Научная статья
УДК 004.45
DOI: https://doi.org/10.17323/tis.2021.13515

Original article

ТСЗАП В СФЕРЕ ЗАЩИТЫ ЦИФРОВОГО КОНТЕНТА: ПРАКТИЧЕСКИЙ ОПЫТ СОЗДАНИЯ ВЕБ-ИНСТРУМЕНТОВ

DRM AS DIGITAL CONTENT PROTECTION TECHNOLOGY: PRACTICAL EXPERIENCE WITH WEB TOOLS DEVELOPMENT

Михаил Иванович ДЕМИДОВ
Национальный исследовательский университет «Высшая школа экономики», Москва, Россия
mi@demidov.us
https://orcid.org/0000-0002-3093-4926

Информация об авторе
М.И. Демидов — кандидат философских наук, заместитель начальника управления инновационной деятельности, генеральный директор ООО «Сайенслист»

Аннотация. Развитие рынка цифрового контента в мире инспирирует разработку системы защиты медиаматериалов от несанкционированного копирования и просмотра в целях повышения безопасности сервисов правообладателей. Создание такой системы защиты, позволяющей разграничивать уровни доступа к запрашиваемой информации, обеспечивает появление комплексного программного обеспечения для работы в веб-обозревателях, мобильных приложениях и интеграционных модулях для систем управления веб-контентом.

Ключевые слова: антипиратство; защита контента; DRM; технические средства защиты авторских прав; ТСЗАП

Для цитирования: *Демидов М.И.* ТСЗАП в сфере защиты цифрового контента: практический опыт создания веб-инструментов // Труды по интеллектуальной собственности (Works on Intellectual Property). 2021. Т. 39, № 4. С. 74–79.
DOI: https://doi.org/10.17323/tis.2021.13515

Mikhail I. DEMIDOV
National Research University Higher School of Economics
mi@demidov.us
https://orcid.org/0000-0002-3093-4926

Information about the author
M.I. Demidov — PhD in Philosophy, Deputy Chief of Innovation and Enterprise Office at National Research University «Higher School of Economics», Chief Executive Officer at ScienceList LLC

Abstract. The growth of world digital content market leads to the development of special released media system with protection from unauthorized access, copying and viewing and increasing safety on copyright holders' servers. Such protection system which is able to delineate access levels to sensitive information, leads to the appearing of universal software for web-browsers, mobile applications and integration middleware at web content management.

Keywords: antipiracy; content protection; DRM; technical tools for copyright protection

For citation: *Demidov M.I.* DRM as digital content protection technology: practical experience with web tools development // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2021. Vol. 39 (4). P. 74–79.
DOI: https://doi.org/10.17323/tis.2021.13515

Ускорение развития науки, технологий и инноваций влечет за собой радикальную трансформацию рынков, бизнес-моделей, способов производства и распространения продуктов и услуг, институтов и социокультурных отношений. Бурный рост неструктурированной информации в сфере науки, технологий и инноваций, которая уже не поддается анализу традиционными методами, становится серьезным вызовом для принятия доказательных и своевременных решений. Только сейчас стало возможным ответить на этот вызов благодаря прогрессу средств обработки больших текстовых данных, защита которых должна быть обеспечена в интернете.

Рынок цифрового контента в России и в большинстве стран появился около 20 лет назад и за это время стал одним из крупнейших сегментов экономики. Товарами служат информационно-развлекательные материалы: аудио, видео, тексты, игры, приложения. Для организации продаж используются виртуальные площадки (магазины приложений, «сторы»), файлы распространяются по цифровым каналам.

Важнейшим условием формирования культуры легального потребления пользователем высококачественного цифрового контента является необходимость развитой инфраструктуры управления доступом к нему. Весомый фактор — эволюция устройств для потребления цифрового контента. Взрывной рост популярности смартфонов и планшетов способствует всеобщей «мобилизации» рынка, получают все большую популярность системы распространения цифрового контента, создаются мультиплатформенные решения — ресурсы и сервисы, предоставляющие доступ к контенту со всех возможных устройств (смартфонов, планшетов и пр.). Поэтому крайне важно разработать эффективные методики и механизмы, регулирующие доступ к цифровому контенту в интернете не только с ПК пользователя, но и при помощи мобильных приложений, рассчитанных на использование различными устройствами.

Система защиты цифрового контента в вебе актуальна в настоящее время и в связи с принятием «антипиратских» законов (например, законопроект «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях») и усилением контроля со стороны Роскомнадзора. Игроки интернет-рынка вынуждены защищать собственный контент от несанкционированного копирования, чтобы выйти из-под ответственности за потенциальные нарушения. Вступившая в силу с 1 января 2008 г. четвертая часть Гражданского кодекса РФ существенно ограничивает деятельность медиаплощадок, связанную с предоставлением во временное безвозмездное пользование экземпляров произведений, защищенных авторских правом, в цифровой форме. Согласно данному закону, это разрешено только при условии исключения возможности создать цифровые копии этих произведений.

Защита от нелегального распространения цифрового контента — одна из основных задач, требующих решения со стороны правообладателя и автора. Типовым подходом к решению задачи является внедрение в приложение для воспроизведения контента некоторого кода DRM-системы (англ. Digital Rights Management — концепция программных и программно-аппаратных средств, позволяющих организовать управление цифровым контентом при помощи моделей разграничения прав доступа на основе лицензии, роли пользователя, привязки к устройству и так далее), который обеспечивал бы неработоспособность приложения без наличия некоторого трудно копируемого внешнего по отношению к приложению объекта (объекта привязки). Внедряемый код DRM-системы должен быть хорошо связан с приложением, чтобы его сложно было бы удалить или заблокировать.

В связи с ростом вычислительных мощностей увеличиваются требования к устойчивости алгоритмов шифрования. Существующие системы управления цифровым контентом имеют невысокую степень защиты от взлома путем реверс-инжиниринга и подмены устанавливаемых драйверов (могут быть взломаны за несколько недель или месяцев), что позволяет при определенных условиях получать доступ к защищенным документам без санкции правообладателя (взламываются программные проигрыватели контейнеров с контентом, используется перехват ввода-вывода информации для получения исходного файла и так далее). Так, известно, что для большинства существу-

ющих DRM-решений на базе привязки к компьютеру конечного пользователя по активационному ключу есть возможность получения генератора ключа, если для его создания не используется криптография с открытым ключом.

Несмотря на очевидность данной угрозы, многие производители DRM-систем отказываются от применения криптографии с открытым ключом из-за большой длины ключа и упрощения атаки методом модификации кода DRM (типовые алгоритмы трудно защитить от анализа и модификации). Также есть возможность создания эмулятора путем взлома и восстановления программы микроконтроллера, используемого в ключе. Сюда относится и возможность изменения данных о лицензии в памяти микроконтроллера. Случаи использования данной уязвимости очень редки. Некоторые производители ключей предлагают штатные средства их эмуляции для целей отладки. Анализ таких средств также может помочь злоумышленнику. Наконец, у DRM-решений на базе электронного ключа или смарт-карты есть возможность создания эмулятора путем анализа протокола обмена данными между защищенным приложением и ключом. Теоретически в ключе можно реализовать сколь угодно сложный код, что сделало бы данную уязвимость несущественной, однако на практике часто данный вопрос плохо проработан (как разработчиками систем DRM, так и программистами, осуществляющими интеграцию системы DRM с приложением), что делает данную уязвимость наиболее важной.

В российском законодательстве для DRM используется термин «технические средства защиты авторских прав» (ТСЗАП). Так, согласно ст. 1299 ГК РФ, «техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения».

При этом законом установлено, что в отношении произведений не допускаются: осуществление без разрешения автора или иного правообладателя действий, направленных на то, чтобы устранить ограничения использования произведения, установленные путем применения технических средств защиты авторских прав; изготовление, распространение, сдача в прокат, предоставление во временное безвозмездное пользование, импорт, реклама любой технологии, любого технического устройства или их компонентов, использование таких технических средств в целях получения прибыли либо оказание соответствующих услуг, если в результате таких действий становится невозможным использование технических средств защиты авторских прав либо эти технические средства не смогут обеспечить надлежащую защиту указанных прав.

За последние 10 лет в научных журналах было опубликовано несколько российских исследований по теме DRM (в частности, [1, 2, 3]). Более актуальные публикации — за 2018–2020 гг. — можно найти в менее известных научных журналах, попадающих в РИНЦ (например, [4, 5]. В них авторы приводят преимущественно общие подходы к определению DRM-защиты и истории применения этих технологий для медиа на примере музыкальных файлов и видеофильмов.

Также в России зарегистрировано не менее трех патентов. Это «Устройство и способ поддержки обмена содержимым между доменами с отличающимися DRM» (авторы Йоон Ки Сонг, Дзеонг Дзеон Дзеонг, Хванг Сеонг Оун, Нам До Вон, Ким Дзеонг Хиун, Парк Дзи Хиун, Дзеонг Санг Вон, Ким Дзун Ил, Ахн Сеонг Мин, Ким Сеонг Хан, Дзанг Ван Хо; опубликован в 2009 г., принадлежит «Электроникс Энд Телекоммьюникейшнз Рисерч Институт Инка Энтуоркс, ИНК.»); «Улучшенная система цифрового управления правами (DRM)» (авторы Бакс Ваутер, Камперман Франсискус Л.А.Й., Ленуар Петрус Й., Шостек Лукаш;, опубликован в 2011 г., принадлежит «Конинклейке Филипс Электроникс Н.В.»); российский патент «Способ управлениями лицензиями в DRM-системе» (А.Н. Зацепин и ООО «Протекшен Технолоджи Ресерч», датирован 2013 г.).

По теме DRM/ТСЗАП в России достаточно мало исследовательских работ, направленных на развитие непосредственно программного обеспечения в области мультимедиа-контента. Одной из немногих диссертаций по этой теме можно считать работу А.Н. Березина «Методы повышения уровня безопасности защитных преобразований информации», защищенную в 2016 г. в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В.И. Ульянова (Ленина).

Одной из компаний, занимающихся научно-исследовательской работой в сфере информационной безопасности применительно к защите цифрового контента от нелегального использования, является ООО «Сайенслист». Ее руководитель — Михаил Иванович Демидов — занимается НИР, посвященными охране цифрового авторского контента. В рамках исследований был сформирован достаточно большой научный задел по реализации НИОКР, который состоит из трех объектов интеллектуальной собственности — программы для ЭВМ «Программный комплекс для защиты авторского цифрового контента для веб-приложений ScienceDRM Cloud Edition», со-

зданной в 2017 г.; программы для ЭВМ «Программное обеспечения для организации мультиарендного доступа к сервисам защиты, хранения и предоставления цифрового контента (версия 1.0)», созданной в рамках выполнения госконтракта в 2020 г., а также программы для ЭВМ для защиты авторского цифрового контента ScienceDRM, зарегистрированной в 2014 г. и описывающей логику работы этих модулей решения.

В научно-техническом отчете 2017 г. о выполнении НИОКР по теме «Разработка клиент-серверного приложения для защиты авторского цифрового контента, а также предоставления авторизованного доступа к нему с разграничением прав» разработчик решения ScienceDRM — коллектив ООО «Сайенслист» — исследовал способы организации архитектуры такого решения [6].

Исследование показало, что качественная и оптимальная архитектура разрабатываемого решения должна интегрировать следующие преимущества:

1) соответствие стандарту REST API программного интерфейса для взаимодействия с внешними программными продуктами, разработанными на любых платформах с поддержкой REST API;

2) возможность изменять оформление встраиваемого виджета под целевой ресурс при помощи технологий CSS; изолированность контекста данных виджета;

3) принудительное шифрование клиент-серверной передачи данных, то есть обеспечение механизмов переброса маршрутов (реороутинг) запросов в защищенные каналы, в том числе SSL;

4) наличие механизмов защищенного обмена (шардинга) хранимых данных для использования сессионных сетей доставки контента;

5) наличие готовых к использованию пользовательских сценариев и автогенерируемого виджета интерфейса для пользовательского взаимодействия;

6) программный код, разработанный с расчетом подключения сообщества независимых разработчиков к развитию программного продукта, в том числе с открытым исходным кодом.

В создаваемом программном обеспечении не предполагаются хранение и обработка конфиденциальной информации, в том числе персональных данных. При этом система должна соответствовать следующим требованиям к защите информации:

1) обеспечивать конфиденциальность, целостность и доступность обрабатываемой в сервисе информации предотвращением несанкционированного доступа неуполномоченных лиц, копирования, распространения, модификации, уничтожения и блокирования;

2) реализовывать разграничение доступа всех пользователей, включая администраторов системы и администраторов безопасности, к информации, обрабатываемой в сервисе, а в случае обработки конфиденциальной информации — предоставлять возможность управления списком пользователей, допущенных к обработке конфиденциального документа, и предоставляемыми этим пользователям правами: «только чтение», «модификация», «разрешена печать» и «управление доступом к документу»;

3) организовывать с помощью SSL-сертификата криптографическую защиту информации, передаваемой по каналам данных, в соответствии с требованиями Законодательства РФ и уполномоченных государственных органов;

4) иметь функции сбора (журналирования) событий безопасности, выполняющие регистрацию следующих действий администраторов и пользователей: дата, время и результат входа/выхода в сервис (успешный/неуспешный/несанкционированный/отказ в доступе и т.п.); создание/удаление/модификация учетных записей администраторов и пользователей и предоставление/изменение им прав доступа; содержание вносимых пользователями и администраторами изменений в данные, обрабатываемые в сервисе, в том числе создание, копирование, удаление и модификация отдельных записей, документов и иных информационных сущностей;

5) обеспечивать целостность и достоверность журнала безопасности, а также сбор событий, связанных с журналом (очистка, модификация);

6) предоставлять инструментарий для анализа накопленной в журнале администратора безопасности информации, поиска по критериям и фильтрации событий информационной безопасности, создания собственных отчетных форм и подготовки отчетов;

7) реализовывать возможность выгрузки журнала событий безопасности администратором безопасности в табличном виде (csv, xls, xml и т.п.);

8) формировать шаблоны отчетных форм, доступные через интерфейс администратора безопасности, структура и содержание которых определяется на этапе проектирования сервиса;

9) программное обеспечение должно быть развернуто внутри периметра безопасности заказчика, на оборудовании, управляемом и администрируемом работниками заказчика;

10) сервисы и приложения программного обеспечения должны запускаться с минимально необходимыми правами и не должны запускаться с правами администратора домена и выше;

11) все учетные записи должны иметь минимально необходимые полномочия;

12) все учетные данные для проверки подлинности (например, пароли/парольные фразы) должны передаваться только в зашифрованном виде с использованием стойкого алгоритма шифрования не ниже TLS 1.2 и храниться только в виде результата необратимого преобразования (хэш) алгоритмом не хуже SHA-256 (или аналогичного по стойкости) на всех компонентах сервиса;

13) должна быть обеспечена возможность автоматического отключения сессии пользователя после заданного (не более 10 минут) периода его неактивности;

14) при использовании в сервисе приложений, построенных на основе веб-технологий, должна обеспечиваться защита от наиболее распространенных типов атак на данный класс приложений типа SQL-injection, cross-site scripting, buffer overflow;

15) должны быть предусмотрены механизмы контроля работоспособности (тестирования) механизмов защиты информации.

Алгоритм модуля обработки и предоставления информации ScienceDRM совместим с форматами входящих файлов и файлов выгрузки обслуживаемых информационных ресурсов (офисные форматы MS Office, PDF, TXT, XML, CSV). В каждом из режимов работы программного обеспечения используются различные входные данные, результаты работы в каждом из режимов также разные. Таким образом, решение имеет модульную структуру, при внедрении интегрируется с существующими системами управления контентом посредствам общепринятых протоколов и концепций обмена данными (REST), обеспечивает защищенность контента.

В рамках проекта НИР ООО «Сайенслист» была создана масштабируемая гибкая система защиты цифрового контента, позволяющая разграничивать уровни доступа к запрашиваемому медиаматериалу (текст, изображение, презентация, видео, аудио) согласно ролевой модели и контролю условий предоставления цифрового контента правообладателями с интеграцией с системой биллинга и сбором статистики. Продукт обеспечивает шифрование и нанесение цифровых водяных знаков на цифровой контент. Архитектура сервиса исключает любую выдачу незащищенного контента за пределы системы распределенного хранения цифрового контента (выдача по сильно защищенным ссылкам в средстве просмотра веб-документов, которыми нельзя воспользоваться для выкачивания контента). Цифровой документ, просматриваемый постранично в защищенном таким способом виджете, невозможно скопировать вручную в неизменном виде. Разработка и применение дорогостоящих средств автоматизации и распознавания текста с экрана (для обхода этого ограничения) в таком контексте становятся бессмысленными при наличии недорогого доступа к легальному (санкционированному правообладателем, автором, администратором сайта) просмотру контента с возможностью эквайринга (приема платежей) за право доступа к защищенному контенту. Результатом этого проекта стала комплексная программная веб-платформа с личным кабинетом, биллингом, встраиваемой библиотекой для защищенного просмотра контента (виджетом) и интеграции на интернет-сайты (по аналогии с собственными средствами просмотра у Google Books, SlideShare, Scribd) и масштабируемой инфраструктурой.

Разработка такой программной платформы позволила: создать эффективный в контексте технической реализации механизм защиты цифрового контента от несанкционированного доступа; интегрировать решение по защите цифрового контента в большинство существующих систем управления контентом (CMS) через гибкий программный интерфейс (API); создавать различным разработчикам новые контентные решения, которые будут масштабироваться по мере расширения аудитории, производственных мощностей; значительно упростить создание коммерческих продуктов на базе дистрибуции авторского цифрового контента.

СПИСОК ИСТОЧНИКОВ

1. *Никифоров М.Д.* Контейнер защищенного воспроизведения как метод защиты информации в системах дистанционного обучения // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 378–382.
2. *Любименко А.И., Чигиринова М.В.* Проблемы защиты авторского права в электронных и интернет-изданиях и пути их решения // Печать и слово Санкт-Петербурга (Петербургские чтения – 2016): сборник научных трудов XVIII Всероссийской научной конференции. В 2-х частях. СПб: ИПЦ СПГУТД, 2017. С. 86–90.
3. *Куканов А.А.* Современные средства защиты видеоконтента в сети Интернет // Международный студенческий научный вестник. 2016. № 2. С. 128.
4. *Циноева А.В.* Самозащита авторских прав в сети Интернет при помощи технических средств защиты авторских прав // Аллея науки. 2020. Т. 2. № 5 (44). С. 625–632.
5. *Черный А.В.* Технологии охраны результатов интеллектуальной деятельности // Технологии XXI века в юриспруденции: Материалы Всероссийской научно-практической конференции / под ред. Д.В. Бахтеева). Екатеринбург, Уральский государственный юридический университет, 2019. С. 166-170.

6. ООО «Сайенслист». Сведения о результатах научно-исследовательской работы с отчетом № AAAA-Б17-217041310031-9 https://esu.citis.ru/ikrbs/XHW7RWWGCWDBUJLF3LXUBNGE (дата обращения: 01.12.2021).

REFERENCES

1. *Nikiforov M.D.* Konteyner zashchishchonnogo vosproizvedeniya kak me-tod zashchity informatsii v sistemakh distantsionnogo obucheniya // Iz-vestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki. 2013. No. 3. S. 37–382.
2. *Lyubimenko A.I., Chigirinova M.V.* Problemy zashchity avtorskogo prava v elektronnykh i internet-izdaniyakh i puti ikh resheniya // Pe-chat' i slovo Sankt-Peterburga (Peterburgskiye chteniya – 2016) Sbor-nik nauchnykh trudov XVIII Vserossiyskoy nauchnoy konferentsii. V 2-kh chastyakh. SPb, 2017. S. 86-90.
3. *Kukanov A.A.* Sovremennyye sredstva zashchity vid-eokontenta v seti Internet // Mezhdunarodnyy stu-dencheskiy nauchnyy vestnik. 2016. No. 2. P. 128.
4. *Tsinoyeva A.V.* Samozashchita avtorskikh prav v seti "Internet" pri pomoshchi tekhnicheskikh sredstv zashchity avtorskikh prav // Alleya nauki. 2020. T. 2. No. 5 (44). S. 625–632.
5. *Chernyy A.V.* Tekhnologii okhrany rezul'tatov intellektu-al'noy deya-tel'nosti // Tekhnologii XXI veka v yurispru-dentsii: Materialy Vserossiyskoy nauchno-prakticheskoy konferentsii / pod redaktsiyey D.V. Bakhteyeva. Ekater-inburg. 2019. S. 166–170.
6. OOO "Sayyenslist", Svedeniya o rezul'tatakh nauchno-issledovatel'skoy raboty s otchotom No. AAAA-B17-217041310031-9 https://esu.citis.ru/ikrbs/XHW7RWWGCWDBUJLF3LXUBNGE (data obrashche-niya: 01.12.2021).