ПЕРЕДМОВА

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

У публікації «Обеспечение электронной сохранности за гроши: Невозможно?» розглянуто проблеми збереження електронних документів, наведено можливі шляхи вирішення цих питань.

У публікації «Зберігання електронних документів: як правильно організувати?» наведено витяги з законів та керівних документів щодо зберігання електронних документів.

У публікації «Архивы группы «Всемирный Банк» выложили набор методических материалов по управлению документами» наведено дорожню карту управління документами.

У публікації «Федеративное управление документами: Объединение всех деловых документов в единое согласованное представление» розповідається про вирішення проблеми управління документами що зберігаються в кількох сховищах контенту, ряді ділових додатків, різних хмарних додатках і додатках для соціальних мереж за допомогою федеративного (об'єднаного) управління документами.

У публікації «Судьба Перечня НТД: Неожиданный поворот» розповідається, про розробку та затвердження переліків документів, які утворюються під час діяльності федеральних органів виконавчої влади, а також підвідомчих їм організацій, з вказівкою термінів зберігання.

У публікації «Южная Корея реформирует свой «Закон об электронных подписях» в пользу технологического нейтралитета» розповідається про зміни направлені на забезпечення більшої гнучкості під час вибору та використання електронних подписів у відповідності з світовими тенденціями.

У публікації ««Стратегическое управление информацией» и продолжающаяся война с управлением документами» розповідається, що «Стратегічне управління інформацією» - це фактично маркетинговий термін, який створили керівники корпоративних служб продаж.

У публікації «США: Идеи «Совета по рассекречиванию в интересах общественности» по реформированию системы грифов секретности» розповідається про модернізацію системи установлення та зняття грифів таємності для відомостей що містять державну таємницю.

У публікації «США: «Совет по рассекречиванию в интересах общественности» дал ответы на ряд вопросов общественности» розповідається про модернізацію системи установлення та зняття грифів таємності для даних що містять державну таємницю.

У публікації «Национальный институт стандартов и технологий США начал публичное обсуждение специальной публикации NIST SP 800-53B «Базовые профили мер контроля и управления для информационных систем и организаций»» розповідається про викладений для публічного обговорення

проєкт нової спеціальної публікації NIST SP 800-53B «Базові профілі заходів контролю і управління для інформаційних систем і організацій». Звертаються до представників установ та громадян з проханням до участі у обговоренні.

У публікації «США: «Конференция Седона» опубликовала для публичного обсуждения проект 2-й редакции «Комментария по доказательствам в виде сохраняемой электронным образом информации и их допустимости»» розповідається про викладену для публічного обговорення версію другої редакції документа «Коментар Конференції Седона по доказам у вигляді зберігаємої електронним чином інформації та можливості її допущення».

У публікації «США: Конференция Седона опубликовала проект Комментария по поводу исполнимости в США решений, принятых на основании европейского закона о защите персональных данных GDPR» розповідається про викладений для публічного обговорення коментар конференції мета якого полягає в тому, щоб дати зацікавленим сторонам в ЄС і США рекомендації по факторам - як юридичним, так і практичним - які пов'язані з забезпеченням виконання вимог GDPR через судові розгляди в США.

У публікації «Открытые данные: Преодоление неравенства в доступе к данным» розповідається про нерівний доступ до великих обсягів даних або «цифровій нерівності». Ідея про ліквідацію цього розриву послужила поштовхом для запуску компанією Microsoft «Кампанії за відкриті дані».

У публікації «ePADD: Архивирование электронных писем с помощью инструмента с открытым исходным кодом» розповідається про розробку програмного забезпечення з метою створення надійного інструменту з відкритим вихідним кодом для роботи з архівом електронної пошти.

У публікації «Национальный институт стандартов и технологий США начал публичное обсуждение специальной публикации NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения»» розповідається про викладену для публічного обговорення версію документа.

У публікації «Стандарт ISO/IEC 29134:2017 «Руководство по оценке воздействия на неприкосновенность частной жизни»» розповідається про принципи проведення «оцінки впливу на недоторканність приватного життя». Наведено рекомендації та зміст документа.

ОБЕСПЕЧЕНИЕ ЭЛЕКТРОННОЙ СОХРАННОСТИ ЗА ГРОШИ: НЕВОЗМОЖНО?

Источник: блог МСА https://blog-ica.org/2020/06/10/digital-preservation-on-a-shoestring-impossible/ Антея Селес (Anthea Seles)

Обеспечение электронной сохранности должно быть стандартной услугой, поддерживаемой и предлагаемой архивами, однако многих архивистов пугает подобная перспектива; они часто не знают, с чего начать, особенно когда имеющиеся в их распоряжении ресурсы (кадры, инфраструктура и финансы) невелики. Так возможна ли электронная сохранность «за гроши»? И если да, то каким образом? А если нет, то что в таком случае происходит с ценными электронными документами?

Стандарты и модели зрелости электронной сохранности

Существуют два международных стандарта, которые направляют и поддерживают деятельность в области электронной сохранности: это стандарт ISO 14721:2012 «Системы передачи данных и информации о космическом пространстве. **Открытая архивная информационная система (OAIS). Эталонная модель**» (Space data and information transfer systems - Open archival information system (OAIS) - Reference model) и стандарт ISO 16363:2012 «Системы передачи данных и информации о космическом пространстве – **Аудит и сертификация доверенных электронных хранилищ**» (Space data and information transfer systems - Audit and certification of trustworthy digital repositories).

OAIS - это концептуальная модель, а не модель для сертификации; это означает, что она была разработана с целью определения общей терминологии для представителей различных специальностей, используемой при обсуждении электронных объектов, их захвата, сохранения и распространения. Не существует такой вещи, как «хранилище, соответствующее OAIS», и если Вы хотите определить степень соответствия электронного хранилища, то Вам нужно использовать сертификационный стандарт, такой, как ISO 16363. Этот стандарт описывает различные элементы, которые должны присутствовать в электронном хранилище для того, чтобы оно могло быть сертифицировано как «доверенное».

Во время обучения в аспирантуре Университетского колледжа Лондона (University College London) я изучала и исследовала применимость этих двух стандартов для использования в ситуации ограниченных ресурсов (см. https://discovery.ucl.ac.uk/id/eprint/1473881/) и поняла, что они исходят из целого ряда предположений – да, даже концептуальная модель! – помимо прочего, об инфраструктуре и наличии обученного персонала. Я полагаю, что выполнение требований сертификационного стандарта ISO 16363 не по силам даже для учреждений с хорошими ресурсами; но я согласна с тем, что сертификация на соответствие многим стандартам сертификации электронных

хранилищ является недостижимой, если организация не располагает значительными ресурсами.

Конечно, сертификация должна быть требовательной для того, чтобы обеспечить надлежащий захват, сохранение и доступность электронных материалов, – но если требования сертификационных стандартов недостижимы даже для самых хорошо обеспеченных ресурсами организаций, то в чём тогда ценность этой сертификации?

Использование модели зрелости может быть хорошим способом помочь организациям пройти свой путь к сертификации, а модель быстрой оценки (Rapid Assessment Model, https://www.dpconline.org/our-work/dpc-ram), разработанная британской Коалицией по электронной сохранности (Digital Preservation Coalition, DPC), является удобным инструментом для определения организациями их отправной точки и дальнейших действий по совершенствованию. Но все ещё остается вопрос о том, как будет выглядеть электронная сохранность при ограниченных ресурсах.

До конца света ещё далеко

Возможно, я нарисовала довольно мрачную картину в плане применимости стандартов электронной сохранности, но это ещё не конец света! Когда я пришла на кафедру архивного дела, у нас не было практического обучения по вопросам электронной сохранности – сейчас ситуация меняется, и это здорово! Но в мире по-прежнему есть факультеты и кафедры архивного дела и информатики, где такого рода подготовка отсутствует или недоступна. Более того, курсы повышения квалификации по данной теме немногочисленны, хотя здесь ситуация тоже улучшается. В качестве примера курсов начального уровня можно назвать учебный курс DPC «От новичка до ниндзя» (Novice to ninja, https://www.dpconline.org/knowledge-base/training/n2kh-online-training - *точное название «От новичка до знатока», Novice to Know-How*) и предстоящий курс Международного совета архивов «Управление электронными архивами» (Managing Digital Archives, осень 2020 года, см. https://www.ica.org/en/training-programme).

Также доступны отличные вебинары, на которых обсуждается и анализируется вопрос о том, что следует учитывать учреждениям, когда они начинают заниматься электронной сохранностью. Взгляните на один из них, подготовленный университетом Вестминстера (University of Westminster), см. https://www.youtube.com/watch?v=k-SVO6lQEZM&feature=youtu.be . Я уверена, что можно найти много других ресурсов, и буду благодарна за информацию о них!

Итак, я уже и так, и сяк касалась этого вопроса, - но как всё-таки выглядит электронная сохранность при скудных ресурсах? Если у организации нет ресурсов и она ищет, с чего бы начать, то я бы назвала три важнейших аспекта:

- **Определите свои файловые форматы** - Вам сначала нужно понять, что у Вас есть, чтобы понять, как начать работу по обеспечению сохранности этих материалов;

- **Проверка целостности** - также известная как вычисление контрольных сумм (*или хешей*), которые представляют собой буквенно-цифровые последовательности, позволяющие Вам убедиться в том, что электронные документы со временем не были попорчены или изменены;
- **Резервные копии** – «Копируйте!» - это мантра электронного архивиста. Обеспечение сохранности электронных документов означает, что Вы должны обеспечить избыточность, так что если документы будут повреждены, у Вас должна иметься на этот случай резервная копия. Важно иметь как минимум 2-3 копии Ваших электронных документов / фондов.

Существует множество бесплатных инструментов, которые помогут Вам выполнить идентификацию файловых форматов и проверки целостности. Одним из знакомых и нравящихся мне инструментов является программа DROID (https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/file-profiling-tool-droid/), поддерживаемая Национальными Архивами Великобритании, - но есть и другие. Опять же, если у Вас есть хороший, бесплатный, простой в использовании инструмент, дайте мне знать!

Трудно описать в коротком посте в блоге все различные аспекты выполнения работы по обеспечению электронной сохранности при скудных ресурсах, и перечислить всё, о чём стоит подумать. Одна вещь, о которой я хочу сказать, заключается в том, что обеспечение электронной сохранности в таких условиях – это в огромной степени трудоёмкая ручная работа, сфокусированная на деталях! «Электронно-цифровой» - **не то же самое**, что «автоматизированный». Также Вам очень пригодятся навыки работы с CSV-файлами и с Excel, поэтому Вам стоит посетить курсы Excel или познакомиться с учебными пособиями по Excel на сайте YouTube. Существуют замечательные ресурсы, и я надеюсь, что коллеги поделятся своим опытом обеспечения электронной сохранности в условиях, когда у Вас ничего нет.

Мой призыв к профессиональному сообществу: не бойтесь попробовать! Я знаю, что это страшновато, но существует множество ресурсов, которые могут в этом помочь. Каждый должен с чего-то начать.

ЗБЕРІГАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ: ЯК ПРАВИЛЬНО ОРГАНІЗУВАТИ?

Джерело інформації: https://news.dtkt.ua/accounting/reposts/63470

Електронні форми первинних документів, а також архів файлів звітності повинні зберігатися на електронних носіях інформації у формі, що дає змогу здійснити перевірку їх цілісності на цих носіях.

Податківці у підкатегорії 129.03 «ЗІР» зауважили, що платники податків зобов'язані забезпечити зберігання документів, визначених п. 44.1 ст. 44 ПКУ, а також документів, пов'язаних із виконанням вимог законодавства, контроль за дотриманням якого покладено на контролюючі органи, протягом визначених законодавством термінів, але не менш як визначено ст. 44 ПКУ.

Згідно зі ст. 13 Закону України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» (далі – Закон №851) зі змінами та доповненнями суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов’язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб’єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така установа додержується вимог цієї статті. Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

Частиною третьою ст. 8 Закону України від 16 липня 1999 року №996-XIV «Про бухгалтерський облік та фінансову звітність в Україні» зі змінами та доповненнями встановлено, що відповідальність, зокрема, за збереження оброблених документів, регістрів і звітності протягом встановленого терміну, але не менше трьох років, несе уповноважений орган (посадова особа), який здійснює керівництво підприємством, або власник відповідно до законодавства та установчих документів.

Отже, електронні форми первинних документів, пов’язаних з обчисленням і сплатою податків та зборів (крім єдиного внеску на загальнообов’язкове державне соціальне страхування), а також архів файлів звітності, поданої контролюючим органам в електронному вигляді, повинні зберігатися платниками податку на електронних носіях інформації у формі, що дає змогу здійснити перевірку їх цілісності на цих носіях, протягом строку, встановленого законодавством для зберігання відповідних документів на папері.

АРХИВЫ ГРУППЫ «ВСЕМИРНЫЙ БАНК» ВЫЛОЖИЛИ НАБОР МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ПО УПРАВЛЕНИЮ ДОКУМЕНТАМИ

Источник: новостная рассылка МСА / сайт Всемирного Банка https://www.worldbank.org/en/about/archives/RecordsManagementRoadmap

Архивы группы «Всемирный банк» (World Bank Group Archives) опубликовали **«Дорожную карту управления документами»** (Records Management Roadmap, https://www.worldbank.org/en/about/archives/RecordsManagementRoadmap), адресованную государственным органам и организациям государственного сектора, с целью помочь им внедрить эффективные стратегические программы управления документами.

Почему Вам следует использовать «Дорожную карту»?

Данная «Дорожная карта» призвана помочь Вашей организации спланировать и разработать эффективную программу управления документами – такую, которую Ваша организация сможет поддерживать и выполнять в течение длительного времени. Несколько частей, составляющих эту «Дорожную карту», образуют пакет - «инструментальный набор», - который должен помочь организациям:

- Оценить сильные и слабые стороны, выявить недостатки текущих практик управления документами;
- Определить цели изменений и совершенствования этих практик;
- Спланировать стратегические действия, направленные на совершенствование оперативной деятельности;
- Выявлять источники наилучшей практики;
- Обеспечивать непрерывное совершенствование с течением времени.

Каким образом Ваша организация формирует хорошую программу управления документами? Данная дорожная карта разработана для того, чтобы помочь Вам в этом. Отправляйтесь же в путь!

«Дорожная карта» представляет собой инструментальный набор из девяти частей (*девятой частью является общее Предисловие*) для организаций, желающих улучшить управление своими документами. Он включает руководства и рекомендации, инструменты оценки, объяснения терминов и понятий, а также ресурсы, позволяющие организациям оценить свои потребности в плане управлении документами и определить приоритеты для дальнейших действий.

«Дорожная карта управления документами» состоит из девяти частей:

«Предисловие, авторские права и благодарности» (Foreword, Copyright and Acknowledgements), см. http://pubdocs.worldbank.org/en/661661594921725648/pdf/RM-Roadmap-Foreword.pdf

Часть 1: «Введение» (Part 1: Introduction). Данный документ объясняет цель и структуру «Дорожной карты», описывает целевую аудиторию инструментов, и содержит предложения о том, как Вы могли бы использовать данный инструмент для поддержки управления документами в Вашей собственной организации.

http://pubdocs.worldbank.org/en/162301594065762880/WBG-RM-Roadmap-002-Part-1-Introduction-FINAL-PDF.pdf

Часть 2: «Карта» (Part 2: Map). Данный документ иллюстрирует все пункты назначения и промежуточные вехи, предусмотренные «Дорожной картой» см. http://pubdocs.worldbank.org/en/439481594065766990/WBG-RM-Roadmap-004-Part-2-Outline-Map-FINAL-PDF.pdf

Часть 3: «Обзор основных принципов и практик управления документами» (Part 3: Overview of key records management principles and practices). Описывает концептуальную основу инструмента оценки уровня управления документами. http://pubdocs.worldbank.org/en/694361594065756366/WBG-RM-Roadmap-005-Part-3-RM-Overview-FINAL-PDF.pdf

Часть 4: «Инструмент оценки уровня управления документами» (Part 4: Records management assessment tool). Помогает Вашей организации определить свои сильные и слабые стороны в сфере управлении документами, см. http://pubdocs.worldbank.org/en/473561594065771119/WBG-RM-Roadmap-006-Part-4-Assessment-Tool-FINAL-PDF.pdf

Часть 5: «Список контрольных вопросов для оценки уровня управления документами» (Part 5: Assessment checklist). Помогает подтвердить степень продвижения Вашей организации в достижении целей и выполнении этапов, установленных по результатам оценки, см. http://pubdocs.worldbank.org/en/377591594065764926/WBG-RM-Roadmap-007-Part-5-Assessment-Checklist-FINAL-MASTER.xlsx

Часть 6: «Перечень разрабатываемых документов» (Part 6: List of outputs). Перечисляет документы, которые Ваша организация может разработать для поддержки совершенствования практики управления документами, см. http://pubdocs.worldbank.org/en/859381594065769059/WBG-RM-Roadmap-008-Part-6-Outputs-FINAL-PDF.pdf

Часть 7: «Перечень ресурсов» (Part 7: List of resources). Помогает Вашей организации найти примеры передового опыта, руководства и рекомендации по планированию и развитию управления документами, см. http://pubdocs.worldbank.org/en/489521594065775305/WBG-RM-Roadmap-009-Part-7-Resources-FINAL-PDF.pdf

Часть 8: «Глоссарий» (Part 8: Glossary). Содержит ключевые термины сферы управления документами, используемые в «Дорожной карте»., см. http://pubdocs.worldbank.org/en/902721594065773238/WBG-RM-Roadmap-010-Part-8-Glossary-FINAL-PDF.pdf

«Дорожная карта» был подготовлена Лорой Миллар (Laura Millar), специалистами по управлению документами группы «Всемирного Банка» и консультантами по вопросам государственного управления. Целью «Дорожной карты» является поддержка усилий государственных органов и организаций государственного сектора в области планировании и проектирования

эффективных программ управления документами. В «Дорожной карте» подчеркивается значение управления документами для обеспечения подотчетности, прозрачности и эффективности, которые имеют ключевое значение для хорошего государственного управления и для укрепления способности государственных органов оказывать высококачественные услуги и поддержку гражданам.

Хотя основной целевой аудиторией «Дорожной карты» являются государственные органы и организации государственного сектора, мы считаем, что данный инструмент будет полезен организациям любого типа, где бы они ни действовали.

С комментариями или вопросами, пожалуйста, обращайтесь в Архивы группы «Всемирного Банка».

С наилучшими пожеланиями всем Вам,

Эйприл Миллер (April Miller) Менеджер архивно-библиотечной службы группы «Всемирный банк»

ФЕДЕРАТИВНОЕ УПРАВЛЕНИЕ ДОКУМЕНТАМИ: ОБЪЕДИНЕНИЕ ВСЕХ ДЕЛОВЫХ ДОКУМЕНТОВ В ЕДИНОЕ СОГЛАСОВАННОЕ ПРЕДСТАВЛЕНИЕ

Источник: блог компании Formtek http://formtek.com/blog/records-management-federating-all-business-records-into-a-single-consistent-view/

Управление документами является сложным делом, поскольку лишь очень немногие компании хранят свои документы в одном месте. К тому же они часто используют несколько хранилищ контента, ряд деловых приложений и различные облачные приложения и приложения для социальных сетей. То, что документы могут храниться в любом из этих мест, делает проблематичным применение средств управления документами в отношении многих различных типов документов.

Эту проблему пытается решить федеративное (объединённое) управление документами (federated records management). При этом подходе используется централизованное приложение для каталогизации, отслеживания и поиска контента документов, которые хранятся во многих местах. Сам контент не перемещается и хранится «по месту».

Когда элемент контента регистрируется как документ, то, в случае использования федеративного подхода, его не нужно перемещать в центральное хранилище. И как только документ включается в объединённый каталог, его можно отыскивать при поиске, выполняемом в интересах управления документами и электронного раскрытия (eDiscovery); при этом

документ остаётся отыскиваемым и доступным для пользователей в его «родном» хранилище или приложении.

При федеративном управлении документами, номенклатуры дел и инструкции в отношении жизненного цикла (*иными словами, правила структуризации и указания по срокам хранения и действиям по их истечении*) применяются централизованно, а политики для всех документов компании можно просматривать и управлять с единой согласованной информационно-контрольной панели (dashboard). Такие поставщики, как Alfresco и Gimmal, уже предлагают инструменты для федеративного управления документами.

Директор по продуктам компании Alfresco Тони Гроут (Tony Grout, https://www.bloomberg.com/profile/person/20966912) говорит, что «в эти беспрецедентные времена ключевой по важности является возможность управлять информацией там, где она сейчас находится («управление по месту»), и контролировать контент и документы, которые распределены по различным системам. Где бы контент ни хранился, сотрудники в таком случае могут выполнять поиск и управлять документами (а также применять согласованные политики отслеживания сроков хранения для всего своего контента) – независимо от того, хранится ли он в приложениях Alfresco или иных разработчиков» (https://www.businesswire.com/news/home/20200422005043/en/Alfresco-Unveils-New-Generation-Federation-Services).

СУДЬБА ПЕРЕЧНЯ НТД: НЕОЖИДАННЫЙ ПОВОРОТ

Источник: сайт YouTube https://www.youtube.com/watch?v=QLK4Ccep_FA

25 июня 2020 года на научно-практическом семинаре «Перспективы и задачи комплектования НТД в условиях современной работы госархивов» прозвучало восемь докладов, семь из которых представили архивисты-практики, непосредственно занимающиеся комплектованием и хранением научно-технической документации в государственных архивах, – а заведующая отделом архивоведения Всероссийского Научно-исследовательского института документоведения и архивного дела (ВНИИДАД) **Лада Павловна Афанасьева** выступила с докладом **«Сроки хранения научно-технической документации в типовых и отраслевых перечнях документов с указанием сроков хранения»** (в видеозаписи семинара, доступной по адресу https://www.youtube.com/watch?v=QLK4Ccep_FA , её доклад начинается на отметке 1 час 31 минут 10 секунд).

В докладе затронута еще одна больная тему отрасли – перечни видов документов с указанием сроков их хранения. Она отметила, что Правительством РФ 26 марта 2020 года было дано поручение №ДЧ-П44-2409

федеральным органам исполнительной власти «обеспечить разработку и утверждение перечней документов, образующихся в процессе деятельности федеральных органов исполнительной власти, а также в процессе деятельности подведомственных им организаций, с указанием сроков хранения». А это 71 федеральное ведомство!

В докладе приведены следующие данные. В период с 1970 по 1991 год, т.е. в советский период, был разработан 61 ведомственный перечень. В настоящее время у 71 федерального органа исполнительной власти в наличии имеются 24 ведомственных перечня.

Но самым интересным в этом докладе была информация о том, что ВНИИДАД приступил к работе по пересмотру «Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения». Работу планируется провести в 2020-2021 годах.

Изменение планов работ связано с тем, что у большей части федеральных органов исполнительной власти образуется значительное количество научно-технической документации, и без актуального перечня НТД они не смогут качественно разработать свои ведомственные перечни.

При этом вопросов по содержанию перечня НТД много, – например, к документам по автоматизированным системам. Сейчас только федеральных государственных информационных систем (ФГИС) зарегистрировано 348.

Одновременная разработка более 70 перечней – это беспрецедентное дело.

ЮЖНАЯ КОРЕЯ РЕФОРМИРУЕТ СВОЙ «ЗАКОН ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ» В ПОЛЬЗУ ТЕХНОЛОГИЧЕСКОГО НЕЙТРАЛИТЕТА

Источник: сайт LinkedIn https://www.linkedin.com/posts/activity-6669153850450067456-BmYY

Парламент Республики Корея 20 мая 2020 года одобрил пересмотренный Закон об электронных подписях, при этом внесённые изменения направлены на прекращение обязательного использования национальной системы цифровых сертификатов.

Эта система, которая использовалась для онлайн-аутентификации в течение более чем 20 лет, критиковалась пользователями как громоздкая и неудобная, в том числе из-за её требования ежегодного обновления сертификатов, а также из-за проблем, с которыми сталкиваются проживающие в Республике Корея иностранцы. Данная система также препятствовала

взаимному признанию зарубежных электронных подписей. Совсем недавно бизнес-группы выступили за реформу существующей системы, обосновывая это её полезностью для смягчения экономических последствий пандемии Covid-19.

Этот долгожданный шаг направлен на обеспечение большей гибкости в выборе и использовании электронных подписей в соответствии с мировыми тенденциями. Будет интересно проследить за дальнейшим развитием рынка и экономическим воздействием данного решения. Развивающиеся страны с особым вниманием изучить данный пример, учитывая то, как они полагаются на электронные цифровые подписи.

«СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ» И ПРОДОЛЖАЮЩАЯСЯ ВОЙНА С УПРАВЛЕНИЕМ ДОКУМЕНТАМИ

Источник: блог «Управление документами следующего поколения» https://nextgenrm.com/2020/05/28/information-governance-and-the-continuing-war-on-records-management/ Автор: *Дон Людерс*

Ровно шесть лет назад я опубликовал в ежеквартальном журнале по вопросам управления документами «IQ – The RIM Quarterly Magazine» для специалистов по управлению из Австралии и Азии (см. https://search.informit.com.au/browseJournalTitle;res=IELBUS;issn=0816-200X , *журнал выпускается Австралийской ассоциацией по управлению документами (Records Management Association of Australia, RMAA*), статью «Управление документами, стратегическое управление информацией и будущее управления жизненным циклом информации» (Records Management, Information Governance, and the Future of Information Lifecycle Management, https://nextgenerationrm.files.wordpress.com/2020/05/records-management-information-governance-and-the-future-of-information-lifecycle-management.pdf).

Отвлекитесь и прочитайте её, я подожду.

В то время, когда я опубликовал эту статью, мои тревожные предупреждения о попытках продвижения новой, совершенно неопределенной «дисциплины» за счёт традиционного управления документами остались почти полностью незамеченными. И всё же, практически по любой мерке, я оказался прав.

«Стратегическое (полномасштабное) управление информацией» (Information governance) никогда не было полностью отдельной профессиональной дисциплиной, сколько-нибудь существенно отличающейся

от управления документами. Его также нельзя считать «эволюционировавшей» формой традиционного управления документами. Оно не является областью строгих академических исследований с устоявшейся тематикой и долгой историей интеллектуальных дебатов. Также оно не занимает позиции признанной доверенной дисциплины, поддерживающей уникальные доверительные отношения между клиентом и управляемой информацией.

«Стратегическое управление информацией» - это фактически не более чем маркетинговый термин-пустышка, созданный руководителями корпоративных служб продаж, которые хотели, чтобы традиционные практики управления документами выглядели как ремесло, а не как древняя благородная дисциплина, которой является управление документами.

Продвижение «стратегического управления информацией» как самостоятельной дисциплины - это лишь одна битва в гораздо более широкомасштабной продолжающейся войне с управлением документами - войне, которая на протяжении почти двух десятилетий уже привела к неисчислимым потерям, утратам и человеческим трагедиям.

В течение последних нескольких лет вместе с рядом преданных своему делу профессиональных специалистов по управлению документами я делал всё возможное для защиты нашей профессии. И нам повезло, мы добились ряда реальных успехов (я особенно горжусь нашими усилиями, разоблачающими трагические результаты «стратегического управления информацией» в практике управления федеральными документами в США, описанными в расследовании, опубликовано в издании Epoch Times, https://www.theepochtimes.com/the-illusion-of-transparency_3234958.html).

Но, мы, к сожалению - небольшая группа, и наших усилий было недостаточно. Куда бы Вы ни посмотрели, продолжает царить информационный хаос. Его можно наблюдать в больших и малых организациях, в государственных учреждениях и частных компаниях – и последствия этого катастрофичны.

Настало время вернуть себе нашу профессию, отобрав её у людей, которые упорно хотят её уничтожить. Если Вы специалист в области управления документами, присоединяйтесь к нам в публичном осуждении движения за «стратегическое управление информацией», поддерживая возвращение к традиционным практикам жизненного цикла информации, которые специалисты по управлению документами применяли на протяжении тысячелетий.

Если Вы специалист в области управления документами, который также считает себя «специалистом в области стратегического управления информацией», пожалуйста, поймите, что на самом деле здесь никогда не было никакой разницы, и вернитесь в лоно нашей гордой профессии.

Ну а если вы «специалист по стратегическому управлению информацией», не имеющий никакого систематического образования или обучения по вопросам управления документами, прекратите себя обманывать. У вас нет законной карьеры. Либо начните изучать традиционное управление документами с целью получения осмысленной профессиональной

сертификации, такой как CRM (*«сертифицированный специалист по управлению документами», авторитетная в США и Канаде профессиональная сертификация*), либо, пока не поздно, серьезно подумайте о другой профессии, где Вы могли бы внести позитивный вклад в развитие общества.

США: ИДЕИ «СОВЕТА ПО РАССЕКРЕЧИВАНИЮ В ИНТЕРЕСАХ ОБЩЕСТВЕННОСТИ» ПО РЕФОРМИРОВАНИЮ СИСТЕМЫ ГРИФОВ СЕКРЕТНОСТИ

Источник: сайт Национальных Архивов США https://www.archives.gov/files/declassification/pidb/meetings/06052020-nara-pidb-writtentranscript.pdf

5 июня 2020 года американский «Совет по рассекречиванию в интересах общественности» (Public Interest Declassification Board, PIDB) провёл виртуальное публичное заседание в связи с публикацией подготовленного им доклада для Президента США за 2020 год «Видение для цифровой эпохи: Модернизация системы установления и снятия грифов секретности для сведений, содержащих государственную тайну» (A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System, см. https://www.archives.gov/files/declassification/pidb/recommendations/pidb-vision-for-digital-age-may-2020.pdf).

Через месяц на сайте Национальных Архивов США была выложена стенограмма этого заседания (см. https://www.archives.gov/files/declassification/pidb/meetings/06052020-nara-pidb-writtentranscript.pdf), с которой стоило бы познакомиться и тем, кто отвечает за секретное делопроизводство и рассекречивание.

Американские руководители и специалисты вполне откровенно признают накопившиеся проблемы – и то, что существующая практика мотивирует избыточное засекречивание, и то, что практику управления секретными документами срочно надо выводить если не на уровень 21-го века, то хотя бы конца 20-го. Решение проблемы они видят как в традиционных организационных мерах (назначение уполномоченного органа и руководителя, координирующего вопросы назначения и снятия грифов в масштабах федерального правительства), так и в широком применении современных технологий, особенно когда речь идёт о стремительно нарастающих объёмах изначально-электронных секретных документов.

Предлагается вниманию читателей фрагмент стенограммы, в котором генеральный юрисконсульт Сухопутных сил США Алисса Старзак рассказывает о предлагаемой «Советом по рассекречиванию в интересах общественности» реформе системе грифов секретности:

«…Кроме того, наша существующая система установления грифов секретности слишком сложна. Как и в нашем предыдущем отчете, мы продолжаем рекомендовать упрощение этой системы. Действующая трехуровневая система классификации с грифами «совершенно секретно» (Top Secret), «секретно» (Secret) и «конфиденциально» (Confidential – *примерно соответствует грифу «для служебного пользования»*) используется уже более 60 лет. Однако сегодня на практическом уровне, если Вы на самом деле работаете в органах федерального правительства, используются только две системы работы с грифованными документами - одна на уровне «секретно», и одна на уровне «совершенно секретно». Разведывательное сообщество практически отказалось от использования грифа «конфиденциально».

Учитывая конструкцию этих систем, больше нет необходимости в третьем уровне, который редко используется и не поддерживается соответствующей системой. Федеральное правительство также не выдает своим сотрудникам допуск на уровне «конфиденциально». Удаление этого уровня позволит правительству переосмыслить стандарты установления и снятия грифов, и привести их в соответствие с потребностями современной рабочей среды, требующей быстрого обмена информацией в электронном виде, а также нынешней многогранной средой угроз, которая больше не является монолитной.

У нас нет отдельной системы для работы с конфиденциальными документами, несмотря на то, что мы поддерживаем отдельный гриф «конфиденциально». Я уже отметила, что разведывательное сообщество США перестало использовать этот гриф; в то время, как по данным Офиса по контролю за информационной безопасностью (Information Security Oversight Office, ISOO) существует менее десятка лиц и органов, уполномоченных устанавливать первичные грифы секретности, полномочия которых ограничены только грифом «конфиденциально». Согласно ISOO, число таких лиц и органов продолжает из года в год уменьшаться. Тем не менее, правительство по-прежнему держится за этот унаследованный гриф.

С нашей точки зрения, Вы можете посмотреть на то, что считается конфиденциальной информацией, провести её экспертизу и либо рассекретить её, принять решение больше не устанавливать ей гриф секретности, рассматривать её как контролируемую несекретную информацию (Controlled Unclassified Information) - или установить ей гриф «секретно».

В идеале это должно произойти после того, как правительство пересмотрит критерии отнесения информации к «секретной» и «совершенно секретной», с тем, чтобы они были более точными и более сфокусированными на причинённом вреде (harm), вместо ныне используемого туманного термина «ущерб» (damage).

Подобное упрощение улучшит процесс управления грифами секретности в целом. Основной вопрос, который мы рассматриваем на протяжении всего нашего доклада, заключается в том, что вся система установления и снятия грифов секретности действительно нуждается в полном пересмотре.

Роль «Совета по рассекречиванию в интересах общественности» в проведении этой перестройки действительно очень важна. Мы можем многое сделать для того, чтобы побудить общественность, Конгресс и исполнительную ветвь власти обратить внимание на то, что должно происходить в органах федерального правительства, - потому что это область, несмотря на свою большую важность для нашей национальной безопасности и нашей демократии, не получает достаточного внимания.»

США: «СОВЕТ ПО РАССЕКРЕЧИВАНИЮ В ИНТЕРЕСАХ ОБЩЕСТВЕННОСТИ» ДАЛ ОТВЕТЫ НА РЯД ВОПРОСОВ ОБЩЕСТВЕННОСТИ

Источник: блог PIDB https://transforming-classification.blogs.archives.gov/2020/07/16/pidb-posts-transcript-of-virtual-public-meeting-responds-to-public-questions/

«Совет по рассекречиванию в интересах общественности» является консультативным органом, созданным Конгрессом США для способствования максимально возможной доступности для общественности полной, точной и надежной документации, отражающей существенные решения и действия США в сфере обеспечения национальной безопасности. В обязанности Совета входит консультирование Президента и других руководителей по политикам, вытекающим из издаваемых Президентом исполнительных приказов (executive orders), касающихся порядка установления грифов секретности и рассекречивания информации, содержащей государственную тайну.

Повестка дня и стенограмма виртуального публичного заседания «Совета по рассекречиванию в интересах общественности» (Public Interest Declassification Board, PIDB), состоявшегося 5 июня 2020 года, теперь доступны в Интернете на странице по адресу: https://www.archives.gov/declassification/pidb/meetings/pidb2020

Данная телеконференции стала началом важной дискуссии по докладу PIDB для Президента США за 2020 год «Видение для цифровой эпохи: Модернизация системы установления и снятия грифов секретности для сведений, содержащих государственную тайну» (A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System, см.

https://www.archives.gov/files/declassification/pidb/recommendations/pidb-vision-for-digital-age-may-2020.pdf).

Чтобы продолжить эту дискуссию и обсуждение иных вопросов, PIDB предлагает Вам либо написать свои комментарии в его блоге, либо отправить электронное письмо на адрес PIDB@nara.gov .

Во время виртуальной встречи члены совета PIDB ответили на несколько вопросов, заданных представителями общественности. Время, однако, не позволило дать ответы на все поступившие вопросы. Ниже приведены вопросы, на которые во время встречи ответы не были даны:

Выступая за введение двухуровневой системы грифов (отказываясь от грифа «конфиденциально» - confidential), чтобы обеспечить лучшее соответствие тому, как государственные системы работает на практике, предлагает ли «Совет по рассекречиванию в интересах общественности» также избавиться от классификаций SCI и/или SAP?

Секретная информация с особым режимом хранения (Sensitive compartmented information, SCI) - американская классификация информации, касающейся или полученной с использованием чувствительных разведисточников, методов и аналитических процессов. Формально не является грифом секретности, однако имеет свой порядок допуска, близкий к порядку допуска к сведениям уровня «совершенно секретно». См. Википедию, https://en.wikipedia.org/wiki/Sensitive_Compartmented_Information.

В органах правительства США под «программами доступа по особому разрешению» (Special Access Program, SAP) понимаются протоколы безопасности, обеспечивающие для информации высокой степени секретности уровень защиты, превышающий тот, что обеспечивается для «обычной» секретной информации. См. также Википедию, https://en.wikipedia.org/wiki/Special_access_program

Нет, Совет не предлагает отказаться от SCI и SAP при переходе на двухуровневую систему грифов. Секретная информация с особым режимом хранения (Sensitive Compartmented Information, (SCI)) и программы доступа по особому разрешению (Special Access Programs, SAPs) являются типами программ контролируемого доступа, а не уровнями системы грифов. Информация с любым грифом может существовать в системе с режимом управления SCI или содержать информацию, относимую к SAP.

Почему PIDB предпочитает выборочный тематический подход к рассекречиванию, в противовес к уважению происхождения документов и поддержке приоритизации проведения экспертизы и рассекречивания конкретных серий документов, представляющих «большой интерес»?

Совет считает необходимым сбалансировать рассекречивание серий документов, представляющих «большой интерес», с тематической приоритизацией, целью которой являются наиболее востребованные общественностью документы и информация. Совет также признает, что, хотя рассекречивание серий документов необходимо в отношение некоторых секретных текстовых документов, процессы рассекречивания требуют модернизации. Совет признаёт, что традиционные архивные принципы и

практики работы с текстовыми документами больше не работают в электронной среде, где стандарты метаданных, облачное хранение и вопросы управления доступом и безопасности имеют решающее значение. Процессы рассекречивания также необходимо модернизировать - уходя от основанной на работе с текстами аналоговой системы к системе, способной эффективно работать с большими объемами изначально-электронных секретных документов.

Рассматривается ли вопрос о том, чтобы исследователь мог подавать электронные запросы на проведение обязательной экспертизы на возможность рассекречивания (mandatory declassification review, MDR) непосредственно в Национальные Архивы США с использованием электронных носителей информации (флеш-накопителей и т.п.)?

Комиссия не видит причин возражать против того, чтобы исследователь мог подать MDR-запрос или апелляцию в электронном виде. Национальные Архивы и Межведомственная апелляционная комиссия по грифам секретности (Interagency Security Classification Appeals Panel, ISCAP) принимают MDR-запросы и апелляции в электронной форме по электронной почте. Однако вероятны проблемы с безопасностью в случае приема MDR-запросов с использованием USB-накопителей.

Сможет ли общественность получать информацию о том, какие документы проходят экспертизу на предмет рассекречивания, и её результаты? Будут ли изменения в том, каким образом общественность получает доступ к рассекреченным документам? Основными каналами доступа являются веб-сайты федеральных органов исполнительной власти и президентских библиотек, либо личное посещение президентских библиотек или отделения Национальных Архивов в Колледж-парке (College Park). Будут ли эти сайты значительно расширены? Что касается Колледж-парка, то огромные массивы секретных документов постоянного срока хранения возраста 25 лет и старше туда даже не поступили, хотя сроки их ведомственного хранения давно истекли. Например, в этом отделении Национальных Архивов хранится очень мало документов о деятельности ЦРУ, АНБ, Разведывательного управления Министерства обороны США (DIA), Объединённого комитета начальников штабов (Генштаба США) и ФБР - ограниченное их количество имеется в Вашингтонском национальном центре хранения документации (Washington National Records Center), однако подавляющее большинство таких документов по-прежнему хранится в самих федеральных органах. Кто будет проводить их экспертизу и как будет организован доступ общественности к рассекреченным документам?

Национальный центр по рассекречиванию (National Declassification Center, NDC) при Национальных Архивах США отвечает за координацию процессов рассекречивания документов. В настоящее время на его веб-сайте (https://www.archives.gov/declassification) выложены списки серии документов, рассекречивание которых является приоритетным. Национальный центр по

рассекречиванию также отвечает за проведение экспертизы секретных президентских документов и материалов с целью их рассекречивания.

Национальные Архивы отвечают за поддержание и обновление своего онлайн-каталога, включающего как сведения о доступных для исследований сериях документов, так и электронные образы отдельных документов. Национальные Архивы приветствуют публичные обсуждения на своих блогах, в том числе по вопросам, связанным с доступностью документов для общественности.

В отношении документов, юридическая ответственность за которые ещё не передана Национальным Архивам, их экспертизу на предмет рассекречивания должны проводить соответствующие федеральные органы исполнительной власти. В рамках новой системы, которую мы предлагаем в нашем отчете, Исполнительный комитет, возглавляемый директором национальных разведслужб США (Director of National Intelligence) и включающий представителей федеральных ведомств, разработает руководство по определению приоритетов рассекречивания, которые позволят улучшить доступность документов для общественности.

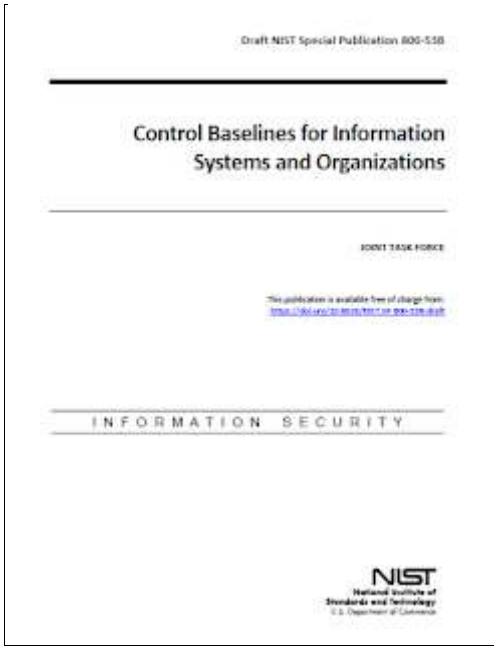
НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ США НАЧАЛ ПУБЛИЧНОЕ ОБСУЖДЕНИЕ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ SP 800-53B «БАЗОВЫЕ ПРОФИЛИ МЕР КОНТРОЛЯ И УПРАВЛЕНИЯ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ И ОРГАНИЗАЦИЙ»

Источник: сайт NIST https://csrc.nist.gov/publications/detail/sp/800-53b/draft https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B-draft.pdf

Американский Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST) 31 июля 2020 года выложил для публичного обсуждения проект новой специальной публикации **NIST SP 800-53B «Базовые профили мер контроля и управления для информационных систем и организаций»** (Control Baselines for Information Systems and Organizations) объёмом 85 страниц, см. https://csrc.nist.gov/publications/detail/sp/800-53b/draft ; прямая ссылка на PDF-файл: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B-draft.pdf .

NIST SP 800-53B предусматривает три базовых профиля для обеспечения безопасности (security control baseline) для федеральных систем с низким,

средним и высоким уровнем воздействия, а также базовый профиль для обеспечения неприкосновенности частной жизни для систем - вне зависимости от их уровня воздействия.



Базовые профили обеспечения безопасности и неприкосновенности частной жизни были дополнены мерами контроля и управления, описанными в специальной публикации NIST SP 800-53 «Меры обеспечения безопасности и неприкосновенности частной жизни для информационных систем и организаций» 5-й редакции. Содержание базовых профилей отражает результаты всестороннего межведомственного анализа, проведенного в 2017 году, а также постоянно поступающие материалы и результаты анализа данных об угрозах и реальных кибератаках, собранные после обновления публикации NIST SP 800-53.

В дополнение к базовым профилям, данная публикация содержит руководство по адаптации и набор рабочих предположений, которые помогут направлять и формировать проводимый организациями процесс отбора мер и средств контроля и управления.

Наконец, данная публикация содержит руководство по разработке расширений профилей (overlays), с тем, чтобы облегчить подстройку базовых профилей под потребности и особенности конкретных сообществ по интересам, технологий и условий деятельности. Базовые профили ранее входили в состав публикации NIST SP 800-53, но были выделены из неё в отдельный документ - с тем, чтобы публикация NIST SP 800-53 могла служить объединённым каталогом мер и средств контроля и управления, применяемых для обеспечения безопасности и неприкосновенности частной жизни, пригодным для использования различными сообществами по интересам.

Помимо Вашего мнения о трёх базовых профилях безопасности, NIST также хотел бы узнать Ваше мнение о базовом профиле для обеспечения неприкосновенности частной жизни и соответствующих критериях отбора.

Поскольку отбор элементов этого базового уровня основан на сопоставлении мер и средств контроля и управления и их расширений, описанных в NIST SP 800-53, с обязанностями, установленными программой обеспечения конфиденциальности в соответствии с циркуляром A-130 «Управление информацией как стратегическим ресурсом» (Circular No.A-130, Managing Information as a Strategic Resource, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf) Административно-бюджетного управления президентской администрации (Office of Management and Budget, OMB), - предлагаемые изменения в базовом профиле для обеспечения неприкосновенности частной жизни должны поддерживаться ссылкой на циркуляр OMB A-130. В качестве альтернативы, Вы можете предоставить описание и обоснование новых или модифицированных критериев отбора элементов для этого базового профиля.

Ваше мнение об этом проекте специальной публикации очень важно для нас. Мы ценим вклад каждого из наших рецензентов – представителей как государственного, так и частного секторов, национальных и зарубежных специалистов, помогающих нам формировать публикации NIST таким образом, чтобы они соответствовали потребностям и ожиданиям наших клиентов.

Содержание документа следующее:
Глава 1: Введение
Глава 2: Основные положения
Глава 3: Профили
Литература

Приложение A. Глоссарий
Приложение B. Сокращения
Приложение C. Расширения профилей (overlays)

США: «КОНФЕРЕНЦИЯ СЕДОНА» ОПУБЛИКОВАЛА ДЛЯ ПУБЛИЧНОГО ОБСУЖДЕНИЯ ПРОЕКТ 2-Й РЕДАКЦИИ «КОММЕНТАРИЯ ПО ДОКАЗАТЕЛЬСТВАМ В ВИДЕ СОХРАНЯЕМОЙ ЭЛЕКТРОННЫМ ОБРАЗОМ ИНФОРМАЦИИ И ИХ ДОПУСТИМОСТИ»

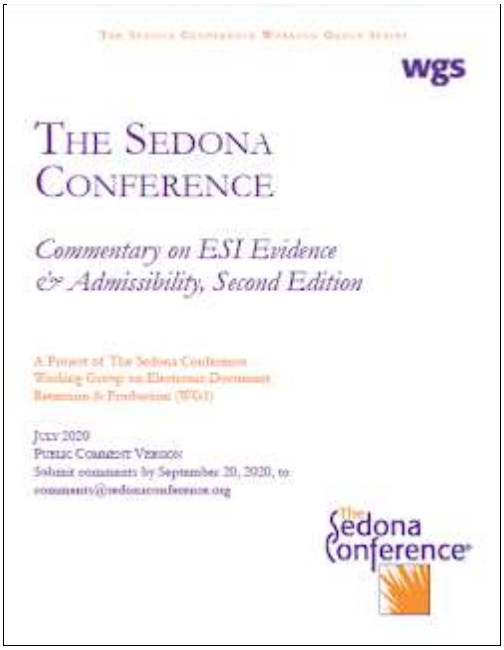
Источник: сайт Конференции Седона https://thesedonaconference.org/download-publication?fid=5334

https://thesedonaconference.org/publication/Commentary_on_ESI_Evidence_and_Admissibility

21 июля 2020 года сайт «Конференции Седона» и ее рабочая группа WG1 по хранению и представлению электронных документов (Electronic Document Retention and Production) сообщили о публикации версии для публичного обсуждения второй редакции документа **«Комментарий Конференции Седона по доказательствам в виде сохраняемой электронным образом информации и их допустимости»** (Sedona Conference Commentary on ESI Evidence and Admissibility).

Первое издание этого «Комментария» было опубликовано в 2008 году. Вторая редакция отражает существенные изменения, внесённые в 2017 и 2019 годах в Федеральные правила представления доказательств (Federal Rules of Evidence), а также то, как эти изменения и остальные правила применяются в условиях постоянно меняющегося технологического ландшафта.

Главный редактор документа Кевин Брэйди (Kevin Brady), советник по правовым вопросам Пол Гримм (Paul W. Grimm – судья федерального окружного суда США, округ Мэриленд) и члены редакционной группы 26 августа 2020 года примут участие в вебинаре, посвящённом обсуждению изменений в «Комментарии», с целью помочь специалистам-практикам лучше понять, как эти изменения повлияют на их деятельность. Следите за своей электронной почтой, чтобы получить дополнительную информацию о нём, когда та станет доступна.



Кроме того, редакционная группа и руководящий комитет рабочей группы WG1 заинтересованы в получении Ваших замечаний и предложений до

того, как к концу этого года будет подготовлена окончательная версия «Комментария». Предложения по улучшению документа предлагается направлять по электронной почте на адрес comments@sedonaconference.org .

Документ объёмом 89 страниц можно бесплатно скачать по адресу https://thesedonaconference.org/download-publication?fid=5334 .

Содержание документа следующее:

I. Введение

II. Применение существующих правил и прецедентного права к электронным доказательствам

A. Раннее повышенное внимание к вопросам аутентификации и представления доказательств

B. Ходатайства о разрешении спора в упрощённом порядке и электронные доказательства

C. Средства аутентификации: правила 104, 901 и 902

D. Различные типы электронной информации требуют разных подходов

E. Твердые копии

F. Потенциальные проблемы применения правила 902 (14)

G. Недавние изменения в правиле 807 (остаточное исключение из правила слухов)

III. Появляющиеся проблемы использования электронной информации в качестве доказательств

A. Установление владельца / создателя электронной информации

B. Понимание пределов возможностей технологий

C. Применение федеральных правил и прецедентов в судах штатов и наоборот

IV. Практическое руководство по использованию электронных доказательств в суде

A. Использование электронной информации в статическом формате, в сравнении с её использованием в первоначальном/применяемом в реальных системах формате

B. Доказательства, помогающее жюри в разрешении вопроса о санкциях за порчу доказательств

C. Практические советы по представлению электронной информации в качестве доказательств

D. Практические советы по поиску оснований для приёма электронной информации в качестве доказательств.

V. Использование искусственного интеллекта в деловой деятельности и в области права

Приложения.

В «Комментарии» о технологии блокчейна и распределенных реестров (п. III B(5)). В принципе записи в блокчейне могут быть использованы в качестве доказательств, но при определённых условиях. Отдельно

подчёркивается, что технология блокчейна сама по себе не гарантирует верности записанных в блокчейне сведений.

США: КОНФЕРЕНЦИЯ СЕДОНА ОПУБЛИКОВАЛА ПРОЕКТ КОММЕНТАРИЯ ПО ПОВОДУ ИСПОЛНИМОСТИ В США РЕШЕНИЙ, ПРИНЯТЫХ НА ОСНОВАНИИ ЕВРОПЕЙСКОГО ЗАКОНА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ GDPR

Источник: сайт Конференции Седона https://thesedonaconference.org/node/9656

30 июня 2020 года сайт «Конференции Седона» (Sedona Conference®) – очень авторитетного американского некоммерческого правового идейного центра, в основном занимающегося вопросами раскрытия в ходе судебных разбирательств и расследований сохраняемой в электронном виде информации (э-раскрытия), – выложил для публичного обсуждения проект **«Комментария Конференции Седона о возможности приведения в исполнение в США судебных приказов и решений, принятых на основе закона GDPR»** (Sedona Conference Commentary on the Enforceability in U.S. Court of Orders and Judgments Entered Under GDPR) объёмом 41 страница, см. https://thesedonaconference.org/... . Документ подготовлен рабочей группой WG11 по защите данных и ответственности за нарушение неприкосновенности частной жизни (Data Security and Privacy Liability).


The Sedona Conference Commentary
on the Enforceability in U.S. Courts
of Orders and Judgments Entered under GDPR

JULY 2020 PUBLIC COMMENT VERSION

wgs

Речь идёт о том, как быть со столь неудобными для многих американских компаний «Общими правилами защиты персональных данных» Евросоюза (General Data Protection Regulation, GDPR, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504).

Вместе с полным документом также выложено краткое одностраничное извещение, см. https://thesedonaconference.org/sites/default/files/Handout%20-%20Enforcement%20of%20GDPR%20in%20US%20Public%20Comment%20Version.pdf

Во вводной части документа, в частности, отмечается следующее:

«Рабочая группа WG11 разработала настоящий Комментарий для оценки возможности приведения в исполнение через суды США приказов или решений, принятых на основании «Общих правил защиты персональных данных» Евросоюза (GDPR) европейским судом или контролирующим органом государства-члена Евросоюза, против оператора или обработчика персональных данных, зарегистрированного в США. Цель Комментария заключается в том, чтобы дать заинтересованным сторонам в ЕС и США рекомендации по факторам - как юридическим, так и практическим - которые связаны с обеспечением исполнения требований GDPR через судебные разбирательства в США.

Вопрос о том, как и при каких обстоятельствах может быть обеспечено исполнение требований GDPR в рамках судебного разбирательства в США, возникает в результате широкого территориального охвата закона GDPR. В этом плане закон GDPR представляет собой «существенную эволюцию» территориального охвата европейского законодательства о защите персональных данных по сравнению с его предшественником, и отражает намерение «обеспечить всестороннюю защиту прав субъектов данных в Евросоюзе и создать равное игровое поле для компаний, действующих на рынках Евросоюза, в контексте глобальных потоков данных».

Из-за этой эволюции в плане территориального охвата, базирующиеся за пределами Евросоюза, в том числе в США, организации, которые ранее не подпадали под правила защиты персональных данных Евросоюза или не сталкивались с последствиями их нарушения, теперь могут столкнуться и с тем, и с другим. Но, как объясняется в недавнем отчете «Сети «Интернет и юрисдикционная политика»» (Internet and Jurisdiction Policy Network, https://www.internetjurisdiction.net/), «способность государства обеспечивать соблюдение своих законов часто более ограничена, чем заявления, которые оно делает в отношении сферы действия своих законов». Таким образом, неизбежно возникают вопросы о том, как контролирующие органы и субъекты персональных данных могут добиться исполнения требований GDPR в отношении этих неевропейских организаций.

В некоторых случаях ответ будет простым. Когда у организации есть филиал, дочернее предприятие или иные активы в Евросоюзе, европейские контролирующие органы и субъекты персональных данных могут добиться применения требований GDPR против организации в границах Евросоюза.

Если организация нарушает GDPR, но физически не присутствует и не располагает иными активами в Евросоюзе. В этом случае контролирующие органы и субъекты персональных данных Евросоюза могут издать приказ или получить судебное решение против организации. Если, однако, эта организация не желает добровольно выполнить такой приказ или решение, контролирующему органу или субъекту персональных данных может потребоваться зарубежная помощь для обеспечения его исполнения.

Когда нарушителем является организация, базирующаяся в США, одним из потенциальных источников помощи является судебная система США. В США существует устоявшееся законодательство по вопросу признания и приведении в исполнение судами США иностранных судебных решений в иных контекстах».

Содержание документа следующее:

Введение

I. Обзор экстерриториального охвата закона GDPR

II. Признание и приведение в исполнение иностранных судебных решений в судах США: Обзор действующего законодательства

III. Признание и приведение в исполнение приказов и судебных решений на основе GDPR в судах США: Частные действия субъектов персональных данных и организаций-представителей

IV. Признание и приведение в исполнение приказов и судебных решений на основе GDPR в судах США: Приказы об устранении нарушений, принятые контрольными органами Евросоюза

V. Потенциальная защита в соответствии с законодательством США от исков, требующих признания и приведение в исполнение приказа или судебного решения на основе GDPR

VI. Альтернативные пути обеспечения исполнения GDPR в судах США: Федеральная комиссия США по торговле (Federal Trade Commission, FTC), соглашение о взаимной защите персональных данных между США и Евросоюзом (Privacy Shield) и претензии по контрактам

VII. Заключение

ОТКРЫТЫЕ ДАННЫЕ: ПРЕОДОЛЕНИЕ НЕРАВЕНСТВА В ДОСТУПЕ К ДАННЫМ

Источник: блог компании Formtek http://formtek.com/blog/open-data-bridging-the-data-inequality-gap/

Ведущие технологические компании укрепляют своё доминирование благодаря доступу к большим объемам данных.

Президент Microsoft Брэд Смит (Brad Smith, https://en.wikipedia.org/wiki/Brad_Smith_(American_lawyer)) отметил, что половина всех создаваемых в Интернете данных собирается менее чем 100 технологическими компаниями, расположенными либо на западном побережье США, либо восточном побережье Китая (см. https://www.geekwire.com/2020/microsoft-seeks-narrow-data-divide-information-consolidated-among-companies-countries/).

Microsoft называет это неравенство между крупными технологическими компаниями и всеми остальными в плане доступа к большим объёмам данных «цифровым неравенством» (digital divide). Идея о том, что этот разрыв можно ликвидировать, послужила толчком для недавнего запуска компанией Microsoft «Кампании за открытые данные» (Open Data Campaign, https://news.microsoft.com/opendata/). Коммерческие организации любого размера должны иметь доступ и возможность получить отдачу от больших наборов данных.

Главный советник Microsoft по вопросам интеллектуальной собственности Дженнифер Йокояма (Jennifer Yokoyama, https://www.iam-media.com/copyright/new-microsoft-ip-head) пишет, что «сокращение разрыва в доступе к данным является большой проблемой. Однако польза от этого для организаций всех размеров и для общества в целом будут значительными, если мы сможем работать вместе для того, чтобы добиться прогресса в открытых данных. Мы стремимся внести свой вклад, и мы с нетерпением ждем возможности поработать с другими и поучиться у них, чтобы каждый мог понять пользу от данных» (см. https://blogs.microsoft.com/on-the-issues/2020/04/21/open-data-campaign-divide/).

Йокояма пишет, что «Начиная от изменения климата и до пандемии COVID-19, – ясно, что данные играют критически-важную роль, помогая нам понять эти проблемы и справиться с ними. Чтобы полностью реализовать потенциал данных, нам необходимо развивать возможности для коллективного использования данных через границы организаций безопасным и надежным образом, позволяющим эффективно их использовать. Если когда-либо было подходящее время для ускорения всемирных усилий в области открытых данных, то это сейчас».

Сам по себе доступ к большим наборам данных ничего не значит. Доступ необходим к сравнительно узкому подмножеству данных, полезных для конкретного вида деятельности, – и также необходимы инструменты и специалисты для обработки этих данных, которые во многих случаях являются более труднодоступным ресурсом.

ePADD: АРХИВИРОВАНИЕ ЭЛЕКТРОННЫХ ПИСЕМ С ПОМОЩЬЮ ИНСТРУМЕНТА С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Источник: блог MCA https://blog-ica.org/2020/06/13/epadd-archiving-emails-with-an-open-source-tool/

Около десяти лет тому назад архивисты Стэнфордского университета (Stanford University) выделили электронную почту как один из наиболее важных форматов, долговременную сохранность и доступность которых для исследователей необходимо обеспечить. Мы изучили положение дел в этой области и обнаружили, что во всех предыдущих проектах основное внимание уделялось обеспечению сохранности, а не поиску, раскрытию или доступу. Очень удачным оказалось то, в 2011 году мы встретились с Судхендрой Хангалом (Sudheendra Hangal), в то время аспирантом факультета компьютерных наук Стэнфордского университета, который создал программу под названием MUSE (https://mobisocial.stanford.edu/muse/) в качестве инструмента просмотра личного архива электронной почты. Программа предлагала функциональные возможности, которых не было где-либо ещё, и она давала нам возможность анализировать изображения и текст на предмет наличия в них чувствительного контента. Открытие доступа исследователям к материалам из архивов электронной почты могло осуществляться через отдельную систему в нашем читальном зале.

Идея дальнейшей разработки этого программного обеспечения с целью создания более надежного инструмента с открытым исходным кодом захватила нас всех. Вместе с Судхендрой мы подготовили нашу первую заявку на грант Национальной комиссии по историческим публикациям и документам (National Historical Publications and Records Commission, NHPRC – через эту комиссию финансируются публикации исторических документов, выдаются гранты на обеспечение сохранности, доступа и на оцифровку архивов и т.д.), см. https://library.stanford.edu/projects/epadd/development/nhprc-phase-1). Спустя два года, в 2015 году, мы выпустили базовый прототип решения ePADD (от «Email: Process Appraise Discover Deliver» – «Электронная почта: Обработка, экспертиза ценности, поиск, предоставление доступа»). Наши главные цели заключались в том, чтобы получить возможность выявлять персональные данные и чувствительные материалы, а также обеспечить большую гибкость в плане стратегий поиска. Ещё одной важной задачей было создание сайта для поиска материалов, где мы исходили из предпосылки о том, что для того, чтобы исследователи могли найти нужный им контент, нам необходимо опубликовать метаданные.

После этого мы получили грант от Института музейно–библиотечных услуг (Institute of Museum and Library Services, IMLS, https://www.imls.gov/ – независимый орган правительства США, оказывающий поддержку музеям и

библиотекам всех видов) на 2015-2018 годы (см. https://library.stanford.edu/projects/epadd/about/imls-phase-2) – для продолжения разработок и для расширения сообщества пользователей. Что касается модуля онлайн-поиска, то нам нужно было заверить доноров, а также директоров наших библиотек, что будут опубликованы только описательные метаданные. Это требование соблюдается в нашей текущей версии (7.2), которая доступна через сайт GitHub.

В этом году мы получили грант Фонда Эндрю Меллона (Andrew W. Mellon Foundation, https://library.stanford.edu/projects/epadd/about/andrew-w-mellon-foundation-phase-3) и снова договорились о сотрудничестве с библиотекой Гарвардского университета о дальнейшем развитии решения. Наша главная цель – переработать функцию анализа присоединённых файлов, поскольку она основана на технологии Adobe Flash, которая перестанет поддерживаться в декабре 2020 года. Нарождающееся решение заключается в создании панели для просмотра и анализа всех вложений, использующей Apache Tika для визуализации простого текста для многих распространенных текстовых типов файлов.

Также ставится задача во взаимодействии с нашими партнерами разработать функциональные требования для включения в ePADD действий по обеспечению долговременной сохранности, которые сделают возможным экспорт в долговременные хранилища. Мы пришли к этой стратегии после нескольких месяцев встреч, направленных на обеспечение интероперабельности между ePADD и решением EAS Гарвардского университета (https://wiki.harvard.edu/confluence/display/LibraryStaffDoc/2.+Overview+of+EASi). В эти усилия теперь также вовлечены сотрудники университета Манчестера (https://rylandscollections.com/2020/02/05/introducing-epadd-for-email-archives-at-the-university-of-manchester/), которые самостоятельно работали с ePADD в прошлом году. Наше сотрудничество с этими двумя учреждениями было великолепно плодотворным и конструктивным, в результате были разработаны планы будущей работы по обеспечению долговременной сохранности электронной почты и расширению поддержки в ePADD дополнительных языков.

В этом году работать в проекте развития ePADD было весьма интересно. Вместо личных встреч с нашими партнерами и разработчиками, которые продолжались в течение нескольких дней, мы сейчас полагаемся на более частые виртуальные встречи – развернуть полностью виртуальный проект оказалось гораздо проще, чем предполагалось.

ИСО: СРЕДИ ПОЛЬЗОВАТЕЛЕЙ СТАНДАРТОВ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА ПРОВОДИТСЯ ОНЛАЙН-ОПРОС, РЕЗУЛЬТАТЫ КОТОРОГО БУДУТ УЧТЕНЫ В ПРОЦЕССЕ ПЕРЕСМОТРА СТАНДАРТА ISO 9001

Источник: веб-сайт ИСО / сайт Surveymonkey https://www.surveymonkey.com/r/ISO9001_User_Survey_2020?lang=ru

29 июля 2020 года профильный технический подкомитет ИСО ТС176/SC2 «Менеджмент качества и обеспечение уверенности в качестве – Системы менеджмента качества» (Quality Management and Quality Assurance/Quality Systems) распространил документ следующего содержания, попросив распространять эту информацию дальше:

Опрос 2020 года пользователей стандарта ISO 9001

В настоящее время стандарт ISO 9001:2015 «Системы менеджмента качества – Требования» (Quality management systems – Requirements) проходит процесс официального «систематического пересмотра», который должен завершиться 2 декабря. После этого у технического подкомитета ТС176/SC2 будет до 6 месяцев для принятия решения о том, должен ли стандарт быть подтвержден (то есть оставлен без изменений), пересмотрен или скорректирован, либо отменён.

Подкомитет, принимая такое решение, хотел бы знать мнение пользователей стандарта ISO 9001:2015 о том, является ли стандарт адекватным или его следует улучшить.

Помимо того, технический комитет ТС176 рассматривает «будущие концепции» менеджмента качества. Подкомитет SC2 хотел бы проверить приемлемость таких концепций для пользователей, имея в виду их возможное включение в будущую редакцию ISO 9001.

Онлайн-опрос для получения обратной связи от пользователей создан на Surveymonkey. Опрос доступен на 13 различных языках, плюс дополнительная версия на персидском языке (фарси) на сайте Google Forms. (Для просмотра доступных языков см. раскрывающийся список в верхнем правом углу опроса).

Принять участие в опросе можно по ссылке https://www.surveymonkey.com/r/ISO9001_User_Survey_2020 ; персидская версия доступна по адресу https://forms.gle/KrnB8GmyowP5aeKr5 .

США: НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ НАЧАЛ ПУБЛИЧНОЕ ОБСУЖДЕНИЕ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ NIST SP 800-209 «РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ДЛЯ ИНФРАСТРУКТУРЫ ХРАНЕНИЯ»

Источник: сайт NIST

https://www.nist.gov/itl/information-technology-laboratory-itl-patent-policy-inclusion-patents-itl-publications

https://csrc.nist.gov/publications/detail/sp/800-209/draft

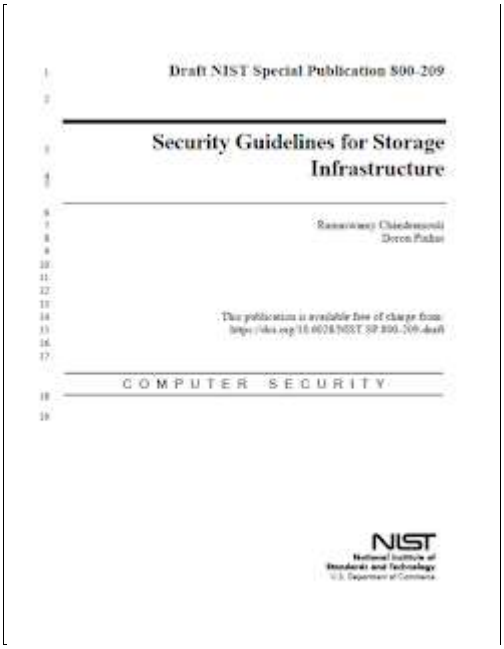
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209-draft.pdf

Американский Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST) 21 июля 2020 года выложил для публичного обсуждения проект новой **специальной публикации NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения»** (Security Guidelines for Storage Infrastructure).

Инфраструктура хранения, наряду с вычислительной инфраструктурой (включающей операционную систему и аппаратное обеспечение хоста) и сетевой инфраструктурой, является одним из трех основных столпов информационных технологий (ИТ). Тем не менее, когда речь идет о безопасности, ей, по сравнению с вычислительной и сетевой инфраструктурами, уделяется сравнительно ограниченное внимание, - даже несмотря на то, что компрометация данных может оказать на организацию негативное воздействие такого же масштаба, как и нарушения безопасности в вычислительной и сетевой инфраструктурах.

Чтобы устранить этот пробел, Национальный институт стандартов и технологий (NIST) подготовил проект специальной публикации NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения» объёмом 65 страниц, см. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209-draft.pdf , который включает в себя всесторонние рекомендации по безопасности для инфраструктур хранения.

Рассматриваемые в этом документе направления деятельности в сфере безопасности охватывают не только те области, которые являются общими для всей ИТ-инфраструктуры, такие, как физическая безопасность, аутентификация и авторизация, управление изменениями, контроль конфигурации, реагирование на инциденты и восстановление после них; но также и те, которые являются специфическими для инфраструктуры хранения – это, например, защита данных, изоляция, обеспечение уверенности в возможности восстановления, а также шифрование данных.



В аннотации на документ сказано следующее:

«Технология хранения, как и вычислительные и сетевые технологии, ушла в своей эволюции от традиционных форм оказания услуг хранения, таких, как блок, файл и объект. В частности, эволюция прошла в двух направлениях:

- по пути увеличения ёмкости запоминающих устройств (таких, как, лента, жесткий диск, твердотельный SSD-диск);

- по архитектурному фронту, начиная от непосредственно подключаемых систем хранения (direct attached storage, DAS), через размещение ресурсов хранения в выделенных сетях, доступных через различные интерфейсы и протоколы, и до ресурсов хранения с облачным доступом, что обеспечивает абстрагирование от базовых технологий хранения посредством программного обеспечения.

Эволюция сопровождается увеличением сложности управления, что, как следствие, увеличивает вероятность ошибок конфигурации и взаимосвязанных угроз безопасности.

В настоящем документе дается обзор эволюции ландшафта технологий хранения, текущих угроз безопасности и связанных с ними рисков. Основное внимание в этом документе уделяется предоставлению всестороннего набора рекомендаций по безопасности, направленных на устранение угроз. Рекомендации охватывают не только те области менеджмента безопасности, которые являются общими для инфраструктуры информационных технологий (это, например, физическая безопасность, аутентификация и авторизация, управление изменениями, контроль конфигурации, а также реагирование на инциденты и восстановление после них), - но также и на те, которые являются специфическими для инфраструктуры хранения (например, защита данных, изоляция, обеспечение уверенности в возможности восстановления, а также шифрование данных)».

Содержание документа следующее:
Резюме для руководства
1. Введение
2. Технологии хранения данных: Предыстория
3. Угрозы, риски и виды атак
4. Рекомендации по безопасности при развёртывании систем хранения
5. Итоги и выводы

СТАНДАРТ ISO/IEC 29134:2017 «РУКОВОДСТВО ПО ОЦЕНКЕ ВОЗДЕЙСТВИЯ НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ»

Источник: сайт ИСО https://www.iso.org/standard/62289.html
https://www.iso.org/obp/ui/#!iso:std:62289:en

Стандарт **ISO/IEC 29134:2017 «Информационные технологии – Методы и средства обеспечения безопасности – Руководство по оценке воздействия на неприкосновенность частной жизни»** (Information technology - Security techniques - Guidelines for privacy impact assessment) объёмом 52 страницы.

Стандарт описывает принципы проведения «оценки воздействия на неприкосновенность частной жизни» (персональные данные), с тем, чтобы уменьшить разнобой в подходах и повысить качество такой оценки. Оценка воздействия является главным новшеством статьи 35 «Общих правил защиты персональных данных» Евросоюза (General Data Protection Regulation, GDPR, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504). Ответственный за обработку оператор – в данном случае, пользователь облачных услуг – обязан провести анализ воздействия предполагаемых в ходе обработки операций на защиту персональных данных, если такая обработка способна создать повышенные риски для прав и свобод физических лиц.

Как отмечается в этом документе, оценка воздействия на неприкосновенность частной жизни (privacy impact assessment, PIA) является инструментом для оценки потенциального воздействия на неприкосновенность частной жизни процесса, информационной системы, программного обеспечения, программного модуля, устройства или иных инициатив, которые обрабатывают персональные данные (personally identifiable information, PII). Она также служит для того, чтобы, консультируясь с заинтересованными сторонами, принять необходимые меры для обработки риска для неприкосновенности частной жизни.

Оценка воздействия является неотъемлемой частью процесса обработки риска неприкосновенности частной жизни / ПДн. Отчет о такой оценке может включать документацию о мерах, принятых для обработки риска - например, о мерах, связанные с использованием системы менеджмента информационной безопасности (СМИБ) на основе стандарта ISO/IEC 27001.

Оценка воздействия – это нечто большее, чем просто инструмент: это процесс, который начинается на возможно более ранних стадиях проекта/инициативы, когда ещё есть возможности повлиять на его результаты и тем самым обеспечить запроектированную защиту персональных данных (privacy by design). Этот процесс продолжается в течение всего процесса внедрения проекта и даже после его окончания.

Настоящий стандарт предназначен для использования в тех случаях, когда при оценке воздействия на неприкосновенность частной жизни субъектов персональных данных следует принять во внимание процессы, информационные системы и/или программ, где:

- Ответственность за реализацию и/или поставку процесса, информационной системы или программы разделяется с другими организациями, и необходимо обеспечить, чтобы каждая организация надлежащим образом реагировала на выявленные риски;
- Организация осуществляет управление рисками для неприкосновенности частной жизни в рамках своих общих усилий по управлению рисками, в процессе подготовки к внедрению или совершенствованию системы менеджмента информационной безопасности на основе стандарта ISO|IEC 27001 или эквивалентной системы менеджмента; - либо в организации управлением такими рисками занимается отдельная служба;
- Организация (например, правительство) осуществляет инициативу (например, программу государственно-частного партнерства), и неизвестно, какая организация станет оператором ПДн, вследствие чего будут сложности с

непосредственным исполнением плана обработки риска. В таком случае план обработки риска должен взамен стать предметом законодательно-нормативного регулирования или частью договора;

- Организация хочет действовать ответственно в отношении субъектов ПДн.

Настоящий международный стандарт содержит рекомендации по:

- Процессу проведения оценки воздействия на неприкосновенность частной жизни;
- Структуре и содержанию отчета об оценке.

Стандарт применим в организациях любого типа и размера, в том числе в государственных и частных компаниях, в государственных органах и в организациях.

Настоящий стандарт представляет интерес для тех, кто участвует в разработке и реализации проектов, в том числе для сторон, являющихся операторами систем обработки данных и услуг, имеющих дело с ПДн.

Структура документа следующая:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Аббревиатуры
5. Подготовка к проведению оценки воздействия на неприкосновенность частной жизни
6. Руководство по процессу проведения оценки воздействия
7. Отчет о результатах оценки воздействия
8. Приложения
9. Библиография

ЗМІСТ