ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27050-1— 2019

Информационные технологии. Методы обеспечения безопасности

ВЫЯВЛЕНИЕ И РАСКРЫТИЕ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

Часть 1

Обзор и концепции

(ISO/IEC 27050-1:2016, IDT)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» совместно с Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 459 «Информационная поддержка жизненного цикла изделий»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 октября 2019 г. № 824-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27050-1:2016 «Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации. Часть 1. Обзор и концепции» (ISO/IEC 27050-1:2016 «Information technology — Security techniques — Electronic discovery — Part 1: Overview and concepts», IDT).

5 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 настоящем стандарте представлен обзор темы электронного раскрытия (э-раскрытия) и описана соответствующая терминология, концепции и процессы, которые предназначены для использования в других частях комплекса стандартов ИСО/МЭК 27050.

Электронное раскрытие (э-раскрытие — electronic discovery) часто служит движущей силой как при проведении расследований, так и в ходе работы по сбору и обработке доказательств (ИСО/МЭК 27037). Кроме того, конфиденциальность и критичность данных иногда делают необходимым применение мер защиты, таких как обеспечение безопасности при хранении, для предотвращения несанкционированного доступа к данным (ИСО/МЭК 27040).

Настоящий стандарт не является справочным или нормативным документом в том, что касается законодательно-нормативных требований по безопасности. Хотя в нем подчеркивается важность влияния требований такого рода, он не может сформулировать их конкретно, поскольку они зависят от страны, вида деловой деятельности и т. д.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии. Методы обеспечения безопасности

ВЫЯВЛЕНИЕ И РАСКРЫТИЕ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

Часть 1

Обзор и концепции

Information technology. Security techniques. Electronic discovery.
Part 1. Overview and concepts

Дата введения — 2020—10—01

1 Область применения

Электронное раскрытие (э-раскрытие) представляет собой процесс выявления и представления соответствующей сохраняемой в электронном виде информации (Electronically Stored Information, ESI) или данных одной или несколькими сторонами, участвующими в расследовании или судебном разбирательстве либо в аналогичных процедурах.

Настоящий стандарт содержит общее описание э-раскрытия. Кроме того, в нем определены соответствующие термины и описаны понятия и концепции, включая такие (но не ограничиваясь ими) как выявление, сбор, обработка, проверка, анализ и представление сохраняемой в электронном виде информации. В настоящем стандарте также перечислены другие имеющие отношение к данной теме стандарты (например, ИСО/МЭК 27037) и показано, как они связаны с деятельностью по э-раскрытию и влияют на нее.

Настоящий стандарт будет полезен как для технического, так и для нетехнического персонала, вовлеченного в те или иные действия по э-раскрытию. Стандарт может использоваться в той мере, в какой он не противоречит законам и нормативным актам соответствующей юрисдикции, поэтому необходимо позаботиться об обеспечении соответствия действующим законодательно-нормативным требованиям.

2 Нормативные ссылки

Настоящий стандарт не содержит нормативных ссылок.

3 Термины и определения

В настоящем стандарте применены термины и определения по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для применения в области стандартизации, расположенные по следующим адресам.

- база МЭК «Electropedia»: доступна по адресу http://www.electropedia.org/;
- база ИСО «Online browsing platform»: доступна по адресу http://www.iso.org.obp.

3.1 **непрерывная последовательность ответственного хранения** (chain of custody). Доказуемая история владения, перемещения, обработки и местоположения материалов, от одной точки во времени до другой.

Издание официальное

3.2 **хранитель** (custodian): Лицо или организация, являющееся ответственным хранителем, контролирующее либо обладающее *сохраняемой в электронном виде информацией* (3.9).

3.3 **утечка данных** (data breach): Компрометация безопасности, приводящая к неумышленному или незаконному уничтожению, утрате, изменению, несанкционированному раскрытию или доступу к защищаемым данным, которые передаются, *хранятся* (3.26) или обрабатываются иным образом.

[ИСО/МЭК 27040:2015, статья 3.7]

3.4 **раскрытие** (discovery): Процесс, при помощи которого каждая из сторон по делу получает относящуюся к рассматриваемому вопросу информацию, имеющуюся у другой стороны либо у лица, не являющегося стороной по делу.

Примечания

1 Процесс *раскрытия* не ограничивается раскрытием информации противоборствующими в спорах сторонами и применяется более широко.

2 Процесс *раскрытия* также включает в себя раскрытие противоборствующими сторонами физических документов, *сохраняемой в электронном виде информации* (3.9) и материальных объектов.

3 В некоторых юрисдикциях англоязычные термины disclosure и discovery используются как синонимы.

3.5 **решение судьбы документов** (уничтожение/передача документов) (disposition): Совокупность процессов, связанных с выполнением решений относительно сроков хранения документов и их последующего уничтожения либо передачи, зафиксированных в соответствующих *нормативно-правовых документах* (3.6) или в иных инструментах.

[ИСО 15489-1:2016, статья 3.8]

3.6 **нормативно-правовой документ, регламентирующий уничтожение/передачу документов** (disposition authority): Инструмент, определяющий действия по уничтожению/передаче, авторизованные для определенных видов документов.

[ИСО 15489-1:2016, статья 3.9]

3.7 **электронный архив** (electronic archive): Хранилище для долговременного хранения *сохраняемой в электронном виде информации* (3.9)

Примечания

1 Электронные архивы могут работать как в онлайн-режиме и, следовательно, быть доступными; так и в автономном режиме, не являясь в этом случае легкодоступными.

2 Системы резервного копирования (например, на магнитных лентах, виртуальных лентах и т.п.) не предназначены для использования в качестве электронных архивов и представляют собой системы защиты данных (т.е. это механизмы восстановления данных для целей возобновления деловой деятельности после катастроф и для обеспечения непрерывности деловой деятельности).

3.8 **электронное раскрытие;** э-раскрытие (electronic discovery): Процесс *раскрытия* (3.4), включающий выявление, обеспечение сохранности, сбор, обработку, проверку, анализ и представление *сохраняемой в электронном виде информации* (3.9).

Примечание — Хотя электронное раскрытие часто рассматривается как элемент процессуальных действий, его использование не ограничивается сферой права.

3.9 **сохраняемая в электронном виде информация** (Electronically Stored Information, ESI): Данные или информация любого вида и из любого источника, свидетельством существования которых в определенный момент времени является их сохранение в/на каком-либо электронном носителе информации.

Примечания

1 Понятие «сохраняемой в электронном виде информации» охватывает традиционную электронную почту, докладные записки, письма, электронные таблицы, базы данных, офисные документы, презентации и иные электронные форматы, обычно встречающиеся на компьютере. Оно также охватывает системные, прикладные и ассоциированные с файлами *метаданные* (3.19), такие как отметки времени, история изменений, тип файла и т.д.

2 Одним из видов электронных носителей информации (но не единственно возможным) являются запоминающие устройства и элементы.

[ИСО/МЭК 27040:2015, статья 3.16]

3.10 **анализ сохраняемой в электронном виде информации** (ESI analysis): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется оценке со-

держания и контекста *сохраняемой в электронном виде информации* (3.9) с целью выявления фактов, взаимосвязей, ключевых закономерностей и иных особенностей, которые способствуют лучшему пониманию располагаемой *сохраняемой в электронном виде информации* (3.9).

Примечание — Содержание и контекст могут включать основные закономерности, темы, сведения о людях и обсуждавшихся вопросах.

3.11 **сбор сохраняемой в электронном виде информации** (ESI collection): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется сбору *сохраняемой в электронном виде информации* (3.9) и иных относящихся к предмету раскрытия материалов.

3.12 **выявление сохраняемой в электронном виде информации** (ESI identification): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется локализации потенциальных источников и критериям отбора потенциально относящейся к предмету раскрытия *сохраняемой в электронном виде информации* (3.9).

3.13 **обеспечение сохранности сохраняемой в электронном виде информации (**ESI preservation): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется поддержанию *сохраняемой в электронном виде информации* (3.9) в ее первоначальном или текущем состоянии.

Примечание — В некоторых ситуациях и/или юрисдикциях могут существовать требования по предотвращению преднамеренного уничтожения или искажения (3.24) *сохраняемой в электронном виде информации* (3.9).

3.14 **обработка сохраняемой в электронном виде информации** (ESI processing): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется извлечению *сохраняемой в электронном виде информации* (3.9) и, при необходимости, преобразованию ее в формы, более пригодные для *проверки* (3.16) и *анализа* (3.10).

3.15 **представление сохраняемой в электронном виде информации** (ESI production): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется передаче либо открытию доступа запрашивающей стороне к *сохраняемой в электронном виде информации* (3.9).

Примечания

1 Представление *сохраняемой в электронном виде информации* (3.9) также может включать в себя ее передачу в подходящих формах и с использованием соответствующих механизмов доставки.

2 Представление сохраняемой в электронном виде информации может осуществляться по запросу любого лица или организации.

3.16 **проверка сохраняемой в электронном виде информации** (ESI review): Составная часть процесса *электронного раскрытия* (3.8), в рамках которой основное внимание уделяется отсеву части *сохраняемой в электронном виде информации* (3.9) на основе определенных критериев.

Примечание — В некоторых ситуациях и/или юрисдикциях *сохраняемая в электронном виде информация* (3.9), которая признается привилегированной, может не предоставляться запрашивающей стороне.

3.17 **расследование** (investigation): Систематический и/или формализованный процесс поиска, сбора и изучения фактов и материалов, связанных с соответствующим вопросом.

Примечание — Материалы могут быть представлены в форме аналоговых документов или же в форме *сохраняемой в электронном виде информации* (3.9).

3.18 **запрет на уничтожение** (legal hold): Процесс приостановления обычных процессов *уничтожения/передачи* (3.5) *и/или обработки документов* и *сохраняемой в электронном виде информации* (3.9) ввиду идущего или ожидаемого судебного разбирательства, аудита, проводимого государственными органами расследования и т. п.

Примечание — Выпущенное распоряжение или уведомление, вводящее запрет на уничтожение, может называться «приостановлением уничтожения» (hold), «распоряжением об обеспечении сохранности» (preservation order), «уведомлением об обеспечении сохранности» (preservation notice), «приказом о приостановлении уничтожения» (suspension order, hold order), «уведомлением о замораживании» (freeze notice) или «уведомлением о приостановлении уничтожения» (hold notice).

3.19 **метаданные** (metadata): Данные, определяющие и описывающие другие данные.

[ИСО/МЭК 11179-1:2015, статья 3.2.16]

3.20 **энергонезависимое хранилище данных** (non-volatile storage): *Хранилище данных* (3.25), содержимое которого сохраняется даже после отключения питания.

[ИСО/МЭК 27040:2015, статья 3.30]

3.21 **файловый формат раскрытия данных** (production file format): Организация и способ представления данных и *метаданных* (3.19), передаваемых запрашивающей стороне.

3.22 **происхождение** (provenance): Сведения, документирующие источник *сохраняемой в электронном виде информации* (3.9), все изменения, имевшие место с момента ее создания, а также ее хранителей начиная с момента ее создания.

3.23 **очистка носителей информации** (sanitization): Процесс удаления информации с носителей таким образом, чтобы восстановление данных было невозможным при заданном уровне усилий.

[ИСО/МЭК 27040:2015, статья 3.38, модифицированное]

Примечание — Для очистки носителей информации могут быть использованы такие действия, как стирание с помощью общедоступных средств, надежное удаление с помощью специализированных средств и инструментов (purge) и физическое уничтожение носителей.

3.24 **преднамеренная порча доказательств** (spoliation): Действия либо допущение действий по внесению изменений, либо уничтожению *сохраняемой в электронном виде информации* (3.9) при наличии требования обеспечить ее целостность и сохранность.

Примечание — Порча доказательств может выражаться в уничтожении, искажении или изменении *сохраняемой в электронном виде информации* (3.9) или ассоциированных с ней *метаданных* (3.19), а также в потере доступности *сохраняемой в электронном виде информации* (3.9) (например, из-за отсутствия доступа к ключу дешифрования для зашифрованной информации; утраты носителя информации, находящегося под контролем третьей стороны, и т. д.).

3.25 **хранилище данных** (storage): Устройство, функция или сервис, поддерживающие ввод и извлечение данных.

[ИСО/МЭК 27040:2015, статья 3.43]

3.26 **сохранение** (store): запись данных в *энергозависимое* (3.27) либо в *энергонезависимое* (3.20) *хранилище данных*.

[ИСО/МЭК 27040:2015, статья 3.50]

3.27 **энергозависимое хранилище данных** (volatile storage): *Хранилище данных* (3.25), содержимое которого не сохраняется после отключения питания.

[ИСО/МЭК 27040:2015, статья 3.53]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

CD — компакт-диск (compact disc);

DVD — цифровой многоцелевой диск (digital versatile disc);

EDMS — электронная система управления контентом (electronic document management system);

ERMS — электронная система управления документами (electronic records management system);

ИКТ — информационно-коммуникационные технологии;

NAS — сетевая система хранения данных (network attached storage);

OCR — оптическое распознавание символов (optical character recognition);

ПДн — персональные данные;

ОЗУ — оперативное запоминающее устройство.

5 Общая структура и содержание частей стандарта ИСО/МЭК 27050

5.1 Назначение и структура

Стандарт ИСО/МЭК 27050 (все части) содержит требования и рекомендации в отношении процесса выявления и представления (раскрытия) имеющей отношение к делу сохраняемой в электронном виде информации или данных одной или несколькими сторонами, участвующими в расследовании или судебном разбирательстве либо в аналогичных процедурах. На рисунке 1 схематически показана архитектура стандарта ИСО/МЭК 27050 в целом.

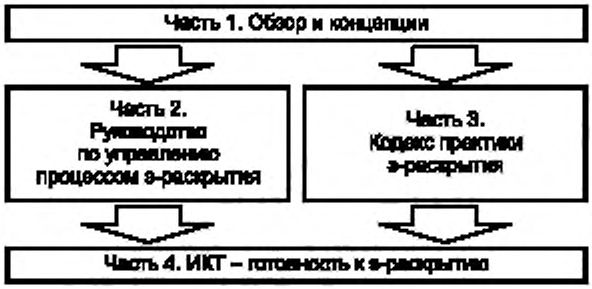

Рисунок 1 — Архитектура стандарта ИСО/МЭК 27050

5.2 Содержание части 1 стандарта ИСО/МЭК 27050: Обзор и концепции

В части 1 стандарта ИСО/МЭК 27050 содержится общее описание э-раскрытия, вводятся соответствующие терминология, понятия и процессы. Данный документ является справочным.

5.3 Содержание части 2 стандарта ИСО/МЭК 27050: Руководство по управлению процессом э-раскрытия

В части 2 стандарта ИСО/МЭК 27050 рассматривается, каким образом лица, занимающие в организации высшие руководящие посты, могут выявлять связанные с э-раскрытием риски и становиться их владельцами, устанавливать политику в отношении э-раскрытия и обеспечивать соответствие внешним и внутренним требованиям в отношении э-раскрытия.

5.4 Содержание части 3 стандарта ИСО/МЭК 27050: Кодекс практики э-раскрытия

В части 3 стандарта ИСО/МЭК 27050 рассматриваются по отдельности основные элементы процесса э-раскрытия (выявление, обеспечение сохранности, сбор, обработка, проверка, анализ и представление сохраняемой в электронном виде информации). Для каждого элемента процесса э-раскрытия указаны (i) цели, (ii) соображения по предотвращению неудач и (iii) конкретные требования и рекомендации по обеспечению соответствия стандарту ИСО/МЭК 27050 в целом.

5.5 Содержание части 4 стандарта ИСО/МЭК 27050: ИКТ-готовность к э-раскрытию

В части 4 стандарта ИСО/МЭК 27050 содержатся рекомендации относительно того, каким образом организация может лучше подготовиться к решению задач э-раскрытия с точки зрения как технологий, так и процессов.

6 Общее представление об э-раскрытии

6.1 Общие положения

Э-раскрытие приобретает все большее значение как внутри организаций, так и в правовых системах ряда юрисдикций. Ожидается, что эта тенденция будет продолжаться по мере того, как все чаще электронные документы и информация (или сохраняемая в электронном виде информация) создаются, модифицируются, обрабатываются, используются и в конечном итоге уничтожаются, никогда не принимая какой-либо физической формы (например, формы печатного документа).

То, что предпочтительным способом представления информации становится ее представление в форме «сохраняемой в электронном виде информации», создает новые проблемы, связанные с локализацией такого рода информации, обработкой огромного количества данных, обеспечением ее сохранности и отслеживанием сроков хранения, обеспечением аутентичности, целостности и конфиденциальности данных, очистки данных или носителей информации и т. д.

Потребности в части э-раскрытия и способы реагирования различаются в зависимости от ситуации, однако неспособность надлежащим образом провести процесс э-раскрытия с учетом особенностей конкретной ситуации может привести к необходимости выполнить работу повторно, к ненужным

затратам, возможным санкциям и к материальной и правовой ответственности в соответствии с законодательством (legal liability).

Стандарт ИСО/МЭК 27050 (все части) решает эти проблемы путем.

- продвижения единого подхода, понимания и языка для э-раскрытия;
- поощрения практичного и экономически эффективного раскрытия сохраняемой в электронном виде информации теми, кому поручено управлять ею в рамках этого процесса;
- определения необходимых областей компетенции для тех, кто вовлечен в э-раскрытие;
- содействие принятию во внимание возможностей для упреждающего (proactive) использования технологий с целью снижения издержек и рисков, а также повышения эффективности на протяжении всего процесса раскрытия и
- предложения способов избежать непреднамеренного раскрытия потенциально привилегированной, конфиденциальной или чувствительной информации.

Главная цель заключается в том, чтобы помочь организациям планировать и реализовывать свои цели и обязательства в области э-раскрытия, если таковые имеются, соразмерно с потребностями в условиях каждой конкретной ситуации.

6.2 Основные понятия

Полезно заранее обратить внимание на перечисленные ниже проблемы э-раскрытия. Степень важности этих проблем и необходимость их решения варьируются в зависимости от ситуации и должны быть оценены в соответствии с потребностями в условиях конкретной ситуации:

- область э-раскрытия;
- стратегическое и оперативное управление э-раскрытием;
- установление ответственности за каждый аспект проекта э-раскрытия;
- выявление систем, хранящих потенциально подлежащую раскрытию информацию;
- выявление потенциально подлежащей раскрытию информации;
- создание соответствующей документации на протяжении процесса э-раскрытия;
- ожидаемые расходы и их предлагаемое распределение между сторонами;
- обеспечение сохранности информации, включая процесс установления запретов на уничтожение;
- раскрытие сведений о методах хранения электронной информации, о соответствующем оборудовании и программном обеспечении;
- сбор/приобретение электронной информации;
- обработка электронной информации;
- проверка и анализ электронной информации;
- представление электронной информации, включая форму представления.

Участникам процесса э-раскрытия приходится принимать во внимание множество специфических для конкретной ситуации факторов. Среди них важное место занимают затраты на э-раскрытие. Основные причины роста затрат включают:

- сбор: поиск и извлечение потенциально подлежащей раскрытию информации;
- объемы: количество первичной информации, подлежащей сбору, обработке или проверке;
- количество источников: в зависимости от числа хранителей, корпоративных систем и внешних систем, и приложений, находящихся под контролем занимающегося сбором подлежащей раскрытию информации субъекта, соответствующие время и усилия могут экспоненциально увеличиться;
- компетенции персонала: потребность в квалифицированных специалистах, способных выполнять функции, необходимые для эффективного извлечения, обработки, поиска и заключительной проверки информации на относимость и привилегированность, а также ее классификации (в плане, например, относимости, привилегированности, наличия коммерческой тайны, конфиденциальности или потребности в специальной обработке); эти компетенции могут включать в себя знания и навыки в области информационных технологий, компьютерных технологий, статистики, методов поиска и права;
- сложность дела: в простых случаях может быть достаточно э-раскрытия, ограниченного по своему охвату и сложности процесса проверки, однако в более сложных случаях могут понадобиться сложные стратегии и процессы проверки документов и информации.

Время, необходимое для поиска и извлечения информации, объемы информации, число подлежащих исследованию источников и в конечном счете признание электронной информации надежной в ходе судебного разбирательства или расследования тесно увязаны с практикой и политиками, внедрен-

ными организацией для управления сохраняемой в электронном виде информацией на протяжении всего ее жизненного цикла в организации. Организации, которые встраивают готовность к э-раскрытию в свои структуры полномасштабного управления информацией еще до возникновения потребности в э-раскрытии, скорее всего, будут способны более продуктивно и экономически эффективно выполнить требования к э-раскрытию. Стандарты ИСО/МЭК 27050-2 и ИСО/МЭК 27050-4 содержат конкретные рекомендации в этом отношении.

6.3 Цели э-раскрытия

Цели э-раскрытия зависят от конкретной ситуации. В зависимости от ситуации эти цели могут включать следующее:

- обеспечить соблюдение установленных соответствующими законами, нормативными актами, правилами и ожиданиями ограничений на доступ к данным, их использование, обработку или передачу, связанных с конфиденциальностью, защитой персональных данных и др.;
- выявить потенциальные источники подлежащей раскрытию электронной информации;
- надлежащим образом обеспечить сохранность и отслеживание сроков хранения потенциально подлежащей раскрытию электронной информации;
- преобразовать подлежащую раскрытию информацию в формат, способствующий эффективному поиску или проверке;
- минимизировать риск невключения в состав раскрываемой той информации, которая подлежит раскрытию;
- минимизировать риск включения в состав раскрываемой той информации, которая не подлежит раскрытию;
- минимизировать риск невключения в состав исключаемой из раскрытия или требующей специального обращения той информации, которая удовлетворяет требованиям к исключению из раскрытия или специальному обращению;
- минимизировать риск включения в состав исключаемой из раскрытия или требующей специального обращения той информации, которая не удовлетворяет требованиям к исключению из раскрытия или специальному обращению;
- представить подлежащую раскрытию электронную информацию в форме, пригодной для использования запрашивающей стороной;
- рассмотреть вопрос о пропорциональности реагирования в контексте предмета э-раскрытия и соответствующих затрат;
- использовать технологии для снижения рисков и затрат на протяжении всего проекта.

6.4 Основы э-раскрытия

6.4.1 Общие положения

В процесс э-раскрытия часто вовлечены стороны с конфликтующими интересами, которые в худшем случае могут быть враждебными друг другу. Э-раскрытие может сыграть ключевую роль в разрешении конфликта или вопроса, но только тогда, когда оно проводится на основе, обеспечивающей определенный уровень доверия.

Такую основу для э-раскрытия обеспечивает адекватное решение вопросов компетентности, этичности (candour), сотрудничества сторон, полноты и пропорциональности, для чего может потребоваться согласование требований э-раскрытия с требованиями других процессов, с ценностями и принципами.

6.4.2 Компетентность

Учитывая связанные с э-раскрытием сложности, важно, чтобы лица, вовлеченные в процесс э-раскрытия, обладали соответствующими техническими или юридическими компетенциями. Они должны быть способны доказать при необходимости, что прошли надлежащую подготовку и имеют достаточные технические или юридические знания и навыки для надлежащего управления электронной информацией и для выполнения процесса э-раскрытия от имени стороны.

6.4.3 Этичность

Ожидается, что выполняющие э-раскрытие стороны будут придерживаться применимых стандартов профессионализма и этического поведения. В некоторых юрисдикциях это означает, что стороны обязаны исправлять и дополнять представленную документацию (например, проводить дополнительные раскрытия или корректировать ранее представленные материалы). Кроме того, все вовлеченные стороны должны избегать умышленных задержек в проведении процесса э-раскрытия.

6.4.4 Сотрудничество сторон

В судах ряда юрисдикций ожидается, что стороны будут сотрудничать по вопросам, связанным с обеспечение сохранности, сбором, поиском, проверкой и представлением электронной информации, и в таких судах подобное сотрудничество обычно не ставит под сомнение добросовестность действий представителей интересов клиента. Кроме того, сотрудничество в контексте судебного разбирательства, направленное, с одной стороны, на разумное ограничение запросов на раскрытие электронной информации, а с другой — на разумное реагирование на такие запросы, может уменьшить затраты и задержки. Взаимный обмен информацией на самых ранних стадиях раскрытия может быть полезен, где это уместно.

6.4.5 Полнота

Целью представляющей информацию стороны является извлечение и представление набора (непривилегированной) электронной информации, который, при конкретных обстоятельствах, является полным и точным ответом на запрос.

6.4.6 Пропорциональность

В условиях стремительного нарастания объемов электронной информации усиливается озабоченность вопросом поиска наилучшего распределения бремени и затрат, связанных с процессом раскрытия. Один из подходов к решению этой проблемы заключается в принятии мер для обеспечения того, чтобы отдача от э-раскрытия была соизмерима с соответствующим бременем. Связанное с э-раскрытием бремя может принимать различные формы, включая (но не ограничиваясь этим) нарушения обычного хода деловых операций, финансовые затраты или вторжения в частную жизнь отдельных лиц.

6.5 Стратегическое управление и э-раскрытие

6.5.1 Общие положения

Стандарт ГОСТ Р ИСО/МЭК 38500 устанавливает шесть принципов эффективного управления ИКТ, касающихся ответственности, стратегии, приобретения, эффективности, соответствия требованиям и поведения человека. Эти принципы определяют предпочтительное поведение, которым следует руководствоваться при принятии решений (т.е. каждый принцип описывает, что должно происходить, но не описывает, каким образом, когда и кем должны быть реализованы эти принципы, поскольку такие аспекты в значительной мере зависят от природы организации, реализующей эти принципы). Руководящим органам рекомендуется требовать применения этих принципов, и в результате это поможет руководящим органам управлять рисками и поощрять использование возможностей, связанных с применением ИКТ.

Согласно ГОСТ Р ИСО/МЭК 38500, хорошее стратегическое управление ИКТ также помогает руководящим органам обеспечивать соответствие обязательным требованиям (законодательно-нормативным требованиям, договорным обязательствам) в отношении приемлемого использования ИКТ.

В целом тема стратегического управления в связи с э-раскрытием обсуждается в стандарте ИСО/МЭК 27050-2, однако в разделе 6.5, с целью привлечь внимание к соответствующим вопросам, рассмотрены некоторые из наиболее важных элементов.

6.5.2 Факторы риска и особенностей деловой деятельности

Э-раскрытие потенциально может сделать организацию или ее руководящие органы уязвимыми к угрозам, что может повлечь за собой пагубные последствия. Стратегическое управление способно помочь избежать негативных последствий в виде:

- нарушения законодательно-нормативных требований в отношении неприкосновенности частной жизни, охраны здоровья и безопасности и управления документами;
- несоответствия стандартам по вопросам безопасности и социальной ответственности и
- проблем, связанных с правами интеллектуальной собственности, включая лицензионные соглашения.

Избежание негативных последствий, связанных с этими угрозами, требует обеспечения осведомленности и принятия мер по смягчению рисков, которые бы охватывали как процесс э-раскрытия, так и такие проблемы, как неадекватность ИКТ-систем и ненадлежащее или недопустимое использование информационно-коммуникационных технологий.

6.5.3 Исполнение законодательно-нормативных требований и процесс проверки раскрываемой информации

Многие организации сталкиваются с проблемами исполнения законодательно-нормативных, правовых и иных требований. Эти требования могут быть причиной выполнения организацией действий по э-раскрытию, но с большей вероятностью они будут влиять на то, как осуществляется про-

цесс э-раскрытия. Например, могут существовать ограничения на то, кто может видеть электронную информацию, каким образом эта информация может передаваться и храниться, а также конкретные проблемы, связанные с отслеживанием сроков хранения или проведением уничтожения. Важно обеспечить, чтобы процесс э-раскрытия выполнялся в рамках соответствующих законодательно-нормативных требований.

6.5.4 Защита неприкосновенности частной жизни и персональных данных

Помимо нормативно-правовых ограничений и необходимости исполнения законодательно-нормативных требований, о чем было сказано в п.6.5.3, важно знать об определенных ограничениях на использование имеющихся у хранителя данных, связанных с защитой неприкосновенности частной жизни (см. также стандарт ИСО/МЭК 29100). В частности, могут существовать ограничения на обработку персональных данных, содержащихся в источниках данных под контролем хранителя, которые должны учитываться при управлении сохраняемой в электронном виде информацией.

Если э-раскрытие затрагивает персональные данные, то в некоторых юрисдикциях могут существовать жесткие ограничения на то, что с ними можно сделать (например, они не могут быть перемещены через границы). Даже в отсутствие таких ограничений часто необходимы дополнительные меры защиты данных для того, чтобы обеспечить конфиденциальность и предотвратить утечки данных. Стандарт ИСО/МЭК 27050-4, в сочетании со стандартом ИСО/МЭК 27040, содержит дополнительные указания и материалы, которые могут помочь в решении такого рода проблем.

6.6 ИКТ-готовность к э-раскрытию

6.6.1 Общие положения

На протяжении всего процесса э-раскрытия вовлеченные в него стороны собирают, обрабатывают и манипулируют сохраняемой в электронном виде информацией. Часто эта электронная информация извлекается из специально спроектированной для ее защиты среды вычислений или хранения. Для выведенной или скопированной из таких сред информации могут потребоваться аналогичные меры защиты.

В стандарте ИСО/МЭК 27050-4 рассматриваются многие из таких вопросов в контексте э-раскрытия.

6.6.2 Долговременное хранение электронной информации

Э-раскрытие обычно выполняется на ранних стадиях судебного разбирательства, аудита, проводимого государственными органами расследования или в иных подобных случаях. Пока такое разбирательство или расследование продолжается, сторонам необходимо хранить соответствующую электронную информацию таким образом, чтобы она продолжала оставаться доступной и сохранялась ее целостность. Адекватные меры по обеспечению непрерывности деловой деятельности и восстановлению после катастроф, наряду с обычными механизмами защиты данных (такими, как резервное копирование) могут быть важными элементами программы хранения электронной информации.

При принятии решений о долговременном хранении электронной информации важно принять во внимание соответствующие временные рамки. Существуют существенные различия между подходами, используемыми для хранения электронной информации в течение нескольких недель или месяцев, в сравнении с теми, что используются для хранения такой информации в течение десятилетий (например, в случае сложного гражданского спора, который проходит через многочисленные апелляции) в электронных архивах.

Необходимо также подумать о том, влияют ли требования по защите неприкосновенности частной жизни и персональных данных на то, сколь долго могут храниться персональные данные; и не требуют ли обстоятельства дела приостановления отсчета обычных сроков хранения данных. Подходы к решению таких вопросов могут значительно различаться в разных юрисдикциях.

6.6.3 Сохранение конфиденциальности электронной информации

Сохраняемая в электронном виде информация часто содержит защищенную правами собственности, привилегированную и чувствительную информацию, которую необходимо обрабатывать и хранить таким образом, чтобы обеспечить защиту ее конфиденциальности. Неспособность адекватно контролировать чувствительную электронную информацию может привести к серьезным последствиям в случае, если произойдет утечка данных.

В зависимости от степени чувствительности информации могут понадобиться такие меры безопасности, как шифрование данных в процессе передачи и при хранении, а также, вероятно, потребуется обеспечить соответствующее управление ключами шифрования.

6.6.4 Уничтожение электронной информации

Когда электронная информация перестает быть нужной, важно уничтожить ее таким образом, чтобы избежать утечек данных. Это обычно означает, что логическое хранилище и/или носители данных, используемые для хранения информации, должны быть надлежащим образом очищены (например, с использованием методов перезаписи или технологии криптографического стирания).

6.7 Планирование и составление бюджета проекта э-раскрытия

Разнообразные движущие силы, влияющие на проект э-раскрытия, затрудняют заблаговременное, за много месяцев до его начала, планирование такого проекта. Ввиду этого такие проекты, как правило, управляются на индивидуальной основе, что может значительно увеличить затраты. Как и в случае любых других проектов и вне зависимости от срочности запроса на представление информации, усилия на планирование, затраченные в самом начале проекта, обычно позволяют сэкономить значительное время и расходы на более поздних стадиях проекта. Это особенно важно ввиду того, что для многих этапов типичного проекта э-раскрытия их повторное выполнение на более поздних стадиях оказывается непропорционально дорогостоящим. Например, если структура и формат представления информации не были согласованы заранее, до проведения проверки, а массивы электронной информации или физических документов не были последовательно промаркированы, то это может привести к необходимости частично повторить процесс проверки.

Одним из важных первых шагов является формирование группы проекта э-раскрытия, которая, как минимум, включает куратора (project sponsor) и менеджера проекта, представляющего интересы деловой деятельности/организации; менеджера проекта от юридической или следственной группы; и менеджера проекта с точки зрения ИКТ. Этот треугольник взаимодействия между деловой деятельностью/организацией, юридической службой/следователями и ИКТ-службой имеет жизненно важное значение для успеха проекта.

Также одним из важных первых шагов является разработка плана выполнения проекта э-раскрытия с максимально возможной детализацией. Как и план любого другого проекта, план э-раскрытия должен включать основные этапы проекта (такие, например, как выявление, обеспечение сохранности/сбор, обработка, проверка, анализ, представление другой стороне и, возможно, демонстрация); отдельные шаги, которые необходимо выполнить на каждом из этапов, и отдельные задания на каждом шаге.

Учитывая затраты, с которыми связан типичный проект э-раскрытия, важным вопросом является подготовка с самого начала и мониторинг детального бюджета.

Этот бюджет должен учитывать разнообразный профессиональный состав группы э-раскрытия и тот факт, что в состав такой группы могут входить внутренние и внешние юридические консультанты, а также консультанты по вопросам ИКТ и э-раскрытия. Важно сформировать бюджет для каждого этапа плана процесса э-раскрытия, а в некоторых случаях — для каждого шага каждого этапа этого процесса, с тем, чтобы можно было определить, является ли предлагаемый подход пропорциональным в контексте текущей ситуации.

Примечание — Хотя положения п. 6.5 в большей степени ориентированы на крупные организации, вовлеченные в крупные судебные споры и расследования, и могут быть не в полной мере применимы в отношении менее крупных организаций или более мелких споров, однако поставленные в данном разделе вопросы по-прежнему заслуживают внимательного рассмотрения.

7 Сохраняемая в электронном виде информация (ESI)

7.1 Общие положения

Сохраняемая в электронном виде информация (electronically stored information, ESI) в настоящее время является неотъемлемой частью как деловой, так и индивидуальной среды. Как следствие, она становится все более важным источником соответствующих материалов в современных спорах или разбирательствах (делах).

Сохраняемая в электронном виде информация заслуживает того, чтобы связанные с ней вопросы были приняты во внимание на самых ранних этапах дела. Она может быть чрезвычайно хрупкой, и некоторые ее виды могут быть легко утрачены или изменены даже просто при открытии документа. Продумывание в первые же дни после того, как становится известно о начале спора или разбирательства, таких элементов процесса э-раскрытия, как выявление, обеспечение сохранности и, возможно,

сбор электронной информации, может способствовать принятию ответственных решений и способно обеспечить значительную экономию времени и средств в более длительной перспективе.

Управление сохраняемой в электронном виде информацией оказывает все большее воздействие на деловые организации и на отдельных лиц; объемы, размеры, сложность и диапазон такой информации часто могут быть огромными, а сама электронная информация может содержать конфиденциальные, привилегированные или затрагивающие частную жизнь сведения, о которых следует подумать отдельно. Управление сохраняемой в электронном виде информацией часто не рассматривается как приоритетный вид деятельности до тех пор, пока истинная ее ценность и стоимость локализации не станут очевидными в ходе соответствующего дела. Организации и отдельные лица часто:

- сосредотачивают свои усилия по сохранению электронной информации на ее хранении исключительно в оперативных деловых целях, не рассматривая вопрос в более широком контексте;
- в минимальной степени учитывают свои обязательства по исполнению законодательно-нормативных требований в отношении электронных документов;
- имеют ограниченное представление о доказательной ценности хороших деловых документов, и
- не имеют четкого понимания затрат и рисков, связанных с плохой практикой управления информацией.

Плохое управление сохраняемой в электронном виде информацией может создать дополнительные проблемы, когда дело доходит до выявления и извлечения такой информации в ответ на запрос о ее раскрытии или же представлении в соответствии с требованиями законодательства, поскольку:

- контент подпадает под ограничения на доступ, связанные защитой персональных данных и другими аналогичным требованиями, а также под ограничения, связанные с правом собственности и контролем;
- информация оказывается более объемной, чем ожидалось, из-за того, что она хранилась дольше установленных сроков хранения;
- часто в организации недостаточно знаний о том, где можно найти потенциально относящуюся к делу электронную информацию;
- объемы и сложность информации оказываются слишком большими даже для специалистов в области ИКТ;
- текучесть кадров и организационные изменения (такие, как слияния, поглощения и продажи) приводят к тому, что определенная электронная информация хотя и сохраняется, но утрачиваются организационные знания и контекст;
- ИКТ-среда и системы могут быть плохо документированы, и
- электронная информация может находиться во внешних приложениях и ИКТ-инфраструктуре (например, в социальных сетях, средах облачных вычислений и т.д.).

В зависимости от обстоятельств, эти факторы могут привести к увеличению затрат на локализацию и обработку относящихся к рассматриваемому делу данных. Это может вызвать задержки и увеличение затрат на процесс раскрытия, а также привести к тому, что потенциально относящаяся к делу электронная информация будет пропущена.

7.2 Распространенные типы сохраняемой в электронном виде информации

7.2.1 Общие положения

Отнесение источников сохраняемой в электронном виде информации к категории легкодоступных (или «активных») либо к категории труднодоступных (или неактивных, остаточных или унаследованных), с обоснованием такой категоризации в каждом конкретном случае, является важным видом деятельности на ранних этапах э-раскрытия. В увязке с подготовкой бюджета такая категоризация может помочь в определении того, является ли обеспечение сохранности и сбор информации из таких источников пропорциональным.

7.2.2 Активные данные

Сохраняемая в электронном виде информация данного типа «активно» используется и располагается на жестких дисках или на иных устройствах хранения компьютеров сотрудников, а также на серверах, приводах и в базах данных организации. Доступ к активным данным обычно можно получить при помощи средств файловой системы либо с помощью приложения, в котором они были созданы. Пользователи могут получить доступ к активным данным немедленно, без выполнения операций восстановления или реконструкции. По мере роста популярности облачных вычислений и вычислительных онлайн-услуг такие данные также могут находиться на устройствах хранения внешних поставщиков

услуг. В рамках большинства судебных споров и расследований в первую очередь требуется сохранить и представить активные данные.

Получить доступ к активным данным и собрать их может быть относительно легко, по крайней мере, по сравнению с другими типами сохраняемой электронным образом информации. Они также могут быть легко удалены или изменены, поэтому вопрос об обеспечении их сохранности необходимо рассмотреть как можно скорее.

7.2.3 Неактивные данные

К этому типу относят электронную информацию, связанную с закрытыми, завершенными или законченными действиями, включая информацию, которую организация поддерживает в целях ее долговременного хранения и в интересах управления документами, но которая не является немедленно доступной пользователю компьютерной системы. В число источников неактивных данных могут входить многие из названных выше источников активных данных.

Заархивированные данные часто хранятся в сжатом формате и могут поддерживаться на системных приводах или на автономных устройствах, таких, как ленточные или дисковые накопители и оптические носители. В некоторых системах пользователям предоставляется возможность напрямую самим извлекать архивные данные, в то время как в других системах для этого требуется помощь ИКТ-специалиста. Проблемы сохранения и сбора включают выявление относящихся к делу неактивных и заархивированных данных, определение местонахождения и способа их хранения и восстановление их из сжатого формата.

Еще одной формой неактивных данных является электронная информация, хранящаяся в системах защиты данных (например, в системах резервного копирования). Такого рода неактивные данные могут стать источником проблем, поскольку они, как правило, хранятся в течение коротких периодов времени (например, резервные носители могут регулярно циклически перезаписываться); могут отсутствовать механизмы для определения того, что конкретно находится на носителе; а сохраненные данные могут быть фрагментарными (например, могут быть записаны только изменения по сравнению с предыдущей резервной копией). Ситуация усложняется тем, что ИКТ-персонал может создавать дополнительные резервные копии вне рамок обычных операций (например, проводя ротацию, документирование и т.д.), и выявить эти потенциальные источники сохраняемой в электронном виде информации может быть чрезвычайно сложно. С этим типом данных связаны те же проблемы, что и с архивными данными, при этом дополнительные сложности возникают ввиду коротких сроков хранения, что требует быстрых действий для приостановки автоматического уничтожения этой электронной информации в ситуациях, когда возникает необходимость ее сохранить.

Подраздел 7.3.3 содержит дополнительную информацию о резервных копиях и архивах.

7.2.4 Остаточные данные

Электронная информация этого типа является скрытой и не может быть просмотрена с использованием программных приложений (примером могут служить системные файлы), или же это информация, которая была удалена, фрагментирована или повреждена. Для сбора электронной информации данного типа обычно требуется создание точной побитовой копии всего физического носителя информации (например, жесткого диска, CD или DVD-диска, ленты), включая все активные и остаточные данные, а также нераспределенное или неиспользуемое пространство на носителе.

Для создания образов носителей информации и последующего извлечения остаточных данных могут потребоваться услуги специалиста по электронным доказательствам, умеющего использовать специальные инструменты (см. ИСО/МЭК 27037), и такой процесс может потребовать много времени и затрат. Тем не менее, в некоторых случаях компании могут принять решение о создании образов жестких дисков особо важных ключевых хранителей информации, чтобы гарантировать сохранение всех их данных, включая те файлы, которые хранитель мог непреднамеренно или умышленно удалить, или частично перезаписать.

7.2.5 Унаследованные данные

Данный тип сохраняемой в электронном виде информации создан с использованием вышедшего из употребления или морально устаревшего программного обеспечения и оборудования (унаследованные системы). К числу унаследованных может быть отнесена система, которую компания по-прежнему использует, но которую больше уже не поддерживает поставщик оборудования или программного обеспечения. Это также может быть система, которую компания вывела из эксплуатации, однако сохраняет ее на случай, если содержащаяся в ней информация потребуется в будущем.

Относимость к предмету раскрытия унаследованных данных иногда сложно определить, не проведя их восстановление или реконструкцию, что может оказаться дорогостоящим делом. Если необхо-

димо обеспечить сохранность унаследованных данных, то компании, возможно, потребуется сохранить устаревшее оборудование и программное обеспечение, если нет иного способа просмотра и использования данных.

7.3 Распространенные источники сохраняемой в электронном виде информации

7.3.1 Общие положения

Электронную информацию, потенциально относящуюся к предмету судебного спора или расследования, можно найти в широком диапазоне источников. Чтобы способствовать выявлению таких источников, важно проанализировать как находящиеся под прямым контролем хранителей системы и ресурсы, к которым те имеют доступ, так и те системы и ресурсы, которые не находятся под контролем хранителей.

7.3.2 Подконтрольные хранителям источники

Подконтрольным хранителю источником сохраняемой в электронном виде информации является такой источник, над которым отдельный хранитель непосредственным образом осуществляет опеку или контроль. К ним относятся, помимо прочего, следующие источники:

- компьютеры: потенциально относящаяся к делу электронная информация может располагаться на настольных компьютерах, ноутбуках или домашних компьютерах хранителей, а также на съемных носителях информации, таких как флеш-накопители, внешние жесткие диски, DVD-диски или компакт-диски;
- мобильные устройства: потенциально относящаяся к делу электронная информация может содержаться на личных устройствах хранителя, таких, как мобильные телефоны, смартфоны, планшеты, системы глобального позиционирования (Global Positioning Systems, GPS) и т.д.

С корпоративной точки зрения, базы данных и программные приложения, системы сетевого хранения, системы резервного копирования и электронные архивы, перечисленные в п.7.3.3, также могут считаться подконтрольными хранителям источниками.

7.3.3 Неподконтрольные хранителям источники

Неподконтрольные хранителям источники сохраняемой в электронном виде информации являются либо внутренними, либо внешними по отношению к организации.

Внутренними являются те источники, к которым имеет доступ один или несколько хранителей, но которые контролируются иным хранителем, таким как ИКТ-администратор. В число внутренних неподконтрольных хранителям источников, помимо прочего, входят:

- базы данных и приложения: связанная с динамическими базами данных электронная информация может в ряде случаев иметь отношение к предмету э-раскрытия, и, в зависимости от обстоятельств, раскрытие может затронуть электронную систему управления контентом (EDMS) организации, электронную систему управления документами (ERMS) или инструменты, используемые для коллективной работы;
- сетевые системы хранения данных: электронная информация может храниться в различных местах во внутренней сети организации (например, на коллективно используемых жестких дисках, на сетевых дисках и серверах), а также с использованием специализированных технологий, таких, как сетевые хранилища данных (Network Attached Storage, NAS) и сети хранения данных (Storage Area Networks, SAN);
- системы резервного копирования: электронная информация копируется или резервируется из информационных систем в системы защиты данных, использующие ленты или другие носители;
- электронные архивы: электронная информация, содержащаяся в электронных (цифровых) архивах (хранилищах данных), как правило, представляет собой официальные деловые документы, а также документы, сохраняемые во исполнение законодательно-нормативных требований либо ввиду их исторической ценности, и т. д.

В число внешних неподконтрольных хранителям источников, помимо прочего, входят:

- облачное хранение: облачные решения, которые часто используются для решения многих прикладных задач, а также для целей восстановления после катастроф и обеспечения непрерывности деловой деятельности;
- социальные сети: социальные сети содержат электронную информацию, которой группы людей обмениваются в основном для целей социального общения. Все чаще, однако, социальные сети используются для деловых целей, что может привести к проблемам, поскольку эта информация обычно находится вне сферы непосредственного контроля организации.

7.3.4 Потенциально исключаемые источники сохраняемой в электронном виде информации

Электронную информацию необходимо сохранять не изо всех источников. Следующие источники потенциально могут быть исключены из процесса э-раскрытия:

- удаленные данные, данные в нераспределенных или неиспользуемых зонах на жестких дисках;
- данные в оперативной памяти (ОЗУ) или иные недолговечные данные;
- данные в часто обновляемых автоматически полях метаданных, такие, например, как дата последнего открытия файла.

Примечание — Необходимо провести тщательный анализ и проконсультироваться по вопросу о том, какие поля метаданных должны быть сохранены, поскольку может быть трудно, а зачастую и невозможно, восстановить их значения после внесения каких-либо изменений. Например, информация в метаданных о времени создания или последней модификации документа может иметь решающее значение для отбора информации на последующих этапах процесса э-раскрытия, поэтому ее необходимо сохранять;

- данные на резервных копиях, которые, по существу, дублируют более доступные из иных источников данные;
- тестовые данные, предназначенные для временного использования;
- иные формы электронной информации, для сохранения которых требуются неординарные активные меры, не применяемые в ходе обычной повседневной деловой деятельности.

Может оказаться полезной попытка договориться с противными сторонами в судебном споре или со следствием о том, что электронную информацию такого рода сохранять не нужно.

7.4 Форматы представления сохраняемой в электронном виде информации

7.4.1 Общие положения

В состав имеющей отношение к конкретному вопросу электронной информации могут входить текстовые файлы, электронные таблицы, сообщения электронной почты, базы данных, чертежи, фотографии, данные из проприетарных приложений, данные на веб-сайтах, сообщения голосовой почты и многое другое. Форматы сбора и представления электронной информации можно классифицировать как первоначальные (native), близкие к первоначальным (near-native), форматы графических образов (бумагоподобные, near-paper) и бумажные.

7.4.2 Первоначальные форматы

Файлы в том формате, в котором они были созданы и поддерживались, называются файлами в первоначальном формате. Первоначальный формат часто рекомендуется для тех файлов, которые не предназначались для распечатывания, такие, как электронные таблицы и небольшие базы данных. Для некоторых типов файлов первоначальный формат может быть единственным способом адекватного представления электронной информации.

Представление в первоначальном формате не требует от представляющей стороны затрат на преобразование данных в другой формат; однако получающей стороне для открытия файлов может понадобиться первоначальное программное приложение или проприетарное программное обеспечение представляющей информацию стороны.

В случае, если сторона решает преобразовать электронную информацию в другой формат, могут потребоваться меры, обеспечивающие, чтобы элементы этой информации, такие, как метаданные, не были непреднамеренно потеряны или скрыты в результате процесса преобразования.

7.4.3 Форматы, близкие к первоначальным

Некоторые файлы (например, электронной почты и баз данных) невозможно просмотреть, не проводя преобразования в какой-либо форме. Например, большинство файлов электронной почты необходимо извлечь и преобразовать в отдельные файлы, и в результате формат изменяется, и они больше не находятся в первоначальном формате.

Большие базы и коллекции данных обычно представляются в формате, близком к первоначальному. Базы данных могут содержать огромное количество неотличимых друг от друга таблиц данных. Корпоративные деловые системы могут содержать сотни таблиц и тысячи полей данных. Для использования систем могут требоваться разнообразные СУБД и проприетарное программное обеспечение. По этим причинам большие базы и коллекции данных обычно не представляются в их первоначальном формате. Часто требуется провести анализ этих баз данных с привлечением соответствующего персонала для выделения подлежащих раскрытию данных и определения подходящего формата, близкого к первоначальному.

Экспорт из таких баз данных часто осуществляется в виде текстовых файлов с разделителями. В некоторых случаях текстовые файлы сопровождаются схемой базы данных, словарем данных, метаданными и/или программным обеспечением. Данные также можно экспортировать в распространенные форматы электронных таблиц.

7.4.4 Форматы графических образов (бумагоподобные)

Электронная информация также может быть представлена в форматах графических образов (бумагоподобных форматах). Создание (рендеринг) графического образа — это процесс преобразования электронной информации либо сканирования бумажного документа в нередактируемый электронный файл. В ходе этого процесса делается «снимок» файла в том виде, в каком он выглядит или мог бы выглядеть в бумажном формате. В зависимости от параметров печати в документе, принтере и/или компьютере возможно изменение данных в образе или их отсутствие. Для минимизации этих проблем необходимы экспертные знания в области инструментов для э-раскрытия и создания графических образов.

7.4.5 Бумажные форматы

Вместо того чтобы иметь дело с раскрываемой информацией в ее электронном виде, может оказаться разумной и практичной фиксация электронной информации в какой-либо аналоговой форме (например, в виде распечатки на бумаге, фотографии и т. д.) и последующее использование в деле информации в этой форме. Как и при преобразовании электронной информации в форматы графических образов (см. 7.4.4), преобразование электронной информации в какую-либо аналоговую форму может привести к утрате или изменению данных. Как следствие, для минимизации этих проблем в процессе вывода на печать либо создания графических образов могут потребоваться экспертные знания в области инструментов для э-раскрытия и создания графических образов.

7.5 Неэлектронная информация как часть процесса раскрытия

Хотя основная часть деловой информации хранится в электронном виде, однако проект раскрытия может охватить, как минимум, небольшое количество традиционных аналоговых/бумажных документов (в отличие от распечатанной электронной информации, о которой шла речь в 7.4.5). Если принято решение о сборе аналоговых материалов, то чем более процесс сбора сфокусирован на предмете раскрытия, тем потенциально меньше работы потребуется для выделения из множества собранных материалов подмножества тех, что имеют отношение к делу.

Когда имеется набор относящихся к делу аналоговых документов, одним из вариантов дальнейших действий может быть их сканирование в электронный формат* с последующим включением в процесс проверки вместе с электронными документами. Следует проверить, есть ли документы, которые тесно с ними взаимосвязаны (как, например, приложения). Перед представлением такие документы следует проверить, промаркировать и, возможно, отцензурировать. Использование одних и тех же технологий и процессов для управления, как аналоговыми документами, так и электронной информацией может сделать весь процесс в целом более эффективным.

8 Процесс электронного раскрытия

8.1 Обзор

Электронное раскрытие (э-раскрытие) является формой традиционного раскрытия информации, которая обычно включает в себя выявление, обеспечение сохранности, сбор, обработку, проверку, анализ и представление сохраняемой в электронном виде информации (ESI), потенциально имеющей отношение к конкретному судебному спору или расследованию. Потенциально относящаяся к делу электронная информация обычно:

- выявляется посредством итеративного процесса исследований и собеседований с сотрудниками и ИКТ-персоналом;
- сохраняется благодаря принятию мер для уведомления соответствующих лиц о том, что им следует воздерживаться от ее удаления или уничтожения, а также путем отключения систем, которые делают это автоматически;

---

* Этот процесс может включать использование технологий оптического распознавания символов (OCR) для обеспечения возможности полнотекстового поиска, а также ручное кодирование с целью захвата соответствующих метаданных.

- собирается из первоисточника, с применением одной или нескольких методик извлечения или сбора, обеспечивающих сохранение целостности данных;
- обрабатывается с использованием одного или нескольких технологических инструментов, индексируется для обеспечения возможности полнотекстового поиска;
- одним или несколькими способами проверяется на относимость к делу экспертами в области права или в предметной области, которым в этом помогают различные инструменты, а также лица, обладающие опытом эффективного использования этих инструментов;
- анализируется для достижения целей соответствующего дела;
- представляется запрашивающей стороне или сторонам в такой форме, которая обеспечивает ее разумную пригодность к использованию, или в форме, согласованной сторонами.

В настоящем стандарте, где это уместно, проводится различие между общими понятиями, такими, как «идентификация/выявление», и конкретными элементами процесса э-раскрытия, путем добавления в название слова «ESI» (например, «выявление ESI»). На рисунке 2 показаны все элементы процесса э-раскрытия.

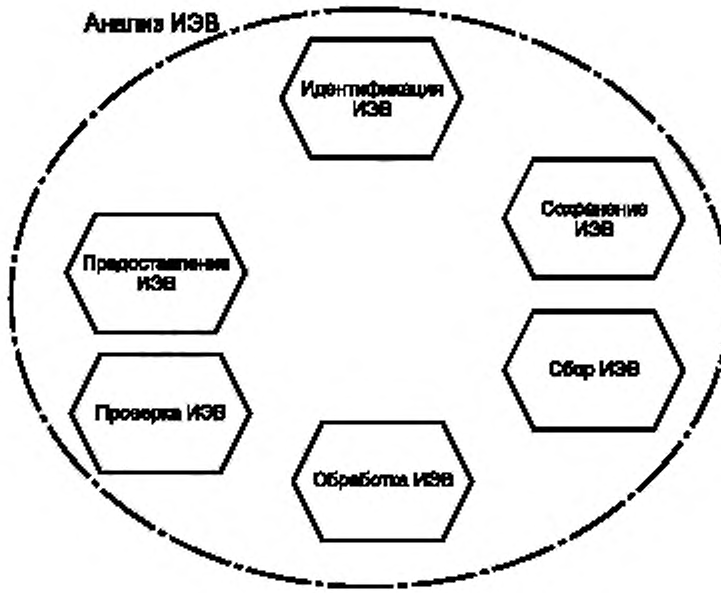

Рисунок 2 — Элементы процесса э-раскрытия

На рисунке 2 также показана взаимосвязь между элементами процесса э-раскрытия. Отображение анализа ESI в виде внешнего кольца призвано показать, что такой анализ опционально может проводиться в сочетании с каждым из остальных элементов процесса э-раскрытия. Например, возможен сценарий, в котором в ходе выявления ESI может потребоваться проведение анализа электронной информации, после чего процесс возвращается к этапу выявления для выполнения дополнительных действий. Течение процесса э-раскрытия может переключаться с одного его элемента (за исключением анализа) на другой, а затем возвращаться обратно к более раннему элементу процесса. Наконец, э-раскрытие часто представляет собой упорядоченный и итеративный процесс, в котором задействованы некоторые или все элементы, и это также отражено на рисунке 2 с помощью круговых стрелок.

Настоящий стандарт призван служить интересам многих заинтересованных сторон, крупных и малых организаций, имеющих и не имеющих отношения к юриспруденции лиц и т.д. Хотя в стандарте описывается надежный процесс э-раскрытия, отсутствует намерение навязывать ненужные процессы. Крупные предприятия, сталкивающиеся со сложными проблемами э-раскрытия, могут использовать

большинство или все описанные здесь элементы процесса, однако это может оказаться непрактичным для небольших организаций или в рамках небольших по охвату дел — в таких случаях может быть достаточно использовать подмножество элементов процесса э-раскрытия.

Предположим, что небольшое число сообщений электронной почты играет ключевую роль в споре или расследовании. Работа начинается с выявления относящейся к делу электронной информации, затем проводится ее анализ с целью выяснения, могут ли существовать дополнительные источники. Если дополнительных источников не обнаружено, собирается электронная переписка, о которой идет речь (пропуская этап обеспечения сохранности). Затем выполняется анализ информации с целью определения адекватности процесса сбора, а также для принятия обоснованного решения пропустить такие элементы, как обработка и проверка. После этого относящиеся к делу сообщения электронной почты представляются в их первоначальном формате в рамках элемента представления электронной информации.

В некоторых юрисдикциях суды, законодательные органы и/или государственные регуляторы разработали правила, регламентирующие порядок выявления организациями электронной информации, особенно в рамках гражданского и уголовного судопроизводства, проведения расследований и аудита. В таких юрисдикциях у организаций может существовать обязанность принять разумные меры для выявления и сохранения потенциально относящейся к делу электронной информации в случаях, когда затрагивающий их судебный спор или расследование уже начались или их можно обоснованно предвидеть. Суть этой обязанности по выявлению и сохранению заключается в том, что организация должна своевременно выявлять и обеспечивать сохранность потенциально относящейся к делу электронной информации. Кроме того, от организаций может ожидаться разработка соответствующих протоколов управления сохраняемой в электронном виде информацией и обеспечения соответствия этим правилам.

8.2 Выявление ESI

Выявление электронной информации — элемент процесса э-раскрытия, в рамках которого сторона, по каким-либо причинам (таким как обоснованное ожидание судебного иска, получение досудебного требования об обеспечении сохранности доказательств, запроса на проведение проверки, письма с требованиями, письма-предупреждения о возможности санкций за незаконные действия или уведомления о неисполнении условий контракта; или даже обсуждение вопроса с противоположной стороной или ее адвокатом), предпринимает шаги для выявления информации, которая потенциально может иметь отношение к соответствующему вопросу.

По сути дела, выявление электронной информации — это усилия, направленные на понимание соответствующего вопроса и на определение отдельных лиц, подразделений и источников электронной информации, которые могли бы с разумной вероятностью привести к потенциально относящейся к делу информации. В случае электронной информации ее источники, вероятно, будут разнообразными и сложными, потенциально охватывая как внутренние, так и внешние места хранения, различные типы серверов и огромное множество электронных устройств. Кроме того, также может потребоваться принять во внимание унаследованные системы (архивы, резервные копии, неактивные системы и данные). Как правило, для определения потенциально важных для конкретного дела источников проводятся собеседования с потенциально вовлеченными в соответствующие события лицами, а также с отдельными сотрудниками ИКТ-подразделения, с тем чтобы выяснить, располагают ли они соответствующей электронной информацией или знают о ее местонахождении. Эти собеседования, в свою очередь, могут привести к выявлению или исключению других ключевых действующих лиц или возможных мест хранения относящейся к делу электронной информации.

Идеальным вариантом с точки зрения выявления отдельных лиц, проведения с ними собеседований и документирования их знаний о типах данных и местах хранения, где может находиться потенциально относящаяся к делу информация, является наличие типовых схем проведения собеседований и механизмов отслеживания. Типовые схемы проведения собеседований могут включать различные вопросы, которые выбираются в зависимости от делового подразделения и роли отдельного лица. Такая документация может помочь в планировании, реализации и отслеживании действий и ответов в процессе выявления, и она может стать отправной точкой в случае, когда ставится вопрос о дополнительных (или потенциально избыточных) источниках информации. Кроме того, ее можно использовать в качестве доказательства того, что процесс выявления был проведен надлежащим образом, если в этом возникнут сомнения.

8.3 Обеспечение сохранности ESI

Обеспечение сохранности — элемент процесса э-раскрытия, в рамках которого, после наступления события-триггера, предпринимаются усилия по защите от изменения или уничтожения информации, которая была идентифицирована как подпадающая под обязательства по обеспечению сохранности в рамках соответствующего дела. Обеспечение сохранности охватывает не только потенциально относящуюся к делу электронную информацию, находящуюся во владении физического лица или организации, но также и информацию, не находящуюся во владения лица или организации. Поскольку обязанности по сохранению информации могут варьироваться в зависимости от юрисдикции, нет какого-то единого стандарта, говорящего о том, как оценить степень адекватности усилий по обеспечению сохранности или же уровень риска или потенциальной ответственности стороны за невыполнение ею своих обязанностей по обеспечению сохранности.

Сохранность электронной информации можно обеспечить путем ее сбора (т.е. копирования непосредственно из ее первоисточника) или же путем принятия соответствующих мер там, где она обычно находится (например, это может быть самостоятельное сохранение хранителем или обеспечение сохранности по месту нахождения с использованием технологических решений), после чего может быть проведен (или не проведен) ее сбор в зависимости от потребностей конкретного дела и стратегии сохранения. Действия по сбору копий электронной информации сами по себе являются формой сохранения, поэтому сбор и сохранение электронной информации могут выполняться совместно. Ключевым отличием элемента обеспечения сохранности является то, что он включает в себя принятие мер по сохранению электронной информации без каких-либо модификаций. В определенных ситуациях может быть оправдано приостановление обычных процедур, способных удалять или изменять потенциально относящиеся к делу данные (таких, как ротация резервных лент или регулярное уничтожение документов с истекшими сроками хранения).

8.4 Сбор ESI

Сбор сохраняемой в электронном виде информации — элемент процесса э-раскрытия, в рамках которого из сохраненных электронной информации и аналоговых документов создается набор данных; впоследствии эта коллекция делается доступной для дальнейшей обработки и завершающей проверки.

По своей сути, сбор информации — это усилия по копированию, в ходе которых создаются копии или образы нужных файлов, включаемые в набор данных, который затем может быть передан для последующей обработки и проверки. Существует широкий спектр инструментов и методов, которые могут использоваться для сбора информации, начиная от тех, что позволяют восстанавливать удаленные пользователем файлы, до тех, которые поддерживают простой экспорт целевых файлов силами пользователя. Инструменты и методы, подходящие для каждой конкретной ситуации, могут различаться в зависимости от характера устройства, с которого собираются файлы (настольный компьютер или, например, смартфон), от природы собираемых файлов (например, электронная почта или же посты на микроблоге), от характера спора или разбирательства, которое послужило причиной для сбора информации (например, уголовное или гражданское), и от юрисдикции, в рамках которой проводится судебное разбирательство или расследование.

8.5 Обработка ESI

Обработка — элемент процесса э-раскрытия, в рамках которого, после того как была обеспечена сохранность информации и проведен ее сбор, предпринимаются шаги для обеспечения возможности поиска по данным и представления их в подходящем для проведения проверки формате. Она может включать применение одного или нескольких методов. Кроме того, существует огромное количество методов, используемых для сужения объемов подлежащих раскрытию данных, начиная с исключения системных файлов и иных файлов, которые вряд ли будут представлять интерес в рамках дела. После этого часто применяется один или несколько методов фильтрации, начиная от фильтрации по диапазону дат и по типу файлов, базовой фильтрации по метаданным или тексту с использованием ключевых слов, и до использования интеллектуальных и «предсказывающих» (predictive) алгоритмов, которые выполняются над предварительно обработанными текстовыми данными. При обработке электронной информации также принимаются решения об исключении избыточных данных. Применяемые при обработке электронной информации методы часто согласовываются сторонами для обеспечения общего понимания того, как данные могут обрабатываться и предоставляться в рамках последующих элементов процесса э-раскрытия.

Помимо сокращения объемов данных, необходимо, чтобы обработка данных поддерживалась защитными процедурами аудита, мерами контроля качества, в состав которых входят как валидация (проверка) данных, так и документирование последовательности ответственного хранения (chain of custody), включающее отслеживание изменений файлов при прохождении ими этапов обработки.

8.6 Проверка ESI

Проверка — элемент процесса э-раскрытия, в рамках которого основное внимание уделяется отсеву электронной информации на основе определенных критериев. Соответствующие критериям представления (раскрытия) документы отделяются от тех документов, которые им не соответствуют.

Существует широкий спектр подходов к проведению проверки, начиная от традиционного последовательного ручного анализа и заканчивая более современными подходами, в которых широко применяются развитые инструменты и методы поиска и извлечения информации. Настоящий стандарт разработан таким образом, чтобы быть применимым ко всем таким подходам.

8.7 Анализ ESI

Анализ электронной информации — элемент процесса э-раскрытия, в рамках которого решается задача применения к электронной информации различных инструментов и методов с целью сбора сведений, которые могут быть использованы для достижения целей каждого из отдельных элементов процесса э-раскрытия. В этом плане, анализ — это деятельность, которая может осуществляться в поддержку любого из итеративно выполняемых элементов процесса э-раскрытия (выявления, обеспечения сохранности, сбора, обработки, проверки и представления).

Существует широкий спектр инструментов и методов, которые могут применяться для целей анализа. Какой именно инструмент или метод подходит в каждом конкретном случае, может зависеть от элемента процесса э-раскрытия, в поддержку которого ведется анализ данных, и от конкретного вопроса, для получения ответа на который проводится анализ данных.

8.8 Представление ESI

Представление — элемент процесса э-раскрытия, в рамках которого сторона готовит файлы для передачи другим сторонам. Процедуры подготовки данных для представления обычно согласовываются при первоначальном планировании проекта.

Данные могут быть представлены в электронном или бумажном форматах, в зависимости от соглашений, заключенных между сторонами. Форматы представления могут варьироваться и включать комбинацию первоначальных (native), близких к первоначальным (near-native), форматов полученных при сканировании бумажных документов графических образов, а также физических бумажных форматов. При подготовке данных к представлению следует принять во внимание технические возможности, которыми располагает получатель данных. Они могут включать в себя имеющиеся возможности и инструменты для просмотра и анализа, представленных данных их получателем. Часто рассматриваются соображения относительно затрат, основанные на объемах данных и формате их представления, с целью ограничения этих затрат.

Как и во многих других элементах процесса э-раскрытия, необходимо уделять внимание документированию представленных файлов и ведению списков файлов, исключенных из представления ввиду наличия привилегированных сведений (privilege logs). Эта документация служит для предоставления детальных сведений о том, какие файлы были представлены, а какие — изъяты.

9 Дополнительные соображения

9.1 Демонстрация ESI

Хотя демонстрация сохраняемой в электронном виде информации не рассматривается как элемент процесса э-раскрытия, важно понимать, каким образом эта информация в конечном итоге может быть использована в ходе судебного спора или расследования (например, представлена в суде).

Демонстрация электронной информации может оказаться проблемой для адвокатов и юристов. В прошлом документальные доказательства демонстрировались в бумажной форме, что и сегодня по-прежнему делается во многих случаях. Благодаря развитию технологий за последнее десятилетие, упростилась демонстрация электронных доказательств в «бумагоподобном» (near-paper) формате

графических образов. В связи с особенностями сохраняемой в электронном виде информации и расширением масштабов представления документов в первоначальных или близких к первоначальным форматах в некоторые случаях теперь требуется, чтобы юридическая группа демонстрировала доказательства в их первоначальном формате.

9.2 Происхождение и непрерывная последовательность ответственного хранения

В зависимости от рассматриваемого вопроса, может быть важно отследить или установить информацию о создании, истории изменений, воздействиях, владении и иные сведения о происхождении (provenance) или «родословной» (lineage), связанные с электронной информацией. Часть такой информации может содержаться в метаданных или может быть создана в рамках процесса э-раскрытия. Эти сведения о происхождении могут сыграть ключевую роль при выработке обоснованных суждений о качестве, целостности и аутентичности электронной информации.

В некоторых случаях сведений о происхождении недостаточно для подтверждения качества, целостности и аутентичности. В таких случаях (например, в ходе уголовных расследований или судебного преследования) необходима формальная хронологическая документация, отражающая владение, контроль, передачу и уничтожение электронной информации. Важно понимать, в каких случаях требуется доказать наличие непрерывной последовательности ответственного хранения (chain of custody), и обеспечить выполнение этих требований.

Библиография

[1] ISO Guide 73, Risk management — Vocabulary (Менеджмент риска. Термины и определения)

[2] ISO 15489-1:2016, Information and documentation — Records management (Информация и документация. Управление документами. Часть 1. Понятия и принципы)

[3] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

[4] ISO/IEC 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (Информационная технология. Методы и средства обеспечения безопасности. Руководство по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме)

[5] ISO/IEC 27040:2015, Information technology — Security techniques — Storage security (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность хранения данных)

[6] ISO/IEC 27041, Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (Информационные технологии. Методы и средства обеспечения безопасности. Руководство по обеспечению пригодности и адекватности метода расследования инцидентов

[7] ISO/IEC 27042, Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по анализу и интерпретации электронных доказательств)

[8] ISO/IEC 27043, Information technology — Security techniques — Incident investigation principles and processes (Информационные технологии. Методы и средства обеспечения безопасности. Принципы и процессы расследования инцидентов)

[9] ISO/IEC 29100, Information technology — Security techniques — Privacy framework (Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности)
http://protect.gost.ru/document1.aspx?control=31&baseC=6&id=186203

[10] ISO/IEC 38500, Information technology — Governance of IT for the organization (Информационная технология. Стратегическое управление ИТ в организации)

[11] Electronic Discovery Reference Model(EDRM), http://www.edrm.net

[12] Good practice guide to eDiscovery in Ireland, Version 1.0, 16 April 2013, http://www.eDiscoveryGroup.ie

[13] New York Bar Association, Best Practices in E-Discovery in New York State and Federal Courts, Version 2.0, December 2012, http://www.nysba.org

[14] Seventh Circuit Electronic Discovery Pilot Program — Final Report on Phase Two, May 2012, http://www.discovery-pilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pd

УДК 004.91 ОКС 35.030

Ключевые слова: управление документами, управление информацией, электронное раскрытие, информационная безопасность

БЗ 8—2019/164

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

Сдано в набор 03.10.2019. Подписано в печать 15.10.2019. Формат 60×84¼. Гарнитура Ариал
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

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