, когда информация извлекается непосредственно из базы данных, минуя стандартизованный экран и отчетную документацию. Например, администраторы баз данных могут запрашивать базу данных для формирования специальных перечней информации, с последующим их предоставлением в отчеты на бумажном носителе или в документацию, выполняемую в каком-либо удобочитаемом цифровом формате, например, в виде электронных таблиц. В процессе извлечения информации из базы данных сотрудником организации (или же сотрудником, запрашивающим эту информацию после ее получения) сформированный информационный актив следует сразу же классифицировать, маркировать и обрабатывать в соответствии с требованиями ICMH-системы (см. также 6.5.3—6.5.5).

В.10.4 Работа с базами данных

Организация должна понимать, что системы управления несколькими базами данных, которые объединяют многочисленные базы данных, а также хранилища данных и программные решения для больших данных, могут содержать огромные объемы информации в табличном формате.

Из любой таблицы, к которой может обеспечиваться доступ, может извлекаться информация с очень низким уровнем конфиденциальности, однако при объединении этих таблиц в отчетной документации или же просто при их совместном сохранении, они обычно организуются в массивы более высокого (часто — значительно более высокого) уровня классификации (см. 6.3.2 и 6.5.5). В таблице В.1 показано, как объединение двух таблиц с данными способно менять их классификацию.

Таблица В.1 — Пример работы с данными

Таблица А		Таблица В	
Имя	Идентификационные данные	Идентификационные данные	Реквизиты кредитных карточек
Антон	12001	12001	1234-5678-1212
Елена	13222	13222	9876-5432-4545

При этом сотрудники организации в соответствии с требованиями ICMH-системы должны давать собственную оценку классификации уже в процессе получения информации, а не полагаться на существующие системы или маркировку информации как окончательную.

В.11 Использование веб-сайтов, сетей Internet и Intranet

В.11.1 Использование веб-сайтов

ICMH-система должна быть применимой к любым веб-сайтам, и поскольку они обладают нелинейной структурой и содержат группы информационных активов, то следует рассматривать вопрос о реализации связанных с ними ICMH-схем и, в частности, соответствующих схем маркировки (см. 6.4 и 6.5). Трудности при этом могут быть связаны с тем, что:

- пользователи имеют широкий выбор способов отображения информации на дисплее;
- пользователи могут выбирать лишь фрагменты веб-страницы для их просмотра или совместного использования;
- пользователи могут не видеть информацию, если она является фрагментом страницы, но не выводится на экран;
- веб-страницы могут формироваться либо динамически («на лету»), либо индивидуально — для конкретных пользователей;
- информация на экране на самом деле может не отражать метаданные, html-коды и т. п.;
- различные браузеры и операционные системы могут по-разному отображать информацию.

Все приведенные выше примеры свидетельствуют о возможности доступа к гораздо большему объему информации, чем при первичном анализе, который предусматривается ICMH-системой.

В.11.2 Использование сети Internet

В большинстве случаев использование сети Internet следует надлежащим образом рассматривать с точки зрения требований к ICMH-системе, описанных в настоящем стандарте. Протоколы, используемые при работе в сети Internet (например, FTP, WebDAV и т. п.), представляют собой просто способы обмена информацией и информационными активами.

Электронную почту следует рассматривать главным образом как способ обмена информационными активами, причем ICMH-система должна определять методы маркировки сообщений (писем) в соответствии с их эквивалентной классификацией (например, в адресной строке).

В.11.3 Использование сетей Intranet

В случае использования внутрикорпоративных сетей Intranet (в дополнение к рекомендациям по использованию общедоступных веб-сайтов) информационные активы должны маркироваться в соответствии с требованиями ICMH-системы и условиями доступа к этим активам (см. 6.5.6 и 6.5.12).

Каждый действующий экран должен маркироваться в соответствии с максимально высоким уровнем классификации (и с соответствующим уровнем маркировки) для всех представленных информационных активов (или их фрагментов) (см. также 6.5.3—6.5.5).

В.12 Использование социальных сетевых сервисов

По своей природе платформы для социальных сетевых сервисов являются «открытыми» платформами, так что размещаемую на них информацию можно однократно и многократно использовать с помощью методов, которые могут оказаться неприемлемыми для той или иной организации, а информация сможет оставаться в общем пользовании неограниченно долго.

Кроме того, организация не может служить источником всей информации, размещаемой в социальных сетях, поэтому она должна четко понимать пределы разрешенных ей способов обработки информации (например, выдачи повторного твита), размещаемой другими организациями.

В последнем случае организация должна:

а) с помощью ICMH-концепции (см. 5.4) разъяснять своим сотрудникам, какую информацию можно (или не допускается) размещать в социальных сетях, а также меры дисциплинарной ответственности, которые будут применяться к ним при нарушении концепции;

б) предоставлять своим сотрудникам возможность обучения и получения информации в соответствии с требованиями концепции (см. 7.3);

в) подвергать информацию аудиту и гарантировать достоверность информации при размещении ее в социальных сетевых сервисах (см. 9.3), а также и во всех иных средствах массовой информации в форматах, рассмотренных в настоящем приложении.

УДК 658:330.341.1:001:330.111.4:0 ОКС 01.140.20; 03.100.99

Ключевые слова: менеджмент знаний, инновационный менеджмент, система менеджмента знаний, сбор информации, классификация информации, маркировка информации, обработка информации

БЗ 10—2019/112

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.09.2019. Подписано в печать 09.10.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,18.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru