



## ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо зберігання і використання мікрофільмів та електронних носіїв інформації в сучасному інформаційному суспільстві.

У публікації «Пережиток прошлого: Николаевские депутаты возмутились значительным тратам на микрофильмирование документов» наведено особисту думку окремих депутатів щодо використання мікрофільмів для створення страхового фонду документації м. Миколаїв.

У публікації «СОМ – микрофильмирование в практике архивов» наведено порівняння використання мікрофільмів та електронних носіїв інформації в сучасному інформаційному суспільстві.

У публікації «Метод хранения цифровой информации на аналоговом носителе с использованием штрих-кодов» розповідається, що в сьогднішній ситуації мається у наявності величезний масив інформації в цифровому вигляді і, одночасно з цим, відсутні надійні технології її довготривалого зберігання. Розроблена технологія зберігання цифрової інформації в кодованому вигляді на мікрофільмі з використанням штрих-кодів дозволяє вирішити цю проблему.

У публікації «Уряд удосконалив порядок проведення перевірок у сфері страхового фонду документації» наведено Постанову від 08.11.2017 р. № 840, якою уряд України затвердив критерії, за якими оцінюється ступінь ризику від провадження господарської діяльності у сфері створення, формування, ведення і використання страхового фонду документації та визначив періодичність здійснення планових заходів державного нагляду.

У публікації «Конференция 2017 года секции деловых архивов Международного совета архивов: Какие проблемы будут для нас основными через 5 лет?» розповідається про конференцію. Наведено 5 головних проблем, з якими через п'ять років будуть стикатися ділові архіви.

У публікації «Польша: Подготовлен проект модернизации интегрированной архивной информационной системы ZoSIA» розповідається про модернізацію інтегрованої архівної інформаційної системи в Польщі.

У публікації «ИСО: Опубликован кодекс практики э-раскрытия» розповідається про видання стандарту ISO/IEC 27050-3:2017 «Информационные технологии – Методы обеспечения безопасности – Выявление и раскрытие электронной информации – Часть 3: Кодекс практики э-раскрытия».

У публікації «Европейский институт телекоммуникационных стандартов ETSI опубликовал технический отчет по исполнению Директивы по сетевой и информационной безопасности» розповідається про технічний звіт Європейського інституту телекомунікаційних стандартів ETSI TR 103 456 за темою «Реалізація положень Директиви про мережеву та інформаційну безпеку».

У публікації «ИСО: Обсуждается проект нового стандарта по технологиям и методам облачных вычислений» розповідається про включення в один документ технологій і методів які запропоновані користувачам на ринку хмарних сервісів.

У публікації «Новые международные стандарты и проекты стандартов в сфере облачных вычислений» наведено перелік проектів, включених до програми роботи технічного підкомітету зі стандартизації ISO / IEC JTC1 / SC38 «Хмарні обчислення та розподілені платформи».

У публікації «Франция: Компания Locarchives опубликовала «белую книгу» по надёжной оцифровке и последующему уничтожению оригиналов» розповідається про видання «білої книги», мета якої дати ясну інформацію для прийняття обґрунтованого рішення про знищення або подальше зберігання паперових оригіналів.

У публікації «ИСО: Опубликован стандарт ISO 17068:2017 «Хранилище электронных документов доверенной третьей стороны»» розповідається, що стандарт ISO 17068 встановлює вимоги до сховища довіреної третьої сторони в інтересах підтримки діяльності уповноваженої служби довіреного зберігання, з тим, щоб та могла забезпечити доказову цілісність і автентичність електронних документів клієнтів і служити джерелом надійних доказів. Наведено розділи, з яких він складається.

У публікації «ИСО: Опубликована новая редакция стандарта принципов управления метаданными документов» наведено особливості нової редакції стандарту.

У публікації «ИСО: Идёт работа над новой редакцией стандарта аутентификации объектов с использованием усиленной электронной подписи» наводяться особливості стандарту, згідно до якого аутентифікація об'єктів / сутностей проводиться згідно з вказаними 10 механізмами використання електронних цифрових підписів.

У публікації «Исследование: Ленточные, дисковые и облачные хранилища. Каковы реальные затраты?» наведено порівняльний аналіз використання стрічкових та дискових носіїв інформації та хмарних сховищ.



## **ПЕРЕЖИТОК ПРОШЛОГО: НИКОЛАЕВСКИЕ ДЕПУТАТЫ ВОЗМУТИЛИСЬ ЗНАЧИТЕЛЬНЫМ ТРАТАМ НА МИКРОФИЛЬМИРОВАНИЕ ДОКУМЕНТОВ**

Источник: <http://svidok.info/ru/news/2485>

В ходе заседания «бюджетной» комиссии депутаты рассматривали проект решения городского совета «Об утверждении Программы создания страхового фонда документации Николаева на 2017-2021гг.». Вопрос докладывал начальник управления по вопросам чрезвычайных ситуаций и гражданской защиты населения Александр Герасименя. В проекте говорится, что его целью является создание страхового фонда документации Николаева для ее долгосрочного и надежного хранения. Для этого основную информацию об объектах, в частности, схемы сетей, конструктивных элементов и т. д., микрофильмируют и закладывают в базу страхового фонда документации. Для каждого региона определен данный фонд. Так, микрофильмы по Николаеву будут изготавливаться и храниться в Южном региональном центре (г. Одесса). Объемы микрофильмирования в рамках программы составит:

- 33545 листов формата А4 для 62 объектов коммунальной собственности;
- 41182 формата А4 для 43 объектов хозяйственной деятельности других форм собственности.

После выступления докладчика у депутатов возникли вопросы о возможных вариантах формы подачи информации. Так, можно ли предоставлять ее не в виде микрофильмов, а на цифровых носителях. Но начальник управления ответил, что государство в данном вопросе выбора не предоставляет, регламентируя четкие правила.

*- На уровне законодательства определены центры, нас обслуживает Южный региональный центр страхового фонда документации, с которым мы согласовываем объекты, подлежащие закладке по количеству листов. Сам порядок регламентирован законом о страховых фондах. Это не мое желание, есть распоряжение, которое надо выполнять. Иногда требуется именно такой пакет документов, например, когда СБУ проводит свои мероприятия и т. д.*

Кроме того, по словам Герасимени, сейчас ГАСК не пропускает объекты на капремонт, если у них нет закладки документов в страховой фонд.

Но депутатов такой ответ не удовлетворил и они продолжили искать возможности для другой формы подачи документов.

Так, Вячеслав Апанасенко напомнил, что в горсовете планируется создание центральной серверной, на которой также будут размещены такие

системы, как «Безопасный город», а также предусмотрено электронное хранение информации. Депутат предположил, что было бы логично и страховой фонд документов хранить на этом сервере в электронном виде, а не использовать микрофильмирование.

Артем Грозов поддержал коллегу и предложил, чтобы юридический департамент посмотрел трактовку закона и сделал вывод, можно ли хранить данную информацию в цифровом формате на той же серверной. Кроме того, в горсовете есть специалисты по ай-ти технологиям, которым также можно поручить проработать этот вопрос и доложить выводы.

Интересовала депутатов и сумма, в которую распорядителям бюджетных средств выльется микрофильмирование необходимых документов. По словам Герасимени, цена одного листа формата А4 обойдется в 6 гривен. Члены комиссии тут же подсчитали, что на данные нужды уйдет около 500 тысяч гривен.

***- Хороший бизнес кто-то организовал, - отметили депутаты.***

В итоге глава комиссии Александр Бернацкий озвучил предложения от комиссии: обратиться в юрдепартамент горсовета и к ай-ти специалистам, чтобы к следующему заседанию комиссии они просмотрели возможность другой формы подачи данной информации. Александр Герасименя вызвался направить запрос в Южный региональный центр для обоснования именно такой формы хранения документов. Депутаты единогласно поддержали эти предложения.

Отметим, что микрофильмирование как форма хранения информации появилась в конце 50-х годов и получила новый виток развития в начале 90-х. Закон «О страховом фонде документации», которым регламентируется данный вопрос, был утвержден в 2001 году. Тогда микропленка в Украине была едва ли не единственным способом компактного хранения информации. Потому, с учетом скачка в развитии информационных технологий, произошедшего в последние несколько лет, претензии к форме подачи информации депутаты считают вполне обоснованными.



## **СОМ – МИКРОФИЛЬМИРОВАНИЕ В ПРАКТИКЕ АРХИВОВ**

Источник: <http://naar.ru/articles/sistemyi-tsifrovogo-mikrofilmirovaniya/>

Как обеспечить наилучшую сохранность документов? Хранение в бумажном виде недолговечно, а электронные копии документов технологически устаревают. На помощь придут системы цифрового микрофильмирования (СОМ), о которых расскажет генеральный директор ООО «Аргентум Диджитал» Юрий Беленький.

## **Введение**

Обеспечение сохранности исторического и культурного наследия народов нашей страны является одной из важнейших задач государства, без решения которой невозможно дальнейшее гармоничное развитие общества. Это в полной мере отражено в действующей в настоящее время Федеральной программе «Культура России», одним из базовых положений которой является задача страхового копирования редких и особо ценных культурных объектов, в частности, архивных дел и отдельных документов, книг, газет, карт, плакатов и других исторических и культурных ценностей, хранящихся в российских архивах. В данной программе прямо указан метод страхового копирования, которым является микрофильмирование, порядок отбора объектов для копирования и сдачи микрофильмов в Единый российский страховой фонд документации (ЕР СФД).

## **Постановка задачи**

Задачу архивов, хранящих сегодня документы национального и всемирного значения, можно определить как двуединую: во-первых, это создание условий для максимально долгого хранения оригиналов, представляющих большую культурную и историческую ценность, а, во-вторых, обеспечение возможности доступа к этим документам не только исследователей и специалистов, но и широкого круга общественности.

Обеспечение сохранности оригиналов документов подразумевает создание особых специальных условий их хранения (температура, влажность, освещенность и пр.), проведение необходимого комплекса реставрационных и профилактических работ, а также ограничение доступа к оригиналам и работы с ними. Все это, на первый взгляд, входит в прямое противоречие со второй важной функцией архивов, просветительской – обеспечением максимально возможного доступа широких масс населения к архивным фондам.

Данное противоречие решается посредством максимально бережного однократного копирования оригиналов и предоставления их копий для работы исследователей-профессионалов, а также всех желающих, заинтересованных в изучении национальной и мировой истории.

## **Анализ методов решения**

Традиционным методом копирования документов является микрофильмирование, которое начало интенсивно развиваться, начиная с 1950-х годов прошлого века, и продолжает широко использоваться в наши дни во всем мире. Классическое микрофильмирование является особой разновидностью фотографии и подразумевает следующие основные технологические операции:

- покадровая съемка оригиналов с помощью микрофильмирующей камеры;
- химико-фотографическая обработка проэкспонированных микроформ;
- контроль их качества;
- окончательный монтаж микрофильма;

- изготовление при необходимости копий микрофильма второго и третьего поколения.

Микрофильм как носитель информации обладает **уникальными свойствами**:

- доказанный срок хранения информации на микрофильме составляет сотни лет;
- копия документа, хранящаяся на микрофильме, непосредственно воспринимается человеком;
- микрофильм не подвержен таким внешним воздействиям как электрические и магнитные поля;
- микрофильм обладает предельно низкой себестоимостью использования, так как при высокой плотности записи информации занимает минимум площади и не требует создания особо жестких условий хранения.

Все эти и ряд других свойств микрофильма как носителя информации обусловили его повсеместное использования для создания СФД, обеспечивающего сохранность информации в долгосрочном плане даже в случае утраты оригиналов. **На сегодняшний день микрофильм как носитель информации не имеет альтернативы для обеспечения сохранности информации на период в сотни лет.**

Однако микрофильм имеет и ряд **недостатков**, ставших особенно очевидными в наши дни, когда потребность в информации должна удовлетворяться практически немедленно и независимо от того, в какой точке земного шара находится источник информации, и где находится ее потребитель. Действительно, современных пользователей не могут устроить следующие свойства микрофильма как носителя информации:

- Медленный доступ к информации. Для того, чтобы прочитать документ, микрофильм необходимо найти в хранилище, что при большом объеме хранения требует значительных затрат времени, далее его необходимо установить в читальный аппарат, найти нужный кадр, и только после этого прочитать документ.

- Проблемы тиражирования и рассылки. В любой момент времени только один человек может работать с конкретным микрофильмом. Для того чтобы расширить круг пользователей, необходимо изготовить определенное количество копий, что требует дополнительных затрат времени. Рассылка документов на микрофильмах осуществляется, по современным меркам, исключительно медленно (транспортные средства, почта).

Таким образом, *микрофильм можно охарактеризовать как исключительно надежное, но медленное средство хранения информации.*

В наши дни бурное развитие цифровых технологий и компьютерной техники предоставляет возможность хранить большие массивы информации в цифровом виде. Практически во всех крупных архивах мира создаются **электронные базы данных** документов, которые, по сути дела, представляют собой электронный фонд пользования. Хранение копий архивных фондов в электронном виде дает следующие возможности:

- максимально быстрый поиск информации и доступ к ней;

- практически мгновенное копирование и рассылку информации в любую точку земного шара с использованием Интернет.

**Проблемы хранения информации в цифровой форме** заключаются в другом:

- цифровая информация не воспринимается непосредственно органами чувств человека. Это особенно важно, когда мы имеем в виду период хранения данных в сотни и сотни лет. Уже сегодня носители цифровой информации, произведенные 20 лет назад, невозможно прочитать в связи с полной сменой парка аппаратных средств, а также программного обеспечения;

- высокая себестоимость хранения информации. Достаточно надежное хранение цифровой информации подразумевает ее обязательное копирование, внедрение и использование специальных программ, обеспечивающих постоянное тестирование базы данных, обеспечение других процедур, направленных на недопущение потери информации. Кроме того, в ситуации, когда полная замена аппаратных и программных средств происходит не реже одного раза за несколько лет, возникает необходимость постоянной закупки новых компьютеров, программ и перезаписи информации. При увеличении объема базы данных затраты на ее поддержание растут в геометрической прогрессии. **Все это приводит к тому, что хранение единицы информации в цифровом виде оказывается дорогим, по крайней мере, значительно дороже, чем хранение на микрофильмах;**

- подверженность внешним воздействиям, таким как электрические и магнитные поля, сбой электропитания и пр.;

- подверженность случайным или намеренным действиям человека. Все современные люди, пользующиеся компьютером, имеют собственный неприятный опыт, когда случайное нажатие клавиши приводило к удалению документа или его части. Безусловно, риск сильно увеличивается, когда мы работаем с объемной электронной базой данных, накапливаемой годами. Непрофессиональные или случайные действия при этом могут иметь катастрофические последствия. Не следует исключать также и злонамеренные действия, различного рода хакерские атаки, рассылки вирусов. К сожалению, миру известны случаи утраты больших электронных баз данных, произошедших в связи с этим.

Таким образом, *электронная форма хранения информации может быть охарактеризована как максимально быстрая, гибкая и оперативная, но дорогая и недостаточно надежная*, когда речь идет о хранении копий документов на протяжении сотен лет.

Оптимальное решение задачи, по мнению экспертного сообщества, заключается в создании **комбинированного хранилища информации**, сочетающего в себе плюсы обеих упомянутых выше технологий.

## Технологии хранения информации

### микрофильм

Срок жизни сотни лет

Воспринимается человеком непосредственно

Не подвержен внешним воздействиям

Низкая себестоимость хранения

Медленный доступ к информации

Проблемы копирования и рассылки

### цифровая

Быстрый доступ к информации

Быстрое копирование и рассылка

Не воспринимается человеком непосредственно

Высокая себестоимость хранения

Подверженность внешним физическим воздействиям

Подверженность воздействию человека

### СОМ-технология микрофильмирования

Можно ли ускорить и значительно повысить качество микрофильмирования, а также сделать этот процесс совместимым с цифровыми технологиями? На сегодняшний день этот вопрос решается положительно с помощью использования так называемых СОМ-систем (Computer Output Microfilming).

**СОМ-технология** предусматривает предварительное сканирование оригинала с последующим выводом полученного графического файла на микроформу (кадр рулонной пленки или кадр микрофиши). Последующая химико-фотографическая обработка микроформ, в зависимости, от их типа может производиться как отдельно, по «классическому» методу, так и автоматически внутри самой СОМ-системы.



Побочным продуктом СОМ-технологии являются **электронные образы документов**. Однако эти электронные образы можно использовать для пополнения электронного фонда пользования. С другой стороны, возможен и обратный процесс - использование уже имеющихся электронных ресурсов для создания страхового фонда на микрофильмах. Таким образом, внедрение СОМ-технологии в архивах для создания СФД отлично

встраивается в уже существующие информационные процессы и происходит в мягком режиме, без глобальных перестроек.

Какие же **преимущества** сулит внедрение СОМ-технологии?



## Argentum Digital

### Преимущества СОМ-технологии



- при работе с документом СОМ-процесс подразумевает только его **однократное сканирование**. Современные книжные сканеры, снабженные специальными книжными колыбелями для бережного обращения с оригиналом, LED-подсветкой, низкой по интенсивности и не содержащей ультрафиолетовой и инфракрасной составляющих, оказывают на оригинал гораздо меньшее влияние, чем микрофильмирующая камера с ее мощным световым потоком;

- **классическое микрофильмирование** ведется практически вслепую, и качество работы можно оценить только после проявки пленки. Если при этом оператор допустил ошибку, например, в расположении страницы в кадре или порядке кадров, ошибся при фокусировке и т.п., оригинал приходится частично или полностью переснимать, что дополнительно его травмирует и требует больших затрат времени. В СОМ-процессе все файлы можно предварительно проконтролировать, установить порядок их следования на печать, и результат будет именно таким, как задумано. Другими словами, СОМ-система позволяет проверить качество микрофильма до его создания, а не после, а качество микрофильма на выходе идеально;

- ряд серийно производимых СОМ-систем позволяют экспонировать пленку со **скоростью до 60 кадров/мин.**, что, безусловно, невозможно обеспечить при работе с микрофильмирующей камерой, которая, даже при самых простых оригиналах даст возможность микрофильмировать со скоростью не более 5-6 кадров/мин.;

- при классическом микрофильмировании для получения микрофильмов второго и последующих поколений используется аппаратура контактного копирования. Она сама по себе не дешева и требует **дополнительных расходов на сервис**, но, что особенно важно, качество последующих копий заметно ниже качества мастер-копии, т.е. читаемость документа снижается при его перекопировании. В СОМ-системах эта проблема полностью отсутствует, поскольку, имея набор файлов, выведенных на пленку в первый раз, вы можете, предварительно сохранив работу, повторить эту операцию многократно, получая микрофильмы с исходной читаемостью. При этом понятно, что дополнительного оборудования не требуется. Ясно также, что микрофильм, утраченный по какой-либо причине, может быть восстановлен максимально быстро и с прежним качеством, что подчас является неразрешимой проблемой при работе классическим методом;

- **СОМ-микрофильмирование не требует создания специальных условий в помещении**, где оно производится. Не нужно зашторивать окна, красить стены специально краской и многое другое. СОМ-системы эксплуатируются в обычных офисных помещениях со стандартным освещением. Это полностью снимает проблему высокой утомляемости операторов микрофильмирующих камер, которые постоянно испытывают большие физические и световые нагрузки. Таким образом, условия труда персонала существенно улучшаются. Кроме того, СОМ-системы гораздо компактнее микрофильмирующих камер и требуют намного меньшей площади помещения для их установки и обслуживания, они также характеризуются пониженным по сравнению с микрофильмирующими камерами энергопотреблением;

- СОМ-системы позволяют микрофильмировать **электронные документы, изначально не существующие на бумаге**, но представляющие ту или иную ценность. Это особенно важно в связи с резким увеличением электронного документооборота во всем мире в последние годы. Данная функция в принципе недоступна классической технологии микрофильмирования.

**Классическое микрофильмирование** с использованием микрофиш в настоящее время практически прекращено во всем мире, и соответствующие микрофильмирующие камеры серийно не производятся. Однако, в силу указанных положительных свойств, микрофиша как носитель информации продолжает быть популярной и широко используется в СОМ-процессе. СОМ-система SMA 105, представляющая собой систему фотографического типа и предназначенная для вывода электронных образов документов на форматную микрофишу, представляет собой законченное устройство,

реализующее процесс dry-to-dry. Подавая на вход файлы, пользователь на выходе получает готовые сухие микрофиши архивного хранения.



Это возможно благодаря встроенной проявочной машине, куда проэкспонированная микрофиша подается автоматически. Некоторые архивы исторически в качестве микроформ для долговременного хранения информации используют микрофиши. Надо отметить, что микрофиша является наиболее емким носителем.

При одинаковом объеме хранимой информации микрофиша занимает гораздо меньший физический объем по сравнению с рулонным микрофильмом. Именно это обстоятельство, а также простота поиска документа, является аргументом в пользу микрофиш.

Система не требует подачи воды и наличия канализации, т.к. использует готовые наборы герметично закрытых химикатов. После отработки химикатов они просто заменяются новыми. Эксплуатация СОМ-системы SMA 105 осуществляется в помещениях офисного типа, специальные требования к которым отсутствуют.

### **Опыт эксплуатации СОМ-систем**

На сегодняшний день мировой опыт эксплуатации СОМ-систем весьма велик. Они используются не только в архивах, но и в библиотеках, министерствах и ведомствах, банках, научных учреждениях, в коммерческих сервисных бюро и пр. по всему миру. В нашей стране практически СОМ-системы используются в повседневной работе с 2004 г. СОМ-технология внедрена в более 10 регионах и субъектах Российской Федерации.

СОМ-системы используются также в Казахстане и Украине. Целый ряд проектов внедрения СОМ-систем находится на стадии завершения.

### **Заключение**

СОМ-технологии за последние пятнадцать-двадцать лет практического использования во всем мире заслужили признание специалистов в связи с их идеальной встраиваемостью в концепцию создания параллельно двух фондов документов – электронного фонда пользования и страхового фонда на микроформах.

СОМ-системы являются полностью автоматическими устройствами. Будучи подключенными к локальной компьютерной сети, они практически выполняют функции фотопринтера, не нуждаясь при этом во вмешательстве человека в процесс микрофильмирования как таковой. Качество микрофильма, полученного с помощью СОМ-системы гораздо выше, чем классического, при этом сам процесс микрофильмирования проходит гораздо быстрее. Все эти и многие другие свойства СОМ-систем обусловили их успешную эксплуатацию во многих архивах мира.



# МЕТОД ХРАНЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ НА АНАЛОГОВОМ НОСИТЕЛЕ С ИСПОЛЬЗОВАНИЕМ ШТРИХ-КОДОВ

Источник: [http://elar.urfu.ru/bitstream/10995/31705/1/conf\\_rtf\\_2015\\_09.pdf](http://elar.urfu.ru/bitstream/10995/31705/1/conf_rtf_2015_09.pdf)

Авторы: Проскураков Н. Е. , Ануфриева А. Ю., Ходов С. И. ТулГУ, Россия

## **Аннотация**

Статья посвящена микрофильмированию и СОМ-технологиям. В статье приведены основные параметры двумерных штрих-кодов. Разработана технология хранения цифровой информации в кодированном виде на микрофильме с использованием штрих-кодов.

## **Введение**

Современное общество характеризуется тем состоянием информатизации, при котором в обороте регулярно находятся терабайты конфиденциальной информации, а в системах хранения – еще большие объемы, но практически ни в одних из них не обеспечивается стопроцентная надежность и защищенность данных. Само понятие надежности в настоящее время не является актуальным без понятия «быстродействие доступа к данным», т. е. надежность хранения данных — это совокупность возможности хранения данных в исходном виде и одновременного обеспечения доступа к ним. Однако на сегодняшний день наблюдается противоположная ситуация: наличие огромного массива информации в цифровом виде и, одновременно с этим, отсутствие надежных технологий ее долговременного хранения.

Таким образом, становится актуальной задача совмещения цифровой обработки информации и ее хранения на аналоговом носителе. Наиболее оптимальным вариантом решения этой задачи является использование штрих-кодов.

## **1. Методы**

В стандартный типовой процесс микрофильмирования с использованием СОМ-систем для достижения большей конфиденциальности хранящихся сведений предлагается на промежуточных стадиях ввести (применительно к электронным образам документов) процедуру кодирования, которая может быть реализована следующим образом:

- получение с помощью сканера электронного образа оригинала;
- дополнительная обработка оператором для устранения дефектов и неточностей (при необходимости);
- перевод электронного образа документа в бинарный вид;
- применение алгоритмов кодирования к двоичному коду (наложение гаммы, блочные замены и т. д.);
- перевод полученных кодированных данных в двумерные штрихкоды;

- вывод двумерных штрих-кодов с помощью гибридных систем на микропленку.

В целях автоматизации производства и уменьшения объемов занимаемой площади битовую информацию цифрового образа оригинала кодируют с помощью разработанного нами специального программного обеспечения (генератора) в шестнадцатеричной системе счисления. Интерфейс генератора представлен на рис. 1.

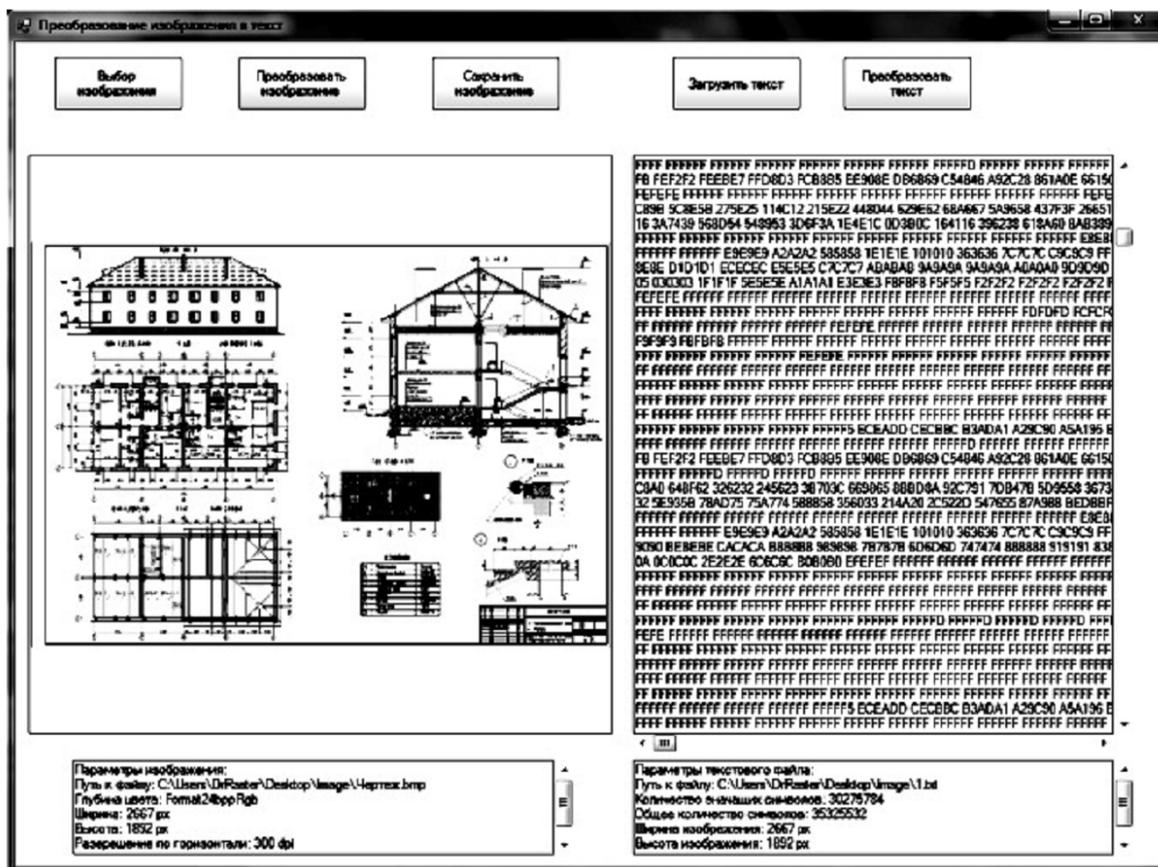


Рис. 1. Интерфейс программы генератора

В данном алгоритме каждый пиксель изображения кодируется тремя парами символов, где каждая пара отвечает за один из трех компонентов цвета в модели RGB. Далее полученный шестнадцатеричный код выводится на микропленку в виде штрих-кода для обеспечения автоматизации процесса ввода/вывода данных при получении цифрового образа графического файла, что позволяет избежать погрешностей при восстановлении оригинала и влияния человеческого фактора на данный процесс. Это особенно актуально для таких типов документов, как художественные картины, документы CAD-приложений и др., содержащих множество мелких деталей, требующих высокой квалификации операторов COM-систем.

На следующем этапе полученный набор данных кодируется с помощью генератора двумерных штрих-кодов DataMatrix, например, программой Labeljoy [1].

Данная технология позволяет помещать информацию в 50 символов на площади размером два квадратных миллиметра. При этом код может быть нанесен на поверхность огромным количеством способов: струйная печать, гравировка, лазер и др. [2].

При необходимости восстановления информации штрих-кодовые данные считываются с микрофильма сканирующим устройством, а затем декодируются, в результате чего происходит восстановление оригинального электронного документа в изначально заданном автором формате [3].

## **2. Результаты**

Черно-белые штрих-коды позволяют добиться относительно высокой плотности записи информации. По имеющимся данным на одном 16-мм микрофильме длиной 30,5 м в штрих-кодах можно сохранить 7200 изображений формата А4 или около 45 Мбайт информации (на 35-мм микрофильме соответственно в 2 раза больше) [2].

Готовые сгенерированные штриховые коды по своим заголовкам (дополнительным данным к файлам) могут быть объединены с ресурсами внешних баз данных, таких как Excel, Access, Outlook, Sendblaster, SqlServer, MySql, Oracle. Автоматизация процесса соотнесения обработанных данных, полученных со сканера штрих-кода, с ресурсами внешних баз данных систем хранения позволяет получать полную информацию в режиме реального времени.

## **3. Выводы**

1. Разработанная технология хранения цифровых данных на микрофильме в виде двухмерного штрих-кода позволяет долгосрочно хранить цифровую информацию, обеспечивая возможность быстрого доступа к цифровому оригиналу и оптимизацию последующей работы.

2. Вне зависимости от первоначально заданного формата на качество восстановленного оригинала влияют только параметры используемого технологического оборудования и микрографических материалов, которые на настоящий момент позволяют значительно приблизиться к решению проблемы хранения цифровых данных и обеспечения их конфиденциальности, целостности и доступности.

## **Список литературы**

1. Программное обеспечение для печати этикеток с автоматической генерацией штрих-кодов [Электронный ресурс]. URL: <http://www.labeljoy.com/ru/> (дата обращения: 17.11.2014).

2. Современные подходы к созданию страховых фондов документации на электронных носителях / Е. Е. Евсеев, А. К. Талалаев, Н. Е. Проскуряков, П. Е. Завалишин, А. Ю. Ануфриева // Страховой фонд документации. № 1. 2014. Харків. С. 3–11.

3. Ануфриева А. Ю., Архангельская Н. Н. Альтернативные методы долгосрочного хранения цифровой информации. Материалы X Международной научно-практической конференции молодых исследователей. Содружество наук. Барановичи. Барановичи : Изд-во БарГУ, 2014. Ч. 2. С. 122–124.



## УРЯД УДОСКОНАЛИВ ПОРЯДОК ПРОВЕДЕННЯ ПЕРЕВІРОК У СФЕРІ СТРАХОВОГО ФОНДУ ДОКУМЕНТАЦІЇ

Джерело інформації: <https://news.dtkk.ua/law/inspections/45984>

Затверджено критерії, за якими оцінюється ступінь ризику від провадження господарської діяльності у сфері створення, формування, ведення і використання страхового фонду документації та визначається періодичність здійснення планових заходів державного нагляду (контролю) Державною архівною службою.

Кабмін постановою від 08.11.2017 р. № 840 затвердив критерії, за якими оцінюється ступінь ризику від провадження господарської діяльності у сфері створення, формування, ведення і використання страхового фонду документації та визначається періодичність здійснення планових заходів державного нагляду (контролю) Державною архівною службою.

Згідно з документом зазначеними **критеріями є:**

- значення для економіки і безпеки держави;
- належність до критичної інфраструктури;
- наявність потенційного рівня небезпеки;
- належність до культурної спадщини;
- призначення страхового фонду документації;
- дотримання вимог законодавства щодо створення, формування, ведення і використання страхового фонду документації.

Відповідно до встановлених критеріїв суб'єкти господарювання належать до одного з трьох ступенів ризику - високого, середнього та незначного.

**Також визначено періодичність здійснення планових заходів державного нагляду (контролю) Державною архівною службою.** Так, планові заходи державного нагляду (контролю) за діяльністю суб'єктів господарювання здійснюватимуться з такою періодичністю:

- з високим ступенем ризику — не частіше одного разу на два роки;
- із середнім ступенем ризику — не частіше одного разу на три роки;
- з незначним ступенем ризику — не частіше одного разу на п'ять років.



## КОНФЕРЕНЦИЯ 2017 ГОДА СЕКЦИИ ДЕЛОВЫХ АРХИВОВ МЕЖДУНАРОДНОГО СОВЕТА АРХИВОВ: КАКИЕ ПРОБЛЕМЫ БУДУТ ДЛЯ НАС ОСНОВНЫМИ ЧЕРЕЗ 5 ЛЕТ?

Источник: сайт Центра деловой истории в Стокгольме  
<http://naringslivshistoria.se/en/cfn-news/ica-sba-17-5-years-will-challenges/>  
Автор: Наташа Храмцовская

*Статья Андерса Хоулца (Anders Houltz) была опубликована 9 октября 2017 года на сайте шведского Центра деловой истории (Center for Business History, <http://naringslivshistoria.se/en/>) в Стокгольме. Этот центр является некоммерческой ассоциацией, занимающейся сохранением и использованием материалов по истории деловых организаций и обслуживающей в качестве клиентов своих же членов. Ассоциация обеспечивает управление 7 тысячами корпоративных архивов.*

*Является ли «цифровая черная дыра» главной проблемой для деловых архивов? На конференции секции деловых архивов (Section on Business Archives, SBA) Международного совета архивов (МСА) в апреле 2017 года мы попросили профессионалов архивного дела из более чем 30 стран перечислить проблемы, с которыми в ближайшем будущем столкнутся архивы коммерческих организаций. Андерс Хоульц подвел итоги опроса и назвал первую пятерку названных ими проблем.*

На прошедшей в Стокгольме в апреле 2017 года конференции секции деловых архивов Международного совета архивов (<http://naringslivshistoria.se/en/cfn-news/future-role-business-archives/>) 150 специалистов из более чем 30 стран в течение двух дней обсуждали будущее архивов коммерческих организаций. В паузе между докладами коллег-архивистов участники конференции нашли время на участие в семинаре на тему «**Какие проблемы будут для нас основными через 5 лет?**».

Среди потока предложений и идей выделялись несколько тенденций. Ниже кратко описана первая пятёрка основных проблем, с которыми, по мнению коллег, через пять лет будут сталкиваться деловые архивы.

### **1. Решение задач по оцифровке**

*Всё, что не в электронной форме, «не существует», а всё электронное трудно сохранять.*

*Существует ожидание, что все материалы будут оцифрованы и легко доступны по нажатию кнопки.*

Оцифровка архивами своих фондов, очевидно, открывает множество возможностей. В то же время это самая неотложная проблема для отрасли, у которой есть множество аспектов. Как формируются процессы и процедуры архивации изначально-электронных материалов? Как проводятся экспертиза ценности и отбор того, что следует сохранить, - или же нам, действительно,

нужно сохранять всё, что есть? Остаётся нерешенным ряд технологических вопросов, и методы пока ещё не стандартизированы ни на уровне организаций, ни на национальном и международном уровнях. Способны ли мы гарантировать долговременную сохранность электронных файлов? Оцифровка также ставит вопрос о статусе аналоговых документов. Можно ли уничтожать аналоговые оригиналы после их оцифровки (сокращая тем самым расходы на хранение)?

Аутентичность и информационная ценность оригинальных [аналоговых] документов сопоставляется с экономичностью и удобством их электронных копий. Наконец, оцифровка означает фундаментальные изменения с точки зрения пользователей архива. Для новых поколений пользователей будет привычным электронный поиск информации, они будут менее склонны посещать физические архивы, искать и читать оригинальные, часто рукописные документы. Они ожидают, что нужная им информация будет доступна через Интернет. Возможности в плане прозрачности и электронного открытого доступа вступают в противоречие с потребностями в защите неприкосновенности частной жизни, прав собственности и корпоративных интересов.

## **2. Задача оставаться нужными**

*Нужно, чтобы руководство осознало, что история - это нечто большее, чем повод для организации юбилеев.*

*Всё ещё сложно убедить руководителей и менеджеров в том, что культурно-историческое наследие важно для будущей деловой деятельности.*

Корпоративные архивы должны постоянно оправдывать своё существование и своё место в организации и в обществе. Им нужно найти аргументы в пользу ценности истории и конкретные примеры, демонстрирующие, что корпоративная история - это актив, который следует принимать во внимание.

Ряд респондентов обеспокоен тем, что в настоящее время мы переживаем волну ностальгии и интереса к прошлому, которая, когда она спадёт, будет заменена однобокой ориентацией на решение предстоящих задач. Чтобы этого избежать, архивы должны демонстрировать значение принятых в прошлом решений как для текущей ситуации, так и для сценариев будущего. Важно подчеркивать, что корпоративная социальная ответственность также включает в себя сохранение истории. Кроме того, с усилением глобализации деятельности корпораций возникает потребность в том, чтобы их архивы отражали и документировали деловую деятельность, осуществляемую во многих странах и в разных уголках мира.

Ускоряются темпы изменений в корпоративной структуре. Учитывая быструю ротацию персонала на влиятельных должностях, архивы должны быть готовы снова и снова осведомлять новые группы людей в организации о важности истории и о том, как она используется. Нужность архивов не достигается раз и навсегда, и её приходится подтверждать даже в компаниях с долгой историей. В новых же компаниях задача заключается в том, чтобы

изначально обосновать необходимость сохранения документов и создания архивов. Это особенно сложная задача в изначально-электронных подразделениях и филиалах.



**Директор по научной работе Центра деловой истории в Стокгольме Андерс Хоулц (Anders Houltz) провел семинар о будущих проблемах деловых архивов. Фото: Linus Sundahl-Djerf**

### **3. Поиск финансирования**

*Налажена работа на профессиональном уровне, созданы музеи – по достижении какого уровня можно перестать расти?*

Экономическое давление всегда будет фактором, требующим от архивистов оправдывать существование своих коллекций. В последние годы многие коллеги столкнулись с ощутимыми сокращениями штатов и финансирования, и, если мы не сможем донести до принимающих решения лиц полезность инвестиций в документирование истории, эта тенденция будет продолжаться.

Постоянно усиливающиеся требования к обеспечению экономической эффективности делают руководителей компаний склонными к сокращению штатных должностей для управления документами. Оцифровка также может уступить место аутсорсингу или же передачи ответственности за ведение архива внешним или внутренним поставщикам услуг, не имеющим профессиональной подготовки и общего понимания вопросов аутентичности, исторической достоверности и долговременной надёжности.

Еще одна экономическая проблема связана с местами хранения: площади хранения растут по мере увеличения объёма архивных документов, что означает для организации увеличение расходов. Архивы на собственной площадке уступают место внеофисным альтернативам, что приводит к ослаблению повседневной связи между управлением организацией и архивом.

#### **4. Сохранение профессиональной компетентности**

*Де-профессионализация профессии становится острой проблемой, когда «архивировать» может любой.*

*В мире пост-правды нас будут рассматривать как угрозу амбициям власть предержащих – и перед нами стоит задача продолжать сохранять и распространять историю. Говорить правду власти.*

С проблемой финансирования тесно связан вопрос обучения, приёма на работу и поддержания квалификации штата профессиональных архивистов и/или специалистов по управлению документами. Новым поколениям архивистов потребуются многогранные, комбинированные знания и навыки для решения ключевых проблем управления культурно-историческим наследием, а также специфических вопросов, связанных как с физическими, так и с электронными архивами.

В условиях электронной среды у руководителей компаний может возникнуть соблазн передать управление документами в отделы ИТ и информационной безопасности. Некоторые из респондентов видят тенденцию игнорирования роли архивиста как эксперта, в ситуации, когда, как видится, практически вся информация доступна в электронном виде. Другие же коллеги, наоборот, видят здесь для архивистов возможность расширить свою сферу ответственности и доказать свою ценность как хранителей всего контента. Однако наиболее широко распространена обеспокоенность по поводу риска для профессиональной идентичности архивиста, когда его профессиональные обязанности дрейфуют в сторону «рассказов о былом», управления брендом и маркетинга – т.е. архивист становится поставщиком контента для отдела маркетинга.

Ключевым фактором является обучение и образование. Ряд опрошенных отметил необходимость в более совершенном, сертифицированном образовании университетского уровня и в более продвинутых курсах повышения квалификации для архивистов, - а также необходимость включения архивных вопросов в программы обучения руководителей для повышения их осведомленности об архивной работе и об управлении культурно-историческим наследием как деловым активом.

#### **5. Сохранение доверия и уважения к профессии**

*Архивисты рискуют стать просто «рассказчиками историй».*

*Мы можем увидеть исчезновение архивного дела как самостоятельной сферы деятельности. Оно может влиться в сферу управления контентом.*

Ряд коллег предвидит исчезновение в будущем архивов как самостоятельной сферы деятельности. Они боятся, что в роли поставщика «жареных фактов» для социальных сетей и других каналов информирования, архивы могут потерять авторитет, который традиционно ассоциируется с аутентичными документами, и в результате стать неактуальными. Проблема заключается в том, чтобы так реагировать на эту и последующие тенденции, чтобы сохранить целостность архивов.

Движение вперед для деловых архивов, как и для всех учреждений, занимающихся сохранением культурного наследия, предусматривает восприимчивость к изменениям и одновременно основное внимание, как и раньше, аутентичному контенту и основанному на фактах описанию истории. Если сохранить этот баланс, то архивы смогут воспринимать такие вызовы, как задача оцифровки и растущий спрос на информацию (хранилищем которой они по существу являются) – как возможности.

**Андерс Хоулц (Anders Houltz)**

**Мой комментарий:** О деловых архивах после 1991 года вспоминают редко, и это самый провальный элемент в российском архивном деле – мы по сути дела давно уже толком не сохраняем свою экономическую историю даже в разрезе предприятий-гигантов индустриальной эпохи. О сохранении истории цифровой экономики пока что смешно даже говорить... Впрочем, Россия в этом плане не особенно хуже даже развитых западных стран, где утрата экономической истории и разорение великолепных корпоративных архивов – тоже вполне обыденное явление. Правда, для тех, кому дорога история отечества, это слабое утешение: (Шведский специалист сказал много правильных слов, однако меня тревожит следующее: он нигде не говорит о вовлечении архивов и служб управления документами в оказание активной поддержки оперативной деловой деятельности, в сотрудничество по вопросам обеспечения информационной безопасности, правовой защиты интересов организации, в деятельность по обеспечению непрерывности деловой деятельности и во многие другие востребованные современные направления деятельности. Без этого, как ни «осведомляй» высшее руководство, архивы будут оставаться затратным подразделением и, в лучшем случае, получать крохи со стола.



## **ПОЛЬША: ПОДГОТОВЛЕН ПРОЕКТ МОДЕРНИЗАЦИИ ИНТЕГРИРОВАННОЙ АРХИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ZOSIA**

Источник: <http://rusrim.blogspot.com/2017/11/zosia.html>

*Данная новость была опубликована 6 ноября 2017 года на сайте Генеральной дирекции государственных архивов Польши (Naczelna Dyrekcja Archiwów Państwowych).*

*Интегрированная архивная информационная система (Zintegrowany System Informacji Archiwalnej, сокращенно ZoSIA – «Зося» - это приложение, предназначенное для управления архивными коллекциями (учета и инвентаризации) на всех уровнях их иерархической структуры - от архива в целом до единицы хранения.*

6 ноября 2017 года состоялась публичная презентация основных положений проекта «Модернизация интегрированной архивной информационной Системы ZoSIA», который планируется реализовать в рамках оперативной программы «Электронная Польша» (Polska Cyfrowa) - это 2-е приоритетное направление, пункт 2.1 «Высокая доступность и качество электронных государственных услуг».

Проект предполагает совершенствование и развитие данной информационной системы в целях эффективной реализации задач государственных архивов, включающих сбор, учет, хранение, поддержание, защиту, создание электронных копий архивных материалов и ведение информационной деятельности.

В рамках проекта предполагается выполнить следующие работы:

- модернизация существующих модулей, в частности, касающихся учета и описания архивных материалов,
- улучшение эргономичности интерфейса,
- повышение производительности системы – скорости записи и передачи данных,
- реализация решений, повышающих безопасность хранящихся в системе данных,
- добавление недостающих функциональных возможностей и модулей для сбора, хранения и распространения архивных материалов.

Ориентировочная стоимость проекта - около 21 миллиона злотых (337 млн. рублей, или 5,8 млн. долларов). Реализация проекта запланирована на период с 3-го квартала 2018 года по 2-й квартал 2021 года.

Система «Зося» может быть использована как в государственных архивах, так и в других организациях за пределами сети государственных архивов. В настоящее время систему используют 93 организации и учреждения (в том числе 17 не входящих в число государственных архивов), а специальная образовательная версия системы используется в 9 польских высших учебных заведениях.

Решение о разработке и внедрении системы было принято Генеральным директором государственных архивов в 2007 году, а её первая версия была введена в эксплуатацию в 2010 году. За годы существования системы проводились работы по её развитию и добавлялись новые функциональные возможности. Дополнительные сведения о системе «Зося» можно найти по адресу <https://www.nac.gov.pl/archiwum-cyfrowe/systemy-i-infrastruktura-it/zosia/>.

В систему загружаются описания архивных материалов, которые выкладываются затем вместе со скан-копиями на сайте «Ищи в архивах» (Szukaj w archiwach, <http://szukajwarchiwach.pl/>). В настоящее время на сайте выложены около 26 миллионов электронных образов.

# ИСО: ОПУБЛИКОВАН КОДЕКС ПРАКТИКИ Э-РАСКРЫТИЯ

Источник: сайт ИСО <https://www.iso.org/standard/66231.html>

Автор: [Наташа Храмцовская](#)



Согласно информации на сайте Международной организации по стандартизации (ИСО), в октябре 2017 года был опубликован стандарт **ISO/IEC 27050-3:2017 «Информационные технологии – Методы обеспечения безопасности - Выявление и раскрытие электронной информации – Часть 3: Кодекс практики э-раскрытия»** (Information technology - Security techniques - Electronic discovery - Part 3: Code of practice for electronic discovery, см. <https://www.iso.org/standard/66231.html> и <https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-3:ed-1:v1:en>) объёмом 28 страниц, подготовленный техническим подкомитетом JTC1/SC27.

Это уже вторая опубликованная часть ISO 27050. Ранее был опубликована часть первая - ISO/IEC 27050-1:2016 «Обзор и основные положения» (Part 1: Overview and concepts, см. <https://www.iso.org/standard/63081.html> и <https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-1:ed-1:v1:en>). Продолжается работа над ещё одной частью - ISO/IEC 27050-2 «Часть 2: Руководство по управлению процессом э-раскрытия» (Part 2: Guidance for governance and management of electronic discovery, см. <https://www.iso.org/standard/66230.html>).

В аннотации отмечается, что ISO/IEC 27050-3:2017 содержит требования и рекомендации по деятельности в области э-раскрытия, включая (но не ограничиваясь) выявление, обеспечение сохранности, сбор, обработку, изучение, анализ и представление сохраняемой электронным образом информации (electronically stored information, ESI – *данный термин американского права, постепенно закрепляющийся в стандартах ИСО, по сути дела является расширением понятия «электронные документы», позволяющим исключить споры о том, имеет ли данный электронный объект статус документа или нет – Н.Х.*). Кроме того, данный стандарт определяет соответствующие меры, которые охватывают жизненный цикл

электронной информации с момента её первоначального создания до окончательного уничтожения.

Настоящий стандарт может быть полезен как нетехническому, так и к техническому персоналу, вовлеченному в мероприятия по э-раскрытию. Важно отметить, что требования и рекомендации следует применять в той мере, в какой они не противоречат законодательно-нормативным требованиям соответствующих юрисдикции, и ожидается, что пользователи стандарта позаботятся о соблюдении существующих требований законодательства.

Содержание документа следующее:

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Сокращения

5. Основные положения э-раскрытия

6. Требования и рекомендации по вопросам э-раскрытия

- 6.1. Общие положения
- 6.2. Выявление сохраняемой электронным образом информации (ESI)
- 6.3. Обеспечение сохранности ESI
- 6.4. Сбор ESI
- 6.5. Обработка ESI
- 6.6. Изучение (review) ESI
- 6.7. Анализ ESI
- 6.8. Представление ESI

Библиография

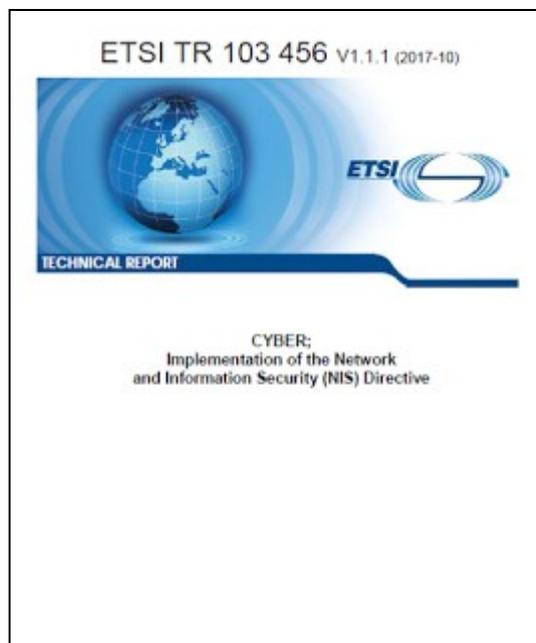


**ЕВРОПЕЙСКИЙ ИНСТИТУТ  
ТЕЛЕКОММУНИКАЦИОННЫХ СТАНДАРТОВ ETSI  
ОПУБЛИКОВАЛ ТЕХНИЧЕСКИЙ ОТЧЕТ  
ПО ИСПОЛНЕНИЮ ДИРЕКТИВЫ ПО СЕТЕВОЙ  
И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Источник: портал Portail de la Qualité Luxembourg <https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2017/etsi-nis.html>

*Новый технический отчет Европейского института телекоммуникационных стандартов ETSI TR 103 456 «Реализация положений Директивы о сетевой и информационной безопасности» (CYBER; Implementation of the Network and Information Security (NIS) Directive, см. [http://www.etsi.org/deliver/etsi\\_tr/103400\\_103499/103456/](http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/)*

[01.01.01\\_60/tr\\_103456v010101p.pdf](http://01.01.01_60/tr_103456v010101p.pdf)), недавно опубликованный Техническим комитетом по стандартизации ETSI/TC CYBER, отвечающим за техническую стандартизацию в области кибербезопасности, содержит рекомендации по реализации положений европейской Директивы 2016/1148 о безопасности сетей и информационных систем.



Новая публикация ETSI содержит руководство по опубликованным или разрабатываемым ключевыми сообществами специалистов по кибербезопасности техническим спецификациям, которые подготовлены таким образом, чтобы соответствовать правовым и техническим требованиям Директивы 2016/1148 от 6 июля 2016 года «О мерах по обеспечению единого высокого уровня безопасности сетей и информационных систем в Евросоюзе» (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, далее - Директива NIS, см. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>).

Технический отчет ETSI TR 103 456 охватывает различные вопросы и требования в сфере кибербезопасности:

- Методы совместного использования и структурированного обмена информацией;
- Уведомление об инцидентах;
- Менеджмент технических и организационных рисков для информационных систем;
- Проблемы и решения;
- Технические рекомендации.

Менеджмент рисков кибербезопасности включает в себя оценку ряда рисков с учетом условий деятельности организации; понимание активов, ресурсов и основных процессов организации; и принятие мер по непрерывному совершенствованию того, как организация защищает себя,

выявляет и реагирует на связанные с этими активами, ресурсами и процессами инциденты.

«Данный новый отчет ETSI охватывает более широкий контекст кибербезопасности, чем тот, что отражён в Директиве NIS или в отчете ENISA о пробелах в стандартизации (Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy, версия 1.0, ноябрь 2016 года, см. [https://www.enisa.europa.eu/publications/gaps-eu-standardisation/at\\_download/fullReport](https://www.enisa.europa.eu/publications/gaps-eu-standardisation/at_download/fullReport) )», - говорит председатель технического комитета CYBER Чарльз Бруксон (Charles Brookson). «Европейским институтом телекоммуникационных стандартов накоплен многолетний опыт в области безопасности, включая работу, проделанную нашим комитетом. Этот отчет должен помочь тем, кто стремится соответствовать требованиям Директивы NIS, снабдив их соответствующими советами и рекомендациями».

Технический отчет ETSI TR 103 456 адресован всем, кто должен учитывать последствия Директивы NIS, использовать её или адаптировать её положения в своё национальное законодательство, включая регуляторов, операторов ключевых сервисов и поставщиков электронных услуг.

В настоящее время ETSI изучает новые технологии, такие как виртуализация сетевых функций (Network Functions Virtualization, NFV, см. *также* *Википедию*: [https://ru.wikipedia.org/wiki/Виртуализация\\_сетевых\\_функций](https://ru.wikipedia.org/wiki/Виртуализация_сетевых_функций)), 5G и квантовые вычисления, которые создают новые проблемы безопасности. Различные группы ETSI тесно сотрудничают с техническим комитетом CYBER, обеспечивая, чтобы аспекты «запроектированной безопасности» были с самого начала включены во все спецификации. Технический комитет CYBER за последние три года уже опубликовал 17 спецификаций и отчетов по кибербезопасности. Они свободно доступны на веб-сайте ETSI (<http://www.etsi.org/standards-search>), а также в интернет-магазине ILNAS (<https://ilnas.services-publics.lu/>).

Структура 28-страничного отчета следующая:

- Предисловие
- Использование модальных глаголов
- Резюме для руководства
- Введение
- 1. Область применения
- 2. Литература
- 3. Определения и сокращения
- 4. Обзор Директивы NIS
- 5. Обмен информацией о киберугрозах: инциденты и риски
- 6. Роль анализа рисков в обеспечении сетевой и информационной безопасности
- 7. Проблемы и решения
- 8. Рекомендации
- Приложение А: История развития обмена информацией о киберугрозах



## ИСО: ОБСУЖДАЕТСЯ ПРОЕКТ НОВОГО СТАНДАРТА ПО ТЕХНОЛОГИЯМ И МЕТОДАМ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Источник: портал Portail de la Qualité Luxembourg <https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/iso-iec-jtc-1sc38-ilnas+debriefingplenarymeeting-v11.pdf>



Технический комитет ИСО/МЭК JTC1/SC38 «Облачные вычисления и распределенные платформы» (Cloud Computing and Distributed Platforms) продолжает работу над стандартами облачных вычислений. В настоящее время проходит голосование по новому проекту **ISO/IEC NP TS 23167 «Информационные технологии – Облачные вычисления – Типичные технологии и методы»** (Information Technology - Cloud Computing - Common Technologies and Techniques), которое завершится в середине декабря 2017 года.

Как отмечается в аннотации на проект, он расширяет описание облачных вычислений, содержащееся в свободно распространяемых стандартах ISO/IEC 17788 «Информационные технологии - Облачные вычисления – Общие положения и словарь» (Information technology - Cloud Computing - Overview and Vocabulary, *адаптирован в СНГ как ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология»*) и ISO/IEC 17789 «Информационные технологии - Облачные вычисления - Эталонная архитектура» (Information technology - Cloud Computing - Reference Architecture).

Новый проект также дополняет материал по облачным приложениям, содержащийся в только что опубликованном стандарте ISO/IEC 19941:2017 «Информационные технологии - Облачные вычисления - Интероперабельность и переносимость» (Information Technology - Cloud Computing - Interoperability and Portability, <https://www.iso.org/standard/66639.html>), в котором отсутствует, однако, описание таких технологий, как виртуальные машины, контейнеры и безсервисные вычисления и того, как они используются в контексте облачных вычислений.

В других технических комитетах выполняются и планируются другие проекты, касающиеся технологий и методов, описанных в

ISO/IEC NP TS 23167. Примером может служить проект ISO/IEC CD 21878 «Информационные технологии - Методы и средства обеспечения безопасности – Руководство по безопасности при проектировании и внедрении виртуализированных серверов» (Information technology - Security techniques - Security guidelines for design and implementation of virtualized servers, см. <https://www.iso.org/standard/72029.html>), над которым работает рабочая группа WG4 технического подкомитета JTC1/SC27 и в котором рассматривается безопасность виртуальных машин.

В ISO/IEC NP TS 23167 описывается ряд технологий и методов, обычно применяемых для создания приложений и систем с использованием облачных вычислений. К ним относятся:

- Виртуальные машины (виртуальные машины) и гипервизоры;
- Контейнеры и системы управления контейнерами;
- «Бессерверные» вычисления;
- Архитектура микросервисов, методология создания приложений «12 факторов», гибкие (agile) методы и автоматизация;
- Платформы как системы обслуживания и их архитектура;
- Услуги хранения;
- Безопасность, масштабируемость и сетевое взаимодействие применительно к вышеупомянутым технологиям облачных вычислений.

Стандарт ISO/IEC 17789 содержит четкое описание архитектуры облачных вычислений. Тем не менее, у клиентов облачных сервисов, создающих приложения и системы с использованием облачных вычислений, есть потребность в понимании типовых технологий и методов, которые могут быть использованы в этих целях.

Фактически, существует потребность в том, чтобы четко описать, как создавать, настраивать, организовывать и эксплуатировать объекты, существующие в сервисном «слое» эталонной архитектуры по ISO/IEC 17789, в особенности для облачных сервисов, обеспечивающих инфраструктурные и платформенные возможности. Это не является обязательным для облачных сервисов, обеспечивающих использование прикладных приложений, поскольку соответствующие усилия предпринимаются поставщиком облачных услуг во время создания облачного сервиса.

В настоящее время существует целый ряд технологий и методов, применяемых в этой области деятельности, которые доступны для использования благодаря широкому спектру предлагаемых на рынке облачных сервисов. Предлагаемый проект направлен на каталогизацию и описание этих технологий и методов, а также на описание того, как они решают определенные вопросы использования облачного сервиса.

В настоящее время отсутствует достаточно хорошее общее описание доступных сегодня на рынке технологий и методов, и в результате пользователям облачных сервисов приходится собирать сведения о них из целого ряда разнородных и иногда противоречащих друг другу источников. Данный документ обеспечит согласованное и всестороннее описание,

собранные в одном месте, что должно облегчить пользователям облачных сервисов задачу выбора соответствующих технологий и методов для решения тех задач, с которыми они сталкиваются.



## НОВЫЕ МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И ПРОЕКТЫ СТАНДАРТОВ В СФЕРЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Источник: портал Portail de la Qualité Luxembourg <https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2017/nouveaux-projets-normes-cloud-computing.html>

Начавший свою деятельность с 2009 года, технический подкомитет по стандартизации ИСО/МЭК JTC1/SC38 «Облачные вычисления и распределенные платформы» (Cloud Computing and Distributed Platforms) является сегодня одним из ведущих органов стандартизации в сфере облачных вычислений. Недавняя пленарная встреча членов подкомитета стала для нас поводом для того, чтобы дать полную картину проектов, включенных в программу его работы, и призвать экспертов Люксембурга присоединиться к национальному зеркальному комитету, отвечающему за мониторинг международной работы по стандартизации по тематике облачных вычислений.



В июле этого года подкомитет SC38 опубликовал новый международный стандарт **ISO/IEC 19086-3:2017 «Информационные технологии - Облачные вычисления - Структура соглашения о качестве предоставляемых услуг (SLA) – Часть 3: Ключевые требования к соответствию»** (Information technology - Cloud computing - Service level agreement (SLA) framework - Part 3: Core conformance requirements, см. <https://www.iso.org/standard/67547.html> и <https://www.iso.org/obp/ui/#!iso:std:67547:en>). Этот стандарт, с одной стороны, определяет основные требования к соответствию для соглашений об уровне обслуживания для облачных сервисов на основе международного стандарта **ISO/IEC 19086-1:2016 «Информационные технологии - Облачные**

**вычисления - Структура соглашения о качестве предоставляемых услуг (SLA) - Часть 1. Обзор и концепции»** (Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts, см. <https://www.iso.org/standard/67545.html> и <https://www.iso.org/obp/ui/#!iso:std:67545:en>), а с другой – содержит рекомендации по реализации этих требований. Данный стандарт предназначен для использования как поставщиками, так и пользователями облачных услуг для их взаимной выгоды.

Подкомитет также опубликовал в сентябре 2017 года новый международный стандарт **ISO/IEC 19944:2017 «Информационные технологии - Облачные вычисления - Облачные сервисы и устройства: Поток, категории и использование данных»** (Information technology - Cloud computing - Cloud services and devices: Data flow, data categories and data use, см. <https://www.iso.org/standard/66674.html> и <https://www.iso.org/obp/ui/#!iso:std:66674:en>), в котором рассматриваются различные вопросы, связанные с потоками данных, путем применения описанной в стандарте ISO/IEC 17789: 2014 эталонной архитектуры облачных вычислений к экосистеме облачных устройств и услуг.

Кроме того, на своей недавней пленарной встрече в Сан-Хосе (San José) подкомитет утвердил публикацию нового международного стандарта **ISO/IEC 19941:2017 «Информационные технологии - Облачные вычисления - Интероперабельность и переносимость»** (Information Technology - Cloud Computing - Interoperability and Portability, <https://www.iso.org/standard/66639.html>), который вскоре будет доступен. В этом стандарте рассматриваются интероперабельность и переносимости данных в облаке. Стандарт определяет типы интероперабельности и переносимости для облака (для сервисов и данных), взаимосвязь между этими двумя аспектами и соответствующую терминологию.

В программу работы подкомитета JTC1/SC38 включены восемь проектов международных стандартов (см. <https://www.iso.org/committee/601355/x/catalogue/p/0/u/1/w/0/d/0>), над которыми зарегистрированные в подкомитете национальные эксперты имеют возможность поработать. В частности, целью этих проектов является завершение серии стандартов по соглашениям о качестве оказания облачных услуг (метрики и основные требования к соответствию), определение видов интероперабельности и переносимости для облачных услуг, способствование прозрачности потоков данных и интеграции различных облачных услуг, а также предоставление рекомендаций по использованию международных стандартов при разработке политик, регулирующих или регламентирующих деятельность поставщиков облачных услуг:

- **ISO/IEC DIS 19086-2 «Информационные технологии - Облачные вычисления - Структура соглашения о качестве предоставляемых услуг (SLA) – Часть 2: Модель метрик»** (Information technology - Cloud computing - Service level agreement (SLA) framework - Part 2:

Metric model, см. <https://www.iso.org/standard/67546.html> и <https://www.iso.org/obp/ui/#!iso:std:67546:en>);

- **ISO/IEC 19941:2017 «Информационные технологии - Облачные вычисления - Интероперабельность и переносимость»** (Information Technology - Cloud Computing - Interoperability and Portability, <https://www.iso.org/standard/66639.html>);

- **ISO/IEC AWI 22123 «Информационные технологии - Облачные вычисления – Понятия и терминология»** (Information Technology - Cloud Computing - Concepts and Terminology, см. <https://www.iso.org/standard/72627.html>);

- **ISO/IEC AWI 22624 «Информационные технологии - Облачные вычисления – Обработка данных облачными сервисами на основе таксономий»** (Information Technology - Cloud Computing – Taxonomy based data handling for cloud services, см. <https://www.iso.org/standard/73614.html>);

- **ISO/IEC NP TR 22678 «Информационные технологии - Облачные вычисления – Рекомендации по разработке политик»** (Information Technologies - Cloud Computing - Guidance for Policy Development, см. <https://www.iso.org/standard/73642.html>);

- **ISO/IEC NP TR 23186 «Информационные технологии - Облачные вычисления – Концепция доверия при обработке данных из нескольких источников»** (Information technology - Cloud computing - Framework of trust for processing of multi-sourced data, см. <https://www.iso.org/standard/74844.html>);

- **ISO/IEC NP TR 23187 «Информационные технологии - Облачные вычисления – Взаимодействие с партнерами облачных услуг»** (Information technology - Cloud computing - Interacting with cloud service partners (CSNs), см. <https://www.iso.org/standard/74845.html>);

- **ISO/IEC NP TR 23188 «Информационные технологии - Облачные вычисления – Ландшафт граничных (edge) вычислений»** (Information technology - Cloud computing - Edge computing landscape, см. <https://www.iso.org/standard/74846.html>).



## **ФРАНЦИЯ: КОМПАНИЯ LOCARCHIVES ОПУБЛИКОВАЛА «БЕЛУЮ КНИГУ» ПО НАДЁЖНОЙ ОЦИФРОВКЕ И ПОСЛЕДУЮЩЕМУ УНИЧТОЖЕНИЮ ОРИГИНАЛОВ**

Источник: сайт компании Locarchives <https://locarchives.fr/actualites/livre-blanc-numerisation-fidele-et-destruction-des-originaux/>

Автор: Наташа Храмцовская

*Данная новость была опубликована 11 сентября 2017 года на сайте французской компании Locarchives (см. <https://locarchives.fr/>), оказывающей услуги по налаживанию делопроизводства и архивного дела, а также услуги доверенного хранилища третьей стороны, удовлетворяющего достаточно строгим национальным требованиям в отношении систем, которые могут использоваться для хранения юридически значимых электронных документов.*

Процессы перехода деловой деятельности на электронные технологии подталкивают компании к глубокой реорганизации своих систем управления документами. Контракты, счета-фактуры, переписка, кадровые досье ... организация этих тысяч входящих и исходящих потоков представляет собой реальную проблему, когда нужно сбалансировать эффективность, рентабельности и риски.

В контексте массового перехода на электронные технологии, надёжная юридически-значимая оцифровка (*numérisation fidèle*) открывает новые перспективы. Но возможно ли при этом систематическое уничтожение оцифрованных бумажных оригиналов без каких-либо оговорок?

Цель опубликованного компанией Locarchives аналитического отчета («белой книги») под названием «надёжная оцифровка и уничтожение оригиналов» (*Numérisation fidèle et destruction des originaux*) – снабдить принимающие решения лица ясной сводной информацией об эволюции законодательно-нормативной базы в том, что касается верных, надежных копий (*copie fiable*) и надёжной оцифровки, с тем, чтобы те могли принимать обоснованные решения об уничтожении либо дальнейшем хранении бумажных оригиналов и организовывать «гибридное» управление своими документами.

Отчет объёмом 32 страницы можно получить бесплатно, заполнив форму (для этого нужно нажать кнопку **Télécharger**) по адресу <https://locarchives.fr/ressources/livre-blanc-numerisation-fidele-et-destruction-des-originaux/>.

Структура аналитического отчета отражает три основных вопроса, которые в нём рассматриваются:

### **1. Что такое «оригинал», «верная копия»?**

Данный аналитический отчет включает материалы, помогающие лучше понять, что это такое с законодательно-нормативной точки зрения. Показывается, в какой степени теперь можно уничтожать бумажные оригиналы благодаря появлению нового стандарта NF Z 42-026. Мы подробно рассматриваем поворотную точку, отмеченную этим новым стандартом, ясно объясняя масштабы происходящих изменений.

*Мой комментарий:* Речь идёт о французском национальном стандарте NF Z 42-026 «*Определение и спецификации услуг по надёжной оцифровке документов на бумажном носителе и контроль над оказанием этих услуг*» (*Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations*, <https://www.boutique.afnor.org/norme/pr-nf-z42-026/definition-et-specifications->

[des-prestations-de-numerisation-fidele-de-documents-et-controle-de-ces-prestations/article/874692/fa187367](https://rusrim.blogspot.ru/2017/06/nf-z-42-026.html) , май 2017 года). О нём см. также посты: <https://rusrim.blogspot.ru/2017/06/nf-z-42-026.html>, <http://rusrim.blogspot.ru/2016/12/nf-z-42-026.html> и [https://rusrim.blogspot.ru/2017/09/blog-post\\_14.html](https://rusrim.blogspot.ru/2017/09/blog-post_14.html) .

## **2. Можно ли уже сегодня на практике уничтожить бумажные оригиналы?**

В отчете показано, что в результате эволюции законодательства появилась возможность принимать решения об уничтожении оригиналов, но при определенных условиях. Мы разъясняем стратегии реализации данного подхода таким образом, чтобы оптимизировать управление документами, одновременно контролируя риски. В частности, в «белой книге» на основе примеров из практики, охватывающих большинство вариантов оцифровки, с которыми сталкиваются организации и учреждения, объясняется, как правильно организовать надёжную оцифровку.

## **3. Что, как и почему следует делать в процессе оцифровки?**

В отчете мы показываем, что для эффективного перехода на электронные технологии и для их масштабирования с целью удовлетворения растущих потребностей организации часто требуется консультационная поддержка. Мы объясняем, как использование аутсорсинга и услуг внешних поставщиков позволяет внедрять современные электронные технологии на основе реалистичного работоспособного видения, что обеспечивает организациям дополнительную гибкость в их деятельности.

Наконец, «белая книга» содержит ряд рекомендаций по выбору надежного партнера, оказывающего консультационную поддержку и способного решать все стоящие перед организацией проблемы в области управления документами.

**Мой комментарий:** Основная мысль, которая проводится в отчете, заключается в следующем. Законодательство прямо не запрещает (но и прямо не авторизует) уничтожение бумажных оригиналов после их оцифровки, а владелец документов при этом берет на себя все риски. В результате решение о замещающей оцифровке в каждом случае приходится принимать отдельно, с учетом всех обстоятельств. В любом случае огромное значение имеет проведение оцифровки и организация последующего хранения электронных копий в соответствии с французскими национальными стандартами, и только в этом случае можно будет рассчитывать на презумпцию верности и аутентичности электронных копий в случае судебных споров или расследований.

Ну а поскольку анализ рисков и обеспечение соответствия существующим требованиям – дело сложное, читателю недвусмысленно намекают на то, что дешевле будет потратиться на услуги внешних консультантов (нетрудно догадаться, кого именно лучше пригласить).



## ИСО: ОПУБЛИКОВАН СТАНДАРТ ISO 17068:2017 «ХРАНИЛИЩЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЫ»

Источник: сайт ИСО <https://www.iso.org/standard/66760.html>

Автор: Наташа Храмцовская

Сайт Международной организации по стандартизации (ИСО) сообщил о публикации в октябре 2017 года стандарта **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>) объёмом 33 страницы.

Подготовленный техническим подкомитетом TC46/SC11 документ представляет собой переработку ранее опубликованного одноименного Технического отчета ISO/TR 17068:2012, о котором я писала здесь: [http://rusrim.blogspot.ru/2012/10/blog-post\\_29.html](http://rusrim.blogspot.ru/2012/10/blog-post_29.html). На блоге также был материал о ходе разработки стандарта, см. [https://rusrim.blogspot.ru/2015/10/blog-post\\_7.html](https://rusrim.blogspot.ru/2015/10/blog-post_7.html).

В аннотации отмечается:

«Стандарт ISO 17068:2017 устанавливает требования к хранилищу доверенной третьей стороны (trusted third party repository, TTPR) в интересах поддержки деятельности уполномоченной службы доверенного хранения, с тем, чтобы та могла обеспечить доказуемую целостность и аутентичность электронных документов клиентов и служить источником надежных доказательств.

Стандарт ISO 17068:2017 применим к услугам хранения в течение установленных сроков используемых в качестве доказательств электронных документов (и, соответственно, к услугам хранилища), для организаций как частного, так и государственного секторов.»

Во введении в стандарт есть интересное упоминание проблем хранения электронных документов, подписанных усиленными электронными подписями:

«Чтобы избежать оспаривания деловых электронных документов в течение периода времени, пока они нужны для исполнения правовых обязательств и требований по срокам хранения, критически-важно обеспечить сохранение их аутентичности, надежности и целостности.

Электронные цифровые подписи (*в европейской терминологии, усиленные электронные подписи – Н.Х.*) - это хорошо известный способ удостоверения того, что электронные документы не подвергались несанкционированному вмешательству. Однако, поскольку ЭЦП защищает целостность лишь в течение срока ее действия (обычно от одного до двух лет или меньше – *грубейшая ошибка, говорящая о том, что, к сожалению, даже*

*эксперты ИСО порой плохо ориентируются в тонкостях информационного права. Подпись не становится недействительной по истечению срока действия сертификата ключа проверки, однако в ряде случаев перепроверить её, если это потребуется, может быть затруднительно. – Н.Х.), то большинство подписанных электронными цифровыми подписями документов не обеспечивают их целостность дольше, чем время действия подписей (ещё одна ошибка – как раз целостность может подтверждать даже ЭЦП неустановленного лица, если можно доказать, что она была наложена в момент создания документа или близкий к нему. Проблема возникает с подтверждением личности и полномочий подписанта т.е. аутентичности – Н.Х.). В результате в рамках отдельной системы хранения документов может оказаться весьма проблематичным доказывание целостности содержащейся в ней документов в течение всего срока хранения, если этот срок превышает срок действия электронной цифровой подписи.*

Возможным решением является использование услуг хранилища доверенной третьей стороны (ТТР). ТТР определяется как квалифицированный сервис услуг хранения третьей стороны, обеспечивающий, что доверенные ему клиентом электронные документы остаются надёжными и аутентичными, с возможностью это подтвердить, – с целью обеспечения клиентам надёжного доступа к управляемым службой электронным документам в течение всего срока хранения. ТТР обеспечивает клиентам надёжные услуги в отношении электронных документов, которые должны проверяться заинтересованными сторонами (например, инспекторами, аудиторами, оценщиками). Эти услуги ТТР полезны для установления допустимости электронных документов клиентов в качестве допустимых доказательств».

С корректностью формулировок есть проблемы, особенно в связи с тем, что стандарт изначально готовился южнокорейскими специалистами, и языковой барьер сыграл свою роль – однако в то же время документ отражает многолетний успешный опыт одной из самых передовых стран мира в части внедрения ИКТ и организации архивного хранения электронных документов, поэтому стандарт заслуживает самого серьёзного внимания.

И, конечно же, ещё одна причина, по которой такой стандарта может быть интересен для российских специалистов – это наша собственная успешная и все время расширяющаяся практика использования услуг доверенных третьих сторон, в том числе и в части поддержки юридически-значимого документооборота, а также хранения бумажных и электронных документов.

Содержание стандарта следующее:

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Общее представление о ТТРР-хранилище доверенной третьей стороны
  5. Услуги ТТРР
  6. Технологические требования
  7. Оперативные требования
- Библиография



## **ИСО: ОПУБЛИКОВАНА НОВАЯ РЕДАКЦИЯ СТАНДАРТА ПРИНЦИПОВ УПРАВЛЕНИЯ МЕТАДАННЫМИ ДОКУМЕНТОВ**

Источник: сайт ИСО <https://www.iso.org/standard/73172.html>

Автор: Наташа Храмцовская

Как сообщил сайт Международной организации по стандартизации, в октябре 2017 года был опубликован стандарт **ISO 23081-1:2017 «Информация и документация – Процессы управления документами – Метаданные документов – Часть 1: Принципы»** (Information and documentation - Records management processes - Metadata for records - Part 1: Principles, см. <https://www.iso.org/standard/73172.html> и <https://www.iso.org/obp/ui/#iso:std:iso:23081:-1:ed-2:v1:en>) объёмом 21 страница, подготовленный техническим подкомитетом TC46/SC11 «Управление документами».



Новый документ заменил ранее действовавший стандарт ISO 23081-1:2006, который был адаптирован в России как ГОСТ Р ИСО 23081-1-2008 «Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы», <http://protect.gost.ru/v.aspx?control=8&baseC=6&id=166090>.

Как отмечается в аннотации, в стандарте ISO 23081-1 сформулирована концепция создания, управления и использования метаданных для управления документами и разъясняются основные принципы, которым метаданные подчиняются.

Данный документ содержит рекомендации, способствующие пониманию, внедрению и использованию метаданных в рамках применения основного стандарта по управлению документами ISO 15489. В нем говорится о значении «делопроизводческих» метаданных для деловых процессов; о различных ролях, выполняемых метаданными; и о различных типах метаданных, поддерживающих процессы основной деловой деятельности и управления документами. В документе также предлагается концепция управления этими метаданными.

Стандарт ISO 23081-1 не определяет обязательного для реализации на практике набора метаданных, поскольку они будут различными в зависимости от потребностей организации и от законодательства, в рамках которого она работает. В нем, однако, дана оценка основных известных наборов метаданных в свете требований стандарта ИСО 15489.

Две другие части стандарта - ISO 23081-2 и ISO 23081-3 – более подробно объясняют вопросы управления метаданными и содержат практические рекомендации по вопросам реализации положений стандарта и по поводу того, как оценивать наборы метаданных для управления документами на соответствие принципам, сформулированным в ISO 23081-1.

ISO 23081-1:2017 устанавливает принципы, лежащие в основе и определяющие порядок управления делопроизводческими метаданными. Эти принципы применимы:

- к документам и их метаданным;
- ко всем процессам, которые их затрагивают;
- ко всем системам, в которых они располагаются;
- ко всем организациям, которые несут ответственность за управление ими.

Содержание документа следующее (оно не изменилось по сравнению с предыдущей редакцией):

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Метаданные для управления документами

5. Назначение метаданных для управления документами и перспективы их использования

6. Роли и обязанности

7. Взаимосвязь метаданных для управления документами и метаданных, используемых для других целей

8. Управление метаданными

9. Типы метаданных, необходимые для реализации положений стандарта ISO 15489-1

Библиография

# ИСО: ИДЁТ РАБОТА НАД НОВОЙ РЕДАКЦИЕЙ СТАНДАРТА АУТЕНТИФИКАЦИИ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ УСИЛЕННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

Источник: сайт ИСО <https://www.iso.org/standard/67115.html>

Автор: [Наташа Храмцовская](#)



Как сообщает официальный сайт ИСО, выходит на финишный этап работа технического комитета ИСО JTC1/SC27 по подготовке новой 3-й редакции стандарта **ISO/IEC 9798-3 «Информационные технологии. Методы защиты. Аутентификация объектов. Часть 3. Механизмы с применением методов цифровой подписи»** (Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques).

Стандарт впервые был принят в далёком 1993 году. В настоящее время действует 2-я редакция 1998 года, которая дополнялась и корректировалась в 2009, 2010 и 2012 годах (см. <https://www.iso.org/standard/29062.html> и <https://www.iso.org/obp/ui/#!iso:std:29062:en>).

В настоящее время идёт голосование по DIS-проекту международного стандарта (см. <https://www.iso.org/standard/67115.html> и <https://www.iso.org/obp/ui/#iso:std:iso-iec:9798:-3:dis:ed-3:v1:en>), объём текста которого существенно увеличился по сравнению с предыдущей редакцией – с 12 до 32 страниц.

Как отмечается в аннотации, в данном документе определены механизмы аутентификации объектов / сущностей (entities) с использованием электронных цифровых подписей на основе асимметричных криптографических методов. Электронная цифровая подпись используется для проверки идентичности объекта.

В документе описаны десять механизмов. Первые пять механизмов не предусматривают использование онлайн-услуг доверенной третьей стороны, в то время, как последние пять используют такого рода услуги. В обеих этих двух категориях два механизма обеспечивают одностороннюю аутентификацию, а остальные три - взаимную аутентификацию.



Содержание документа следующее:

Предисловие

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Символы и сокращения

5. Общие положения

6. Требования

7. Механизмы без использования онлайн-услуг доверенной третьей стороны

8. Механизмы с использованием онлайн-услуг доверенной третьей стороны

Библиография



## **ИССЛЕДОВАНИЕ: ЛЕНТОЧНЫЕ, ДИСКОВЫЕ И ОБЛАЧНЫЕ ХРАНИЛИЩА. КАКОВЫ РЕАЛЬНЫЕ ЗАТРАТЫ?**

Источник: <http://naar.ru/news/issledovanie-lentochnye-diskovye-i-oblachnye-khranilishcha/>

**Оценка общих затрат на хранение данных – важнейшая задача для специалистов, решающих вопросы долговременной сохранности информации.** Сотрудники одной из американских компаний решили подсчитать, сколько же на самом деле стоит хранение на ленте, на дисках и в облаке.

ИТ-специалисты, работающие с данными, заняты решением широкого спектра вопросов: обеспечение доступа к информации, ее долговременная сохранность и защита, комплаенс и др. Как правило, чтобы комплексно их «закрыть», используется стратегически оправданная комбинация технологий.

Ленточные, облачные и дисковые хранилища (на основе жестких дисков, HDD) – самые популярные места хранения данных. Принято считать, что стоимость хранения на ленте (из расчета на 1 гигабайт данных) в два раза дороже, чем на HDD, если сравнивать «сырую» стоимость – за ленточный картридж и за жесткий диск. Однако, по некоторым расчетам, новое поколение ленточных картриджей LTO-7 значительно дешевле SATA HDD: примерно на 1% за каждый гигабайт.

При выборе типа хранилища важно учитывать не только стоимость носителей, но и затраты на последующее копирование и транспортировку данных в связи с их обменом, необходимостью выполнить требования комплаенс и политики на случай ЧС. В случае форс-мажора ленточные носители можно без серьезных затруднений перевезти в другое место. Из-за особенностей строения жестких дисков с ними этот «трюк» выполним, но с большими затратами.

Что еще входит в смету расходов? Согласно данным аналитиков из Enterprise Strategy Group (см. [“Analyzing the Economic Value of LTO Tape for Long-term Data Retention”. ESG Report February 2016](#)), в этом списке должны быть следующие позиции: оборудование, программное обеспечение, инфраструктура/электроэнергия, поддержка, кадры, миграция и доступ к данным. Именно эти параметры отслеживались на протяжении десяти лет работы ленточных хранилищ, используемых для долгосрочного хранения данных. В качестве базы для сравнения были собраны данные по дисковым и облачным хранилищам.

Внедрение ленточных технологий показало «внушительные 577% окупаемости инвестиций за 10 лет с учетом затрат, которые удалось избежать (avoided cost), и усовершенствований, связанных с реализацией модели новой экономики» (новую экономику характеризует преобладание знаний и информационных технологий). Подробные результаты оценки стоимости разных хранилищ представлены в таблице.

«Вопреки предубеждениям, что лента – это ненадежный, медленный и устаревший носитель, мы рады сообщить, что ленточные хранилища находятся в полном здравии и имеют прекрасное будущее в организациях всех размеров», – заключают аналитики Enterprise Strategy Group.

Они также добавляют, что в ходе лабораторных испытаний LTO-7 показали себя достойно. «Вероятность, что в вас ударит молния, в миллион раз выше, чем вероятность того, что вы столкнетесь с невозстанавливаемой ошибкой в ленточном носителе LTO-7», – пишут авторы отчета. Правда, следует обратить внимание на то, что исследование ESG проводилось по инициативе консорциума LTO, в который входят крупнейшие производители ленточных носителей Hewlett-Packard, IBM и Quantum.

Оценка стоимости разных видов хранилищ данных:  
ленточные, дисковые и облачные

Category	LTO Solution	All-disk PMO	Disk/Cloud Hybrid PMO
Hardware	\$496,396	\$3,893,830	\$2,858,598
Software	\$210,000	\$172,894	\$172,894
Media	\$120,710	\$2,159,881	\$1,727,905
Cloud Services	\$0	\$0	\$356,248
Infrastructure	\$527,547	\$982,403	\$787,429
Maintenance and Support	\$85,248	\$1,705,537	\$1,291,441
Staff Personnel	\$910,000	\$6,779,500	\$5,960,500
Data Migration Costs	\$20,284	\$174,640	\$139,712
Data Access Costs	\$40,915	\$40,915	\$606,028
<b>Total ten-year cost of ownership</b>	<b>\$2,411,099</b>	<b>\$16,808,264</b>	<b>\$13,900,747</b>

# ЗМІСТ

Передмова.....	1
Пережиток прошлого: Николаевские депутаты возмутились значительным тратам на микрофильмирование документов.....	3
СОМ – микрофильмирование в практике архивов.....	4
Метод хранения цифровой информации на аналоговом носителе с использованием штрих-кодов.....	12
Уряд удосконалив порядок проведення перевірок у сфері страхового фонду документації.....	15
Конференция 2017 года секции деловых архивов Международного совета архивов: Какие проблемы будут для нас основными через 5 лет?.....	16
Польша: Подготовлен проект модернизации интегрированной архивной информационной системы ZoSIA.....	20
ИСО: Опубликован кодекс практики э-раскрытия.....	22
Европейский институт телекоммуникационных стандартов ETSI опубликовал технический отчет по исполнению Директивы по сетевой и информационной безопасности.....	23
ИСО: Обсуждается проект нового стандарта по технологиям и методам облачных вычислений.....	26
Новые международные стандарты и проекты стандартов в сфере облачных вычислений.....	28
Франция: Компания Locarchives опубликовала «белую книгу» по надёжной оцифровке и последующему уничтожению оригиналов....	30
ИСО: Опубликован стандарт ISO 17068:2017 «Хранилище электронных документов доверенной третьей стороны».....	33
ИСО: Опубликована новая редакция стандарта принципов управления метаданными документов.....	35
ИСО: Идёт работа над новой редакцией стандарта аутентификации объектов с использованием усиленной электронной подписи.....	37
Исследование: Ленточные, дисковые и облачные хранилища. Каковы реальные затраты?.....	38