ПЕРЕДМОВА

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

У публікації «Международное сотрудничество в области обеспечения информационной безопасности» розглядається стан інформаційної безпеки на сучасному етапі розвитку відносин між державами. Визначені направлення співробітництва з питань інформаційної безпеки.

У публікації «Использование технологии blockchain при обработке информации» представлено аналіз використання технології блокчейн. Розглянуто ефективність цієї технології під час обробки інформації.

У публікації «Организация электронного документооборота в органах государственного управления» наведено аналіз електронного документообігу в органах державного управління Російської федерації.

У публікації «Профессор Шерри Сье об электронных документах и электронных цифровых подписях» наведено дискусію фахівців щодо використання електронного цифрового підпису під час архівного зберігання.

У публікації «ИСО и МЭК работают над стандартами доверия к интернету вещей» розповідається про методологію забезпечення та підтримки довіри до IoT-систем та послуг.

У публікації «Технология блокчейна является технологией управления документами!» наведено стислий огляд технологій блокчейна (Blockchain) та розподілених реєстрів (Distributed Ledger Technologies, DLT), який адресовано фахівцям з управління документами та інформацією.

У публікації «США: «Конференция Седона» опубликовала документ об обеспечении безопасности данных и защите персональных данных в случае слияния или поглощения организаций» наведено коментарі конференції з питань забезпечення безпеки даних та захисту особистих даних.

У публікації «ИСО: Подготовлен новый стандарт ISO 22396 «Жизнестойкость сообществ – Руководство по информационному обмену между организациями»» розповідається про голосування з цього стандарту.

У публікації «ИСО: Какие национальные стандарты технический подкомитет ТС46/SC11 «Управление документами» мог бы взять за основу будущих проектов?» наведено пропозиції Південної Кореї та Італії.

У публікації «Сертификат и ключи усиленной электронной подписи можно получить без ведома владельца» розповідається як прогалини у законодавстві призводять до незаконного використання ЕЦП аферистами.

У публікації «ИСО: Завершается работа над стандартом ISO 31022, посвящённом менеджменту правовых рисков» розповідається про публічне обговорення проекту стандарту ISO/DIS 31022.

У публікації «ИСО: Пересмотр ряда стандартов ИСО по вопросам управления контентом» розповідається про початок перегляду стандартів.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник: http://xn--80aa3afkgvdfe5he.xn--p1ai/%D0%A0%D0%9D%D0%A1%D0%9C-12_originalmaket_N.pdf
Авторы: Нечаева Т. А., Костюков А. А.

В статье рассматривается вопрос об информационной безопасности на современном этапе развития отношений между государствами. Представлены направления сотрудничества в области информационной безопасности.

Международное сотрудничество в области обеспечения информационной безопасности - неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества [1].

Стремительное развитие и широкое использование (ИКТ) привело к формированию фундаментальной зависимости важных национальных инфраструктур от этих технологий и обусловило возникновение принципиально новых угроз. Эти угрозы связаны, прежде всего, с возможностью использования ИКТ в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека. Особую озабоченность вызывает возможность разработки, применения и распространения информационного оружия и возникающая в этой связи угроза информационных войн и информационного терроризма [2].

Усиление технологического отрыва ведущих держав мира и наращивание их возможностей для создания «информационного оружия» может привести к новому этапу развертывания гонки вооружений в информационной сфере [1].

В октябре 2012 года была издана секретная директива Президента США, согласно которой наступательные операции в информационном пространстве предоставляют исключительные возможности для США продвигать свои национальные интересы в глобальных масштабах.

Американским военным и разведывательным службам, как это отмечали западные СМИ, было поручено подготовить план с указанием списка целей, против которых будет применяться кибер-оружие. Операции должны осуществляться без предупреждения противника. Предусматривается нейтрализация инфраструктуры неприятеля, в частности вывод из строя, ослабление или уничтожение компьютерных систем [3].

Впервые киберугрозы заняли первое место в этом списке, опередив терроризм. Причем одним и главных вызовов названа возможность хакерской атаки со стороны отдельного государства или негосударственных субъектов на критическую информационную инфраструктуру США. Россия и Китай упоминались в докладе опосредованно, как одни из ведущих государств в информационном пространстве. Отмечалось, что возможность совершения атаки с их стороны на информационные системы США ничтожно мала [1].

В связи с тем, что международная информационная безопасность важна для всего международного сообщества, особое внимание должно придаватться развитию сотрудничества в глобальном масштабе для противодействия им, а также обсуждению данных вопросов на ключевых международных и региональных площадках. Россия стала первым государством, которое внесло предложение о включении проблемы обеспечения международной информационной безопасности в повестку дня ООН [3].

Основными направлениями международного сотрудничества в области обеспечения информационной безопасности являются:

• запрещение разработки, распространения и применения «информационного оружия»;

• обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

• координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

• предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также с торговлей людьми.

Для осуществления международного сотрудничества по указанным основным направлениям необходимо обеспечить активное участие всех международных организаций, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации [1].

Список цитируемой литературы:

1. http://scibook.net/jiznedeyatelnosti-bjd-bezopasnost/mejdunarodnoe-sotrudnichestvo-rossii-oblasti-3570.html

2. http://www.mid.ru/obsie-voprosy-mezdunarodnoj-bezopasnosti-i-kontrola-nad- vooruzeniami/-/asset_publisher/6sN03cZTYZOC/content/id/486848

3. https://interaffairs.ru/jauthor/material/1351

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BLOCKCHAIN ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ

Источник: http://xn--80aa3afkgvdfe5he.xn--p1ai/%D0%A0%D0%9D%D0%A1%D0%9C-12_originalmaket_N.pdf

В статье представлено подробное описание и анализ применения технологии блокчейн. Рассматривается эффективность использования данной технологии при обработке информации.

Ключевые слова: технология блокчейн, биткоин, шифрование, безопасность информации

Деятельность современного человека напрямую связана с данными, документами и деньгами. Таким образом, он каждый раз вынужден полагаться на то, что ему сообщат подлинную информацию. Например, банк предоставит верные данные о личном счете, или почтовый провайдер, что сообщение доставлено адресату, антивирус, что файлы и данные пользователя в безопасности. Люди должны взаимодействовать с многочисленными посредниками, выдающими документы, финансы и информацию, проверяющими их, заверяющими их достоверность.

Данная технология делает возможным взаимодействие людей между собой без необходимости взаимного доверия и привлечения посредника. В блокчейн истории всех сделок транслируются на все полные узлы сети. Таким образом, управление данными заняло бы огромное количество ресурсов, что практически невозможно.

Согласно определению английского слова «blockchain» состоящего из 2 частей: block (блок) и chain (цепь). Другими словами, это практически новая технология, которая способна сделать любую передачу данных, в частности конфиденциальную информацию, к примеру, банковские операции, как алгоритм действий «один за одним».

Соответственно, отдельный блок данной последовательности содержит цифровую информацию обо всем множестве других блоков. Все участники данного алгоритма, осуществляющие передачу данных в подобной системе, имеют разрешение доступа к данным из участков всей цепи. Каждая последующая операция добавляется в структуру подобно новому блоку, который содержит сведения обо всех предыдущих действиях в цепочке. Таким образом, в уже имеющихся блоках создается информация о новых. [3]

После добавления новых отдельных блоков одним из участников системы, вся база данных самостоятельно изменяется до актуальной версии у всех остальных участников. Исходя их этого несанкционированные и мошеннические действия с изменением данных становятся невозможными. Следовательно, любую ранее зафиксированную информацию уже никогда невозможно будет изменить или стереть. Наглядным примером является технология блокчейн биткоина, он содержит абсолютно корректные и достоверные данные обо всех совершенных операциях с криптовалютой

биткоин. Таким образом, именно криптовалюта запустила развитие технологии блокчейн. Данная технология является сложным процессом, состоящим и з алгоритма, базирующемся на трех существенных принципах: распределенность, открытость, защищенность.

Исходя из вышеизложенного, для технологии блокчейн необходима распределенная экосистема, обеспечивающая всестороннюю операционную помощь в ресурсах. Данная технология является децентрализованным журналом записей операций, являющимся одним из наиболее распространенной вычислительной инфраструктуры. В свою очередь, ей необходимо содержать огромное количество других ресурсов, таких как: хранение, коммуникацию, обработку данных и архивацию. Конкретным проектом разработанного решения для данной экосистемы технологии блокчейн можно выделить Storj (хранение всего многообразия типов информации – текста, иллюстраций, аудиозаписей, мультимедиа-файлов); IPFS (обработка данных, хранение и обслуживание ссылок); помимо этого, можно отметить Maidsafe и Ethereum (резервирование, коммуникация и обработка данных) [1].

Для представленной технологии в первую очередь нужно надежное и независимое хранилище за пределами блокчейна, применяемое для консолидации больших данных, наподобие электронных медицинских карт (EMR), геномов или документов с расширением docx (MS Office), которые невозможно поместить в ячейку объемом 40 байт (40 символов) OP_RETURN, используемую для пометки биткойн-операций [2].

Неотъемлемой частью данной технологии является обработка данных. Изобретатели системы IPFS придумали необычный подход к децентрализованной и безопасной обработке данных. Технология соединяет систему одноранговой отправки файлов BitTorrent с функцией распределенного метода управлением выпусками Git, применяемой в глобальной связи к разным цифровым средствам. Иначе говоря, IPFS является глобальной версионированной одноранговой файловой системой, четко сравнивающей уникальность файлов, расположенных в любом месте интернет-пространства (взамен применения централизованного репозитория), имеющей уникальный цифровой код (хеш), подтверждающий цельность данных и исключение вредоносных программ и нежелательной рекламы (спама).

По общему мнению большинства ученых, бизнес-аналитиков и риск-менеджеров, технология блокчейн станет всеобщим средством хранения всех данных человечества, поэтому нужно организовать возможность строгой сохранности, архивирования, регулирования срока службы и предоставления доступности. Реализация данных механизмов, способных архивировать незадействованные распределенные реестры данных и обеспечивать весь их жизненный цикл, даст возможность большому расширению технологии блокчейн.

Для обеспечения безопасности информации и данных людей в технологии блокчейн применяется шифрование. С помощью данного

алгоритма любой пользователь сети получает открытые и достоверные сведения от других участников при условии полного недоверия к ним.

В заключение, хотелось бы добавить, что у технологии блокчейн есть большой ряд ярко выраженных преимуществ. Наибольшим преимуществом является обеспечение абсолютной надежности и безопасности. Тем не менее, на сегодняшний день многие специалисты не пришли к единому мнению о целесообразности глобального использования этой системы. Следовательно, пока еще рано говорить о повсеместном внедрении технологии блокчейн. Кроме того, используется не так много приложений, в основе которых лежит данная технология. И это только начало великой технологии, которая в скором времени распространится по всему миру и будет востребована в глобальных масштабах.

Список цитируемой литературы:

1. Мелани Свон. Блокчейн. Схема новой экономики / М. Свон – Москва, Олимп-Бизнес, 2017. 51 с.

2. Дон Тэпскотт, Алекс Тэпскотт. Революция блокчейн. Как технология, стоящая за биткоин, меняет деньги, бизнес и Мир / Д. Тэпскотт, А. Тэпскотт – London, Portfolio, 2016. 126 с.

3. Блокчейн – технология близкого будущего [Электронный ресурс]. – Режим доступа: http://www.moneyinformer.ru/chto-takoe/blockchain.html

ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНАХ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Источник: http://xn--80aa3afkgvdfe5he.xn--p1ai/%D0%A0%D0%9D%D0%A1%D0%9C-12_originalmaket_N.pdf

Проанализирован вопрос организации электронного документооборота в органах государственного управления. Представлена схема информационного обеспечения документооборотом.

Ключевые слова: электронный документооборот, государственное управление, региональное управление

Изучая вопрос управления государственными учреждениями в регионе, в стороне не остается проблема документооборота. Здесь важным является создание и оформление документов, которые отражают результаты и ведение деятельности организации, ее финансовое состояние, кадровую работу, материально-техническое обеспечение и т. д. Именно документы обеспечивают реализацию управленческих функций, т. к. в них определены

основные планы, зафиксированы учетные и отчетные показатели и прочая информация.

О необходимости документирования и его правилах указано в перечне нормативно-правовых актов. Например, гражданское законодательство регулирует правовое положение юридических и физических лиц в процессах предпринимательской деятельности, а также документирование различных отношений, возникающих между ее участниками. В основе гражданского законодательства стоит Гражданский кодекс. В кодексе прописаны виды и разновидности документов, их сила, которые создаются с целью фиксации актов гражданских взаимоотношений, регистрации фактов их возникновения или прекращения, подтверждения правоотношений и т. д. К примеру, некоторые статьи ГК РФ устанавливают виды документов, которые могут быть применимы при создании, регистрации, реорганизации и ликвидации юридического лица.

На текущий момент существует ряд общегосударственных законодательных и нормативных актов, которые регламентируют общие правила в подготовке, оформлении и организации работы с документами в госслужбах, организациях и учреждениях, в том числе региональных. Документы по документационному обеспечению управления разрабатываются различными органами госвласти и управления в соответствии с их компетенцией.

Схематично, ДОУ в системе информационного обеспечения документооборота можно изобразить так, как показано на рисунке 1.

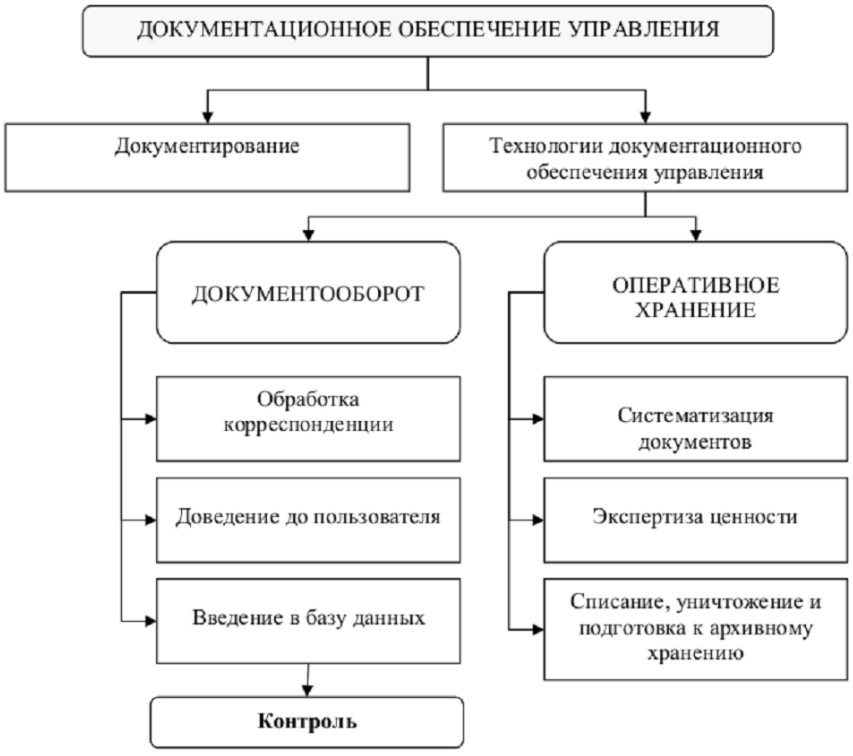


Рисунок 1. Схема информационного обеспечения документооборота

Под документооборотом понимается движение документов с периода их создания или получения до завершения исполнения, т.е. отправки их получателю или направлению в дело. Принципы организации документооборота определяются следующими составляющими: прохождение документов должно быть оперативным; каждое перемещение документа должно быть оправданным, необходимо исключить или ограничить возвратные перемещения документов; порядок прохождения и процессы обработки основных видов документов должны быть единообразными.

Выделяют положительные стороны автоматизации документационных процессов в госслужбах:

• хранение документов в электронном архиве большого объема, простота поиска;

• единообразие формирования, создания, регистрации документов;

• создание документов из шаблона, простота использования, уменьшение времени создания и коррекции документа.

Есть и отрицательные стороны электронного документооборота. Это, прежде всего, значительные расходы на его внедрение, обучение персонала работе с информационными технологиями.

На сегодня ни одна организация, ни одно крупное предприятие не может функционировать без возможности организации автоматизированного документооборота. В первую очередь такие системы разрабатываются, чтобы обеспечить помощь в наиболее эффективном управлении.

Если говорить о региональных и муниципальных государственных учреждениях системы электронного документооборота, то они становятся обязательным элементом ИТ-инфраструктуры. С их помощью повышается эффективность деятельности и решаются задачи внутреннего управления, межведомственного взаимодействия и взаимодействия с населением. Общепринятой аббревиатурой является система электронного документооборота, хотя наравне с ней также используют систему автоматизации делопроизводства, систему электронного документооборота и систему автоматизации документооборота.

В итоге становится понятно, что современный документооборот госслужб и учреждений следует рассматривать как смешанный документооборот, который основан на приоритетном использовании электронной технологии работы с документами. Документооборот государственного сектора включает значительную часть избыточных документов и инстанций их рассмотрения, а принимаемые решения нередко дублируют друг друга, а иногда носят противоречивый характер. Это приводит к фактической неуправляемости гос.учреждения.

К настоящему моменту в работу госслужб и учреждений пришел именно электронный документооборот. Основная цель автоматизации документационных процессов состоит в переходе на безбумажный документооборот. Это способствует явной выгоде учреждения. Причем данные выгоды связаны со снижением затрат на поддержку бумажного

документооборота, с качественным повышением эффективности ведения деятельности. Процесс внедрения электронного документооборота направлен на достижение поставленных целей, которые несомненно связаны с общим улучшением качества ведения деятельности, а в некоторых случая и для достижения конкретных количественных характеристик.

ПРОФЕССОР ШЕРРИ СЬЕ ОБ ЭЛЕКТРОННЫХ ДОКУМЕНТАХ И ЭЛЕКТРОННЫХ ЦИФРОВЫХ ПОДПИСЯХ

Источник: http://rusrim.blogspot.com/2019/05/blog-post_18.html
Автор: Наташа Храмцовская

В конце апреля – начале мая в листе рассылки проекта InterPARES Trust завязалась интересная дискуссия. Всё началось с просьбы одной из коллег поделиться национальным опытом архивного хранения электронных документов, подписных усиленными электронными подписями. Дальше – больше, пошёл разговор о том, а нужно ли вообще сохранять ЭЦП, и не лучше ли их сразу «снимать». Сегодня я предлагаю Вашему вниманию одно из писем известного китайского специалиста профессора Шерри Сье (Sherry Li Xie), работающей сейчас на факультете управления информационными ресурсами Народного университета Китая в Пекине.

В какой-то момент мне даже показалось, что я снова оказалась на заседании участников проекта InterPARES 2, где мы обсуждали электронные цифровые подписи (digital signatures) и обеспечение долговременной сохранности электронных документов.

Извините меня, но данная дискуссия меня смутила, поскольку мне казалось, что мы завершили обсуждение данной темы и что все согласились с тем, что ЭЦП должны быть удалены при передаче документов на архивное хранение.

Возможно, появляются новые законы / стандарты, которые ещё больше запутывают нас, вводя «юридические определения» ... требуется больше времени на то, чтобы это проверить, а в данный момент я хотела бы сказать следующее:

Поскольку мы все согласны (так мне, по крайней мере, кажется) с тем, что подписи и печати играют разные роли в разных контекстах (или, точнее говоря, посредством различных процедур), - то как насчёт того, чтобы нам для начала разделить эти функции, в интересах как концептуальных, так и практических целей, перечислив их одну за одной?

Если процедура требует наличия подписи для того, чтобы документ был завершённым, то давайте смотреть на неё только так, оставляя в стороне

выполняемую ею функцию аутентификации. То же самое касается печати. Если процедура требует наличия печати для того, чтобы документ был завершённым, то в этом случае давайте считать её частью документа и ничем иным. Не все процедуры требуют одновременно и подписи, и печати; но когда это имеет место, давайте рассмотрим оба эти элемента как часть документа.

Процедура также может потребовать использования разных печатей для разных типов документов одного и того же автора. Заметьте, пожалуйста, я говорю здесь не «создатель» (creator), а «автор / писатель» (author/writer).

В древней китайской практике у чиновников / лиц умственного труда было несколько печатей, для разных «шляп» (*т.е выполнявшихся ими функций*), которые они носили в своей общественной и личной жизни. Проще говоря, печать, использовавшаяся для письма от отца к сыну, отличалась от печати, использовавшейся тем же человеком в переписке с его коллегами, начальством или друзьями. Таким образом, можно утверждать, что печать служила не только в качестве средства аутентификации, но и элемента контента, поскольку она показывала отношения / настроения.

До сих пор речь шла только о завершённости (completeness) документа - будь то PDF-файл с отсканированными образами подписей и печатей или база данных с метаданными, выполняющими функции подписей и печатей (только для целей обеспечения завершённости). На данном этапе средства аутентификации не рассматриваются; - и когда они рассматриваются, мы не называем их «подписью» или «печатью». Всегда утешительно находить электронные эквиваленты дорогих нам физических вещей, - но с некоторыми из них, как ни больно, придётся расставаться.

Теперь я ещё раз повторю ключевые идеи, но с добавлением китайских ингредиентов. Электронная цифровая подпись не является традиционной подписью, несмотря на то, что она выполняет одну из функций традиционной подписи. Эта функция, однако, является вторичной. Как говорит Лючиана [Дюранти], подпись в первую очередь удостоверяет контент (мой китайский пример связывает печать с контентом, поэтому я включаю сюда и электронную печать).

Как я поняла много лет назад, электронная цифровая подпись нацелена на выполнение всех функций аутентификации, ранее выполнявшихся печатью, носителем информации, почерком (включая собственноручную подпись) ... т.е. всеми элементами дипломатики, которым меня научила Лючиана, а также кодовыми словами, использованием определенной цветовой схемы, присоединённого ювелирного украшения, следов слёз – элементами китайского стиля аутентификации древних документов и их контента. Так зачем называть ЭЦП «подписью»?

В древнем Китае наиболее эффективным средством аутентификации приказов императоров (в том числе его королевы и его матери) был носитель информации, - а не почерк (потому документ во многих случаях писался не им) и даже не печать. Важность печати возросла только в необычные времена, когда поставки дорогих и сложных в изготовлении носителей

прервались. Императорская печать стала эффективным инструментом, потому что её было гораздо легче изготовить (шёлк против камня).

В современном китайском бумажном документообороте, из всех средств аутентификации - носителя, печати и подписи, подпись является самым слабым (хотя подделка носителя и печати тоже не так уж и сложна). Единственный надёжный способ аутентификации бумажного документа - это его проверка, однако подпись и печать обязательны для завершённости официальных и административных документов.

В электронной среде, в рамках обычной деятельности обычных людей, их электронные учётные записи устанавливают их личность и обеспечивают неотказуемость, а работающий телефон обеспечивает аутентификацию. Когда содержимое учётной записи необходимо представить в рамках юридических споров, телефонный аппарат и контент оба могут быть использованы в качестве доказательств. Если представлен телефон, то средства аутентификации не нужны. Для содержимого, отделенного от телефона, аутентификация требуется, и, в соответствии с правилами недавно созданного Интернет-суда, доказательства должны быть зафиксированы в блокчейне. Однако в настоящее время всё это не является проблемой долговременного хранения, поскольку дела, рассматриваемые в Интернет-суде, не требуют долгосрочного сохранения. Но поставьте на место телефона информационную систему, а на место контента - отдельные документы. В чем разница?

Что касается обеспечения долговременной сохранности электронных документов, я согласна с теми, кто считает, что электронная цифровая подпись, электронная печать, электронная отметка времени и т.д. должны рассматриваться в качестве средств аутентификации лишь в течение конечного периода времени, и их следует удалить, как только они перешагнут порог архивов. Удаление средств аутентификации не повлияет на завершённость документов; и для непрерывного подтверждения аутентичности всегда есть другие средства аутентификации, которые могут применяться с момента попадания документов в архив. Что касается электронных архивов, которые решили поддерживать электронные цифровые подписи для PDF-файлов, мне всё еще трудно понять их подход.

С искренним уважением,

Шерри Сье

Мой комментарий: Я задала Шерри по поводу её письма вопрос, который, как мне кажется, для нас очень актуален:

Уважаемая Шерри.

Согласитесь, ли Вы со мной, что так называемое «снятие/удаление электронных цифровых подписей» на самом деле не означает их физическое удаление; а подразумевает, что – хотя данные оригинальной ЭЦП могут по-прежнему сохраняться в качестве артефакта, - ЭЦП в будущем уже не используются для целей проверки и аутентификации?

Это различие важно, поскольку кое-кто понимает «удаление» буквально.

В моей стране нам потребуется изменить законодательство для того, чтобы использовать подобный подход.

С уважением, **Наташа Храмцовская**

Ответ я получила следующий:

Уважаемая Наташа.

Я действительно имею в виду физическое удаление, то есть уничтожение данных подписи. Разумеется, это относится к «обычным» документам (которых большинство) и при условии, что архивами была успешно проведена проверка подписей в ходе приёма на хранение.

Доверенное хранилище может быть достаточно защищённым, и мы знаем, что ни одна система (в том числе с использованием хешей и инфраструктуры PKI) не является неуязвимой от злонамеренных атак. У меня нет цифр в плане объёмов хранения и стоимости периодической проверки, но я не думаю, что сохранение данных электронной подписи и/или проведение периодических повторных проверок подписей является лучшей идеей.

Если система достаточно защищена, то почему мы меньше думаем о системе, и больше – об отдельных PDF-файлах? Я понимаю, что цифровая криминалистическая экспертиза всё ещё стоит дорого, но надеюсь, что мониторинг системы (который может включать мониторинг отдельных документов) может вскоре стать более простым и экономически эффективным, так что даже действия инсайдеров можно будет выявлять и предотвращать.

Шерри Сье

Не знаю, согласитесь ли Вы со мной, уважаемые читатели, однако моя позиция следующая: светила мировой архивной науки могут быть вполне правы в том, что в длительной перспективе сохранение электронных оригиналов и уж тем более оригинальных электронных подписей, отметок времени, печатей и т.п., не является самоцелью; наших потомков, вполне вероятно, устроят заверенные электронные копии, сохраняемые доверенным хранилищем. Это, однако, отдаленное – и отнюдь не гарантированное – будущее, ну а пока что мы живём в том правовом поле, которое имеем, и по-прежнему сохраняет свою актуальность совет Остапа Бендера чтить Уголовный кодекс (и все прочие Кодексы тоже!).

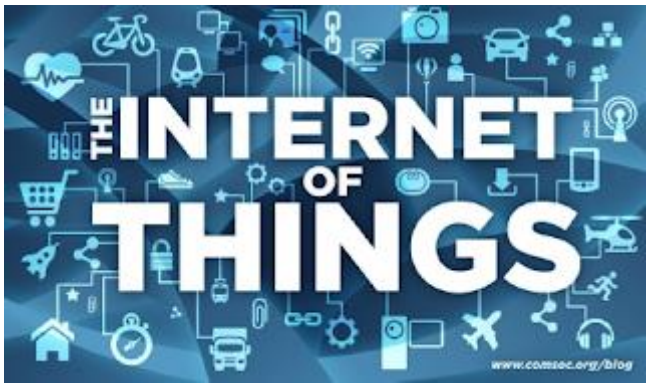
В электронные архивы пойдут достаточно «молодые» документы, которые могут потребоваться в качестве доказательств в судебных спорах и расследованиях, и вряд ли нам сильно захочется без веских на то оснований ставить под сомнение юридическую и доказательную силу тех документов, что хранят наши архивы. Нам приходится учитывать и то, что в ходе спора противная сторона может предъявить свой экземпляр электронного

подлинника, который по умолчанию будет иметь большую доказательную силу, чем копия.

В общем, я считаю, что нам следует – пока что – проявлять разумную консервативность. До тех пор, пока не накопится опыт и не сложится практика работы электронных архивов, как мне кажется, лучше немножко перестраховываться. Наверное, кое-где придётся по тем или иным причинам прокладывать путь «по целине» и идти на риск несоответствия устаревшим нормам права, но в этом случае нужно будет тщательно сопоставлять риск и ожидаемую деловую отдачу, и принимать решения «с открытыми глазами».

ИСО И МЭК РАБОТАЮТ НАД СТАНДАРТАМИ ДОВЕРИЯ К ИНТЕРНЕТУ ВЕЩЕЙ

Источники: сайт ИСО / сайт МЭК
https://www.iso.org/contents/data/standard/05/32/53267.html
https://www.iso.org/contents/data/standard/05/32/53269.html
https://www.iec.ch/dyn/www/f?p=103:38:17324040970164:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,101891
https://www.iec.ch/dyn/www/f?p=103:38:17324040970164:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,102266



Одна из сильных сторон специалистов в области управления документами и архивного дела – это понимание того, каким образом обеспечивается доверие к документам и информации. В части доверия мы можем оказаться полезными в междисциплинарных проектах, и именно поэтому я слежу за тем, как вопросы обеспечения такого доверия решаются в сопредельных отраслях.

В последнее время вопросами доверия решил вплотную заняться технический подкомитет SC41 «Интернет вещей и взаимосвязанные технологии» (Internet of Things and related technologies,

https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:20486) объединённого технического комитета ИСО/МЭК JTC1.

Недавно опубликованный терминологический стандарт ISO/IEC 20924:2018 «Информационные технологии – Интернет вещей (IoT) – Словарь» (Information technology - Internet of Things (IoT) - Vocabulary, см.https://www.iso.org/contents/data/standard/06/94/69470.html и https://www.iso.org/obp/ui/#!iso:std:69470:en, а также мой пост о нём http://rusrim.blogspot.com/2019/01/isoiec-20924.html) так определяет свойство «заслуживать доверие» (trustworthiness):

3.1.32 благонадёжность (trustworthiness) - свойство заслуживать доверие или уверенность;

3.2.10. благонадёжность компоненты интернета вещей (IoT trustworthiness) - свойство компоненты интернета вещей заслуживать доверие или уверенность в том, что в течение всего своего жизненного цикла она будет способна обеспечить безопасность, неприкосновенность частной жизни, защищенность, надёжность и жизнестойкость (resiliency).

Подкомитет JTC1/ SC41 работает над следующими проектами документов:

ISO/IEC 30147 «Интернет вещей (IoT) – Методология обеспечения и поддержания доверия к системам и сервисам интернета вещей» (название на сайте ИСО: “Information technology - Internet of things - Methodology for trustworthiness of IoT system/service”, см. https://www.iso.org/contents/data/standard/05/32/53267.html; и, несколько иное, на сайте МЭК: “Internet of Things (IoT) – Methodology for implementing and maintaining trustworthiness of IoT systems and services”, https://www.iec.ch/dyn/www/f?p=103:38:17324040970164::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,101891).

В аннотации на документ отмечается:

«В рамках интернета вещей (IoT) все IoT-устройства могут быть взаимно соединены друг с другом, и это, как ожидается, привнесёт новые удобства в повседневную жизнь. С другой стороны, у ряда устройств, которые прежде не подключались к интернету, при подключении могут возникнуть проблемы с доверием к ним, что может повлечь серьёзные негативные последствия для повседневной жизни, в сравнении с серверами и персональными компьютерами, которые уже давно работают в Интернете.

Тем самым подразумевается, что у IoT-систем и услуг имеются специфические свойства и характеристики, отличающие их от соответствующих характеристик иных существующих ИТ-систем и услуг. Можно привести следующие примеры:

- Широта охвата и степень воздействия угроз очень велики;
- Жизненный цикл IoT-систем и услуг очень длительный;
- Проводить мониторинг и управлять некоторыми типами IoT-устройств может быть очень сложно;

- Для субъектов телекоммуникационного обмена, включая IoT-устройства, может быть сложно в достаточной степени знать условия деятельности друг друга;
- Функциональные возможности и характеристики некоторых IoT-устройств могут быть ограничены технологически;
- В рамках IoT-систем и услуг взаимосвязи между компонентами могут быть установлены способами, которые их разработчики не предвидели.

Цель настоящего документа заключается в том, чтобы предложить методологию обеспечения и поддержания доверия к IoT-системам и услугам, поскольку уже существующие методологии предназначены для отдельных областей применения и не обязательно охватывают все проблемы, с которыми сталкиваются IoT-системы и услуги ввиду упомянутых выше характерные особенностей. Методология описана для каждого из процессов, перечисленных в стандарте ISO/IEC/IEEE 15288:2015 Системная и программная инженерия - Процессы жизненного цикла систем (Systems and software engineering - System life cycle processes, см. https://www.iso.org/contents/data/standard/06/37/63711.html и https://www.iso.org/obp/ui/#!iso:std:63711:en).»

Содержание документа следующее:

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Символы и сокращения

5. Специфические характеристики IoT-систем и сервисов

6. Специфические для IoT-систем и сервисов вопросы, которые необходимо принять во внимание

7. Обзор методологии и её применения

8. Методологии обеспечения и поддержания доверия

Приложение А (справочное): Доверие к промышленным IoT-системам – вариант применения и модель для анализа

Библиография

ISO/IEC 30149 «Интернет вещей (IoT) – Концепция обеспечения доверия» (Internet of things (IoT) - Trustworthiness framework, см.

https://www.iso.org/contents/data/standard/05/32/53269.html и https://www.iec.ch/dyn/www/f?p=103:38:17324040970164:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,102266).

В аннотации на документ отмечается:

«Цель настоящего международного стандарта - помочь организациям органически интегрировать обеспечения доверия на протяжении всего жизненного цикла их IoT-систем посредством:

а) формулирования понятий, принципов, концепций, описания компонентов и процессов;

b) предоставления процессно-ориентированных механизмов для установления требований к обеспечению доверия, оценки соответствующих рисков, назначения уровней доверия (Levels of Trust) и для выбора соответствующих мер безопасности и верификации;

c) рекомендаций по вопросам установления критериев приемлемости для организаций, передающих на аутсорсинг разработку или эксплуатацию IoT-систем, и для организаций, закупающих решения третьих сторон;

d) предоставления процессно-ориентированных механизмов для выявления, генерирования и сбора доказательств, необходимых для демонстрации того, что их IoT-системы заслуживают доверия при определенных условиях;

e) поддержки общих концепций, описанных в стандартах ISO/IEC 30141, ISO 30147, ISO/IEC 27001, ISO/IEC 27005 и в стандартах серии ISO/IEC 27034, содействия тем самым удовлетворительному обеспечения доверия с помощью подхода на основе менеджмента риска; а также

f) формулировки концепций, помогающих адаптировать и внедрять меры и средства обеспечения доверия, безопасности и защиты персональных данных, описанные в других стандартах, таких как ISO/IEC 27002.

Настоящий международный стандарт:

a) применим в отношении базового программного обеспечения и оборудования IoT-системы, а также факторов, влияющим на доверие к ней, таких, как данные, технологии, процессы жизненного цикла разработки системы, поддерживающие процессы и действующие лица; а также

b) применим в организациях любого типа и размера, независимо от сектора, к которому они принадлежат (например, в коммерческих предприятиях, отраслях промышленности, в государственных органах, в некоммерческих организациях и домашних хозяйствах), которые подвержены рискам, связанным с IoT-системами».

Содержание документа следующее:

ТЕХНОЛОГИЯ БЛОКЧЕЙНА ЯВЛЯЕТСЯ ТЕХНОЛОГИЕЙ УПРАВЛЕНИЯ ДОКУМЕНТАМИ!

Источник: сайт IG GURU https://igguru.net/2019/05/01/blockchain-technology-is-recordkeeping-technology/
Автор: Патриция Фрэнкс

Специалистам по управлению документами и информацией и раньше часто приходилось разбираться с последствиями внедрения трансформирующих технологий на программы и практики управления документами и информацией. В 19-м веке это было изобретение пишущей машинки. В течение 20-го века появились программируемые компьютеры и ПК. В начале 21-го века это были технологии социальных сетей. Сегодня нам приходится иметь дело, помимо прочего, с большими данными и искусственным интеллектом.

Неудивительно поэтому, что занимающиеся управлением документами и информацией профессионалы в настоящее время изучают влияние технологий блокчейна и распределенных реестров. В данной статье дан краткий обзор технологий блокчейна (Blockchain) и распределенных реестров (Distributed Ledger Technologies, DLT), адресованный специалистам по управлению документами и информацией.

Основы технологии блокчейна и распределенных реестров

Нет какого-то единого общепринятого определения блокчейна. В 2016 году Дон и Алекс Тэпскотты (Don and Alex Tapscott) говорили о блокчейне как о «неподверженном порче реестре экономических транзакций, который можно использовать для документирования не только финансовых транзакций, но и любых активов» (Tapscott, 2016).

В 2018 году американский Национальный институт стандартов и технологий (NIST) описал распределенный регистр как состоящий из «подписанных криптографическим образом транзакций, которые сгруппированы в блоки, причем каждый блок, после проверки и принятия решения на основе консенсуса, криптографически связывается с предыдущим». Каждый из узлов блокчейн-сети хранит собственный экземпляр одного и того же реестра, и конфликты разрешаются автоматически в соответствии с установленными правилами. Распределенный реестр представляет собой неподверженный изменениям единственный источник истины. Следовательно, использование распределенного реестра означает распределенное доверие.

Полезно представлять себе распределенный реестр как базу данных, которая совместно используется и синхронизируется на основе консенсуса многочисленными сайтами, учреждениями или географическими регионами. Однако между традиционной базой данных и распределенным реестром существуют различия, отражённые в Таблице 1.

Таблица 1: Сопоставление традиционной базы данных и распределённого реестра

Централизованная база данных	Распределённый реестр
Нужно внешнее и внутреннее согласование	Консенсус в отношении данных
Нет ограничений	Неподверженность изменениям
Единая точка отказа	Распределён по сети узлов
Единая точка контроля	Децентрализованный контроль
Вовлечены шлюзы и посредники	Прямое взаимодействие участников
Криптография как довесок	Криптографическая верификация
Действия выполняются от имени других лиц	Криптографическая аутентификация/авторизация
Резервное копирование обеспечивается «вручную»	Усиление живучести и доступности при росте числа узлов

Был опубликован ряд древовидных схем принятия решений. Все они предполагают, что Вы, отвечая на вопросы, в конечном итоге приходите к одному из двух возможных результатов:

1) Вам следует использовать традиционную базу данных;

2) Вам может подойти распределенный реестр. Обратите внимание на слово «может» - даже если Вы получите рекомендацию использовать распределенный реестр, Вам следует принять во внимание следующие вопросы:

- Может ли в будущем возникнуть необходимость изменить или удалить какие-либо из хранимых данных?
- Будут ли храниться персональные и/или «чувствительные» данные?
- Будут ли храниться «большие данные»?

Если Вы подумываете об использовании распределенного реестра, то в случае положительного ответа на какой-либо их этих вопросов Вам стоит рассмотреть альтернативные варианты хранения, например, хранение в блокчейне только хешей данных, а самих данных – вне блокчейн-цепочки.

Примеры использования технологий блокчейна и распределенных реестров

Воздействие технологий блокчейна и распределенных реестров на Ваши программы понять проще, если вы знакомы с примерами внедрения этих технологий. В то же время большинство соответствующих разработок находятся на стадии пилотных проектов или на ранних стадиях внедрения, когда нельзя ещё говорить об успехе в длительной перспективе.

Пилотные проекты внедрения технологий блокчейна и распределённых реестров появляются сейчас практически в каждой отрасли, включая

здравоохранение, управление цепочками поставок, образование и государственное управление, как показано в Таблице 2.

Таблица 2: Примеры пилотных проектов внедрения блокчейн-технологий

Вариант применения	Проблема	Предлагаемое решение
Здравоохранение	Врачебные ошибки – третья по частоте причина смертей. Сведения о здоровье пациента могут храниться в нескольких базах данных различных поставщиков. Эти изолированные друг от друга источники часто содержат неполные или устаревшие сведения.	Инициатива MedRec университета MIT предусматривает использование блокчейна для управления документами пациента на протяжении его жизни, по мере их перемещения между поставщиками медицинских услуг. MedRec не хранит сами документы, а регистрирует метаданные, обеспечивающие защищённый доступ.
Управление цепочками поставок: безопасность продуктов питания	Серьёзным недостатком является неспособность быстро выделить некачественные продукты и изъять из оборота только их, а не все продукты данной категории	Блокчейн-решение FoodTrust фирмы IBM обеспечивает прослеживаемость движения продуктов от начала до конца между оптовиками и розничной торговлей.
Образование	Выпускникам вузов приходится обращаться за получением официальных копий документов об образовании, необходимых для последующего обучения и трудоустройства.	Коммьюнити-колледж, штат Нью-Мексико, использует блокчейн для выдачи студентам электронных дипломов. Третьи стороны могут мгновенно проверить верность сведений
Госуправление: электронное голосование	Расквартированные за рубежом военнослужащие и проживающие за рубежом граждане не могут быть уверены в учёте их голосов, поданных по спецбюллетеням, ввиду ряда проблем с почтой и оформлением	На выборах 2018 года в штате Западная Вирджиния 144 военнослужащих, несущих службу в 24 странах, смогли проголосовать с использованием блокчейн-технологии.

Обратите внимание на то, что в таблице для каждого варианта применения указана проблема, которая может быть решена благодаря использованию технологий блокчейна и распределенных реестров.

Сильные и слабые стороны

Блокчейн - это документационная технология, у которой есть как сильные, так и слабые стороны. Её сильной стороной является то, что записи в блокчейне о транзакциях неподвержены изменениям. Кроме того, существует множество копий, поскольку каждый узел (компьютер) в сети обладает точной копией блокчейн-цепочки. Технология блокчейна устраняет потребность в посредниках и позволяет осуществлять транзакции с использованием одноранговой (peer-to-peer) технологии прямого

информационного взаимодействия между участниками, повышая эффективность и сокращая время исполнения транзакций.

Однако у этой технологии есть и слабые стороны. Неизменность записей создаёт проблемы в случае, если в блокчейне хранятся персональные данные или чувствительная информация. Согласно как законодательству Евросоюза о защите персональных данных (GDPR), так и закону штата Калифорния о защите неприкосновенности частной жизни потребителей граждане имеют право требовать по запросу, за некоторыми исключениями, «стирания» информации (право быть забытым).

Сегодня нет способов удаления данных из блокчейна, но это может измениться. Пока же лучший способ обеспечить соблюдение законодательно-нормативных требований в отношении защиты неприкосновенности частной жизни - хранить такие данные вне блокчейн-цепочки. Избыточность также создает проблемы, поскольку чем больше информации сохраняется в большой сети узлов, тем сильнее замедляется весь процесс. Из-за того, что документированная информация хранится в многочисленных блоках и блокчейнах, происходит потеря контекста. Существует риск для неприкосновенности частной жизни, связанный с тем, что технология использует псевдонимы, а не анонимизацию. Уже разработаны приложения для анализа транзакций и IP-адресов на основе данных в публичных блокчейнах. Кроме того, непрерывно меняются как технологии, так и нормативно-правовая среда.

Воздействие на программы и практики управления документами и информацией

Независимо от того, в какой отрасли Вы работаете, Вам следует понимать, какие типы проблем существуют, и способны ли технологии блокчейна и распределённых реестров их решить. Воздействие, которое такие решения оказывают на программы и практики управления документами и информацией и практики, может быть различным в зависимости от обстоятельств.

Проблемы внедрения схожи с теми, что возникают при работе с документами, сохраняемыми с помощью любой другой технологии. Ниже перечислен ряд вопросов, которые следует задать и на которые нужно получить ответ:

- Как хранящиеся вне блокчейн-цепочки данные будут интегрированы с блокчейном (как данные организации, так и информация, необходимая третьей стороне для выполнения смарт-контрактов)?
- Соответствует ли решение географическим / юрисдикционным ограничениям на размещение данных?
- Требуются ли права доступа, или же транзакционная информация и электронный контент будут полностью прозрачными для всех участников сети?
- Существует ли потребность в интеграции информации в блокчейне с электронным контентом, хранимым вне блокчейна? Если да, то возможно ли это?

- Соответствует ли блокчейн-решение применимому законодательству, такому, как законы GDPR и CCPA?
- Создаются ли при использовании блокчейн-решения новые документы, которыми нужно управлять? Если да, то какие политики следует для этого разработать?

Блокчейн и отрасль управления документами и информацией

В данный момент технология блокчейна не считается заменой для практики управления электронными документами, однако в этом вопросе наблюдается определенное движение в отрасли. Осуществляется интеграция с блокчейн-решениями существующих решений для управления документами и информацией –например в Голландии компания Sphereon (см.https://sphereon.com/solutions-for-blockchain/) предлагает два расширения для служб управления контентом и процессов решения Alfresco, которые обеспечивают ведение протокола аудита и аутентификации на основе блокчейна, а также API-интерфейс и инструментальный набор для разработки программного обеспечения, которые можно использовать в качестве элементиов рабочих процессов.

В Гибралтаре платформа RecordsKeeper (см. https://www.recordskeeper.co/) построена на основе многоцепочечной (multichain) технологии, поддерживающей глобально доступную децентрализованную систему управления документами. RecordsKeeper позволяет публиковать неизменяемые объекты данных размером до 10 МБ в блоке в блокчейне RecordsKeeper Blockchain с использованием токенов XRK в качестве «горючего».

Выводы

Технологии блокчейна и распределенных реестров не являются альтернативой современной практике управления электронными документами и информацией. Прежде чем рассматривать полномасштабное внедрение этих технологий, убедитесь, что текущие процедуры работы с данными, документами и информацией являются эффективными, и проведите оценку блокчейн-технологии и вариантов использования. Если принято решение внедрить блокчейн-решение, то разработайте политики для реагирования на последствия для управления документами. Внедрите системы для реализации новых политик. Убедитесь, что записанные в блокчейне документы / транзакционные данные будут оставаться доступными с течением времени. Определите, сможете ли Вы осуществить уничтожение/передачу документов / транзакционных данных в блокчейне по истечении сроков хранения, и если да, то каким образом. И, наконец, внедряйте блокчейн, но делайте это с осторожностью.

Литература:

[1] Дон и Алекс Тэпскотты (Tapscott, Don and Alex) «Блокчейн-революция» (Blockchain Revolution), Нью-Йорк, изд-во Penguin Random House, 2016 г.

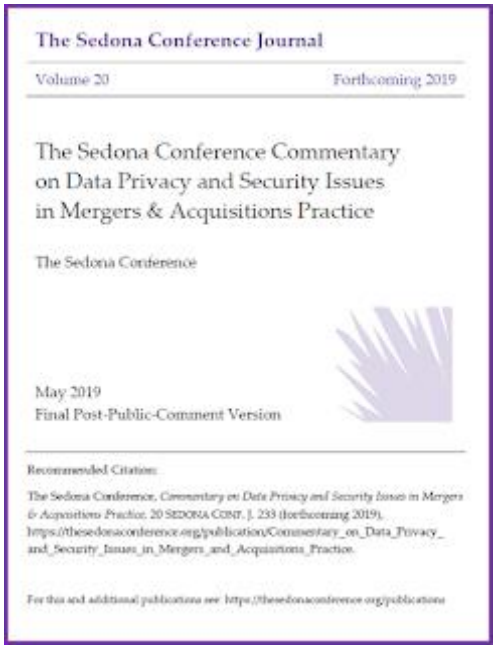
[2] Национальный институт стандартов и технологий (NIST), межведомственный отчёт NISTIR 8202 «Обзор технологии блокчейна» (NIST

Interagency Report (NISTIR) 8202: Blockchain Technology Overview), октябрь 2018 г., см.https://csrc.nist.gov/publications/detail/nistir/8202/final , прямая ссылка: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

США: «КОНФЕРЕНЦИЯ СЕДОНА» ОПУБЛИКОВАЛА ДОКУМЕНТ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ДАННЫХ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ СЛИЯНИЯ ИЛИ ПОГЛОЩЕНИЯ ОРГАНИЗАЦИЙ

Источник: сайт Конференции Седона
https://thesedonaconference.org/publication/Commentary_on_Data_Privacy_and_Security_Issues_in_Mergers_and_Acquisitions_Practice

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), - сообщил о публикации окончательной версии «Комментария Конференции Седона по вопросам обеспечения безопасности данных и защиты персональных данных в ходе слияний и поглощений».



Конференция Седона (Sedona Conference) и ее рабочая группа WG11 по ответственности за защиту персональных данных и неприкосновенности частной жизни (Data Security and Privacy Liability) рады сообщить о публикации финальной, 2019 года редакции **«Комментария Конференции Седона по вопросам обеспечения безопасности данных и защиты персональных данных в ходе слияний и поглощений»**. (The Sedona Conference Commentary on Data Privacy and Security Issues in Mergers and Acquisitions Practice).

Рабочая группа WG11 разработала настоящий Комментарий по слияниям и поглощениям, в качестве практического руководства по вопросам безопасности данных и защиты персональных данных, которые необходимо учитывать при потенциальном слиянии или поглощении. При этом Комментарий подходит к этим вопросам с точки зрения покупателя. Он не предназначен быть исчерпывающим, а, скорее, должен послужить основой для решения вопросов безопасности и защиты персональных данных, которые могут повлиять на подобную сделку.

Данный документ адресован не только специалистам, готовящим слияние / поглощении, но и тем лицам, кто уже после заключения сделки будет заниматься интеграцией приобретенных активов. Для того, чтобы сделать документ более удобным для практического применения, к нему добавлен перечень категорий и типов данных, связанных с анализом сделки; образцы заверений и гарантий, касающихся проблемы защиты персональных данных и безопасности данных; и основные требования в части проявления должной осмотрительности.

Документ объёмом 110 страниц можно бесплатно скачать (при условии предоставления персональных данных) с веб-страницы сайта Конференции Седона по адресу: https://thesedonaconference.org/publication/Commentary_on_Data_Privacy_and_Security_Issues_in_Mergers_and_Acquisitions_Practice

ИСО: ПОДГОТОВЛЕН НОВЫЙ СТАНДАРТ ISO 22396 «ЖИЗНЕСТОЙКОСТЬ СООБЩЕСТВ – РУКОВОДСТВО ПО ИНФОРМАЦИОННОМУ ОБМЕНУ МЕЖДУ ОРГАНИЗАЦИЯМИ»

Источник: сайт ИСО
https://www.iso.org/contents/data/standard/05/02/50292.html
https://www.iso.org/obp/ui/#!iso:std:50292:en

Как сообщили сайты Международной организации по стандартизации

(ИСО) и Британского института стандартов (BSI), в настоящее время идёт голосование по проекту стандарта **ISO 22396 «Безопасность и жизнестойкость – Жизнестойкость сообществ - Руководство по информационному обмену между организациями»** (Security and resilience - Community resilience - Guidelines for information exchange between organizations) объёмом 14 страниц основного текста, см.https://www.iso.org/contents/data/standard/05/02/50292.html и https://www.iso.org/obp/ui/#!iso:std:50292:en . Стандарт разработан техническим комитетом ISO/TC 292 «Безопасность и жизнестойкость» (Security and resilience).

Познакомиться с текстом документа и принять участие в его обсуждении можно до 22 мая 2019 года на сайте Британского института стандартов по адресу https://standardsdevelopment.bsigroup.com/projects/2016-00357 .

В аннотации на документ отмечается:

«Настоящий документ содержит рекомендации по обмену информацией. Он включает в себя принципы, рамочную структуру и процесс обмена информацией. Стандарт определяет механизмы обмена информацией, которые позволяют участвующей организации учиться на чужом опыте, ошибках и успехах. Он может использоваться в качестве руководства при поддержке механизма обмена информацией с целью повышения заинтересованности и вовлечения. Он предусматривает меры, которые повышают способность участвующей организации справляться с риском перебоев в её деловой деятельности.

Настоящий документ может использоваться частными и государственными субъектами, которым требуется руководство по созданию условий для поддержки обмена информацией.

Настоящий документ не охватывает технические аспекты, и основное внимание в нём уделяется вопросах методологии.»

Содержание документа следующее:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Принципы
5. Рамочная структура
6. Внедрение

Приложение А: Протокол «Светофор» (Traffic light protocol, TLP)

Библиография

Более подробно цели и задачи стандарта раскрываются следующим образом:

«Ландшафт риска изменился для всех действующих лиц общества: частных предприятий, государственных и негосударственных организаций. Люди стали более взаимосвязанными и взаимозависимыми, что приводит к тому, что риски накладываются друг на друга и пересекают границы.

Изменение формы собственности на объекты критически-важной социальной инфраструктуры и на сервисы означает, что частные предприятия должны быть вовлечены в разработку механизмов для повышения способности справляться с проблемами и нештатными ситуациями, для расширения обмена опытом и знаниями. Ключевая социальная инфраструктура и услуги все чаще находятся в частном управлении или собственности, что создает новые требования в отношении сотрудничества и обмена информацией в целях наращивания потенциала для преодоления трудностей.

В то время, как органы власти в юрисдикции несут основную ответственность за обслуживание и защиту своих граждан, решения часто отыскиваются в частном секторе, несмотря на то, что превентивные меры для повышения безопасности критически-важных общественных функций традиционно включаются в сферу основной деятельности правительства и государственных органов. В целях усиления и поддержки превентивных мер защиты, многочисленные действующие лица как из частного, так и из государственного секторов должны иметь возможность эффективно и безопасно обмениваться информацией в целях повышения общественной безопасности и жизнестойкости общества.

Как правило, целью сотрудничества является определение и инициирование действий по повышению безопасности и снижению уязвимости. Обмен информацией о возможной материальной ответственности, рисках и уязвимостях может повысить эффективность и результативность деятельности организаций.

Сложно, но необходимо установить четкие границы между организациями в отношении обмена информацией. Ответственность за координацию также сложно установить, поскольку координация усилий в этих областях требует специальных решений, адаптированных внутри сектора - для каждого отдельного сектора, региона или страны.

Действующим лицам из частного сектора также требуются гарантии того, что не будет утечек их конфиденциальной деловой информации, что она не будет использована препятствования конкуренции или нанесения ущерба их деловой деятельности и торговой марке. Следовательно, безопасность обмена информацией является важнейшим условием его успешности и эффективности информацией как для государственных, так и для частных организаций.

Организации, участвующие в соглашениях об обмене информацией, могут расширить свои знания и понимание событий и рисков с целью повышения своей жизнестойкости. Эффективные механизмы обмена информацией способны дать этим организациям и другие преимущества, в том числе:

- ознакомление организаций, которые могли не иметь доступа к соответствующей информации при использовании обычных способов;
- расширение возможностей благодаря разблокирования доступа к информации ограниченного доступа;

- создание централизованной информационной биржи, способствующей информационному обмену;
- увеличивает возможностей для распространения информации; а также
- создание чувства общности благодаря внимательному отношению друг к другу и коллективному использованию информации и ресурсов.

Настоящий документ разделен на три сегмента: принципы, рамочная структура и процесс. Принципы представляют собой ядро стандарта. Рамочная структура определяет необходимые элементы для разработки механизмов обмена информацией. Процесс описывает процедуры обмена информацией, реализующие и поддерживающие соответствующие соглашения.»

ИСО: КАКИЕ НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ТЕХНИЧЕСКИЙ ПОДКОМИТЕТ ТС46/SC11 «УПРАВЛЕНИЕ ДОКУМЕНТАМИ» МОГ БЫ ВЗЯТЬ ЗА ОСНОВУ БУДУЩИХ ПРОЕКТОВ?

Источник: сайт итальянского национального органа по стандартизации UNI
http://store.uni.com/catalogo/index.php/uni-11386-2010.html
http://store.uni.com/catalogo/index.php/uni-11536-2014.html

Ежегодно технический подкомитет ИСО ТС46/SC11 «Управление документами» требует от участвующих в его работе национальных технических комитетов и подкомитетов отчёты об их деятельности. В частности, задаётся вопрос о том, какие национальные стандарты можно было бы использовать в качестве основы для новых проектов ИСО.

В этом году на данный вопрос ответили две страны: Южная Корея и Италия, - и, как оказалось, названные ими документы мне пока что «на зуб» не попадались, так что я решила собрать о них информацию.

Южная Корея

Корейский специалист Чо Сун-ам (Song-Ahm Cho), рассказывая в 2015 году на блоге технического подкомитета ИСО ТС46/SC11 о национальных стандартах в сфере управления документами и архивного дела (см.https://committee.iso.org/sites/tc46sc11/home/news/content-left-area/news-about-standarization-in-t-1/records-management-standards-in.html), сообщила, что «Разработка стандартов архивного дела и управления документами в Южной Корее идёт по двум направлениям. Разработка общенациональных стандартов управления документами возложена на Корейское агентство по

технологиям и стандартам (Korea Agency for Technology and Standards, KATS, http://www.kats.go.kr/en/main.do) в соответствии с Законом о промышленной стандартизации. Кроме того, Национальные Архивы Кореи разрабатывает стандарты управления государственными архивами и документами для государственных учреждений и организаций на основе Закона об управлении государственными документами».

И если стандарты Национальных Архивов выложены в свободном доступе, то документы, разработанные под эгидой KATS, являются платными и, соответственно, добраться до них сложно.

KS X 6500:2010 (подтверждён в 2015 году) «Управление важнейшими документами и готовность на случай катастроф» (самоназвание на английском языке: Essential records management and disaster planning for records), см. https://www.kssn.net/search/stddetail.do?itemNo=K001010108787

Как отмечается в аннотации, настоящий стандарт содержит рекомендации в отношении процедур и требований к управлению важнейшими документами и их внедрению, с тем, чтобы защитить документальные активы организации и обеспечить непрерывность деловой деятельности в случаях, когда государственная или частная организация - создатель документов, сталкивается с катастрофической ситуацией.

Поскольку общие требования к документами, а также к проектированию и внедрению документных систем установлены стандартом ISO 15489 «Информация и документация - Управление документами», то данный стандарт определяет принципы и требования, специфические для управления важнейшими документами в соответствии с рекомендациями по менеджменту готовности к нештатным ситуациям и реагированию на них в соответствии с ситуацией, и устанавливает необходимую для этих целей программу управления документами, а также процедуры поддержки управления документами организации в случае катастроф.

Настоящий стандарт был разработан в качестве руководства по вопросам защиты, хранения, классификации, использования и планирования важнейших документов. Он описывает стандартный способ выявления и защиты документов и информации, относящихся к категории «важнейших». Стандарт также описывает методы оценки последствий для организации утраты важнейших документов и информации.

Небольшие организации, не имеющие кадровых ресурсов для менеджмента рисков или выполнения работ в условиях чрезвычайных ситуаций, должны распределять обязанности и определять, как они могут надлежащим образом применять данный стандарт.

KS X 7501:2010 (подтверждён в 2015 году) «Хранилища электронных документов доверенной третьей стороны» (само название на английском языке: Trustworthy third party repositories for electronic records), см.https://www.kssn.net/search/stddetail.do?itemNo=K001010108789

Как отмечается в аннотации, настоящий стандарт содержит все необходимые рекомендации для организаций, оказывающих услуги

электронного хранилища доверенной третьей стороны (в дальнейшем именуемыми TTPR), по надёжному управлению доверенными им электронными документами.

Для того чтобы надёжно управлять электронными хранилищами, должны быть выполнены все требования к управлению электронными документами, в том числе в отношении разработки политик, стандартов и технологий для стабильного управления в долгосрочной перспективе.

Таким образом, настоящий стандарт охватывает не только функциональные требования к системам в части защищённого управления электронными документами, но и требования в отношении менеджмента цифровых объектов и всестороннего развития технологий.

Италия

Новый проект стандарта UNI, пока ещё без номера, «Информация и документация – Управление документами – Словарь» (Informazione e documentazione – Gestione documentale – Vocabolario).

Планируется разработать национальный итальянский терминологический стандарт для области управления документами, в котором будут изжиты все серьёзные несоответствия и ошибки (!), характерные для международного стандарта ISO 30300.

Звучит это очень интригующе, и мне будет очень интересно посмотреть на конечный результат – прежде всего на то, как и какие определения будут отличаться от определений, предлагаемых в стандартах ИСО.

Стандарт UNI 11386:2010 «Поддержка интероперабельности при обеспечении сохранности и извлечении электронных объектов» (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO), английское самоназвание: Supporting Interoperability in Preservation and Retrieval of Digital Objects), см. http://store.uni.com/catalogo/index.php/uni-11386-2010.html

Настоящий стандарт определяет структуру набора данных, поддерживающего процесс замещающего сканирования (*в оригинале: conservazione sostitutiva – замещающее сохранение*). В частности, он уточняет и интегрирует ряд положений, содержащихся в техническом регламенте хранения электронных документов, введённого решением №11/2004 от 19 февраля 2004 года Национального центра по информатике в государственных и муниципальных органах (Centro Nazionale per Informatica nella Pubblica Amministrazione, CNIPA) – см. https://www.agid.gov.it/sites/default/files/repository_files/circolari/deliberazione-cnipa-19-02-04_0.pdf, определяющих информационные элементы, необходимые для создания «индекса хранения» (indice di conservazione - так называемого «закрывающего файла», file di chiusura) и описывающих как семантику, так и структуру с помощью формального языка XML.

Цель стандарта заключается в том, чтобы дать заинтересованным сторонам возможность использовать общую структуру данных для

обеспечения удовлетворительной степени интероперабельности в процессах миграции, благодаря применению специально разработанной XML-схемы.

Стандарт UNI 11536:2014 «Квалификации специалистов в области обработки данных и документов – Профессиональный профиль архивиста – Требования к знаниям, навыкам и компетенциям» (Qualificazione delle professioni per il trattamento di dati e documenti – Figura professionale dell'archivista – Requisiti di conoscenza, abilità e competenza, самоназвание на английском языке: Qualifying professions focused on processing data and documents – Professional archivist's profile – Defining requirements on knowledge, skills and competences), см. http://store.uni.com/catalogo/index.php/uni-11536-2014.html

Настоящий стандарт определяет требования к знаниям, навыкам и технико-культурным компетенциям, необходимым для выполнения профессиональной деятельности архивиста в соответствии с Европейской системой квалификаций (European Qualifications Framework, EQF). При этом специалисты по управлению документами и архивисты считаются представителями одной профессии.

До этого стандарта мне очень хотелось бы добраться – и сопоставить его с профессиональными и учебными стандартами для архивистов, которые разрабатывают в нашей стране).

Интересную статью (на английском языке) известного итальянского специалиста в области управления документами и архивного дела Джованни Мичетти (Giovanni Michetti), сопоставляющую данный стандарт с Европейской системой квалификаций, можно найти по адресу: http://www.ica-sae.org/proceedings/beijing2013/Michetti.pdf . Статья, опубликованная в 2014 году, называется «Знания, навыки и компетенции: Итальянский стандарт должен определить профиль архивиста в соответствии с Европейской системой квалификаций (Knowledge, skills, and competences: An Italian standard to define the archivist's profile within the European Qualifications Framework).

По словам Мичетти, стандарт представляет собой иерархическую схему. На первом уровне выделены три основные миссии архивиста, в рамках каждой из которых указаны основные функции:

Миссия: Управление документами на протяжении всего их жизненного цикла, начиная от проектирования, создания и упорядочивания до стадии длительного или постоянного хранения. Функции:

1. Управление документами
2. Обеспечение защиты
3. Экспертиза ценности и уничтожение/передача на архивное хранение
4. Упорядочение и описание
5. Обеспечение долговременной сохранности
6. Проектирование и экспертиза ценности информационных систем и приложений

Миссия: Предоставление доступа к документам, внедрение и оказание услуг/сервисов для пользователей, продвижение знаний об архивных ресурсах поощрение обучения и образования. Функции:

7. Услуги для пользователей

8. Информационно-пропагандистская деятельность, обучение и образование

9. Исследования

Миссия: Менеджмент и оперативное оказание архивно-документационных услуг, планирование их развития и стратегическое управление соответствующими ресурсами. Функции

10. Стратегическое управление и администрирование

В список вошли все функции, имеющие непосредственное отношение к профессии архивиста. Для каждой функции стандарт даёт краткое описание. В стандарте отмечается, что каждый отдельный архивист не обязан выполнять абсолютно все эти функции, и уже тем более ежедневно; и что приветствуется специализация в отдельных областях.

Для функций, в свою очередь, названы соответствующие виды деятельности, от двух до шести.

Далее, стандарт предлагает таблицы, показывающие взаимосвязь компетенций, навыков и знаний для каждого из видов деятельности. В статье приведены примеры таких таблиц.

СЕРТИФИКАТ И КЛЮЧИ УСИЛЕННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ МОЖНО ПОЛУЧИТЬ БЕЗ ВЕДОМА ВЛАДЕЛЬЦА

Источник: Сайт РЕН ТВ / сайт НТВ / сайт Москва 24

Автор: Наташа Храмцовская

В последние дни в российской прессе активно обсуждается новость, вышедшая под громкими заголовками. Вот только некоторые из них:

- «Новый вид мошенничества: Как москвич «подарил» квартиру уфимцу», https://gtrk.tv/novosti/133909-novyy-vid-moshennichestva-kak-moskvich-podaril-kvartiru-ufimcu
- «Мошенники украли квартиру в Москве при помощи электронной подписи», https://news.ru/obshestvo/moshenniki-ukraili-kvartiru-v-moskve-pri-pomoshi-elektronnoj-podpisi/
- «В России впервые украли квартиру с помощью электронной подписи», http://www.cnews.ru/news/top/2019-05-17_v_rossii_vpervye_ukrali_kvartiru_s_pomoshchyu_elektronnoj

- «Лишиться квартиры и даже не сразу узнать об этом: афера с электронной подписью или сбой в системе»,https://www.1tv.ru/news/2019-05-16/365234-lishitsya_kvartiry_i_dazhe_ne_srazu_uznat_ob_etom_afera_s_elektronnoy_podpisyu_ili_sboy_v_sisteme
- «Квартиру в центре Москвы украли с помощью электронной подписи. Как это?», https://www.anews.com/p/110591140-kvartiru-v-centre-moskvy-ukrali-s-pomoshhyu-ehlektronnoj-podpisi-kak-ehto/

Суть истории в каждой новости изложена по-своему, но стабильно упоминаются несколько следующих важных моментов:

- Был оформлен договор дарения московской квартиры в простой письменной форме;
- Комплект документов для перерегистрации права собственности был подан в Росреестр в электронном виде и подписан сторонами сделки своими усиленными электронными подписями;
- Участники сделки в настоящее время заявляют, что договор дарения не заключали;
- Участники сделки заявили также, что никаких усиленных электронных подписей у удостоверяющем центре не получали и для подписания документа для подачи в Росреестр не использовали.

Ключевым в данной истории является вопрос о том, в каком удостоверяющем центре были получены усиленные электронные подписи участников сделки с недвижимостью, и кто вместо них их получил.

К сожалению, до сих пор процедура взаимодействия с удостоверяющими центрами при оформлении усиленных электронных подписей предоставляет возможность получить ключевой носитель не лично гражданину, а любому уполномоченному им лицу, который может предъявить простую письменную доверенность. И эту брешь в срочном порядке нужно закрывать, поскольку это не далеко первый и вряд ли последний случай неправомерного использования УКЭП.

За эти дни три телекомпании связались со мной и попросили меня прокомментировать ситуацию. Соответствующие видеофрагменты (в среднем из 20 минут беседы в эфир пошла дай бог одна) можно посмотреть в сети:

- «РЕН ТВ выяснил, кому аферисты «передали» квартиру в Москве с помощью электронной подписи», http://ren.tv/novosti/2019-05-16/ren-tv-vyyasnil-komu-aferisty-peredali-kvartiru-v-moskve-s-pomoshchyu-elektronnoy
- «Цифровые мошенники отнимают квартиру у москвича», https://www.ntv.ru/novosti/2192301/
- «Появилась новая схема мошенничества с квартирами москвичей», https://www.m24.ru/videos/video/20052019/205846

К О М М Е Н Т А Р И И*:*

1. **Анонимный**

Вероятно, получить подпись за другого можно довольно легко почти в любом УЦ - вот здесь журналисты сделали "контрольную закупку", удалось в

одном из самых известных УЦ, в СКБ Контур - http://47news.ru/articles/156549/ o_O

Наталья, может, дело в том, что в ФЗ об ЭП №63 нет чётких требований по проверке документов, как итог наверняка нельзя такому пользователю привлечь УЦ в суде с возмещением ущерба (вы знаете о таких случаях?)? Если бы была законодательная база нормальна, тогда была бы и возможность реальной ответственности УЦ перед заявителями, тогда УЦ бы боясь понести убытки сами следили но-нормальному за своей технологией идентификации (а лучше, если бы за УЦ следила страховая компании , так же боясь понести убытки).

В проекте редакции ФЗ об ЭЦП ничего принципиально в этом плане не изменилось увы https://regulation.gov.ru/projects#npa=79636. В попытке ограничить количество УЦ почему-то не подумали, что при отсутствии правил работы, нарушать будут хоть 5, хоть 10, хоть 100 УЦ.

Что думаете?

Ответы

Наташа Храмцовская

На мой взгляд, эта проблема многоплановая. Для её решения нужен целый комплекс мер: сокращение числа УЦ до разумного минимума, ужесточение правил получения сертификатов на уровне законодательства, увеличение пределов материальной ответственности УЦ, создание централизованного реестра сертификатов и системы оповещения граждан о выдачи сертификатов на их имя, ужесточение наказаний для мошенников и разгильдяев, распространение среди масс минимальных знаний о технологии ЭЦП и о мерах предосторожности и т.д. – но нужно понимать, что 100% безопасности никогда не будет, как её никогда не было и в бумажной среде.

Первостепенная задача, с моей точки зрения, – сделать атаки настолько дорогостоящими, а последствия поимки настолько болезненными, чтобы пропала всякая охота атаковать даже представителей среднего класса. Ну а миллиардеры, думаю, как-нибудь сумеют за себя постоять).

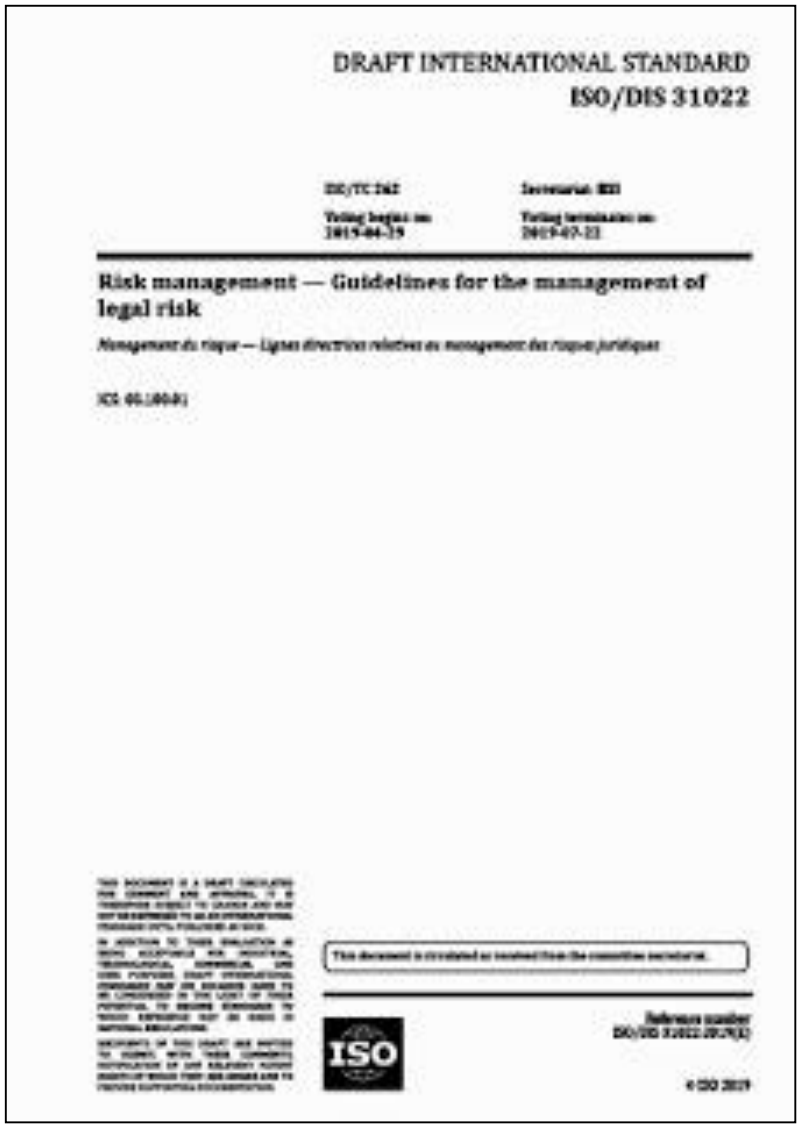
Обязательно будут выявляться новые технические, правовые и организационные уязвимости, и здесь важно наладить систему быстрого реагирования на них. Закрывать дыры в законодательстве нужно столь же быстро, как Windows патчит свою операционную систему.

Нужно также заставить энтузиастов ИТ-технологий поумерить свою прыть во внедрении потенциально опасных технологий, таких, как очень модная идея удалённого подписания документов усиленными подписями на сервере.

ИСО: ЗАВЕРШАЕТСЯ РАБОТА НАД СТАНДАРТОМ ISO 31022, ПОСВЯЩЁННЫМ МЕНЕДЖМЕНТУ ПРАВОВЫХ РИСКОВ

Источник: сайт ИСО
https://www.iso.org/standard/69295.html
https://www.iso.org/obp/ui/#!iso:std:69295:en

Сайт ИСО сообщил о начале 3-месячного публичного обсуждения проекта стандарта **ISO/DIS 31022 «Менеджмент риска – Руководство по менеджменту правовых рисков»** (Risk management - Guidelines for the management of legal risk) объёмом 42 страницы, см. https://www.iso.org/standard/69295.html и https://www.iso.org/obp/ui/#!iso:std:69295:en . Стандарт подготовлен техническим комитетом ТС 262 «Менеджмента риска» (Risk management).



DRAFT INTERNATIONAL STANDARD
ISO/DIS 31022

Risk management — Guidelines for the management of legal risk

Во вводной части документа, в частности, отмечается следующее:

«Организациям приходится действовать в условиях сложной среды, где присутствуют различные правовые риски.

Организации обязаны соблюдать законодательно-нормативные требования во всех странах, в которых они работают, при этом в разных странах эти требования могут различаться, что усиливает необходимость понимания и уверенности в используемых процессам.

Организации должны идти в ногу с изменениями в нормативно-правовой среде и пересматривать свои потребности по мере появления новых видов деятельности и операций.

Организации приходится иметь дело со значительной неопределенностью при принятии решений и выполнении действий, которые могут повлечь существенные правовые последствия. Менеджмент правовых рисков помогает организациям сберечь и повысить свою ценность.

Настоящий документ содержит руководство по действиям, которые необходимо предпринять для того, чтобы помочь владельцам рисков эффективно и экономно оценивать и обрабатывать риски с тем, чтобы соответствовать ожиданиям широкого круга заинтересованных сторон. Невыполнение требований и ожиданий заинтересованных сторон в таких условиях может иметь значительные и немедленные негативные последствия, способные повлиять на показатели и репутацию, и даже привести к уголовному преследованию высшего руководства.

Следует отметить, что понятие правового риска (legal risk) в настоящем документе трактуется достаточно широко и не ограничивается, например, рисками, связанными с исполнением законодательно-нормативных требований и договорными вопросами. Оно их охватывает, но при этом данное понятие преднамеренно определено таким образом, чтобы также охватывать риски, проистекающие или затрагивающие третьи стороны в отсутствие договорных отношений, но когда возможны судебные разбирательства или иные действия, зависящие от договорных требований третьих сторон с соответствующими заинтересованными сторонами.

Настоящий документ:

- Нацелен на поддержку действий, направленных на исполнение законодательно-нормативных требований и на обеспечение необходимой уверенности в выполнении организацией своих обязательств и в достижения своих целей;
- Предназначен для использования организациями любого типа и размера с целью обеспечения более структурированного и последовательного подхода к менеджменту правовых рисков на благо организации и соответствующих заинтересованных сторон во процессах оперативной деятельности. Кроме того, предполагается, что посредством применения данного документа организации могут получить выгоду от улучшения коммерческих и операционных результатов, к числу которых относятся повышение репутации, сокращение текучести кадров, улучшение отношений

с заинтересованными сторонами и большая синергия между ресурсами и способностями;

- Предлагает более систематический и интегрированный управленческий подход к выявлению, прогнозированию и управлению правовыми рисками. Этот подход поддерживает и дополняет существующие подходы, усиливая их посредством предоставления более качественной информации и лучшего понимания потенциальных проблем, с которыми организация может столкнуться;
- Поддерживает все процессы исполнения законодательно-нормативных и иных требований, которые могут иметься в организации, включая, например, систему обеспечения соответствия или систему менеджмента; а также
- Поддерживает деятельность службы комплайнса посредством более широкомасштабного выявления юридических и договорных прав и обязательств организации.

Хотя настоящий документ предназначен для использования в рамках структуры стандартов серии ISO 31000, он также может использоваться как отдельно, так и совместно со стандартами других систем менеджмента.»

Содержание документа следующее:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Принципы
5. Процесс менеджмента правовых рисков
6. Внедрение менеджмента правовых рисков

Приложение А: Пример метода выявления правовых рисков

Приложение В: Пример реестра правовых рисков

Приложение С: Оценка вероятности событий, связанных с правовыми рисками

Приложение D: Оценка последствий событий, связанных с правовыми рисками

Приложение Е: Ключевые положения, которые принять во внимание при анализе контрактов

Библиография

Важнейшие определения следующие:

3.1 Правовой риск (legal risk) - влияние неопределенности на достижение целей, связанное с правовыми, нормативными и договорными вопросами, а также с внедоговорными правами и обязанностями.

Примечание 1: Правовые вопросы могут проистекать из политических решений, национального или международного права, включая законодательство, прецедентное и некодифицированное право,

административные и нормативные акты, судебные и арбитражные решения, процессуальные нормы, протоколы о намерениях и контракты.

Примечание 2: Договорные вопросы связаны с ситуациями, когда организация не выполняет свои договорные обязательства, не может реализовать свои договорные права или заключает договора на условиях, которые являются неоправданно обременительными, неадекватными, несправедливыми и/или неисполнимыми.

Примечание 3: Риски, связанные с недоговорными правами - это риски того, что организация не сможет защитить свои недоговорные права. Примером может служить неспособность организации обеспечить защиту своих прав интеллектуальной собственности, таких, как права, связанные с авторским правом, товарными знаками, патентами, коммерческой тайной и конфиденциальной информацией.

Примечание 4: Риски, вытекающий из недоговорных обязательств, - это риски того, что процесс принятия решений и поведение организации могут привести к незаконному поведению, к невыполнению обязанности проявлять осмотрительность и должную заботу (или неисполнению гражданского долга) перед третьими сторонами. Примером может служить нарушение организацией прав интеллектуальной собственности третьих сторон, несоблюдение требуемых стандартов оказания услуг клиентам (например, введение в заблуждение инвесторов или покупателей), или ненадлежащее использование или управление социальными сетями, следствие которого является иск третьей стороны о клевете или вреде репутации.

3.2 Право (law) - система правил, принципов и практик, посредством которой регион, страна или сообщество регулирует жизнь и деятельность лиц и организаций.

Примечание 1: Право может включать:

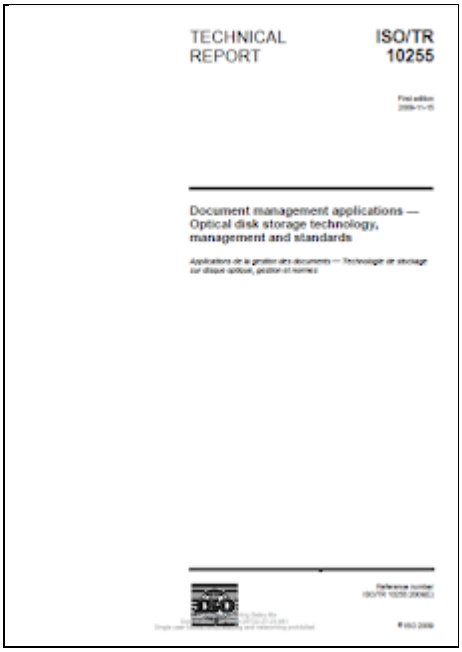
- *законы, нормативные акты, внутренние нормативные акты, постановления и подзаконные акты;*
- *неформализованное и прецедентное право;*
- *обязывающие судебные приказы, решения и постановления;*
- *применимые отраслевые кодексы, политики, в каждом конкретном случае обязательны к исполнению по закону.*

ИСО: ПЕРЕСМОТР РЯДА СТАНДАРТОВ ИСО ПО ВОПРОСАМ УПРАВЛЕНИЯ КОНТЕНТОМ

Источник: сайт ИСО https://www.iso.org/standard/45936.html
https://www.iso.org/obp/ui/#!iso:std:45936:en
https://www.iso.org/standard/42170.html
https://www.iso.org/obp/ui/#!iso:std:42170:en
https://www.iso.org/standard/52072.html
https://www.iso.org/obp/ui/#!iso:std:52072:en

Недавно в профильном техническом подкомитете Международной организации по стандартизации (ИСО) TC171/SC2 начался процесс пересмотра нескольких малоизвестных у нас стандартов, и это даёт повод напомнить об их существовании).

С момента их принятия уже прошло десять лет и кое-какая фактическая информация, естественно, устарела; однако высокоуровневые рекомендации в целом сохраняют свою актуальность.


TECHNICAL REPORT

ISO/TR 10255

Document management applications — Optical disk storage technology, management and standards

ISO/TR 10255:2009 «Приложения для управления контентом – Технология хранения, управление и стандарты оптических дисков» (Document management applications - Optical disk storage technology, management and standards) объёмом 32 страницы, см. https://www.iso.org/standard/45936.html и https://www.iso.org/obp/ui/#!iso:std:45936:en , а также пост https://rusrim.blogspot.com/2009/12/blog-post_03.html

Данный технический отчет содержит рекомендации и советы по вопросам поддержания архивных коллекций оптических дисков. В нем описываются различные сервисы, необходимые для того, чтобы управление

системой, построенной на основе оптических носителей информации, обеспечило успешное внедрение этой технологии.

ISO/TR 10255:2009 также:

- Содержит указания по поддержанию данных, хранящихся в цифровых оптических устройствах, как постоянно подключенных (on-line), так и подключаемых по запросу (near-line) и автономных (off-line);
- Предлагает план действий, обеспечивающий миграцию электронной информации с устаревших и ныне используемых технологий и оптических носителей на новые технологии и носители;
- Описывает непосредственные и долгосрочные последствия, связанные с конечным сроком службы цифровых оптических устройств хранения данных, и предлагает соответствующие рекомендации.

Кроме того, технический отчёт описывает виды оптических носителей информации, включая диски однократной записи (WORM), магнитно-оптические диски (MO), компакт-диски (CD), цифровые универсальные диски (DVD) и более новые технологии.

ISO/TR 12033:2009 «Управление контентом – Управление электронными графическими образами – Руководство по выбору методов сжатия образов документов» (Document management - Electronic imaging - Guidance for the selection of document image compression methods) объёмом 22 страницы, см. https://www.iso.org/standard/42170.html и https://www.iso.org/obp/ui/#!iso:std:42170:en

Технический отчёт ISO/TR 12033:2009 предоставляет информацию, помогающую пользователю и интеграторам решений для управления электронными графическими образами принимать обоснованные решения о выборе методов сжатия для электронных образов деловых документов. Документ содержит рекомендации по анализу конкретного типа документов и определению того, какие методы сжатия наиболее подходят для конкретных типов документов с целью оптимизации их хранения и использования.

Пользователи могут найти в техническом отчёте сведения о методах сжатия изображений, встроенных в аппаратное и/или программное обеспечение, что поможет им при выборе оборудования, в котором такие методы реализованы.

Разработчики оборудования и программного обеспечения найдут в документе предоставляет информацию о планировании.

Технический отчёт ISO/TR 12033:2009 применим лишь в отношении неподвижных растровых изображений. В нём рассматриваются только алгоритмы сжатия, основанные на хорошо проверенных математических разработках.

На данный технический отчёт ссылается наш ГОСТ Р 54471-2011/ISO/TR 15801:2009 «Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности».

ISO/TR 14105:2011 «Управление контентом – Управление изменениями в интересах успешного внедрения системы управления контентом (ECM)» (Document management - Change management for successful electronic document management system (EDMS) implementation) объёмом 24 страницы, см. https://www.iso.org/standard/52072.html и https://www.iso.org/obp/ui/#!iso:std:52072:en ; см. также мой пост https://rusrim.blogspot.com/2013/05/i.html.

Данный технический отчет определяет когнитивные, физические, организационные и человеческие факторы, связанные с критерием удобства использования, применяемым при разработке, выборе и внедрении систем управления электронным контентом (ECM).

В техническом отчете ISO/TR 14105:2011 предлагаются концептуальные рамки для понимания основных вопросов и понятий, связанных с организационным и человеческим факторами, проявляющимися при внедрении ECM-технологий. В нем описаны принципы эргономики и учёта человеческого фактора в связи с критерием удобства использования, применяемым при планировании и внедрении ECM-технологий; в отношении экологических вопросов и проблем внедрения; а также подготовки кадров в интересах повышения производительности в долгосрочной перспективе.

ЗМІСТ