ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 18829-

Управление документооборотом

ОЦЕНКА ВНЕДРЕНИЙ ECM/EDRM

Достоверность

(ISO 18829:2017, IDT)

Document management — Assessing ECM/EDRM implementations — Trustworthiness

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
ФГБУ «Институт стандартизации»
2023

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») и Общество с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») на основе собственного перевода на русский язык англоязычной версии международного 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__ _____ 202_ г. № ____

4 Настоящий стандарт идентичен международному стандарту ИСО 18829:2017 «Управление документооборотом. Оценка внедрений CM/EDRM. Достоверность» (Document management — Assessing ECM/EDRM implementations — Trustworthiness, IDT)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

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

Настоящий документ предлагает методологию для организаций, стремящихся оценить, соответствует ли их ECM-среда ключевым концепциям доверенности и надёжности информации, определенным в ГОСТ Р 54471-2011 / ISO/TR 15801:2009 и ИСО/ТО 22957.

В настоящее время от многих организаций требуется обеспечить безопасное и защищённое создание, хранение и в конечном итоге уничтожение их относящейся к деловой деятельности сохраняемой электронным в электронном виде информации (ESI), с целью обеспечить аутентичность и точность электронной информации, а также безопасность и надежность организации.

Данный документ определяет виды деятельности и операции, которые организация должна выполнить, чтобы:

— обеспечить, чтобы вся сохраняемая в электронном виде информация (ESI) создавалась и поддерживалась надежным и доверенным образом на всём протяжении её жизненного цикла, и

— провести оценку имеющихся ECM-систем управления корпоративным контентом и/или EDRM-систем управления электронными документами и контентом на соответствие применимым стандартам ИСО.

Стандарты ГОСТ Р ИСО 15489-1-2019, ГОСТ Р 54471-2011 / ISO/TR 15801:2009 и ISO/TO 22957 содержат рекомендации для организаций по проектированию их ECM-систем управления корпоративным контентом; однако от организаций может также потребоваться представление проверяемых доказательств того, что эти системы обеспечивают безопасную среду для сохраняемой в электронном виде информации, соответствующую всем юридическим, техническим и политическим обязательствам организации и применимым стандартам ИСО.

Любое надежное и доверенное ECM/EDRM-решение должно быть в состоянии проходить аудит с воспроизводимыми результатами. Также необходим метод независимой проверки заявлений поставщиков программного и аппаратного обеспечения о том, что информация защищена и хранится надежным образом. Организациям необходимо будет позаботиться о том, чтобы их поддерживающая документация отражала эти требования.

Если стандартизированные ECM-решения с большой вероятностью поддаются аудиту и могут быть легко проверены, то нестандартные и/или проприетарные решения

для хранения информации могут не обеспечивать наличия всей необходимой контрольной информации в журналах аудита, и провести независимую проверку заявлений поставщиков о безопасности ECM/EDRM-решений может быть сложно. Независимо от того, является ли технология хранения стандартизированной или проприетарной, организация сталкивается с необходимостью быть в состоянии провести проверку соответствия ECM/EDRM-решения всем применимым требованиям.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Управление документооборотом

ОЦЕНКА ВНЕДРЕНИЙ ECM/EDRM

Достоверность

Document management — Assessing ECM/EDRM implementations — Trustworthiness

Дата введения –

1 Область применения

В настоящем документе описаны действия и операции, которые организация должна выполнить для того, чтобы оценить, поддерживается ли и поддерживалась ли ранее сохраняемая в электронном виде информация (electronically stored information, ESI) в надежной и доверенной среде (средах). В этих средах используются технологии управления контентом и документами, обычно известные как «системы управления корпоративным контентом» (ECM-системы - enterprise content management, ECM) или как «электронные системы управления документами и информацией» (electronic document and records management, EDRM; в России также используются термины «система электронного документооборота» (СЭД), «система управления документами» (СУД) и им подобные), обеспечивающее исполнение утвержденных организациями политик управления документами и указаний по срокам их хранения.

Хорошие практики, связанные с внедрением доверенных сред управления документами и контентом, описаны в таких документах, как стандарты ГОСТ Р 54471-2011 / ISO/TR 15801:2009 и ГОСТ Р ИСО 15489-1-2019. Тем не менее, необходим также стандарт, описывающий методологию для оценки данных типов сред управления документами и контентом независимо от того, какие технологии в настоящее время используются организацией. Настоящий документ устанавливает методологию оценки, которой следует придерживаться для определения уровня соответствия организации указанным выше стандартам в плане обеспечения надежности и достоверности информации, хранящейся в этих средах.

Настоящий документ применим в отношении уже существующих или планируемых ECM-систем. Установление факта наличия надежной доверенной системы является важным шагом в документировании надежности сохраняемой в электронном виде информации, поддерживаемой в рамках этой системы или среды.

Данный документ предназначен для использования организациями, оценивающими степень доверия к существующим средам управления документами и контентом. В нём указаны все обязательные виды деятельности и области, которые необходимо изучить с привлечением лиц, имеющих детальные технические и эксплуатационные знания о конкретных изучаемых технологиях и методологиях, а также понимание процессов и действий в области управления документами.

2 Нормативные ссылки

Ссылки на перечисленные ниже стандарты приводятся в тексте таким образом, что их содержание полностью или частично представляет собой требования настоящего документа. Для датированных ссылок применима только та редакция, которая упомянута в тексте. В случае недатированных ссылок необходимо использовать последнюю редакцию документа (включая опубликованные поправки).

ИСО 12651-1 «Управление электронным контентом – Словарь – Часть 1: Управление электронными графическими образами документов» (Electronic document management - Vocabulary - Part 1: Electronic document imaging), см. https://www.iso.org/standard/54755.html *и https://www.iso.org/obp/ui/#!iso:std:54755:en*

ГОСТ Р ИСО 15489-1-2019 «Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы», https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&id=232615

3 Термины и определения

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации, расположенные по следующим адресам:

Платформа ИСО для онлайн-просмотра материалов по стандартам (Online Browsing Platform, OBP) доступна по адресу https://www.iso.org/obp/ui

База данных МЭК «Электропедия» (IEC Electropedia) доступна по адресу http://www.electropedia.org/

Для целей настоящего документа применяются термины и определения, данные в ИСО 12651-1 и ГОСТ Р ИСО 15489-1-2019, а также следующие:

3.1 аутентичный документ (authentic record)[1]: документ, в отношении которого может быть доказано, что он:

a) является именно тем, чем претендует быть;

b) был создан или послан именно тем действующим лицом, которое указано в качестве его создателя или отправителя;

c) был создан или послан именно в то время, которое в нём указано.

3.2 документация по деловой практике, BPD-документация (business practice documentation, BPD): подробная документация[2] по деловым процессам, описывающая процессы, политики и процедуры, которым следует организация, и в том числе то, как информация поступает, хранится и управляется.

Примечание 1 – Документация по деловой практике содержит достаточные сведения, позволяющие организации установить или удостоверить, что содержащаяся в электронной системе управления документами/контентом электронная информация является точной, надежной и заслуживающей доверия.

Примечание 2 – В некоторых прикладных областях данную документацию называют мастер-руководством по процедурам (master procedure manual).

3.3 сохраняемая в электронном виде информация (electronically stored information, ESI) : информация, которая создается, используется и хранится в электронной форме, и для доступа к которой требуется компьютер или иное устройство[3].

---

1 Более «человечное» определение можно найти в отчёте ARMA International TR30-2017 «Внедрение Общепринятых принципов делопроизводства GARP» (Implementing the Generally Accepted Recordkeeping Principles), п.2, см. https://www.arma.org/store/viewproduct.aspx?id=20218809 , где сказано «Аутентичность (authenticity) - совокупность качеств документа, устанавливающая его происхождение, надёжность, достоверность (trustworthiness) и корректность его содержания» - *прим. переводчика*

2 По тексту оригинала говорится то об одном «документе», то о «документации». Представляется, что термин документация (т.е. один или несколько документов) лучше соответствует реальной практике – *прим. переводчика*

3 В стандарте ГОСТ Р ИСО/МЭК 27050-1-2019 «Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации», п.3.9, предлагается несколько иное определение: «Сохраняемая в электронном виде информация (Electronically Stored Information, ESI): Данные или информация любого вида и из любого источника, свиде-

Примечание 1 – Для целей настоящего документа, понятие сохраняемой в электронном виде информации охватывает документы и контент, созданные и/или управляемые организацией в ходе её деловой деятельности. Электронные данные, содержащиеся в реляционных базах данных, и специализированные прикладные наборы данных не считаются частью изучаемой в процессе проведения данной оценки сохраняемой в электронном виде информации.

3.4 читаемость (readability): способность системы с течением времени точно, согласованным образом воспроизводить сохраненную информацию без каких-либо изменений в первоначальном контенте, которые бы существенно изменяли то, что было изначально сохранено.

3.5 надежный[4] (reliable): свойство документа/контента, отражающее доверие к тому, что он является полным и точным представлением подтверждаемых им операций, действий или фактов, и возможность положиться на него в ходе последующих операций или действий.

3.6 заслуживающий доверия, достоверный (trustworthy): документ/контент, сохраняемый в электронном виде таким образом, который поддерживает во времени его целостность, точность, надежность и пригодность к использованию / читаемость[5].

Примечание 1 – См. ГОСТ Р 54471-2011 / ISO/TR 15801:2009.

4 Оценка доверенных ECM-систем

4.1 Общие положения

4.1.1 Результаты оценки

тельством существования которых в определенный момент времени является их сохранение в/на каком-либо электронном носителе информации» - *прим. переводчика*.

4 В переводах ВНИИДАД reliable обычно переводится как «достоверный» - так же, как и более широкий термин authoritative. Например: «Достоверным является документ: a) содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов; b) которому можно доверять в последующих операциях или в последующей деятельности» [ГОСТ Р ИСО 15489-1-2019, п. 5.2.2.2] - *прим. переводчика*

5 В данном определении в оригинальном стандарте ИСО пропущено ключевое по важности качество – аутентичность. Следует также отметить, что в документах профильного технического подкомитета ИСО по вопросам управления документами TC46/SC11 вместо термина trustworthy в том же смысле используется термин authoritative («авторитетный»), который в ГОСТ Р ИСО 15489-1-2019 переведен как «достоверный» - *прим. переводчика*

Доверенные ECM-системы должны обеспечивать возможность надёжного воспроизведения управляемой ими информации и предотвращать несанкционированные модификации и изменения контента и взаимосвязанных с ним метаданных. Это касается любой сохраняемой в электронном виде информации (ESI), созданной в разнообразных офисных приложениях, использующих внешние источники для «пополнения» контента/документа, когда тот создаётся и/или распечатываются / сохраняются, как это сочтёт уместным организация.[6]

Результаты такой стандартизированной оценки должны включать подробный отчет, содержащий достаточную информацию, позволяющую организации определить, как лучше всего корректировать те аспекты, в которых, как было установлено, не было полного соответствия требованиям. Данный отчет также должен включать, наряду с подробным описанием технологии (где это уместно), рекомендации и связанные с управлением контентом/документами политики и процедуры, которые необходимы для достижения полного соответствия требованиям.

Ключевым элементом настоящего стандарта оценки является предоставление организации подробной информации, касающейся общей надежности и доверенности их ECM-среды, - вместе с рекомендациями о том, как исправлять те аспекты, которые, согласно результатам оценки, не соответствуют требованиям стандартов, относящихся к управлению корпоративным контентом (ECM) и документами.

По завершении любой оценки, соответствующей стандарту ISO 18829, проводившая оценку группа специалистов (далее – группа оценки) должна подготовить подробный отчет, содержащий, как минимум, следующее:

- деловые потребности и/или деловое обоснование. Данный раздел отчета должен включать описание использованных процессов оценки документов, краткое изложение установленных фактов и результатов анализа в отношении физических и электронных документов, а также выявленные в ходе оценки проблемные вопросы, имеющие отношение к деловой деятельности;
- аналитический раздел, содержащий подробные сведения, увязанные с четко определённым набором объективных принципов управления документами и информацией, нацеленных на формирование для документации измеримой, последовательной информационной структуры, полностью лишённой инди-

6 Здесь речь идёт о формировании документов, прямо подгружающих, использующих или ссылающихся на внешние ресурсы (элементы текста, изображения, шрифты, мультимедийные объекты и т.п.) – *прим. переводчика*

видуальной и организационной предвзятости. Данные принципы, ранее известные как «Общепринятые принципы делопроизводства» (Generally Accepted Recordkeeping Principles, GARP[7]), сейчас рассматриваются в отрасли управления документами как те «Принципы», которые определяют очень конкретные уровни зрелости программы управления документами[8];

- раздел анализа пробелов в технологиях, содержащий описание всех используемых в настоящее время организацией соответствующих технологий управлению корпоративным контентом и документами, и иных технологий хранения и создания, имеющих отношение к контенту/документам;
- раздел с техническими и касающимися документов рекомендациями. Данный раздел должен включать рекомендации, связанные с изменением существующего положения дел в управлении документами с целью создания надежной и доверенной ECM-среды.

4.1.2 Анализ процессов

Любая оценка доверенных ECM-систем должна начинаться с анализа процессов и процедур, имеющих отношение ко всей среде, в рамках которой осуществляется управление сохраняемой в электронном виде информацией. Сюда входит анализ не только фактических процессов и процедур, но и документации по деловой практике (BPD-документации). Следует провести оценку следующего:

- как документы, контент и/или информация вводятся в систему (т.е. как физические материалы преобразуются в электронный формат, как поступает и обрабатываются существующая электронная информация и т.д.);
- как система управляет, осуществляет аудит и защищает электронную информацию; и

---

7 Речь идёт о принципах, разработанных международной ассоциацией специалистов по управлению документами ARMA International, см. https://imageadvantage.com/wp-content/uploads/2011/01/GARP.pdf . ARMA в 2017 году опубликовала отчёт TR 30-2017 «Внедрение Общепринятых принципов делопроизводства GARP» (Implementing the Generally Accepted Recordkeeping Principles, см. https://www.arma.org/store/viewproduct.aspx?id=20218809), о котором см. также пост http://rusrim.blogspot.com/2017/09/arma-international.html . Упомянутый отчёт, помимо прочего, включает в себя полный текст «Модели зрелости для полномасштабного/стратегического управления информацией» (Information Governance Maturity Model). – *прим. переводчика*

8 Данные принципы, действительно, пользовались большим авторитетом у замечательного предыдущего поколения американских специалистов по управлению документами, которое к данному моменту практически полностью ушло. Представители нового поколения такого пиетета к «Принципам» и к основанной на них модели зрелости уже не питают – *прим. переводчика*

- как система (включая оборудование) обеспечивает безопасность хранения информации, предотвращая несанкционированное изменение, модификацию и/или удаление.

Если доступна документация по деловой практике, то следует проверить соответствие существующих процессов и процедур этой документации с целью установления факта соответствия и/или определения требующих улучшения аспектов, включая анализ:

- того, как будут исполняться все процедуры управления корпоративным контентом;
- того, как осуществлялись и/или осуществляются импорт/сканирование, индексирование и проверка информации;
- того, как осуществлялась и/или осуществляется защита системы от несанкционированного доступа;
- того, как осуществлялась и/или осуществляется защита контента от несанкционированной модификации или изменения;
- того, как осуществлялось и/или осуществляется управление авторизованным внесением изменений в контент/документы, включая выполнение требований к сохранению контрольной информации в журналах аудита и к обеспечению возможности извлечения любой предыдущей версии контента/документа;
- того, как осуществлялось и/или осуществляется сохранение и управление примечаниями и аннотациями (если таковые имеются), если они являются частью деловой документации; и
- того, какие меры и средства контроля и управления используются системой для установления и отслеживания сроков хранения для всей сохраняемой в электронном виде информации в соответствии с утверждёнными указаниями по срокам хранения документов.

Если используется развёрнутое на внешнем сервере решение и/или внеофисные (в т.ч. облачные[9]) компоненты, не находящиеся под непосредственным контролем организации как ответственного хранителя, то группа оценки должна также провести анализ степени соответствия требованиям стандарта ISO 17068:2017 «Информация и до-

9 Вставлено при переводе – в настоящее время несколько более широкая тема внеофисного хранения практически перестала обсуждаться, т.к. её заменила чуть боле узкая, но гораздо более востребованная тема облачного хранения – *прим. переводчика*

кументация – Хранилище электронных документов доверенной третьей стороны»[10]. ISO 17068 содержит подробные сведения и рекомендации, касающиеся требований к поставщикам услуг внеофисного (облачного[11]) хранения, процедур и соглашений с поставщиками, которые следует принять во внимание перед передачей контента на хранение в не находящуюся под полным контролем организации внешнюю среду.

Если документация по деловой практике неполна или отсутствует, то вслед за проведением оценки может последовать создание такой документации. Документация по деловой практике является обязательным компонентом любой надежной и доверенной среды. Хотя создание этой документации уже после того, как среда была запущена в промышленную эксплуатацию, чревато риском того, что доверие к уже имевшейся в системе информации может быть поставлено под сомнение, - тем не менее, для добавляемой впоследствии информации соответствующие процессы должны быть четко задокументированы.

Исполнение законодательно-нормативных требований

От организаций, на которые распространяются законодательно-нормативные требования в отношении сохраняемой в электронном виде информации, может потребоваться подтверждение целостности и подлинности электронной информации в даваемых под присягой показаниях. Поддержание четко сформулированных политик и процедур, документации по деловой практике, а также наличие заверенных журналов аудита, подробно отражающих то, как была собрана и упорядочена электронная информация, будет иметь решающее значение для установления аутентичности сохраняемой в электронном виде информации.

4.2 Действия в рамках проведения оценки

4.2.1 Анализ документации по существующей деловой практике и иной документации организации

Группа оценки должна изучить ранее разработанную документацию по деловой практике (BPD-документацию) с тем, чтобы последовательным образом объяснить

10 Речь идёт о стандарте ISO 17068:2017 «Информация и документация – Хранилище электронных документов доверенной третьей стороны» (Information and documentation - Trusted third party repository for digital records, см. https://www.iso.org/standard/66760.html и https://www.iso.org/obp/ui/#iso:std:iso:17068:ed-1:v1:en); о нём также см. пост http://rusrim.blogspot.com/2017/11/iso-170682017.html . В России данный стандарт не адаптировался – *прим. переводчика*

11 Вставлено при переводе – *прим. переводчика*

взаимосвязь между различными политиками и процедурами организации, оказывающими влияние на хранение электронной информации.

Группой оценки должна быть проанализирована каждая из областей, охватываемых названными в BPD-документации политиками и процедурами, с тем, чтобы определить, были ли эти политики и процедуры (наряду с аппаратным обеспечением, носителями информации и программным обеспечением для управления контентом/документами) реализованы в соответствии с принципами проектирования, описанными в ISO/TR 22957 [3], ГОСТ Р 54471-2011 / ISO/TR 15801:2009 и ГОСТ Р ИСО 15489-1-2019. Если документация по деловой практике неполна или отсутствует, то группа оценки должна провести оценку аспектов ECM-системы, сосредоточив внимание на политиках и процедурах, связанных с тем, как осуществляется захват информации, управление ею и обеспечение её безопасности.

Кроме того, группа оценки должна проанализировать, каким образом в организации осуществлялось информирование о политиках и процедурах и ознакомление с ними, в том числе посредством программ обучения; и убедиться в знакомстве с ними лиц, ответственных за внедрение или обеспечение исполнения данных политик.

В частности, даже в случае отсутствия документации по деловой практике, группа оценки должна дать оценку всех политик и процедур, реализованных в соответствии с принципами, сформулированными в ГОСТ Р 54471-2011 / ISO/TR 15801:2009 и ISO/TR 22957 в отношении надежной и доверенной ECM-системы. Хотя терминология в этих документах слегка различается, однако лежащая в основе ключевых видов деятельности концепция одинакова.

Хотя выбор названий и/или наличие определённых политик или процедур зависит от конкретной деловой операции, ожидается, что группа оценки получит и проанализирует политики и процедуры, перечисленные в п.4.2.2.

4.2.2 Оценка включаемой в систему информации

Общие положения

Группа оценки должна подробно проанализировать процессы, связанные с импортом изначально-электронных данных и конвертированной из аналоговых форматов информации. Используемые для создания сохраняемой в электронном виде информации процессы импорта, миграции и/или конверсии должны быть детально проанализированы, с тем, чтобы обеспечить доступность для поиска и извлечения всеми конечными пользователями по их запросу всей импортированной/конвертированной и про-

индексированной информации (в соответствии с документацией по деловой практике, если таковая существует - в противном случае документацию по деловой практике необходимо разработать; см. 4.1.1).

Группа оценки должна подготовить тестовые сценарии, в рамках которых общее количество импортированных и/или конвертированных страниц и документов может быть сопоставлено и проверено в сравнении с объёмом информации в первоначальных форматах и структурах.

Конверсия данных из аналогового формата в электронный формат

Группа оценки должна оценить, каким образом контент был подготовлен для проведения его конверсии и как организация обеспечила конверсию всех документов, примечаний и т.д. из аналогового формата в формат сохраняемой в электронном виде информации в соответствии с документацией по деловой практике. Такая оценка должна включать проверку соблюдения пользователями процессов и процедур; а также выявление процессов и процедур, которые не соответствуют международным стандартам и передовой практике.

Захват изначально-электронных материалов

В этом подразделе рассматривается захват изначально-электронных данных и их хранение в оцениваемой ECM-среде/решении. Группа оценки должна оценить процесс, используемый для захвата данных с внешних носителей информации, чтобы установить следующее:

- используемый процесс обеспечивает, чтобы все данные, которые предполагалось сохранить в надежном и доверенном ECM-решении, действительно были захвачены, проиндексированы и сохранены в соответствии с тем, как это описано в политиках и процедурах;
- процесс, используемый для выявления дублирования данных и/или их репликации между пользователями, у которых может иметься несколько копий одного и того же документа;
- процесс, используемый для конверсии любого существующего контента из устаревших или проприетарных форматов; и то, как пользователь/группа миграции обеспечили конверсию всех соответствующих данных без потери их достоверности и читаемости, одновременно обеспечив конверсию всей «су-

щественной» информации в соответствии с документацией по деловой практике.

В отношении данных, для которых потребовалось проведения конверсии, в случае, если определённая информация была потеряна из-за неспособности инструмента конверсии провести конверсию в соответствии с документацией по деловой практике, - группа оценки должна проверить, сохранили ли пользователь/группа миграции также и исходные данные в их первоначальном формате для исторических целей.

Группа оценки должна выявить и проверить процессы, используемые в ходе ввода той электронной информации, для которой потребовалось проведение конверсии из иных форматов, в которых эта информация была первоначально получена.

4.2.3 Читаемость

Надежные и доверенные ECM-системы поддерживают концепцию читаемости сохраняемой в электронном виде информации. Читаемость – это способность системы с течением времени точно, согласованным образом воспроизводить сохраненную информацию без каких-либо изменений в первоначальном контенте, которые бы существенно изменяли то, что было изначально сохранено.

Группа оценки должна подготовить тестовые сценарии, используя процесс проверки читаемости образцов импортированной и/или конвертированной информации с использованием стандартизированных средств просмотра изображений/данных. Проприетарное и специализированное программное обеспечение для просмотра изображений/данных не должно использоваться для проверки читаемости сохраняемой в электронном виде информации, за исключением тех случаев, когда такое программное обеспечение является единственным имеющимся программным обеспечением для доступа к оцениваемой электронной информации. В последнем случае группа оценки должна, когда это возможно, оценить программное обеспечение для просмотра изображений/данных с точки зрения его доступности в будущем. Эти тестовые сценарии должны быть выполнены системой, а выходные данные для выборки сохраняемой в электронном виде информации должны быть проверены группой оценки с целью:

- определить, имела ли место непреднамеренная модификация управляемой системой электронной информации;
- дать возможность группе оценки определись наличие различий контента исходного материала/документа в сравнении с его электронной версией;

- выявить, требуются ли какие-либо специализированные инструменты для извлечения/отображения информации, которые выполняют какую-либо интерполяцию или экстраполяцию данных, и/или
- определить, являются ли форматы/структуры сохраняемой в электронном виде информации стандартизированными, и какие именно стандарты используются.

4.3 Оценка процессов отслеживания сроков хранения информации, обеспечения её долговременной сохранности и уничтожения

4.3.1 Интероперабельность приложений

Оцените, дублируются ли используемые в ECM-системе метаданные между ECM-системами; могут ли они быть изменены или модифицированы таким образом, чтобы изменить доступность сохраняемой в электронном виде информации или воспрепятствовать доступу в будущем; и/или могут ли они привести к разным результатам в зависимости от того, какая система используется для поиска, хранения и/или извлечения сохраняемой в электронном виде информации.

Миграция данных между электронными носителями информации

Оцените, как проводилась миграция информации в ECM-решение, включая процедуры, обеспечивающие неизменность электронной информации и соответствующих метаданных, в том числе файловых форматов, сжатия, метаданных и т.д. Оцените тип и уровень аудита, который был реализован в ходе миграции, и то, как организация определила, что вся электронная информация, которую предполагалось мигрировать, действительно была мигрирована в соответствии с документацией по деловой практике.

4.3.2 Конверсия форматов данных

Оцените процесс, который использовался для конверсии сохраняемой в электронном виде информации из первоначального формата в желаемый формат. Оцените методологию, используемую для обеспечения отсутствия потерь информации, а также процессную документацию по процедурам, выполняемым для осуществления конверсии.

4.3.3 Программа мониторинга носителей информации

Оцените технологию хранения, используемую для ESI-данных, а также всю документацию, касающуюся того, как обеспечивается защита хранимой информации в соответствии с применимыми международными стандартами, относящимися к надежным и доверенным средами хранения (ГОСТ Р 54471-2011 / ISO/TR 15801:2009, ISO/TR 22957 и т.д.).

4.3.4 Необратимое уничтожение / удаление данных

Оцените, каким образом организация обрабатывает запросы на уничтожение, а также формализованный процесс управления удалением сохраняемой в электронном виде информации, которая ECM-системой была помечена как требующая либо архивации во внешней системе, либо удаления после достижения этой электронной информацией конца её жизненного цикла.

Группа оценки должна проанализировать политику в отношении сроков хранения документов и контента и перечень видов документов с указанием сроков хранения и действий по их истечении, с тем, чтобы убедиться, что соответствующая электронная информация была идентифицирована, а модуль ECM-решения для отслеживания сроков хранения был настроен в соответствии с политикой и перечнем. Наряду с анализом этой информации, группа оценки должна проанализировать все версии перечней и политик в отношении сроков хранения, чтобы установить, являются ли изменения и обновления в них четко идентифицируемыми, и вся ли содержащаяся в ECM-решении информация управляется в соответствии с тем, как это установлено и задокументировано. Группе оценки также желательно проанализировать все процессы ручного управления документами, которые могут применяться в отсутствие (или вместо) автоматизированного процесса.

Кроме того, должна быть сделана оценка того, как исполнение указаний по срокам хранения и действий по их истечении (retention schedule) может быть приостановлено с целью исполнения процедур реагирования на запросы на выявление и представление электронных доказательств и/или политик приостановки уничтожения документов и информации в связи с судебными разбирательствами и расследованиями (litigation hold).

4.4 Безопасность системы

4.4.1 Связанная с безопасностью информация, подлежащая сбору и анализу

Группа оценки должна оценить политики и процедуры организации, установленные / реализованные в отношении доступа, захвата, управления и/или создания сохраняемой в электронном виде информации при одновременном сохранении её достоверности и надежности. В отношении информации, которая захватывается, управляется и защищается в ECM-системе, - группа оценки должна определить, захватываются ли сведения (история операций в журналах аудита), документирующие любые (как успешные, так и неудачные) попытки добавления, модификации или удаления сохраняемой в электронном виде информации на протяжении её жизненного цикла, наряду с отслеживанием истории иных аспектов активности пользователей.

Такая оценка должна включать анализ технической архитектуры, программного обеспечения ECM-системы, надежности носителей данных, - в том числе вопросы системной и сетевой безопасности, а также наличия в системе мер и средств контроля и управления, достаточных для предотвращения несанкционированного доступа как к системе, так и к хранящимся в ECM-среде хранения данным.

Группа оценки должна получить информацию от группы поддержки сети и/или от группы по инфраструктуре организации, чтобы оценить, каким образом сеть организации защищена от несанкционированного доступа, как электронного, так и физического. Кроме того, группа оценки должна оценить ECM-решение на предмет того, могут ли пользователи получить доступ к сохраняемой в электронном виде информации, к данным в базе данных или к иной связанной с ECM-решением информации за пределами предоставленных им прав доступа и/или надлежащих уровней допуска.

4.4.2 Защита информации с целью предотвращения несанкционированной модификации или удаления электронной информации

Этот шаг требует оценки функциональных возможностей для обеспечения безопасности как на уровне системы, так и на уровне документа/контента, с тем, чтобы определить, какие реализованы меры защиты для предотвращения несанкционированных модификаций или изменений сохраняемой в электронном виде информации. На уровне системы, группа оценки должна проанализировать выборки из существующей контрольной информации в журналах аудита и из запротоколированной истории операций. Журналы аудита и запротоколированная история операций должны содержать сведения о попытках входа в систему (как успешных, так и неудачных), а также о попытках доступа к данным (как успешных, так и неудачных).

На уровне документа/контента, сохраняемая в электронном виде информация должна храниться в ECM-решениях, сконфигурированных и настроенных таким образом, чтобы предотвращать несанкционированный доступ, модификацию или удаление, и вести журналы аудита, подтверждающие, что электронная информация не был изменена по сравнению с её первоначальной формой. Обеспечение невозможности несанкционированной модификации или изменения электронной информации после её ввода в систему является целью большинства организаций. Поскольку не все ECM-решения обеспечивают подобный уровень безопасности на уровне системы и/или документа/контента, и не все они могут быть настроены так, проектировалось/планировалось, необходимо в полной мере оценить решение в целом для установления соответствия как общим политикам и процедурам организации, так и политикам и процедурам по вопросам управления документами.

4.5 Оценка доступа к информации

4.5.1 Общие положения

Следует определить и задокументировать шаги, предпринятые для предотвращения несанкционированного доступа к ECM-системе. Например, размещение сохраняемой в электронном виде информации на сетевом диске даже в случае применения мер безопасности на различных уровнях может оказаться недостаточно безопасным, если будут возможен доступ к информации без регистрации сведений о нём в журнале аудита.

Группа оценки должна оценить, каким образом сохраняемая в электронном виде информация хранится в защищённой среде, где все операции доступа полностью протоколируются и отслеживаются, предотвращая доступ любого пользователя к данным с использованием непротоколируемых режимов/инструментов. Такая оценка должна включать анализ процесса, реализованного организацией для обеспечения сохранения на носителях информации по крайней мере двух экземпляров информации с использованием методов и оптимизаций, обеспечивающих своевременное создание точных копий информации на нескольких носителях. Информация не должна передаваться на носитель информации способами, которые могут приводить к распространению возникших при передаче ошибок в данных (например, путем создания копий в отсутствие строгого контроля целостности).

Оценка должна включать проверку ECM-системы с целью подтверждения того, что ошибки при передаче данных на все носители информации документируются, и что

существует механизм для своевременного исправления таких ошибок. Для всех носителей следует документировать сведения о фактах успешной и неуспешной записи электронной информации на носитель, включающие различные контрольные суммы или иные результаты побитного сравнения, если те были созданы/использованы носителем информации (или подсистемой хранения).[12]

Группа оценки должна подготовить тестовые сценарии, используя процесс проверки того, что электронная информация хранится в нескольких местах, и что при этом по крайней мере один экземпляр информации хранится с использованием технологии хранения, не допускающей никаких модификаций, изменений или удалений, которые были бы неподконтрольны системе управления документами и/или мерам и средствами контроля и управления доверенных ECM-систем. В этих тестовых сценариях должен использоваться процесс выделения выборки электронной информации, изучаемой с целью:

- определить, когда сохраняемая в электронном виде информация хранится на различных носителях информации;
- оценивать хранение электронной информации и протоколирование операций в системе;
- изучить возможность доступа к электронной информации в обход мер и средств контроля и управления, предоставляемых ECM-решением, и
- определить, может ли информация быть изменена или удалена с помощью иных средств, не охватываемых мерами и средствами контроля и управления, предоставляемыми ECM-решением.

4.5.2 Управление авторизованными модификациями

Общие положения

Признавая возможность наличия деловых причин для того, чтобы разрешать внесение модификаций и изменений, крайне важно чётко установить, что подобные ситуации являются исключением, а не правилом. Следует выявить политики и процедуры, которые нужно соблюдать в тех случаях, когда могут вноситься изменения, и выяснить, действительно ли они соблюдаются. В журнале аудита следует четко идентифи-

[12] Данный текст в его первоначальной редакции был написан ещё в то время (в 2012 году), когда хеши, усиленные электронные подписи, печати и отметки времени ещё не получили широкого распространения – отсюда и акцент на контрольных суммах – *прим. переводчика*.

цировать вносимое изменение, выполняющего изменение авторизованного пользователя и причину для внесения изменения.

Типы и классы документов и сведения о доступе к документам

Процессы и процедуры, связанные с тем, как документируются и поддерживаются таксономия и классификация сохраняемой в электронном виде информации, должны быть надлежащим образом проанализированы и проверены. Группа оценки также должна проверить, являются ли вносимые изменения и обновления четко идентифицируемыми, и вся ли содержащаяся в ECM-решении информация является доступной и извлекаемой после перевода ECM-решения в режим промышленной эксплуатации.

Ответственные хранители документов

Группа оценки должна проверить уровень подготовки и опытности ответственных хранителей документов с тем, чтобы определить, понимают ли они политики и то, как их следует применять.

4.6 Оценка процесса протоколирования истории операций

4.6.1 Общие положения

Демонстрация согласованности между декларированными политиками организации и влияющими на сохраняемую в электронном виде информация процедурами, связанными с использованием ECM-систем или систем управления документами, имеет критически-важное значение для установления точности сохраняемой в электронном виде информации, и это следует учитывать при ведении журнала аудита.

Например, если об информации в политиках сказано, что она хранится, управляется и уничтожается определённым образом, то неисполнение этих положений позволяет усомниться в том, что информация действительно хранится в надёжной и доверенной системе.

В частности, если в политике по срокам хранения и/или в перечне видов документов с указанием сроков хранения и действий по истечении этих сроков о процессе необратимого уничтожения (expunging) сказано, что все бумажные экземпляры и копии, и вся электронная информация должны быть «уничтожены» (или «удалены», «стёрты» и т.п.), но при этом сотрудники заявляют, что они или не знают, или не следуют описанному в политике и/или перечне процессу, - то утверждение организации о наличии надёжного и доверенного хранилища вызывает сомнения, поскольку можно доказать,

что организация не следует собственным процедурам в отношении обработки информации.

Кроме того, несоблюдение установленных политик может привести к значительным затратам организации на выявление, анализ и представление в ходе судебных разбирательств или проводимых контролирующими органами расследований всей той информации, которую в противном случае организация могла бы удалить из своей системы.

В подразделах 4.6.2–4.6.4 выделены различные аспекты протоколирования операций в системе и истории функционирования системы, которые группа оценки должна в полной мере оценить.

4.6.2 Извлечение предыдущей версии документа, которая подлежала сохранению

Если ECM-решение сконфигурировано и настроено таким образом, чтобы дать пользователям возможность хранить документы/контент с использованием мер и средств контроля и управления их версиями или редакциями, то в политике организации по срокам хранения и/или в перечне видов документов с указанием сроков хранения должно быть четко установлено, в каких случаях система должна автоматически удалять версии или редакции документа/контента после его окончательного утверждения.

Для организаций, которые считают целесообразным сохранять более ранние версии электронной информации, система должна предоставить механизм для поиска и извлечения предыдущих версий электронной информации. Система также должна протоколировать факт сохранения новой версии документа/контента.

Если организация использует меры и средства контроля и управления редакциями (уже после создания документа/контента в законченном виде) для отслеживания вносимых в документы/контент изменений, то система должна протоколировать факты сохранения новых редакций документа, наряду с фиксацией иной информации, такой как дата, время, причина пересмотра, выполнивший действие пользователь и т.д.

Группа оценки должна оценить, каким образом организация управляет версиями и/или редакциями документов/контента, если таковые используются в ECM-решении.

4.6.3 Управление примечаниями и аннотациями как составной частью деловых документов

В некоторых организациях и для некоторых типов документов/контента следует сохранять примечания и/или аннотации, обеспечивая для них тот же уровень защиты, что и для исходного документа/контента. Отделение примечания/аннотации от документа/контента, с которой те взаимосвязаны, например, посредством процесса разделения на слои (layering process), может не обеспечить достаточной защиты для того, чтобы считать, что примечание/аннотация хранится в надёжной и доверенной системе.

Необходима тщательная оценка методов хранения «многослойной» информации в контексте деловых потребностей. Требуется обеспечить связывание примечания/аннотации с исходным документом/контентом контролируемым образом.

Если организация использует примечания и/или аннотации в качестве элементов делового процесса, автоматизированного с использованием технологий управления потоками рабочих процессов (workflow), то группа оценки должна оценить процедуры, которым следует организация.

В число подлежащих оценке входят процессы и процедуры, связанные со следующим:

- как организация контролирует аспекты безопасности, связанную с тем, как осуществляется управление и хранение примечаниями и/или аннотациями;
- охвачена ли эта информация иными, отличающимися мерами по отслеживанию сроков хранения;
- как организация обеспечивает захват и управление ECM-системой достаточной контрольной (в журналах аудита) и исторической информацией, идентифицируя и протоколируя любые изменения в любых примечаниях и/или аннотациях, независимо от того, хранятся ли они как часть документа или как часть потока рабочих процессов.

При отсутствии в организации какой-либо формально утверждённой документации группа оценки должна оценить, посредством изучения архитектуры существующей ECM-системы и средств контроля и управления системного уровня, как в текущей ECM-среде осуществляются управление и защита данных этого типа. Группа оценки также должна представить рекомендации по обеспечению необходимых уровней контроля и управления.

Группа оценки должна оценить, как организация управляет примечаниями и/или аннотациями, если они используются в ECM-решении.

4.6.4 Управление электронной информацией, содержащей макросы и/или внешние ссылки

Традиционные представления о том, какие типы документов/контента могут храниться в ECM-системе, ограничивались офисными документами, сообщениями электронной почты, факсами и отсканированными документами. Быстро идущая интеграция большинства деловых приложений с офисными приложениями с целью создания документов и/или сообщений электронной почты требует, чтобы любая доверенная ECM-система поддерживала возможность сохранения экземпляра того, что было создано деловым приложением, в защищённом от изменений формате, таком как формат PDF или иной стандартизированный в отрасли формат.

Благодаря интеграции этих технологий, сохраняемая в электронном виде информация теперь обычно создается деловыми приложениями, включая те, что могут использовать «макросы» (которые, например, автоматически вставляют в поля документа текущую дату или другие данные), внешние ссылки на другие файлы во внутренней сети или даже ссылки на внешние документы, находящиеся за пределами организации (используя, например, URL-адрес в Интернете). Такая сформированная электронная информация затем обычно загружается в ECM-решение для последующего управления ею.

Группа оценки должна оценить, каким образом ECM-решение управляет:

- электронным контентом, созданным в деловых приложениях,
- электронным контентом, созданным с использованием «макросов» (т.е. встроенного в документ кода, который выполняется при его отображении или печати), и/или
- ссылками на другие документы/контент, внешние по отношению к ECM-решению.

4.7 Оценка технической среды и среды хранения данных

4.7.1 Модели информационной безопасности

Предотвращение несанкционированных изменений/удаления на протяжении всего жизненного цикла сохраняемой информации является критически-важной характеристикой надежной и доверенной ECM-системы. Группа оценки должна установить, обеспечивает ли модель информационной безопасности предотвращение изменений/удаления в течение жизненного цикла сохраняемой информации. Группа оценки

также должна изучить политики и конфигурацию информационной безопасности, чтобы установить, как минимум, следующее:

- обеспечивается полная защищённость и безопасность при любом доступе пользователей;
- протоколируются попытки доступа в систему неавторизованных пользователей;
- внешние каналы связи с системой шифруются; их использование допускается только авторизованными пользователями, применяющими VPN-решения с шифрованием или иные сетевые технологии, предотвращающие доступ к сохраняемой в электронном виде информации и/или её передачу способами, которые могут быть перехвачены;
- система конфигурируется и настраивается таким образом, чтобы реализовать управление доступом на основе ролевой модели, дающее возможность авторизованным пользователям получать необходимый доступ (который может включать права на чтение, на модификацию, и иные уровни доступа) к документам/контенту; и/или
- в надежной и доверенной ECM-среде только авторизованные пользователи могут добавлять/отбирать/модифицировать права и привилегии пользователей.

4.7.2 Оценка технологий хранения

Группа оценки должна изучить и оценить использование текущей системы хранения электронной информации. Оценка используемых технологий хранения/носителей информации должна включать анализ возможности изменить электронную информацию - например, используются ли перезаписываемые сетевые диски, применяются ли какие-либо варианты технологий однократной записи-многократного чтения (WORM), и проводится ли аудит технологий хранения.

Группа оценки должна оценить, можно ли получить доступ к сохраняемой в электронном виде информации в обход контролирующего её ECM-решения и можно ли получить доступ к электронной информации и/или модифицировать её без надлежащего протоколирования, отслеживания и применения мер и средств обеспечения безопасности; - а также определить, записывается ли несколько экземпляров информации, чтобы при этом как минимум один экземпляр хранился в не допускающим внесение изменений виде в течение всего жизненного цикла этой информации.

Если используется развёрнутое на внешнем сервере решение и/или внеофисные (в т.ч. облачные[13]) компоненты, не находящиеся под непосредственным контролем организации как ответственного хранителя, то группа оценки должна также провести анализ степени соответствия требованиям стандарта ISO 17068:2017 «Информация и документация – Хранилище электронных документов доверенной третьей стороны», в котором рассматриваются все соответствующие аспекты того, как ведёт свою деятельность поставщик услуг хостинга, как используются функциональные возможности решения и как обеспечивается управление / защита от несанкционированного доступа и/или модификации сохраняемой в электронном виде информации.

4.7.3 Технологические стандарты, которым следует организация

Группа оценки должна взять образцы сохраняемой в электронном виде информации для, выявления используемых форматов данных, с тем, чтобы установить, соответствуют ли форматы электронной информации отраслевым стандартам, а также стандартам сжатия. Исходя из этого оценивается пригодность к использованию и читаемость информации в будущем по мере продолжающегося изменения технологий.

4.7.4 Первичное и вторичное хранилища

Ключевым элементом концепции надежного и доверенного хранения является способность любой системы сохранять по меньшей мере два экземпляра/копии информации в безопасных, отдельно расположенных местах (которые рассматриваются как первичное или вторичное хранилища). Первичным, основным хранилищем считается местом хранения первого экземпляра сохраняемой в электронном виде информации, а вторичное хранилище - местом, где организация хранит её второй экземпляр. Группа оценки должна изучить технологии, используемые как первичным, так и вторичным хранилищами, с тем, чтобы установить, хранилась ли вся сохраняемая в электронном виде информация согласно политикам и процедурам, описанным в документации по деловой практике, и в соответствии с применимыми международными стандартами и законодательно-нормативными требованиями.

Группа оценки должна изучить различные места хранения данных, чтобы определить используемые организацией процессы, обеспечивающие, что:

---

[13] Вставлено при переводе – в настоящее время несколько более широкая тема внеофисного хранения практически перестала обсуждаться, т.к. её заменила чуть боле узкая, но гораздо более востребованная тема облачного хранения – *прим. переводчика*

- как минимум, две экземпляра информации хранятся в разных физических местах, и/или
- как минимум, один экземпляр информации хранится на носителе, который не допускает несанкционированных модификаций, изменений или удалений на протяжении жизненного цикла информации.

Приложение ДА

(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 15489-1:2016 «Информация и документация. Управление документами. Часть 1. Понятия и принципы» (Information and documentation - Records management - Part 1: Concepts and principles)	IDT*	ГОСТ Р ИСО 15489-1-2019 «Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы»
ISO 12651-1:2012 «Управление электронным контентом – Словарь – Часть 1: Управление электронными графическими образами документов» (Electronic document management - Vocabulary - Part 1: Electronic document imaging)	-	-
ISO 17068:2017 «Информация и документация – Хранилище электронных документов доверенной третьей стороны» (Information and documentation - Trusted third party repository for digital records)	-	-
ISO/TR 15801:2017 «Управление контентом - Информация, сохраняемая в электронном виде - Рекомендации по	IDT**	ГОСТ Р 54471-2011 / ISO/TR 15801:2009 «Системы электрон-

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
обеспечению достоверности и надёжности» Document management - Information stored electronically - Recommendations for trustworthiness and reliability)		ного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Ре-комендации по обеспечению до-стоверности и надёжности»
*IDT –- идентичный стандарт. ** в России адаптирована более ранняя редакция международного стандарта		

Библиография

[1] ISO/TR 15801:2017 «Управление контентом - Информация, сохраняемая в электронном виде - Рекомендации по обеспечению достоверности и надёжности» (Document management - Information stored electronically - Recommendations for trustworthiness and reliability), см. https://www.iso.org/standard/66856.html и https://www.iso.org/obp/ui/#!iso:std:66856:en . Стандарт адаптирован в России как ГОСТ Р 54471-2011 / ISO/TR 15801:2009 «Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надёжности», https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&id=179897

[2] ISO 17068:2017 «Информация и документация – Хранилище электронных документов доверенной третьей стороны» (Information and documentation - Trusted third party repository for digital records), см. https://www.iso.org/standard/66760.html и https://www.iso.org/obp/ui/#!iso:std:66760:en

[3] ISO/TR 22957:2018 «Управление контентом - Анализ, выбор и внедрение систем управления корпоративным контентом (ECM)» (Document management - Analysis, selection and implementation of enterprise content management (ECM) systems), см. https://www.iso.org/standard/71605.html и https://www.iso.org/obp/ui/#!iso:std:71605:en

УДК 004.912:004.932:006.354 ОКС 01.140.20

Ключевые слова: доверенные системы, информационная безопасность, СЭД, управление документами, управление контентом, управление информацией, ECM, оценка надёжности систем

Руководитель организации-разработчика
Общество с ограниченной ответственностью «ЭОС Тех»

Генеральный директор _____Е.П. Пушкарев

Руководитель разработки
к.и.н., Председатель Совета директоров, Председатель ПК 6 «Жизненный цикл электронного документооборота» ТК 459
_____В.Э. Баласанян

Исполнитель
к.и.н., ведущий эксперт по управлению документацией Общества с ограниченной ответственностью «ЭОС Тех», эксперт ИСО,
_____Н.А. Храмцовская