

др *Вугоје СПАСИЋ*
доцент Правног факултета Универзитета у Нишу

ДИГИТАЛНО УПРАВЉАЊЕ ПРАВИМА

Резиме

Дигитална технологија доводи до суштинских промена одређених аспеката ауторској и сродних права. Ново, изв. мрежно окружење нужно захтева нове начине заштите интелектуалних стваралаца и њихових права од неовлашћених употреба њихових творевина. Као одговор на новонастале проблеме појављује се различите технике криптирације, као и систем дигиталној управљања правима, енгл. „Digital Rights Management“. Овај систем базира се на коришћењу дигиталне технологије а усмерен је на заштити ауторској равној зашћеној садржаја, управо, од саме технологије. Генерално, „Digital Rights Management“ представља ошћи назив за скуи технологија које носиоцима права омоућавају контролу употребе дигиталној садржаја од стране корисника, односно публике (јавности). За сада најважније технике дигиталној управљања правима представљају digital watermarking и trusted computing.

Кључне речи: *дигитална дела, управљање правима, дигитална заштита.*

I Увод у систем дигиталног управљања правима

Дигитално окружење мења многе стандарде и узусе у области интелектуалног стваралаштва. Да би ауторско право могло да превлада тешкоће и искушења са којима се сусреће потребне су одговарајуће промене и прилагођавања. У том смислу, поред досадашњих стандардних

мера и активности усмерених на заштиту духовних творевина и интелектуалних права потребне су и нови додатни потези и инструменти усмерени ка том циљу. Један од кључних чинилаца очувања и развоја интелектуалног стваралаштва представља дигитална заштита ауторских права. Ово је један веома комплексан и сложен феномен. Он обухвата све начине за контролу коришћења садржаја заштићених ауторским правима, а који се остварује уз помоћ техничко-технолошких средстава. Поред криптографије, кључну улогу у заштити ауторских дела има систем назван „Дигитално управљање правима“.

У најширем смислу, дигитално управљање правима (енгл. „*Digital Rights Management*“ – *DRM*) представља заједнички назив за скуп технологија које свим носиоцима ауторских права омогућују контролу употребе неког дигиталног записа, односно садржаја ма које врсте. Овај појам има додирних тачака са заштитом од копирања (енгл. *copy protection*), али *DRM* системи се, пре свега, користе за заштиту духовних (интелектуалних) садржаја, као што су музика и филм, док се заштита од копирања најчешће односи на програмску подршку (енгл. *software*). Суштински, дигитална заштита ауторских права укида власнику дигиталног медијума потпуну контролу над њим и преноси је компјутерском програму.

Менаџмент дигиталних права треба да омогући компромис између безбедности садржаја, коју захтева власник, односно носилац права, приватности крајњег корисника (уживаоца), као и цене система који ће бити коришћен између учесника у том ланцу. У дигиталном свету, безбедност и приватност се имплементирају коришћењем разних криптографских алгоритама и протокола. На самом крају ланца, дигитални садржај се приказује у аналогној форми: дигитална слика се трансформише у светло путем дисплеја, док се дигитални звук трансформише у акустичке таласе. Уз то, поновна дигитализација ових аналогних сигнала увек је могућа.¹

DRM системи представљају један је од највећих изазова дигиталног доба. Одмах на почетку треба истаћи да се синтагма „*Digital Rights Management*“ односи на „дигитално управљање правима“ („*digital management of rights*“), а не на „управљање дигиталним правима“ („*management of digital rights*“). То значи да се овај систем бави управљањем *свих* права, а не само оних примењивих на дозволе које се тичу приступања дигиталним садржајима. С друге стране, суштински, права су јединствена и не постоји подела на аналогна и дигитална права, већ такви могу бити само предмети (објекти) заштите, односно заштићени садржаји.

1 Иако је контрола умножавања и коришћења програмске подршке с прекидима у употреби од 70-их година 20-ог века, назив *DRM* односи се пре свега на интелектуалне садржаје, као што су, нпр. уметничка или књижевна дела.

Нема никакве сумње да је неовлашћену употребу „класичног“, или тзв. „аналогног“ садржаја знатно лакше спречити, пре свега захваљујући самој „физичкој“ природи материјала, која представља одређену брану и помаже при заштити ауторских права. Насупрот томе, захваљујући информатичкој технологији данас смо суочени са озбиљним угрожавањем и кршењем ауторских права. Ово је само природан рефлекс чињенице да се дигитални садржај може много лакше умножавати и трансмитовати на разне начине.

Технологије дигиталног управљања правима могуће је, према подручју примене, поделити на технологије коришћене за заштиту видео садржаја, односно филмова, аудио садржаја, односно музике, и технологије за заштиту докумената.

Могућности и начини примене *DRM* технологије су, практично бесконачни. Ево само неколико типичних примера њене примене:

- Компанија подешава своје сервере електронске поште тако да блокирају слање електронских порука које садрже осетљиве, тј. тајне информације.
- *E-book* сервер ограничава приступ, копирање и штампање електронских књига по правилима носиоца ауторских права.
- Филмски студио на својим *DVD*-има поставља софтвер који ограничава број копија које корисник може да сачини.
- Дискографска кућа издаје своје наслове на специјалним *CD*-има који садрже елементе дизајниране за збуњивање програма за екстракцију аудио дискова.

Централни (али не и једини) део савремених *DRM* система представља техника водермаркига (воденог жига), која подразумева утискивање дигиталних сигнала у виду жигова, како би се остварило праћење и контрола дигиталних копија, чак и приликом трансформације у аналогне сигнале. Сусретање са проблемом специфичних верзија таласних сигнала, укључујући и њихово аналогно представљање, доводи до сложених критеријума. Процес водермаркига може да се посматра кроз анализу ризика (са аспекта провајдера), као и преко анализе добити крајњег корисника (уживаоца дела). Као најважније намеће се питање који је ризик за провајдера, ако уведе водермаркинг, као и која би корист за крајњег корисника, ако покуша да уклони водени жиг са дигиталног медијума.

Један од главних циљева и задатака *DRM* технологија јесте идентификовање и анализира потенцијалне слабости у безбедности на сваком пункту дистрибуционог ланца, као и предлагање мера и средства које треба предузети у циљу њиховог превазилажења.

Прва генерација *DRM*-а усредсређена је на сигурност и енкрипцију као средства заштите од неовлашћеног копирања. На тај начин чини се покушај да се садржај на неки начин „закључа“ и ограничи његова дистрибуција само на овлашћене кориснике, односно оне који плате за његово коришћење. Ипак, могућности *DRM* а пуно су шире од тога и то користи друга генерација овог система. Друга генерација ових система обухвата опис, идентификацију, размену, заштиту, посматрање и праћење свих начина употребе права било опипљивог, било неопипљивог садржаја.

E-DRM (енгл. *Enterprise – DRM*) је заједнички назив за све технологије управљања дигиталним правима коришћеним за заштиту пословних докумената у различитим форматима, као што су *Microsoft Word*, *PDF* (енгл. *Portable Document Format*), *AutoCAD*, електронска писма и веб странице унутар интерне рачунарске мреже неке организације.²

Суштински, приликом дизајнирања и имплементације *DRM* система треба обратити пажњу на две кључне архитектуре. Прва је функцијска архитектура (*Functional Architecture*), која покрива *high-level* модуле и компоненте *DRM* система који осигуравају *end-to-end* управљање правима. Друга је информацијска архитектура (*Information Architecture*). Она обухвата моделирање ентитета унутар *DRM* система као и њихове односе. Постоје још и концептуални, модуларни, извршни и кодни слојеви архитектуре (*Conceptual, Module, Execution and Code layers*).

У наставку рада детаљније ћемо обрадити систем и функционисање *DRM* технологија. Уз историјски осврт, даћемо приказ најчешће коришћених технологија за заштиту видео и аудио садржаја, кратак преглед правних аспеката имплементације ових технологија и опис њихових најзначајнијих недостатака.

Генерално, основна намена *DRM* технологија је контрола коришћења дигиталних садржаја путем онемогућавања приступа, умножавања, трансмисије и претварања у друге формате. Кроз историју, аутори, власници (носиоци) ауторских права, као и корисници ауторских дела противили су се технологијама које омогућују копирање садржаја. Примери управљања правима, пре настанка дигиталних технологија, обухватају заштиту перфорисаних трака намењених механичким клавирима с почетка 20. века и заштиту аудио и видео магнетских трака.

Дигитални формати записа садржаја знатно олакшавају умножавање (у форми копирања и сл.) садржаја због чега су умногостручени напори власника ауторских права уложени у њихову заштиту. Оно што

2 Сопствене *DRM* технологије за заштиту докумената поседују фирме: *Microsoft*, *Adobe Systems*, *Liquid Machines*, *Oracle*, *EMC Corporation* и друге.

је веома карактеристично, то је да се узастопним копирањем садржаја с аналогних медијума неизбежно губи квалитет, док се дигитални медијуми, понекад чак и током нормалне употребе, могу копирати неограничен број пута без икаквог губитка квалитета. Ово, стога, што у дигиталној технологији нема никакве разлике између оригиналног и копирног примерка. Популаризација личних рачунара, лакоћа снимања садржаја аудио *CD* медија (енгл. *CD ripping*) и радио емисија, уз популарне сервисе за размену датотека на интернету, учинили су размену неовлашћених копија заштићених садржаја (енгл. *digital piracy*) изузетно лако, брзо и јефтино.

Дигитално управљање ауторским (и сродним) правима над заштићеним садржајима највише се користи у забавној индустрији (нарочито у филмској и музичкој индустрији), али се појављује и у другим сегментима.³

II Архитектура *DRM*

1. Функцијска архитектура

Целокупна окосница *DRM*-а намењена стварању система за заштиту права може се поделити у три основна подручја:

- *Intellectual Property (IP) Asset Creation and Capture* (стварање имовине и задржавање интелектуалне својине): односи се на могућност како управљати стварањем одређеног садржаја да би се он могао размењивати. Ово укључује утврђивање и учвршћивање права након што је садржај првобитно креиран (или поново употребљен и проширен од лица које на то има право).
- *IP Asset Management* (управљање имовином и интелектуалном својином): овај део односи се на трговину створеним садржајем, односно на омогућавање и управљање тог трансфера. Ово подручје укључује преузимање садржаја од онога ко га је створио и његово укључивање у систем управљања имовином. Системи трговања требали би управљати описним подацима и подацима о правима.

3 Многе фирме које се баве дистрибуцијом и продајом музике на интернету, као што је *iTunes*, и поједини издавачи електронских књига (енгл. *e-books*) развили су различите стратегија управљања дигиталним правима. Током последњих година бројни телевизијски продуценти захтевају имплементацију *DRM* мера како би се контролисао приступ њиховим програмима због раста популарности *DRV* (енгл. *Digital Video Recorder*) уређаја.

- *IP Asset Usage* (употреба имовине обухваћене интелектуалном својином): овај део *DRM*-а посвећен је управљању употребом садржаја, након што је он пуштен у размену (продају). То укључује и подржавање одређених ограничења над размењеним садржајем употребљеним на одређеном систему/програму. Горњи модели обухватају широка подручја потребна за *DRM*. Но, они морају бити допуњени функцијском архитектуром која обезбеђује окосницу за модуле којима се имплементира функционалност *DRM*-а.

Кључни задатак функцијске архитектуре је одређивање улоге и понашање многобројних кооперативних и интероперативних модула унутар три подручја интелектуалне својине (*IP*): *Asset Creation, Management, Usage*.

Модул за стварање и одржавање имовине у оквиру интелектуалне својине (*IP Asset Creation And Capture*) подржава:

- Озакоњивање права (*Rights Validation*) – осигуравање да садржај који је креиран из неког постојећег садржаја укључује права за тај чин.
- Стварање права (*Rights Creation*) – дозвољавање да права буду додељена новом садржају, нпр. специфицирање власника права и дозвола за употребу.
- Ток стварања права (*Rights Workflow*) – дозвољавање да садржај прође кроз низ корака при којима се одобравају како садржај, тако и права.

Модул за управљање имовином под окриљем интелектуалне својине (*IP Asset Management*) подржава:

- Функције за складиштење (*Repository functions*) – омогућавање приступа/побољшавања садржаја у потенцијално дистрибуираним базама података и приступа/побољшавања метаподатака (*metadata*).⁴
- Функције трговања (размене) (*Trading functions*) – омогућавање додељивања лиценци странама које су размениле договоре о правима на садржај. То укључује и плаћање лиценци онима који држе права над садржајем. У неким случајевима садржај мора проћи кроз низ операција да би задовољио уговор о лиценци.⁵

4 Метаподаци обухватају стране (*Parties*), права (*Rights*) и дела (*Works*).

5 Тако, на пример, може бити потребно садржај криптовалити/заштитити за неку одређену врсту употребе.

Модул за употребу имовине под интелектуалном својином (*IP Asset Usage*) подржава:

- Управљање дозволама (*Permission Management*) – обезбеђује да субјекти која употребљавају заштићени садржај поштују права везана уз њега. Тако, на пример, ако корисник има право само гледања документа, штампање му неће бити дозвољено.
- Управљање праћења (*Tracking Management*) – омогућава праћење употребе садржаја тамо где је такво праћење договорено условима постављеним у лиценци (нпр. корисник има дозволу да погледа видео снимак одређени број пута). Овај модул задужен је и за учествовање у систему трговања на начин да прати употребу и новчане трансакције у случају да је сваку употребу садржаја потребно платити.

Сва три модула заједно чине језгро функционирања *DRM* система. Такође, захтева се да модули заједнички делују са другим, постојећим *e-business* модулима (као што су *shopping carts*, *consumer personalization* итд.) и *Digital Asset Management* модулима (као што су *version control*, *updates* итд.). Било би идеално када би ови модули били пројектовани као компонента која би омогућавала системима да буду изграђени модуларно. Међутим, то би захтевало низ уобичајених и стандардних интерфејса и протокола између модула, који још не постоје. Временом, са развојем и сазревањем *DRM* технологија и индустрија ће тежити оваквој стандардизацији.

Функционална архитектура само је један од одговора изазовима *DRM*-а. Управљање правима врло брзо може постати изузетно сложено. Као резултат тога *DRM* системи морају подржавати најфлексибилнији могући информацијски модел да би на тај начин осигурали ове сложене и слојевите везе. Због тога *DRM* системе, осим функцијске чини и информацијска архитектура.

2. Информацијска архитектура

Информацијска архитектура односи се на начине моделирања појединих ентитета у свеопшту окосницу *DRM*-а и на њихово повезивање. Основна питања која се тичу структуре и развоја *DRM* информацијског модела инкорпоришу:

- моделирање ентитета;
- идентификацију и опис ентитета;
- изражавање тврдњи о правима.

а) Моделирање ентитетима

Оно што је јако битно за *DRM* моделе, као и за њихове везе с другим ентитетима, јесте да буду „чисти“ и да их је могуће проширити. Основно начело модела који се користи разликује три идентитета која чине језгро система: корисници, садржај и права. Постоји више типова корисника, почев од оних који су власници права, па све до крајњих корисника (уживалаца). Садржај представља било који тип материјала у било ком стадијуму агрегације. Права су ентитет који у једном изразу окупља дозволе, забране и обавезе које корисник има према садржају. Главни разлог што се користи овакав модел јесте тај што он обезбеђује велику флексибилност приликом додељивања права било којем споју корисника и садржаја. Овакав модел (*Core Entities Model*) не ограничава коришћење садржаја у неким новим и развијеним пословним моделима (*business models*).

Према овом моделу метаподаци било којег од три ентитета морају садржавати механизам који ће ентитете међусобно спајати. Сам садржај, такође, мора бити моделиран. Главно начело при моделирању садржаја је то да се садржај мора састојати од више „нивоа“ (*levels*) из различитих интелектуалних стадијума, односно мора се видети еволуција његовог развитка. Такав модел омогућује јасније дефинисање информације о правима. Као пример можемо узети неки садржај и поделити га у следеће слојеве: рад (дело; *Work*), приказе дела (*Expression*), начине приказа дела (*Manifestation*), конкретне предмете (*Items*). Сваки од ових слојева може подржавати различита права и власнике права.

Слојеви садржаја дефинисани као дело (засебна интелектуална или уметничка творевина) и приказ дела (интелектуална или уметничка реализација рада) одражавају учен или креативан садржај. С друге стране, остали слојеви садржаја одражавају физички или дигитални облик садржаја.

Оно што је најбитније у оваквом моделу јесте то да у било којем тренутку можемо препознати различите власнике права. Потреба за мало другачијим приступом додељивања права јавља се када је садржај састављен од мноштва делова.⁶ Неки од ових делова могу бити повезани са различитим правима и мора постојати могућност да се то разазна када посматрамо садржај као целину.

б) Идентификација и опис ентитетима

Основни принцип је да сви ентитети морају бити јасно идентификовани и описани. Идентификација модела постиже се помоћу отво-

6 Ово нарочито долази до изражаја код дигиталних слика.

рених и стандардних механизма, одређених за сваки поједини ентитет. У сваком случају, мора постојати могућност идентификовања како ентитета, тако и метаподатака. Постоје неки стандарди који се користе за овакву идентификацију права (*Uniform Resource Identifiers (URI)*, *Digital Object Identifiers (DOI)*, *ISO International Standard Textual Work Code (ISTC)*).

Садржај би требало да буде описан најприкладнијим стандардом метаподатака за тај жанр. Врло је битно да у овим стандардима нису садржани елементи метаподатака који се односе на информацију о управљању правима, јер би то довело до нејасноћа о томе где су описани изрази о правима.⁷

в) Изражавање њврђњи о ѡравима

Субјект права дозвољава изразе о дозволама, ограничењима, обавезама и осталим информацијама повезаним с правима, а које се тичу корисника и садржаја. Према томе, субјект права је јако битан, јер представља изражајност језика који се користи да би се информисало о метаподацима везаним уз права.

Ради једноставности, изрази везани уз права, такође, се моделирају. Изрази о правима састоје се из следећих делова:

- дозволе – говоре о томе што се сме учинити;
- ограничења – описују рестрикције везане уз дозволе;
- обавезе – говоре о томе што се мора учинити/осигурати/прихватити;
- власници права – говоре о томе ко су носиоци каквих права поводом чега.

Као пример израза везаног уз права можемо навести следеће: овакви изрази могу говорити о томе да неки снимак сме бити погледан максимално тачно одређени број пута, у сваком семестру, уз прописану цену. Сваки пут кад је снимак погледан носиоци права добијају проценат од наплаћеног износа. Важи принцип да, ако неко право није експлицитно наведено у изразу то значи да онда то право није ни одобрено.

ј) Пример имплементације DRM система

Један од типичних примера коришћења DRM система јесте *online ebook* трговина *OzAuthors*.⁸ Њихов циљ био је обезбедити члановима

⁷ За опис корисника најчешће се користи *vCard* стандард, као најпознатији стандард за описивање људи и организација.

⁸ *OzAuthors* услуга је коју пружа *Australian Society of Authors* у сарадњи са *IPR Systems*.

друштва (ауторима и публицистима) да на једноставан начин осигурају да се њихов садржај појави на тржишту уз ниске трошкове и максималну накнаду за власнике садржаја.

Одређене интерфејс услуге омогућавају спецификацију информација о правима. Рубрика „*Usage Rights and Pricing*“ омогућава да особа која нуди садржај да информацију о дозволама за читање и штампање, о ценама и о сигурности. Додатно се може навести и број страница које потенцијални купац може бесплатно видети да би се лакше одлучио на куповину. Други део интерфејса описује ко има права на садржај, која је улога појединог власника права, као и колики удео та особа има при подели зараде. За сваку продату књигу, власници права аутоматски добијају свој удео зараде.⁹

2. Поборници и противници *DRM* система

Паралено са појавом *DRM* система јавиле су се многе полемике и дилеме о његовој потреби и употреби. Иако се може рећи да је сама идеја *DRM*-а, у бити, позитивна, чини се да систем ипак није довољно добро развијен. Упркос неким добрим својствима и покушају да се заштите права једних, на тај се начин крше права других.

Коришћење система за дигитално управљање правима, од самих њихових почетака, предстаља извор бројних контроверзи. Несугласице које се јављају око *DRM* система, само су наставак низа конфликта између носиоца права на садржаје и поборника употребе нових технологија за копирање тих садржаја. Појавом дигиталних технологија, у овој борби превагу су почели да остварују ови потоњи.

Копирање, односно умножавање разних садржаја постало је изузетно једноставно, а појавом интернета изгубила се чак и потреба за преношењем садржаја на физичком медију. У појединим земљама су са развојем *DRM* система предложени чак и закони који захтевају да сви рачунари поседују механизме који би контролисали употребу дигиталних медија.

До данас су развијени различити *DRM* системи, али ни један од њих није успео успоставити задовољавајућу равнотежу између заштите права власника садржаја и заштите права оних који купују те садржаје. Ниједан од система до сада није успео спречити организовано, нелиценцирано, комерцијално копирање, за које нису заслужни појединци већ организоване групе „пирата“.

9 Све информације кодиране су у *HML*-у који користи језик права *ODRL*. Овакво кодирање омогућава размену информација с осталим продавцима књига који подржавају исту семантику језика. На тај начин постављени су темељи за потпуну и аутоматску интероперабилност.

3. DRM системи и њихове мане

Поборници DRM технологија тврде како су оне власницима ауторских права неопходне за онемогућавање неовлашћеног копирања и-или трансмитовања, а самим тиме и осигуравање константног прилива прихода. С друге стране, неки критичари, као што је, нпр. FSF (енгл. *Free Software Foundation*) непрофитна корпорација, истрајавају на ставу да се не ради о управљању правима већ искључиво о наметању ограничења, па они синтагму DRM пежоративно интерпретирају као: *Digital Restriction Management*. Њихов став је да власници ауторских права помоћу DRM технологија покушавају наметнути ограничења која превазилазе законске и уговорне оквире.

Други велики противник система за управљање дигиталним правима, EFF (енгл. *Electronic Frontier Foundation*) организација, ове технологије сматра начином ограничавања тржишне утакмице онемогућавањем конкуренције. Поједини критичари DRM технологија истичу како, поред спречавања злоупотребе заштићених садржаја, управљање дигиталним правима понекад, наноси неоправдану штету у виду онемогућавања њихове легалне употребе.

Осим раније изнетих позитивних карактеристика DRM-а, постоје и одређени недостаци, који никако нису занемарљиви. У даљем таксту наведени су покушаји имплементације DRM-а и неке мане које карактеришу те системе:

- Физичка заштита – користе се физичке компоненте које се прикључују на рачунар пре употребе садржаја и осигуравају легалну употребу. Проблем који се овде јавља је тај да садржај који се легално плати може бити коришћен само на једном рачунару, што ограничава мобилност, не само рачунара, већ у крајњем случају и самог његовог корисника.
- DIVX – овај назив не односи се на компресију снимака (*DivX*), већ на још један релативно неуспео покушај имплементације DRM-а. Овај систем повезује телефонску линију корисника са његовим DVD уређајем на којем ће легално прибављен садржај бити употребљен. На овај начин онемогућава се кориснику мобилна употреба садржаја. Да би га могао употребљавати на другом месту, изван куће, морао би са собом носити DVD уређај или пак пребацити рачун на другу телефонску линију.
- CSS – онемогућава се кориснику да DVD купљен у једној земљи погледа у другој. На овај начин заштита права власника садржаја је остварена у потпуности на уштрб корисника, који је садржај легално стекао, али га не може у потпуности искористити.

- Активација производа – спречава употребу производа пре него што се посебним идентификацијским кодом региструје код издавача. На овај начин производ се повезује са конфигурацијом хардвера на коме ће купљени програм бити коришћен.
- Дигитални „водени жиг“ – допушта додавање скривених порука за верификацију производа. Овакав начин заштите не ограничава употребу, али омогућује проналажење изворног носиоца права.

Као што је већ истакнуто, *DRM* технологије, ограничавањем начина употребе, власницима ауторских права омогућују контролу над заштићеним садржајима. Самим тим, *DRM* системи предмет су бројних несугласица. Наиме, увођење ограничења над употребом таквих садржаја може представљати нарушавање законских права (енгл. *Fair use rights*) власника легалних копија. *DRM* технологије мета су критика и због тога што отежавају, а у неким случајевима и потпуно онемогућују, ефикасно архивирање садржаја, као и историјска истраживања.

Противници система за управљање дигиталним правима истичу, такође, како ови системи нису ефикасни у спречавању стварања илегалних копија садржаја које би требали штитити, јер ни један *DRM* систем није, нити може бити, у потпуности отпоран на нападе. Након пробијања заштите само једне верзије неког садржаја, или у случају копирања незаштићене верзије, он постаје широко доступан путем интернета или неког другог вида комерцијалног пиратства.

Постоје различити начини заобилажења *DRM* система. На располагању су бројни методи заобилажења *DRM* система за заштиту аудио и видео садржаја:

- посредно копирање помоћу аудио *CD*-диска;
- копирање пресретањем тока података;
- аналогна рупа.

4. *DRM* – заштита права или кршење приватности?

Противници *DRM*-а посебно наглашавају да би се контролом приступа рачунару и његовим програмима, односно забраном приступа било коме осим кориснику, повећао ризик појаве проблема узрокованих приступом треће особе. Такви проблеми увелико прелазе границе заштите власника права. Тако би се могло догодити да „*bug*“ (баг) који се појави у систему за контролу употребе купљеног програма (а познато је да је вероватноћа за његову појаву врло велика), узрокује да корисник уопште не може приступити своме рачунару, нити једном његовом програму. Ово би било својерсно кршење права корисника.

Према важећој легислативи, интелектуална својина након одређеног периода пада у јавни домен, тј. постаје доступна јавности на слободно коришћење и њен власник губи сва права. Међутим, *DRM* заштитом оваква поставка се доводи у питање. Садржај, односно производ чије је коришћење лимитирано *DRM* системом заувек штити права свога власника и на тај начин улази у сукоб са законом.

Поборници *DRM* система отишли су, чак, тако далеко да су предложили да би носиоцима права требало дати могућност да купљени садржај избришу са корисничког рачунара, уколико уоче било какве неправилности у његовом коришћењу. Јасно је да би то био флагрантан пример нарушавања приватности корисника. Већина програма још увек садржи разне „рупе“ и „багове“ и тешко је поверовати да би програм направљен у ову сврху радио беспрекорно. Увек би постојала могућност да, уместо да учини оно за што је намењен, избрише са корисничког рачунара неки сасвим други програм, који потенцијално може бити неопходан за рад рачунара. Оваква технологија која омогућава да подаци буду прочитани само на одређеном уређају могла би учинити немогућим поново добијање истих у будућности.¹⁰

III Дигитални водени жиг

Дигитални водени жигови користе се за различите врсте означавања дигиталних докумената, као нпр. „дигитални потпис“, отисци прстију, аутентификација, контрола копирања (умножавања) или тајна комуникација.

Брзим развојем умрежених рачунара и интернета, друштвено-економске прилике се стално мењају и стварају се нови послови у различитим областима, а нарочити у области електронског пословања и интелектуалног стваралаштва. Документи који су некада били у папирном облику у архивама, сада се налазе у дигиталном облику на рачунарима. Дигитална технологија је постала увелико популарна и проширила се на све врсте аналогних података: аудио, видео, фотографије и сл. Претварањем аналогних података настају дигитални мултимедијски документи, који се све више дистрибуирају на интернету.

Криптовањем (шифровањем) података омогућена је тајност података приликом дистрибуције путем јавног канала, односно онлајн трансфера. Али, поставља се питање како заштитити оригинал који је дешифрован и информације које су лако читљиве? На ово питање одговор даје дигитални водени жиг.

10 Због тога, не каже се без разлога да би, чак и будућим историчарима, *DRM* систем могао представљати баријеру.

Заштита података коришћењем система дигиталног воденог жига, заснива се на идеји скривања података (информације) у оригиналном документу, било да је реч о фотографији или којем другом мултимедијском документу. Начини скривања информације у документу су дигитални потпис (енгл. *digital signature*), право имена (енгл. *copyright label*), дигитални жиг (енгл. *digital watermark*). Смештањем такве информације у оригинал, овај постаје интелектуална својина лица које је унело податак.

Дигитални водени жигови су ново подручје у информатичкој науци, криптографији, дигиталној обради сигнала и комуникацијама. Сврха постојања тог новог подручја је омогућавање заштите мултимедијских докумената у смислу ауторског права, које већ постојеће технологије не решавају на задовољавајући начин.

Поступак дигиталног означавања или *Digital Watermarking* темељи се на уметању податка, воденог жига (енгл. *watermark*), у оригинални документ за сврху поновне детекције. Документ који се означава може бити различитог садржаја. То може бити било која врста информације, мултимедијски документ, видео, слика, звук, текст, и сл. Док жиг може садржавати било коју информацију, идентификацију купца, продавца или нешто друго.

Алгоритам или шема која описује поступак означавања докумената дигиталним жигом састоји се од три дела:

- *водени жиџ*;
- *кодер* – алгоритам коришћен за уметање жига;
- *декодер и комџарациџор* – алгоритам који служи за вађење жига и верификацију.

Сваки корисник има само један жиг који га на јединствен начин идентификује. Жиг се може уметати у било који документ помоћу алгоритма кодирања. С друге стране, алгоритмом декодирања вади се жиг из означеног документа и једнозначно се одређује власник и интегритет документа.

Дигитални водени жиг (енгл. *watermark*) је неупадљиви елемент који је у електронски садржај уграђен током његове производње или дистрибуције. Могуће су различите примене ове технологије, између осталог за:

- означавање власника ауторских права;
- означавање дистрибутера;
- означавање дистрибутивног ланца; и
- идентификовање купца.

Веома је важно истаћи да дигитални жигови нису потпуни *DRM* системи. Они не штите садржаје непосредно, већ се користе као елемент таквих система приликом прикупљања доказа у судским процесима везаним уз дигитално управљање правима.¹¹

IV *Trusted computing*

Trusted computing представља нову технологију коју промовишу велике *IT* компаније, која би требало да повећа безбедност рачунара и њихових корисника. Ова идеја требало би да у великој мери промени концепт функционисања савремених рачунара, јер би произвођачи имали већу контролу над корисницима и хардвером. Корисници на овај начин губе контролу над рачунаром (нпр. проток и складиштење података), као и анонимност на мрежи, јер ће бити могуће лоцирати и установити сваки потез корисника.¹²

Намера *trusted Computing*-а је да реши неке од данашњих проблема сигурности, кроз промене *hardwera* личних рачунара. Остваривање циљева *trusted computing*-а имају и високу цену за сигурност: Они дају сигурност корисницима, али с друге стране дају трећој страни моћ да намеће своју политику корисницима. Крилатица „рачунари против корисника“ – могла би се реално остварити ако препустимо део контроле над *PC*-ом неком другом. То је појава која би се могла злоупотребити, тако да аутори софтвера угуше конкурентски софтвер. Али, то не мора нужно бити тако: промена планова *trusted computing*-а би могла сачувати добре стране сигурности рачунара, а да притом воља *PC* корисника не мора увек подлегати ономе ко је инсталирао софтвер у његов *PC*.

Постоји раширено мишљење, да је *PC* сигурност у јако лошем стању и да се нешто мора учинити да се то поправи. Постоје много обећавајућих приступа да се поправи тренутно стање сигурности, нпр. редизајнирање операцијског система, промена методологија програмирања или промена *PC* хардвера. Најважнији модел ове технике састоји се у редизајнирању *PC* хардвера у корист сигурности.

Добро је познато да ће свеобухватна одбрана, против сигурносних претњи укључивати неколико приступа, а не само један. Несигуран систем не може само тако постати сигуран да се дода само један део технологије.

Промена дизајна *PC* хардвера је само једно корисно оруђе између многих за побољшање сигурности. Док промене хардвера нису преду-

11 На пример, дигиталним воденим жиговима означене су *iTunes* песме чије копирање није онемогућено.

12 *Richard Stallman* је у својој критици оваквог концепта поменуо да адекватно име за ову технологију *Treacherous computing*.

слови за повећање сигурности, оне су без сумње корисне – нпр. начин за сигурно чување приватних кључева (а тиме личних докумената које штите ти кључеви). Једна породица пројеката за повећање сигурности РС-у је путем промене хардвера, позната као *trusted computing*. Тај термин обухвата скуп произвођача хардвера (процесора, састављача рачунала...) и софтвера, уз њих се вежу два већа пројекта.

Први од њих је операцијски систем *Microsoft*-а – званично назван *Paladium*. Сада се референцира као *Microsoft Next-Generation Secure Computing Base* или *NGSCB*. *NGSCB* пројект специфицира промене софтвера које би користиле предности, омогућене планираним новим РС дизајном.

Други пројект су нове спецификације хардвера које промовише конзорцијум прво названа *Trusted Computing Platform Alliance* или *TCPA*. *TCPA* је издао неколико докумената спецификација и тада променио име у *trusted computing group* или *TCG*. Међусобно су та два пројекта створила низ нових збуњујућих терминологија, укључујући обавезну карту нових акронима (скраћеница). У неколико случајева је један пројект измислио много различитих имена за један концепт, иако је већ други пројект имао потпуно другу терминологију за исту ствар. Потпуни речник за та два пројекта би био поприлично велики. Због једноставности овде ћемо рећи да се захтеви *NGSCB*-а претварају у појмове дизајна специфициране од *TCG*-а. *Microsoft* је члан *TCG*-а и изразио је интерес за коришћење *TCG* дизајна у улози хардвер компоненти потребних за *NGSCB*. Неки *OEM*-и (*original computer manufactur*) су почели интегрисати прве *TCG* чипове на своје матичне плоче: у будућности би могло више фирми које састављају рачунаре, укључити у своје конфигурације напредније верзије *trusted computing* чипова. *NGSCB* софтвер би могла бити једна од апликација која би могла извући корист од тих чипова. Засад су још оба пројекта засебна, али се назире да ће постојати јединствена *trusted computing* архитектура.

Подршка великих компанија технологији као што је *trusted computing* не чуди, јер ће боља контрола довести до још већег прихода истих, без обзира на ограничавање слободе корисника. На срећу свих, прва предиздања *GPL* лиценце верзије 3 доносе заштиту слободног софтвера од будућих система контроле и ограничавања слободе.

V Закључак

Нема никакве сумње да дигитална технологија и њено окружење захтевају креирање и имплементирање нових система контроле употребе и заштите интелектуалних творевина. У том смислу појављују

се системи дигиталног управљања ауторским правима – *DRM* системи. Они омогућују продавцима и власницима производа, односно носиоцима права да на електронски начин контролишу употребу садржаја и ограниче његову употребу само на одређене, односно овлашћене кориснике. У прошлости, док су сви садржаји били тзв. „аналогне“ природе није било потребе за *DRM* технологијом било које врсте. Кориснику је било једноставније (а често и јефтиније) купити нови примерак неког садржаја (била то књига, филм, аудио-касета) него посегнути за копирањем истог. Исто тако, копија оригиналног садржаја често би била незадовољавајућег квалитета.

У данашње време са појавом дигиталних технологија ове препреке су нестале и копирање је постало изузетно једноставно. Јасно је да се појавила потреба за заштитом права власника. Тако су се почеле развијати разне верзије *DRM* система. Иако креиране са dobrим намерама и циљевима, чини се да ни једна од њих није наишла на позитивније одобравање, осим од стране власника права. Кључни проблем својеврсног скептицизма па чак и анимозитета према *DRM* система, од стране одређених субјеката, је у томе што не постоји апсолутни начин заштите који на неки начин не би задирао или у приватност корисника, или у његова права. Пракса је показала да заштита права једног лица узрокује задирање у права другог, али и ограничавање коришћења легално купљеног садржаја корисника, који га жели искоришћавати у потпуности. На овоме проблему раде многи стручњаци различитих профила, пре свега они које занима како заштитити своја права, али и правници, информатичари и многи други. Надајмо се да ће једнога дана и овај проблем бити решен, иако вероватноћа да ће се то у потпуности догодити није претерано велика. У сваком случају време ће потврдити или негирати исправност појединих мишљења и концепата.

Vidoje SPASIĆ, PhD

Assistant Professor at the University of Niš, Faculty of Law

DIGITAL RIGHTS MANAGEMENT

Summary

Digital technology leads to essential changes in certain aspects of the copyright and related rights. The new environment, well-known as the network environment necessarily requires new ways of protecting intellectual property

creators and their rights that arise from unauthorized use of their creations. In response to new problems, various different cryptographic techniques and digital rights management systems have appear. This system is based on the use of digital technology with a focus on protecting the copyrighted content from the technology itself. Generally, "Digital Rights Management" is a general term for set of technologies that gives rights to holders to control usage of digital content by users, or audience (the public). However, the most important techniques of digital rights management, up to now, are the digital watermark and trusted computing.

Key words: *digital works, rights management, digital protection.*