ФЕДЕРАЛЬНОЕ АРХИВНОЕ АГЕНТСТВО

ФЕДЕРАЛЬНОЕ АРХИВНОЕ АГЕНТСТВО

ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ДОКУМЕНТОВЕДЕНИЯ И АРХИВНОГО ДЕЛА

ОТРАСЛЕВОЙ ЦЕНТР НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ

ДОКУМЕНТОВЕДЕНИЕ И АРХИВНОЕ ДЕЛО ЗА РУБЕЖОМ

Информационный сборник

№ 2 (45) / 2018

Москва
2018

ГРНТИ: 13.71.91
УДК 930.22+930.25+651.5

Ответственный редактор
доктор юридических наук *Н. Н. Куняев*

Ответственные за выпуск
кандидат экономических наук *В. Н. Сорокин, Н. Е. Зверева*

Сборник подготовлен сотрудниками сектора зарубежной информации Отраслевого центра научно-технической информации (ОЦНТИ) ВНИИДАД

Документоведение и архивное дело за рубежом: информационное издание: сборник обзоров и рефератов, библиографической информации, переводов на основе печатных и интернет-публикаций. Продолжающееся издание / Всероссийский научно-исследовательский институт документоведения и архивного дела. – М., 2018. № 2 (45). 120 с.

ISSN 2619-1032

СОДЕРЖАНИЕ

I. РЕФЕРАТЫ, ПЕРЕВОДЫ, РЕФЕРАТИВНЫЕ СООБЩЕНИЯ

Литовская Республика: правила управления электронными документами*

I. Общие положения

1. Правила управления электронными документами (далее – Правила) устанавливают общие требования к подготовке электронных документов, управлению ими, организации их учета и хранения, к системам управления электронными документами государственных и муниципальных учреждений, предприятий, организаций и других структур, уполномоченных исполнять публичные административные функции, к лицам, уполномоченным государством (далее – Организации).

2. Для неправительственных организаций и частных юридических лиц требования, устанавливаемые настоящими Правилами, носят рекомендательный характер; однако эти Организации и юридические лица должны создавать электронные документы, подготовка которых регламентирована нормативными актами, в соответствии с процедурой, установленной законами и иными нормативными актами, хранить такие документы в течение необходимого периода времени и обеспечивать аутентичность, надежность и доступность имеющихся у них документов на протяжении всего периода их хранения.

3. Термины, используемые в настоящих Правилах:

архивная электронная подпись – электронная подпись, посредством которой удостоверяется преобразованная копия электронного документа, предназначенного для хранения с применением информационных технологий;

электронный файл – набор электронных документов и связанной с ними информации, структурированный в соответствии с определенными критериями;

---

* Правила управления электронными документами изданы в Литовской Республике и одобрены приказом Главного архивиста Литовской Республики от 29 декабря 2011 г. № V-158 (с учетом изменений, внесенных приказом Главного архивиста Литвы от 2 июля 2012 г. № V-68). Источник: Electronic Document Management Regulations. Интернет-сайт Главного архивиста Литовской Республики (англоязычная версия) – http://www.archyvai.lt/en/new/management.html (дата последнего обращения 12 апреля 2018 г.).

выписка из электронного документа – часть запрашиваемого текста или иных данных, полученных из электронного документа, и равносильная письменному документу;

контент электронного документа – часть электронного документа, в которой информация дается в текстовой, графической или иной форме, не включая метаданные и электронные подписи;

хранилище электронных документов – совокупность технических средств и программного обеспечения для хранения электронных документов, данных относящихся к ним учетных документов и иной связанной с ними информации;

система управления электронными документами – часть системы управления документами предприятия, базирующаяся на информационных технологиях и предназначенная для создания электронных документов и управления ими, включая их учет, хранение и уничтожение;

копия электронного документа – полный текст и другие данные электронного документа, равносильна письменному документу;

преобразованная копия – данные электронного документа, полученные в результате преобразования контента электронного документа и/или метаданных;

электронная подпись, удостоверяющая копии – квалифицированная электронная подпись, посредством которой подтверждается аутентичность копии, резервной копии или извлечения из преобразованной электронной версии документа организации;

квалифицированная электронная подпись – усовершенствованная электронная подпись, созданная при помощи устройства, обеспечивающего ее защиту, и подтвержденная действительным квалифицированным сертификатом;

метаданные – структурные данные, описывающие состав документа, его реквизиты, процесс управления им на протяжении всего периода его существования.

Иные термины, применяемые в Правилах, соответствуют терминам, применяемым в Законе Литовской Республики «О документах и архивах», Законе Литовской Республики «Об электронной подписи», в Правилах подготовки документов, утвержденным приказом Главного архивиста Литовской Республики № V-117 от 4 июля 2011 г., и Правилах учета документов и управления документами, утвержденным приказом Главного архивиста Литовской Республики № V-118 от 4 июля 2011 г.*

* В тексте содержатся ссылки (не приводятся) на официальную публикацию каждого из упомянутых актов. – Прим. переводчика.

II. Организация управления электронными документами

Общие требования к управлению электронными документами

4. Общие положения об управлении документами, доступе к документам и их использовании, утвержденные законами и иными правовыми актами, применяются и в отношении электронных документов.

5. Руководитель организации или иное уполномоченное им лицо (в дальнейшем – руководитель):

5.1. принимает решения, какие информационные технологии должны использоваться в организации для управления электронными документами, создания и обслуживания системы управления электронными документами;

5.2. назначает структурные подразделения или сотрудников, ответственных за администрирование системы управления электронными документами и электронного документооборота, определяет их полномочия и обязанности, способы доступа к электронным документам;

5.3. устанавливает, какие организационные и технические средства должны использоваться для поддержания аутентичности, целостности, надежности электронных документов, их пригодности на протяжении всего периода существования; для передачи с целью их дальнейшего хранения (если в соответствии с порядком, установленным законодательством, документы должны быть переданы для дальнейшего хранения); для соответствующей защиты тех документов, доступ к которым ограничен законодательством;

5.4. принимает решения относительно действий, связанных с хранением электронных документов в Организации;

5.5. обеспечивает проведение мер безопасности в отношении электронных документов и систем управления электронными документами;

5.6. устанавливает, какие электронные документы, связанные с деятельностью Организации, для которых установлен непродолжительный срок хранения и которые не подлежат передаче другим физическим или юридическим лицам, могут быть составлены не в соответствии со спецификациями электронных документов (далее – Спецификации), одобренными Главным архивистом Литовской Республики или согласованными с ним, и подписаны электронной подписью, имеющей юридическую силу, но не являющейся квалифицированной электронной подписью.

6. Подразделение или работник, ответственный за администрирование системы управления электронными документами организации:

6.1. наблюдает за функционированием системы управления электронными документами Организации, выявляет ошибки и недостатки в ее работе и принимает меры к их устранению;

6.2. предписывает системе управления электронными документами те или иные функции или права доступа к документам, изменяет или отменяет их в соответствии с решением, принятым руководителем и касающимся отдельных работников или групп работников;

6.3. осуществляет передачу информации, имеющейся в системе управления электронными документами, в системы, базирующиеся на более совершенных информационных технологиях, для того чтобы сохранить целостность данных;

6.4. вводит в систему, изменяет или отменяет ограничения доступа к электронным документам, электронным файлам или томам файлов в соответствии с нормами законодательства (все изменения фиксируются в метаданных);

6.5. представляет руководителю Организации предложения, связанные с администрированием системы управления электронными документами, а также по другим вопросам ее функционирования.

Общие требования к системам управления электронными документами

7. Руководитель принимает решения, касающиеся функций, выполняемых системой управления электронными документами, с учетом того, какие функции возложены на Организацию, а также требований законодательства и настоящих Правил.

8. Система управления электронными документами должна выполнять следующие функции:

8.1. управлять (создавать, обрабатывать, учитывать, сохранять) электронными документами, которые соответствуют, по меньшей мере, одной Спецификации;

8.2. устанавливать соответствие электронного документа Спецификации;

8.3. в соответствии с процедурой, установленной Правилами создания спецификаций и электронных подписей, создавать и удостоверять электронные подписи, хранить подтверждения их действительности;

8.4. обеспечивать невозможность повторной регистрации одного и того же электронного документа;

8.5. вести поиск на всех уровнях системы управления электронными документами (поля активности, или функции, электронные файлы и их тома, электронные данные, метаданные и др.) и выдавать отчеты о результатах поиска;

8.6. составлять список всех действий, выполняемых в процессе перемещения электронного документа (например, в другую информационную систему);

8.7. препятствовать уничтожению или удалению из системы электронных файлов, томов электронных файлов, привязанных к ним электронных документов, равно как и их метаданных, в случае, если информация об одобрении сертификата удаления документа не введена в метаданные электронного файла или тома файлов.

9. Система управления электронными документами может выполнять и другие функции:

9.1. автоматически заполнять метаданные электронного документа;

9.2. автоматически регистрировать электронные документы;

9.3. автоматически устанавливать или при необходимости изменять установленный период хранения электронного файла, тома файлов или электронного документа;

9.4.автоматически комплектовать электронные файлы и их тома;

9.5. распечатывать контент электронных документов, их метаданные, информацию об электронных подписях и иную информацию, имеющуюся в системе управления электронными документами (результаты поиска электронных документов, отчеты о совершенных действиях по управлению документами и т.д.);

9.6. изготавливать копии, выписки из электронного документа или преобразованные копии, указывая в метаданных название работы, имя и фамилию лица, санкционировавшего изготовление копии, выписки или преобразованной копии, а также дату получения такой санкции и основание для этого;

9.7. передавать электронные документы в соответствии с установленным порядком в государственный архив для хранения;

9.8. передавать учетные данные на электронные документы в государственные архивы;

9.9. составлять отчеты, в которых содержатся данные, подтверждающие удаление электронных документов;

9.10. выполнять иные функции, необходимые для организации.

10. Метаданные электронных документов (файлов) накапливаются в процессе электронного документооборота (Приложения 1 и 2). Метаданные, указанные в Приложении 1 к настоящему документу, используются в той мере, в какой это соответствует требованиям для метаданных, установленным в Спецификациях.

III. Подготовка электронных документов

11. Общие требования к структуре электронного документа устанавливаются в соответствии с описанием требований Спецификации электрон-

ного документа, которая подлежит утверждению приказом Главного архивиста Литовской Республики.

12. Электронные документы, готовящиеся в организации, а также выписки, копии, преобразованные копии должны соответствовать требованиям, установленным в Спецификации. Требования к электронным документам, устанавливаемые в настоящих Правилах, применимы в той мере, в какой они не противоречат требованиям, установленным в Спецификации и других правовых актах.

13. В готовящихся электронных документах форматы контента должны быть такими, какие указаны в Спецификациях.

14. Контент электронного документа должен быть выполнен в соответствии с требованиями, установленными в Правилах подготовки документов, если другими правовыми актами и настоящими Правилами не установлено иное.

Контент электронного документа, равносильного письменного документу, должен быть создан таким образом, чтобы при любом просмотре с помощью информационных технологий постоянно имелась возможность видеть его.

15. Электронный документ должен быть согласован (когда согласование осуществляется с юридическими лицами), утвержден и подписан квалифицированной электронной подписью.

Электронные документы, передаваемые в государственные архивы в соответствии с процедурой, установленной законодательством, должны быть подписаны электронной подписью формата XAdES-X-L или выше, как это предусмотрено положениями Пункта 15.3 Правил передачи электронных документов, образующихся в деятельности государственных и муниципальных органов, предприятий и Организаций в государственные архивы, утвержденных приказом Главного архивиста Литовской Республики № V-63 (далее – Правила передачи)*.

Полный контент электронного документа и другие элементы должны быть подписаны квалифицированной электронной подписью, если другими правовыми актами не будет установлено иное. Если отдельные части электронного документа (например, приложения) должны быть утверждены в соответствии с процедурой, предусмотренной законодательством, и такие документы передаются на хранение в государственный архив, то электронная подпись, подтверждающая акт утверждения, должна быть доведена до формата XAdES-X-L.

В контенте электронного документа реквизит подписи должен быть выполнен без подписи, а реквизиты согласования и утверждения – без подписи и даты.

---

* Official Gazette, 2012, No. 72-3767 – Примеч. пер.

Если должность подписавшего документ лица указана в сертификате электронной подписи, нет необходимости обозначать ее в контенте электронного документа, а грифы утверждения и согласования могут быть исполнены без указания должности, имени и фамилии подписавшего лица.

16. В контенте электронного документа не должны быть сведения об утверждении документа, резолюции, пометки о его просмотре.

Для удостоверения утверждения документа, исполнения резолюции или фиксации просмотра документа Организация может выбрать:

16.1. квалифицированную электронную подпись;

16.2. электронную подпись, имеющую юридическую силу, но не являющуюся квалифицированной электронной подписью (в этом случае должна быть предусмотрена возможность определить лицо, которое исполняло резолюцию, утвердило документ или просматривало его, так же как и возможность сохранить данные об этих действиях).

17. Электронная подпись, удостоверяющая копии, должна применяться для заверения копий, выписок и преобразованных копий электронного документа.

Контент электронного документа должен содержать следующие элементы: специальную пометку (слово «выписка», напечатанное жирным шрифтом), фамилию автора документа, название документа (заголовок), дату создания документа, регистрационный номер, полный текст документа, реквизит подписи (без самой подписи).

Выписка из контента электронного документа должна содержать следующие элементы: специальную пометку (слово «выписка», набранное жирным шрифтом), фамилию автора документа, название документа (заголовок), дату создания документа, регистрационный номер, запрашиваемую часть текста документа, реквизит подписи (без самой подписи).

18. Электронные подписи должны соответствовать требованиям к созданию и подтверждению электронных подписей, установленных Спецификациями и правилами, устанавливающими порядок создания электронных подписей и работы с ними.

Если определенные временны́е метки включены в квалифицированную электронную подпись, они должны соответствовать требованиям, установленным законами или иными правовыми актами.

IV. Регистрация электронных документов, прием полученных электронных документов, управление исходящими электронными документами

19. Электронные документы, исходящие из Организации или полученные ею, должны быть зарегистрированы.

20. Электронные документы должны быть зарегистрированы в реестрах документов Организации согласно перечням реестров документов, утверждаемых руководителем.

21. Электронные документы могут быть зарегистрированы в общем или сводном реестре документов Организации вместе с бумажными документами; при этом должно быть указано, что данный документ является электронным.

С учетом характера деятельности Организации ее руководитель может также создать специальный реестр электронных документов.

Если создается отдельный регистр электронных документов, его идентификационный знак должен быть дополнен буквой «Е», указывающей на специфическую форму регистра (электронного).

22. Электронные документы должны быть зарегистрированы в день, когда они поступили, подписаны или утверждены.

23. При регистрации электронного документа ему присваивается регистрационный номер, состоящий из идентификационной отметки реестра документов и номера, под которым документ значится в данном реестре. Регистрационные данные должны быть уникальными.

В реестре документов регистрируются электронные документы, созданные или полученные в течение календарного года, если законодательством не установлено иное.

24. Электронный документ должен регистрироваться один раз, и присвоенный ему регистрационный номер не может быть изменен.

25. Сведения о регистрации электронного документа, подготовленного в Организации (дата создания и регистрационный номер), должны быть указаны в метаданных.

Если электронный документ зарегистрирован до его подписания, дата регистрации и регистрационный номер могут быть указаны в контенте документа, созданного Организацией.

26. Электронный документ, созданный в Организации, может быть направлен адресату как после процедуры утверждения, так и до нее.

Если в Организации принята процедура утверждения документов в соответствии с пунктом 16.1 настоящих Правил и Организация намеревается отправить адресату документ без прохождения такой процедуры, могут быть изготовлены две копии электронного документа, одна из которых утверждается ответственным лицом, а другая, не проходя процедуры утверждения, подписывается квалифицированной электронной подписью, направляется адресату и хранится в Организации не менее одного года.

Если в организации принята процедура утверждения документов в соответствии с пунктом 16.2 настоящих Правил, действия, связанные с ут-

верждением документа, должны быть зафиксированы в системе управления электронными документами, а электронный документ, подписанный квалифицированной электронной подписью, но без пометок о его одобрении, направляется адресату и сохраняется в Организации в течение установленного периода. Сведения о действиях, связанных с утверждением документа, должны сохраняться в системе управления электронными документами в течение не менее одного года.

27. Полученный электронный документ должен быть зарегистрирован, если он соответствует Спецификации, подписан имеющей силу электронной подписью и есть возможность идентифицировать его контент. Документ, не отвечающий этим требованиям, не регистрируется, о чем уведомляется отправитель, если имеется возможность установить его данные или его связи.

Если документ, не отвечающий требованиям Спецификации, получен от иностранных отправителей, решение о включении его в систему учета и о дальнейших действиях с ним принимает руководитель Организации.

28. Данные о регистрации полученного электронного документа (дата поступления документа в Организацию, регистрационный номер документа, наименование и код Организации, получившей документ) указываются в метаданных. Дата поступления документа в Организацию, регистрационный номер, наименование и код Организации не должны указываться в контенте документа.

V. Создание электронных файлов

Создание электронных файлов

29. Электронные документы, созданные или полученные в Организации и зарегистрированные, должны быть систематизированы в электронных файлах в соответствии с планом ведения документации в Организации.

Электронные файлы должны быть указаны в плане ведения документации в Организации в соответствии с возложенными на нее функциями и с учетом структуры Организации, а также имеющихся разрешений.

30. Все электронные файлы, создание или пополнение которых ожидается в следующем году, должны быть включены в план ведения документации в Организации с указанием ответственных за их подготовку структурных подразделений или исполнителей.

31. Каждому электронному файлу присваивается индекс, состоящий из номера пункта и подпункта плана ведения документации в Организации и пометки «Е», указывающей на то, что файл является электронным. Индекс может быть дополнен данными, указывающими место создания

файла (к примеру, в индексе 1.1-03 Е элемент 1.1 означает номер пункта плана, 03 – структурное подразделение, Е – электронную форму).

32. Электронный файл может быть разделен на тома, которые формируются в соответствии с выбранным признаком систематизации электронных документов (к примеру, формат электронного документа в соответствии со Спецификацией).

33. Если файл разделен на тома, то индекс файла, указанный в плане ведения документации в организации, присваивается каждому тому электронного файла (например, в индексе 1.1 Е1 цифры 1.1 означают номер пункта плана ведения документации в организации, символ Е – электронную форму файла и 1 – номер электронного тома. Указывается также заголовок, который должен соответствовать заголовку файла, и срок хранения. Каждый заголовок электронного файла может быть дополнен подзаголовком с учетом контента электронного документа или иного признака, по которому систематизируются документы.

34. Срок хранения электронных документов устанавливается в соответствии с требованиями, предусмотренными Правилами учета документов и управления документами.

Управление завершенными электронными файлами

35. С электронными файлами, работа с которыми не предполагается в следующем году, должны быть по окончании календарного года выполнены определенные процедуры завершения работы и управления ими.

36. Сотрудники, отвечающие за управление электронными файлами, могут вносить при необходимости поправки в файлы или отдельные тома.

37. Управление электронными файлами осуществляется следующим образом:

37.1. Сроки хранения каждого файла, относящихся к нему томов и документов сверяются в соответствии с планом ведения документации в организации и в соответствии с правовыми актами, которыми такие сроки установлены. Если имеются документы, которые не соответствуют заголовку или подзаголовку (при наличии такового) файла, или срок их хранения иной, чем установлен для данного файла, они перемещаются в соответствующие электронные файлы.

37.2. Принадлежность электронного документа к соответствующему электронному файлу или тому должна быть проверена с учетом установленного или выбранного признака отнесения к данному файлу или тому. При обнаружении ошибок документы должны быть заново отнесены к соответствующему тому или файлу.

38. Электронные файлы, относящиеся к ним тома и отдельные документы, а также их метаданные должны быть защищены от повреждений, возможности незаконного перемещения и удаления.

VI. Экспертиза ценности электронных документов

39. Электронные документы должны оцениваться в соответствии с критериями важности документов, установленными в Правилах управления документами и учета документов и в других документах, связанных с установлением или изменением сроков оценки и хранения документов.

40. Срок хранения электронного документа отсчитывается от окончания года формирования электронного файла. По завершении установленного срока хранения должна быть проведена экспертиза ценности и принято решение о дальнейшем хранении или об уничтожении документа (файла).

41. Электронные файлы, срок хранения которых продлен, учитываются в составляемых и утверждаемых в соответствии с требованиями, установленными Правилами управления документами и учета документов, списках электронных файлов.

42. В отношении электронных документов, отобранных для удаления, составляется сертификат удаления документов, который согласовывается и утверждается в соответствии с Правилами управления документами и учета документов.

43. В Организации должны быть предприняты все меры организационного и технического характера с тем, чтобы все электронные файлы, отобранные для удаления, относящиеся к ним тома, электронные документы и страховые копии были удалены полностью и чтобы была исключена возможность их восстановления с использованием стандартных или специальных средств восстановления.

44. При передаче электронных документов другому держателю и получении подтверждения, что передача осуществлена успешно, электронные файлы, относящиеся к ним тома и электронные документы удаляются таким образом, чтобы исключить возможность их восстановления.

VII. Учет завершенных электронных файлов

45. Предусматривается отдельное описание электронных файлов, которые будут храниться постоянно или в течение длительного времени.

46. Электронные файлы, указанные в пункте 45 настоящих Правил, включаются в лист описания файлов, который составляется в соответствии с требованиями, установленными Правилами управления документами и учета документов, а также утвержденными формами описания файлов.

47. Управление файлами, включенными в лист описания файлов, должно осуществляться в соответствии с процедурой, предусмотренной пунктом 37 настоящих Правил.

48. Записи, относящиеся к описанию электронных файлов, должны рассматриваться, согласовываться и утверждаться в соответствии с требованиями, установленными в Правилах управления документами и учета документов.

VIII. Хранение электронных документов

49. В Организации необходимо обеспечить наличие на протяжении всего периода хранения электронного документа возможности понять контент документа и относящиеся к этому документу метаданные, а также удостоверить квалифицированную электронную подпись.

50. Страховые копии электронных документов и относящихся к ним данных должны создаваться в Организации путем передачи данных с основного носителя на другие носители.

51. С учетом используемых в Организации технологий могут быть приняты другие меры для сохранения электронных документов:

51.1. Обновление носителей – данные носителей, на которых хранятся электронные документы, могут быть переписаны на носители нового поколения;

51.2. Замена упаковки – упаковка электронного документа заменяется без причинения ущерба контенту электронного документа, метаданным или однородности электронной подписи (например, путем создания более поздней версии электронного документа или создания электронного документа, соответствующего другим утвержденным спецификациям);

51.3. Обратимое преобразование – сохранение электронного документа или отдельных составных его частей (контента, метаданных, электронной подписи) и возможность восстановления его до состояния, в котором он находился перед преобразованием (например, сохранение отдельных составных частей электронного документа, не находящегося в упаковке).

52. С целью сохранения контента документов необходимо:

52.1. Периодически просматривать и обновлять список форматов контента электронных документов;

52.2. Постоянно проверять и обновлять, если это необходимо, средства программного обеспечения, при помощи которого и в целях использования электронных документов в поддерживаемых форматах могут:

• отображаться контент электронных документов;

• с применением информационных технологий создаваться копии преобразованного контента электронных документов, которые заверяются электронной подписью, удостоверяющей копии.

53. С целью сохранения свидетельства, подтверждающего действительность электронной подписи Организации, необходимо:

53.1. Накапливать и сохранять данные об одобрении сертификата подлинности подписи лица, создающего ее (например, путем создания электронной подписи в формате XAdES-X-L);

53.2. Осуществлять мониторинг электронных подписей и накопленных данных проверки с учетом ограниченного срока действия сертификата, возможной дискредитации сертификата, уменьшения действенности используемых криптографических методов в процессе смены технологий; при необходимости следует осуществить управление рисками (например, включить в электронную подпись архивную метку времени и создать электронную подпись в формате XAdES-A).

54. Требования, изложенные в пункте 53 настоящих Правил, не применяются в отношении документов, указанных в пункте 5.6. Правил. В этом случае руководитель организации сам выбирает и определяет организационно-технические средства подписания таких документов.

55. С целью обеспечения контроля за сохранностью и целостностью электронных документов Организация должна:

55.1. задействовать средства, обеспечивающие сохранность электронных документов и сохранение их учетных данных; устанавливать соответствующие процедуры;

55.2. использовать средства записи формата хранения электронных документов и процедуры контроля;

55.3. использовать средства фиксации ошибок в средах и системах хранения электронных документов и установить порядок устранения этих ошибок;

55.4. вводить в средства записи информации данные о передвижении (о перемещении на хранение) электронных файлов, входящих в них томов и относящихся к ним электронных документов, а также о процедурах контроля;

55.5. устанавливать средства и определять процедуры создания страховых копий электронных документов и их учетных данных; средства контроля и восстановления из страховых копий;

55.6. предусматривать заранее средства управления рисками, связанными с хранением тех электронных документов, которые хранятся постоянно или в течение длительного времени, имея в виду, что программное обеспечение и технические средства для хранения электронных документов со временем устаревают.

56. Устройства носителей информации электронных документов должны проверяться не реже одного раза в два года. Результаты проверки должны быть зафиксированы в сертификате, в который записывается информация о ситуации в момент проверки, о выявленных ошибках и о мерах, которые следует принять для их устранения.

IX. Заключительные положения

57. Электронные документы должны храниться в Организации на протяжении установленного периода или же передаваться для дальнейшего хранения в соответствии с процедурами, установленными правовыми актами.

58. Электронные документы передаются для дальнейшего хранения в государственные архивы с соблюдением требований, установленных Правилами передачи. Электронные документы передаются в другие организации для дальнейшего хранения и использования в соответствии с процедурой, устанавливаемой иными правовыми актами.

Приложение 1
к Правилам управления
электронными документами

Обязательные метаданные

I. Метаданные электронного документа
1.1. Автор документа (например, наименование юридического лица, имя и фамилия лица, уполномоченного государством)
1.2. Код автора документа (юридического лица)
1.3. Адрес (например, наименование юридического лица, имя и фамилия физического лица) (если электронный документ предполагается куда-либо послать)
1.4. Название документа (заголовок)
1.5. Дата регистрации документа
1.6. Регистрационный номер документа
1.7. Название организации, получившей документ
1.8. Код организации, получившей документ
1.9. Дата получения документа
1.10. Входящий регистрационный номер документа
1.11. Индекс электронного файла, к которому был приписан документ
1.12. Идентификационная отметка спецификации электронного документа
Метаданные электронной подписи
1.13. Имя и фамилия лица, создавшего подпись
1.14. Должность лица, создавшего подпись (представителя юридического лица)
1.15. Дата создания подписи
1.16. Назначение подписи (например, подписание, заверение, согласование, утверждение)
1.17. Идентификационный номер или контрольная сигнатура
II. Метаданные электронного файла
2.1. Индекс функции или области деятельности Организации
2.2. Наименование функции или области деятельности Организации
2.3. Наименование Организации или структурного подразделения, создавшего файл
2.4. Индекс файла или тома

Окончание таблицы

2.5. Заголовок и подзаголовок (если имеется) файла и тома
2.6. Период хранения файла, тома
2.7. Хронологические рамки или дата создания файла, тома
2.8. Номер относящегося к файлу тома
2.9. Информация о подтверждении удаления электронного документа
III. Другие метаданные, относящиеся к управлению электронными документами и использованию электронных документов (файлов)
Метаданные, относящиеся к процедурам создания электронного документа и его подписания*
3.1. Должность, имя и фамилия лица, утвердившего документ, дата утверждения (если документ утвержден электронной подписью, имеющей юридическую силу, но не являющейся квалифицированной электронной подписью)
3.2. Имя и фамилия лица, утвердившего документ**, дата утверждения (если документ утвержден электронной подписью, имеющей юридическую силу, но не являющейся квалифицированной электронной подписью)
3.3. Должность, имя и фамилия лица, подписавшего документ, дата подписания (если документ подписан электронной подписью, имеющей юридическую силу, но не являющейся квалифицированной электронной подписью)
Метаданные, относящиеся к управлению электронными документами
3.4. Имя и фамилия лица, просматривавшего документ, дата просмотра
3.5. Имя и фамилия лица, написавшего резолюцию; дата написания резолюции
3.6. Текст резолюции: имя и фамилия лица или наименование структурного подразделения, которое должно выполнить поручение; содержание поручения; срок исполнения (если необходимо)
3.7. Информация об изменениях, внесенных в электронный документ или в электронный файл (например, содержание изменений, основание для их внесения; лицо, внесшее изменения и т.д.)
3.8. Информация об ограничении доступа к электронному документу, электронному файлу и (или) их метаданным
3.9. Информация об изменениях в ограничении доступа к электронному документу, электронному файлу и (или) их метаданным
Метаданные, связанные с хранением электронных документов (файлов)
3.10. Информация о страховых копиях электронного документа (их число, формат, носители, место хранения и т.д.)
3.11. Информация об изменении электронного документа или его восстановлении из страховой копии
IV. Технические метаданные электронного документа (файла)
4.1. Форматы контента электронного документа
4.2. Информация о риске, связанном с имеющейся электронной подписью (например, срок действия сертификата подтверждения электронной подписи)

* Метаданные должны быть внесены в систему управления электронными документами.

** Если утверждение осуществляется в соответствии с процедурой, установленной правовыми актами.

Приложение 2
к Правилам управления
электронными документами

Примеры метаданных, не являющихся обязательными

I. Метаданные электронного документа
1.1. Код лица, создавшего документ (физическое лицо)
1.2. Адрес лица, создавшего документ
1.3. Код адресата (если адресат является юридическим лицом)
1.4. Вид документа (приказ, письмо или что-либо иное)
1.5. Дата, время и место создания документа
1.6. Автор документа
1.7. Время регистрации документа
1.8. Сведения о поступившем электронном документе (дата и регистрационный номер электронного документа, на который должен быть подготовлен ответ)
1.9. Информация о приложениях к документу (их число, названия и т.д.)
1.10. Отправитель (наименование юридического лица, имя и фамилия физического лица)
1.11. Код отправителя
1.12. Метаданные, относящиеся к кодированию документа
1.13. Идентификационный номер копии документа
Метаданные электронной подписи
1.14. Комментарии лица, создавшего подпись
II. Метаданные электронного файла
2.1. Дата завершения формирования файла (тома)
2.2. Информация о продлении срока хранения файла
III. Другие метаданные, относящиеся к управлению электронными документами и использованию электронных документов (файлов)
3.1. Информация об отправке документа (название организации-отправителя, имя и фамилия лица, отправившего документ, адрес отправителя, дата отправки и т.д.)
3.2. Сведения о поиске электронного документа или файла в системе управления электронными документами
3.3. Информация о копии документа, преобразованной копии или выписке, предназначенной для просмотра и использования (дата создания копии, преобразованной копии или выписки, причины создания и т.д.)
3.4. Сведения об изменении сроков выполнения задания (задачи), изменении контрольных отметок
3.5. Хранилище, в котором хранится электронный документ или электронный файл
3.6. Должность лица, просматривавшего документ
3.7. Должность, имя и фамилия лица, заверившего преобразованную копию, копию документа, выписку из документа; основания для их приготовления
3.8. Даты и основания перемещения электронных документов или электронных файлов (например, в другие информационные системы)

Окончание таблицы

3.9. Информация об удалении электронного документа или электронного файла (в частности, дата, основания)
3.10. Сотрудники, отвечающие за управление документами, учет, хранение, удаление, отправку и прием документов (файлов)
IV. Технические метаданные электронного документа (файла)
4.1. Формат электронного файла
4.2. Название программного обеспечения, с использованием которого электронный файл (документ) был создан и (или) сохранен (например, название системы управления электронными документами, версия)
4.3. Название и версия операционной системы, в которой был создан электронный документ
4.4. Название аппаратуры, с использованием которой сохраняется электронный файл или документ

Реферативный перевод В.И. Глотовой

Инициатива по модернизации управления электронными документами в федеральных органах власти США*

Вводные замечания

Инициатива по модернизации управления электронными документами в федеральных органах власти (Federal Electronic Records Modernization Initiative, FERMI) является частью программы Национальных архивов и Управления документации США (NARA) по разработке всеобъемлющей правительственной стратегии по приобретению решений и услуг для управления документами. Две основные цели FERMI:

• оказывать помощь федеральным органам исполнительной власти (агентствам) с приобретением соответствующих их потребностям решений и услуг для управления электронными документами путем совершенствования процесса закупок;

• заблаговременно принимать во внимание меняющиеся тенденции в управлении электронными документами путем формирования политики для новых решений и услуг.

С целью оказания помощи федеральным органам исполнительной власти (агентствам) в достижении этих целей, Национальные архивы США

* Источник: NARA Federal Electronic Records Modernization Initiative (FERMI). Use Cases for Electronic Messages. [Digital resourse]. – URL: https://recordsexpress.files.wordpress.com/2018/01/nara-fermi-electronic-messages-use-cases-1-25-2018.docx

разработали «Универсальные требования к управлению электронными документами» (Universal Electronic Records Management Requirements, UERM*), представляющие собой упрощенный набор высокоуровневых программных и функциональных требований для управления электронными документами во всех федеральных органах исполнительной власти. Национальные Архивы (NARA) сотрудничали с Управлением общих служб правительства США (U.S. General Services Administration, GSA**) для обновления 36-го Перечня (GSA Schedule 36***). Это привело к изменению механизмов осуществления закупок, связанных с управлением документами на традиционных носителях (SIN 51 504) и управлением электронными документами (SIN 51 600), которые были опубликованы в начале 2018 финансового года. Кроме того, NARA координирует работу с Управлением менеджмента объединенных общих служб (Unified Shared Services Management, USSM****) для создания Службы управления электронными документами (ERM), которая будет осуществлять надзор за потенциальными ERM-решениями и совместно используемыми сервисами.

Агентства могут использовать ресурсы FERMI для соблюдения политик и правил, установленных Национальными архивами и Административно-Бюджетным управлением США (Office of Management and Budget, OMB*****). Данные ресурсы помогут агентствам достичь большей согласованности, надежности и эффективности управления электронными документами.

Потенциальные ERM-решения и сервисы

FERMI сосредоточена на улучшении способности агентств приобретать и внедрять ERM-решения и услуги. Универсальные требования ERM, Федеральная интегрированная бизнес-платформа ERM (ERM-FIBF) и варианты использования (use cases) не предназначены для ограничения поставщиков или агентств в отношении типов решений и услуг, которые они приобретают. Тем не менее, ресурсы FERMI служат отправной точкой для агентств, которые адаптируются в соответствии с конкретными потребно-

* Universal Electronic Records Management (ERM) Requirements / National Archives [Digital resourse]. – URL: https://www.archives.gov/records-mgmt/policy/universalermrequirements

** U.S. General Services Administration [Digital resourse]. – URL: https://www.gsa.gov/

*** Schedule 36 | The Office, Imaging & Document Solution / U.S. General Services Administration [Digital resourse]. – URL: https://www.gsa.gov/acquisition/purchasing-programs/gsa-schedules/list-of-gsa-schedules/schedule-36the-office-imaging-document-solution/

**** Unified Shared Services Management [Digital resourse]. – URL: https://www.ussm.gov/

***** Office of Management and Budget / The White House [Digital resourse]. – URL: https://www.whitehouse.gov/omb/

стями бизнеса. Существуют несколько вариантов агентств и поставщиков, использующих ERM-решения и сервисы для внедрения (которыми при этом они не ограничиваются):

1. *Традиционные системы управления электронными документами (СЭД – ERMS)*. В данной модели каждое агентство имеет собственную автономную систему ERM или решение. Агентство закупает решение или услугу, предназначенную для управления электронными документами. Такой подход может быть идеальным для малых и средних предприятий с прямой миссией. Например, Генеральный инспектор или агентство по управлению делами;

2. *Принятый Управлением электронными документами как сервис (ERMaaS)*. В данной модели одноранговое решение ERMS реализовано как сервис агентства или поставщика. Затем он может быть передан другим учреждениям. Если это будет организовано агентством, хостинговое агентство будет заниматься управлением данным инструментом, а затраты на реализацию будут переданы агентствам, использующим услугу;

3. *Встроенный ERM*. В данной модели функции управления электронными документами встроены в существующее или внедренное бизнес-приложение, которое является источником документации. Этот параметр обеспечивает документы лучшего качества и усовершенствованный пользовательский интерфейс, и, в данном случае, пользователям не нужно будет изучать, как использовать новую систему управления документами;

4. *Микро-сервисы ERMaaS*. В данной модели функции управления документами реализованы как единый набор общих микро-сервисов, к которым будут подключаться бизнес-приложения для выполнения функций ERM. Данный вариант обеспечивает преимущества встроенной ERM в сочетании с централизацией размещенного решения. В настоящее время это редчайшее решение.

Федеральным органам исполнительной власти (агентствам) следует придерживаться наиболее сообразных для их конкретных обстоятельств подходов. В то время как поощряется автоматизация процессов управления документами для снижения нагрузки на конечных пользователей, NARA не настаивает на применении конкретного, определенного подхода. Приведенные в данном документе примеры использования предназначены для применения к любому подходу, который принимает агентство.

Цель

NARA разрабатывает примеры использования (кейсы) для обеспечения агентств и поставщиков продуктов и услуг примерами процессов управ-

ления электронными документами, т.е. ERM. Агентства сопоставляют основные бизнес-возможности в рабочих процессах и получают инструмент, позволяющий оценить поставщиков на соответствие требуемым возможностям ERM. Описанные рабочие процессы можно использовать в качестве инструмента для сравнения, предлагая различным поставщикам выполнять один и тот же рабочий процесс с целью демонстрации того, как они достигают цели управления электронными документами. Это может быть особенно полезно, если решения не были разработаны специально для управления документами.

После того, как решение или сервис начинают удовлетворять Универсальным требованиям ERM, GSA может включить их в Перечень 36 как доступные для осуществления закупок. Примеры использования составляют основу для всеобъемлющей федеральной стратегии закупок ERM.

Документ «Примеры использования для электронных сообщений» основывается на федеральной интегрированной бизнес-платформе ERM (ERM-FIBF). ERM-FIBF – это инструмент, который идентифицирует ключевые функции, действия и возможности, необходимые агентствам для управления электронными документами.

NARA разработали ERM-FIBF в соответствии со стандартами, установленными Федеральной интегрированной бизнес-платформой USSM (FIBF). Она служит моделью, помогающей федеральному правительству координировать и документировать общие бизнес-потребности, улучшать процессы и производительность труда. С развитием ERM-FIBF NARA надеется обеспечить соответствие требованиям по управлению документами FIBF во всех федеральных службах.

На основе различных бизнес-сценариев данный документ демонстрирует применение ERM-FIBF при управлении электронными сообщениями. Бизнес-сценарии показывают эталонный ход событий. Агентствам необходимо предпринимать конкретные шаги (которые не рассматриваются в данном документе) для управления своими электронными сообщениями, например, осуществление ручного ввода в систему или обращение к новой платформе обмена сообщениями. Кроме того, возможны осуществление дополнительных пусков и остановки для процессов, которые здесь не указаны.

NARA будет продолжать создавать кейсы для иных форм электронных документов, помимо электронных сообщений, например, социальных сетей. Создавая бизнес-сценарии, документирующие основные виды деятельности, материалы, результаты и пересечения с другими федеральными службами, NARA надеется обеспечить для поставщиков услуг наиболее эффективные описания федеральных требований для управления электронными документами.

Область применения

1. *Компоненты FIBF.* Примеры использования (кейсы) для электронных сообщений основаны на ERM-FIBF. ERM-FIBF создает область обслуживания управления электронными документами. Ее компонентами являются функции, действия, возможности и бизнес-сценарии. Функции представляют фазы в жизненном цикле документов. Действия – это процессы внутри каждой функции, которые обеспечивают идентифицируемые результаты. Для достижения идентифицируемых результатов каждая деятельность делится на возможности. Возможности определяют входы, выходы и процессы, необходимые для получения результатов. Они могут быть выполнены вручную или автоматизированы и являются агностическими.

2. *Бизнес-сценарии.* Определяют события управления электронными документами (ERM), возникающие при выполнении бизнес-процесса управления документами. Каждый бизнес-сценарий идентифицируется уникальным номером, связанным с уровнем категории. Сценарии классифицируются следующим образом:

• уровень 1 (L1) – оказывает влияние на большинство федеральных агентств и/или на большой объем транзакций, или стоимость доллара в федеральном правительстве;

• уровень 2 (L2) – оказывает влияние на несколько федеральных агентств и требует некоторой специализированной обработки с точки зрения потребителя услуг или аудитора;

• уровень 3 (L3) – оказывает влияние на несколько федеральных агентств и требует уникальной обработки, но в соответствии с законодательством.

3. *Примеры использования (кейсы) – Use Cases*. В этом документе описываются четыре варианта использования, основанные на жизненном цикле управления документами: «сбор/ввод в систему, хранение и использование, уничтожение, передача». Кейсы определяют бизнес-события, входы и выходы, необходимые для выполнения процессов управления документами. Они основываются на бизнес-сценариях и сгруппированы для создания историй, которые иллюстрируют выполнение бизнес-возможностей.

Примеры использования иллюстрируют жизненный цикл электронных сообщений. Бизнес-актеры – это лица, которые участвуют в каждом бизнес-сценарии. Предположения – это условия, которые существуют или были выполнены до начала кейса. Событие представляет собой строительный блок, формирующий бизнес-сценарий; вход(ы) – это элемент или группа элементов, необходимых для выполнения события; выход(ы) является результатом выполняемого события и обеспечивает возможность перехода к следующему событию в бизнес-сценарии.

Ниже приведен список вариантов использования и связанных с ними бизнес-сценариев для управления электронными сообщениями.

ERM.010. Ввод электронного сообщения в систему;

ERM.010.L1.01. Определить, соответствует ли электронное сообщение критериям документа;

ERM.010.L1.02. Определить, можно ли разместить электронное сообщение под контроль управления документами;

ERM.010.L1.03. Убедиться, что электронное сообщение обладает характеристиками документа: надежностью, подлинностью, целостностью и удобством использования;

ERM.010.L1.04. Определить, к какому перечню относится электронное сообщение;

ERM.010.L3.01. Ввести в систему электронные сообщения, отправленные или полученные с личных аккаунтов в течение двадцати дней;

ERM.020. Хранение и использование электронных сообщений;

ERM.020.L1.01. Определить подходящий уровень доступа для электронного сообщения;

ERM.020.L1.02. Изменить уровень доступа электронного сообщения;

ERM.020.L1.03. Проверить журнал аудита для получения информации о внесенных в контент изменениях, метаданных или уровне доступа к документам;

ERM.020.L1.04. Проанализировать документы для определения сроков хранения, основываясь на деловой значимости;

ERM.020.L1.05. Получить подтверждение срока хранения документов;

ERM.020.L1.06. Сохранить документы электронных сообщений;

ERM.020.L1.07. Определить документы, необходимые для удовлетворения информационного запроса;

ERM.020.L1.08. Экспорт документов из старой системы для миграции;

ERM.020.L2.01. Перевести документы в приемлемые форматы для обеспечения защиты от технологического устаревания;

ERM.030 – Уничтожить/удалить электронное сообщение;

ERM.030.L1.01. Уведомить руководство об отобранных для удаления документах;

ERM.030.L1.02. Удалить отобранные документы;

ERM.030.L2.01. Изменить срок хранения документов со временным сроком хранения, одобренных для удаления, в установленном порядке, в соответствии с законодательством или бизнес-обоснованием;

ERM.040 – Передача электронных сообщений;

ERM.040.L1.01. Утвердить передачу в NARA документов с постоянным сроком хранения;

ERM.040.L1.02. Подготовить документы для передачи в NARA;

ERM.040.L1.03. Передать права на хранение документов из агентства в NARA;

ERM.040.L2.01. Продлить сроки, в течение которых агентство сохраняет право на хранение документов с постоянными сроками хранения в установленном порядке, в соответствии с законодательством или бизнес-обоснованием.

Примеры использования (кейсы) для электронных сообщений и рабочих процессов (Workflows)

Примеры использования для электронных сообщений и рабочих процессов охватывают процессы высокого уровня и все типы электронных сообщений. Требования к базовому уровню для всех электронных сообщений одинаковы: документы должны регистрироваться и контролироваться. Это позволяет предположить, что различные типы электронных сообщений потребуют разных подходов к управлению. Важно помнить об этом при использовании кейсов для демонстрации удовлетворения всех необходимых требований поставщиками услуг. Например, шаги для ввода в систему и управления текстовыми сообщениями могут отличаться от подхода к электронной почте. Этапы жизненного цикла способны выполняться автоматически, полуавтоматически или вручную. Национальные архивы рекомендуют агентствам переходить на полную автоматизацию. Из-за ограниченных ресурсов и других проблем агентства могут оказаться не в состоянии осуществить этот переход.

При обработке большего контента FIBF область ERM немного отличается. Требования к управлению документами необходимо встроить во все другие сквозные процессы, которые создают документы в остальных областях обслуживания. Например, ввод документов в систему в процессе начисления заработной платы и обеспечение их надлежащего расположения в соответствии с перечнем NARA. NARA продолжит работу с USSM для гарантии того, что ERM-FIBF включается во все другие соответствующие области обслуживания.

Каждый раздел также включает в себя визуализацию рабочих процессов. Они показывают, как поток событий может возникать в каждом бизнес-сценарии. Как было сказано ранее, данные рабочие процессы показывают эталонные бизнес-сценарии. Агентства могут включаться и выходить из процесса, который необходимо устранить или который не отображается в визуализации рабочего процесса. События, составляющие каждый бизнес-сценарий, необязательно выстраиваются в последовательном порядке.

Кроме того, на рабочие процессы будет влиять модель решений и услуг, выбранная и развернутая агентством. Независимо от того, использует ли агентство традиционную систему СЭД, внедрены ли управление документами или микро-сервисы ERMaaS, рабочие процессы необходимо изменить для обеспечения их соответствия различным подходам.

Реферат О.В. Каплиной

О защите данных в Соединенном Королевстве (Англия и Уэльс)*

Джоанн Боун, Крис Бриджес

Вводные замечания

1. Сбор и использование персональных данных в Соединенном Королевстве регулируется Законом о защите данных от 1998 г. (https://www.legislation.gov.uk/ukpga/1998/29/contents), подготовленном на основе Директивы 95/46/ЕС по защите данных.

Регламент (ЕС) 679/2016 по защите физических лиц в отношении обработки и свободного перемещения персональных данных (Общий регламент по защите данных) вступает в силу 25 мая 2018 г. в странах Европейского Союза. Общий регламент по защите данных будет применяться в Соединенном Королевстве, несмотря на решение о выходе из ЕС (Brexit). Подготовленный Законопроект о защите данных, включающий Общий регламент по защите данных в законодательство Соединенного Королевства, сейчас находится на утверждении в Парламенте.

Следующие секторальные законы относятся к сбору и использованию персональных данных в Соединенном Королевстве:

• *Регламент о защите частной жизни и электронных коммуникационных сообщений (Директива ЕС) от 2003 г.* На основе этого Регламента осуществляется Директива 2002/58/ЕС о защите информации о частной жизни в сфере электронных коммуникаций (E-Privacy Directive). В Регламенте содержатся следующие дополнительные обязательства в сфере:

– индустрии электронных коммуникаций;

– электронного маркетинга (например, электронная почта, смс и телефонные звонки).

* Источник: Joanne Bone, Chris Bridges, Irwin Mitchell. Data Protection in the UK (England and Wales): Overview; https://uk.practicallaw.thomsonreuters.com/1-502-1544?transitionType=Default&contextData=(sc.Default)&firstPage=true&

Во время подготовки этого нормативного документа рассматривался проект по Регламенту ЕС о защите информации о частной жизни в сфере электронных коммуникаций, который аннулирует и заменит Директиву о защите информации о частной жизни в сфере электронных коммуникаций. По мнению авторов, Соединенное Королевство одобрит новый нормативно-правовой документ, несмотря на выход из ЕС.

• *Закон о свободе информации от 2000 г. (FOIA).* Этот закон регулирует доступ к информации, осуществляемый органами с государственными функциями.

• *Закон о полномочиях следственных органов от 2016 г.* Этот закон регулирует сферу, затрагивающую такие нарушения, как перехват коммуникаций, вмешательство другого оборудования (взлом), а также комплектование и хранение коммуникационных данных правоохранительными органами.

2. *В Законе о защите данных (DPA)* определены обязательства контроллеров (обработки) данных (т.е. объектов, определяющих цель и способ обработки любых персональных данных). Определения терминов: «персональные данные», «обработанные данные» и «данные в процессе обработки» см. в п. 3 и п. 4

В то время как процессоры данных (т.е. объекты, которые обрабатывают персональные данные от имени контроллера данных в соответствии с их инструкциями) напрямую не подчиняются закону DPA, здесь вступают в силу обязательства по контракту.

Согласно Общему регламенту по защите данных, процессоры данных имеют прямые обязательства в определенных ситуациях.

3. Закон о защите данных (DPA) применяется к персональным данным. Это данные, касающиеся ныне живущего человека (субъекта данных), который идентифицируется по следующим признакам:

• по одним только данным;

• по данным, объединенным с другими данными и доступным посредством контроллера данных (например, данные, которые уже имеются у контроллера данных или доступны ему из определенного источника).

По закону DPA данные включают:

• информацию, хранящуюся в электронном виде;

• информацию, являющуюся частью соответствующей системы регистрации (например, данные, структурированные по принципу свободного доступа к данным, касающимся конкретного лица без необходимости поиска с помощью данных);

• информацию, которая не относятся ни к одной из вышеупомянутых категорий, но является также:

– документом, касающимся здоровья или образования;

– данными, зафиксированными государственным органом.

Особые правила применяются к конфиденциальным персональным данным (см. п. 11).

4. Закон о защите данных регулирует обработку персональных данных. Процесс обработки понимается в законе в широком смысле, охватывая почти каждый закон, связанный с персональными данными. Он включает в себя (но не ограничивается этим) поиск, консультации, передачу, сбор, размещение, хранение или анализ данных.

5. Закон о защите данных (DPA) применяется к следующим контроллерам данных:

• общепризнанным в Соединенном Королевстве, которые обрабатывают данные в контексте соответствующих условий;

• не признанным в Соединенном Королевстве или странах-членах ЕС, но имеющих место для использование оборудования для обработки данных (за исключением транзитных данных).

В Законе DPA под термином «признанный» подразумевается:

• отдельный индивид – обычно житель Соединенного Королевства;

• орган, зарегистрированный в Соединенном Королевстве;

• компании и другие некорпоративные органы, находящиеся на территории Соединенного Королевства по закону этой страны;

• любое другое лицо, которое осуществляет:

– свою деятельность в офисе, отделении или управлении в Соединенном Королевстве;

– регулярную практическую работу в Соединенном Королевстве.

6. Что касается исключений из положений Закона о защите данных, то к ним относятся следующие категории:

• национальная безопасность (раздел 28, DPA);

• правонарушения и налогообложение (раздел 29, DPA);

• здравоохранение, образование и социальная сфера (раздел 30, DPA);

• нормативно-правовая деятельность (раздел 31, DPA);

• журналистика, литература и искусство (раздел 32, DPA);

• научные исследования, история и статистика (раздел 33, DPA);

• ручной ввод данных, осуществляемый государственными органами (раздел 33A, DPA);

• информация, доступная обществу (раздел 34, DPA);

• обнародование данных, требуемых законом или созданных в связи с процессуальными действиями (раздел 35, DPA);

• внутренние цели страны (раздел 36, DPA);

• разные другие исключения (раздел 37/Приложение 7, DPA).

7. В случае обработки персональных данных в электронном виде от контроллера данных потребуется уведомление, которое необходимо пред-

ставить в Управление по информации (Information Commissioner's Office, ICO). Контроллер данных освобождается от обязанности уведомления Комиссариата в следующих случаях:

• при обработке персональных данных только в административных целях, а также для рекламы, маркетинга, связи с общественностью и/или отчетов и регистрации информации;

• при обработке персональных данных для выполнения судебных функций;

• контроллер данных установлен в некоммерческих целях, не с целью получения прибыли (или не использует полученную прибыль для обогащения людей), а только для использования данных для управления и поддержки базы данных, ограничения их распределения до предела необходимости в целях своей деятельности;

• при обработке персональных данных только в целях ведения государственного реестра;

• при обработке персональных данных только для внутренних целей (например, по личным, семейным или домашним причинам, включая сферу развлечений).

Уведомления должны быть представлены в ICO в соответствующей форме ежегодно. Также необходимо фиксировать любые изменения информации в течение года. Отказ от предоставления уведомления является уголовным преступлением.

При подготовке и передаче уведомления в ICO взимается ежегодная плата – 500 британских фунтов стерлингов, если контроллер данных имеет годовой оборот, равный 25,9 млн британских фунтов стерлингов или более; имеет более 249 штатных единиц; если контроллер данных является государственным органом, имеющим более 249 штатных единиц.

Однако с контроллеров данных взимается ежегодная плата в 35 британских фунтов стерлингов при следующих обстоятельствах:

• ни одно из вышеупомянутых условий не применяется;

• контроллер данных работает в благотворительных целях;

• контроллер данных – это небольшая профессиональная программа пенсионного обеспечения;

• контроллер данных существует меньше 1 месяца.

Основные правила и принципы защиты данных. Основные обязательства и требования к обработке

8. Восемь основных принципов лежат в основе обработки персональных данных, согласно Закону DPA, а именно (Приложение 1, DPA):

1) персональные данные должны обрабатываться беспристрастно и в соответствии с Законом и, в частности, не должны подвергаться обработке, если:

• по крайней мере, соблюдается одно из положений Приложения 2 Закона DPA (см. п.10);

• для конфиденциальных персональных данных также соблюдается, по крайней мере, одно из положений Приложения 3 Закона DPA (см. п.11);

2) персональные данные могут быть получены только для одной или нескольких указанных законных целей и не могут быть далее обработаны никаким способом, который несовместим с этой/этими целями;

3) персональные данные должны быть адекватными, обоснованными и соответствовать рамкам указанной цели/целей, для которой они обрабатываются;

4) персональные данные должны быть точными и актуальными;

5) персональные данные, обработанные для любой цели, не должны храниться дольше, чем это необходимо для выполнения этой/этих целей;

6) персональные данные должны обрабатываться в соответствии с правами субъекта данных и с Законом DPA;

7) соответствующие технические и организационные меры должны быть приняты против несанкционированной или незаконной обработки персональных данных и во избежание случайной потери, разрушения или повреждения персональных данных;

8) персональные данные не должны быть переданы стране или на территорию за пределами Европейской экономической зоны (ЕЭЗ), если та страна или территория не гарантируют соответствующий уровень защиты прав и свобод субъектов данных, касающихся обработки персональных данных.

Закон DPA обеспечивает более подробную информацию о предназначении этих принципов во второй части Приложения 1. Управление по информации обеспечивает дальнейшее руководство на своем веб-сайте*.

9. Согласие субъектов данных – это только одно из семи условий, позволяющих законным образом использовать персональные данные (остальные условий см. в п.10). Согласие является обычно не самым значимым условием, обеспечивающим нормативные правила в соответствии с Директивой по защите данных и руководством Комиссариата по защите информации.

Директива по защите данных подразумевает под согласием «желание субъекта данных быть подробно проинформированным для свободного предоставления информации, т.е. своих персональных данных на обработку», а именно:

---

* Information Commissioner's Office [Digital resource]. – URL: https://ico.org.uk

• «Свободно предоставлять информацию» означает, что у субъекта данных есть выбор, давать согласие или нет. Это усложняет выполнение условий при данном согласии, поскольку не должно быть дисбаланса между контроллером данных и субъектом данных. Это мешает принимать решение о согласии при определенных обстоятельствах (например, при трудоустройстве, хотя, в сущности, согласие широко используется по Закону о защите данных (DPA) в контексте трудоустройства).

• «Подробно» означает, что субъекту данных необходимо предоставить обоснованную подробную информацию о том, на что они дают согласие (т.е. какая подразумевается обработка, и с какой целью).

• «Проинформированный» означает, что субъект данных должен понимать, на что он соглашается. Используемый язык должен быть четким и недвусмысленным (например, в терминах и условиях).

• «Подразумевает» означает, что должна быть некая связь между контроллером данных и субъектом данных: отказ от ответа не является согласием, и также отказ от прочтения терминов и условий. По форме это означает, что должно быть следующее:

– определенная сетевая услуга opt-in, когда субъект данных делает отметку на непомеченном блоке;

– предварительно помеченный блок сетевой услуги opt-in («opt-in» – это заявление, которое уведомляет человека о том, какие виды использования будут размещены, и просит его активно согласиться с ними. Обычно есть галочка, которая не должна быть предварительно отмечена). Если человек делает отметку в поле выбора, он дает согласие на использование своих данных или «opt-out» с четкой формулировкой и четким действием (на примере ICO «Предоставляя такую регистрационную форму, вы указываете свое согласие на получение электронных сообщений о маркетинге от нас. Если Вы не желаете получать такие сообщения, сделайте здесь пометку [ ]».

Кроме того, авторы рекомендуют учитывать следующее:

• предполагаемое согласие возможно при определенных ограниченных обстоятельствах, когда ясно из контекста, что человек дает согласие (например, когда единственной целью является заполнение формы для подписания информационного письма, и в данном случае понятно, что согласие дается для получения этого документа);

• в Законе DPA не требуется, чтобы для подачи согласия субъект данных был определенного возраста, в руководстве ICO указано, что субъект данных, возраст которого менее 12 лет, не в состоянии дать согласие, и что любой ребенок в возрасте от 12 лет или старше в состоянии дать согласие только тогда, когда он в достаточно созрел для этого (например, необходимо принять во внимание сложность обработки, ясность информации, данной им, и любой риск, которому может подвергаться ребенок);

• особые правила для подачи согласия применяются в контексте электронного маркетинга (электронная почта, смс-сообщения, телефонные звонки) в соответствии с Директивой о защите информации о частной жизни в сфере электронных коммуникаций (см. п.19);

• согласие в отношении обработки конфиденциальных данных должно быть точным и ясным (это означает, что предварительно помеченные блоки сетевой услуги opt-in или opt-out недостаточны);

• согласно Общему Регламенту по защите данных получение согласия становится более сложной процедурой; прежде всего, оно должно быть недвусмысленным и, по сути, более близким к согласию на получение конфиденциальных данных по текущим правилам.

10. Согласие – это только одно из семи условий для легализации обработки персональных данных. Другие условия изложены в Приложении 2 Закона о защите информации:

• обработка необходима или для выполнения контракта, в котором участвует субъект данных, или для реализации шагов по требованию субъекта данных с целью заключения контракта (договорная необходимость);

• обработка необходима для соответствия любому юридическому обязательству, которое необходимо выполнять контроллеру данных, а не тех обязательств, которые выполняются в соответствии с контрактом;

• обработка необходима для защиты жизненно важных интересов субъекта данных;

• обработка необходима для осуществления правосудия или государственной функции;

• обработка необходима в целях законных интересов по условиям контроллера данных, или третьего лица или сторон, которым предоставляются данные, кроме случаев, когда обработка не гарантирована из-за предвзятого мнения о правах и свободах или законных интересах субъекта данных;

• обработка необходима в целях обеспечения доверия со стороны публики в соответствии с Законом о противодействии терроризму от 2000 г. и Законом о противодействии экстремистской деятельности от 2002 г.

Термин «необходимость», используемый в вышеупомянутых принципах, означает, что обработка не будет необходима при следующих обстоятельствах:

• обработка может быть проведена другими рациональными средствами;

• это просто удобно для контроллера данных;

• это слишком сложная процедура для выполнения.

Законные интересы и договорная необходимость, как правило, самые важные условия для контроллера данных в частном секторе.

Особые правила

11. Когда контроллер данных обрабатывает конфиденциальные персональные данные, легализация использования этих данных должна выполняться на основании условий, применимых к конфиденциальным данным и изложенных в Приложении 3 Закона о защите информации. Эти условия актуальны, когда:

- субъект данных дает свое явное согласие на обработку персональных данных;
- обработка необходима в целях осуществления или выполнения любого права или обязательства, которые по закону должен исполнять контроллер данных;
- обработка необходима для защиты жизненно важных интересов субъекта данных (в случае, когда согласие невозможно получить приемлемым образом) или другого человека (когда согласие этого человека невозможно получить приемлемым образом);
- обработка выполняется некоммерческой организацией и не обнародуется третьим лицам без согласия;
- субъект данных сознательно раскрывает конфиденциальные персональные данные, доступные публике;
- обработка необходима в целях или в связи с процессуальными действиями, для получения юридической консультации или в целях установления, выполнения или защиты законных прав;
- обработка необходима для осуществления правосудия или государственной функции;
- обработка необходима для предотвращения мошенничества;
- обработка необходима с целью обеспечения доверия публики в соответствии с Законом о противодействии терроризму от 2000 г. и Законом о противодействии экстремистской деятельности от 2002 г.;
- обработка осуществляется в медицинских целях и предпринимается медицинским работником или кем-либо, кто выполняет эквивалентную обязанность по сохранению конфиденциальности по отношению к медицинскому работнику.

Конфиденциальные данные включают данные, касающиеся субъекта данных, а именно, его:

- расовой или этнической принадлежности;
- политических мировоззрений;
- религиозных верований (или верований аналогичного характера);
- членства в профсоюзах;
- физического или психического здоровья;
- сексуальной жизни;

• совершения или предполагаемого совершения уголовного преступления;

• слушания против него/ее о совершении уголовного преступления или предполагаемого уголовного преступления, включая рассмотрение этих слушаний или приговора.

Права человека

12. При сборе данных контроллер данных обязан (с ограниченными исключениями) предоставить следующую информацию субъекту данных, независимо от того, были ли эти персональные данные получены непосредственно от субъекта данных или косвенно через третье лицо:

• указание личности контроллера данных;

• является ли контроллер данных представителем для выполнения целей Закона о защите информации, и если это так, указать личность этого представителя.

• цель (и), для которой предназначены данные для обработки;

• любая необходимая информация с учетом определенных обстоятельств, при которых данные обрабатываются или должны быть обработаны, для обеспечения доверия субъекта данных к их обработке.

Вышеупомянутая информация не должна быть предоставлена при следующих обстоятельствах:

• предоставление информации потребует непропорциональных усилий;

• обработка информации необходима для соответствия юридическому обязательству, которое необходимо выполнить контроллеру данных (не включая юридические обязательства в соответствии с контрактом).

13. Права субъекта данных изложены в Части II Закона о защите данных (DPA). Сюда включены следующие права:

Право на доступ к персональным данным (раздел 7, DPA). Субъект данных может запросить следующую информацию в письменной форме от контроллера данных (так называемый «запрос субъекта данных»):

• подтверждение об обработке своих персональных данных от контроллера данных;

• копию своих персональных данных;

• подробные цели, для которых проводится обработка;

• подробности о любых получателях или группах получателей, которым эти персональные данные могут быть представлены;

• источник (и) персональных данных.

Существует множество обстоятельств, при которых контроллер данных не обязан обеспечивать или может задержать предоставление данных (изло-

жено в разделах 7 – 9A Закона DPA). Контроллер данных может взимать до 10 британских фунтов стерлингов в качестве платы за обслуживание и должен в течение 40 дней получить письменный запрос.

Право предотвращения обработки при вероятности нанесения ущерба или причинения вреда (раздел 10, DPA). Нанесение ущерба или причинение вреда как для субъекта данных, так и для другого лица является незаконным и реальным. Запрос должен быть представлен в письменной форме и действует в течение 21 дня.

Право предотвращения обработки в целях персонализированного маркетинга (раздел 11, DPA). Действует в любое время. Запрос необходимо представить в письменной форме в течение соответствующего времени в данных обстоятельствах, что составляет, по предположениям ICO, 28 дней для запросов и электронного маркетинга и 2 месяца – для почтового маркетинга.

Право на неподчинение автоматизированной системе поддержке принятия решения (раздел 12, DPA). Применяется только при автоматизированной системе поддержке принятия решения (т.е. без вмешательства человека), и существенным образом оказывает влияние на субъект данных. Запрос должен действовать в течение 21 дня.

Однако контроллер данных не должен выполнять такой запрос в случае, когда:

• решение или принято в целях заключения (или принимается в ходе) контракта, или разрешено законом;

• решение состоит в предоставлении запроса субъекта данных, или гарантии его готовности к использованию с целью защиты законных интересов субъекта данных.

Право на компенсацию (раздел 13, DPA). Действует, если при нарушении Закона DPA нанесен ущерб или вред. После случая с Апелляционным судом, имевшим место в 2015 г., субъект данных не должен терпеть денежные убытки для предъявления претензий в случае получения вреда или ущерба.

14. Субъекты данных имеют право на предъявление запроса об уничтожении своих персональных данных (раздел 14, DPA). В этом случае субъект данных должен обратиться в суд. Это право применяется только тогда, когда рассматриваемые персональные данные неточные или являются точкой зрения, основанной на неточных персональных данных. В случае с Google Spain SL v Agencia Española de Protección de Datos (C-131/12) суд Европейского Союза признал, что это право распространялось на поисковые интернет-индексы, где основная интернет-страница устарела или потеряла свою значимость даже если ее законно опубликовал подлинный издатель. Контроллеры данных должны учитывать четвертый принцип за-

щиты данных, где сказано, что они должны действовать в соответствии с основным обязательством по обеспечению точности и актуальности персональных данных (см. п. 8).

Требования к безопасности

15. В седьмом принципе защиты данных указывается, что контроллеры данных должны принять «соответствующие технические и организационные меры» против несанкционированной или незаконной обработки персональных данных и против случайной потери или разрушения, или нанесения ущерба персональным данным. Этот принцип является общим.

Управление по информации (ICO) указывает в своем руководстве, что контроллеры данных должны учитывать риски при определении уровня необходимой безопасности. В этой сфере ICO учредил самые большие штрафы.

В определении риска контроллеры данных должны учитывать следующее:

• природу персональных данных;

• вред, который можно причинить при их неправильном использовании или случайной потере или разрушении.

В Законе DPA представлены разъяснения в Ч. II Приложения 1:

Учитывая состояние технического прогресса и затраты на осуществление любых мероприятий, необходимо гарантировать уровень безопасности, который относится:

• к нанесению вреда как результата несанкционированной или незаконной обработки или случайной потери, разрушения, как указано в седьмом принципе;

• к природе данных, которым обеспечивается защита.

Контроллеру данных необходимо предпринять соответствующие шаги с целью обеспечения надежности своих сотрудников, имеющих доступ к персональным данным.

16. В соответствии с Законом DPA не существует никаких обязательств перед Управлением по информации в сфере регистрации нарушений правил безопасности. Уведомление, как правило, рассматривается как фактор смягчения, если дело доходит до судебного взыскания.

В руководстве ICO говорится о том, что серьезные нарушения правил безопасности необходимо регистрировать для ICO и соответствующим субъектам данных, если это в их интересах.

В соответствии с Директивой о защите информации о частной жизни в сфере электронных коммуникаций провайдеры госуслуг в сфере электронных средств связи должны уведомить ICO о нарушениях правил безопасности в течение 24 часов после получения информации об этом.

Обработка третьими лицами

17. Под седьмым принципом о защите данных (безопасность, см. п. 15) при использовании процессора данных контроллеры данных обязаны:

• выбирать процессор данных, обеспечивающий достаточные гарантии относительно технических и организационных мер безопасности, управляющих их обработкой;

• предпринимать разумные шаги с целью гарантии выполнения процессором данных этих мер;

• иметь в наличии письменный договор с любым процессором данных, в соответствии с которым:

– процессор данных выполняет операции согласно инструкциям контроллера данных;

– процессор данных выполняет обязательства, эквивалентные тем, которые выполняет контроллер данных согласно седьмому принципу.

Электронные средства связи

18. Никакого согласия не потребуется, если файлы cookies также:

• используются для выполнения единственной цели или для облегчения передачи информации по сети электронных коммуникаций;

• крайне необходимы для предоставления информационной услуги обществу.

В Директиве о защите информации о частной жизни в сфере электронных коммуникаций требуется согласие контроллеров данных для размещения файлов cookies, а именно:

• субъекту данных предоставляется ясная и исчерпывающая информация о целях их хранения, или доступ к этому файлу;

• субъекту данных дается возможность отказаться от их хранения или доступа.

Второе требование, изложенное выше, предполагает, что «отказа от участия (opt-out)» достаточно, и этот подход одобряется Управлением по информации. В Руководстве ICO указывается, что подразумеваемое согласие является достаточным, когда пользователь предпринимает некоторые действия, на основании которых достигается их согласие (например, продолжение использования веб-сайта и «переход от одной страницы к другой» с пониманием того, что они согласны с размещенными файлами cookies).

Согласие на размещение таких файлов потребуется только первоначально, когда пользователь посещает веб-сайт: как только человек согласился, файлы cookies, как правило, символизируют это согласие.

Контроллеры данных обязаны обеспечить субъектов данных информацией об используемых файлах cookies, включая их вид (например, относятся ли они только к конкретному сетевому соединению или они постоянны), а также цель с ссылкой, визуально демонстрируемой на веб-сайте, как правило, с любой формулировкой согласия.

Электронные средства связи (электронная почта и смс) в письменной форме и автоматизированные телефонные звонки

В Директиве о защите информации о частной жизни в сфере электронных коммуникаций (PECR) указано, что эти виды электронных средств связи могут передаваться только в случаях, когда получатель «уведомил отправителя» о том, что он дает свое согласие (через опцию «opt-in») на получение таких сообщений, передаваемых «в данный момент». В Руководстве ICO поясняется, что:

• под «отправителем» подразумевается только отправитель (а не третье лицо), который может опираться на согласие;

• выражение «в данный момент» означает, что согласие дается только на короткий период времени и истекает после окончания этого периода; если обстоятельства меняются (например, когда получатель отказывается от услуги, предоставляемой отправителем), то согласие более не действительно;

• выражение «такие сообщения» означает, что потребуется отдельное согласие (или в случае гибкой опции «opt-in»), обсуждаемой ниже, отдельный отказ («opt-out») для каждого метода получения электронных сообщений, например, «Я хотел бы получить маркетинговые сообщения о подобных продуктах и услугах через: [ ] электронную почту; [ ] смс; [ ] автоматизированный телефонный звонок».

ICO использует такие выражения для получения согласия в виде опции «opt-in» (это означает, что не должно быть предварительно отмеченных опций «opt-in» и «opt-out»). Однако в Директиве PECR есть ограниченное исключение, известное как «мягкий отказ» или мягкая опция («soft opt-in»), когда:

• организация получила контактную информацию человека в ходе продаж или переговоров относительно продаж (только организация, осуществляющая продажи или ведущая переговоры, может рассчитывать на согласие).

• маркетинг касается подобных продуктов или услуг той организации (означает, что он не может иметь отношение к продукции или услугам третьей стороны).

• получателю предлагают возможность отказаться от такого маркетинга в следующих случаях:

– в то время, когда контактный адрес был уже получен (например, после использования опции отказа);

– в каждом случае, когда организация контактирует с получателем (например, используя отказ от ссылки на подписку в каждом сообщении электронной почты).

Это условие, указанное в PECR, не относится к корпоративным получателям, но действительно для индивидуальных предпринимателей и обычных партнеров (в противовес ограниченному партнерству или партнерству с ограниченной ответственностью, которые имеют свои корпоративные индивидуальные особенности).

Международная передача данных.Передача данных вне юрисдикции

20. По Закону о защите информации (DPA) контроллер данных может свободно передавать персональные данные по всей территории Европейской экономической зоны (EEA) без ограничений. Однако, для передачи персональных данных за пределами EEA контроллер данных обязан:

• выполнять одно из условий в соответствии с Приложением 4 Закона DPA;

• соблюдать режим соответствующих гарантий.

Условиями Приложения 4 являются следующие:

• субъект данных дал свое согласие на передачу данных.

• передача необходима для следующих операций:

– исполнение контракта между контроллером данных и субъектом данных; или

– для осуществления операций по запросу субъекта данных в целях заключения контракта;

• передача данных необходима в связи с важными государственными интересами.

• передача необходима в целях, или в связи с фактическими или предполагаемыми процессуальными действиями для получения юридической консультации или утверждения, исполнения или защиты законных прав.

• передача необходима для защиты жизненных интересов субъекта данных.

• передача является частью персональных данных, включенных в государственный реестр, и любые условия, на основании которых этот реестр доступен для контроля, соблюдаются каждым человеком, которому эти данные могут быть представлены после передачи.

Управление по информации (ICO) может взыскивать штрафы с контроллера данных до 500 000 британских фунтов стерлингов за нарушение Закона о защите информации и/или Директивы PECR в случае, если это нарушение:

• является достаточно серьезным;

• может нанести существенный ущерб, или привести к бедствию;

• является сознательным со стороны контроллера данных, или диспетчер данных должен осознавать, что вероятность нарушения существует, и что, если бы оно произошло, то привело бы к нанесению существенного ущерба или к бедствию.

ICO имеет право взыскивать фиксированный штраф в размере 1000 британских фунтов стерлингов, когда провайдер служб по передаче электронных сообщений не зарегистрировал нарушение правил безопасности в соответствии с законом PECR.

Практика показывает, что за последнее время увеличилось количество штрафов. В период с 15 сентября 2015 г. по 14 сентября 2016 г. Управление по информации ICO выписало 35 уведомлений о денежном штрафе (Monetary Penalty Notice, MPN). За тот же период в 2017 г. было выписано 58 MPN's.

Рекордная сумма штрафа составляет 400 000 британских фунтов стерлингов, которая была взыскана только дважды: против британской компании TalkTalk Group за нарушение правил безопасности, приведшее к потере персональных данных 156 959 клиентов (многие данные содержали банковские реквизиты), и против компании Keurboom Communications Limited за совершение 99,5 млн сорванных звонков.

Уголовные преследования

ICO может осуществлять уголовное преследование в соответствии с Законом DPA по обвинению:

• контроллера данных;

• любого человека, который сознательно или по неосторожности получил персональные данные от контроллера данных (или стал причиной раскрытия таких данных);

• директоров контроллера данных при определенных обстоятельствах.

Уголовные преследования приводят к взысканию неограниченных штрафов, но не к лишению свободы. Тем не менее, правительство имеет право приговорить нарушителя к тюремному заключению сроком до двух лет за незаконное получение или раскрытие персональных данных.

На практике ICO преследует нарушителя по суду гораздо реже, чем взыскивает штрафы. В период с 15 сентября 2015 г. по 14 сентября 2016 г. ICO возбудило 12 судебных дел. В тот же период 2017 г. было возбуждено 19 судебных дел.

Права субъектов данных

Согласно Разделу 13 Закона DPA субъект данных получает компенсацию за нанесение ему ущерба и/или вреда как результат нарушения Закона DPA контроллером данных в отношении их персональных данных. Кроме того, субъекты данных могут добиться исполнения отдельных прав, указанных в Законе DPA, в судах, хотя на практике, прежде всего, они имеют дело с ICO.

Сферы ответственности Управления по информации (ICO)

ICO отвечает за регулирование и соблюдение Закона о защите информации от 1998 г., Директивы ЕС о защите информации о частной жизни в сфере электронных коммуникаций от 2003 г., Закона о свободе информации от 2000 г., Директивы об экологической ответственности в отношении предотвращения и ликвидации вреда окружающей среде от 2004 г., Постановления Европейского парламента и Совета (ЕС) по электронной идентификации и услугах доверия в отношении электронных трансакций на внутреннем рынке (ЕС) 910/2014 и Директивы INSPIRE от 2009 г.

Реферативный перевод Н.Е. Зверевой

От точной копии документа к копии надежной*

Бруно Кудерк, Франция

В статье руководителя одной из рабочих групп Французской ассоциации по стандартизации (Association française de normalisation, AFNOR) обобщен опыт создания надежных цифровых копий бумажных документов в соответствии с национальными стандартами Франции, многие из которых также являются стандартами ISO. Прежде всего, речь идет о принятом в мае 2017 г. стандарте NF Z42-026 «Определения и спецификации услуг по точной оцифровке документов на бумажном носителе и контроль каче-

* Источник: *Couderc B.* De la copie fidèle à la copie fiable // Archimag : stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – mars 2018. № 312. P. 42–43; *Texier B.* Des scanners haut volume pour les grands comptes // Archimag : stratégie & ressources de la mémoire & du savoir). – Paris, décembre 2017 – février 2018. № 311. P. 34–35.

ства таких услуг». Как самое важное в новом стандарте автор отмечает то, что понятие «формально верных» копий шире, чем понятие о верности информации, содержащейся в копии, той информации, которая содержится в оригинале, потому что совпадать должно не только содержание, но и форма двух документов. Критерии соответствия копии оригиналу несложно соблюсти, так как оценка идентичности копий производится на глаз, т.е. при наглядном сравнении исходного документа и копии. Физиологические характеристики глаза как оптического прибора известны, поэтому стандарт NF Z42-026 требует, чтобы «надежная копия» была выполнена с разрешением в 300 dpi и кодировкой цветов при глубине 24 бита.

Создание сканированной цифровой копии исходного документа, имеющей указанные характеристики, это только первый этап. Когда копия создана, становится актуальным вопрос обеспечения ее целостности и неизменности на протяжении всего периода ее хранения. Для решения этой проблемы стандарт NF Z42-026 предлагает следующие пути: хранение электронной копии документа в электронном архиве, соответствующем требованиям стандарта NF Z42-013/ИСО, декрета № 2016-1673 от 5 декабря 2016 г., а также заверка этой копии хеш-кодом, проставление на ней метки времени, заверка ее «квалифицированной» электронной печатью или «квалифицированной» электронной подписью.

Разумеется, рекомендуется оцифровка не всех, а только значимых в работе данного юридического лица документов.

Поскольку критерии оценки результатов оцифровки «на глазок» остаются слишком приблизительными, занимающиеся оцифровкой фирмы, входящие в Национальную федерацию третьих доверенных лиц (First National Trustee Company Limited, FNTC), попросили у Французской ассоциации стандартизации Франции разработать специальную процедуру сертификации соответствия их услуг требованиям стандарта NF 40-026 и соответствующий знак качества NF544, подготовка которых в настоящее время завершается. Особенность сертифицированных процедур состоит в том, что каждый этап работы документируется. Б. Кудерк уточняет, что стандарт NF Z42-026 является нормой организационного, а не технического характера. Например, передача исполнителю оцифровки бумажных документов по описи, разделение их вкладышами и удаление пустых страниц считаются достаточными гарантиями должной организации подлежащего оцифровке фонда. Минимальный состав метаданных для оцифрованных документов зависит только от составленных заказчиком технических условий.

Сертифицированная процедура оцифровки предусматривает:

1) контроль качества изображений непосредственно оператором;

2) контроль готовых файлов с метаданными при возможности распознавать текст контролером качества фирмы-исполнителя;

3) итоговый контроль качества выполнения заказа и его количественных параметров заказчиком.

Большое значение имеет то, что фирма-исполнитель обязуется уничтожить цифровые образы документов после завершения операций по оцифровке. Это особенно важно для работы с медицинскими документами, содержащими персональную информацию, – делами о госпитализации или медицинскими картами пациентов. Исключением из этого правила может стать нередкая на французском рынке ситуация – когда оператор оцифровки предоставляет заказчику также и услугу «электронный архив» как сервис.

Автор приводит четыре типичных примера оцифровки документов согласно требованиям стандарта NF Z42-026:

1) проводимая в заданный период времени («централизованная») оцифровка всего комплекса документов, хранящихся в организации, например, завершенных в делопроизводстве дел;

2) проводимая в заданный период времени («централизованная») оцифровка определенной группы дел, хранящихся в организации, например, в ее архиве или в одном из подразделений;

3) постоянная («централизованная») оцифровка входящего документопотока, например, переписки;

4) по необходимости («нецентрализованная») оцифровка отдельных документов и их групп из входящего документопотока, например, документов, передаваемых клиентами в банк для оформления открытия счетов и проведения сделок.

Три первых типа оцифровки должны использовать сканеры, обрабатывающие большие объемы документов за счет оцифровки до 130 страниц в минуту. Оцифровка «по требованию» может опираться только на сканер, успевающий обрабатывать до 80 страниц в минуту.

Всего двенадцать компаний на французском рынке предлагают сканеры, способные оцифровывать до 150 000 страниц в день. Их стоимость начинается от 4 000 € и может превысить 26 000 €. Приобретающей их фирме нужно очень четко представлять, какую именно обработку документов должна осуществлять данная машина. Эксперты советуют обращать внимание на следующие вопросы:

1) *Требуется ли от сканера распознавать формуляр документа, и является ли формуляр подлежащих оцифровке документов типовым?* Самообучающийся сканер может стоить гораздо дороже, так же, как и регулярная перенастройка достаточно простого сканера; нередко, определенный производитель сканеров специализируется на распознавании формуляров тех или иных видов документов – чеков, счетов-фактур, опросников;

2) *Подлежащие оцифровке документы являются цветными или черно-белыми, и каким будет их цифровое изображение?* Далеко не все марки быстрых сканеров могут оцифровывать в цвете с хорошим разрешением;

3) *Какое разрешение выбирается для изображения, исходя из требований удобства пользования, стоимости хранения и доказательства подлинности?* Практика показала, что разрешение в 250 dpi остается необходимым минимумом;

4) *Какая обработка запланирована для оцифрованных документов: переадресация и размещение в схеме классификации, индексация или извлечение данных?* Часто для работы с входящими документами заказчик нуждается во всех трех операциях, что требует не только определенной отладки и качества работы сканера, но и его совместимости с СЭД, электронным архивом и другим программным обеспечением заказчика;

5) *Какова будет стоимость технического обслуживания сканера?* Особенно если его продавец не является его производителем и нет гарантии, что его фирма просуществует на рынке столько же, сколько сканер будет находиться в рабочем состоянии.

Даже если оцифровка прошла удачно, для держателя документов остается открытым еще один важный вопрос. Декрет № 2016-1673 «О надежности копий и применении статьи 1379 гражданского кодекса» от 5 декабря 2016 г. разрешает после создания «надежной цифровой» копии уничтожить бумажный оригинал, но далеко не все держатели документов идут на такой риск. Б. Кудерк приводит пример сохранения одной фирмой бумажного договора на очень значительную сумму, даже после оцифровки.

Реферат В.Б. Прозоровой

Исследование возможностей предоставления государственных архивных услуг в контексте структурной реформы стимулирования предложения*

Чжу Тиемяу, Китай

Архивы являются не только важной основой хранения архивных материалов, но также служат местом для использования хранимых материалов и предоставления услуг. Расширение перечня оказываемых государствен-

* Источник: *Zhu T.* Research on Public Services Capability Construction of Archives in the Context of Supply-side Reform // 6th Scientific Conference with International Participation «All about people: challenges for science and education». Alma Mater Europaea-ECM. Maribor, 2018. March 9–10. № 3. Pp. 80–87.

ных архивных услуг является основным требованием улучшения функции архивов, а также важным содержанием национального культурного строительства. В настоящее время структурная реформа, основанная на стимулировании предложения, является важным фактором экономического развития. Ее основные принципы также могут быть применены к созданию дополнительных государственных архивных услуг. Отталкиваясь от идеи «структурной реформы стимулирования предложения» («supply-side structural reform»), автор статьи анализирует основные проблемы, существующие в архивной сфере, и рассматривает возможные направления развития и совершенствования государственных услуг в архивном деле. В статье перечислены главные области оказываемых архивами услуг и предложен ряд конкретных мер для расширения государственных архивных услуг.

В ноябре 2015 г. Председатель КНР Си Цзиньпин впервые озвучил «реформу стимулирования предложения» на Центральной конференции по экономической работе. В своем выступлении он отметил: «Умеренно повышая агрегацию спроса, мы приложим все усилия, чтобы усилить структурную реформу стимулирования предложения, чтобы улучшить качество и эффективность системы поставки, чтобы увеличить движущую силу для длительного экономического роста». С тех пор «реформа стимулирования предложения» стала целенаправленно реализовываться в экономической области, и достигла значимого эффекта, получив большое социальное значение. Понятие «реформа стимулирования предложения» является общепринятым сокращением «структурной реформы стимулирования предложения». Начало мероприятий по улучшению качества предложения связывается с началом реализации «реформы стимулирования предложения» и означает:

• структурное регулирование в различных сферах экономики на основе реформы;

• повышение эффективности и адаптируемости структуры предложений к изменениям требований;

• наиболее полное удовлетворение возрастающих потребностей общества.

Данная реформа является эффективной мерой развития в различных сферах экономики, в том числе вполне применима и к архивному делу.

Расширение возможностей предоставления государственных архивных услуг всегда было важной частью организации архивного дела страны и становится еще более актуальным, поскольку в этой сфере формируются общественные потребности в культурном развитии. Государственные услуги

архивов являются отражением спроса и предложения потребностей общества. Условно можно представить, что архивы находятся на стороне предложения, в то время как общество – на стороне спроса. Государственные архивные услуги должны отвечать потребностям общества, обеспечив актуальность и полноту предлагаемых услуг. Поэтому расширение возможностей государственных архивных услуг должно также предусматривать «реформу стимулирования предложения».

В данной статье автором излагается основной принцип «реформы стимулирования предложения» и рассмотрены ключевые факторы, способствующие стимулированию предложения в целях экономического развития. Отмечается, что возможности архивов по предоставлению государственных услуг в настоящее время все еще не достаточно высоки, ограничены и не отвечают потребностям общества. Существующее положение диктует необходимость проведения реформы предлагаемых архивных услуг. Объединяя ключевые факторы «реформы стимулирования предложения» с проблемами, существующими в сфере государственных архивных услуг, автор анализирует основную структуру предоставляемых государственных архивных услуг и рассматривает направления их совершенствования. Эти направления основываются на полезном практическом опыте Администрации государственных архивов КНР, ряда передовых государственных архивов КНР, а также региональных архивов в области предоставления государственных архивных услуг.

Если говорить о структурной реформе стимулирования предложения, то следует отметить, что она является уже давно и широко известной в западных экономических кругах теорией. Ее авторство принадлежит французскому экономисту Жану-Батисту Сею (1767–1832), профессору промышленной экономики, создателю собственной концепции ценности, автору «Трактата», в котором он изложил теорию производственных факторов и сформулировал законы рынка. Он утверждал, что все виды промышленного производства состоят из трех различных, но взаимосвязанных факторов: труда, земли и капитала. Цена каждого фактора определяется ценой на производимый товар, а в конечном счете – соотношением спроса на этот товар и предложением производственного сектора. Особое внимание Ж-Б. Сей уделял предприятиям, которые комбинируют производственные услуги с целью удовлетворения потребительского спроса. При участии данных предприятий осуществляется распределение благ в обществе.

В КНР значение реформы стимулирования предложения достаточно подробно изложено в работе Ван Хэйджуна и Фэн Цяня «Теоретическая

коннотация структурного реформирования стимулирования предложения – на основе анализа модели совокупного спроса и совокупного предложения», вышедшей в 2016 г. Перспективы развития экономики на основе стимулирования предложения нашли отражение также в более поздних работах западных ученых, в частности, экономистов Манделла и Лейвера, и стали теоретическим обоснованием для внедрения принципов экономической политики. Так, например, Администрация М. Тэтчер в Соединенном Королевстве и Администрация Р. Рейгана в Соединенных Штатах Америки применили на практике многие рекомендации при осуществлении экономических преобразований в своих государствах. Это позволило им добиться определенных успехов в реструктуризации экономики и достижении экономического роста.

Как показывает опыт ведущих мировых стран, «реформа стимулирования предложения» способствует активизации различных факторов, стимулирующих развитие экономики. К их числу можно отнести:

• прогрессивные промышленные и управленческие технологии, инновации;

• модернизацию знаний;

• внедрение передовых достижений науки и техники, новых продуктов и услуг;

• улучшение делового климата;

• поддержку производителей новых товаров и услуг, в том числе путем сокращения налогов, расширения доступа к рынку, а также за счет прогрессивного государственного управления.

Следует отметить, что преобразования в экономике Китая на основе использования ряда положений «реформы стимулирования предложения» не являются слепым копированием опыта западных стран. В Китае их осуществляют, исходя из специфики китайской экономики и под государственным контролем. Это является своеобразной защитной мерой, не позволяющей рынку полностью управлять экономическими преобразованиями, руководствуясь только спросом и предложением товаров и услуг. Правительство играет роль регулятора, который гарантирует интересы общества в экономических преобразованиях и обеспечивает устойчивое поступательное развитие экономики страны и повышение уровня благосостояния трудящихся.

В последние годы в различных отраслях экономики Китая проведены и продолжаются осуществляться значительные экономические преобразования. Они проводились также и в архивном деле Китая, в котором постоянно ведется работа по расширению числа оказываемых услуг. Несмотря

на это, как отмечает автор статьи, ряд проблем все еще остается нерешенным и не позволяет полностью удовлетворять интересы и требования потребителей.

Как было отмечено автором ранее, архивы условно можно отнести к стороне организаций, обеспечивающих формирование предложений в сфере услуг, в то время как потребители услуг условно принадлежат к стороне спроса. Общий уровень и эффективность оказываемых услуг остается относительно низким. Только небольшая часть архивов может предоставлять услуги, такие как, например, тематический поиск в режиме онлайн. Стоит отметить, что в последнее время в Китае в ходе выполнения двенадцатого пятилетнего плана достаточно эффективно велась оцифровка архивных фондов. Однако по ряду причин, в числе которых недостаточное количество электронных архивов, незавершенность оцифровки архивного фонда, несовершенное программное обеспечение, а также значительный объем архивных документов, относящихся к категории документов, содержащих государственную тайну, получение услуг в виде предоставления оцифрованного полнотекстового документа в режиме онлайн пока достаточно проблематично.

Кроме того, потребители архивных услуг отмечают такой недостаток, как низкое качество услуг и неудовлетворительный уровень обслуживания. Они связывают эти проблемы с недостаточно высоким уровнем общей организации работы архивов, неполнотой и погрешностями информационных каталогов и путеводителей, небольшими объемами оцифрованных архивных материалов. Это не позволяет полностью удовлетворить запросы потребителей, использующих современные информационные технологии в поиске нужной информации. В этой связи автором отмечается, что многие формы оказания услуг являются морально и технически устаревшими.

В настоящее время основным видом и способом обслуживания архивами потребителей заключается в предоставлении услуг на запросы в форме различных справок, выписок, копий документов и других архивных материалов на бумажной основе, организации выставок и презентаций хранимых документов. Эти устаревшие формы и методы работы не связаны с мультимедийной эрой в информационном обществе и не позволяют достигать желаемых результатов. При этом уровни оказываемых услуг в различных архивах не равнозначны и во многом зависят от их материально-технического, финансового и кадрового обеспечения.

Устранение многих перечисленных недостатков возможно в ходе активно осуществляемой в экономике страны структурной реформы стимулиро-

вания предложения применительно к архивному делу. Автором исследованы и проанализированы основные направления проведения мероприятий по совершенствованию структуры государственных архивных услуг. Условно они сводятся к трем основным аспектам: «эффективный вход, модернизация элементов и инновации работы».

1. *Эффективный вход*. В отличие от большинства обычных предприятий, архивы являются государственными учреждениями, подчиняющимися органам исполнительной власти соответствующего уровня. Эффективный вход, по мнению автора, необходим для обеспечения высокого качества оказываемых архивами услуг и осуществления ими возложенных на них функций. Для качественного исполнения данных работ необходимо наличие четырех основных факторов:

- подходящего места осуществления работ;
- соответствующего штата;
- полноты архивного фонда;
- достаточных финансовых ресурсов.

2. *Модернизация элементов*. Для обеспечения эффективного входа центр структурной реформы стимулирования предложения должен улучшить пропорцию элементов, таких как технология и инновации, чтобы увеличить эффективность и качество поставки. Для архивов, соответственно, следует обратить внимание на улучшение трех аспектов:

- способности управления работой сервисных служб;
- применения передовых технологий;
- качества (компетентности) штата сотрудников.

3. *Инновации работы*. Ключ к реформе стимулирования предложения. Инновации государственных архивных услуг должны включать инновации в области идей, инновации совершенствования обслуживания и инновации продуктов развития.

4. *Стратегии и методы создания государственных архивных услуг в контексте реформы стимулирования предложения*. Основной принцип «реформы стимулирования предложения» состоит в том, что предложение может создавать требование. В настоящее время архивы сталкиваются с двумя проблемами в этой сфере. Их смысл заключается в том, что архив не всегда может удовлетворить некоторые требования общества, но даже после этого он должен уделять внимание использованию созданных ресурсов, чтобы предоставить новые услуги в целях дальнейшей успешной работы. Только таким образом архивы могут стимулировать новые социальные требования, повышать и расширять уровни оказываемых услуг.

Кроме того, необходимо улучшать организацию и совершенствовать управление архивными ресурсами, оптимизируя структуру архивных фондов. Чем крупнее фонды архивов, тем больше вероятность расширения объема и перечня предоставляемых архивных услуг. Таким образом, организация ориентированных на интересы потребителей архивных ресурсов является основанием для расширения перечня оказываемых услуг. В процессе оптимизации структуры архивных фондов представляется целесообразным сосредоточиться на двух аспектах:

1. Создать наиболее полный архивный фонд в указанном объеме и в соответствии с требованиями Администрации государственных архивов КНР и инструктивных материалов для архивов всех уровней.

2. При формировании архивного фонда следует обратить внимание на сбор и подготовку материалов с учетом актуальных и востребованных интересов общества. К числу таких архивных материалов можно отнести:

- типовые управленческие архивные документы;
- документы по личному составу;
- документы учебных и научных учреждений;
- документы служб занятости;
- акты гражданского состояния;
- документы по пенсионному обеспечению, социальному страхованию, здравоохранению, регистрации недвижимости;
- банковские документы.

Эти документы имеют высокий уровень востребованности и играют важную роль в охране прав и интересов людей (производственных и личных), урегулировании споров, обеспечении судебных исков и делопроизводства и т.д.

Некоторые специализированные архивы (исторические, военные, научно-технические, литературные, содержащие фонды знаменитых в стране людей и т.д.) могли бы заинтересовать общество своими уникальными фондами. До некоторой степени это может стать целью стимулирования требования. В целях популяризации этих фондов в последние годы Администрация государственных архивов КНР выпустила два издания ста основных национальных профессиональных информационных каталогов существующих архивных фондов.

В настоящее время в КНР насчитывается более четырех тысяч архивов разных уровней. Из-за ограничений финансового, материально-технического и социального развития, функциональные возможности архивов неравны. В целях устранения подобной дифференциации, следует как можно скорее усилить операционную стандартизацию и способствовать всесторонней

модернизации и унификации основных видов архивной работы. В 2018 г. Администрация государственных архивов КНР начала работу над документом «Оценка операционного строительства архивов всех уровней» и сформулировала основные правила оценки в общей сложности по 96 критериям. В этом документе обследование, описание и анализ архивных фондов являются важными частями оценки. Впоследствии команды экспертов будут направлены в архивы, чтобы проверить их работу и определить объективность оценки. Стандартизация операций поможет архивам выявить существующие проблемы, принять меры по ликвидации недостатков и улучшить стандарты их работы. В то же время это поможет сократить различия между архивами и сделать возможным предоставление потребителям в различных регионах страны унифицированных актуальных архивных услуг.

Для более полного предоставления архивных услуг архивам необходимо также наличие хорошо развитой инфраструктуры, ориентированной на обслуживание различной категории потребителей, в числе которых могут быть пожилые люди, люди с ограниченными возможностями и дети. В последние годы с учетом этих факторов и при финансовой поддержке государства многие региональные архивы открыли свои филиалы (отделения) и улучшили условия обслуживания потребителей услуг.

В процессе осуществления государственных архивных услуг большое значение имеют количество и компетентность штата сотрудников соответствующего архива. Подготовка кадров архивов должна быть организована на регулярной основе. Учебные программы подготовки и переподготовки должны включать основы теории архивного дела, архивных технологий защиты и сохранности документов, знания информатизации архивного дела, сбора, обработки и хранения электронных документов и т.д. С начала 2017 г. Администрации государственных архивов КНР практикуют переподготовку руководящих кадров региональных архивов. Пункт о подготовке и переподготовке кадров архивистов отражен в «Схеме отбора и подготовки национальных архивных экспертов», а также в соответствующем разделе тринадцатого пятилетнего плана.

Применение современных информационных технологий является главной движущей силой для того, чтобы повысить сервисную эффективность архивных организаций. Новые технологии помогут усовершенствовать систему управления фондами архивов и эффективно использовать возможности веб-сайтов в архивном деле. Следует активно использовать информационные технологии, чтобы улучшить систему управления фондами архива, и постепенно решать ряд текущих проблем, в том числе для связи и восстановления данных. Информационные технологии следует шире

использовать при создании электронных архивов, а также при сборе, обработке, хранении и применении оцифрованных архивных материалов. Архивам следует активно присоединяться к национальным исследованиям в области применения информационно-коммуникационных технологий, таким как большие данные и хранение архивных данных в «облаках». В этих целях Администрация государственных архивов КНР выпустила методические материалы «Цифровые архивы – руководство и построение» и «Цифровые системные методы проверки архивов», позволившие шестнадцати государственным архивам пройти соответствующие тесты. Отмечено, что создание цифровых архивов улучшает управление архивным фондом и значительно повышает эффективность оказываемых услуг. Администрация государственных архивов КНР и Архивы Циндао в целях повышения эффективности и точности архивной оценочной работы успешно провели совместное исследование, чтобы проверить новый справочный тезаурус, основанный на технологии анализа данных в открытой системе оценки архивов.

Инновации являются основным стимулом для реализации реформы стимулирования предложения. Необходимо полагаться на инновационную способность для существенного изменения в лучшую сторону существующей ситуации в архивном деле. Целесообразно обращать внимание на инновации не только работы, но также и ее содержания. В целях совершенствования форм и методов работы архивы должны предоставлять услуги, используя удобные и приемлемые решения. Например, некоторые архивы в настоящее время используют популярный социальный «ВиЧат» («WeChat»), представляющий из себя мобильную коммуникационную систему для передачи текстовых и голосовых сообщений, разработанную китайской компанией «Tencent». Данную систему скачали и установили более 900 миллионов пользователей. Первый релиз на основе этой системы был выпущен в январе 2011 г. для размещения в рекламных целях архивной информации и продвижения архивных услуг.

Что касается содержания работы, прежде всего следует предлагать актуальные и востребованные архивные услуги, которыми заинтересуются потенциальные потребители. Причем предлагаемые архивные услуги могут быть неординарными и неожиданными. Так, Шанхайские Архивы и Архивы Сямыня запустили проект «Архивы мечты», рассчитанный на школьников и студентов и помогающий им сохранить их мечты. Школьники и студенты могли заполнить карты мечты, которые будут сохранены архивами в течение десяти лет. Данный проект был с интересом воспринят многочисленными представителями молодого поколения китайских граждан и успешно реализован.

Реферат В.Н. Сорокина

Электронные архивы в эпоху изобилия данных*

Круглый стол

В круглом столе, организованном на салоне «Докумасьон» (Documation) – в 2018 г. журналом «Аршимаг», участвовали эксперты Роже Гименез (Roger Gimenez) из компании «X demat», Оливье Ражман (Olivier Rajman) из компании «Docuware» и Доминик Лопиталь (Dominique Lhopital), генеральный директор «Arcsys softwere». Характерно, что все три приглашенных журналом специалиста являются по образованию инженерами в сфере информационных технологий, а на архивной проблематике они специализировались, участвуя в разработке СЭД и АЭ в своих фирмах. Их взгляд на электронные архивы и программное обеспечение для работы с ними пронизан характерной для частного сектора логикой рентабельности. Приведенные ими факты и оценки тенденций довольно интересны.

На французском рынке, по мнению О. Ражмана, действительно остались практически только крупные игроки. Все эксперты согласились, что французский рынок программного обеспечения для управления архивами и документами – зрелый, стоимость технической компоненты продолжает снижаться – хранение 1 мегаоктета стоит уже 1 евро. О. Ражман подчеркнул, что рынок программного обеспечения для электронных архивов, несмотря на свою зрелость во Франции, не испытывает застоя: «Docuware» последние четыре года приобретает по 120 новых клиентов в мире. Все эксперты согласились с тем, что у их клиентов – крупных и средних фирм сложилось понимание, что все документы не должны обязательно оказываться в СЭД, не говоря уже о гораздо более строгом их отборе для электронного архива. По-прежнему остается вопрос: должны ли юридические лица прибегать к аутсорсингу или создавать внутренние структуры? Этот выбор зависит как от финансовых возможностей организации, так и от

* Источники: *Rajzman O.* DocuWare expose avec ses partenaires et anime une conférence // Blog DocuWare [Digital resource]. – URL: http://fr.blog.docuware.com/docuware-expose-avec-ses-partenaires-et-anime-une-conference; 6 questions à Dominique Lhopital, Directeur général chez Arcsys Software: «La conservation des données est une problèmatique commune à toutes les entreprises // http://www.sollan.com/www/fr/sollan-news-item/6-questions-a-dlhopital-arcsys-software-la-conservation-de-la-donnee-est-une-problematique-commune; Резюме круглого стола на сайте салона «Докумасьон – 2018» [Digital resource]. – URL: http://www.documation.fr/info_event/42/l'archivage-a-l'heure-de-surcharge-de-donnees--enjeux-et-defis.html; Сайт компании Xdemat: http://www.xdemat.fr/cat/evenements/conferences/

методов работы ее партнеров и рисков утечки или непредоставления важной информации.

Доминик Лопиталь из «Arcsys softwere» поделился опытом работы с большими транснациональными структурами, крупными научными учреждениями и Министерством обороны. Эти организации все чаще выкладывают в электронные системы документы в зашифрованном формате, в том числе очень много видеодокументов, как статичных – фотографий и технических чертежей, созданных в программе «Autocad», так и кинодокументов разных форматов. В целом информационные системы работают с 6000 наиболее распространенных форматов, что вполне объяснимо, если учесть, что у одного только формата PDF насчитывается 32 разновидности. При этом для архивного хранения рекомендуется использовать не более 15–20 форматов, в основном, широко распространенных, с открытыми для сообщества пользователей спецификациями. Узким местом довольно многих СЭД является просмотр хранящихся в них документов, например, СЭД может хранить формат видео 3D, а данная программа не может его отрыть.

Д. Лопиталь подчеркнул, что грамотное управление версиями документов в процессе их подготовки и утверждения снимает проблему наличия в системе избыточного количества версий одного документа, если установить правило, что утвержденный, конечный документ должен иметь формат архивного хранения, например, PDF/A. Эксперты сомневаются, что какой-либо формат сможет прожить более двадцати лет, так как для дальнейшего хранения в любом случае придется его конвертировать. Это достаточно тревожные данные для крупных предприятий транспортной, химической и фармацевтической промышленности, так как сроки хранения документов в них значительно превосходят названные двадцать лет. Например, в авиационной промышленности срок хранения технической документации на модель самолета составляет тридцать лет с момента продажи последнего воздушного судна данной модели. В фармацевтике сроки тоже постоянно удлиняются, что отражает увеличение сроков жизни. В госсекторе вообще создается довольно много документов вечного хранения: документы ЗАГС и кадастра, документы о влиянии тех или иных явлений на окружающую среду. Р. Гименез подчеркнул, что, по его наблюдениям, документы сегодня могут очень быстро переходить из статуса «мертвых» архивов в статус «очень часто используемых». Д. Лопиталь уточнил, что по статистике, собранной «Arcsys softwere», «очень частое использование» означает несколько сотен консультаций в секунду для архивных документов предприятий. Это, собственно, статистика текущих и промежуточных архивов фирм, не учитывающая открытые данные предприятий, выложенные на их сайтах.

Эксперты остановились и на изменениях технических характеристик электронных систем хранения и обращения документов. Они подчеркнули, что использование криптографии во Франции поддерживается нормативно – хранение расчетных листов заработной платы предполагает использование электронного репозитария с алгоритмами криптографии. Также все согласились, что внедрение в программное обеспечение требований «Общего регламента о защите данных» (RGPD) оказало несомненную услугу разработчикам и пользователям СЭД и ЭА, так как заставило их максимально прояснить требования к хранению и защите определенной группы документов, содержащих персональную информацию.

Гораздо интереснее был небольшой спор о периметре СЭД и ЭА. Д. Лопиталь поделился наблюдением, которое он сделал на последних проектах, о том, что граница между СЭД и ЭА постепенно стирается, так как на любом этапе жизни утвержденного документа все его характеристики, в частности, неизменность и подлинность, должны быть абсолютно защищены для эффективной работы и защиты прав предприятия. Ему возразил О. Ражман, сказав, что загружать в электронный архив еще документы, еще обращающиеся между сотрудниками учреждения в процессе разработки, исполнения или использования, равносильно превращению этого архива в «мусорную корзину». Их компания рекомендует своим клиентам неукоснительно поддерживать границу между СЭД и ЭА. Все участники круглого стола и их слушатели подтвердили, что в последнее время СЭД сильно страдает от распространения стиля работы «открытое предприятие», когда документы доступны не только сотрудникам фирмы, но и ее клиентам и партнерам (хотя их права и определены линейкой правил доступа).

Часто клиенты даже не знают, какими внутренними информационными ресурсами уже располагает его фирма, и стремятся купить еще одну программу вместо того, чтобы оптимизировать использование существующего программного обеспечения (это общая проблема крупных госкорпораций). Многие юридические лица имеют много «параллельных» вертикальных СЭД, а «сквозная» СЭД часто не приживается из-за различий в методике работы подразделений. Эксперты рекомендовали начинать проект СЭД с тех подразделений, которые в большей степени страдают от ее отсутствия, так как их сотрудники смогут донести выгоды внедрения новых методов работы до других подразделений, которые «подтянутся», а также будут сознательно отстаивать финансирование проекта перед руководством, смогут быть его «послами» на всех необходимых уровнях.

«Урбанизация» архитектуры информационных систем, правильное использование которой может избежать внедрения провальных «сквозных» СЭД, не используемых никем, должна обязательно учитывать эту тенден-

цию «открытых предприятий». Иначе возникнут ситуации, когда клиент, потерпевший ущерб, откажется от системы в принципе, тогда как случаи и параметры ее «открытого» использования можно было предусмотреть в технических условиях и нормально отконфигурировать. Эксперты рекомендовали на этапе технико-экономического обоснования изучать риски как минимум по матрице ССВУ (SWORT) или оставить для этих процессов, исходящих документопотоков в направлении ключевых партнеров с высоким юридическим риском, бумажные документы.

Очень важно обеспечить координацию проектами управления электронными документами на правильном управленческом уровне. Если хранение электронных архивов останется на откуп функциональным подразделениям (в малых фирмах это часто бухгалтерия) или службам информатики, оно сведется к простому складированию данных на серверах, без организации их в системы. При составлении технических условий очень важно сразу указать не только риски, но и объем, случаи и процедуры использования документов и их групп, существующую техническую и функциональную архитектуру.

Миграция остается «ахиллесовой пятой» систем оборота и хранения документов, так как это – точка «разрыва доверия» в жизненном цикле документов. При установке системы необходимо всегда требовать возможности обязательного вывода в исходном виде тех данных, которые загружаются в систему. Нужно, чтобы в СЭД или ЭА было встроено решение для технического осуществления такой обратимости, потому что если фирма, которая продала программное обеспечение с прописанной в договоре услугой «обратимого извлечения» данных, исчезнет, ни один приговор суда не найдет технического решения.

Поэтому нужно требовать включения в систему блоков для обеспечения ее обратимости и совместимости сразу при установке, а не в качестве обещания, выполнимого в конце договора на техническое обслуживание данной системы. Это требование касается и использования облачных технологий. Именно в интересах обеспечения совместимости и обратимости, по мнению экспертов, нужно избегать проприетарных систем и форматов. Если фирма-подрядчик, внедрившая программное обеспечение исчезает, то при проприетарной программе и форматах, фирме-пользователю бывает быстрее и дешевле забросить старую базу данных, чем найти способ перенести ее из старой системы в новую.

Всем желающим внедрить электронные системы управления документами эксперты рекомендовали:

• тщательно изучать как фонды документов, так и имеющиеся у них информационные ресурсы,

• при знакомстве с опытом других учреждений и подразделений запрашивать окупаемость инвестиций в программное обеспечение по отделу, по хронологии (за год и за пять-шесть лет), а также «аналитическую окупаемость» по отдельному документу, сравнительно с его хранением и использованием на бумажном носителе.

Обзор В.Б. Прозоровой

Сложности внедрения «Генерального регламента о защите данных» (RGPD) и 40-летие «Закона об информатике и свободах»*

6 января 2018 г. Франция отмечала сорокалетие принятия «Закона об информатике и свободах», утвержденного 6 января 1978 г., и продолжает готовиться к принятию «Генерального регламента о защите данных» (RGPD), запланированному на май 2018 г.

Сама идея о принятии закона «Об информатике и свободах» возникла в результате дебатов по поводу статьи Ф. Буше «Сафари или охота на Французов», опубликованной в социалистической газете «Монд» 21 марта 1974 г., где рассказывалось о проекте общей базы населения, составленной из отдельных баз центрального аппарата полиции, министерства обороны, юстиции, социальных служб, банков. В ту эпоху базы данных центрального аппарата, охватывающие, по мнению журналистов канала «Антенн 2», 400 картотек с более чем 100 млн записей, выражали новую форму централизации управления – централизацию информации об управляемых.

Пресс-секретарь правительства А. Росси сказал в ходе дебатов, что «ни один француз не будет внесен в базы данных так, чтобы он этого не знал». В 1978 г. был принят закон «Об информатике и архивах», первая статья

* Источники: *Texier B.* La loi Informatique et libertés a 40 ans // Archimag: stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – janvier 2018. № 310. P. 4–5; *Texier B.* RGPD: des outils pour se mettre en conformité// Archimag: stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – janvier 2018. № 310. P. 17; *Texier B.* Les CIL devront se mettre à niveau pour devenir DPO // Archimag: stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – janvier 2018. № 310. P.20; Delahaye P. RGPD: l'archivage électronique est aussi concerné // Archimag: stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – janvier 2018. № 310. P. 22–23; Real GDPR solution: la suite logicielle pour se mettre en conformité intégralement, rapidement et sans risqué // Archimag: stratégie & ressources de la mémoire & du savoir). Paris, décembre 2017 – janvier 2018. № 310. P. 18–19/

которого гласила: «Информатика должна служить каждому гражданину… Она не должна наносить ущерб ни человеческому достоинству, ни правам человека, ни его частной жизни, ни его личным и общественным свободам». Журналисты «Аршимага» справедливо отмечают, что эта формулировка – фактически манифест и она не устарела в наши дни, разве что неплохо было бы заменить «информатику» на «новейшие информационные технологии».

Основными требованиями Закона от 1978 г. стали обязательное получение от физического лица разрешения на сбор информации о нем (ст. 26 и 27), а также предоставление ему права доступа, исправления и уничтожения этой информации (ст. 3). Органом проведения в жизнь положений Закона стала созданная в 1978 г. «Государственная комиссия по информатике и свободам» (CNIL) – независимый контрольный орган, сменивший за сорок лет семь председателей и насчитывающий сегодня в своем составе двести экспертов. Комиссия следит за защитой частной жизни в самых разных проектах обработки информации. В поле ее внимания по мере появления попали базы данных госучреждений, каталоги потенциальных клиентов у коммерсантов, мобильные приложения для обмена данными, чат-боты и программы, использующие искусственный интеллект, данные, собираемые датчиками в «подключенных к Интернету городах». В 2016 г. председатель CNIL Изабель Фальк-Пьеротен процитировала исследование компании Garthier, предсказавшей, что в 2018 г. на улицах связанных с Интернетом городов Франции, будет постоянно работать 3,3 млрд датчиков и других устройств, собирающих данные. Исследование банка Морган Стенли оценивает количество подключенных к Интернету умных предметов в мире в ближайшие годы на уровне 75 млрд.

В этом контексте Комиссия по информатике и свободном (CNIL) продолжает свою традиционную работу по информированию граждан и ответам на их запросы, консультирование специалистов сектора информационных технологий и информационную поддержку работы уполномоченных по персональным данным (digital privacy officer). На основании обращений граждан комиссия будет по-прежнему контролировать и санкционировать нарушения в работе юридических лиц с персональными данными.

В последние годы всю большую часть рабочего времени сотрудников Лаборатории, созданной при Комиссии CNIL, занимает профилактика киберпреступлений. Экспертам и консультантам лаборатории приходится работать в нескольких смежных областях: биометрических данных, подключенных к Интернету объектов, банковских операций, криптографии. Их задача – дать юристам комиссии надежную информацию о технических аспектах проблемы, которую им предстоит решить. Для этого приходится

не только проверять соответствие устройств стандартам, но и выявлять нестандартные случаи их использования.

Если французы в целом довольны работой своей Комиссии CNIL, то аналогичная комиссия Евросоюза, созданная из членов аналогичных комиссий стран-участниц Евросоюза, называющаяся G29 и собирающаяся каждые два месяца в Брюсселе, вызывает серьезную критику со стороны ассоциации «Квадратура Интернета» (Quadrature du Net), объединяющей пользователей Сети. Члены этой ассоциации критикуют новый проект регламента ePrivacy, за разрешение провайдерам собирать и анализировать данные о навигации их клиентов в Сети, а также определять с помощью функции геолокации местоположение мобильных устройств их клиентов.

«Генеральный регламент о защите данных» (RGPD) усилил требования к защите хранимых организациями персональных данных от потери, кражи и злоупотреблений за счет проектируемой конфиденциальности (privacy by design) и безопасности по умолчанию (security by default). Финансирование выполнения этих требований вполне может окупиться, так как их соблюдение улучшит отношения многих частных и государственных юридических лиц с клиентами и пользователями. Неслучайно большинство санкций и штрафов, наложенных Комиссией по информатике и свободам (CNIL) в последние годы, касались именно утечки клиентских данных.

«Генеральный регламент» потребует не только модернизации программного обеспечения, но и изменения практики работы, хотя бы временного, согласно пошаговому плану внедрения «Регламента». Новостью стала и необходимость отчитываться не только перед национальными, но и перед зарубежными или европейскими контрольными органами, компетентными в сфере защиты данных.

По данным П.-О. Жильбера, Председателя «Французской ассоциации корреспондентов по защите персональных данных» (AFCDP) меньше чем за год до вступления «Регламента» в силу (запланированного на 28 мая 2018 г.) почти все крупные предприятия Франции начали проекты по приведению своей деятельности и программного обеспечения в соответствие с его требованиями. Однако консалтинговая компания IDC привела в обследовании 2017 г. пугающую цифру: всего в 9% французских предприятий управление данными действительно отвечает требованиям «Регламента». П.-О. Жильбер считает, что эта цифра не может быть поводом для паники, так как далеко не все предприятия страны используют в своей работе персональные и другие критически важные данные. Проблема персональных данных, в первую очередь, касается предприятий, работающих по модели B2C. Другим слабым местом реформы может стать человеческий фактор: нужно обучить уже работающих «корреспондентов по информатике и свобо-

дам» (CIL) пониманию и применению требований «Регламента», который серьезно изменяет отношения между контрольными и контролирующими организациями, чтобы они смогли стать Уполномоченными по защите данных (DPO) в своих организациях.

Эти 17 500 специалистов составят костяк будущего корпуса из 80 000 управляющих по защите данных. «Управляющие» (Регламент 2016 г.) как и «корреспонденты» (Закон от 1978 г.) не осуществляют сами обработку данных, а только советуют осуществляющим ее специалистам, как им лучше соблюсти требования Закона, поддерживают связь с контрольными органами и ведут технологический и правовой мониторинг. Они также будут отвечать за грамотное документирование значимых для «Регламента» аспектов работы программного обеспечения, за учет всех операций по обработке данных и изучение последствий внедрения тех или иных изменений для безопасности данных.

Если «корреспонденты по информатике и свободам» нередко работали на половину или четверть ставки, то «уполномоченные», скорее всего, будут работать на полную ставку или будут вынуждены привлекать к своим проектам на постоянной основе других сотрудников. В любом случае новые специалисты не останутся без поддержки: в Евросоюзе работает Конфедерация европейских организаций, защищающих данные (Confederation of european data protection organisations). В странах-членах Евросоюза их поддержат национальные ассоциации, такие как «Французская ассоциации корреспондентов по защите персональных данных» (AFCDP), которая организует для французских специалистов в этот сложный период 3-4 совещания в месяц и 24 января 2018 г. в Париже – зимний «Университет уполномоченных по защите данных» (DPO).

Одним из возможных последствий внедрения «Генерального регламента о защите данных» (RGPD) может стать усиление позиций Комиссии CNIL, но за шесть месяцев до его вступления в силу самым заметным изменением остается актуализация программного обеспечения для работы с персональными данными согласно новым требованиям. Ален Эскафр, директор производства компании Nuxeo, в интервью «Аршимагу» подчеркнул, что «внедрение Регламента потребует от программного обеспечения, занятого управлением контентом, более умной работы (распознавания информации явно персонального характера), а также способности объединять разнородную информацию из разных источников, чтобы применять к ней единые линейки правил и процедуры обработки».

Один из специалистов по электронным репозитариям Ф. Делае (Кредитно-депозитная касса – CDC) также считает, что «Регламент» обяжет включить в программное обеспечение более подробные и тонкие меха-

низмы управления сроками ведомственного хранения документов с целью избежания избыточного хранения персональной информации, которая больше не нужна для работы и должна быть уничтожена сразу же по прекращении надобности.

В связи со вступлением в силу «Регламента» фирма Nuxeo решила дополнить свою традиционную программу по управлению цифровым контентом программой «акселератором (RGPD)», работающим с конкретными делами, отобранными на основании каких-либо критериев или характеристик (case management).

«Акселератор (RGPD)» фирмы Nuxeo имеет много интересных функций:

• автоматизацию запросов на доступ к персональным данным, достаточное для проверки законности;

• документирование доступа;

• нюансированное управление доступа к документам одного лица, в зависимости от полномочий другого.

Несмотря на это, его разработчики считают, что только внедрение программы не может обеспечить юридическому лицу полное соответствие требованиям «Генерального регламента о защите данных» (RGPD), потому что значительная часть требований относится к культуре управления, далеко не всегда формально сводимой к программному обеспечению. По мнению директора по производству компании Nuxeo Алена Эскафра, программ, полностью отвечающих требованиям нового Регламента, просто «не существует».

Очевидно, к такому же мнению пришли и специалисты IBM, потому что компания заключила в Европе партнерские соглашения с адвокатскими и аудиторскими конторами, чтобы предоставить клиентам комплексные услуги по приведению их методов работы с данными в соответствие с требованиями «Регламента». Первый этап такого сопровождения длится от нескольких недель до нескольких месяцев (в зависимости от размеров юридического лица) и заключается в оценке ситуации с данными на предприятии юристами, специалистами по информационным технологиям и советниками по организации производственных и управленческих процессов.

Причем аудит программного обеспечения на соответствие «Регламенту» становится, по мнению ответственного в IBM за внедрение Регламента Тьери Брюна, «менее декларативным», учитывает поведение информационной системы в конкретной опасной для утечки данных ситуации. По окончании проверки фирма-клиент получает рекомендации либо об обезличивании своих данных, либо о шифровании своих электронных документопотоков, либо об уничтожении части данных или об их помещении в «карантин».

Поскольку базы данных нередко хранят персональную информацию, фирма Oracle предложила своим клиентам три модуля для обеспечения соответствия их баз требованиям «Регламента». Первый модуль, предназначенный для экспертизы данных, определяет степень их конфиденциальности и уязвимости, состав и связанные с ними риски. Второй модуль занят предупреждением выявленных рисков: шифрованием, обезличиванием данных или присвоением упомянутым в них физическим лицам псевдонимов, контролем за использованием данных на основании весьма подробно разработанной линейки правил доступа. Третий модуль по своим функциям ближе всего к системе безопасности, защищающей как структуру и правила работы базы данных, так и сами находящиеся в ней данные.

Фирма GlassIG разработала новую программу «GlassIG GDPR Edition», позволяющую организовать управление моделями персональных данных в организации.

Программное обеспечение ARM компании ActeCil позволяет организации, передающей свои данные на обработку зарубежному подрядчику, а также самому субподрядчику-соисполнителю регистрировать в электронном журнале «подряда на обработку данных» всю необходимую, согласно требованиям «Регламента», информацию: категорию обрабатываемых данных, тип обработки каждого пакета данных, название и координаты фирмы-подрядчика и фирмы-клиента, координаты Уполномоченного по защите данных (DPO) этой фирмы.

Уже упомянутая компания ActeCil разработала совместно с компаниями Rever и Geolsemantics, программное обеспечение «Real DRGP Solution», отвечающее требованиям «Регламента» и состоящее из описанного выше журнала обработки данных и из журнала учета взаимодействия данного программного обеспечения с другими. Программа «Real DRGP Solution» может взаимодействовать со всем комплексом программного обеспечения организации и позволяет Уполномоченному по защите данных (DPO) отрегулировать управление данными, содержащими персональную информацию, в конкретной организации. Программа автоматически проводит семантический анализ поля «свободные комментарии» клиентских баз данных на предмет выявления несоответствий с «Генеральным регламентом», в том числе некорректных высказываний о клиентах и партнерах (например, оценок здоровья, состояния психики и умственных способностей физических лиц), за которые несколько французских фирм уже заплатили в прошлые годы солидные штрафы.

Программа работает со всеми типами постоянных данных, независимо от того, являются ли они просто файлами (форматов COBOL, csv, XML, HTML или неструктурированными) или хранятся в базах данных, как реля-

ционных или NoSQL, так и Legacy (с сервис-ориентированной архитектурой), или в тексте документов и сообщений электронной почты. Контейнер, содержащий данные, является для этих программ «прозрачным», если он доступен для программ, работающих в алгоритме SAAS «программное приложение как услуга».

«Real DRGP Solution» позволяет документировать алгоритмы обработки данных, индивидуальные права физических лиц на доступ к данным, обезличивание данных, аудит их содержания, применение «проектируемой конфиденциальности» (privacy by design). Программа написана так, что она и защищает персональную информацию физических лиц, и позволяет Уполномоченному по защите данных (DPO) оперативно отвечать на запросы Государственной комиссии по информатике и свободам (CNIL) или других независимых контролирующих органов. Например, коммерческие организации могут благодаря этому приложению запрограммировать автоматическое уничтожение информации о потенциальных клиентах или заказчиках через полгода после последней записи о них.

Этого времени вполне достаточно, чтобы потенциальный клиент заключил договор, и данные о нем перешли бы в «клиентскую» базу данных, а информация о несостоявшихся клиентах потеряла бы актуальность. Программу также можно настроить на поиск информации годичной давности о потенциальных клиентах и на ее уничтожение – либо автоматическое, либо в ручном режиме – после просмотра оператором базы данных. «Real DRGP Solution» облегчает работу функциональных аналитиков, устанавливая при помощи специального модуля и на основе информации о структуре и содержании данных четкие связи между описываемыми юристами в обязательных журналах для регистрации обработки данных операциями и реальными технологическими процессами в информационных системах.

Сотрудник Кредитно-депозитной кассы (CDC) Франции, разработавшей и предоставившей в распоряжение физических и юридических лиц первый в стране электронный репозитарий, Филипп Делае считает, что внедрение «Регламента» обязывает фирмы-подрядчики, занятые хранением электронных документов (многие из которых – расчетные листы заработной платы, медицинские карты, трудовые договора и договора о потребительских кредитах, содержащие персональную информацию), создавать постоянные должности «уполномоченных по защите данных» (DPO), которые будут доказывать клиентам совместимость программного обеспечения и практики работы своих фирм с требованиями «Регламента».

Кроме того, целесообразно предусмотреть для платформ, хранящих электронные документы, проектируемую конфиденциальность (privacy by design), в которую данный специалист включает защищенный канал связи

с клиентом, запрет на анализ содержания поступающих документов, в особенности для индексации, традиционные гарантию их неизменности в период хранения и контроль доступа. Проблема заключается в том, как именно требования «Регламента» будут интерпретированы в коммерческом дискурсе фирм, потому что в отличие от функциональной аккредитации Межведомственной архивной службы Франции (SIAF) и отраслевых аккредитаций Агентства информационных систем здравоохранения ASIPsanté и Министерства обороны, официальных способов заверить соответствие данной организации требованиям «Регламента» во Франции пока не существует. Однако все специалисты согласны, что соответствие требованиям всех уже существующих стандартов, в том числе и ИСО 27001, создает хорошую основу для соответствия новым требованиям.

Реферат В.Б. Прозоровой

Этические проблемы цифровизации культурного наследия*

Зинаида Манжуч, Вильнюсский университет

Вводные положения

Профессиональная этика традиционно призвана служить принятым ценностям и нормам и исключать неприемлемое поведение профессионалов, что обеспечивает общественное доверие к услугам, предоставляемым определенными организациями. Изменения заставляют специалистов формировать новые способы поддержки профессиональных ценностей. Архивы, библиотеки и музеи активно вовлечены в процесс цифровизации культурного наследия уже на протяжении нескольких десятков лет.

Проекты по цифровизации создали новые организационные формы и сети сотрудничества, а также типы услуг, основанных на культурном наследии, и, естественно, послужили причиной изменений во взглядах, стратегиях и процессах. Большое количество примеров и исследований определенных этических проблем доказывают, что цифровизация значительно влияет на управление онлайн-вовлеченностью в коллекции наследия, обеспечение конфиденциальности персональной информации в документах наследия, обеспечение аутентичности, организацию доступа к объектам на-

* Источник: *Manžuch Z.* Ethical issues in digitization of cultural heritage // Published by EliScholar – A Digital Platform for Scholary Publishing at Yale, 2017 [Digital resource]. – URL: https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=1036&context=jcas.

следия и осуществление отбора и интерпретации. Новый профессиональный опыт по цифровизации привел к появлению новых этических проблем.

Этика цифровизации не рассматривается как отдельная область научной и профессиональной дискуссии, однако существуют отдельные публикации, связанные с более широким спектром проблем, в которых признается, что в проектах по цифровизации возникают этические проблем. Многочисленные публикации, связанные с ними, появляются вследствие того, что подразумеваемые исходные положения, установившиеся этические нормы, принятые у архивистов, библиотекарей и музейных работников, не работают при цифровизации культурного наследия.

В связи с этим необходимо явно показать этические проблемы цифровизации и проанализировать существующие мнения в данной области. Это может быть полезно для:

• поиска и формирования работающих решений этических проблем цифровизации;

• установления четких взаимосвязей между этическими проблемами цифровизации и ролью архивов, библиотек и музеев, и подходов к профессиональной этике вообще;

• понимания, как этические проблемы могут влиять на управление цифровизацией наследия.

Главной целью данной работы является определение того, какие этические проблемы возникают при цифровизации культурного наследия и как они влияют на принимаемые решения и организацию процессов цифровизации. В целях обсуждения этических аспектов цифровизации важно дать четкое определение данному понятию. Определение цифровизации, которое сформулировано ЮНЕСКО, привязывает его к широкому контексту решений и деятельности организаций, осуществляющих хранение.

Цифровизация* – это создание цифровых объектов из физических, аналоговых оригиналов средствами сканирования, фотооборудования и других электронных устройств. Оно осуществляется как часть процесса, который включает в себя отбор, оценку, учет потребностей, установление приоритетов, подготовку оригиналов к оцифровке, сбор и создание метаданных, оцифровку и создание коллекций данных, предоставление цифровых ресур-

* Данный термин может быть переведен как «оцифровка», чему соответствует определение, содержащееся в первом предложении определения. Однако по тексту данного материала термин «digitization» и этические проблемы, связанные с ним, используется в контексте всех процессов и деятельности, которые далее перечислены в данном определении. Поэтому при составлении настоящего реферата в случаях, если проблемы, затрагивали только деятельность по созданию цифровых образов, использовался термин «оцифровка», в случаях прочей деятельности использовался термин «цифровизация». – *Примечание автора реферата.*

сов в системы предоставления доступа и репозитарии. Этот процесс сопровождается управлением, включая управление правами интеллектуальной собственности, контролем качества и его оценкой.

В работе это понятие используется в соответствии с данным определением, в ней представлены этические проблемы, которые возникают на всех стадиях цифровизации.

С этическими проблемами при цифровизации сталкиваются архивы, библиотеки и музеи. Зонтичный термин «организации, осуществляющие хранение» используется в данной работе, что соответствует их общему назначению, связанному с управлением коллекциями культурного наследия с целью удовлетворения потребности общества в сохранении памяти. Сходство целей и функций этих организаций подчеркивается многими исследователями. При этом признаются и различия в профессиональных подходах к культурному наследию, принятых в архивах, библиотеках и музеях. В данной работе акцент делается на анализе общих этических проблем и решений при цифровизации. Исходные принципы, учитываемые при проведении данного анализа, изложены в международных кодексах этики архивистов, библиотекарей и музейных работников, а также Всеобщей декларации прав человека ООН (1948).

Изменения, возникающие при цифровизации, и связанные с ними этические проблемы

Обзор литературы выявляет несколько проблемных областей, связанных с цифровизацией, которые приводят к возникновению этических проблем и конфликтов. Некоторые из них, например, возникновение цифровых архивов сообществ, представляют контекстные факторы, стимулирующие изменения в подходах к цифровизации организаций, осуществляющих хранение. Другие, такие как новые модели финансирования оцифровки, напрямую связаны с методами управления цифровизацией, которые приводят к возникновению этических проблем в организациях, осуществляющих хранение. В то же время, среди прочих можно отметить простоту распространения и манипуляции цифровым контентом, а также онлайн-вовлеченность в наследие в глобальном цифровом пространстве и влияние цифровых технологий на способы обработки и предоставления объектов наследия в цифровом пространстве.

Тема этики цифровизации очень широка и включает обсуждение изменений в этой сфере и проблемы, которые не решены, а также примеры практических решений, поэтому обзор и анализ, представленный в этой статье, по определению не является полным.

Возникновение цифровых архивов сообществ

Расширение доступности легких для использования и относительно дешевых инструментов цифровизации и развитие Web 2.0 способствует развитию любительской оцифровки и возникновению альтернативных, непрофессиональных цифровых архивов, создаваемых индивидуумами и различными сообществами. Социальные группы и сообщества, которые маргинализировались или подвергнулись преследованиям – сообщества местного населения (аборигенов), миноритарные группы по религиозной и расовой принадлежности, сексуальной ориентации или гендерной идентификации, а также страны, которые были ранее колонизированы, используют цифровые онлайн-коллекции как платформу, позволяющую сделать их голос слышимым и/или получить или вернуть контроль над своим наследием. Прошлое этих групп представлено в архивах, библиотеках и музеях через призму доминирующих, обладающих властью групп и сообществ. Данная ситуация послужила импульсом к появлению движения так называемых «архивов сообществ» или «независимых архивов», в рамках которого организации и сообщества начали создавать и поддерживать цифровые коллекции независимо от государственных архивов, библиотек и музеев.

Местные сообщества используют цифровизацию, чтобы вернуть контроль над традиционными культурными знаниями, которые излишне коммерциализированы и используются без согласия создавших их сообществ. Всемирная организация интеллектуальной собственности побуждает местные сообщества оцифровывать их нематериальное наследие (например, песни, танцы, ритуалы и т.п.), поскольку данные активы не защищены конвенциональной системой интеллектуальной собственности. Данное нематериальное наследие, записанное исследователями, также появляется в коллекциях архивов, библиотек и музеев. Часто оцифровка, отбор и систематизация таких материалов наряду с широким онлайн-доступом к ним противоречат традиционным взглядам местных сообществ.

Возникновение «архивов сообществ» и инициатив по защите наследия местного населения побуждает архивы, библиотеки и музеи учитывать взаимосвязи между культурным наследием и взгляды на мир сообществ, которые создали и практикуют его. Это создает значительные проблемы для традиционного понимания того, как ценности нейтралитета и объективности должны поддерживаться при управлении и обеспечении доступа к культурному контенту. Цифровые архивы сообществ выявили проблемы неравенства, субъективных суждений, дискриминации и т.д., которые возникли в результате решений, принятых организациями, осуществляющими хранение. Изначально сформированные как организации, призванные транслировать наследие национальных государств, они оказались в ситуации

многофакторного разнообразия памяти и наследия различных сообществ и групп, составляющих наше общество. Все большее признание получает тот факт, что конфликтующие и противоречащие интересы, властные связи и политический и правовой контекст оказывают огромное влияние на решения, принимаемые архивами, библиотеками и музеями.

Вследствие изменения подхода к наследию сообществ стала очевидной предвзятость при отборе и интерпретации культурного наследия для цифровизации. Обсуждая цифровизацию африканского наследия, исследователи констатируют предвзятость при отборе и доминирующий «западный подход» к прошлому, особенно когда оцифровываются африканские коллекции, содержащиеся в зарубежных организациях, осуществляющих хранение. Часто различные противоречащие взгляды на события прошлого не видны при осуществлении проектов по цифровизации африканского наследия.

Новые модели финансирования оцифровки

Стоимость оцифровки высока, поэтому большинство инициатив зависят от внешнего финансирования или поддержки спонсоров. Чтобы формировать фонды для оцифровки и обеспечивать устойчивость хранения оцифрованного контента, организации все чаще используют бизнес-подходы. Такие подходы основываются на потенциальной возможности использования объектов оцифрованного наследия для разработки коммерческих услуг и контента. Они включают инициативы хранящих организаций по взиманию платы за доступ к оцифрованному контенту, партнерству с частными хозяйствующими субъектами и поиск поддержки от спонсоров. В этих инициативах хранящие организации преследуют цели снижения бремени затрат на оцифровку, привлечения финансов, инфраструктуры или компетенций, в то время как целями их коммерческих партнеров является повторное использование оцифрованного контента для предоставления коммерческих услуг или создания продуктов.

Использование бизнес-подходов в государственном секторе поднимает две этические проблемы.

1. *Предвзятость отбора.* В государственно-частном партнерстве спонсоры и партнеры из частного сектора оказывают влияние на отбор и интерпретацию контента, который должен быть оцифрован. Исследователи отмечают, что предпочтения спонсоров могут приводить к определенным решениям при отборе и интерпретации (пример: влияние зарубежных спонсоров на интерпретацию в африканских проектах по оцифровке, гендерные пробелы в представлении Гражданской войны США).

Организации, осуществляющие хранение, могут оказаться в ситуации, в которой они вынуждены оцифровывать только тот контент, который интересен спонсору.

2. *Ограничения доступа.* В погоне за прибылью партнеры из частного сектора, вкладывающие значительные средства в оцифровку или осуществляющие ее, настаивают на ограничении доступа к оцифрованному контенту в течение некоторого периода, который может достигать десяти лет ограничения онлайн-доступа. Это ставит вопрос о доступности оцифрованного контента, особенно в случае, если проект по оцифровке частично финансировался из государственных фондов (в результате конечный пользователь информации платит дважды). Более того, этические проблемы возникают, когда организации, осуществляющие хранение, имеют намерение взимать плату за повторное использование оцифрованного контента в государственном секторе.

Задачу комбинирования частного и государственного финансирования и проблему предвзятости, возникающие при осуществлении спонсорской поддержки, довольно сложно решить. Организации, осуществляющие хранение, вынуждены признать, что оцифровка является дорогой и рассчитывать только на государственное финансирование – невозможно. Широко распространено решение, используемое хранящими документы организациями, а именно, разделение деятельности, создающей доход, и инициатив по оцифровке, финансируемых государством. Например, Национальная библиотека Франции и Британская библиотека создали дочерние компании, которые осуществляют коммерческую деятельность с целью поддержки оцифровки культурного наследия. Данное решение позволяет избежать вовлеченности государственных учреждений в формирование поступлений для финансирования оцифровки.

Легкость распространения и манипулирования цифровым контентом

В отличие от традиционных объектов культурного наследия, цифровой контент может легко распространяться, комбинироваться, группироваться в онлайн-режиме. Его содержимое можно также легко изменить. Это обеспечивает ряд преимуществ для пользователей цифрового контента по расширению доступа к оцифрованным коллекциям и позволяет осуществлять их повторное использование в целях проведения исследований, обучения и разработки нового коммерческого контента. Однако простота распространения и внесения изменений в цифровые файлы усложняет задачи защиты личной информации, содержащейся в оцифрованных документах, и обеспечения доверия к ним.

Обязанность соблюдения условий неприкосновенности частной жизни в явном виде документируется в кодексах профессионального поведения организаций, осуществляющих хранение, и в статье 12 Всеобщей декларации прав человека ООН: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию». При этом зачастую задача обеспечения неприкосновенности частной жизни противоречит целям обеспечения онлайн-доступа к объектам документального наследия.

Проблема обеспечения доступа к личной информации связана с тем, что в документах и объектах культурного наследия содержится большое ее количество, а также с тем, что в условиях цифровизации существуют беспрецедентные возможности по онлайн-доступу к ней, ее поиску и сбору из различных источников. В качестве примеров «личной» информации можно привести этнографические материалы с интимными подробностями, мнениями, упоминанием других лиц и событий, сделанные информантами (носитель языка, осуществляющий помощь при сборе этнографических данных), медицинские документы, архивные документы, содержащие данные об отдельных индивидуумах, газеты и т.п. Во многих случаях онлайн-доступ к этой информации при ее создании не предполагался и поэтому не оговаривался с информантами и дарителями материалов наследия.

Новый взгляд на обеспечение тайны личной жизни в цифровом пространстве – право быть забытым – делает процесс поиска решения этических проблем обеспечения тайны личной жизни еще более сложным. Право быть забытым – это новая концепция, введенная Общим регламентом Европейского союза по защите персональных данных в 2016 г. Она обеспечивает человеку возможность извлекать информацию из сети Интернет или делать ее анонимной, и, таким образом, позволяет ему контролировать личную информацию в сети. Право быть забытым тесно переплетается с проблемами манипулирования или разрушения прошлого, которые возникают, если документы и записи извлекаются или удаляются. Большинство практических решений этического характера, связанных с обеспечением тайны личной жизни и правом быть забытым выявляют потребность в формировании адекватного баланса между доступом с целью обеспечения интересов общества в исследовании и защиты человека, который упомянут, представлен или выразил свое мнение в объекте документального наследия.

Положения, связанные с информацией, ассоциирующейся с личностями в исторических документах, и право быть забытым, сформулированные Международной федерацией библиотечных ассоциаций и организаций (International Federation of Library Associations and Institutions, IFLA) по-

казывают, что ценности интеллектуальной свободы и обеспечения доступа остаются руководящими принципами профессионалов организаций, осуществляющих хранение. При этом признается возможное влияние результатов оцифровки коллекций на живущих людей.

Изучение отдельных случаев оцифровки показывает, что профессионалы организаций, осуществляющих хранение, стали более чувствительны к последствиям и урону, который повсеместный онлайн-доступ может нанести личной жизни. Обсуждались инициативы по оцифровке, в которых индивидуальные случаи должны подвергаться пересмотру, предполагающему тщательную оценку возможного вреда, и были разработаны информационные системы, предоставляющие различные уровни доступа.

Выделение и защита персональной информации в рамках крупных инициатив оцифровки остается значительной проблемой. Соответственно, необходимо установление новой политики, практики и процессов, позволяющих сбалансировать право быть забытым с другими правами, такими как право на интеллектуальную свободу. Недостаточная ясность применения права быть забытым может стать существенной проблемой для осуществления проектов по оцифровке в Европе.

Другой этической проблемой, связанной с легкостью манипулирования, копирования и изменения назначения цифровых суррогатов, является обеспечение аутентичности оцифрованного контента. Аутентичность определяется как «качество объекта быть тем, чем он должен быть (признаваемый, реальный, подлинный), проверенное в архивах и специальных коллекциях в процессе проведения исследования, называемого аутентификацией». Намерение по обеспечению аутентичности явно прописано в этическом кодексе Международного совета архивов, где указано, что «архивисты должны обеспечивать аутентичность документов в процессе архивной обработки, хранения и использования». Кроме этого, этический кодекс IFLA библиотекарей и профессионалов в области работы с информацией подчеркивает обязанность обеспечения прозрачности при предоставлении информации, в то время как этический кодекс Международного совета музеев содержит обязанность музеев фиксировать первичное доказательство (свидетельства). Обеспечение аутентичности тесно связано с полномочиями и доверием к архивам, библиотекам и музеям. Концепция аутентичности лежит в основе отбора, цифровой конверсии и решений по хранению, осуществляемых профессиональными архивистами, библиотекарями и музейными работниками.

Цифровая реставрация оцифрованных материалов может сделать их более удобными для использования, однако при этом возникает задача поддержания аутентичности документа/объекта в ее традиционном понимании.

Исследователи и практики обеспокоены тем влиянием, которое определенная конфигурация аппаратного и программного обеспечения, применяемая для цифровой конверсии, и методы сжатия данных и методы улучшения, применяемые после осуществления конверсии, оказывают на восприятие оригинальных объектов наследия в цифровом виде.

Руководство по оцифровке рекомендует создание архивного мастер-файла, который не содержит изменения для улучшения восприятия пользователя. Однако большинство пользователей никогда не получат доступа к архивному мастер-файлу. Тем не менее, прозрачная доступная публичная информация о политике оцифровки в организациях, осуществляющих хранение, наряду с информированием пользователей (особенно ученых) о проблемах аутентичности в цифровом пространстве могут быть одним из возможных решений. Кроме этого, цифровой заменитель не отражает все характеристики оригинального документа или объекта наследия. Тем не менее, зачастую нет ни возможности, ни разумной цели максимизировать качество цифровой конверсии.

Однако, по мнению автора, этические проблемы определения требований к аутентичности оцифрованного контента еще не решены. Наконец, для того, чтобы хранить оцифрованный контент в долгосрочной перспективе и преодолеть технологическое устаревание программного и аппаратного обеспечения, должны вноситься изменения в цифровые файлы. Это также создает проблему обеспечения аутентичности. Чтобы решить их, организации, осуществляющие хранение, внедряют различные модели сертификации репозитариев цифровых материалов и осуществляют мониторинг процесса обеспечения цифровой сохранности.

Понятие аутентичности является социальной конструкцией. Аутентичность вплетена в набор установленных и согласованных практик. Погружение профессионалов организаций, осуществляющих хранение, в потребности и практику определенных сообществ формирует понимание того, что делает объект или документ аутентичным в определенном контексте использования. В настоящее время специалисты в организациях, осуществляющих хранение, сталкиваются с потребностью устанавливать процессы и практику обеспечения аутентичности в цифровом пространстве.

Онлайн-вовлеченность в наследие в глобальной цифровой среде

Приверженность ценностям интеллектуальной свободы, включая «свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ», заявленную в Статье 19 Всеобщей декларации прав человека ООН, служит руководством для про-

ектов по оцифровке. Подобные ценности доступа заявлены в профессиональных кодексах ICA, IFLA и ICOM. Основной целью большинства проектов по оцифровке является расширение доступа и использования через публикацию контента в онлайн-режиме.

Несмотря на то, что цифровизация обещает всеобщий доступ к информации наследия, она приводит к новым типам неравенства и конфликтам между различными подходами к прошлому, которые возникают в различных национальных рамках. Оцифровка и использование социальных медиа для вовлеченного взаимодействия пользователей в коллекции культурного наследия также требуют значительных изменений в подходах предоставления наследия организациями, осуществляющими хранение.

В глобальном масштабе оцифровка предоставляет возможность «виртуального возврата» культурного наследия, которое было изъято у создавших его сообществ и наций в результате колонизации, вооруженных конфликтов, природных катастроф и т.п. Возможность оцифровки изъятого наследия приводит к новым формам неравенства. Зачастую сообщества, которые должны получать пользу от подобных проектов, не могут получить к ним доступ из-за барьеров, создаваемых организациями, осуществляющими хранение. Рассматривая оцифровку изъятых подобным образом архивных материалов, исследователи констатируют, что использование организациями, осуществляющими хранение, собственного языка при описании оцифрованных документов ограничивает возможности пользователей из сообществ, создавших наследие, в его использовании. Другие исследователи показывают, что имеет место ограничение доступа, создаваемое платой за подписку, отсутствие хорошо развитой технической инфраструктуры в сообществах пользователей, а также невозможность адаптировать проекты к контексту жизни людей, которые, как предполагается, должны получать пользу от доступа к оцифрованным коллекциям.

Часто уровень обобщения информации и технологии ее передачи, уровень навыка и возможности ее получения, а также традиции использования цифровых инструментов в сообществах бенефициариев вообще не учитываются. Устойчивость проектов оцифровки изъятого наследия также вызывает сомнения. Организации, осуществляющие хранение, действуют в рамках национальных политик и финансирования, при которых оцифровка и поддержка «чужого» наследия зачастую не являются приоритетным.

В этом случае представление о том, что всеобщий доступ становится возможным только благодаря цифровым технологиям, является иллюзией вследствие комплекса сложных факторов власти, финансовых, инфраструктурных, образовательных и других, являющихся необходимым условием доступности цифрового контента. Однако в свете этого автор отмечает

роль организаций, осуществляющих хранение, как апологетов цифрового доступа к наследию в глобальном масштабе, за рамками национальных приоритетов и границ.

Социальные медиа стали популярным инструментом, который обеспечивает более инклюзивную, демократичную и вовлеченную передачу цифрового культурного наследия в онлайн-режиме. Влияние технологий Web 2.0 выходит за рамки простого использования популярных инструментов для реализации подходов участия и сотрудничества, которые размывают традиционные границы между профессиональными организациями, осуществляющими хранение, и их пользователями. Быстрое принятие Web 2.0 без учета изменений, которые необходимы, чтобы сделать ее действительно обеспечивающей реальное участие, привело к возникновению этических проблем. Некоторые из них связаны с недостатком устойчивых решений для поддержки коммуникаций в глобальном масштабе на платформах социальных медиа и согласованности права свободы мнений и их выражения по отношению к людям и сообществам. Другие исследователи выражают беспокойство в отношении возможных ограничений участия пользователей в процессах передачи культурного наследия.

1. Исследователи сомневаются в том, что технологии социальных медиа являются инклюзивными и демократичными по определению. Без применения философии участия в организациях, осуществляющих хранение, социальные сети могут сформировать предвзятое коммуникационное пространство. Некоторые исследователи подчеркивают, что не полное представление контента в социальных сетях – наследие и/или взгляды некоторых социальных групп представлены в недостаточном объеме, – может привести к неверной интерпретации; доступность инструментов и навыков загрузки, комментирования и распространения онлайн-контента определенными группами предопределяют их уровень онлайн-вовлеченности.

2. Доступность инструментов комментирования, распространения и повторного использования контента ставит вопросы о роли организаций, осуществляющих хранение, в поддержке этих процессов. С одной стороны, увеличение оскорбительных комментариев и выражения ненависти приводит к тому, что организации, осуществляющие хранение, ощущают потребность действовать как модератор, который может обеспечить этичное отношение ко всем сообществам. С другой – практика контроля зачастую базируется на субъективных суждениях и непрозрачна. Модерирование различных точек зрения и мнений, особенно в случаях наследия, связанного с трагедиями, также является очень сложным аспектом применения концепции участия на практике.

3. Web 2.0 значительно расширяет возможность пользователей принимать участие в формировании, интерпретации и распространении цифрового на-

следия в онлайн-режиме. Организации, осуществляющие хранение, сталкиваются с проблемами владения и распоряжения контентом, возникающими в связи с возможностью его распространения. Организации, осуществляющие хранение, сообщают о нарушениях при повторном использовании, которое создается вводящими в заблуждение комментариями или информацией. Однако организации, осуществляющие хранение, часто не готовы к активной вовлеченности пользователей в предоставление наследия.

Исследователи утверждают, что организации, осуществляющие хранение, имеют законное право владеть *и* предоставлять коллекции для общества, *а* не *с* помощью общества. В качестве примера они приводят дела, рассмотренные в суде, в которых библиотеки и музеи ограничивают повторное использование высококачественного оцифрованного контента третьими сторонами (например, Википедией и проч.). Аналогично организации, осуществляющие хранение, зачастую имеют тенденцию играть патерналистскую роль в определении того, что́ должно быть предоставлено в сети и ка́к. При этом они оставляют пользователю некоторые возможности реагировать, но не принимать участие на равных в совместном создании и интерпретации прошлого. Очевидно, исследователи признают, что такие этические проблемы возникают из-за различных и взаимоисключающих сознательных и скрытых мотиваций и понимания роли и обязанностей организаций, осуществляющих хранение (например, эксперт/координатор/со-куратор и т.п.).

Рассмотрение этических проблем цифровизации отражает фундаментальные изменения, которые происходят не равномерно, сопровождаются проблемами и неудачами в понимании роли организаций, осуществляющих хранение, и того, каким образом они встраиваются в высокоуровневые процессы сохранения памяти. Обращение к этическим проблемам цифровизации позволяет профессионалам охватить спектр последствий решений и пересмотреть базовые концепции профессии хранителей, объединяя цифровизацию и основную роль организаций, осуществляющих хранение, в обществе, и осуществляя гуманизацию и связывая ее с жизнью и потребностями сообществ и людей. Анализ исследований в области этики цифровизации и отдельных случаев показывает, что организации, осуществляющие хранение, применяют подходы, предполагающие участие и вовлеченность сообществ, создающих и сохраняющих объекты наследия, в формирование устойчивых и прозрачных моделей принятия решений.

Организации, осуществляющие хранение, рассматривают объекты и коллекции наследия в более широком контексте формирования и реконструкции прошлого, выстраивая множественные взаимоотношения и учитывая взгляды людей и сообществ, вовлеченных в определенные события и деятельность. Этот сдвиг подтверждается вниманием к влиянию, которое оказывает цифровизация на жизнь/ценности/поведение/потребности

определенных сообществ и людей, и множеством случаев работы для и с сообществами с целью разработки методов отбора, представления и организации оцифрованного наследия в онлайн-режиме с целью обеспечения более полного, динамичного и инклюзивного вовлечения в изучение истории. Подобные изменения могут позитивно влиять на понимание целей цифровизации в целом и привести к предоставлению более интересных и содержательных услуг, основанных на наследии, в цифровой форме.

Этические проблемы, поднимаемые в литературе по цифровизации также показывают более зрелый подход к цифровым технологиями и их влиянию на часть архивистов, библиотекарей и музейных работников. Большинство участников и исследователей инициатив по цифровизации признают, что как социально недискриминационный, так и эксклюзивный подходы могут иметь место. Это подтверждается тем, что подвергаются сомнению предположения о всеобщей доступности оцифрованных материалов в онлайн режиме; вызывает беспокойство тот факт, что технологии являются инструментом усиления доминирования экономически и политически властных сообществ и групп; подвергается сомнению отсутствие дискриминации в социальных медиа и признается разрушительное влияние на тайну личной жизни, вызываемое инструментами комплексного поиска и массовой агрегации личного контента.

Вызовом для организаций, осуществляющих хранение, становится задача становления их как институтов, которые вовлекают заинтересованных лиц в принятие решений по цифровизации. Понимание себя как ответственной и чуткой организации, учитывающей взаимные интересы, на практике может быть очень сложно. Это связано с необходимостью преодоления скрытого и неосознанного восприятия ролей организаций, осуществляющих хранение, сложностями в поддержании баланса конфликтующих взглядов на прошлое и ограничениями в обеспечении недискриминации всех групп в сопричастности к прошлому.

Научные исследования показывают, что этические проблемы влияют на принятие решений и организацию процессов на различных стадиях цифровизации от отбора и организации информации до разработки информационных систем и онлайн-представления оцифрованного контента. Этические проблемы оказывают влияние как на деятельность вообще, так и на продолжительность и стоимость решения проблем цифровизации в будущем.

Аргументы, представленные выше, ясно показывают, что необходимо прояснить комплексную картину этических проблем, возникающих при цифровизации, и сформировать эффективные решения, которые связаны с базовыми ролями и этикой организаций, осуществляющих хранение.

Реферат А.М. Лобановой

Новые и комплексные средства связи и проблемы использования заказных электронных писем во Франции*

Новые электронные средства связи могли бы еще сильнее изменить организацию работы во Франции, но потребители электронных услуг относятся к ним с осторожностью. Фирма Silverpears предлагает одноименную программу для быстрой текстовой и видеосвязи через Интернет с удобной интеграцией справочников по персоналу предприятий и возможностью работы с мобильных устройств. Это предложение является чем-то средним между программой для связи по IP-протоколу и совместной рабочей средой. Фирма DPII Telecoms & Services разработала Email Track программу для отправки электронной почты, отслеживаемость сообщений в которой приближается если не к удостоверенным актам (ст. 1369 ГК Франции), то к факсу, который с 1960-х гг. имеет доказательственную силу. Преимуществом программы является ее совместимость с IBM Power Systems.

Сложности этого сегмента рынка особенно хорошо иллюстрирует заметка Кристиана Дюбура, директора по маркетингу систем электронного документооборота (СЭД) и АЭ Spark Archives (созданного компанией Klee Group), опубликованная на сайте этой компании, где изложены преимущества электронного заказного письма по сравнению с традиционным.

С тех пор, как декрет 2017–1416 от 28 сентября 2017 г. «Об электронной подписи» имплементировал во французское право положения eIDAS о презумпции надежности электронных копий документов, если они были заверены защищенной зашифрованным сертификатом электронной подписью автора или третьей стороны, обличенной правом заверки (фирмы-сертификатора электронных подписей или нотариуса) и содержит изображение их печатей, многие третьи доверенные лица, которых вытесняет с рынка распространение блокчейна, пытаются продавать клиентам новые услуги по заверению надежной электронной подписью различных документов, в том числе и заказных писем.

К. Дюбур разъясняет в своей заметке, опубликованной на сайте компании Klee group в ноябре 2017 г., правила для обеспечения надежности электронных заказных писем, опубликованные Национальным агентством безопасности информационных систем (ANSSI) еще 1 января 2017 г. Они содержат следующие требования:

* Источники: Services d'envoi recommané éléctronique qualifiés . Critères d'evaluation de la conformité au règlement eIDAS : version 1.0 du 03.01.2017 = Услуги по отправке заказных электронных писем. Критерии оценки соответствия требованиям регламента eIDAS/Premier ministre. ANSSI. 12 p. Accès: https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf; *Dubourg Ch.* La signature électronique est morte, vive la signature électronique qualifié : décret 2017–1416 du 28 septembre 2017. Источник: https://www.spark-archives.com/en/tags/eidas

• использование для создания электронной подписи хеш-кода и метки времени программного обеспечения, отвечающих требованиям «Перечня требований безопасности» (RGS);

• сохранение информации, выданной и полученной при доставке заказного электронного письма;

• обеспечение непрерывности обслуживания клиентов фирмы после прекращения ею деятельности по отправке заказных электронных писем;

• проставление метки времени о дате и часе отправки письма, фиксирование всякого изменения данных при помощи проставления меток времени о них;

• идентификация отправителя при помощи индивидуального электронного сертификата.

Услуга по отправке электронных заказных писем может предоставляться одним или несколькими сертифицированными («квалифицированными») третьими доверенными лицами (принцип технологической матрешки). Разумеется, что в пакет услуг также входит «уведомление отправителя и получателя данных о любых изменениях в данных, которые были необходимы для их отправки или получения»;

К. Дюбур пишет, что передаваемые данные должны быть защищены «с помощью усиленной электронной подписи или усиленной электронной печати третьего доверенного лица, чтобы исключить любую возможность их недетектируемого изменения. Он также пишет, что обязательной является «идентификация получателя перед передачей ему данных». Далее мы увидим, что это не совсем так.

Подчеркнем, что в гражданском праве Франции отправление и получение заказных писем является точкой отсчета времени процедуры по различным искам между физическими и юридическими лицами. Однако, несмотря на то что «Закон о цифровой Республике» 2016-1321 от 7 октября 2016 г. (в соответствии со ст. 44 eIDAS) уравнивает доставку заказного письма по электронной и традиционной почте в доказательной силе, он никак не отменяет принципиальной разницы между двумя этими способами коммуникации. Традиционное заказное письмо может служить для передачи информации между двумя любыми лицами без предварительной о том договоренности, а электронное может быть отправлено физическому лицу на его личный, не профессиональный адрес электронной почты только с его предварительного задокументированного согласия. То есть электронное заказное письмо может использоваться только между двумя юридическими лицами частного или публичного права, в том числе и работающими по модели BtoB (но по всему Евросоюзу), а между юридическим лицом с одной стороны и физическим лицом, выступающим в роли клиента, гражданина, получателя госуслуги, а не сотрудника какого – либо юридического лица, –

только с его согласия. Это положение, защищающее дорогое французам «равенство перед информатикой» резко снижает интерес электронных заказных писем для фирм, работающих по модели BtoC. Понятно, что на практике заказные письма на бумажном и электронном носителе во Франции отнюдь не равноправны.

С технической точки зрения для выполнения требований ANSSI либо фактически создается электронный архив для электронной почты, соответствующий требованиям стандарта ИСО 14641-1 (Французский стандарт NF Z42-013), «Электронные архивы. Технические условия проектирования и функционирования электронной системы для хранения электронных документов», либо периодически обновляется метка времени, связанная с электронной подписью (PAdES LTV), причем эту услугу может представлять группа третьих доверенных лиц. И в случае электронного архива, и в случае регулярного обновления метки времени мы имеем дело с технологической «матрешкой» (электронный репозитарий в сочетании с электронно-цифровой подписью, электронной печатью или иным алгоритмом хеширования), но это не является самой главной проблемой потребителя данной услуги.

В том же нормативном документе ANSSI потребовало, чтобы третьи доверенные лица соблюдали европейский стандарт «ETSI EN_319_401» в отношении обеспечения сохранности доказательств после прекращения услуг в случае прекращения оказания данной услуги, для чего они должны иметь специально разработанный «план по прекращению деятельности». Требования этого стандарта минимальны: сохранить ссылку на документ и данные об его отправке (запись в метаданных или в журнале системы о том, что был отправлен тем-то тому-то тогда-то документ такого-то формата и объема).

При этом сам документ и, что самое главное, его основная характеристика должны сохраняться и быть доступными отправителю в течение одного года, что совершенно недостаточно при минимальной длительности судебных процессов в три года.

При том, что редкий электронный архив действует без серьезной миграции более пятнадцати лет, мы не можем рассматривать регламент eIDAS как нормативный документ архивной отрасли. Сфера его компетенции (сервисы и транзакции в электронной среде) и сроки жизни технологий, которые он регулирует, не простираются дальше, чем сроки хранения документов в текущем архиве юридического лица. Необходимо признать, что все попытки фирм-разработчиков программного обеспечения, в том числе и Klee Group, представить соответствие этому Регламенту eIDAS как преимущество для их электронного архива, являются просто коммерческой акцией.

Реферат В.Б. Прозоровой

Поиск способов сохранения архивов учреждений и служб юридической защиты молодежи (PJJ) во Франции: память завтрашнего дня под угрозой*

Служебная записка «Управление архивами учреждений и служб юридической защиты молодежи (PJJ): память завтрашнего дня», утвержденная и разосланная как циркуляр, была составлена для разъяснения источникам комплектования невыполненного ими циркуляра от 26 мая 2010 г. «Об управлении архивами местных (департаментских и муниципальных во французской терминологии) служб юридической защиты молодежи (PJJ)» . Именно поэтому циркуляр 2017 г. начинается с напоминания руководителям юридических служб на местах о том, что «решение о полном, выборочном хранении или уничтожении содержания бумажных или электронных дел не может приниматься одними только учреждениями и службами. Они должны обязательно обращаться к директорам департаментских архивов – государственным служащим центрального аппарата, работающим при советах департаментов для осуществления научно-технического контроля над государственными архивами, создающимися на территории данного департамента». Далее циркуляр напоминает определение архивов согласно ст. L211-1 Кодекса национального достояния и подчеркивает, что тот же кодекс обязывает государственные учреждения хранить создающиеся в ходе их деятельности публичные архивы. При этом указано, что конкретные методические указания по работе с ведомственными архивами даны не в подзаконной (содержащей регламенты) части Кодекса национального достояния, а в отдельном, полном и подробном документе – «Перечне требований к хранению государственных архивов» (R2GA), опубликованном под эгидой Премьер-министра.

Поскольку ситуация с архивами ювенальной юстиции во Франции столь плачевна, что «Ассоциация истории юридической защиты малолетних» (AHPJM) организовала и провела совместно с Управлением юридической защиты молодежи (DPJJ) министерства Юстиции кампанию «Спасем архивы», авторы циркуляра не надеются, что ювенальные юристы откроют «Перечень требований к хранению государственных архивов» (R2GA) и кратко изложат его основные требования:

• определение сроков ведомственного хранения публичных архивов и их назначения по истечении этих сроков (уничтожение, выборочное или пол-

* Источники: Archives des tribunaux de commerce et des tribunaux de l'ordre judiciaire à compétence commerciale et notamment au registre du commerce et des sociétés : note conjointe № DGP/SIAF/2018/005 du 30 janvier 2018 par le Directeur des Archives de France et de la Directrice de la protection judiciaire de la jeunesse. 4 p.; Circulaire № DGP/SIAF/2010/011 du 26 mai 2010 relative à la gestion des archives des services déconcentrés des établissements relevant de la protection judiciaire de la jeunesse. 10 p.

ное хранение в исторических государственных архивах) совместным решением архивной администрации (в данном случае – департаментского архива) и руководства данных учреждений, согласно статьям ст. L212-2, L212-3, R212-4 и R212-13 Кодекса национального достояния;

• уголовную ответственность (наказание сроком до трех лет тюрьмы и до 45 тыс. евро штрафа) всякого держателя публичных архивов за их уничтожение или недолжное использование согласно статье L212-2 Кодекса национального достояния.

Если архивы были уничтожены не преднамеренно, а «по небрежности», штраф для отдельного чиновника может быть снижен до 15 тыс. евро. Отметим, что для учреждений эта сумма становится вовсе нечувствительным штрафом.

С целью убеждения чиновников ювенальной юстиции не практиковать, как в Средневековье, уничтожение документов в качестве защиты от их недолжного использования или подделки, циркуляр напоминает им, что во Франции действует не только европейский «Генеральный регламент о защите данных» (RGPD), но и французский «Закон об информатике и свободах» от 1978 г., который предусматривает сохранение как аутентичной, так и обезличенной персональной информации в целях исторических исследований по согласованию между фондообразователем (а также его ведомством или правопреемником) и архивной службой страны. При общем отставании государственных учреждений Франции по внедрению «Генерального регламента о защите данных» (RGPD) могут также возникнуть трудности с отбором на временное хранение документов, содержащих персональные данные.

Специальный раздел циркуляра разъясняет ценность архивов учреждений и служб юридической защиты молодежи (PJJ) для изучения истории образования и гражданского общества в целом, сохранения информации о разнообразии методик воспитательной работы с проблемной молодежью, а также для защиты интересов физических и юридических лиц.

Учреждения и службы юридической защиты молодежи (PJJ) – это те структуры, где ведется реальная работа, предписанная решениями ювенальной юстиции. Сохранение архивов этих служб, в особенности, личных дел малолетних правонарушителей, помещенных в эти учреждения (позиция ETS02 перечня), принципиально важно для оценки эффективности существующих правовых норм и воспитательных методик. Циркуляр напоминает, что срок ведомственного хранения для личных дел составляет 5 лет с момента закрытия или по достижении 21 года малолетним правонарушителем, на которого оно заведено.

Циркуляр напоминает, что при передаче дел на промежуточное хранение из подразделений в ведомственный архив учреждения или их группы никакого отбора документов на уничтожение внутри дел производиться не

должно. К сожалению, во французских учреждениях была утеряна традиция делопроизводства, документы внутри большинства дел никак не организованы, дела содержат много дублей. Это провоцирует сотрудников учреждений изобретать собственные теории и критерии отбора.

Такая ситуация тем более опасна, что «Методологические основы для экспертизы ценности и отбора на хранение публичных архивов» (2014), отменившие простые пошаговые хронологические и алфавитные выборки, остались, судя по всему, непонятыми источниками комплектования для архивистов, не получивших специального образования, каких довольно много на низовых должностях в госучреждениях. Полагаем, что большинство непрофессиональных архивистов в принципе не оценит гибкости новых методик и не сможет, в частности, сформулировать четкого мнения о предпочтительности для дел, хранимых в данном учреждении, одного или нескольких из рекомендованных «Методикой» критериев:

• полного сохранения некоторых дел;

• выборка нескольких дел, показательных и типичных для отражения работы с подростками за какой-либо период времени (например, выборка по воспитательному учреждению, по применяемой воспитательной мере);

• выборка по определенному алгоритму или признаку: случайная выборка, выборка дел определенного объема или относящихся к определенным датам по установленным математическим критериям, гарантирующим репрезентативность.

В конечном итоге, выбор все равно будет сделан департаментскими архивистами, поэтому жаль, что не был составлен и распространен циркуляром единый для всей страны перечень, как это делалось в 1980–2010 гг. Написав, что «оказалось невозможным заранее определить обязательные правила отбора на хранение» авторы циркуляра расписались в методическом бессилии, и напомнили, что предыдущий циркуляр 2010 г. «выявил несколько элементов для ориентировки»:

• дела 1945–1980 гг. представляют значительный интерес;

• дела за период действия закона от 2 января 2002 г. «Об обновлении социальной и медико-социальной работы», действующего и поныне, также могут представлять интерес, поскольку должны содержать большое количество информации.

В заключение циркуляра учреждениям и службам юридической защиты молодежи (PJJ) предписывается:

• назначить в каждом учреждении «референта по архивам» (отметим, что составители циркуляра отказались от наименования «корреспондент по архивам», как от заведомо занижающего престиж данной функции) и возложить на него обязанности внедрять циркуляры 2010 г. и 2018 г. в работу подразделений с архивами;

• обязательно провести в каждом учреждении серию совещаний с территориально компетентным департаментским архивом, чтобы определить наиболее подходящие для данного учреждения методы управления электронными и бумажными документами, а также методику их отбора на постоянное хранение;

• регулярно проводить компании по уничтожению и передаче на государственное хранение своих архивов, но исключительно с разрешения территориально компетентных государственных архивов;

Неслучайно циркуляр завершается самым важным для учреждения-фондообразователя разделом «Что будет с этими документами?» Авторы циркуляра настаивают, что акт выделения дел на уничтожение особенно нужен именно для конфиденциальных документов, поэтому его утверждение департаментским архивом является обязательным предварительным условием для приглашения специализированной фирмы-подрядчика для защищенного, лицензированного уничтожения этих документов с последующей выдачей фондообразователю сертификата. Дела, поступившие на постоянное хранение в департаментские архивы, попадают под столетний срок секретности (ст. L 213-2 Кодекса национального достояния), начиная от даты закрытия дела, а до его истечения они могут быть выданы только самому несовершеннолетнему по его просьбе или третьим лицам, если доступ к содержащейся в них информации «не наносит чрезмерного ущерба интересам, защищенным законом» (ст.L 213-3 Кодекса национального достояния).

Чтобы и этот циркуляр не остался неисполненным, составители просят сообщать Архивной службе Франции обо всех сложностях, которые могут возникнуть при его применении.

Реферат В.Б. Прозоровой

Наше цифровое наследие: архивы в перспективе*

Майкл С. Мосс, Тим Дж. Голлинс,
Университет в г. Ньюкасл-апон-Тайне, Англия,
Национальные документы Шотландии, г. Эдинбург

Большинство дискуссий о сохранении наследия мира цифровых технологий ведутся главным образом с технической точки зрения. Основная часть этого обсуждения основана на ложном предположении, что мало что со-

* Источник: *Moss M.S., Gollins T.J.* Our Digital Legacy: an Archival Perspective// Journal of Contemporary Archival Studies. Vol. 4. Article 3. 2017 [Digital resource]. – URL: http://elischolar.library.yale.edu/jcas/vol4/iss2/3

хранится (все поглотит так называемая цифровая черная дыра), быстро изменяющийся формат файлов и постоянное обновление программного обеспечения приведут к тому, что уцелевшее станет трудным, если не невозможным, для воспроизведения.

Эти россказни вкупе с тревожащими историями о высокой стоимости курации в цифровых хранилищах, которым доверяют архивы, пугали и отвлекали внимание от главных вопросов архивной науки: оценки (что хранить), определения секретности (идентификации материала, который не может быть раскрыт по этическим или юридическим причинам), получения доступа. Пути реализации этих основных принципов архивоведением с целью реакции на «сверхновую звезду» цифрового материала, который действительно выживет, и определит наше цифровое наследие.

Многие в архивном сообществе медлили признавать, что мир цифровых технологий существенно изменил методы управления документооборотом и ведения архивов только из-за способа, каким это теперь работает. Электронная почта по умолчанию сохраняет каждое сообщение, которое мы посылаем или получаем. Почту больше не держат в чем-то, что напоминает «манильскую картонную папку», но она хранится в системе. Даже если письма уже удалены, они, как правило, все еще «где-то там». В аналоговом мире нужно было принять сознательное решение, чтобы сделать копию письма.

Подшивка и современная регистрации документов еще в эпоху Ренессанса в определенном смысле была систематизированы Лукой Пачоли в его труде «Summadearithmetica, geometria, proportioni и proportionalita», в главе «Decomputisetscripturis» («Подробности расчета и записи»), изданном в 1494 г.

К началу XIX в. на гражданской службе в Соединенном Королевстве важной целью было обеспечить легкодоступность поиска и извлечения документа из последовательных записей реестра или папок архива.

С ростом бюрократии система учета и ведения записей стала более громоздкой и сложной. Однако у них были строгие правила по поводу того, что необходимо отбросить, а что – сохранить, что определить как значительное, а что – как несущественное. Они организовали хорошо построенные серии и планы файлов архива, наладили процесс регистрации под контролем секретарей, которые не зависели от основной деятельности и отвечали за проверку документов или файлов. Для отдельного государственного служащего, создающего документы, было чрезвычайно трудно избежать или обойти систему, ее неотъемлемый процесс проверки и процедуры учета. Не только документы и письма должны были быть подготовлены и написаны в стандартной форме, но даже неофициальные беседы подвергались протоколизации. Дублирование документов было дорогостоящим и имело свои пределы, затрудняло разработку систем учета. До появления ксерокса копировальные работники могли делать только три-четыре разборчивые копии на печатной машинке.

Бумажные системы учета записей были долговечны как в отношении самих документов, так и административных структур, которые создавали, управляли и вели учет. «Смерть» бумажных документов редко происходила, за исключением случаев, когда организация прекращала работу, как, например, министерства военного времени. Их структура реестров была удивительно устойчивой и постоянной и порой существовала более сотни лет. С появлением сетевых персональных компьютеров и Интернета во многих странах реестры и системы, которые ранее были внедрены, отменили. Компьютеры служили той же цели, поскольку они хранили записи, хотя и не в картотеках, напоминавших бумажные файлы.

Во имя эффективности были сокращены должности секретарей. Менеджеры, большинство из которых не были знакомы с системой регистрацией, начали создавать свои собственные файлы для документов и электронных писем. Справочные папки-досье исчезли очень быстро. Все, что осталось, – это почтовые заголовки, которые, как правило, дают мало сведений о содержании или связи с предыдущим обменом сообщениями. Электронные письма начали заменять телефонные разговоры, которые в государственных учреждениях Соединенного Королевства всегда протоколировались, если были значительными.

По мере сокращения бюджета и роста скорости сделок оставалось мало времени для размышлений. Чиновники начали реализовывать политику через быструю электронную почту. В качестве меры предосторожности все больше и больше адресатов получают копии сообщений. В результате, такой обмен оставляет свой след на многих серверах получателей. Последствием этого стало переполнение серверов и жестких дисков огромным количеством материала, который мы могли бы охарактеризовать как ослепительный взрыв информации, «сверхновую звезду».

В последнее время появление инструментов и среды для совместной работы создало еще более подвижный процесс, в котором сама концепция документа была подорвана. Сообщения электронной почты теперь связывают ссылки с общими рабочими областями или корпоративными сайтами, а программное обеспечение Wiki позволяет установить, где, в какое время и какое слово ввел пользователь. Принципы авторства становятся спорными.

Эта новая среда расстраивает архивистов. Но во всей этой ситуации при этом упускается нечто действительно жизненно важное: систематизация документов не исчезла, она просто трансформировалась. Установленная человеком система, описанная выше, была не только системой учета, но и системой создания документации. Как только мы признаем это, то сможем переоценить взгляды на систему электронной почты, инструментарий и среду сотрудничества и проанализировать, что было потеряно при быстром переходе на цифру. Программы электронной почты имеют механизмы для

хранения и нахождения содержания сообщений, а элементов для коммуникации с адресатами и того больше. Они не имеют некоторых контролирующих функций канцелярии, но это не катастрофично. Большое преимущество состоит в том, что они работают на пользу предприятий, помогая людям создавать и многократно использовать информацию в интересах бизнеса.

Преимущества Электронного документооборота и Европейской системы управления справочными данными (ERDMS), часто нахваливаемые сторонниками техноцентричной замены реестров, автору статьи пока сложно ясно сформулировать. Он считает, что на данный момент база EDRMS – это место, где записи будут «похоронены» (в отличие от бумажных реестров). Что еще хуже, как думает автор, эти EDRMS требуют значительных усилий от каждого отдельного пользователя, чтобы вносить туда данные.

Со времени культовой статьи специалиста по электронным документам из Калифорнии Дж. Ротенберга, опубликованной в 1995 г., архивное сообщество зациклилось на технических проблемах цифрового сохранения. Разработка эталонной модели Открытой архивной информационной системы (OAIS) и последующих стандартов ISO служили лишь укреплению этого технического уклона и предубежденности в отношении хранения.

Совсем недавно разработка концепции «бережливого хранения» в Национальном архиве Соединенного Королевства, отражающей начала демонстрировать, что многие из аспектов этих технических проблем неуместны. Ее авторство принадлежит Тиму Голлинсу. Он создал ее на основе работы Дэвида Розенталя (сотрудник Библиотеки Стенфордского университета) и отразил в ней мало цитируемую работу Криса Расбриджа (директора библиотеки Университета Глазго).

В то время как существует много разнообразных угроз успешной курации цифрового материала, благодаря маркетологам создается впечатление, что неизбежное технологическое (речь о программном обеспечении или форматах данных) устаревание является главной угрозой. Это порождает веру в то, что единственный способ успешно перейти на цифровое хранение заключается в инвестировании капитала в крупную, технически сложную, дорогостоящую и сложную в эксплуатации интегрированную цифровую систему хранения.

Используя принцип парсимонии, Голлинс утверждает, что, хотя угроза технологического устаревания реальна в некоторых конкретных случаях, более неминуемой угрозой являются некачественные сбор и комплектование плюс неспособность обеспечить безопасное и надежное хранение исходного материала. Применяя принцип бережливости к цифровому хранению, учреждения могут найти пути продвижения вперед, которые поэтапны, контролируемы и достигают цели сохранения цифрового материала для следующего поколения.

Архивы теперь имеют опыт фактической курации цифровых документов. Они обнаружили, что проблемы заключаются не в глубоких аспектах устаревания формата файла или в дебатах между эмуляцией и миграцией, а в тривиальных мелочах человеческой непоследовательности в использовании системы, в которой создали документы. Человеческий фактор делает документ достаточно неустойчивым элементом в структуре, чтобы сломать или засорить идеалистически построенные автоматизированные рабочие процессы. Прочные и терпимые к изменению технологические процессы трудно организовать. Их успех часто кардинально зависит от упрощения задач, метаданных (см. ниже) и предположений об обрабатываемых отчетах. В этой области меньше – это больше. На первый план должна выйти концепция бережливости – только для того, чтобы сделать минимум, необходимый для непосредственного управления.

Нужно понять, что большинство трудностей является не результатом технологических процессов, а частью таких проблем, как описание и представление материалов для использования. Еще раз, не контейнер представляет собой проблему, а его содержание.

Традиционным ответом на такой вызов со стороны многих архивариусов стали применение и генерирование метаданных. При этом мало кто задумывался о том, как их можно эффективно и без особых усилий внедрить в повседневную работу занятых сотрудников.

Что такое метаданные? Классическое определение утверждает, что это – «информация об информации». В некотором смысле это, конечно, неправильное употребление термина: данные – это просто данные, которые должны обрабатываться какой-то вычислительной или информационной системой.

Действительно, материал, который рассматривается в качестве метаданных одной системой, может быть основным для другой системы (например, заголовки электронной почты, не представляющие интереса для обычного пользователя, являются основными данными, созданными и обработанными базовыми системами связи электронной почты, содержание сообщения является единственным полем множества).

Если яснее, то метаданные, о которых здесь говорится, называются «описательными метаданными», т.е. такими, которые описывают или дополняют отдельные экземпляры содержимого основных данных (описание архивного каталога, запись о поиске). Традиционно в архивном и библиотечном сообществах такие описательные метаданные готовятся вручную. Это источник проблем, с которыми сталкивается архив в процессе перехода на цифру. Ручные записи не будут считываться.

На всем протяжении процесса надо сосредоточиться на том, что́ может быть лучше всего охарактеризовано как работы промышленного масштаба, так как мы имеем дело с данными, генерируемыми машинами.

Автор на протяжении всего эссе надеется продемонстрировать, что некоторые навыки, освоенные в аналоговом мире, могут быть применены в цифровой среде. В информатике ученые, размышляя об эффективных поисковых системах, используют понятия «особенности» или «значительные свойства» объекта. Многих удивляет, что они эквивалентны понятиям в архивном деле. Автор считает, что открытость к междисциплинарным связям поможет найти решения многих из обсуждаемых здесь проблем в области цифрового архивирования.

Есть вопросы исследования, на которые может ответить только полностью изначально цифровая коллекция (где полностью тексты записей доступны для компьютерной обработки) и на которые невозможно ответить, пользуясь эквивалентной бумажной коллекцией документов. Некоторые факты могут автоматически извлекаться из цифровых записей, включая даты, имена и адреса. Теоретически, отчеты могут быть составлены с использованием инструментов, разработанных на основе многолетних исследований в области обработки текстов и поиска информации. Ни один из этих вопросов не является тривиальным, поэтому проблемы применения этих методов к разнородным данным, которые формируют архивные документы, значительны.

Автор предполагает, что такие инструменты находятся в пределах досягаемости, если архивисты и программисты будут сотрудничать. Инвестиции в такие прагматические и практические научные разработки, несомненно, преуспеют в предоставлении архивистам инструментов, в которых они нуждаются. Чтобы извлечь выгоду из этих событий, архивное сообщество должно радикально изменить свой образ мышления.

Недавно многие члены архивного сообщества думали, что могут влиять на управление информацией и диктовать передовые методики, начиная «с колыбели и кончая могилой» документа. Они настаивают на том, чтобы организации внедрили системы электронного документооборота (EDRMS). Руководители коммерческих организаций возмущаются таким вмешательством, если только это не включает дополнительных затрат на офис или подразумевает окупаемость инвестиций, чего практически невозможно достичь, поскольку архивное сообщество не имеет опыта проектирования систем для потребностей бизнеса. Проблемы архивистов будут иметь относительно небольшое влияние, поскольку такие системы существуют для повышения эффективности функционирования организации. Эта статья утверждает, что архив должен делать то, что необходимо в первую очередь для пользователей.

Когда становится очевидным, что большие фрагменты цифрового контента «выживают» и остаются читаемыми, решения должны приниматься о том, что из всего объема сохранять. Выбор может колебаться от решения сохранить все зависимое от технически практичного, но дорогостоящего и чреватого юридическими рисками процесса, до выбора лишь некоторых категорий документов.

Если выбор должен быть сделан, он должен быть осуществлен на какой-то рациональной основе. Однако оценка категорически не может быть такой же, как прежде. В бумажном мире, где записи хранятся в папках, это было относительно легко, поскольку структуры, используемые организациями для навигации по своим записям, могли использовать и в качестве основания для выбора (например, реестровые индексные книги и планы файлов). Работа с частными документами более трудная, так как для их организации часто не хватало структуры, хотя объем не был большим.

Первая проблема заключается в том, что записи, которые «выживают», становятся легально доступными. Это не вызывает беспокойства в государственном секторе, который обычно пользуется защитой. Даже здесь есть опасения, которые разделяет и частный сектор относительно документов, которые неуместны для раскрытия, но переданы в архив. Анализ разнородных материалов на определение «секретного контента» или «деликатного характера» занимает много времени и стоит дорого, как и его хранение в течение длительного времени. Анализ затрат и выгод является неотъемлемой частью уравнения при любом рассмотрении сохранения и обработки цифрового наследия.

Во многих областях оцифровка незаметно вынуждает к созданию новых бизнес-моделей. Первая проблема тут состоит в том, что у нас есть большие банки и сети магазинов и небольшие независимые учреждения, которые не могут позволить себе капиталовложения или преимущества ценообразования гигантов.

Вторая проблема заключается в том, что документы коренным образом изменили свой характер. Термин «однодневка» часто используется для описания элементов информации, которые предназначены только для использования в течение короткого времени и, таким образом, в долгосрочной перспективе незначительны. Во многих новых цифровых средах разрушилось понятие короткого периода полезности и долгосрочного существенного значения.

Так, твиты Дональда Трампа – полезный пример цифровых объектов, первоначально предназначенных как краткосрочные, которые теперь должны рассматриваться как имеющие огромную долгосрочную значимость. Автор считает, что этот распад является одним из многих неожиданных последствий появления новых цифровых форм информации. Более того, причина, по которой такие последствия являются неожиданными, проистекает из ошибки атрибуции, которая рассматривает цифровые материалы как цифровые суррогаты бумажных эквивалентов.

Само слово «документ» иллюстрирует это в термине «электронные системы документооборота». Твиты, посты Facebook, мгновенные сообщения, видео на YouTube и веб-сайты просто не ведут себя как документы или не имеют их свойств. Учитывая, что экономические издержки, связанные с сохранением всего, неприемлемо высоки, как выбирать то, что сохранить? Чтобы сделать это, как и многое другое, связанное с цифровыми технологиями, придется

доверять людям с современными навыками, которые понимают лишь немногие из нас. Когда мы помещаем банковскую карту в банкомат вдали от дома, мы доверяем некоторым сложным математическим системам, чтобы проверить, что у нас достаточно кредита, чтобы удовлетворить транзакцию, и что банк, которому принадлежит аппарат, не обманывает. Примечательно, что нужно доверять такому же математическому моделированию, когда мы входим в мир цифрового архивирования. Нам нужно моделировать материал с помощью инструментов, которые только сейчас находятся в процессе разработки.

Можно использовать цифровые инструменты криминалистов, чтобы распутать преступление, поскольку их компоненты были созданы для этой цели, и обратиться к методам графического и сетевого анализа, разработанным полицией и разведывательными сообществами для анализа ссылок, связей и следов информационного брака, ведущих в никуда (например, в электронном письме, чтобы идентифицировать людей, которые были скопированы в сообщение, но не должны там быть).

Необходимо иметь возможность использовать новые интегрированные службы для выявления дубликатов и удаления копий, которые можно безопасно удалить, т.е. копий без аннотаций. С точки зрения перспективы в архивировании, необходимо срочно продумать критерии отбора материала для постоянного хранения. В прошлом архивисты прятались под покровом воображаемой объективности, но на самом деле есть тенденция не оставлять на хранение то, что никто никогда не станет использовать. Ранее традиционно останавливали внимание на документах, связанных с политикой и стратегией, но это уже невозможно даже в аналоговом мире.

Всплеск интереса к семейной истории означает, что многочисленное сообщество пользователей хочет, чтобы контент пополнялся именами. Имена и адреса представляют проблему. Попытка найти зерно полезной информации среди гор песка будет трудной, но цифровые инструменты криминалистики начинают добывать некоторые свойства, такие как длина документа или количество и типы слов. Они могут предложить подсказки для экспертизы. Все это, в сочетании с заменой меток электронной почты, расшифровкой стенограммы цифрового видео и признанными значительными политическими заявлениями из твитов означает, что мы будем копить гораздо больше, чем раньше, возможно, целых 20%, а не 5%, как это традиционно имеет место в аналоговых контекстах. Само по себе, это добавит затрат на обработку и хранение. Пока еще нет никакого решения этой проблемы – только осознание того, что нынешние методологии оценки безнадежно неадекватны.

Десять лет назад британский социолог Майк Фитэрстоун пригласил архивистов принять этот вызов, когда написал: «Как найти решение о том, что собирать, что хранить, что выбросить и что должно быть каталогизировано?»

После того, как архив принял решение о сохранении цифрового контента, перед ним встает еще больший вопрос: к чему можно смело допускать поль-

зователей? Архивное сообщество в значительной степени упускает из виду деликатность и даже право интеллектуальной собственности (IPR) цифровых материалов, поскольку архивисты поглощены техническими проблемами.

В цифровую эру «секретность документа» уже далека от простой. Она включает в себя понимание о взаимосвязи между контролем и демократией, которая до сих пор вызывала противоречивые отклики. На это накладываются дополнительные соображения, касающиеся идентификации и сохранения подробных доказательств, позволяющих восстановить справедливость при уважении всеобщего права на неприкосновенность частной жизни и информации.

За последние десять лет конфиденциальный характер личной информации привлек внимание СМИ. Разоблачения Эдварда Сноудена в 2013 г. о деятельности Агентства национальной безопасности США и обнародование документов вызвали бурю протеста во всем мире против того, как органы безопасности во многих странах собирают данные о физических лицах. После разоблачений Сноудена японское правительство провело драконовский закон, устанавливающий «безжалостные штрафы и наказания для лиц, раскрывающих или ищущих информацию, которую правительство, без какого-либо независимого надзора, объявляет секретной, согласно стандартам, оставшимся неопределенным».

Это также отозвалось протестами. Такие проблемы стали более острыми из-за сообщений о том, как компании собирают и анализируют персональные данные для манипулирования общественным мнением, в частности, на референдуме в Великобритании (Brexit) и выборах в США. Совпадение разоблачений Сноудена 2013–2014 гг. и пугающего романа Джорджа Оруэлла не было упущено комментаторами, которые вызывают в воображении кошмарный мир Старшего Брата, помноженные на квантовые вычисления, какие даже Оруэлл никогда не мог себе представить. Оруэлл был созвучен Уильяму Гибсону, который в 1984 г. написал роман «Нейромант» и придумал термин «киберпространство», предсказав, где миллионы операторов собирают данные из вездесущих компьютеров. Отказавшись от своей карьеры в органах безопасности, Эдвард Сноуден стал защитником права на конфиденциальность данных и призвал к фундаментальному переосмыслению роли Интернета в жизни и законов, которые защищают его. Он не легкомысленный критик спецслужб и признает, что они делают полезные вещи, которые должны быть проведены в нестабильном мире. Однако его беспокоит, какой путь выбирают крупнейшие интернет-провайдеры, позволив скрутить себе руки, и открывая ресурсы личных данных, которые им доступны.

Персональные данные стали предметом торга для аналитических компаний. Задолго до разоблачений Сноудена в Великобритании информационный комиссар, который осуществляет надзор за защитой данных, уполномочил подготовить всеобъемлющий отчет об «Обществе слежения» и предупредил о своих опасениях. Отчет комиссару по вопросам информации о слежении в Интернете начинался словами: «Мы живем в обществе

наблюдения. Бессмысленно говорить об "Обществе слежения" в будущем времени. Во всех развитых странах мира повседневная жизнь заполнена столкновениями со слежкой, не просто с утра до вечера, а двадцать четыре часа семь дней в неделю».

Вместо того, чтобы критиковать общество слежки как «нечто зловещее, с привкусом диктатуры и тоталитаризма», авторы охарактеризовали его в вэберических терминах, таких как «прогресс в направлении эффективного управления» и естественное продолжение «современности».

Государство документировало сведения о людях не менее двух тысяч лет. Вместе с тем в докладе признается, что цифровая технология позволила обеспечить быстрый обмен информацией с присущей ей опасностью «расползания функций», поскольку данные, собираемые для одной цели, могут легко использоваться для другой. Автор рекомендует не оставлять на усмотрение отдельных лиц возможность оспаривать ненадлежащее использование личных данных: «появление современного общества слежки требует, чтобы мы перешли от самозащиты частной жизни к ответственности обработчиков данных».

После утечки данных о начислении пособий на детей и доходах таможни в Великобритании в октябре 2007 г. в Палате общин Комитет внутренних дел приступил к большому расследованию. Комиссар по информации Великобритании предпринял шаги, чтобы ответить на опасения Комитета, издав «Руководство по оценке воздействия на конфиденциальность» и опираясь на базовые принципы защиты приватности и неприкосновенности частной жизни. Тем не менее, озабоченность в обществе усилилась после широко распространенных утверждений о манипулировании демократическим процессом с использованием сложной аналитики данных для получения голосов колеблющихся избирателей.

Совсем недавно в ответ на протесты после разоблачений Сноудена, Комитет по разведке и безопасности британского Парламента опубликовал всеобъемлющий обзор ряда интрузивных возможностей, имеющихся в распоряжении разведывательных органов Великобритании, в которых, защищая принципы слежки в условиях демократии, они рекомендовали «заменить всю правовую базу, которая применяется к спецслужбам».

Цель такого всеобъемлющего пересмотра системы управления слежением состояла бы в повышении прозрачности работы и контроле за деятельностью разведывательных органов и, таким образом, в улучшении понимания общественностью их работы и укреплении доверия к ней.

Совместное заключительное мероприятие финансируемого Европейским союзом проекта «DEMOSEC: демократия и безопасность» состоялось в конце октября 2014 г.

На одном из заседаний рассматривалась эта центральная тема: в контексте «контроля и демократии» контролируемый доступ к субъектам и от-

ветственность лежат в основе взаимоотношений между гражданином и лицами, занимающимися сбором информации.

Субъект персональных данных имеет право знать, какие данные собираются о нем и кем, как обрабатываются и кому раскрываются. Кроме того, они имеют право проверять данные, обеспечивать их точность и подавать жалобы независимому надзорному органу, который может проводить расследования от их имени. Заявление может показаться неубедительным и согласуется с мнением Тима Бернерса Ли, одного из основателей всемирной паутины, который призвал к новой модели конфиденциальности в Интернете: «Я хотел бы, чтобы мы построили мир, в котором я имею контроль над своими данными. Я могу продать их, и мы можем договориться о цене, но что еще более важно у меня будет юридическая собственность на все данные обо мне».

Тем не менее, не все согласны, а некоторые утверждают, что мы существуем в мире пост-приватной жизни. Джеймс Дер Дериан из Университета Сиднея определяет «намного более тревожащую картину приближающейся современности, в которой антиутопические видения Оруэлла и Гибсона сходятся в мире Uber-слежки, уменьшая приватность жизни и минимизируя инакомыслие». Картина современности перекликается с образами общества Вебера, который видел процесс рационализации, то есть перехода общества от традиционного состояния к современному, что отражает и широкое разочарование, которым легко манипулировать.

Существует другая сторона вопроса, в достаточной мере мрачная. Она касается доступа к личным документам ради исправления судебных или исторических ошибок. Есть много примеров, таких, как файлы Штази, секретной полиции бывшей Восточной Германии, которые в настоящее время доступны в Интернете. На первой странице своего веб-сайта они заявляют: «Чем лучше мы поймем диктатуру, тем лучше мы сформируем демократию».

Это смелое утверждение предполагает, что если постигнуть антиутопию, есть надежда на лучшее будущее, что недалеко уходит от призывов DEMOSEC. В Великобритании разоблачения о футбольной катастрофе Хиллсборо в 1989 г., когда 96 человек погибли и 786 были ранены, зависели от обнаружения доказательств, противоречащих официальной версии событий, предоставленной полицией.

Кроме того, обнаружение масштабов жестокого обращения с детьми и их эксплуатации в последнее время, будь то сексуальное надругательство или принудительное удаление детей от их родителей, справедливо привело к ожиданиям привлечения к ответственности учреждений и правонарушителей (например, в Великобритании Независимое расследование случаев сексуального надругательства над детьми – IICSA). Заявления о злоупотреблениях могут расследоваться только в том случае, если имеются соответствующие записи.

В Австралии, как и во многих других странах, большая часть нарушений и жестокое обращение имели место в детских домах. Огромный национальный проект «Find and Connect» определяет, где хранятся документы, которые могут принести пользу пережившим обиды, которые надо исправить. Необходимость сохранения личных данных, которые затрагивают слабых и уязвимых, и в то же время защиты тех, кто находится у власти, от необоснованных обвинений, согласуется с концепцией подотчетности владельцев данных и управления базами. Это не имеет ничего общего с преувеличенными взглядами на мир пост-приватности, где цели всегда оправдывают средства.

Однако это не так просто. Имеется двусмысленность в желании сохранить конфиденциальность частной жизни при том факте, что миллиард человек подписался на Facebook, начиная с 2004 г., где многие легко делятся личной информацией.

Некоторым не приходит в голову, что небезобидные организации также промышляют сбором данных. Встает огромная дилемма. Мы хотим, с одной стороны, защитить частную жизнь, с другой – чтобы достоверные записи хранились, и можно было исправить ошибки, защитить невинных. Плюс мы хотим использовать возможности Интернета, чтобы контактировать с людьми по всему миру.

Эта дилемма не может быть снята только введением наблюдения или хранением записей. Речь идет о правительстве и руководстве. Власти устанавливают границы, в которых действуют службы безопасности, и правительства должны быть привлечены к ответственности, если террористы осуществляют свои действия. Именно правительства, а в некоторых случаях и международные соглашения предписывают законодательную среду, в которой организации государственного и частного секторов могут использовать персональные данные. В случаях жестокого обращения с детьми виноваты те, кто управлял детскими домами и позволял педофилам оставаться незамеченными и безнаказанными.

Какими способами социальные сети используют наши данные и как уполномоченные компании обеспечивают безопасность, соответствуя законам стран, где они предоставляют свои услуги. Для властей и лиц, отвечающих за надлежащее управление данными необходимо задать критерии управления для контроля, который сделает ответственность реальной даже спустя долгое время. Широкая огласка нарушений в области безопасности и разоблачения Сноудена привели к ужесточению правил конфиденциальности, в том числе к введению в Европейском союзе «права на забвение», обозначающего право редактировать и удалять со страниц сайтов и соцсетей историю своих записей.

Регулирование возлагает бремя ответственности на поставщиков данных. Зачастую предусмотрены суровые наказания за их несоблюдение.

Когда документы передаются в архив, есть четкое понимание, что они будут обнародованы.

Изначально-цифровые документы появляются с теми же ожиданиями, что соотносимо с текущими планами Национального архива Великобритании.

После того, как контент в Интернете будет повсеместно индексироваться веб-поисковыми системами, его содержание станет легко обнаружить таким образом, как в аналоговом мире было невозможно. Это ставит архив в центр дискуссии о конфиденциальности, независимо от того, понимает это большинство архивистов или нет. Архивы сталкиваются с серьезными препятствиями в предоставлении доступа к контенту на фоне ужесточения режимов конфиденциальности и ужесточения общественного отношения к ненадлежащему раскрытию информации.

Совет библиотечно-информационных ресурсов США (Council on Library and Information Resources, CLIR) предупредил архивы не принимать цифровой контент, если он не был изучен на предмет такой «чувствительности», потому что после того, как материал сдан на хранение, архивы подвергаются уголовной ответственности и могут быть привлечены для судебного разбирательства. Создатели документов и архивы подпадают под различные виды юрисдикции и отвечают за различные аспекты процесса. Тем не менее, в какой бы плоскости не лежала ответственность, остается вопрос о том, как это можно осуществить, если для передачи в архив доступна большая коллекция материалов в самых разных форматах?

В аналоговом мире, где документы были организованы в папки и по умолчанию существовала корзина для мусора, оценка секретности сводилась просто к проверке содержания и ограничивалась либо исправлением оскорбительных элементов, либо удалением частей, например, страниц из документов. Только в крайних случаях, когда упоминалось очень много имен, закрывались целые папки.

Наиболее секретным содержанием является личная информация, которая в настоящее время закрыта в большинстве европейских стран в течение от 100 до 110 лет. Если возраст лица неизвестен, то для несовершеннолетних он закрывается на весь срок, а для лиц, которые считаются старше шестнадцати, – на 80 или 94 года. Есть веские причины для таких длительных периодов закрытия. Он защищает человека, особенно, если материал может повлиять на его здоровье и благополучие, и помогает предотвратить кражу личных данных, используемую преступниками и, к сожалению, некоторыми сотрудниками правоохранительных органов.

Европейские страны уважают взаимность, поэтому такое закрытие применяется и к личной информации о лицах, которые не являются европейскими гражданами, поскольку европейские страны ожидают, что и другие стороны будут держать данные закрытыми в течение аналогичных периодов, особенно если их разгласила конфиденциально третья сторона.

В любом случае при массовом глобальном обмене информацией мы движемся к международным конвенциям, которые уже существуют для некоторых категорий данных, например, Женевской конвенции.

В цифровой реальности шансы на утечку личной информации увеличиваются. Это может оказаться даже незаметным и неявным выводом из последовательности источников данных, которые могут быть объединены в так называемые «мозаики» (такая практика используется в журналистских расследованиях или спецслужбами).

Несколько удивительно, что предмет, который, по-видимому, хорошо понятен и очевиден для всех, трудно конкретизировать. Он может касаться личных, институциональных, политических вопросов и вопросов национальной безопасности и других коннотаций в зависимости от контекста. В правительстве Великобритании в Законе «О свободе информации» делается попытка определить его, разделив типы документов по секретности на двадцати четыре исключения из файлов: «национальной безопасности» (сектор 24), «ущерб международным отношениям» (сектор 27) «личная информация» (сектор 40), «коммерческая информация» (сектор 43).

Это кодирование на самом деле не имеет отношения к сути, поскольку в некоторых случаях оно предполагает, что лишь предмет документа делает его секретным. Но это не единственный фактор.

Рассмотрим, например, текст, описывающий возможности военной техники.

Если он создан и опубликован журналистом и скопирован в правительственную систему для справки, он не является секретным. Вместе с тем тот же текст, подготовленный госслужащим, потенциально может быть чрезвычайно секретным лишь в силу полномочий, предоставленных автору. Из этого следует, что авторство (кто сказал) тоже является аспектом для определения статуса секретности.

Рассмотрим другой текст, описывающий коммерческое соглашение со значительными рыночными последствиями для заинтересованных компаний. В этом случае до официального анонса документ является секретным, а после объявления – становится общеизвестным фактом. Аналогично в контексте государственного сектора экономическая или торговая политика в период ее создания может быть весьма засекреченной, однако после опубликования или принятия решений она вообще не является таковой. Из этого мы видим, что время (когда было сказано) является тоже значительным аспектом.

Рассмотрим еще один текст, касающийся сделки по продаже оружия другой страной. Если в страна установлена современная либеральная демократия, с которой есть известные дружеские отношения, то сделка носит характер малой секретности. Однако если она управляется династическим и репрессивным режимом, с которым отношения сглажены компромиссами и поэтому возможны, характер сделки может стать высоко секретным.

Из этого следует, что другие вовлеченные стороны (кому было сказано) – еще один аспект, который необходимо учитывать.

Наконец, рассмотрим текст XVII века, в котором описываются религиозные или этнические меньшинства. В контексте исторического документа язык и формулировки (хотя в настоящее время они и предосудительны), как правило, не считаются особо чувствительными. В контексте современного документа будет верно обратное. Из этого выходит, что дух времени в публикации (контекст, в котором было сказано) является чрезвычайно важным.

Еще один дополнительный фактор играет роль в определении секретности – юрисдикция, под которой проводится оценка. Секретность, определенная в Законе Великобритании о свободе информации, представляет собой лишь одну из многочисленных кодировок во всем мире. Таким образом, секретность может рассматриваться как предмет, зависящий от того, кто, что, кому, когда и в каком контексте сказал и под какой юрисдикцией. Люди легко могут обнаружить и распознать эти нюансы, определить контекст, когда смотрят на документ или текст. Однако когда компьютеры обрабатывают цифровые материалы, это может оказаться не так просто.

Способность архивов в будущем справляться с «промышленными» объемами цифровых документов зависит от развития автоматизированных процессов. Оценка секретности, в частности, является исключительно человеческим вопросом, который нелегко поддается индустриализации. Поэтому автор считает, что архивы должны разработать инструменты оказания помощи, позволяющие людям справляться с объемом материалов, подлежащих пересмотру.

Общими инструментами обработки информации (например, в корпоративных поисковых системах, инструментах электронного обнаружения и инструментах судебно-медицинской экспертизы) обрабатывается либо текстовое содержимое записи, либо метаданные такого документа (например, хранящиеся в EDRMS или зарегистрированные на сайте SharePoint или в виде файла на общем диске). Известно, что метаданные, сформированные во время создания документа, ненадежны, частичны или часто почти полностью отсутствуют.

Только один из шести аспектов, которые управляют секретностью записи, скорее всего, будет явно содержаться в тексте документа, но какой конкретно? Кто-Кому-Когда – эти аспекты могут частично присутствовать в исходных метаданных, но в целом нет. А если контекст отсутствует?

Недавняя работа автора, спонсируемая Фондом Университета Глазго, Национальным архивом, ITAAU (IT as a Utility Network+), Национальными документами Шотландии и Правительством Уэльса, подтвердила наличие этих проблем и сформировала контекст для исследований в этой сложной области.

Учитывая это положение, каким можно представить себе инструмент будущего для определения секретности цифровых документов?

Прежде, чем говорить о вспомогательном инструменте оценки цифровой секретности, рассмотрим другие типы инструментов, которые обрабатывают текст, чтобы помочь пользователям находить информацию или принимать решения на основе содержания документов, и то, что эти инструменты имеют общего.

Многие современные инструменты такого рода предварительно переводят документы, над которыми они работают, в форму, известную, как «мешок слов», где каждый документ представлен в виде списка слов с подсчетом количества раз, когда слово появляется в тексте. Вдобавок, предварительная обработка может фиксировать, где в документе стоит каждое слово (например, путем подсчета слов или букв от начала документа). Эти фундаментальные представления появились в результате десятилетий исследований в области поиска и извлечения информации.

Образы, используемые при поиске в Интернете, являются расширениями того, так как в дополнение к словам и их положению (или близости, которая вычисляется из положения) они рассматривают способ, которым веб-страницы связаны друг с другом в сети ссылок на другие страницы. Для того чтобы эти образы работали хорошо, необходима достаточная плотность ссылок, а их связь должна каким-то образом представлять человеческое понимание ценности связанной страницы. Это значение может быть не более, чем «вот страница по теме X», но агрегация этих ссылок дает некий смысл. Именно это закодированное оценочное суждение используют большинство веб-поисковых систем.

К сожалению, в сборниках документов, которые составляют отчеты большинства организаций, даже такие связи, хоть и существуют в определенной степени, но не имеют достаточной плотности, чтобы быть пригодными к использованию аналогичным образом.

Все эти факты о документе – количество слов, положение, ссылки и так далее – известны как «свойства». Таким образом, мы можем рассматривать отображение документов в этих инструментах как набор конкретных свойств, по которым пытаются уловить значение документа в контексте конкретной проблемы (веб-поиск или электронное обнаружение).

Для этих представлений, образов и признаков общим является фундаментальный акцент на предмете, на том, о чем идет речь в тексте. Как автор говорил ранее, этот аспект касается секретности лишь частично. Эти инструменты, как правило, не улавливают и не используют какие-либо свойства документа или его контекста, чтобы понять «Кто-Кому-Когда-Что» в более широком смысле. Если создавать инструменты, помогающие людям в определении секретности документа, то нужно обратить взгляд на все деликатные аспекты и понять, какие еще свойства документов эти новые инструменты должны использовать.

Какие характеристики могут определять недостающую информацию? Какие свойства информации изучают и используют люди для принятия решений о секретности?

Сначала это может показаться простым вопросом для понимания. Почему бы просто не спросить рецензентов. Как и многие люди, которые используют свой накопленный опыт для принятия тонких решений, рецензенты редко могут сформулировать в целом, на чем они фокусируются при оценке проверяемых документов. Для того чтобы даже начать понимать, что происходит, требуется много подробных и тщательных антропологических наблюдений, опросов и анализ.

Несмотря на потребность в таком исследовании, уже можно сделать некоторые независимые успехи, исследуя поставленные вопросы «Кто-Кому-Когда-Что» и контекст сказанного.

Представим компонент инструмента, который мог бы примерно оценить авторство документа или электронной почты, изучая шаблоны в заголовках, колонтитулах или приветствии. Такие методы разработаны относительно недавно в области информатики, но их концепция знакома любому архивисту. Аналогично, учитывая печально известную ненадежность автоматической датировки в метаданных документа, можно было бы разработать систему автоматизированной эвристики для определения «наиболее вероятной» даты путем изучения и сопоставления дат в документе с датами, содержащимися в метаданных.

Таким способом уже проделана работа по установлению и определению «речевых актов» в президентских отчетах в США. Как только она будет завершена, можно говорить о дальнейшей автоматизации структурного анализа для извлечения списков рассылки и других аналогичных полезных индикаторов.

Наконец, можно сравнивать секретность документа во время его создания и в период его передачи в архив, работая онлайн. Это может подойти для кодирования контекста или «духа времени». Изучение прагматики семиотическим сообществом должно обеспечить дальнейшее понимание и расшифровку образов контекста.

Конечно, все это – потенциальные источники свойств документа. Только при тщательном рассмотрении юрисдикции оценки и должном уровне процесса оценки секретности и навыков людей, которые это делают, сравнении их результатов с воображаемым будущим инструментом, можно установить, какие из характеристик являются действительно полезными индикаторами в каждом случае.

Несмотря на то, что определен ряд свойств, предстоит провести значительное исследование внутреннего отображения признаков (упомянутая выше модель «мешка слов») и вопроса о поиске наилучшего алгоритма для оказания помощи рецензенту.

Можно использовать ряд методов, от основанных на «ранжировании» (классический поиск информации) до использующих «классификацию» и «кластеризацию». Любой из них использует машинные принципы, такие как «тематическое моделирование» и «построение ряда».

В последнее время исследователи из Университета Глазго работают над проблемами, связанными с пересмотром секретности документов, которые будут храниться в Национальном архиве Великобритании. Их подход заключался в разработке элементов вспомогательной технологии, которые могли бы предсказывать деликатность записей и использовать эти прогнозы для повышения эффективности и результативности работы экспертов по анализу секретности. Методы, использующие машинные классификаторы, показали, что отчасти секретность можно предсказать, но идеальное определение деликатности документа еще долго будет оставаться сложной задачей. Другая работа была сделана с применением «моделирования темы» и связанных методов искусственного интеллекта и апробирована при проверке маркировки безопасности систем связи Госдепартамента США.

Отойдем от алгоритмических задач и рассмотрим наилучший способ представления массива документов рецензентам. Предположим, что воображаемый будущий инструмент имеет возможность учиться у пользователя, а также, что доверие к машине будет иметь решающее значение. Какой в этом случае ряд документов должен быть предложен для работы?

Мы привыкли к поисковым системам, представляющим документы в «наиболее вероятном» релевантном запросу порядке. Это может дать пользователю уверенность в машине, но компьютер не обязательно улучшит пропускную способность и объемы выдачи, если пользователи просто подтвердят очевидное в течение длительного времени прежде, чем они достигнут точки, где их понимание предмета действительно необходимо. Аналогичную трудность можно наблюдать и при «наименее секретном первом» запросе.

Последние работы показали, что этот метод многообещающий, потому что он выбирает порядок представления для активного изучения конкретных различий, которые определяют секретные документы в конкретной выборке. На практике такая систематизация может быть менее интуитивной для потенциального человека-рецензента. Если решения рецензентов-людей зависят от контекста, а изначально цифровые записи по своей природе более взаимосвязаны ссылками, то необходимо продолжить поиск других методов визуализации коллекции оцениваемых документов.

Этот аспект может быть наименее понятным из всех. Даже в научных областях, которые являются гораздо более общими, понимание формы и характеристик цифровых объектов остается чрезвычайно сложной областью исследований. Проблема описания большого количества взаимосвязанных документов знакома каждому, кто пытался выбрать оптимальный подход к потоковой цепочке электронной почты.

Управление документами в основном связано с управлением рисками в контексте законодательства, регулирования и репутации при одновременном взвешивании затрат и выгод. Хранение и опубликование документов с конфиденциальным содержимым, особенно с тем, что может быть истолковано, как личная информация, – это риск.

Многие учреждения, особенно в государственном секторе, не расположены рисковать.

На фоне ужесточения регулирования, о котором уже говорилось, организация, не склонная к риску, закроет или уничтожит документы в качестве меры предосторожности из-за опасений причинить ущерб репутации, который может возникнуть в результате ненадлежащего раскрытия информации. Такие крайние меры излишни, поскольку не всякое разглашение им эквивалентно.

К примеру, раскрытие банальных персональных данных человека, родившегося в 1930-х гг.: человек может быть мертв, и личная информация, возможно, к этому моменту давно устареет.

В аналоговом бумажном мире архивы регулярно публикуют записи, содержащие такую информацию, не задумываясь о последствиях.

Как и многое другое, оцифровка меняет парадигму, так как эти данные сегодня гораздо легче обнаружить. Очень трудно представить себе, каким образом в мире цифровых технологий можно сохранить позицию полного отказа от риска, если записи должны быть доступны для общественности.

Если мы сможем разработать алгоритм, который позволит ранжировать материал по уровню секретности и уровню его дифференцированного воздействия, тогда мы сможем убедить тех, кто несет ответственность в организациях за риски. Как правило, эти аудиторы и комитеты управления рисками способны принять более гибкий подход, понизив статус некоторых рисков до нейтральных, подходящих политике смягчения воздействия в случае протестов.

Некоторые архивные учреждения уже делают это. Национальный архив Великобритании поместил имена всех тех, кто служил в Первой мировой войне в Интернете. Технически некоторые из них все еще могли быть живы в то время, следовательно, их данные должны быть закрыты. На тот момент возражений не было.

Важно, чтобы любые риски, заложенные информационными структурами, находились в реестрах рисков учреждений и лица, отвечающие за управление информацией, регулярно взаимодействовали с комитетами по аудиту и управлению рисками для достижения сбалансированных результатов.

Вся тема оценки секретности документов, в конечном счете, связана с риском опубликования, когда этого не должно быть, а также причинения реального вреда и материального ущерба, риска потерять репутацию надежности организацией из-за неправильного хранения щекотливого, но

доброкачественного материала дольше, чем это разрешено. Для многих архивистов в Европе это еще незнакомая территория, на которую неизбежно придется вступить, потому что пользователи имеют очень большие ожидания от архивов в цифровую эпоху.

Управление рисками является корпоративной ответственностью и может быть делегировано только в рамках установленных параметров, в стороне от архивистов. Несмотря на то влияние, которое они могут оказать, здесь практически нет места для маневра.

Цифровой текст имеет возможность полностью изменить природу исследования, что начинают демонстрировать все последние изыскания в области гуманитарных дисциплин.

Содержание цифрового архива не сводится к набору отдельных документов, с которыми ученый взаимодействует один на один. Это коллекция, которую необходимо изучать в целом или по частям, анализировать с использованием всех статистических и дедуктивных методов, и которая была бы выведена общностью баз данных. Новые труды в дискретной математике по теории графов могут помочь определить новые шаблоны или горячие точки в поиске по контенту.

Изучение оценки секретности или чувствительности документа, которое сделано выше, приведет к появлению целого комплекса новых внутренних контекстуальных свойств, которые могут быть включены в систему, что позволит пользователям архива исследовать этот лабиринт. Они включают характеристики длины слова, структуры, частоты повторения слова или определенной части речи или строки, использование приветствий, прощаний, адресов и даты. Если эти особенности позволят архивистам различать между собой нюансы секретности, то они будут отличными индикаторами и других свойств.

Изучение закономерности признаков и распределения свойств порождает новые исследовательские вопросы или дает указания на комплекс документов, которые в противном случае пропустили бы и обошли стороной, как незначительные.

По мере развития и расширения семантической лексики машины, становится намного проще, быстрее и с большей уверенностью связывать документы в контексте, в котором они были созданы. В теле цифровых документов, которые трудно атрибутировать, уже возможно использование приемов, заимствованных из мира лингвистики, для выявления авторов. Нужно привыкнуть к новым способам запросов в архивы в цифровой среде, что будет сильно отличаться от бумажного мира, который мы оставили позади. Невозможно игнорировать то, что оказалось возможным прочитать все электронные письма, собранные во время расследования скандала с компанией Энрон в октябре 2001 г.

Как автор ранее подчеркивал, архив станет в основном служебной структурой доступа с небольшой предварительной обработкой материалов. Не будет никаких обычных каталогов, и пользователи должны будут изучить, как использовать машинные методы.

Инструменты для обработки больших массивов цифровых данных все еще разрабатываются.

Использование сложных методов позволит исследователям отбрасывать ложные маршруты, отображать трафик для обнаружения пиков, получать подсказки относительно тем, которые находились в центре внимания в определенное время. Инструменты смогут учиться на наших собственных решениях и описывать материал необычными способами, чтобы позволить машине изучать наши потребности. Позже машина сможет описывать существенный материал, непосредственно понимая его содержание. Мы будем в состоянии использовать графы, чтобы нанести на карту интернет-сети схему «Кто-Что-Кому-Когда» говорит. Для этого потребуется доступ к персональным данным, которые могут считаться общедоступными, например, роль или должность, занимаемые пользователем. Для нас станет возможно составить семейные родословные, используя данные, которые будут в открытом доступе, таких как рождение, брак и свидетельства о смерти, хотя ряд других не будет открытым, например официальная перепись населения.

Граница между общественным достоянием и «закрытым доступом в общественных интересах» является нечеткой, изменяющейся и оспариваемой. То, что должны делать контент-провайдеры, – это осознавать и быть готовыми к решению проблем, связанных с продолжением защиты традиции открытости в цифровой среде.

Как утверждает автор, это неизбежно потребует от управленцев, менеджеров и архивистов аргументировать снижение неблагоприятных рисков в отношении к разглашению информации. Если это не удастся, в государственном секторе повысятся риски оказаться перегруженными запросами о свободе информации для доступа к превентивно закрытым файлам. Если в доступе все еще будет отказано, вопрос должен решать суд. В цифровую эпоху даже это не так просто, а суды могут быть гораздо менее благосклонны во избежание риска.

Лорд Дэвид Нойбергер, до недавнего времени президент Верховного суда Великобритании, напомнил об этом в лекции о персональной информации в Сингапуре в 2015 г.: « … далеко идущие события в IT-сфере требуют, чтобы были предприняты меры, способные надлежащим образом защитить право на частную жизнь. Однако должно помнить о возможности, по сути, вероятности того, что взаимосвязь между развитием событий в этой области и основными правами не является улицей с односторонним движени-

ем. Развитие технологий, свидетелями которого мы являемся, неизбежно изменит отношение к конфиденциальности. По сути, это объясняется двумя причинами.

Во-первых, нужно оценить, каким способом IT изменил модели и характер всех аспектов жизни, чтобы увидеть, что это затронет все наши ценности. Во-вторых, существование Интернета неизбежно влияет на то, что может быть практически достигнуто в плане обеспечения конфиденциальности. Закон никогда не должен стремиться признавать или обеспечивать соблюдение прав, которые на практике не имеют законной силы».

В Великобритании Суд королевской скамьи, который слушает дела против исполнительной власти, уже забит тяжбами, добивающимися судебного пересмотра. В мире пост-правды, где даже верховенство закона омрачено мажоритизмом, этого может быть недостаточно, чтобы удержать недобросовестных политиков от игнорирования судебных решений, высмеивания или увольнения членов судебной власти. Специалисты в области информации должны сохранять приверженность к своим основным ценностям сохранения и защиты «доказательств», которые могут недвусмысленно использоваться в рамках верховенства права для привлечения правительства и исполнительной власти к ответственности в государственном и частном секторах.

В цифровой среде этот священный долг, каким видел его сэр Хилари Дженкинсон, ставит огромные задачи, которые требуют разделения этой ответственности с технологами. Должен вестись более широкий диалог с пользователями, с более широкими слоями общества, юристами и политиками при принятии решения о том, что должно быть сохранено и какими должны быть условия доступа.

Реферат Е.Н. Бартеневой

II. АННОТАЦИИ

Республика Словения

Все для людей: актуальные задачи в области науки и образования (Archives in the Service of People – People in the Service of Archives). Сборник докладов 6-й Международной научной конференции, организованной Европейской академией наук и искусств и Университетом Europaea AMEU-ECM. Марибор (Республика Словения). 9–10 марта 2018 г.

Стандарт ISO 15489-1:2016 и оценка: что нового?

Semlič R. Standard ISO 15489-1:2016 and appraisal: what is new? // Archives in the Service of People – People in the Service of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 1. Pp. 43–52.

Оценка – одна из самых важных задач каждого архивиста. Процесс определения архивной ценности документов влияет на все другие архивные процессы, а также затрагивает документальную память общества в целом. Поскольку оценка является одной из важнейших задач, архивистам необходимо педантично подходить к его проведению. В статье автор представляет оценку, исходя из определения, данного в стандарте ISO 15489-1:2016, а также предлагает новый проект технической спецификации по Оценке для управления документами, где процесс оценки документов определяется более подробно.

Архивное законодательство для новой Европы

Tato G. Which archival legislation for new Europe? // Archives in the Service of People – People in the Service of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 1. Pp. 57–61.

Подчеркивается потребность в стандартизации архивного законодательства на европейском уровне, чтобы гражданам ЕС было легче найти схожие термины при поиске необходимой информации в информационной среде Европейского союза. Изложены некоторые критические замечания, касающиеся выбора времени для передачи исторических архивов в учреждения для их хранения, консультаций и доступа. Вопрос в том, почему историки,

чиновники и политики «опасаются» архивов, а также архивистов, которые являются хранителями наследия. Причины различны: историки боятся, что архивы могут раскрыть нежелательные истины, или они не хотят заниматься исследованиями, которые всегда являются сложными, длительными и проблемными, считая, что более «удобным» повторное использование текстов других или распространение теорий, которые не были доказаны документально; администраторы опасаются беспорядка, затрат, пыли, необходимого обслуживания и внимания; некоторые политики не хотят разглашать некоторую информацию об их решениях, суждениях и мнениях, которые исходят из личного интереса и т.д.

Создание общих функциональных классификаций. Опыт финского государственного сектора в области управления документами

Henttonen P. Creating common functional classifications. Experiences oft he finnish public-sector records management // Archives in the Service of People – People in the Service of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 1. Pp. 93–100.

В статье исследуется опыт создания функциональных схем классификации для организаций государственного сектора Финляндии. Функциональные классификации в Финляндии имеют свою историю развития. В Директивах по управлению документами в организациях государственного сектора Финляндии утвержден функциональный подход в научных организациях с начала 1990-х гг. Общие функциональные схемы классификации являются более современными явлениями. Создание общей схемы оказалось более сложным процессом, чем ожидалось. Существует множество проблем: слабая теоретическая основа схем; постоянно изменяющиеся юридические и административные условия приводят к противоречивым требованиям к их содержанию; обсуждение схемы – это социальный процесс, в котором некоторые стороны имеют больше полномочий, чем другие; наконец, недостаток ресурсов ведет к ограничениям того, что может быть достигнуто в приемлемый период времени.

Состояние документов спустя 120 лет: исследования на конкретном примере

Tomažič J. The condition of documents after 120 years: case study // Archives in the Service of People – People in the Service of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 1. Pp. 118–130.

Медная коробка, содержащая документы, фотографию, печатные материалы и монеты, была встроена в стенную нишу за облицовочным камнем

старого зала Средней школы в г. Крань 18 сентября 1897 г., когда новое школьное помещение было открыто. 28 февраля 2017 г. эту коробку случайно обнаружили во время работ по реконструкции здания. Экспертиза доказала, что коробка и ее содержимое хорошо сохранились. Печатные материалы находятся в превосходном состоянии, не считая фрагментов с металлическими скрепками. Физическое состояние фотографии несколько хуже, поскольку есть пятна на изображении, вызванные влажностью. Тем не менее, состояние фотографии стабильное. Рукописный меморандум – в очень плохом состоянии, поскольку его написали на прозрачной бумаге железо-галловыми чернилами. Автор представляет состояние недавно найденных документов и дает рекомендации по обеспечению их сохранности и организации их выставки.

Автоматизированная оценка и отбор электронных документов.

Hajtnik T., Babic A. Automated appraisal and selection of electronic records // Archives in the Service of People – People in the Service of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 1. Pp. 140–154.

На сегодняшний день большинство документов, созданных или полученных создателями в процессе своей деятельности, находятся в электронной форме. Передовые технологии позволяют пользователям сохранить все сообщения электронной почты и другие виды созданных ими электронных документов. Таким образом, они смогут работать в течение многих лет. Документы, первоначально созданные в электронной форме, имеют многократные копии в многократных версиях. Они могут храниться в различных местах, предпочтительно под разными именами и в разных форматах. Все это вызывает возрастающее беспокойство для компетентных государственных архивов, которым необходимо будет пересмотреть процедуру отбора архивных электронных документов своих создателей. В статье авторы пытаются найти ответы на вопрос, смогут ли архивисты использовать новые технологии для оценки электронных документов или возможна ли, по крайней мере, частичная автоматизированная оценка электронных документов? В этой статье проанализированы прошлые практические методы в этой области с целью установления возможной структуры для автоматизированной оценки электронных документов с использованием синтеза традиционной методологии архивной оценки и возможностей, предлагаемых технологиями.

Понятие о виртуальном архивном читальном зале: электронный архив e-ARH.si: VARR

Koncilija Ž., Hajtnik T. The Concept of a virtual archival reading room: e-ARH.si: VARR // Archives in the Service of People – People in the Service

of Archives. 6th Scientific Conference with International Participation. Alma Mater Europaea, Maribor. March 10, 2018. № 01. Pp. 154–163.

С быстрым развитием информационно-коммуникационных технологий и всеобъемлющей оцифровкой общества архивам также не избежать процессов модернизации рабочих процедур. Виртуализация услуг словенских государственных архивов требует от учреждений и их сотрудников множества новых предложений и «цифровых» корректировок. Стратегия и план по внедрению и развитию словенского электронного архива определены на период с 2016 по 2020 гг. На их основе разработан проект по созданию электронного архива e-ARH.si, который отвечает на одну из ключевых проблем по обеспечению удаленного доступа к электронным архивным документам и понятие о виртуальном архивном читальном зале, как представлено в этой статье. Этот читальный зал – VARR – разработан как модульная, технологически совершенная, постоянно развивающаяся, обновляемая и безопасная информационно-коммуникационная система.

III. СИГНАЛЬНАЯ ИНФОРМАЦИЯ

Симпозиум «Архив на службе у человека – человек на службе архива». 6-я Международная научная конференция «Все для людей: актуальные задачи в области науки и образования» (6th Scientific Conference with International Participation «All About People: Challenges for Science and Education» // Symposium «Archives at the Service of Man – Man in the Service of Archives»). Alma Mater Europaea-ECM. Maribor, 2018. March 9–10. № 3/I-II

№ 3. Часть I

№ 3. Часть II

Журнал по управлению информацией, издаваемый Американской Ассоциацией по управлению документацией (ARMA). (Information management. An ARMA International Publication). USA. Январь–февраль 2018. Т. 52. № 1

Журнал по управлению информацией, издаваемый Американской Ассоциацией по управлению документацией (АРМА). (Information management. An ARMA International Publication). USA. Март-апрель 2018. Т. 52. № 2

Французская республика
Аршимаг: стратегия и ресурсы памяти и познания (Archimag: stratégie & ressources de la mémoire & du savoir). Париж. Февраль, 2018 . № 311

Новости

Аршимаг: стратегия и ресурсы памяти и познания (Archimag: stratégie & ressources de la mémoire & du savoir). Париж. Март, 2018. № 312

Информационное издание

ДОКУМЕНТОВЕДЕНИЕ И АРХИВНОЕ ДЕЛО ЗА РУБЕЖОМ

Информационный сборник: продолжающееся издание

Редактор-корректор *С.В. Морозов*
Верстка и дизайн *А.М. Моисеева*

Составитель и правообладатель Всероссийский научно-исследовательский институт документоведения и архивного дела (сектор зарубежной информации ОЦНТИ)
Телефон для справок: (495) 334-48-52
Адрес: 117393, г. Москва, ул. Профсоюзная, д. 82
Электронная почта: ocnti@vniidad.ru
Факс: (495) 718-78-74

Издатель Редакционно-издательский дом Российского нового университета
Почтовый адрес: 111024, г. Москва, ул. Авиамоторная, д. 55, корп. 31
Тел.: (495) 981-51-12, 221-50-16

Подписано в печать 05.09.18. Формат 60x90/16.
Печать офсетная. Бумага офсетная. 7,5 печ. л.
Тираж 120 экз.

Перевод оригинальных публикаций с иностранных языков на русский можно заказать в Отраслевом центре научно-технической информации (ОЦНТИ) ВНИИДАД с оплатой по договору.
Заказывайте переводы по телефону (495) 334-48-52
и электронной почте ocnti@vniidad.ru

По вопросам издания литературы обращаться по адресу:
111024, Москва, ул. Авиамоторная, д. 55, корп. 31
Тел.: (495) 981-51-12, +7 (985) 165-36-36
Электронная почта: universitas@mail.ru