ЭЛЕКТРОННЫЕ РЕСУРСЫ. ЭЛЕКТРОННЫЕ БИБЛИОТЕКИ

УДК 002:34+004:34
doi: 10.33186/1027-3689-2021-11-85-104

И. В. Тимошенко
ГПНТБ России, Москва, Российская Федерация

Управление цифровыми правами доступа в информационных системах электронных библиотек и архивов

Аннотация. Представлены основные виды защиты содержимого электронных документов от несанкционированного доступа и распространения, применяемые издательскими и книготорговыми организациями. Рассмотрены принципы управления цифровыми правами доступа (DRM) к электронным документам. Проанализированы виды электронных документов, используемых в библиотеках и архивах, к которым целесообразно применение DRM-систем, а также их наиболее распространённые форматы. Рассмотрены примеры коммерческих решений DRM-систем, применяемых для наиболее популярного PDF-формата электронных документов. Доказана важность стандартизации DRM-систем для повышения удобства использования электронных документов как для читателей, так и для правообладателей, распространяющих электронные издания. Рассмотрены существующие международные стандарты, составляющие нормативную базу DRM-систем и введённые в действие в этом году. Показана представленная в стандартах типология технических средств защиты авторских прав, а также регламентированные характеристики DRM-систем, основанных на шифрации данных. В качестве примера стандартизованного подхода к разработке DRM-систем представлен проект Readium, развиваемый некоммерческой международной организацией Readium Foundation, цель которого – создание и развитие программных модулей для интеграции стандартной DRM-технологии в автоматизированные информационные системы, в том числе с библиотечной спецификой.

Статья написана в рамках проведения работ по государственному заданию 730000Ф.99.1.БВ09АА00006.

Ключевые слова: электронная книга, библиотечный фонд, электронный формат, электронные библиотеки, PDF, EPUB, DRM, цифровые права доступа, информационные системы, ISO, международная стандартизация

DIGITAL RESOURCES. ELECTRONIC LIBRARIES

UDC 002:34+004:34
doi: 10.33186/1027-3689-2021-11-85-104

Igor V. Timoshenko
Russian National Public Library for Science and Technology,
Moscow, Russian Federation

Digital access rights management in the information systems of e-libraries and digital archives

Abstract. The author reviews the basic types of digital document content protection from unauthorized access and dissemination applied by publishers and book trading companies. The principles of digital rights management (DRM) while accessing digital documents. The author suggests that DRM systems are efficient to be applied to certain types and formats of digital documents in libraries and archives. He also reviews several commercial solutions for DRM-systems plied to the most popular PDF-format and substantiates the importance of DRM-systems standardization for digital document friendliness both for the users and rights holders disseminating digital publications. Existing and newly introduced international standards for DRM-systems are discussed. The typology of digital rights protection software as provided for by the standards is presented along with regulated DRM-system features based on data coding. Readium project by international non-profit Readium Foundation exemplifies standard approach to DRM-system design. The project goal is to develop software modules to integrate standard DRM-technology into computer information systems including ALIS.

The article is prepared within the framework of the State Order No. 730000F.99.1.BV09AA00006.

Keywords: e-book, library collection, digital format, e-library, PDF, EPUB, DRM, digital access rights, information system, ISO, internation standardization

---

Электронные и компьютерные технологии внесли кардинальные изменения в жизненный уклад современного человека, создали предпосылки для появления информационного общества. Сегодня информация становится основным продуктом производства, определяющим

все остальные виды производств. Взрывное увеличение её объёма стало возможным благодаря появлению новой электронной коммуникационной среды – глобальной компьютерной сети Интернет, а также такого феномена техники, как электронный документ. Как продукт производства он участвует в экономических процессах, неотъемлемая часть которых – товарно-денежные отношения. Применительно к электронным документам это означает ограничение возможностей действий с ними, связанное с оплатой пользователями прав на такие действия. В полной мере это можно отнести и к электронным книгам.

Сегодня они заняли прочное место в информационном пространстве, существенно потеснив традиционные бумажные издания. Электронные книги обладают такими преимуществами электронных документов, как: компактность, возможность изменить оформление текста и изображений для комфортного использования, гигиеничность и экологичность и, одно из основных, – высокая скорость и низкая стоимость копирования и распространения. Именно это преимущество одновременно является и недостатком, ограничивающим их применение в книготорговых организациях и библиотеках. Обратная сторона свободы пользователей копировать и распространять электронные документы – это ограничение прав владельцев на получение вознаграждения за свой труд, на выбор целевой аудитории и т. д. Для баланса интересов владельцев и пользователей необходимо иметь возможность управлять доступом к электронным документам в соответствии с правовыми соглашениями сторон. Это относится не только к книготорговым организациям. Работа библиотек и архивов также основана на ограничении возможных действий с документами фондов, к числу которых могут относиться и электронные документы, книги.

Для защиты прав владельцев электронных документов используются различные методы, которые можно условно разделить на социальные и технико-технологические.

Социальные меры – принятие законов, предусматривающих ответственность за несанкционированное использование электронных документов. В нашей стране этому вопросу посвящена гл. 70, разд. VII, ч. 4 ГК РФ – «Авторское право» [**1**]. Закон регулирует вопросы авторского и смежных прав. ГК РФ – федеральный закон, регулирующий

гражданско-правовые отношения и имеющий приоритет перед другими федеральными законами.

Авторские права регулируют также ст. 146 «Нарушение авторских и смежных прав», 180 «Незаконное использование средств индивидуализации товаров (работ, услуг)» УК РФ [**2**] и ст. 7.12 «Нарушение авторских и смежных прав, изобретательских и патентных прав» КоАП РФ [**3**]. Федеральные законы обеспечивают высокую степень защиты авторских прав на объекты интеллектуальной собственности в виде электронных документов. На практике социальные механизмы защиты интеллектуальных прав работают не всегда.

Надёжная защита обеспечивается совместно с техническими устройствами, физически защищающими содержимое документов. Сегодня известно множество устройств, управляющих правами доступа к электронным документам, объединяемых в один класс *DRM*-систем *(Digital Right Management)*. *DRM*-системы – программные или программно-аппаратные средства, управляемо ограничивающие действия с электронными ресурсами (просмотр, копирование, модификацию и т. п.). Их основные функции – защита авторских и лицензионных прав, а также сбор статистической информации об использовании ресурсов, что имеет важное значение как для коммерческих организаций, так и для библиотек. Техническая реализация различных *DRM*-систем может различаться, но все они основаны на одном принципе. Содержимое защищаемого документа шифруется. Для шифрования используются криптосистемы с открытым ключом [**4**], основанные на односторонних функциях, где применяется два ключа – открытый и закрытый. Шифрация производится с использованием открытого ключа. Пользователь получает документ по открытому каналу в зашифрованном виде. Вместе с ним, по защищённому каналу, получает закрытый ключ. Устройство чтения дешифрует содержимое документа и делает его доступным для чтения.

Принцип *DRM*-системы можно проиллюстрировать схемой, выполненной в соответствии со спецификацией протокола обмена электронными книгами *EBX (Electronic Book Exchange)*, разработанной организацией *IDPF (International Digital Publishing Forum)* [**5**] (см. рис.). В протоколе используется две пары асимметричных ключей шифрования: одна – для защиты книги, другая – для защиты данных о предоставляемых на неё правах.

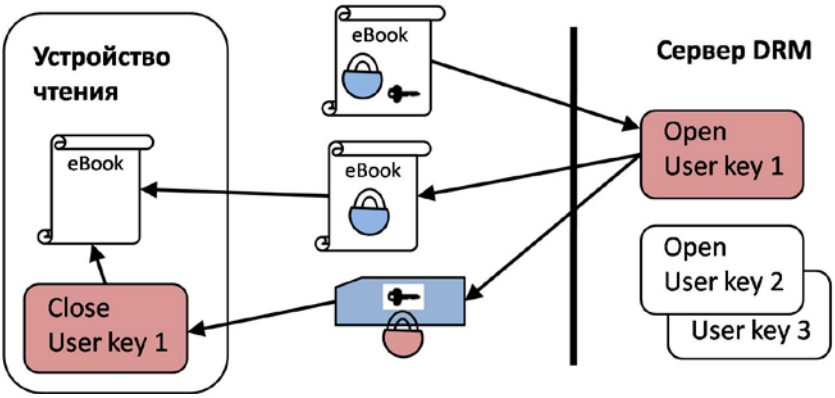

Схема работы *DRM*-системы по протоколу *EBX*

В соответствии с протоколом пользователь регистрирует устройство для чтения на сервере *DRM*, где для него генерируется пара ключей шифрования. Открытый ключ сохраняется на сервере, а закрытый – в устройстве для чтения, в не доступном для пользователя виде. Для приобретаемой книги генерируется другая пара ключей. Открытым ключом шифруется её содержимое, после чего книга передаётся на устройство для чтения пользователя. Одновременно с книгой передаётся специальный файл – «ваучер», зашифрованный открытым ключом пользователя, хранимым на сервере *DRM*. Ваучер содержит закрытый ключ для доступа к содержимому книги, а также дополнительную информацию о правах пользователя на определённые действия с этой книгой (копирование, вывод на печать, период доступа и т. д.). Устройство дешифрует содержимое книги и предоставляет её пользователю в соответствии с приобретённым набором прав.

При всём сходстве принципов технические особенности реализации современных *DRM*-систем разных производителей существенно отличаются, что делает эти системы несовместимыми. Сегодня каждый крупный провайдер электронных ресурсов имеет свой оригинальный набор технических средств, включая устройства для чтения – электронную книгу или компьютерную программу, которые позволяют читать только «свои» книги. Это привязывает пользователя к конкретному устройству, что существенно снижает удобство использования электронных книг и, как следствие, интерес к ним пользователей.

Важное значение для обеспечения защиты электронного документа имеет его формат. Форматом определяются правила, устанавливающие набор символов, порядок их расположения в документе. Правила позволяют распознавать элементы данных, задающие общую семантику документа, и определяют набор возможных действий с документом. Сегодня в интернете представлены электронные документы в разных форматах, каждый из которых имеет набор специфических характеристик и своё назначение [**6**]. Применительно к библиотеке целесообразно рассмотреть электронные форматы издательской продукции, составляющей основу библиотечных фондов. Такие форматы можно разделить на две основные категории: фиксированные и адаптивные.

Особенность фиксированных форматов – сохранение исходной вёрстки электронного документа при его визуализации на любых экранах. Их часто используют для архивного хранения электронных копий бумажных документов, создания электронных копий печатных изданий. Наиболее распространённый формат таких документов – *PDF,* имеющий ряд разновидностей, от компании *Adobe*.

Адаптивные форматы позволяют изменять вёрстку документа исходя из характеристик экрана и параметров, заданных пользователем. Такой документ во многом подобен веб-странице и обычно применяется при создании самостоятельных электронных изданий. Наиболее распространённым форматом таких изданий в нашей стране является *FictionBook2 (FB2)*, предложенный группой российских разработчиков.

Для фиксированных форматов семейства *PDF* на сегодняшний день разработано достаточно много программных и программно-аппаратных систем защиты. Для адаптивных форматов ситуация выглядит иначе. В упомянутом формате *FB2* изначально не была предусмотрена возможность защиты содержимого, поэтому набор возможных методов защиты для него очень ограничен. Наиболее перспективным на сегодняшний день динамическим форматом является *EPUB*, продвигаемый рядом авторитетных международных организаций и основанный на языке разметки *HTML*. Формат позволяет создавать как фиксированные, так и адаптивные электронные документы. В нём заложена возможность полнофункциональной защиты содержимого. Но сегодня он недостаточно распространён в российских библиотеках.

Исторически для *PDF*-документов первой *DRM*-системой была *Adobe PDF Merchant*. Система была реализована в составе подгружаемого программного модуля для *Acrobat Reader 4.0.5* и серверной части *Adobe PDF DRM*. При попытке открыть защищённую книгу в приложении *Acrobat Reader* на сервер отправлялись запрос с информацией об открываемом файле и идентификатор компьютера, с которого происходил запрос, или идентификатор учётной записи пользователя. На сервере полученная информация проверялась, и, в случае успеха, в ответ отправлялся зашифрованный *RMF*-файл *(Right Management Format)* с ключом для расшифровки *PDF* и условиями, при которых был возможен доступ к книге. При эксплуатации системы был выявлен ряд её уязвимостей, поэтому в настоящее время в продуктах компании *Adobe* применяется решение *Adobe DRM (EBXJHANDLER)*, которое реализует управление правами доступа в соответствии со спецификацией протокола обмена электронными книгами *(Electronic Book Exchange, EBX)*, разрабатываемым рабочей группой *EBX Workgroup IDPF*. Работа протокола также основана на использовании пары асимметричных ключей. Решение *Adobe DRM* отличается дополнительными мерами защиты ключей от доступа пользователем. Закрытый ключ пользователя хранится в устройстве для чтения – в программе *Adobe Acrobat Reader*, и дополнительно шифруется. У пользователя нет к нему доступа. Данные для предоставления доступа к документу от пользователя скрыты. Начиная с шестой версии *Adobe Acrobat Reader* для шифрации нескольких фрагментов документа в системе используются различные способы. Всё это повышает защищённость документа, но не делает её идеальной. Следующий шаг в развитии *DRM* от компании *Adobe* – появление в 2007 г. программы *Adobe Digital Editions*. С её помощью можно читать защищённые электронные книги не только в *PDF*, но и в *EPUB*-формате. Работа с программой предполагает регистрацию пользователем всех устройств, с которых он будет получать доступ к книгам, на сайте *Adobe* и получение *Adobe ID*. Для получения доступа к книге с сервера провайдера скачивается специальный *acsm*-файл *(Adobe Content Server Manager),* в котором содержатся ссылка на книгу и необходимые данные для получения доступа к её содержимому. Существуют версии программы для устройств с различными операционными системами.

Работа программы поддерживается большинством электронных книг для чтения.

Поскольку *Adobe PDF* сегодня является самым распространённым в издательствах, книготорговых организациях и библиотеках, на рынке появилось множество *DRM*-систем, поддерживающих этот формат. Кроме *DRM* от компании *Adobe*, можно назвать такие наиболее известные системы, как *DocProtect (Excel Software)*, *Safeguard PDF Security (Locklizard Limited)*, *PDF Security OwnerGuard (Armjisoft)*, *Seclore FileSecure (Seclore)*, обеспечивающие защиту и управление доступом к *PDF*-документам.

В 2018 г. компания «ЛитРес» объявила о создании собственной *DRM*-системы [**7**], поддерживающей формат *FB2* и не поддерживающей *EPUB*.

В качестве ещё одного примера можно привести систему *StarForse DRM*, разработанную российской компанией «Протекшен Технолоджи» [**8**], специализирующейся на разработке систем защиты интеллектуальной собственности для различных областей деятельности. Предлагаемая *DRM*-система представляет собой комплексное решение, позволяющее не только защищать интеллектуальную собственность издателям, авторам и книготорговым организациям, но и управлять процессом распространения электронных ресурсов. Каждому пользователю предоставляется личный кабинет, в котором можно создавать проекты и управлять ими: собирать статистику активаций. При помощи *StarForce API* можно интегрировать предлагаемое *DRM*-решение в специализированные издательские и библиотечные информационные системы.

Следует констатировать, что имеющиеся решения *DRM* от разных разработчиков не совместимы между собой – это существенно ограничивает удобство использования защищаемых электронных документов.

Наряду с форматом *PDF* важное значение для распространения электронных публикаций в интернете имеет формат *EPUB*. Он сегодня получил широкое распространение в мире и является основным форматом публикаций с «плавающей» вёрсткой. В нашей стране он только начинает приобретать популярность у книгоиздателей для самостоятельных электронных изданий. Документ в формате *EPUB* представляет собой *ZIP*-архив, в котором наряду с распространяемым контентом содержатся файлы с дополнительной информацией об отображении документа на устройстве для чтения и мерах защиты его содержимого.

Контент документа может быть представлен *HTML*-страницами, включающими в себя, кроме текста, мультимедиаэлементы, а также иметь содержимое в произвольных форматах, включая *PDF*-документы.

Формат *EPUB* был предложен международной некоммерческой организацией *IDPF (International Digital Publishing Forum)* в 1999 г. В 2011 г. инициативу поддержали международные организации по стандартизации ИСО и МЭК. С 2017 г. продвижением формата занимается организация *W3C (World Wide Web Consortium)*, являющаяся головной в разработке стандартов современного Интернета в рамках концепций Всемирной паутины и Семантического веба. Сегодня *EPUB* поддерживается практически любыми устройствами для чтения, и уже можно сказать, что распространение электронных книг по всему миру основано на стандарте *EPUB*, при этом большинство книготорговых организаций используют проприетарные технологии *DRM* для защиты авторских прав. Таким образом, высокий уровень совместимости и доступности электронных книг, полученный за счёт использования стандартного формата публикации, сводится на нет использованием закрытых локальных технологий *DRM*.

Решить эту проблему призвана система стандартов, разработанная совместной рабочей группой *ISO/IEC JTC 1/SC 34/JWG 7 «EPUB»*, ИСО 23078:2020 «Информационные технологии. Спецификация *DRM*-технологии для цифровых публикаций». Система стандартов состоит из трёх частей:

Часть 1. Обзор технологий защиты авторских прав, применяемых в издательской индустрии.

Часть 2. Защита, основанная на пользовательских ключах.

Часть 3. Защита, основанная на ключах устройства.

В первой части [**9**] описаны три типа технологий, применяемых в издательской индустрии для защиты авторских прав:

без *DRM* («социальный *DRM*»);

DRM на основе пользовательских ключей – для случаев, когда права пользователя могут быть ограничены, но он имеет возможность доступа к содержимому документа с разных устройств;

DRM на основе ключей устройства, для случаев, когда передача публикаций с одного устройства на другое должна быть строго ограничена.

Защита без *DRM* («социальный *DRM*») – технологии, которые не полагаются на шифрование содержимого, а используют различные включения в документ для его уникальной идентификации при проверке легальности использования. Обычно такие включения представляют собой «цифровой отпечаток» или «водяные знаки». Такие технологии применяются в случаях, когда удобство пользователя является главным приоритетом. Строго говоря, эти технологии не являются *DRM* и называются так по аналогии с решаемыми задачами.

Цифровой отпечаток формируется из уникального набора свойств, присущих документу. Обычно это набор буквенно-цифровых строк (хэшей), по которым можно идентифицировать документ. Создание уникального отпечатка возможно без изменения публикации, он хранится в базе данных и используется для проверки идентичности документа. Его создание происходит без участия пользователя, он никогда не увидит каких-либо признаков наличия отпечатка у приобретаемого документа. Цифровые отпечатки используют для отслеживания документа службами интернет-мониторинга при помощи поисковых роботов. Часто эта технология используется при обмене контентом, для опроса конкретной службы и определения легальности загрузки электронного документа. Это позволяет избежать дальнейших затрат на судебные процессы. Сложность реализации этой технологии состоит в том, чтобы сохранять правильное определение цифрового отпечатка документа независимо от возможных форматов его представления (*PDF* или *EPUB* и т. д.) или внесения незначительных изменений в его содержимое.

Технология водяных знаков основана на создании уникальной копии лицензируемого электронного документа, которая содержит дополнительную как видимую, так и невидимую информацию о лицензиате. Видимая информация может содержать напоминание о запрете бесплатного распространения цифровой публикации или правила использования документа. Технология водяных знаков основана на обфускации. Невидимая информация может формироваться множеством методов, создающих сложности исключения её из документа таким образом, что злоумышленник не может узнать, все ли водяные знаки были удалены из документа. Сложность создания водяных знаков в том, что при их создании не может быть затронуто текстовое содержимое документа. Текст электронной книги должен остаться таким, как

его задумали автор и издатель. Методы нанесения водяных знаков используют пространства между символами в строке, между строками в виде непечатных символов, добавляемых к тексту, дополнительных кодов, встраиваемых в иллюстрации и т. д. Технология водяных знаков обычно используется при продажах электронных книг, также при распространении препринтов или обзорных публикаций. Она не может быть использована при выдаче книг в библиотеках, для этого используются методы *DRM*-защиты. К недостаткам этой технологии также можно отнести высокие затраты на формирование водяных знаков для каждого лицензиата, сложности индексирования *EPUB*-документов с водяными знаками в интернете. Но основной недостаток – сложности с соблюдением положений Европейского регламента по защите персональных данных *(GDPR)* в части защиты граждан от несанкционированной обработки их персональных данных, соблюдения мер безопасности при хранении таких данных и права удаления личной информации, если она больше не используется. Таких проблем лишены технологии *DRM*-защиты контента электронных документов.

Во многих случаях издатели не могут полагаться на социальные методы защиты и «социальный *DRM*» и предпочитают решения, которые технически обеспечивают соблюдение цифровых прав, предоставляемых пользователям. Такая защита обеспечивается шифрованием содержимого документа и применяется в программно-аппаратных решениях *DRM*. Расшифровать документ может только владелец ключа дешифрования. Сложность реализации такого *DRM* заключается в безопасной передаче ключа приобретателю прав, так чтобы злоумышленник не получил к нему доступа, а также не смог распространить расшифрованный контент.

Технология *DRM* особенно полезна для библиотек, при передаче электронных книг во временное пользование. По прошествии срока выдачи пользователь не должен иметь доступ к книге. Для электронных книг такое условие выполнимо только при использовании *DRM*.

В библиотеках сегодня существует проблема привязки конкретных систем к «своим» провайдерам. При использовании *DRM* провайдеры вынуждают пользователя создавать учётные записи в своих сервисах, использовать проприетарные устройства для чтения и продвигать свой контент. Такой подход неприемлем для библиотек, где дол-

жен быть обеспечен единообразный доступ ко всем электронным документам как своего фонда, так и фондов других библиотек.

В системе межбиблиотечного абонемента, сегодня это системы электронной доставки документов, стандартная *DRM* может позволить переслать полные документы для предоставления доступа через АБИС другой библиотеки с сохранением прав автора и библиотеки-владельца.

Кроме того, посетители библиотек могут иметь ограниченные возможности (слепота, дислексия и т. д.) и получать доступ к книгам через специализированные приложения, используемые в конкретной библиотеке. Важно, чтобы через эти приложения также можно было получать доступ к книгам, защищённым *DRM*-системами. Похожие требования могут предъявляться и со стороны независимых книготорговых организаций, которым также нужны независимые технологии защиты продаваемых электронных книг, не связанные с закрытыми и несовместимыми решениями крупных издателей и ретейлеров.

Кроме того, библиотеки могут использовать *DRM* книготорговых организаций и издательств, работающих по договору с библиотекой. По запросу читателя библиотека покупает электронную книгу и предоставляет её в пользование на время. Затем книга поступает в фонд библиотеки. В дальнейшем её выдача читателям должна происходить через *DRM* библиотеки.

Важное свойство хорошей технологии *DRM* – её незаметность для пользователя. Сегодня это возможно только в рамках закрытых локальных решений. Как только пользователь попытается переместить приобретённую электронную книгу на устройство для чтения, не входящее в эту систему, он столкнётся с проблемами, часто неразрешимыми. Существующие открытые программные решения для чтения электронных книг требуют от пользователя много дополнительных действий, необходимых для получения доступа к приобретённой книге. Перед чтением нужно войти в систему стороннего поставщика, загрузить файл лицензии, импортировать его в используемое программное обеспечение. Только после этого можно увидеть приобретённую книгу на виртуальной полке программы для чтения. Эти дополнительные сложности и являются главной причиной того, что проприетарные *DRM*-системы, используемые за пределами своих закрытых сред, отвергаются большинством пользователей.

Решением этой проблемы могла бы стать стандартная *DRM*-система, не зависимая от производителей и поставщиков, которая обеспечила бы баланс между требованиями авторов и издателей к защите авторских прав и потребностями пользователей с точки зрения доступности и простоты использования.

В стандартной спецификации *DRM*-технологии для цифровых публикаций представлены нормативные требования к двум видам защиты на основе шифрования: с применением пользовательских и аппаратных ключей.

Защита на основе пользовательского ключа используется в случаях, когда ограничения доступа к документу могут быть установлены для пользователя. Такая технология основана на использовании парольной фразы. В издательской индустрии она известна как технология *Readium LCP (Licensed Content Protection)* [**10**]. Эта технология позволяет достичь приемлемого баланса между простотой использования и защитой авторских прав.

Установлены следующие требования к *DRM*-защите на основе пользовательского ключа со стороны издателей и дистрибьютеров:

использование надёжных технологий шифрования, не допускающих быстрый взлом путём простого перебора ключей;

наличие своего ключа дешифрования у каждой публикации. Не должно быть возможности расшифровки нескольких публикаций с помощью одного ключа;

не должно быть возможности получить ключ дешифрования только с использованием информации, содержащейся в файле лицензии;

не должно быть возможности изменения прав, включённых в файл лицензии;

возможность установления временного диапазона, за пределами которого чтение публикации запрещено;

возможность указания количества страниц, которое пользователь может распечатать в течение срока действия лицензии;

возможность указания объёма текста, который пользователь может копировать в течение срока действия лицензии;

возможность продления срок лицензии по запросу пользователя;

возможность досрочного завершения действия лицензии по запросу пользователя;

возможность досрочного отзыва лицензии в случае неправомерных действий со стороны пользователя (например, выкладывание защищённой книги с ключом в открытый доступ в интернете);

возможность применения решения *DRM* на разных устройствах для чтения, без привязки к конкретному поставщику;

применимость для разных форматов электронных публикаций. Сегодня предпочтительными являются форматы *EPUB*, *PDF* и веб-публикация *W3C*;

возможность контроля техподдержки *DRM*-системы, получение статистических данных о количестве и характере проблем, возникающих у пользователей.

В стандарте также установлен перечень требований к *DRM*-системе – основе пользовательского ключа с точки зрения пользователей:

незаметность – пользователь не должен создавать специальную учётную запись для чтения электронных книг, защищённых *DRM;*

возможность получения доступа к защищённой электронной книге с разных устройств и приложений, в том числе специализированных, для людей с нарушениями зрения и восприятия текста;

загрузка и чтение защищённой публикации должны быть возможны в автономном режиме, без подключения к интернету;

DRM не должен допускать утечки персональных данных без согласия пользователя. Персональные данные могут предоставляться продавцу или персоналу публичной библиотеки, но они не должны передаваться третьей стороне, например поставщику *DRM;*

возможность переноса электронной книги на различные устройства в течение периода использования. Пользователи могут читать книгу на смартфоне в дороге, на планшете дома, могут поменять смартфон на новый во время использования электронной книги.

В некоторых случаях издатели предъявляют дополнительные требования к *DRM*-системам. Защита на основе ключа устройства используется, когда требуется строгое ограничение передачи публикации с одного устройства на другое. Технически этот вариант защиты аналогичен защите на основе пользовательского ключа дополненной асимметричным ключом для определения «своего» устройства и блокиров-

ки остальных. Такой вариант защиты используется для публикации ценного контента, например, под грифом, ограничивающим целевую аудиторию, дорогих публикаций, отчётов о научных, маркетинговых исследованиях и т. д.

Требования к защите на основе ключа устройства аналогичны перечисленным выше для систем с пользовательским ключом, но со следующими дополнениями от издателей:

использование защищённой публикации должно быть привязано к определённому устройству на заданное время;

копирование публикации на другое устройство для чтения должно быть возможным только для ограниченного количества устройств, указанного издателем;

все спецификации протоколов *DRM* должны быть в открытом доступе, чтобы избежать риска утечки закрытой информации, с помощью которой механизм защиты может быть отключён полностью или на время. Тем не менее открытая информация о механизме *DRM* не должна снижать защищённости публикаций.

потенциальное действие скомпрометированной *DRM*-системы не должно иметь глобального масштаба. Даже если инструмент для взлома будет выпущен в свободный доступ или на чёрный рынок, его действие должно быть ограничено одним дистрибьютером.

Дополнительное требование пользователей заключается в том, что, пока устройство подключено к сети, пользователь не должен испытывать трудности при копировании с одного устройства на другое, определённое издателем.

Во второй части стандарта [**11**] перечислена последовательность процессов и операций, необходимых для обеспечения защиты электронных публикаций. Перечень процессов включает в себя:

защиту публикации шифрованием;

создание документа-лицензии, распространяемого в составе защищённой публикации или отдельно;

получение доступа к публикации путём расшифровки его содержимого с использованием документа-лицензии.

В стандарте установлены правила создания канонической формы документа-лицензии; определён словарь метаданных, включаемых в

него для идентификации защищаемого документа, получения к нему доступа, а также для идентификации пользователя и определения перечня прав на действия с документом, предоставляемых в рамках лицензионного соглашения между правообладателем и пользователем. Для предотвращения внесения изменений в документ-лицензию он должен быть защищён цифровой подписью.

Основные положения стандарта базируются на существующей и широко распространённой *DRM*-технологии *Readium LCP*, которая использует стандартные алгоритмы шифрования, определённые в спецификациях *W3C XML Encryption* [**12**] и *W3C XML Signature* [**13**]. Для обеспечения максимальной гибкости эти документы не требуют никаких конкретных алгоритмов. Содержимое документа-лицензии позволяет устройству чтения идентифицировать алгоритмы шифрования, применённые в защищённой публикации. В стандарте определено понятие профиля шифрования, которое представляет собой набор алгоритмов шифрования, используемых в конкретной защищённой публикации и соответствующем лицензионном документе.

В стандарте приведены типовой сценарий организации предоставления электронных ресурсов пользователям через портал электронной библиотеки. Электронная библиотека использует *DRM*-систему для управления цифровыми правами на свои электронные книги. Библиотека имеет портал, на котором посетители могут осуществлять поиск по каталогу, выбирать и загружать электронные книги. Посетитель при записи на библиотечное обслуживание получает парольную фразу (ключ *LCP*), которую он должен ввести для получения доступа к электронным книгам. Парольная фраза связана с текстовой подсказкой, помогающей пользователю запомнить ключ *LCP*. Сотрудник библиотеки советует пользователю проверить наличие устройства, приложения или загрузить приложение для чтения, совместимое с используемой *DRM*-системой. Пользователь импортирует в своё приложение или устройство для чтения файл-лицензию с правами на использование электронных книг этой библиотеки. При первой загрузке файла-лицензии пользователь должен ввести в модальном окне парольную фразу, которую он получил при регистрации в библиотеке. После этого он может загрузить зашифрованную электронную книгу из каталога и открыть её для чтения.

Третья часть стандарта [**14**] определяет технические характеристики более строгого решения для шифрования ресурсов в цифровых публикациях, которое применяется издателями в случаях, когда требуются более строгие меры защиты, предполагающие ограничение возможности переносить публикации с одного устройства чтения на другое. В целом, предлагаемый порядок предоставления доступа к защищённому документу аналогичен описанному во второй части стандарта, но в него добавлен процесс регистрации устройства чтения. Представленная схема лицензирования является расширением схемы *Readium LCP*. Регистрация устройства является обязательной перед получением документа-лицензии. Пользователь, знающий парольную фразу, может зарегистрировать устройство, если накопленное им количество регистраций не превышает установленное поставщиком, после чего он может получать связанные с устройством документы-лицензии, загружать и открывать защищённые публикации.

Представленная в стандарте нормативная база *DRM*-системы основана на технических решениях, разработанных и продвигаемых международной некоммерческой организацией *Readium Foundation* [**15**], она же была инициатором и автором первой редакции проекта международного стандарта. Организация была основана по инициативе ассоциации *IDPF*. Основная цель проекта *Readium* – создание набора надёжных, производительных, соответствующих стандартам наборов инструментов для систем чтения, которые поддерживают форматы цифровых публикаций (*EPUB*, веб-публикации и т. д.) и могут быть развёрнуты в браузерах или встроены в собственные приложения на *iOS*, *Android* или на ОС настольных компьютеров *(Windows, Linux)*. С 2019 г. все продукты *Readium* распространяются под открытой лицензией *(3-part BSD license)*. Применение модулей *Readium* даёт возможность независимым разработчикам информационных систем библиотечного профиля интегрировать стандартные инструменты для работы с цифровыми публикациями *EPUB*-формата, в том числе защищёнными *DRM*-системами, реализованными на основе схемы *Readium LCP*. Применение стандартных инструментов для работы и защиты содержимого электронных публикаций способствует повышению удобства пользования электронными библиотеками и архивами при соблюдении авторских и лицензионных прав владельцев предоставляемых информационных ресурсов.

СПИСОК ИСТОЧНИКОВ

1. **Российская** Федерация. Законы. Гражданский кодекс Российской Федерации : ГК : текст с изменениями на 1 июля 2021 г. – Текст : электронный // Электрон. фонд правовых и нормативно-технических док-ов: [сайт]. – 2021. – URL: https://docs.cntd.ru/document/9027690 (дата обращения: 15.07.2021).

2. **Российская** Федерация. Законы. Уголовный кодекс Российской Федерации : УК : текст с изменениями на 1 июля 2021 г. – Текст : электронный // Электрон. фонд правовых и нормативно-технических док-ов: [сайт]. – 2021. – URL: https://docs.cntd.ru/document/9017477 (дата обращения: 15.07.2021).

3. **Российская** Федерация. Законы. Кодекс Российской Федерации об административных правонарушениях : текст с изменениями на 1 июля 2021 г. – Текст : электронный // Электрон. фонд правовых и нормативно-технических док-ов: [сайт]. – 2021. – URL: https://docs.cntd.ru/document/901807667 (дата обращения: 15.07.2021).

4. **Тульчинский А.** Криптосистемы с открытым ключом / А. Тульчинский. – Текст : электронный // www.comprice.ru: [сайт]. – 2003. – URL: http://www.comprice.ru/articles/detail.php?ID=41120 (дата обращения: 15.07.2021).

5. **International** Digital Publishing Forum : сайт. – 2017. – URL: http://idpf.org/901807667 (дата обращения: 15.07.2021). – Архивная версия. – Текст : электронный.

6. **Тимошенко И. В.** Развитие и стандартизация электронных форматов документов в издательской и библиотечной деятельности / И. В. Тимошенко // Библиотеки и образование : ежегодный межведомственный сборник научных трудов. – Москва : ГПНТБ России, 2018.

7. **ЛитРес** DRM // Сайт ЛитРес. – Текст : электронный. – 19.01.2018. – URL: https://docs.litres.ru/pages/viewpage.action?pageId=6425428#id-ЛитРесDRM-ЛитРесDRM удобен для пользователя (дата обращения: 03.09.2021).

8. **Star Force** : Защита электронных документов и программного обеспечения : сайт. – 2021. – URL: https://www.star-force.ru/solutions/electronic-documents-security/ (дата обращения: 15.07.2021). – Текст : электронный.

9. **ISO/IEC** TS 23078-1:2020 Information technology – Specification of DRM technology for digital publications – Part 1: Overview of copyright protection technologies in use in the publishing industry // Сайт ISO. – 2020. – Текст : электронный. – URL: https://www.iso.org/standard/79484.html (дата обращения: 29.06.2021).

10. **Readium** LCP Specifications industry // Сайт Readium. – Текст : электронный. – URL: https://readium.org/lcp-specs/ (дата обращения: 16.07.2021).

11. **ISO/IEC** TS 23078-2:2020 Information technology — Specification of DRM technology for digital publications – Part 2: User key-based protection // Сайт ISO. – 2020. – Текст : электронный. – URL: https://www.iso.org/standard/79485.html (дата обращения: 29.06.2021).

12. **XML** Encryption Syntax and Processing Version 1.1 : W3C Recommendation // Сайт W3C. – 2013. – Текст : электронный. – URL: https://www.w3.org/TR/xmlenc-core1/ (дата обращения: 15.07.2021).

13. **XML** Signature Syntax and Processing Version 1.1 : W3C Recommendation // Сайт W3C. – 2013. – Текст : электронный. – URL: https://www.w3.org/TR/xmldsig-core1/ (дата обращения: 15.07.2021).

14. **ISO/IEC** TS 23078-3:2020 Information technology – Specification of DRM technology for digital publications – Part 3: Device key-based protection // Сайт ISO. – 2020. – Текст : электронный. – URL: https://www.iso.org/standard/79486.html (дата обращения: 29.06.2021).

15. **Readium** : сайт / Readium Foundation. – 2018. – Текст : электронный. – URL: https://readium.org/index.html (дата обращения: 16.07.2021).

REFERENCES

1. **Rossiyskaya** Federatsiya. Zakony. Grazhdanskiy kodeks Rossiyskoy Federatsii : GK : tekst s izmeneniyami na 1 iyulya 2021 g. – Tekst : elektronnyy // Elektron. fond pravovyh i normativno-tehnicheskih dok-ov: [sayt]. – 2021. – URL: https://docs.cntd.ru/document/9027690 (data obrashcheniya: 15.07.2021).

2. **Rossiyskaya** Federatsiya. Zakony. Ugolovnyy kodeks Rossiyskoy Federatsii : UK : tekst s izmeneniyami na 1 iyulya 2021 g. – Tekst : elektronnyy // Elektron. fond pravovyh i normativno-tehnicheskih dok-ov: [sayt]. – 2021. – URL: https://docs.cntd.ru/document/9017477 (data obrashcheniya: 15.07.2021).

3. **Rossiyskaya** Federatsiya. Zakony. Kodeks Rossiyskoy Federatsii ob administrativnyh pravonarusheniyah : tekst s izmeneniyami na 1 iyulya 2021 g. – Tekst : elektronnyy // Elektron. fond pravovyh i normativno-tehnicheskih dok-ov: [sayt]. – 2021. – URL: https://docs.cntd.ru/document/901807667 (data obrashcheniya: 15.07.2021).

4. **Tulchinskiy A.** Kriptosistemy s otkrytym klyuchom / A. Tulchinskiy. – Tekst : elektronnyy // www.comprice.ru: [sayt]. – 2003. – URL: http://www.comprice.ru/articles/detail.php?ID=41120 (data obrashcheniya: 15.07.2021).

5. **International** Digital Publishing Forum : сайт. – 2017. – URL: http://idpf.org/901807667 (data obrashcheniya: 15.07.2021). – Arhivnaya versiya. – Tekst : elektronnyy.

6. **Timoshenko I. V.** Razvitie i standartizatsiya elektronnyh formatov dokumentov v izdatelskoy i bibliotechnoy deyatelnosti / I. V. Timoshenko // Biblioteki i obrazovanie : ezhegodnyy mezhvedomstvennyy sbornik nauchnyh trudov. – Moskva : GPNTB Rossii, 2018.

7. **LeetRes** DRM // Sayt LeetRes. – Tekst : elektronnyy. – 19.01.2018. – URL: https://docs.litres.ru/pages/viewpage.action?pageId=6425428#id-ЛитРесDRM-ЛитРесDRM удобен для пользователя (data obrashcheniya: 03.09.2021).

8. **Star Force** : Zashchita elektronnyh dokumentov i programmnogo obespecheniya : sayt. – 2021. – URL: https://www.star-force.ru/solutions/electronic-documents-security/ (data obrashcheniya: 15.07.2021). – Tekst : elektronnyy.

9. **ISO/IEC** TS 23078-1:2020 Information technology – Specification of DRM technology for digital publications – Part 1: Overview of copyright protection technologies in use in the publishing industry // Sayt ISO. – 2020. – Tekst : elektronnyy. – URL: https://www.iso.org/standard/79484.html (data obrashcheniya: 29.06.2021).

10. **Readium** LCP Specifications industry // Sayt Readium. – Tekst: elektronnyy. – URL: https://readium.org/lcp-specs/ (data obrashcheniya: 16.07.2021).

11. **ISO/IEC** TS 23078-2:2020 Information technology — Specification of DRM technology for digital publications – Part 2: User key-based protection // Sayt ISO. – 2020. – Tekst : elektronnyy. – URL: https://www.iso.org/standard/79485.html (data obrashcheniya: 29.06.2021).

12. **XML** Encryption Syntax and Processing Version 1.1 : W3C Recommendation // Sayt W3C. – 2013. – Tekst : elektronnyy. – URL: https://www.w3.org/TR/xmlenc-core1/ (data obrashcheniya: 15.07.2021).

13. **XML** Signature Syntax and Processing Version 1.1 : W3C Recommendation // Sayt W3C. – 2013. – Tekst : elektronnyy. – URL: https://www.w3.org/TR/xmldsig-core1/ (data obrashcheniya: 15.07.2021).

14. **ISO/IEC** TS 23078-3:2020 Information technology – Specification of DRM technology for digital publications – Part 3: Device key-based protection // Sayt ISO. – 2020. – Tekst : elektronnyy. – URL: https://www.iso.org/standard/79486.html (data obrashcheniya: 29.06.2021).

15. **Readium** : sayt / Readium Foundation. – 2018. – Tekst : elektronnyy. – URL: https://readium.org/index.html (data obrashcheniya: 16.07.2021).

Информация об авторе / Information about the author

Тимошенко Игорь Владимирович – канд. техн. наук, ведущий научный сотрудник ГПНТБ России, Москва, Российская Федерация

timigor@gpntb.ru

Igor V. Timoshenko – Cand. Sc. (Engineering), Leading Researcher, Russian National Public Library for Science and Technology, Moscow, Russian Federation

timigor@gpntb.ru