Univerzita Pardubice

Fakulta ekonomicko-správní

Klasické a moderní způsoby zabezpečení proti softwarovému pirátství

Bakalářská práce

2025 **Dominik Bříza**

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Dominik Bříza**
Osobní číslo:	**E21787**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Klasické a moderní způsoby zabezpečení proti softwarovému pirátství**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce vypracovat ucelený pohled na klasické a moderní způsoby zabezpečení softwaru proti neoprávněnému užívání a jiným formám softwarového pirátství, porovnat základní charakteristiky z pohledu vývojáře a uživatele.

Osnova:

- Základní pojmy a definice.
- Pohled na pirátství očima vývojáře a uživatele.
- Vývoj pirátství v čase.
- Předpokládaný vývoj pirátství do budoucna.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BURNETT, Mark. *Software Piracy Exposed*. Syngress, 2005. ISBN 978-1932266986.
EVE, Martin Paul. *Warez: The Infrastructure and Aesthetics of Piracy* [online]. punctum books, 2021 [cit. 2023-08-28]. ISBN 9781685710378. Dostupné z: doi:10.53288/0339.1.00
HARRINGTON, Ted. *Hackable: How to Do Application Security Right*. Lioncrest Publishing, 2020. ISBN 978-1544517667.
JANSA, Lukáš, Petr OTEVŘEL a Martin ŠTEVKO. *Softwarové právo*. 3. aktualizované a rozšířené vydání. Brno: Computer Press, 2018. ISBN 978-80-251-4914-0.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji:

Práci s názvem „Klasické a moderní způsoby zabezpečení proti softwarovému pirátství“ jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 31.7.2025

Dominik Bříza v. r.

Poděkování

Tímto bych rád poděkoval své rodině a přátelům za podporu při psaní této práce. Především bych rád poděkoval svému vedoucímu práce, RNDr. Ing. Oldřichu Horákovi, Ph.D., za trpělivost, odborné připomínky a rady, které mi pomohly při dokončování této bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá problematikou softwarového pirátství, jeho dopady, historií a možným budoucím vývojem. Analyzuje negativní i překvapivě pozitivní dopady pirátství na vývojáře a uživatele. Zkoumá vývoj pirátství a opatření k jeho ochraně od 80. let 20. století až po druhé desetiletí 21. století. Na základě aktuálních trendů práce identifikuje klíčové oblasti, jako jsou software jako služba, opuštěný software a umělá inteligence, které mohou míru softwarového pirátství ovlivnit.

KLÍČOVÁ SLOVA

software, pirátství, softwarové pirátství, zabezpečení, uživatel, vývojář

TITLE

The Classic and Modern Approaches to Software Piracy Protection

ANNOTATION

This bachelor's thesis focuses on the issue of software piracy, its impacts, history, and potential future development. It analyzes the negative as well as surprisingly positive effects of piracy on developers and users. The thesis examines the evolution of piracy and protective measures against it from the 1980 to the second decade of the 21st century. Based on current trends, it identifies key areas, such as software as a service, abandonware, and artificial intelligence, that may influence the extent of software piracy.

KEYWORDS

Příklad: *sport, fashion, women, clothing, 19th-20th century*

Obsah

Seznam ilustrací a obrázků

Seznam zkratek

DRM	Digital rights management
BBS	Bulletin board system
BIOS	Basic Input-Output System
FBI	Federal Bureau of Investigation
WWW	World wide web
ISDN	Integrated Services Digital Network
CD	Compact disc
P2P	Peer to peer

Úvod

Softwarové pirátství je jedním z nejvýznamnějších problémů pro vývojáře dnešní doby. Historie této problematiky je však velmi zajímavá a sahá až do 80. let minulého století, kdy bylo možné pozorovat, jak se z původně neškodného kopírování disket postupně stal celosvětový fenomén. V současnosti je softwarové pirátství rozšířeno i na chytrých telefonech a prostřednictvím sdílení souborů přes internet dosahuje takového měřítka, že jeho úplná regulace je prakticky nemožná. Co už ale většina lidí tolik nesleduje, je vývoj ochranných technologií, které se snaží držet krok s pirátstvím od jednoduchých sériových čísel až po moderní technologie, které provádějí nepřetržité ověřování licence přes internet.

Tato práce se zabývá tím, jak softwarové pirátství vnímají uživatelé i vývojáři a jaké pozitivní či negativní dopady na ně tato činnost má. Dále sleduje vývoj technologií mezi lety 1980 až 2020, prostřednictvím kterých distribuce nelicencovaného softwaru probíhala, ale také technologií, které se této distribuci snažily zabránit. V závěru práce jsou pak hypoteticky nastíněna témata, která mohou softwarové pirátství v budoucnu ovlivnit, příkladem může být přechod od jednorázového nákupu k modelu předplatného.

Práce byla vypracována v souladu s doporučením Univerzity Pardubice pro používání nástrojů umělé inteligence a konverzačních modelů při akademickém psaní. Konkrétně byly využity konverzační modely ChatGPT, DeepSeek a Grok pro návrh názvů podkapitol a pro formální úpravu textu.

Cílem práce je vypracovat ucelený pohled na klasické a moderní způsoby zabezpečení softwaru proti neoprávněnému užívání a jiným formám softwarového pirátství, porovnat základní charakteristiky z pohledu vývojáře a uživatele.

1. Základní pojmy a definice

V této kapitole bude vysvětleno a rozlišeno několik základních pojmů, jejichž pochopení je nezbytné k porozumění obsahu práce. Primárně se jedná rozlišení termínů pirátství, digitální pirátství a softwarové pirátství, nicméně je zde několik dalších termínů jejichž význam je pro pochopení práce klíčový.

1.1. Software

Software je soubor instrukcí, dat nebo programů používaných k operaci počítačů a plní specifické cíle. Jedná se o opak hardwaru, což je popis fyzických aspektů počítače. Software je generalizovaný pojem, který chápeme jako aplikace, skripty a programy, které běží na zařízení (HASHEMI-POUR 2024). V této práci budeme software chápat jako například operační systém, videohry, kancelářský software, nebo software na tvorbu obsahu a programování.

1.2. Pirátství

Pojem pirátství má dva významy. První definici chápeme jakožto zločin, při kterém dochází ke krádeži, únosu nebo podobných násilných a destruktivních trestných činech páchané na mořích. Další definici chápeme jako úmyslné porušení práv duševního vlastnictví jiných osob, příkladem jsou třeba knihy, filmy a pro tuto práci podstatný software. (Cornell Law School b.r.)

1.3. Digitální pirátství

Digitální pirátství referuje k nelegálnímu kopírování a distribuce digitálního obsahu chráněného autorskými právy. Negativně ovlivňuje Filmový, televizní, publikační, hudební nebo videoherní průmysl. (Interpol b.r.)

1.4. Softwarové pirátství

Softwarové pirátství označujeme jakožto použití softwaru, který nemá platnou licenci. Mezi toto užití patří kopírování, modifikování, distribuce nebo prodej softwaru, jež porušuje zákony o autorských právech nebo licenční podmínky. Pirátství ztěžuje dodavateli softwaru schopnost prodávat jejich produkt. (revenera b.r.)

Obrázek 1: Pirátství a jeho poddruhy (vlastní zpracování)

1.5. Autorské právo

„Autorské právo náleží spolu s právy s ním souvisejícími mezi práva duševního vlastnictví, resp. práva k nehmotným statkům. Základním právním předpisem je autorský zákon – zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, který je zvláštním zákonem k občanskému zákoníku – zákon č. 89/2012 Sb.“ (Holcová b.r.)

1.6. Zákon o autorských právech k počítačovému softwaru

„Zákon o autorských právech k počítačovému softwaru neboli autorský zákon 121/2000 Sb., uvádí, že se výtvor programátora chrání jako autorské dílo, přičemž pod tuto ochranu spadá zdrojový kód či jakýkoliv vnímatelný zápis. V případě, že se jedná o dílo na objednávku, postupuje naše právní úprava podle § 58 odst. 7 výše zmíněného zákona, a program tak spadá do režimu zaměstnaneckého díla, jelikož se programátor zaváže vykonat konkrétní práci. Počítačový program je tedy chráněn okamžikem svého vzniku bez nutnosti registrace, musí však splňovat podmínku originality, aby byl odlišitelný, od již vzniklých programů.“ (Janzová 2023)

1.7. Hacking

Hacking je použití nekonvenčních nebo nelegálních prostředků k získání přístupu k digitálnímu zařízení, počítačovému systému nebo počítačové síti. Klasickým příkladem je kyberzločinec, který zneužívá bezpečnostních zranitelností k proniknutí do sítě a krádeži dat jako například software, který ještě nebyl zpřístupněn pro veřejnost. (Kosinski 2024)

1.8. Cracking

Jedná se o aktivitu, při níž se modifikuje software tak, aby byla odstraněna jeho ochrana zamezující porušení autorských práv. Tento software je pak distribuován mezi piráty. Osobě, která tuto činnost vykonává se pak přezdívá cracker. Pro tuto práci je nezbytné nezaměnit termín cracking s jinými podobnými termíny jako Hacking nebo Phreaking. (Paul Eve 2021)

1.9. Phreaking

Phreaking je manipulace telefonního signálu za účelem uskutečnění bezplatných telefonních hovorů. Toto bylo uskutečňováno pomocí reverzního inženýrství specifických tónů telefonních společností, které sloužili k přesměrování hovorů na velké vzdálenosti. Díky emulaci těchto tónů mohli phreakeři volat zadarmo po celém světě (Brush b.r.). Tato aktivita byla pro pirátství podstatná především v dobách, kdy se využívali nástěnkové systémy.

1.10. Systémy správy digitálních práv

Systém pro správu digitálních práv, v angličtině známý jako „DRM“ je pojem, který označuje soubor technologických metod, jejichž pomocí se u elektronických produktů zaručuje dodržení autorských práv. Crackeři od vzniku těchto systémů vyvíjejí snahu, ochranu prolomit.

(IT-slovník b.r.)

1.11. Šedý trh

„Šedý trh je obchod pomocí neoficiálních a neregulovaných prostředků, které jsou stále legální“ (Česká bankovní asociace b.r.). V oblasti softwarového pirátství jej chápeme jako prodej licencí k softwaru, jež byl neoprávněně získán bez důkazu neoprávněného získání.

1.12. World wide web

„World Wide Web, v překladu celosvětová síť, je obrovskou sítí veřejných webových stránek uložených na webových serverech, ke kterým mají uživatelé prostřednictvím internetu přístup ze svých místních počítačů nebo jiných zařízení.“ (Collabim b.r.)

2. Pohled na pirátství očima vývojáře a uživatele

Pirátství ovlivňuje jak vývojáře, tak uživatele. Tento vliv není výhradně negativní, ačkoli pirátství přináší značná rizika a problémy, které v dohledné době pravděpodobně nebude možné zcela vyřešit. Přesto nabízí určité výhody, a to pro obě strany.

2.1. Negativní dopady na uživatele

Ačkoli pirátství může uživatelům umožnit ušetřit na nákupu softwaru, přináší více rizik a problémů než výhod. Tyto negativní dopady postihují zejména uživatele, kteří se k nelegálnímu získávání softwaru neuchylují.

2.1.1. Ceny softwaru

Jedním z negativních dopadů pirátství je zvyšování ceny softwaru. V reakci na nelegální šíření softwaru mohou vývojáři zvýšit jeho cenu, aby kompenzovali ztráty. Tato změna však nezatěžuje vývojáře ani piráty, nýbrž legitimní uživatele, kteří hradí vyšší náklady (De Kock et al. 2003, s. 785).

2.1.2. Bezpečnostní rizika

Nelegálně získaný software může obsahovat škodlivý kód, například viry, spyware nebo trojské koně, které ohrožují zejména nezkušené uživatele, kteří nedostatečně ověřují zdroj softwaru. Tyto hrozby však mohou postihnout i zkušené uživatele. Například jeden z uživatelů na fóru *Malwarebytes* (WhiteKing35 2024) popsal ztrátu přihlašovacích údajů kvůli trojskému koni v jeho systému. V některých případech lze účty obnovit prostřednictvím podpory, avšak ne vždy je to možné, například podmínky společnosti *Microsoft* umožňují zablokování účtu v případě narušení bezpečnosti, ne však jeho navrácení (Microsoft 2024), jak zaznamenal uživatel (Sad_System_3314 2025) na platformě *Reddit*. Přestože se jedná o anonymní příspěvky, ukazují konkrétní příklady bezpečnostní hrozeb spojených s nelegálním softwarem.

2.1.3. Stabilita softwaru a požadavky na výkon

Protipirátská ochrana negativně ovlivňuje legitimní uživatele tím, že snižuje stabilitu a výkon softwaru. Jedním z příkladů systémů správy digitálních práv je Denuvo. Testy videoher prokázaly, že software s technologií Denuvo vykazuje nižší počet snímků za sekundu ve srovnání s verzemi bez této ochrany, při použití stejného hardwaru. Výrazný rozdíl byl zaznamenán u titulu *Ghostwire Tokyo*. Ještě větší rozdíl se projevuje v době načítání her, kdy verze bez Denuva se načítá více než dvojnásobně rychleji (Kessler 2023). Přestože bývá ochrana Denuvo časem prolomena, vývojáři mohou tuto technologii následně odstranit, čímž eliminují negativní dopady a ušetří náklady, jak učinila společnost Square Enix u titulu *Final Fantasy XVI* a dalších her (Padapulos 2025).

2.1.4. Nutnost být neustále online

Poslední nevýhodou pro legitimní uživatele uvedenou v tomto dokumentu je požadavek stálého připojení k internetu u některých systémů správy digitálních práv. Ačkoli je internet v současnosti široce dostupný, uživatelé mohou čelit situacím, kdy připojení nemají, i když se většinou nejedná o trvalý problém. Tento požadavek bývá frustrující, protože mnohé funkce softwaru připojení nevyžadují. Například videohry *Diablo III* a *StarCraft II* vyžadovaly stálé připojení i pro režim jednoho hráče, což negativně ovlivnilo jejich hodnocení (Ultimate popculture wiki 2019).

2.2. Pozitivní dopady na uživatele

Pirátství je často vnímáno jako způsob, jak uživatelům umožnit přístup k softwaru bez placení. Je však tato motivace jediným důvodem, nebo existují i jiné faktory, které k němu vedou?

2.2.1. Ceny softwaru

Hlavním důvodem pirátství je snaha ušetřit finanční prostředky. Někteří uživatelé nepovažují software za produkt hodný platby, protože není hmatatelný. Vysoké ceny softwaru, například plánované zvýšení cen her pro Nintendo Switch 2 z průměrných 60 amerických dolarů na 70 amerických dolarů či více, rovněž odrazují od nákupu. Toto zdražení lze částečně odůvodnit stavem světové ekonomiky a také uznávanou kvalitou videoherních titulů od Nintenda, avšak průměrná cena videoher zůstává nezměněna od roku 2006 (Ho 2023). Tento trend může v budoucnu dále motivovat uživatele k stahování softwaru nelegálně.

2.2.2. Přístup před vydáním

Pirátům se často podaří nelegálně získat software ještě před jeho oficiálním vydáním, což umožňuje uživatelům používat pirátskou kopii dříve než legitimní zákazníci. Tato situace je pro ně ve většině případů výhodná, i když takové verze mohou obsahovat chyby nevhodné pro komerční využití. Příkladem je videohra *Polda 7* od společnosti Zima Software, která byla před vydáním neoprávněně zpřístupněna na pirátských serverech kvůli přispěvateli s předběžným přístupem, jak uvedl programátor hry Petr Svoboda v rozhovoru (Indian – pořad o hrách 2022).

2.2.3. Vyzkoušení softwaru

Jedním z pozitivních dopadů pirátství pro uživatele, případně vývojáře, je možnost vyzkoušet software před jeho zakoupením. Uživatele motivuje potřeba ověřit, zda jejich hardware splňuje požadavky softwaru a zajišťuje jeho plynulý chod, nebo zda software splňuje jejich očekávání, aby předešli zbytečným finančním ztrátám, jak uvádí uživatelka na síti quora s podobnou zkušeností (BEX FOSTER 2016). Přestože se jedná o anonymní zdroj, tak tato zkušenost ilustruje běžný motiv uživatelů. Řešením by mohly být demo edice softwaru, poddruh sharewaru, kterým se zabývá jiná část práce. Tyto edice však bývají značně omezené, zatímco pirátství umožňuje neomezené vyzkoušení. Je třeba zdůraznit, že jde opět o nelegální činnost a počet uživatelů s tímto přístupem je zanedbatelný.

2.3.Negativní dopady na vývojáře

Jestli někomu pirátství způsobuje škody, tak jsou to především vývojáři. Finanční ztráty pro ně představují nemalé riziko, které může způsobit vývojářům nebo společnostem vydávající software mnoho potíží.

2.3.1. Finanční ztráty

Finanční ztráty představují nejzávažnější dopad pirátství na vývojáře, neboť mohou omezit či zcela znemožnit výzkum, vývoj a inovace. Tento problém postihuje jak velké korporace, tak malé nezávislé vývojáře, kteří ztráty snášejí hůře (Jindal 2024).

2.3.2. Ztráty pracovních míst

V souvislosti s finančními ztrátami způsobenými pirátstvím je třeba zdůraznit ztráty pracovních míst, které s tímto problémem souvisejí. Podle dostupných údajů přijde ve Spojených státech Amerických kvůli online pirátství o práci přes půl milionu zaměstnanců, ačkoli tato čísla zahrnují nejen softwarové, ale i jiné formy pirátství. Paradoxně však pirátství zvyšuje poptávku po pracovních pozicích v oblasti kybernetické bezpečnosti, které reagují na rostoucí hrozby (Agence PDN 2023).

2.3.3. Prevence proti pirátství

Investice do ochrany před pirátstvím představují značné finanční náklady pro vývojáře. Jak bylo uvedeno v podkapitole o stabilitě softwaru a výkonu, vývojáři musí být schopni efektivně pracovat s protipirátskými řešeními, aby optimalizovali software, což zvyšuje náklady na jejich práci. Přestože tuto optimalizaci mohou vynechat, riskují tím ztrátu reputace mezi uživateli (Ascione 2024).

2.4. Pozitivní dopady na vývojáře

Přestože to může působit překvapivě, pirátství může mít na vývojáře i pozitivní dopady. Ačkoli negativní důsledky značně převažují nad přínosy, existence těchto pozitivních vlivů zůstává nepopiratelná. Většinou však jde jen o to, že softwarové pirátství je lepší než daný software nikdy nepoužívat.

2.4.1. Boj proti šedému trhu

Šedý trh označuje oblast neautorizovaných transakcí, kde prodejci distribuují legální produkty, které však nejsou určeny pro dané lokality nebo nebyly získány legální cestou. V softwarovém prostředí se jedná o portály nabízející předprodej licencí, například aktivačních klíčů pro platformy jako Steam, z nichž vývojáři často nemají zisk kvůli neznámému původu těchto klíčů. Příkladem je e-shop *G2A*, jež takové služby poskytuje (Dring 2017). Nezávislí vývojáři vyzývají zájemce, aby místo nákupu na šedém trhu volili pirátství, protože z těchto transakcí nezískávají zisk a prostředky obvykle obohacují pouze prostředníka (Kelion 2019). Konkrétní případ této výzvy mají na svědomí třeba vývojáři ze studia Running With Scissors (Cvrček 2023).

2.4.2. Reklama

Reklama jako pozitivní dopad softwarového pirátství je kontroverzní téma, protože ztráty způsobené pirátstvím obvykle převyšují hodnotu této reklamy. Přesto nelze popřít, že spokojený pirát může sdílet své pozitivní zkušenosti s potenciálními zákazníky, kteří by jinak o software nejevili zájem (Horton 2019). Tuto problematiku podrobně zkoumá docent Antino Kim z Indiana Univerzity v Bloomingtonu (Kim 2018, s. 1117-1141). Příkladem k této situaci je vyjádření vývojáře videohry *ULTRAKILL*. Vývojář se vyjádřil tak, že by bylo vhodné vývojáře nezávislých her finančně podpořit, avšak si uvědomuje, že ne každý si to může dovolit a že i on sám by nejspíše nevyvíjel hry, kdyby během dospívání neměl jednoduchý přístup k filmům, hudbě a videohrám. Pokud už k pirátění dojde, měl by pirát aspoň vývojáře podpořit dobrým slovem mezi potencionálními zájemci. Dále zmiňuje, že v takovém případě je nejhorší ztráta z prodeje jedné kopie, která se okamžitě vykompenzuje prodáním kopie uživateli, který byl osloven pirátem a bez pirátění by nejspíše osloven nikdy nebyl (Patala 2024).

2.4.3. Reputace

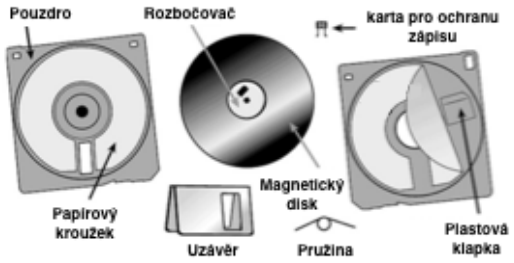
Reputace představuje pozitivní dopad pirátství, podobný reklamě, avšak zaměřený na image vývojáře u uživatelů pirátského softwaru. Statistiky ukazují, že pirátství je nejrozšířenější mezi věkovou skupinou 18–26 let, která často postrádá dostatečné finanční prostředky, což usnadňuje ospravedlnění nelegálního stahování (Revankar 2024). Lze předpokládat, že pokud si tito uživatelé oblíbí pirátský software, mohou po zlepšení své finanční situace v budoucnu zvážit legální nákup novějšího softwaru od vývojáře s dobrou reputací. Pro vývojáře tak pirátství může hypoteticky představovat dlouhodobou investici do budoucích zákazníků, kteří si software aktuálně nemohou dovolit (Kim 2018, s. 1117-1141).

3. Vývoj pirátství v čase

Pirátství je fenoménem známým po staletí. Softwarové pirátství se však začalo šířit až na přelomu sedmdesátých a osmdesátých let 20. století, kdy se na trh dostaly osobní počítače (Craig 2008, s. 27). V této kapitole autor využívá různé zdroje k popisu historického vývoje softwarového pirátství. Vzhledem k tomu, že některá období nejsou dostatečně zdokumentována, jsou zahrnuty i diskusní fóra, dobové články a otevřené encyklopedie s tematickým zaměřením.

3.1. Počátky softwarového pirátství

Softwarové pirátství začalo relativně nevinně. Počítače byly zpočátku určeny především pro firmy a univerzity, ale objevila se malá skupina počítačových nadšenců, kteří je využívali pro osobní účely, i když jich bylo velmi málo. Svůj zájem sdíleli na setkáních a v kroužcích, kde se poprvé objevilo pirátství prostřednictvím kopií na disketách. Později vznikly elektronické nástěnkové systémy (Bulletin Board Systems, BBS), které umožnily členům na různých místech sdílet digitální obsah, od zpráv po aplikace (Craig 2008, s. 28).



Obrázek 2: Součásti diskety (Murphy 1998)

3.1.1. Kopie softwaru na disketách

Diskety sloužily k čtení a zápisu dat, což využívali softwaroví nadšenci, kteří na komunitních setkáních vyměňovali kopie zakoupeného softwaru. Jednotlivec software zkopíroval na diskety a distribuoval jej ostatním nadšencům. Hlavní motivací byla vysoká cena softwaru, který byl často dražší než počítače, protože byl určen především pro podniky s velkými rozpočty (Craig 2008, s. 28).

3.1.2. Ochrana proti kopírování obsahu na disketách

Ochrana softwaru před neoprávněným kopírováním disket zahrnovala tehdy různé metody, které jsou popsány v následujících podkapitolách. Každá metoda se výrazně lišila a každou bylo možné později obejít odlišným způsobem, například pomocí skeneru na obrázky, crackováním nebo specializovanými zařízeními.

3.1.2.1. Copy-Lock

Jednou z metod ochrany softwaru byla fyzická modifikace disket, která měla různé podoby. První z nich, Formaster copy-lock, spočívala v zapsání jednoho segmentu disku pouze z jedné poloviny, zatímco druhá část segmentu zůstávala prázdná. Originální software obcházel BIOS a přímo komunikoval s disketou. Prázdné místo nebylo možné zkopírovat běžným hardwarem, což poskytovalo částečnou ochranu (Rowntree 2024).

3.1.2.2. Slabé bity

Slabé bity představovaly další fyzickou metodu ochrany disket. Tato metoda fungovala odlišně. Disketová mechanika čte data jako jedničky a nuly, přičemž standardní kopírovací programy očekávají stabilní čtení a přepis dat. Slabé bity byly oblasti na disketě, které při čtení poskytovaly nestabilní hodnoty, jež se pokaždé lišily. Zkopírovaná disketa však obsahovala stabilní data. Software kontroloval nestabilní část, takže kopie při ověření nefungovaly. Crackeři se tuto ochranu později pokoušeli obejít odstraněním kontroly (Evans 2020).

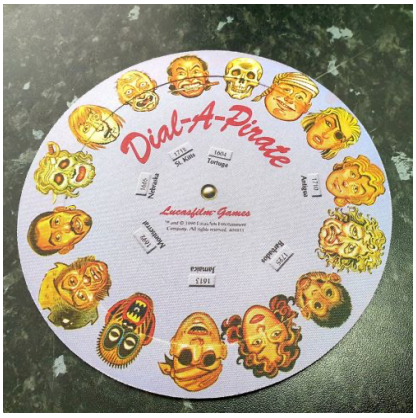
3.1.2.3. Chybějící stopy

Poslední fyzickou metodou ochrany uvedenou v této kapitole je technika chybějících stop, vyvinutá společností Western Security Ltd. Tato metoda spočívala v tom, že část diskety při čtení generovala chybu, kterou software očekával. Pokud zkopírovaná disketa tuto chybu neobsahovala, software se odmítl spustit (Evans 2020).

3.1.2.4. Manuální vyhledávání

Kromě fyzické ochrany existovala i softwarová ochrana. Jednou z metod bylo manuální vyhledávání, kdy uživatel musel použít přiložený návod obsahující kód nebo podobný prvek. Například před aktivací funkce softwaru byl uživatel vyzván, aby uvedl poslední slovo na třetí straně návodu. Uživatelé se zkopírovanými disketami, kterým manuál chyběl, tuto informaci nezjistili.

Tato metoda byla rozšířena u videoher, kde mohla narušit herní zážitek (Stanford University b. r.). Někteří vývojáři přistupovali kreativně, například hra *Secret of the Monkey Island* využívala šifrovací kotouč „Dial A Pirate“, který hravou formou umožňoval získávání kódů pro postup ve hře (Retro Dream 2022).



Obrázek 3: Kotouč ke hře Secret of the Monkey island (Rhayader computers b.r.)

3.1.2.5. Sebe modifikující kód

Další softwarovou metodou ochrany byl sebe modifikující kód, použitý například ve hře *Dungeon Master*. Hra se na první pohled dala zkopírovat, ale pirátům způsobovala problémy. Nesprávné čtení sektorů diskety bránilo spuštění hry, případně nemodifikovaný kód vedl k chybám, jako bylo zaseknutí vrhacích zbraní ve vzduchu, což způsobilo selhání softwaru (Papp 2019).

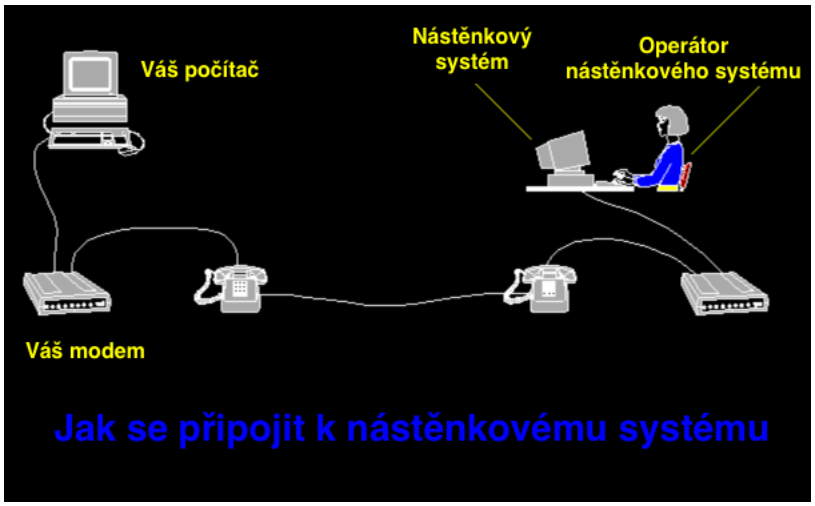
3.1.2.6. Hardwarové klíče

Hardwarovou metodou ochrany byly tzv. „hardwarové klíče“, označované jako dongly. Jednalo se o zařízení dodávané s dražším softwarem, které se připojovalo do vhodného portu počítače. Dongle musel být zapojen po celou dobu běhu softwaru, protože software s ním komunikoval, jinak byl nefunkční (Stanford University b. r.).

Obrázek 4: Hardwarový klíč (Dekay 2006)

3.1.3. Sdílení v rámci nástěnkových systémů

Nástěnkový systém (BBS) je počítač s jedním nebo více modemy, který v bezobslužném režimu čeká na připojení přes telefonní síť. Program na tomto počítači umožňuje uživateli připojení a využití služeb, jako jsou zprávy, archivy souborů nebo her (Peterka 1991). Nástěnkové systémy přispěly k vytvoření pirátských skupin, které soutěžily v prolomení ochran softwaru a jeho nahrání na BBS. Kapacita těchto systémů rychle rostla, některé nabízely přes 1 GB úložiště, což odpovídalo zhruba 700 disketám nebo 250 aplikacím. BBS nejen podporovaly pirátské skupiny, ale také urychlily šíření pirátství, což poškodilo mnoho nezávislých vývojářů, z nichž někteří zkrachovali. Navzdory nespokojenosti vývojářů bylo pirátství obtížné potírat. Policejní možnosti byly omezené a navzdory snahám organizací, jako SPA či CAAST, nabízejících odměny za informace vedoucí k zatčení pirátů, bylo zadrženo jen málo pachatelů. Policie se spoléhala na anonymní zdroje, ale podezřelí byli často chudší občané. Případy byly nákladné a jen málokteré se dostaly k soudu, protože vymáhat finanční náhradu bylo téměř nemožné (Craig 2008, s. 29–31).



Obrázek 5: Připojení k nástěnkovému systému (Thimbuktu 2016)

3.1.4. Ochrana proti sdílení přes nástěnkové systémy

Ochrana proti sdílení přes nástěnkové systémy byla z velké části totožná jako ochrana proti kopírování floppy disků. V následujících podkapitolách jsou popsané některé metody, které se začali používat jako odpověď na pirátskou scénu na nástěnkových systémech, ale byli uplatnitelné i u disket.

3.1.4.1. Systémy zpětného volání

Jednou z metod ochrany softwaru proti pirátství na nástěnkových systémech bylo zpětné volání, které spíše ověřovalo uživatele, než chránilo software (Scott 2005). Ověření probíhalo zadáním telefonního čísla při registraci, na které systém následně zavolal, aby potvrdil jeho existenci a příslušnost k uživateli. Telefonní číslo umožňovalo dohledání uživatele, což odrazovalo od nelegálních aktivit (Dailey b. r.).

3.1.4.2. Kontroly prováděné operátory systémů

Podobnou metodou, která nebyla primárně zaměřena na ochranu před pirátstvím, byly kontroly souborů prováděné operátory nástěnkových systémů, tzv. „Sysops“. Operátoři manuálně kontrolovali obsah, aby zajistili, že jejich systém neobsahuje nelegální aktivity. Je však třeba poznamenat, že někteří operátoři mohli podporovat šíření pirátského softwaru. Existovaly i nástěnkové systémy vytvořené výhradně pro pirátskou činnost. Přesto manuální kontroly některých operátorů přispěly ke snížení počtu pirátských kopií (Scott 2005).

3.1.4.3. Sériová čísla

Další metodou ochrany byly sériová čísla, která jsou například zmiňována již v roce 1984 v akademické práci (Albert, Morse 1984, s. 68). Tato čísla fungovala na principu zadání dlouhého alfanumerického kódu při registraci softwaru. Ve většině případů bylo sériové číslo propojeno s konkrétním uživatelem, čímž umožňovalo jeho zpětnou identifikaci. Bez platného sériového čísla nebylo možné software aktivovat. Pokud se sériový klíč objevil například v nástěnkovém systému a vývojáři tuto skutečnost zjistili, mohli jej následně zablokovat (Craig 2008, s. 61). Je důležité dodat, že tato metoda fungovala i u disket, ale její plný potenciál – zejména co se týče dohledatelnosti online – byl využit až v souvislosti s nástěnkovými systémy.

3.1.4.4. Shareware

Další metodou snižující pirátství, používanou i v současnosti, je shareware. Shareware je software šířený mezi uživateli, obvykle však ne v plné verzi. Mezi jeho typy patří například Adware, Demoware nebo Donationware. Shareware nezaručuje ochranu před pirátstvím, ale spoléhá na čestnost uživatelů, jimž je část softwaru poskytnuta zdarma (Sangfor Technologies 2024). Mezi známé příklady patří videohra *Doom*, která nabízela úvodní část zdarma (Id Software 1993), nebo software *WinRAR*, jenž pouze doporučoval zakoupení, přesto vydělal přes 21 milionů dolarů. Tento model umožnil aktualizace softwaru i po 30 letech od vydání (Elharony 2023).

Obrázek 6: Sharewarová disketa s videohrou Doom (Doom wiki b.r.)

3.1.4.5. Klamavá ochrana

Název této metody není oficiální. Jedná se o metodu, kde sami vývojáři vytvoří modifikovanou verzi softwaru, nejčastěji videoherního, který pak sami distribuují mezi pirátské skupiny. Co ovšem piráti nevědí, je to, že daný software tyto modifikace má. Pro dobro uživatele není tento software nebezpečný na použití a jedná se spíše o vtipný druh ochrany, která buďto udělá průchodu hrou zvláštní, ho po nějaké době znemožní určitou překážkou (Smith 2022).

Jedna ze straších her, s tímto typem ochrany je hra *EarthBound*, tento titul se sice přes BBS nešířil, neboť byl exkluzivní hrou pro systém *Super Nintendo Entertainment System*, kde se tento titul kopíroval, pomocí kopírovače kazet, ale fungoval na stejném principu. První a druhá vrstva ochrany byla techničtějšího rázu, byli tím kontrola regionu a kontrola formátu. Tyto kontroly se však manipulací pirátů odstranili, ale pokud tyto kontroly neproběhly, začali působit kontroly modifikující hru. Jedna z těchto modifikací bylo zvýšení počtu nepřátel, který mohli zkušení hráči vnímat jako neškodnou větší výzvu. Mnohem destruktivnější však byla modifikace způsobující pád hry a odstranění uložené pozice během finále hry (Starman.net b.r.). Příklad dobové videohry, je třeba již zmíněný Dungeon Master.

Obrázek 7: Snímek z cracnuté verze videohry Earthbound (Starman.net b.r.)

3.1.4.6. Zásahy státních orgánů

Jak již bylo zmíněno, zatýkání pirátů bylo poměrně vzácné, mimo jiné i proto, že značná část z nich byla nezletilá. To však neznamená, že k policejním zásahům vůbec nedocházelo. Většina těchto zásahů se nicméně uskutečnila až v průběhu 90. let 20. století (Craig 2008, s. 31). Jeden z nejznámějších případů představoval zásah Federálního úřadu pro vyšetřování (FBI) proti

skupině využívající nástěnkový systém s názvem *Fear and Loathing in Las Vegas*. Při tomto zásahu se FBI zaměřila na uživatele s přezdívkou „Doctor“, jenž byl provozovatelem uvedeného systému. Již před samotným zásahem se FBI do systému infiltrovala jako běžný uživatel a získala důkazy o sdílení nelegálních souborů (Empedocles 1993). Postupem času počet těchto zásahů narůstal.

3.2. Pirátství během 90. let 20. století

Pirátství se na počátku 90. let výrazně nezměnilo – mezi nejrozšířenější způsoby šíření nadále patřilo kopírování fyzických médií a využívání nástěnkových systémů (BBS). Diskety byly postupně nahrazovány kompaktními disky, avšak princip kopírování zůstal v podstatě stejný. Zásadní proměnou však prošly způsoby ochrany proti kopírování. K výraznějšímu zlomu došlo 30. dubna 1993, kdy byl systém *World wide web* poprvé zpřístupněn široké veřejnosti (HISTORY.com Editors 2020). Oproti nástěnkovým systémům nenesly internetové stránky taková omezení v kapacitě paměti ani připojení, a navíc se na internet začaly přesouvat i vydavatelské společnosti. Nejrychlejší formou připojení bylo tehdy ISDN.

Piráti postupně opustili nástěnkové systémy a přesunuli své aktivity do prostředí internetu, kde začali budovat online komunity. V tomto období se softwarové pirátství proměnilo z víceméně neškodné zájmové činnosti v závažnější problém. Původně malé skupiny čítající jednotky členů se mohly rozrůst až na stovky jednotlivců a sdílení softwaru, původně zamýšlené jako forma vzájemné pomoci, se proměnilo v soutěživé prostředí, jehož cílem bylo především překonání ochranných systémů (Craig 2008, s. 32). Významný posun ve vývoji internetového pirátství přišel koncem 90. let se vznikem peer-to-peer (P2P) sítí.

3.2.1. Kopie softwaru na kompaktních discích

S nástupem nové dekády se ve společnosti začala prosazovat nová technologie – kompaktní disk (CD), na jejímž vývoji od roku 1976 spolupracovaly společnosti Philips a Sony v rámci společného výzkumného projektu. Tato spolupráce přinesla své ovoce a výsledná technologie dokázala nahradit diskety nejen větší kapacitou – jeden kompaktní disk mohl pojmout ekvivalent přibližně 1500 disket – ale i nižší výrobní cenou. Tato inovace se však brzy dostala i do rukou softwarových pirátů, kteří dokázali uplatnit některé osvědčené postupy z éry disket i při kopírování nosičů kompaktních disků. To vyvolalo nutnost vývoje nových způsobů ochrany, jejichž cílem bylo co nejvíce ztížit neoprávněné kopírování (GRANT 1994).

3.2.2. Ochrana proti kopírování kompaktních disků

Zpočátku se kopírování kompaktních disků příliš nelišilo od způsobu, jakým byly kopírovány diskety. I když se jednalo o odlišnou technologii, jejíž čtení i zápis vyžadovaly nové nástroje, princip zůstal podobný. Vývojáři softwaru však již měli s pirátstvím předchozí zkušenosti, a tak mohli relativně rychle začít vyvíjet nové a komplexnější ochranné mechanismy, které měly neoprávněnému šíření zabránit.

3.2.2.1. LaserLock

Ochranná technologie LaserLock využívala kombinaci softwarového šifrování a unikátního fyzického značení vytvořeného laserem na povrchu kompaktního disku, což mělo zkopírování nosiče prakticky znemožnit. Každý konkrétní software využíval vlastní zamykací parametr, který byl na disku implementován. Tuto technologii vyvinula společnost MLS LaserLock International Inc. (Maximum PC 2001). Příkladem softwaru, který ochranu LaserLock využíval, je dodnes ikonická počítačová hra Fallout 2 (Mobygames b. r.).

3.2.2.2. SafeDisc

SafeDisc je technologie vyvinutá společností Macrovision Corporation. Stejně jako LaserLock je tvořena dvěma klíčovými částmi. První z nich je digitální podpis, který nelze běžnými metodami zkopírovat, druhou pak kód zajišťující samotné spuštění programu.

V případě, že disk podpis neobsahuje, software se při spuštění nenačte a nelze jej spustit (Maximum PC 2001). Mezi příklady softwaru chráněného technologií SafeDisc patří například interaktivní atlas *Microsoft Encarta – Interactive World Atlas 2000* nebo simulátor stavby zábavních parků *Roller Coaster Tycoon* (Bartoň 2001).

3.2.2.3. SecuROM

Technologie SecuROM, známější veřejnosti než některé jiné ochrany, byla vyvinuta a patentována společností Sony. Její princip spočívá v tom, že každý kompaktní disk obsahuje jedinečný identifikační kód, který nelze běžně kopírovat pomocí standardních vypalovacích mechanik. Při každém spuštění program tento kód ověřuje, a to prostřednictvím subkanálů disku. Kontrola probíhá na pozadí a uživatel si jí obvykle vůbec nevšimne.

Mezi příklady softwaru využívajícího ochranu SecuROM patří videohra *FIFA 99* od společnosti Electronic Arts (Bartoň 2001). Tato ochrana patřila k nejdéle používaným a byla nasazena například i v roce 2017 při vydání hry *Deus Ex: Mankind Divided* (PCGAMINGWIKI 2012). Její širší využití skončilo zejména kvůli postupnému ústupu kompaktních disků jako média.

3.2.2.4. Starforce

Technologie Starforce představovala další ochranu proti kopírování kompaktních disků, tentokrát vyvinutou v Rusku. Zpočátku vývojáři o principu fungování této technologie zveřejňovali pouze marketingové informace. Později však oficiální zdroje potvrdily, že Starforce funguje na principu šifrování souborů a následného zabudování dešifrovacího klíče přímo do média. Chráněné soubory tak bylo možné spustit pouze tehdy, pokud byl originální disk fyzicky přítomen v zařízení (Starforce, b. r.). Experti, kteří se pokoušeli ochranu obejít, potvrdili mimo jiné i to, že software se nespustí v případě, že systém rozpozná disk jako kopii. Technologie Starforce navíc často využívala kombinaci s tzv. CD klíči (Sklyarov 2003, s. 147).

3.2.2.5. Vodoznaky

Jak název napovídá, vodoznaky nejsou přímým prostředkem ochrany proti softwarovému pirátství, ale spíše metodou umožňující identifikaci primárního šiřitele nelegální kopie. Vodoznaky jsou ukryty v určitých souborech na disku a dokážou jednoznačně určit původní médium. Rozlišujeme dva základní typy vodoznaků – statické a dynamické. Statický vodoznak je většinou skrytý textový řetězec umístěný v souborech disku.

Naproti tomu dynamický vodoznak je integrován do samotného běžícího softwaru a aktivuje se až po určité akci, například stisknutím specifické klávesové zkratky. Specifickou formou dynamických vodoznaků jsou tzv. *easter eggy* – skryté funkce nebo zprávy, které často slouží spíše jako zábavné překvapení než jako prostředek k identifikaci kopií. Hlavní nevýhodou vodoznaků je skutečnost, že pirátství nezabraňují přímo, ale mají spíše odstrašující charakter, neboť vzbuzují obavy z dohledatelnosti piráta. Ne každý software byl však označen jako nositel vodoznaku, aby piráti nevěděli, co přesně hledat (HAMILTON 2010).

3.2.2.6. CD klíče

CD klíče představují obdobnou formu ochrany jako sériová čísla, avšak s rozdílem v samotném principu generování. Zatímco sériová čísla mohla být pevně přidělena konkrétnímu uživateli, CD klíče byly vytvářeny algoritmicky na základě matematických vzorců. Každý klíč, přestože působí jako náhodný řetězec znaků, je ve skutečnosti výsledkem složité rovnice, jejíž proměnné mohou zahrnovat typ produktu, region prodeje i pořadové číslo nákupu (Craig 2008, s. 66). Tento způsob ochrany znesnadňoval vytvoření funkčního generátoru klíčů a zvyšoval bezpečnost proti neoprávněnému kopírování. Klíče byli většinou vytištěny na balení kompaktního disku.

3.2.3. Sdílení v rámci P2P sítí

P2P (peer-to-peer) sítě tvoří skupiny zařízení, které společně ukládají a sdílejí soubory. Každý účastník neboli uzel, se do této sítě zapojuje jako samostatná jednotka se stejnými pravomocemi jako ostatní. Ve většině případů P2P sítě nevyužívají centrálního správce ani server, neboť jednotlivé uzly drží kopie souborů nezávisle na sobě. Díky tomu se účastník stává nejen pasivním příjemcem dat, ale i jejich poskytovatelem (Jansa 2016).

P2P sítě lze dále rozdělit podle architektury do tří základních kategorií:

- Nestrukturované P2P sítě: Uzly nejsou organizovány a komunikace mezi nimi probíhá náhodně. Hlavní výhodou je vysoká odolnost vůči fluktuaci uživatelů, nevýhodou jsou však vysoké nároky na výpočetní výkon a paměť.
- Strukturované P2P sítě: Mají organizovanou architekturu umožňující efektivní vyhledávání dat. Tento přístup je efektivnější, ale vyžaduje vyšší náklady na zřízení a správu.
- Hybridní P2P sítě: Kombinují výhody obou předchozích typů a představují kompromis mezi decentralizací a efektivitou (Biance Academy 2022).

3.2.4. Ochrana proti sdílení v rámci P2P sítí

Sdílení na P2P sítích bylo a dodnes je velice problémové, neboť uživatelé spolu mohou sdílet cokoliv od důležitých pracovních dokumentů, přes vlastní fotky až k pirátěnému softwaru. V některých případech nebylo možné jakýmkoliv způsobem kontrolovat, jaký obsah si mezi sebou uživatelé sdíleli, jindy však jeden uživatel soubor sdílel a mohl jej vidět a stáhnout kdokoliv. Prevence v pirátství na P2P sítích byla jak technického rázu, tak právního a trvá dodnes. Některé druhy prevence byli dokonce ilegální například DoS útoky, které měli za úkol napadnou sítě s pirátským obsahem

3.2.4.1. Parodování

Parodování, v angličtině označované jakožto spoofing, je aktivita velice podobná aktivní otravě obsahu, s tím rozdílem, že je méně technicky založená a zároveň se více používala u digitálního pirátství jako takového než vyloženě u softwaru, a to především u hudby. Při parodování dochází k tvorbě poškozených nebo matoucích souborů, které jsou vkládány do P2P sítí s povolením autora originálních souborů. Pokud chceme, aby tato obrana byla efektivní, je potřeba vytvořit mnoho takových souborů, aby se na P2P síti jen velice těžce dali dohledat funkční kopie hledaných souborů. Autoři se většinou k povolení této obrany nepřiznávali a jedním takovým zpěvákem byl například raper Eminem (Mittal 2004, s. 453). I přestože se tahle metoda využívala především u hudebních souborů, tak se dala použít i na software.

3.2.4.2. Konzultační firmy

Další možností, jak chránit svůj software na P2P sítích, byla možnost najmout si konzultační firmu, která zasahovala za své klienty, s cílem chránit obsah spadající pod autorská práva. Úspěch byl měřen podle toho, jak často uživatelé přistupovali k legálním souborům těchto firem, když zjevně hledali pirátský obsah. Příkladem takové firmy, je již dnes neexistující společnost Overpeer, která byla založena v roce 2000 (Mittal 2004, s. 453).

3.2.4.3. DoS útoky

DoS neboli Denial-of-service je typem kybernetického úkolu, který má za úkol zahltit cílový server vysokým množství dat, což znemožní jiným uživatelům přístup ke službám serveru (Kopecký 2023). Nicméně v tomto případě se jednalo o pozitivní věc, neboť byli tyto útoky vedené na P2P servery, na kterých byla zaznamenána aktivita s pirátským obsahem. Jediným problémem v této situaci bylo to, že DoS mohl postihnout i potencionálně nevinné uživatele (Mittal 2004, s. 453).

3.2.4.4. Soudní spory

Vzhledem k tomu, že se na P2P sítích dá sdílet jakýkoliv obsah, tak se dá očekávat, že dřív nebo později budou na P2P podány žaloby od autorů sdílených souborů. Jedním z příkladů, kdy k něčemu takovému došlo, byla třeba síť Napster nebo Kazaa, kde postupem času kvůli těmto problémům došlo k ukončení jejich provozu, protože provozovatelé nebyli schopní pirátství z jejich sítí vymýtit i přesto, že se zaručili, že tak učiní (Novinky.cz 2006).

Příkladem z České republiky je třeba bývalá síť Ulož to, která nyní funguje pouze jako osobní uložiště. Dříve Ulož to fungovalo jako uložiště, kde jste soubory mohli sdílet s ostatními. Tato změna nastala kvůli evropské legislativě, konkrétně zákonu o digitálních službách. (Evropská komise 2022) Vzhledem k tomu, že v evropě se v minulosti pirátství neřešilo na úrovni jako v americe, k tomuto došlo teprve v roce 2022. Ostatně první případ, kdy došlo v České republice k odnětí svobody bylo v roce 2013 (ČT24 2013).

3.3. Pirátství během 1. desetiletí 21. století

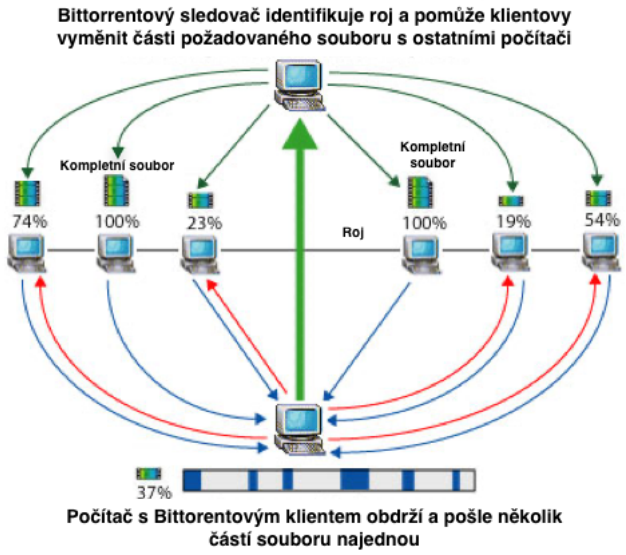
21. století přineslo do oblasti softwarového pirátství mnoho změn. Diskety a nástěnkové systémy se velice rychle přestali používat a primárními technologiemi, které se využívali v oblasti softwarového pirátství, byli především P2P sítě a kopie na CD. Technologie, které měli za úkol software před pirátstvím chránit, nově nebyli reakcí na nové technologie, které se používali k softwarovému pirátství, ale spíše reakcí na pirátství jako takové.

To ale neznamenalo, že se nové technologie přestali objevovat. Asi nejvýraznější technologií byli Bittorrenty, poddruh P2P sítí. Dále také došlo ke vzniku darknetu, jehož primární funkcí pirátství nebylo a mířilo prakticky na jakoukoliv nelegální internetovou činnost. (Bytescare 2024)

3.3.1. Pirátství přes Bittorrent

Bittorrent je P2P protokol, který se ve 21. století stal velice populární. V základech je jiný než předcházející P2P sítě, na rozdíl od jiných P2P totiž nestahuje soubor pouze z jednoho zdroje, ale stahuje části souboru od jiných uživatelů najednou, což způsobuje, že se soubory stahují rychleji (Legout, Urvoy-Keller, Michiardi 2005). Bittorrent taky používá princip „tit-for-tat“, což je hovorové vyjádření pro anglické slovní spojení „This for that“, což znamenalo, že pokud chcete něco dostat, musíte něco darovat, což mělo řešit problém s neštědrými uživateli na Bittorrentu.

V podstatě jste s Bittorrentem mohli dosáhnout rychlejšího stahování souměrně s tím kolik souborů jste sami nahráli. Bittorrent byl vyvíjen Americkým programátorem Bramem Cohenem v roce 2001 v programovacím jazyce Python. Cohen tvrdí, že sám svůj software nezneužil k porušení autorských práv a že jej vytvářel pro komunitu na stránkách etree.org, kde se sdílela hudba, u které bylo sdílení povoleno originálními autory. (Computer timeline b. r.)

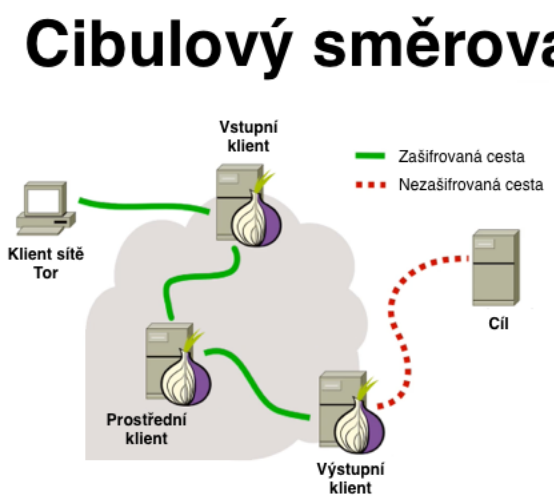


Obrázek 8: Průběh stahování z Bittorrentu (Computer timeline b. r.)

3.3.2. Pirátství přes darknet

O darknetu se poprvé mluvilo už na konci 90. letech 20. století v rámci akademické práce Irského studenta Iana Clarka. Tehdy darknet označován jako Freenet, který v roce 2000 vyvinul a vydal. Freenet umožňoval anonymní komunikaci mezi uživateli díky použití decentralizované sítě (Federrath 2001, s. 47). Termín darknet byl však zpopularizován díky cibulovému směrovači (Onion router) Tor, vyvinutého Americkou státní námořní výzkumnou laboratoří v roce 2002.

Tor byl zprvu využíván anonymně Americkou zpravodajskou komunitou, ale ukázalo se, že je anonymita k ničemu, pokud k ní má přístup pouze jediná zpravodajská služba. Tor byl Americkou vládou sdílen v rámci otevřeného přístupu v roce 2004, která následně finančně přispívala na jeho chod. Jak se doufalo, tak se tor začal používat mezi počítačovými nadšenci, soukromými advokáty a novináři, naneštěstí ho začali používat i Hackeři a teroristi a díky tomu se na Toru začal šířit nelegální obsah jakožto pirátěný software, prodej zbraní, drog nebo nelegální pornografie. Termín dark web byl pak v tisku poprvé použit v roce 2009 ve článku, který popisoval tyto nelegální praktiky. (Volle 2025) (Omar 2020)



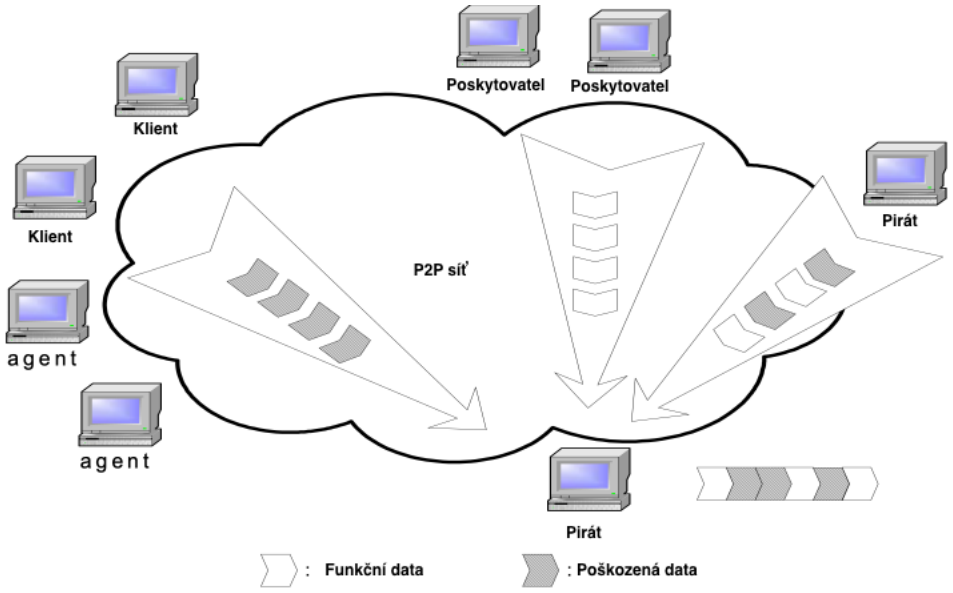
Obrázek 9: Průběh připojení k prohlížeči Tor (Judd 2018)

3.3.3. Ochrana proti pirátství na počátku 21. století

Jak již bylo zmíněno, ochrana proti pirátství ve 21. století už nereagovala na nejrůznější technologie, díky nimž bylo pirátství prováděno. Ochrany byli nyní vyvíjeny proti pirátství obecně a jen vzácně vznikali nějaké, které by svojí funkčností cílili na jedinou technologii. Mezi nejpodstatnější metody ochrany v této době patří online aktivace, limitace počtu instalací a software, který je přidělen osobnímu online účtu.

3.3.3.1. Aktivní otrava obsahu

Aktivní otrava obsahu je asi jedinou ochranou, která vyloženě reagovala na bittorrent. Jedná se o strategii, při které se do P2P sítě cíleně vkládá poškozená nebo nefunkční data, aby zabránila pirátům v získání kompletní a funkční kopie softwaru. Princip spočívá v tom, že piráti nejsou pouze odmítnuti, ale záměrně jim jsou poskytována vadná data, aby se maximalizovala jejich frustrace. Pokud uživatel není v síti rozpoznán jako legitimní, systém jeho žádost o stažení softwaru vyhodnotí jako neautorizovanou. V takovém případě může získat části softwaru od jiného legitimního uživatele, od oficiálního distributora nebo od uživatele, který software sdílí nelegálně. Pirát od nelegálního uzlu obdrží vždy funkční části softwaru, od prvních dvou zdrojů získá záměrně poškozené části. Pokud piráti takto získané nefunkční soubory dále šíří, dochází k rozšíření nekompletních nebo chybových kopií, což v komunitě pirátů zvyšuje celkovou míru frustrace. Aby tomuto předešli, museli by piráti kontrolovat každý soubor zvlášť (Xiaosong, Hwang 2008, s. 5).



Obrázek 10: Ilustrovaný příklad aktivní otravy obsahu na Bittorentové P2P síti (Xiaosong, Hwang 2008)

3.3.3.2. Online aktivace

V roce 2001 vydala společnost *Microsoft* tehdy nejnovější verze svého operačního systému Windows a balíčku kancelářských aplikací Office s názvy verzí XP. Microsoft sice nebyl první, kdo metodu online aktivace u svého softwaru použil, ale byl rozhodně první, kdo tuto metodu použil na velice známé produkty.

Online aktivace, jak už název napovídá, funguje tak, že se legitimnost licence ověří na internetu, nicméně počátky tohoto ověření internet nevyžadovali, neboť zde byla druhá možnost aktivace pomocí telefonu, kde uživatel uskutečnil hovor s technickou podporou, která ověření udělala. Princip je velice podobný jako u aktivačních klíčů, nicméně je zde krok navíc, který kontroluje například to, že daný klíč není sdílený a zároveň pravost klíče. (Afonin 2002)

3.3.3.3. Limit instalací

Limity instalací jdou téměř ve všech případech ruku v ruce s online aktivací, neboť je potřeba počet instalací nějak ověřit. Jednoduše jde o to, že s přístupovými klíčem můžete software aktivovat jen několikrát (Afonin 2002). Dokumentace limitovaných instalací je velice omezená a dnes funguje na trochu jiný princip u softwaru jakožto služby, než fungovala na přelomu 20. a 21. století. Jeden z příkladů dokumentace k tomuto tématu je například zachovalá stránka od společnosti Electronic Arts, kde je zmíněn průvod autorizace zařízení pro software s limitovaným počtem aktivací, zároveň je zde zmíněný i postup, při kterém se danému zařízení autorizace zruší. Proces, pro zrušení autorizace zařízení často vyžadoval pomoc technické podpory. (Electronic Arts 2009)

3.3.3.4. Software spjatý s účtem

Asi nejlepší softwarovou ochranou, která na počátku 21. století vznikla, byla ochrana, kde byl software spjatý s nějakým uživatelským účtem. Díky tomu, nebylo potřeba limitovaných instalací, neboť uživatel mohl software používat na jakémkoliv kompatibilním zařízení, na kterém se mohl přihlásit díky uživatelskému účtu pomocí přihlašovacího identifikátoru a hesla. Tato ochrana je efektivní, protože přístup k softwarové licenci umožní pouze danému uživateli a nikomu jinému, což byla určitě mnohem lepší varianta než aby k jednomu zařízení, na kterém je software nainstalován měl přístup každý, kdo se samotným zařízením přijde do kontaktu. Zároveň tato metoda ochrany byla uživatelsky přívětivější, neboť řešila problém se samotným zrušení autorizace zařízení. (Rahmatallah b.r.)

Příkladem této ochrany je třeba služba *Steam*, která byla v roce 2003 spuštěna jakožto služba, kde společnost *Valve* mohla spravovat aktualizace svých videoher. Postupně se však tato platforma proměnila na největší online obchod s videohrami a jejich licencemi, které byli spjaty se Steam účtem. (Wilde, Sayer 2022)

3.4. Pirátství během 2. desetiletí 21. století

Tato práce sleduje vývoj softwarového pirátství a ochrany proti němu od roku 1980 až po moderní dobu, utnutou v roce 2020. V této kapitole bude podrobněji vysvětleno pirátství na chytrých telefonech, které se objevili na konci prvního desetiletí a zároveň cloudového pirátství, které umožňuje používání softwaru mimo naše vlastní zařízení. Dále zde budou rozvinuty některé moderní metody ochrany jako je například nechvalně proslulá neustálá nutnost připojení k internetu nebo dnes hojně využívaná ochrna *Denuvo* vyvinutá společností *Irdeto* a pár dalších ochran podobného typu.

3.4.1. Pirátství na chytrých telefonech

Když během roku 2007 společnost *Apple* odhalila svůj první chytrý telefon iPhone a operačním systémem pro telefony iOS. S největší pravděpodobností firma Apple změnila to, jak společnost chápala pojem telefon. Netrvalo to dlouho, a rok na to byl odhalen telefon s konkurenčním otevřeným operačním systémem *Android* od společnosti Google. Od té doby, telefonní operační systémy Android a iOS, chápeme dosud jako standart pro telefony. S novou technologií se však objevil i nový prostor, kde se dalo praktikovat pirátství a začalo tak pirátství mobilních aplikací jakožto softwaru. Díky tomu, že platforma Android byla otevřená a umožňovala uživateli větší svobodu se na této platformě dal software stahovat bez placení, a to jednodušeji než na konkurenčním uzavřeném iOS, kde byla instalace aplikací do nedávna povolena pouze z oficiálního obchodu. Na platformě iOS bylo však od roku 2022 v evropské unii díky změně zákonu o digitálních službách povoleno stahování aplikací z jiných zdrojů než z oficiálního obchodu společnosti *Apple*, což posílilo pirátství i na této platformě v oblastech evropské unie (Apple 2024).

3.4.1.1. Stahování mobilních aplikací mimo oficiální obchod

Jak již bylo řečeno, hlavním způsobem pirátství na chytrých telefonech bylo stahování aplikací z alternativních obchodů či přímo z prohlížeče. Uživatel se tak chtěl vyhnout platbě za aplikace a využíval k tomu prostředí jako byl například *GetApk market*, nebo *Aptoid*.

Pochopitelně byli tyto metody do nedávna jednoduše proveditelné pouze na platformě Android, neboť iOS neumožňovalo stahování aplikací z jiných zdrojů než ze svého vlastního. Tato skutečnost ale nic nemění na tom, že se na iOS pirátit dalo. Pirátění na iOS bylo mnohem složitější a vyžadovalo prolomení ochrany v angličtině známé jako „jaibreak“, následně byl postup podobný jako u konkurenčního operačního systému. Vyjímku tvořil pouze rozdíl mezi formáty aplikací pro jednotlivé systémy (Herrman 2020).

3.4.1.2. modifikace mobilních aplikací

Vzhledem k tomu, že monetizace softwaru na telefonech funguje z velké části jinak než u softwaru na počítačích, se dá předpokládat, že stahování aplikací z neoficiálních zdrojů nebyl na telefonech jediný problém. Většina aplikací na telefonech na sebe vydělává prostřednictvím nákupů v aplikacích, protože velké množství aplikací bylo zadarmo. V praxi to vypadalo tak, že například v mobilních hrách od společnosti *Supercell* jste často měli k dispozici 2 herní měny, a to obyčejné zlaťáky a drahokamy. Zatímco zlaťáky byli nezbytné pro průchod hrou a získávali se zadarmo během hraní, drahokamy byli takzvaně prémiovou měnou, která většinou nebyla ke hraní potřeba a sloužila například pro rychlejší průchod hrou nebo kosmetické doplňky, tato měna však byla za peníze.

Mnoho her na telefonech využívá monetizace na podobném základu a díky tomu se vývojáři nemusí bát, že by jejich hry někdo pirátil. Mimo hry se třeba jednalo o software a aplikace se zabudovanou reklamou v aplikaci, která se dala za nízký poplatek trvale odstranit. Zde však hraje důležitou roli modifikace, tedy úprava aplikací, která změní jednotlivé funkce. Pomocí modifikací, které umožňovala například aplikace Lucky Patcher se dala platba obejít a vy jste tak mohli získat prémiové funkce, měnu nebo odstranění reklam z aplikací zadarmo. Je nutné podotknout, mnoho aplikací proti modifikacím měl dobře zabudovanou ochranu a modifikovali se především aplikace, které nevyžadovali neustálé připojení k internetu.

3.4.2. Cloudové pirátství

Mnoho lidí, by si pod pojmem cloudové pirátství mohlo vybavit obyčejné stahování souborů a softwaru z internetu, nicméně tomu tak ale není, jelikož při cloudovém pirátství vlastně vůbec ke stahování nedochází. Cloudové pirátství se především týká digitálního pirátství jako takového spíše než softwarového pirátství, to ale neznamená že u softwaru k této činnosti také nedochází. Cloudové pirátství chápeme jako používání softwaru přímo v prostředí prohlížeče, nebo jiného rozhraní, které uživateli umožňuje software používat mimo svůj vlastní hardware.

Nejlepším příkladem v oblasti digitálního pirátství je sledování filmů a seriálů online a zadarmo v prohlížeči. To že se daný film nenachází přímo na disku uživatele pak dělá způsoby dohledání pirátů mnohem náročnější. Pirátský obsah je navíce používán i v prostředí běžně dostupných cloudových služeb, což může mít negativní dopad na poskytovatele takových služeb, kteří musí pak investovat do různých ochranných systémů na své platformě, aby tak předcházeli právním problémům. (Bytescare 2024)

3.4.3. Moderní ochrana proti pirátství

Trend ve vývoji ochrany proti softwarovému pirátství se na počátku druhého desetiletí nezměnil. Primárně vznikali ochrany se zaměřením na pirátství jako takové, než aby cílili vyloženě na jednu distribuční technologii. V této podkapitole bude rozvedena ochrana vyžadující neustálého online připojení a dále také pár moderních ochran od specifických firem jako například *Denuvo.*

3.4.3.1. Nutnost být neustále online

Jak již bylo zmíněno ve druhé kapitole, ochrana softwaru, kvůli které musí být uživatel neustále online je, pro uživatele značnou překážkou. Žijeme sice v době, kdy máme k internetu jednodušší přístup než kdy dřív, přesto však není neustálý a ochrana tohoto typu může být tím pádem občas spíše nepříjemností. Problém pak nastává, když daný software nevyžaduje internet ke svému běžnému používání jako je příběhová videohra pro jednoho hráče nebo kancelářský software, který ukládá soubory na místní disk. Funkčnost této ochrany, je nehledě na tuto skutečnost vcelku efektivní, protože s neustálou kontrolou v reálném čase, může být složité takovou ochranu prolomit.

Prvními softwary, které tento typ ochrany využili, byli dvě videohry od společnosti *Ubisoft* a to konkrétně *Silent Hunter 5: Battle of the Atlantic* a mnohem známější *Assassin`s creed II* Příběhová hra, která neměla žádné herní funkce závislé na internetu kromě samotné ochrany, tyto videohry byli vydány roku 2010 (Yoon 2021). Důležité je také zmínit, že nutnost být neustále online může v průběhu času způsobit větší množství abandonewaru.

3.4.3.2. Denuvo

Denuvo je specifická ochrana vyvíjená společností *Irdeto*, která kombinuje větší množství ochran softwaru a soustředí se na ochranu videoher. Funkce ochrany Denuvo spočívá v ochraně videoherního titulu před samotným vydáním a po něm. Zatímco před vydáním, využívá technologie jako jsou již zmíněné vodoznaky tak zároveň různé preventivní metody uvnitř

samotného vývojářského studia, po vydání má na starost ochranu proti uživatelům využívající různé podvodné praktiky třetích stran a různé kyberbezpečností služby. Během celého procesu vývoje a vydání videohry také nabízí ochranu rozšíření, ověřování integrity a obfuskaci kódu. Denuvo je technologie kterou lze využít na vícero platformách od počítačů, přes konzole až po chytré telefony a spravuje také ochranu před emulací (Irdeto b.r.). Ochrana *Denuvo* byla podle dostupných informací poprvé použita v roce 2015 při vydání videohry *FIFA 15*. Dlouho byla tato ochrana považována za neprolomitelnou mnoha crackery ale po pár měsících se stejně někomu podařilo *Denuvo* prolomit což zajistilo videohrám celkově dlouhou dobu bez distribuce jejich pirátských kopií. Denuvo je ochranou, která se používá běžně i dnes a často bývá postupem času z videoher odstraněna kvůli nákladům na její provoz, který po cracknutí ztrácí význam.

3.4.3.3. VMProtect

I přestože Denuvo má v povědomí uživatelů, co se týče ochrany softwaru aktuálně asi největší podíl, tak má spoustu konkurentů a jedním z nich je například *VMProtect* vyvíjený ruskou společností *VMProtect* software. Podobně jako Denuvo nabízí VMProtect například obfuskaci kódu a spoustu jiných ochranných technologií fungujících na podobném principu jako *Denuvo*. *VMProtect* má ale i nějaké technologie, které *Denuvo* nepoužívá jako například použití sériových čísel, virtuální stroj, a navíc je ve videohrách ale i neherním softwaru. Někdy také dochází k situacím, kde software obsahuje jak *Denuvo,* tak *VMProtect* (VMProtect software b.r.).

4. Předpokládaný vývoj pirátství do budoucna

Softwarové pirátství zřejmě jen tak nezmizí. Ačkoliv nelze s jistotou předvídat budoucí technologický vývoj, aktuální trendy nám umožňují alespoň částečně odhadnout jeho další směřování. V této kapitole budou hypoteticky analyzovány tři oblasti, které dle osobních názoru autora, mohou v budoucnu pirátství významně ovlivnit: rostoucí počet předplacených služeb na úkor nákupu doživotních licencí, omezené možnosti legálního přístupu ke starším softwarům a vliv umělé inteligence jak na samotné piráty, tak na vývoj ochranných mechanismů.

4.1. Přechod z nákupu licence na předplatné

V roce 1999 představila společnost Salesforce Inc. první softwarové řešení ve formě služby (tzv. SaaS – Software as a Service) (Fryer, b. r.). Tento model postupně převzala řada dalších společností. Například společnost Adobe přešla s verzí Creative Cloud na předplacený model, přičemž ještě nějakou dobu nabízela i poslední samostatně licencovanou verzi CS6. Od roku 2017 se však k programu Photoshop již legálně nelze dostat jinak než skrze předplatné (Dove 2013).

Tento model se stává stále běžnějším – nové softwary vznikají výhradně jako služby a starší produkty jsou převedeny na předplatné. Tím se mění nejen uživatelský přístup, ale i samotná ekonomika softwaru. Otázkou zůstává, zda právě tento přechod nezpůsobí nový nárůst pirátství, jelikož někteří uživatelé nebudou ochotni nebo schopni dlouhodobě platit pravidelné poplatky. Za předpokladu, že by uživatelé platili předplatné za více produktů současně je tento problém mnohem větší.

4.1.1. Proč software přechází na formu předplatného

Hlavním důvodem pro přechod na model předplatného jsou ekonomické výhody jak pro uživatele, tak pro vývojáře, protože vývojáři čelí nižším počátečním nákladům, protože pravidelné příjmy pomáhají firmám lépe řídit výdaje. Je snadnější vybrat si typ předplatného například pro jednotlivce nebo skupiny. Často tyto služby fungují přímo z cloudu, takže je k nim přístup odkudkoliv. Dobře se dají sledovat změny v aktualizacích. Předplatná navíc umožňují pružně reagovat a nové bezpečnostní hrozby. Tyto výhody proto dělají pro vývojáře software jako službu velice atraktivní (Marco 2024).

4.1.2. Jak se s předplatnými změnila úroveň pirátství

Bohužel na tuto otázku neexistují veřejně dostupná data. Průzkumy ale ukazují, který software je nejvíce pirátěný a podle nich je tím nejčastější software od společnosti microsoft a od společnosti adobe, konkrétně Microsoft Windows, Microsoft Office a Adobe Photoshop (Beckett 2022).

Za vysvětlením samozřejmě může stát čistě nespokojenost s předplatnými, ale s největší pravděpodobností je na vinně nutnost softwaru pro normalizovanou funkcionalitu počítačů, co se operačního systému týče. U operačního systému microsoft Windows je možnost předplatného pouze u služby Microsoft 365 business, která cílí na firmy, jinak je platba jednorázová. U microsoft office předplatné je a cílí i na jednotlivce. Toto předplatné ale není agresivní a zároveň zde existuje možnost zakoupení jednorázové licence, nicméně popularita microsoft office jakožto nejpoužívanějšího kancelářského softwaru může být také na vině. Posledním softwarem je již zmíněný adobe photoshop, kde je cena za předplatné už bohužel velmi vysoká ale zároveň je společnost adobe nechvalně známá svou špatnou zákaznickou zkušeností, opět zde ale platí, že photoshop je nejpoužívanější software na úpravu fotografií. Podle průzkumů tedy nemůžeme prozatím dokázat, že software jako služba skutečně úroveň pirátství zvyšuje.

4.1.3. Návrat doživotní licence

Tím, že model software jako služba roste a do budoucna bude růst ještě víc, se nejspíše dočkáme situace, kdy budou lidé nuceni platit za mnoho služeb najednou nemalou sumu. Je tu ale řešení, a to nabídka softwaru za jednorázový poplatek, jako tomu bylo kdysi. Tato možnost se v poslední době opět prosazuje. Dobrým příkladem může být aplikace *Sketch* na tvorbu uživatelských rozhraní a výzkum uživatelské zkušenosti. Sketch byl do nedávna poskytován na bázi předplatného za cenovku 10 amerických dolarů za měsíc, nyní je zde i druhá možnost, a to zakoupení licence za cenu 120 amerických dolarů, u které platí že během následujícího roku dostanete všechny aktualizace poskytované i normálním předplatitelům, po této době vám aplikace zůstane v poslední verzi, která v tomto časovém okně byla poskytnutá, rozdílem zde však je, že tato verze zůstane uživateli trvale (Sketch b. r.). Tato možnost je vhodná pro uživatele, kteří nemají využití pro nové funkce.

Sketch však není jediný, dále je zde třeba již zmíněný microsoft se svými kancelářskými aplikacemi v balíčku microsoft office a i přesto, že se poslední dobou snaží tlačit především

předplatné Microsoft 365 skrze marketingové kampaně, tak zde zůstává možnost koupit si jednorázové verze, které vychází přibližně jednou za 2-4 roky (Microsoft b. r.). Pokud se chceme vyhnout potenciálním problémům, které předplatná mohou do budoucna zavinit v nepřímé podpoře pirátství, tak bychom měli uživatelům dát možnost volby mezi předplatným, i trvalou licencí.

4.2. Abandonware – opuštěný software

Opuštěný software označuje programy, které již nejsou komerčně distribuovány ani podporovány. Lze si představit starší verze běžně používaných programů, například Adobe Photoshop CS6, nebo operačních systémů, jako Windows XP či MacOS X.

K opuštěnému softwaru patří také videohry, které nejsou dostupné v prodeji, zejména tituly pro konzole starší než dvě generace, jejichž fyzické kopie se neprodávají a digitální distribuce byla ukončena v důsledku rušení e-shopů. Stejné riziko hrozí hrám na počítačových platformách z důvodů obdobných těm u konzolí. Pokud uživatel touží takový software používat a neexistuje legální způsob jeho získání, jsou možnosti omezené a často vedou k nelegálnímu stažení. Alternativou je nákup fyzických kopií na sekundárním trhu, avšak tyto mohou mít vysokou sběratelskou hodnotu, což představuje dilema, zejména u předem použitého softwaru. Opuštěný software svou nedostupností podporuje pirátství a s časem se počet takovýchto programů zvyšuje.

4.2.1. Proč chtějí uživatelé používat tento software

Odpověď na otázku, proč někteří uživatelé volí opuštěný software, lze nalézt zejména v oblasti videoher. Nadšenci mohou chtít hrát starší díly známých sérií, například *The Legend of Zelda*, *Pokémon* či *Resident Evil*, aby sledovali vývoj her, doplnili si informace o příběhu nebo z jiných osobních důvodů. V těchto případech nedostupnost legálních kopií často vede k nelegálnímu stažení, protože uživatelé většinou chtějí krátkodobý přístup pouze k dané hře. Naopak sběratelé, kteří preferují fyzické kopie a chtějí software vlastnit, mají mnohem nižší motivaci k pirátství, neboť nelegální digitální verze je nezajímají.

Další skupinou jsou běžní uživatelé, kteří využívají pracovní software, jako Microsoft Office nebo starší operační systémy. Tito uživatelé si mohou klást otázku, proč by měli volit zastaralý software s omezenými funkcemi. Hlavním důvodem je stabilita. Například operační systém Windows 11 čelil problémům s chybnými aktualizacemi, jako byla aktualizace KB5053598,

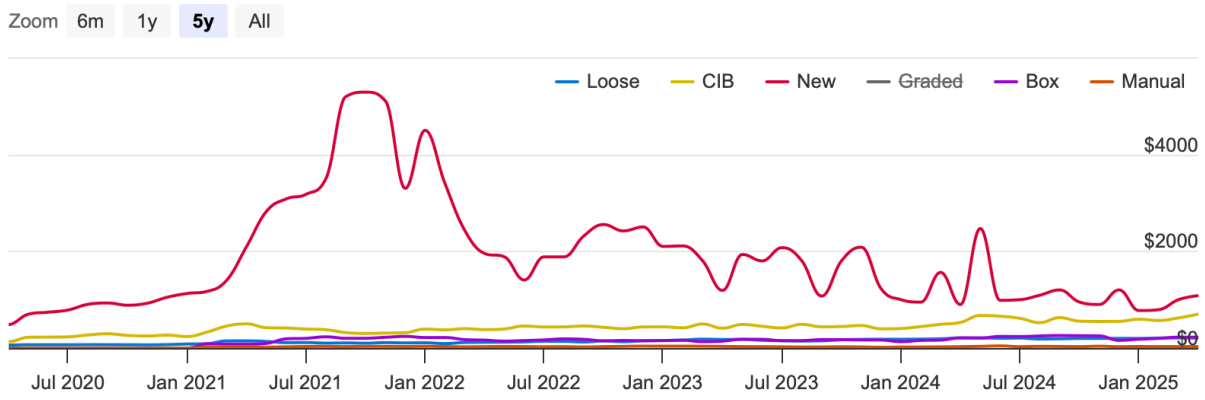
která způsobovala potíže při spouštění zařízení nebo při vzdáleném připojení, kdy docházelo k automatickému odpojení.

(Doffman 2025). Podobné problémy odrazují uživatele Windows 10 od přechodu na novější systém, zejména pokud v minulosti zažívali obdobné obtíže. Starší software je proto preferován pro svou stabilitu, zejména těmi, kteří nepotřebují nové funkce.

Kromě toho existuje software, který byl zcela ukončen, jako Adobe XD, nástroj pro návrh uživatelských rozhraní od společnosti Adobe. Tento software je v současnosti v režimu údržby, kdy stávající uživatelé dostávají bezpečnostní aktualizace, do budoucna je ale v plánu její kompletní zrušení. V takových případech mají uživatelé dvě možnosti: přejít na alternativní nástroje, jako Figma, Sketch a Penpot, nebo se uchýlit k nelegálnímu stažení (UXNESS b. r.).

4.2.2. Výzvy spojené se získáním opuštěného softwaru

Opuštěný software má, jak již bylo uvedeno, pouze jednu legální cestu získání, a to prostřednictvím bazarového prodeje. U některých titulů však cena mnohonásobně převyšuje jejich původní hodnotu při vydání. Pro sběratele je navíc důležité, zda se jedná o použitou, či nepoužitou kopii, přičemž cena nepoužitých kopií dosahuje extrémně vysokých hodnot. Příkladem je videohra *Pokémon Emerald* z roku 2005 pro přenosnou konzoli *GameBoy Advance* od společnosti *Nintendo*. Podle uživatele na sociální síti *Reddit* se tato hra při vydání prodávala za 35 amerických dolarů (102Mich 2023), což v té době odpovídalo přibližně 840 Kč (ČNB 2005). V současnosti se cena použité kopie pohybuje kolem 200 amerických dolarů, což představuje téměř šestinásobek původní ceny. U nepoužité kopie se cena vyšplhá až na 1100 amerických dolarů, což podle aktuálního kurzu odpovídá 24 145Kč (ČNB 2025) (Price Charting 2025). Pro většinu uživatelů, kteří nejsou sběrateli, je taková cena nepřijatelná, zejména s ohledem na potřebu dobového hardwaru. Alternativou je emulace, avšak pokud uživatel nevlastní originální kopii softwaru, i tato varianta je z právního hlediska sporná.



Obrázek 11: Vývoj ceny videohry Pokémon emerald (Price Charting 2025)

Dalším příkladem je software *Photoshop CS6*, který se přestal oficiálně prodávat v roce 2017 a stal se opuštěným softwarem. Při vydání stál tento software 699 amerických dolarů (Blagdon 2012), což v té době odpovídalo přibližně 14 000 Kč. (ČNB 2012) V současnosti je jeho cena výrazně vyšší, například na webu ruzovka.cz lze software nalézt za 39 999 Kč, případně jej zájemci musí hledat na bazarech.

4.2.3. Proč vývojáři a vydavatelé software nezpřístupňují?

Důvodů, proč není opuštěný software běžně zpřístupňován, existuje několik. Hlavním z nich je, že software byl navržen pro starší hardware, a jeho přizpůsobení moderním zařízením by nemuselo být ekonomicky výhodné vzhledem k omezenému zájmu uživatelů. Dalším faktorem je obchodní model společností. Například společnost *Adobe* by nabídkou starší verze *Photoshop CS6* mohla odlákat potenciální zákazníky od novějších verzí, které jsou dostupné formou předplatného a při používání delším než dva a půl roku nabízejí výhodnější cenu (Adobe b. r.). Dalším faktorem je závislost softwaru na serverech, bez nichž není funkční. Příkladem je videohra *Concord*, která byla stažena z prodeje dva týdny po vydání kvůli nízké prodejnosti. Uživatelé, kteří hru vlastnili, ji nemohli dále používat, protože její funkčnost závisela na serverech, které byly rovněž vypnuty. V tomto případě nepomůže ani nelegální získání softwaru (Ellise 2024).

4.2.4. Jak tento problém řešit

Jednou z možností, jak zpřístupnit opuštěný software, je jeho opětovné uvolnění k prodeji a přizpůsobení pro moderní zařízení, což může přinést společnostem zisk. Například společnost *Nintendo* nabízí vybrané starší hry prostřednictvím předplatného služby *Nintendo Switch Online*. Tato služba nezahrnuje všechny tituly a neslouží výhradně k hraní starých her, přesto ji využívá značný počet hráčů, díky čemuž *Nintendo* generuje příjmy, z již existujících

produktů. Další možností je remaster, tedy úprava starší hry tak, aby působila moderněji, při zachování původní podstaty, nebo remake, což je kompletní přepracování titulu od základů, někdy doplněné o nové prvky. Výrazným příkladem remaku je hra *Resident Evil 4* od společnosti *Capcom*, která v roce 2023 získala nominaci na hru roku (The Game Awards 2023). Důležité je uvědomit si, že software, zejména videohry, představuje formu umění, a proto je jeho zachování pro budoucí generace klíčové.

4.3. Umělá inteligence v softwarovém pirátství

V poslední době se umělá inteligence stala velkým společenským tématem. Rozšíření generativních modelů jako např. *ChatGPT* od společnosti *OpenAI*, *Adobe Firefly* od společnosti *Adobe* nebo *Grok* od společnosti *X* na tom měli velký podíl. Umělá inteligence se však používala i předtím, a to dokonce i k ochraně softwaru proti pirátství. Je však zřejmé, že s rostoucí popularitou této technologie se její používání v této oblasti více rozšíří, a to nejen k ochraně softwaru ale nejspíše i k pirátění.

4.3.1. Počátek umělé inteligence v ochraně softwaru

Jak již bylo zmíněno, umělá inteligence se proti pirátství používala už dřív než po nedávném vzrůstu její vnímání společností. První software na ochranu proti digitálnímu pirátství začal vznikat už druhém desetiletí 21. století. Tento software se ze začátku soustředil pouze na ochranu hudby nebo filmů, nikoliv softwaru, ale vzhledem k tomu, že pro softwarové pirátství se dali aplikovat podobná pravidla, tak se brzo rozšířili i do této oblasti. Příkladem takovéto ochrany, je služba od společnosti *Red Points*, která pomocí strojového učení poskytuje mnoho funkcí, jako je rušení online distribuce zpirátěných verzí, boj proti přeprodávání aktivačních klíčů na šedém trhu, nebo rušení viditelnosti souborů na P2P sítích a BitTorrentových stránkách (RedPoints b. r.). Nicméně umělá inteligence nebyla hlavním nástrojem v boji proti softwarovému pirátství.

4.3.2. Zneužívání umělé inteligence

Umělá inteligence nabrala v roce 2023 na popularitě díky jazykovým modelům generativní umělé inteligence a mnoho lidí se jí pokusilo zneužít, například ke generaci obsahu týkající se pornografie, hackování, nebo i pirátění. vývojáři těchto modelů se je pochopitelně snažili vybavit bezpečnostními zásadami, které by jím zabraňovali těmto zneužitím podléhat, nicméně se díky určitým konverzačním metodám podařilo uživatelům tyto příkazy obejít. Častou metodou bylo odůvodnění umělé inteligenci, že nelegální činnost, kterou po ní uživatel žádá,

chce z čistě teoretického a výzkumného důvodu, na čemž pak umělá inteligence přistoupila na uživatelovy požadavky. Tento problém je do budoucna poměrně snadno řešitelný a novější verze těchto generativních modelech umělé inteligencích jim budou schopné čelit lépe než doposud. Příkladem takového zneužití, může být například moment, kdy umělá inteligence ChatGPT poskytla návod na vytvoření bomby uživateli, který v konverzaci zmínil, že se jedná o fiktivní hru. Díky tomu, že umělá inteligence byla přivedena do fiktivního prostoru začala vyhledávat cenzurovaný obsah. (Newman 2024) I přestože tento příklad se netýká softwarového pirátství, tak perfektně ukazuje, jak lze umělou inteligenci využít i k jiným nelegálním aktivitám.

4.3.3. Ochrana i pirátství v budoucnosti

Umělá inteligence bude pro tématiku softwarového pirátství v budoucnu velice podstatná, ať už jakožto zabezpečení softwaru, tak i způsobem, jak software nelegálně a rychle crackovat a poskytovat pirátům. Už nyní umělá inteligence dokáže vyhledat, nebo aktivně monitorovat zpirátěný obsah, ale do budoucna může například vytvářet mnohem sofistikovanější vodoznaky, než měl software doposud.

Naopak piráti budou mít přístup k různým botům nebo nástrojům, jež rychle uvolňují streamovaný obsah (Onsist 2023). Tato technologie začala být populární poměrně nedávno a díky tomu můžeme jen spekulovat, jak přesně se bude dát využít i zneužít.

Závěr

Softwarové pirátství zde bylo, je a s největší pravděpodobností i nadále bude. To však neznamená, že se ochrana proti němu nemůže dál vyvíjet a držet krok, jak se jí to dosud celkem úspěšně dařilo. Klíčem do budoucna je, aby ochrany byly navrženy tak, aby co nejméně zasahovaly do pohodlí legitimního uživatele, a zároveň působily jako překážka, která odradí crackera od pokusu o prolomení.

Práce ukázala, že navzdory slabší dokumentaci tématu existuje překvapivé množství ochranných mechanismů, jak technického, tak právního rázu. Je pravděpodobné, že mnohé z nich byly zapomenuty nebo nikdy důkladně zdokumentovány. Zajímavým tématem byly také méně tradiční přístupy, jako je klamavé protipirátství. Přestože žádná z ochran není stoprocentně účinná, jejich cílem není absolutní neprolomitelnost, ale spíše co nejvíce zdržet nelegální šíření, aby se pirátství stalo méně výhodnou volbou než legální nákup.

Práce dále ukázala dopady pirátství na vývojáře i uživatele – a to jak negativní, tak i určité pozitivní aspekty, například pokud pirátství funguje jako forma šíření nebo zpětné vazby od širší komunity. Zároveň bylo zdůrazněno, že i uživatel nese rizika, například v podobě malwaru, a pirátství se mu nemusí dlouhodobě vyplatit.

V závěru byla nastíněna i témata, která mohou ovlivnit budoucí vývoj v této oblasti, jako je opuštěný software, model software jako služba a umělá inteligence. Tyto oblasti mohou, ale nemusí vývoj pirátství dále formovat.

Cílem této práce bylo vytvořit ucelený přehled klasických i moderních metod ochrany proti softwarovému pirátství a zasadit je do širšího kontextu. Je předpokládáno, že tento cíl byl splněn a že práce může v budoucnu sloužit jako stručný výukový materiál, který čtenáře provede vývojem této stále aktuální problematiky.

Seznam použité literatury

1. 102MICH. Real copy of Emerald from 2002-03. Online. In: Reddit. 2023. Dostupné z: https://www.reddit.com/r/PokemonEmerald/comments/14ce7m6/real_copy_of_emerald_from_200203/. [cit. 2025-04-29].
2. ADOBE. Photoshop. Online. In: Adobe. C2025. Dostupné z: https://www.adobe.com/products/photoshop.html. [cit. 2025-04-29].
3. AFONIN, Oleg. Evaluation of activation based software license enforcement. Thesis/Dissertation. Vancouver: University of British Columbia, 2002.
4. AGENCE PDN. Social Consequences of Piracy (1). Online. In: Agence PDN. 2023. Dostupné z: https://agencepdn.com/en/les-consequences-sociales-du-piratage-lemploi/. [cit. 2025-04-29].
5. ALBERT a MORSE. Combatting Software Piracy by Encryption and Key Management. Online. Computer. 1984, roč. 17, č. 4, s. 68-73. ISSN 0018-9162. Dostupné z: https://doi.org/10.1109/MC.1984.1659112. [cit. 2025-04-29].
6. APPLE. About alternative app distribution in the European Union. Online. In: APPLE. Apple. 2024. Dostupné z: https://support.apple.com/en-us/118110#:~:text=If%20you%20prefer%20using%20apps,App%20Store%20without%20your%20permission. [cit. 2025-07-31].
7. ASCIONE, Claudia. Why Standards Development Organizations Need to Use DRM Software. Online. In: Vitrium. 2024. Dostupné z: https://www.vitrium.com/blog/drm-for-standards-development-organizations. [cit. 2025-04-29].
8. BAINCE ACADEMY, Peer-to-Peer Networks Explained. Online. In: BINANCE. Binance Academy. 2019, 16.10.2022. Dostupné z: https://academy.binance.com/en/articles/peer-to-peer-networks-explained. [cit. 2024-05-22].
9. BARTOŇ, Martin. Vše o ochraně proti kopírování SafeDisc. Online. In: Diit.cz. 2001. Dostupné z: https://diit.cz/clanek/vse-o-ochrane-proti-kopirovani-safedisc. [cit. 2025-04-21].

10. BARTOŇ, Martin. Vše o ochraně proti kopírování SecuRom. Online. In: Diit.cz. 2001. Dostupné z: https://diit.cz/clanek/vse-o-ochrane-proti-kopirovani-securom. [cit. 2025-04-21].
11. BECKETT, Max. Piracy Report. Online. In: RVU. USwitch. 2022. Dostupné z: https://www.uswitch.com/broadband/studies/piracy-report/. [cit. 2025-07-07].
12. BEX FOSTER. Do people pirate games before they buy the actual games? Online. In: Quora. 2016. Dostupné z: https://www.quora.com/Do-people-pirate-games-before-they-buy-the-actual-games. [cit. 2025-04-29].
13. BLAGDON, Jeff. Adobe announces CS6 pricing and pre-orders, estimated delivery May 7th. Online. In: The Verge. 2012. Dostupné z: https://www.theverge.com/2012/4/23/2968192/adobe-cs6-pricing-availability-creative-cloud-announcement. [cit. 2025-04-29].
14. BRUSH, Heidi Marie. Phreaking. Online. In: BRITANNICA. Britannica. B.r. Dostupné z: https://www.britannica.com/technology/telecommunication. [cit. 2025-07-31].
15. BYTESCARE, Blog. History of Digital Piracy – Ultimate Guide. Online. In: BYTESCARE. Bytescare. 2024. Dostupné z: https://bytescare.com/blog/history-of-digital-piracy. [cit. 2025-07-17].
16. BYTESCARE. Understanding Cloud Piracy: Its Forms, Threats, and Solutions. Online. In: Bytescare Blogs. 2024. Dostupné z: https://bytescare.com/blog/cloud-piracy. [cit. 2025-07-31].
17. COLLABIM. Co je to WWW a jak funguje. Online. In: Seo akademie collabim. B.r. Dostupné z: https://www.collabim.cz/akademie/knihovna/co-je-to-www-a-jak-funguje/. [cit. 2025-07-31].
18. COMPUTER TIMELINE. Bram Cohen (BitTorrent). Online. In: Computer timeline. B. r. Dostupné z: http://www.computer-timeline.com/timeline/bram-cohen/. [cit. 2025-07-17].
19. CORNELL LAW SCHOOL. Piracy. Online. In: CORNELL UNIVERSITY. Cornell Law School. B. r. Dostupné z: https://www.law.cornell.edu/wex/piracy. [cit. 2025-07-31].

20. CRAIG, Paul P. a HONICK, Ron. Softwarové pirátství bez záhad. Praha: Grada, 2008. ISBN 978-80-247-1765-4. [cit. 2025-03-04].

21. CVRČEK, Martin. Pokud jste na mizině, radši naše hry nelegálně stahujte a nevyužívejte stránky jako G2A, vzkazují tvůrci Postalu. Online. In: INDIAN. 2023. Dostupné z: https://indian-tv.cz/clanek/pokud-jste-na-mizine-radsi-nase-hry-nelegalne-stahujte-a-e2c6np. [cit. 2025-04-29].

22. ČESKÁ BANKOVNÍ ASOCIACE. Šedý trh. Online. In: Česká bankovní asociace. B.r. Dostupné z: https://www.cbaonline.cz/sedy-trh. [cit. 2025-07-31].

23. ČNB. USD průměrné kurzy 2005, historie kurzů měn. Online. In: Kurzy.cz. 2005. Dostupné z: https://www.kurzy.cz/kurzy-men/historie/USD-americky-dolar/2005/. [cit. 2025-04-29].

24. ČNB. USD průměrné kurzy 2012, historie kurzů měn. Online. In: Kurzy.cz. 2012. Dostupné z: https://www.kurzy.cz/kurzy-men/historie/USD-americky-dolar/2012/. [cit. 2025-04-29].

25. ČNB. USD, americký dolar - převod měn na CZK, českou korunu. Online. In: Kurzy.cz. 2025. Dostupné z: https://www.kurzy.cz/kurzy-men/kurzy.asp?a=X&mena1=USD&mena2=CZK&c=1100&d=25.4.2025&convert=P%F8eve%EF+m%ECnu. [cit. 2025-04-29].

26. ČT24. V Česku padl první nepodmíněný trest za softwarové pirátství. Online. In: ČESKÁ TELEVIZE. ČT24. 2013. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/v-cesku-padl-prvni-nepodmineny-trest-za-softwarove-piratstvi-321519. [cit. 2025-07-17].

27. DAILEY John, Call Back Verification. Online. In: John Dailey Software.com. c2025. Dostupné z: https://www.johndaileysoftware.com/products/bbsutilities/callbackverification. [cit. 2025-04-07].

28. DE KOCK, D; LUBBE, S a KRITZINGER, W. Software piracy – Some aspects for South African managers to keep in mind. Online. South African Journal of Economic and Management Sciences. 2003, roč. 6, č. 4, s. 785-801. ISSN 2222-3436. Dostupné z: https://doi.org/10.4102/sajems.v6i4.1517. [cit. 2025-04-29].

29. DEKAY. Back to the 80s: Dongle Power!. Online. In: DeKay's Lofi Gaming. 2006. Dostupné z: https://lofi-gaming.org.uk/blog/2007/07/back-to-the-80s-dongle-power/. [cit. 2025-08-01].

30. DOFFMAN, Zack. Microsoft 'Install Fails'—New Update Breaks Windows. Online. In: Forbes. 2025. Dostupné z: https://www.forbes.com/sites/zakdoffman/2025/03/14/microsoft-install-fails-new-update-breaks-windows/. [cit. 2025-04-29].

31. DOOM WIKI. Shareware. Online. In: Doom wiki. B.r. Dostupné z: https://doomwiki.org/wiki/Shareware. [cit. 2025-08-01].

32. DOVE, Jackie. Adobe scraps Creative Suite software licenses in favor of cloud subscriptions. Online. In: MacWorld. 2013. Dostupné z: https://web.archive.org/web/20130802100114/http://www.macworld.com/article/2037034/adobe-scraps-software-licenses-in-favor-of-cloud-subscription-scheme-for-creative-suite-line.html. [cit. 2025-04-22].

33. DRING, Christopher. G2A: "We're not a grey marketplace, people just don't understand our business". Online. In: Game Industry.biz. 2017. Dostupné z: https://www.gamesindustry.biz/g2a-were-not-a-grey-marketplace-people-just-dont-understand-our-business. [cit. 2025-04-29].

34. ELECTRONIC ARTS. Deauthorize. Online. ELECTRONIC ARTS. EA. B.r., 2009. Dostupné z: https://activate.ea.com/deauthorize/. [cit. 2025-07-23].

35. ELHARONY Amr, The WinRAR Paradox: Why a "Free Trial" Software Became a Tech Staple. Online. In: Medium. 2023. Dostupné z: https://medium.com/@amrmelharony/the-winrar-paradox-why-a-free-trial-software-became-a-tech-staple-fc500a61b17b#:~:text=With%20the%20advent%20of%20cloud,revenue%2C%20indicating%20a%20solid%20business.. [cit. 2025-04-14].

36. ELLISE, Ryan. An important update on Concord. Online. In: SONY. Playstation. 2024. Dostupné z: https://blog.playstation.com/2024/09/03/an-important-update-on-concord/. [cit. 2025-04-29].

37. EMPEDOCLES. The FEAR & LOATHING in Las Vegas BBS was BUSTED Aug. 3, 1993. Online. In: HIGHER INTELLECT VINTAGE WIKI.

Https://wiki.preterhuman.net/Main_Page. 1993. Dostupné z: https://wiki.preterhuman.net/The_FEAR_%26_LOATHING_in_Las_Vegas_BBS_was_BUSTED_Aug._3,_1993. [cit. 2025-04-16].

38. EVANS, Chris. Hacking everything, by Chris Evans / scarybeasts: The cleverest floppy disc protection ever? Western Security Ltd. Online. In: Blogger. 2020. Dostupné z: https://scarybeastsecurity.blogspot.com/2020/12/the-cleverest-floppy-disc-protection.html?. [cit. 2025-03-04].
39. EVANS, Chris. Hacking everything, by Chris Evans / scarybeasts: Weak bits floppy disc protection: an alternate origins story on 8-bit. Online. In: Blogger. 2020. Dostupné z: https://scarybeastsecurity.blogspot.com/2020/06/weak-bits-floppy-disc-protection.html?. [cit. 2025-03-04].
40. EVROPSKÁ KOMISE. Nařízení o digitálních službách. Online. In: Evropská komise. 2022. Dostupné z: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_cs. [cit. 2025-07-17].
41. FEDERRATH, Hannes (ed.). Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25-26, 2000. Lecture notes in computer science. Berlin: Springer, 2001. ISBN 978-3-540-41724-8. ISSN 0302-9743.
42. FRYER Vicroria, Https://www.bigcommerce.com/blog/history-of-saas/. Online. In: Bigcommerce. 2003. Dostupné z: https://www.bigcommerce.com/blog/history-of-saas/. [cit. 2025-04-22].
43. GRANT, August. Communication Technology Update. 3rd edition. Focal Press, 1994. ISBN 0-7506-9593-5.
44. HAMILTON, James. What is software watermarking? Online. In: DR James Hamilton. 2010. Dostupné z: https://jameshamilton.eu/research/what-software-watermarking. [cit. 2025-04-22].
45. HASHEMI-POUR, Cameron. Software. Online. In: TechTarget. 2024. Dostupné z: https://www.techtarget.com/searchapparchitecture/definition/software. [cit. 2025-07-31].

46. HERRMAN, John. The Myth of iPhone App Piracy. Online. In: Gizmodo. 2020. Dostupné z: https://gizmodo.com/the-myth-of-iphone-app-piracy-5477732. [cit. 2025-07-31].

47. HISTORY.COM EDITORS. World Wide Web (WWW) launches in the public domain. Online. In: A+E NETWORKS EMEA. HISTORY. 2020, 29.4.2024. Dostupné z: https://www.history.com/this-day-in-history/world-wide-web-launches-in-public-domain. [cit. 2024-05-22].

48. HO, Justin. Why more new video games now cost $70. Online. In: Marketplace. 2023. Dostupné z: https://www.marketplace.org/story/2023/02/10/why-more-new-video-games-now-cost-70. [cit. 2025-04-29].

49. HOLCOVÁ, Irena. Autorské právo. Online. In: . B.r. Dostupné z: https://www.advocate.cz/cz/autorske-pravo. [cit. 2025-07-31].

50. HORTON, Samantha. Research Finds Digital Piracy Can Increase Profits For Companies. Online. In: Wyfi Indianapolis. 2019. Dostupné z: https://www.wfyi.org/news/articles/research-finds-digital-piracy-can-increase-profits-for-companies-19rjc#:~:text="People%20have%20argued%20for%20piracy,Business%20assistant%20professor%20Antino%20Kim. [cit. 2025-04-29].

51. ID SOFTWARE, DOOM (Shareware Episode). Online. In: Internet Archive. 1993, 25.6.2012. Dostupné z: https://archive.org/details/DoomsharewareEpisode. [cit. 2025-04-14].

52. INDIAN - POŘAD O HRÁCH. Piráti nám paradoxně pomohli prodat více kopií Poldy 7, přiznává Petr Svoboda - PVP 1s02. Online. In: GOOGLE. YouTube. 2022. Dostupné z: https://www.youtube.com/watch?v=0KT2aIPgdC4&t=130s. [cit. 2025-04-29].

53. INTERPOL. Digital piracy. Online. In: Interpol. B. r. Dostupné z: https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Digital-piracy. [cit. 2025-07-31].

54. IRDETO. Video game security solutions. Online. In: Irdeto. B.r. Dostupné z: https://irdeto.com/video-games. [cit. 2025-07-31].

55. IT-SLOVNÍK. Co znamená zkratka DRM? Zdroj: https://it-slovnik.cz/pojem/drm/?utm_source=cp&utm_medium=link&utm_campaign=cp/?utm_source=cp&utm_medium=link&utm_campaign=cp. Online. In: . B.r. Dostupné z: https://it-slovnik.cz/pojem/drm/?utm_source=cp&utm_medium=link&utm_campaign=cp. [cit. 2025-07-31].

56. JANSA, Lukáš; OTEVŘEL, Petr; ČERMÁK, Jiří; MALIŠ, Petr; HOSTAŠ, Petr et al. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4, s. 334.

57. JANZOVÁ, Adéla. Autorská práva k software. Online. In: Právo21. 2023. Dostupné z: https://pravo21.cz/pravo/autorska-prava-k-software. [cit. 2025-07-31].

58. JINDAL, Manish. How Does Software Piracy Affect Economy? – Brief Guide. Online. In: Bytescare. 2024. Dostupné z: https://bytescare.com/blog/how-does-software-piracy-affect-economy. [cit. 2025-04-29].

59. Kazaa končí s nelegálním sdílením a platí pokutu. Online. In: SEZNAM. Novinky.cz. 2006. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-kazaa-konci-s-nelegalnim-sdilenim-a-plati-pokutu-40123874. [cit. 2025-07-17].

60. KELION, Leo. Pirate our games, don't buy them from key resellers, say indies. Online. In: BBC. 2019. Dostupné z: https://www.bbc.com/news/technology-48908726. [cit. 2025-04-29].

61. KESSLER, Ana. Testing Reveals Games with Denuvo Launch Up to Four Times Slower. Online. In: 80LV. 2023. Dostupné z: https://80.lv/articles/testing-reveals-games-with-denuvo-launch-up-to-four-times-slower/. [cit. 2025-04-29].

62. JUDD, Charles. The Onion Router. Online. In: Kevin Wallace training, LLC. 2018. Dostupné z: https://www.kwtrain.com/blog/the-onion-router. [cit. 2025-07-31].

63. KIM, Antino; LAHIRI, Atanu a DEY, Debabrata. The "Invisible Hand" of Piracy: An Economic Analysis of the Information-Goods Supply Chain. Online. MIS Quarterly. 2018, roč. 42, č. 4, s. 1117-1141. ISSN 02767783. Dostupné z: https://doi.org/10.25300/MISQ/2018/14798. [cit. 2025-04-29].

64. KOPECKÝ, Kamil. Co je to DoS a DDoS?. E-Bezpečí, roč. 8 (2023), č. 1, s. 40-42. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=3172

65. KOSINSKI, Matthew. What is hacking? Online. In: IBM. IBM. 2024. Dostupné z: https://www.ibm.com/think/topics/cyber-hacking. [cit. 2025-07-31].

66. LEGOUT, Arnaud, URVOY-KELLER, Guillaume a MICHIARDI, Pietro. UNDERSTANDING BITTORRENT: AN EXPERIMENTAL PERSPECTIVE: Technická zpráva. ⟨inria-00000156v3⟩. 2005.

67. MARCO. The Pros and Cons of Subscription Based Software. Online. In: Marco. 2024. Dostupné z: https://www.marconet.com/blog/the-pros-cons-of-subscription-based-software. [cit. 2025-04-30].

68. MAXIMUM PC, The Dark Art of Game Backups. MAXIMUM PC. 2001, vol. 4., no. 1, s. 62. ISSN 1522-4279.

69. MICROSOFT. Co je nového v Office 2024. Online. In: MICROSOFT. Microsoft. B. r. Dostupné z: https://www.microsoft.com/cs-cz/microsoft-365/get-started-with-office-2024. [cit. 2025-07-07].

70. MICROSOFT. Microsoft Services Agreement. Online. In: MICROSOFT. Microsoft. 2024. Dostupné z: https://www.microsoft.com/en/servicesagreement#serviceslist. [cit. 2025-04-29].

71. MITTAL, Raman. Journal of Intellectual Property Rights. Online. 2004, roč. 2004, č. 9. CSIR-National Institute of Science Communication and Policy Research (NIScPR), 2004. ISSN 0975-1076. [cit. 2025-07-17].

72. MOBYGAMES, MLS LaserLock International. Online. In: MobyGames. 1999. Dostupné z: https://www.mobygames.com/company/42306/mls-laserlock-international/. [cit. 2025-04-21].

73. MURPHY, Pat; KLAGES, Ellen; SHORE, Linda; GORSKI, Jason a (ORGANIZATION), Exploratorium. The Science Explorer Out and about: Fantastic Science Experiments Your Family Can Do Anywhere!. Owl Books, 1997. ISBN 0-8050-4537-6.

74. NEWMAN, Lily. Security News This Week: A Creative Trick Makes ChatGPT Spit Out Bomb-Making Instructions. Online. In: CONDÉ NAST. Wired. 2024. Dostupné z: https://www.wired.com/story/chatgpt-jailbreak-homemade-bomb-instructions/. [cit. 2025-07-07].

75. OMAR, Zakariye a IBRAHIM, Jamaluddin. ISSN 2348-1196. International Journal of Computer Science and Information Technology Research. 2020, vol. 8., no. 3, s. 110-116. ISSN ISSN 2348-1196.

76. ONSIST. Artificial intelligence and online piracy. Online. In: ONSIST. Onsist. 2023. Dostupné z: https://www.onsist.com/blog/artificial-intelligence-and-online-piracy/. [cit. 2025-07-07].

77. PADAPULOS, John. Square Enix has removed Denuvo from Final Fantasy 16. Online. In: DSOG. 2025. Dostupné z: https://www.dsogaming.com/news/square-enix-has-removed-denuvo-from-final-fantasy-16/. [cit. 2025-04-29].

78. PAPP, Donald. COPY PROTECTION IN THE 80S, SHOWCASED BY CLASSIC GAME DUNGEON MASTER. Online. In: Hackday. 2019. Dostupné z: https://hackaday.com/2019/06/25/copy-protection-in-the-80s-showcased-by-classic-game-dungeon-master/. [cit. 2025-03-11].

79. PATALA, Arsi. You should support indies if you can. Online. In: X. X. 2024. Dostupné z: https://x.com/HakitaDev/status/1797245014268891236?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1797245014268891236%7Ctwgr%5E336bb6b408604debdd0b286769c9884efc232872%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.pcgamer.com%2Fgaming-industry%2Fultrakill-dev-says-its-fine-to-pirate-his-game-if-you-dont-have-money-to-spare-culture-shouldnt-exist-only-for-those-who-can-afford-it%2F. [cit. 2025-07-10].

80. PAUL EVE, Martin. Warez: The Infrastructure and Aesthetics of Piracy. Online. Punctum books, 2021. ISBN 9781685710378. Dostupné z: https://doi.org/10.53288/0339.1.00. [cit. 2023-08-28].

81. PCGAMINGWIKI, SecuROM. Online. In: Pcgamingwiki. 2012. Dostupné z: https://www.pcgamingwiki.com/wiki/SecuROM. [cit. 2025-04-21].

82. PETERKA, Jiří. Bulletin Board Systems - BBS. Online. Computerworld. 1991, č. 52/91, s. 1. Dostupné z: eArchiv, https://www.earchiv.cz/a91/a152c110.php3#. [cit. 2024-05-22].

83. PRICE CHARTING. Pokemon Emerald GameBoy Advance. Online. In: Price Charting. 2025. Dostupné z: https://www.pricecharting.com/game/gameboy-advance/pokemon-emerald#completed-auctions-cib. [cit. 2025-04-29].

84. RAHMATALLAH, Darim. What is Account-Based Licensing? Online. In: Thales. B.r. Dostupné z: https://cpl.thalesgroup.com/software-monetization/account-based-licensing. [cit. 2025-07-31].

85. REDPOINTS. Stop digital piracy at scale. Online. In: REDPOINTS. RedPoints. B. r. Dostupné z: https://www.redpoints.com/solution-piracy/. [cit. 2025-07-07].

86. RETRO DREAMS. Copy Protection in the 1980s | Retro Dreams. Online. In: GOOGLE. YouTube. 2022. Dostupné z: https://www.youtube.com/watch?v=VQ6uz6nJcfI. [cit. 2025-04-29].

87. REVENERA. Software Piracy. Online. In: Revenera. B.r. Dostupné z: https://www.revenera.com/software-monetization/glossary/software-piracy. [cit. 2025-07-31].

88. RHAYADER COMPUTERS. Dial a pirate. Online. In: Rhayader computers. B.r. Dostupné z: https://www.rhayadercomputers.co.uk/details/p4866955_20728399.aspx. [cit. 2025-08-01].

89. ROWNTREE, Dave. EXPLORING PC FLOPPY PROTECTION: FORMASTER COPY-LOCK. Online. In: HACKADAY. 2024/08/27. Dostupné z: https://hackaday.com/2024/08/27/exploring-pc-floppy-protection-formaster-copy-lock. [cit. 2025-03-04].

90. SAD_SYSTEM_3314. Microsoft Lets Hackers Steal Accounts Permanently – No Recovery for the Original Owner. Online. In: Reddit. 2025. Dostupné z: https://www.reddit.com/r/LinusTechTips/comments/1ieo3dx/microsoft_lets_hackers_steal_accounts_permanently/. [cit. 2025-04-29].

91. SANGFOR TECHNOLOGIES, Shareware: Definition, History, and Its Impact on Software Distribution. Online. In: Sangfor. 2024, 3.12.2024. Dostupné z:

https://www.sangfor.com/glossary/cybersecurity/shareware-definition#:~:text=History%20of%20Shareware,the%20honor%20system%20for%20payment.. [cit. 2025-04-14].

92. SCOTT, Jason, BBS The Documentary [Episode 2 of 8: SYSOPS AND USERS]. U.S.: Jason Scott, 2005. Délka 44 min. [cit. 2025-04-07].
93. SCOTT, Jason, BBS The Documentary [Episode 6 of 8: HPAC]. U.S.: Jason Scott, 2005. Délka 38 min. [cit. 2025-04-07].
94. SKETCH. Pricing: b. r. Online. In: SKETCH B.V. Sketch. C2025. Dostupné z: https://www.sketch.com/pricing/. [cit. 2025-07-07].
95. SKLYAROV, Dmitry. Hidden Keys to Software Break-Ins and Unauthorized. USA: БХВ-Петербург, 2003. ISBN 1931769303.
96. SMITH Donnie, 10 Hilarious Examples Of Anti-Piracy Measures In Video Games. Online. In: Screenrant. 2022. Dostupné z: https://screenrant.com/anti-piracy-video-games-funny/. [cit. 2025-04-15].
97. STANFORD UNIVERSITY. Copyright Protection: Techniques. Online. In: Stanford. B. r. Dostupné z: https://cs.stanford.edu/people/eroberts/cs181/projects/software-piracy/copyright.html. [cit. 2025-04-29].
98. STARFORCE. Optical disc protection. CD and DVD protection. Online. In: Star-force. C2000-2025. Dostupné z: https://www.star-force.com/solutions/optical-disc-protection/. [cit. 2025-04-29].
99. STARMEN.NET, EarthBound Anti-Piracy Measures. Online. In: Starmen.net. B. r. Dostupné z: https://starmen.net/mother2/gameinfo/antipiracy/. [cit. 2025-04-15].
100. THE GAME AWARDS. 2023. Online. In: The game Awards. 2023. Dostupné z: https://thegameawards.com/rewind/year-2023. [cit. 2025-04-29].
101. ULTIMATE POP CULTURE WIKI. Always-on DRM. Online. In: FANDOM. Ultimate Pop Culture Wiki. 2019. Dostupné z: https://ultimatepopculture.fandom.com/wiki/Always-on_DRM. [cit. 2025-04-29].
102. UXNESS. The Phasing Out of Adobe XD: What You Need to Know in 2025. Online. In: UXNESS. C2025. Dostupné z: https://www.uxness.in/2024/07/the-phasing-out-of-adobe-xd-2-24.html. [cit. 2025-04-29].

103. VMPROTECT SOFTWARE. VMProtect. Online. In: VMProtect Software. B.r. Dostupné z: https://vmpsoft.com/vmprotect/overview. [cit. 2025-07-31].

104. VOLLE, Adam. Dark web. Online. In: Britanica. 2025. Dostupné z: https://www.britannica.com/technology/dark-web. [cit. 2025-07-17].

105. WHITEKNIGHT35. My accounts have been hacked - Trojan/Malware/Worm. Online. In: Malwarebytes. 2024. Dostupné z: https://forums.malwarebytes.com/topic/312994-my-accounts-have-been-hacked-trojanmalwareworm/. [cit. 2025-04-29].

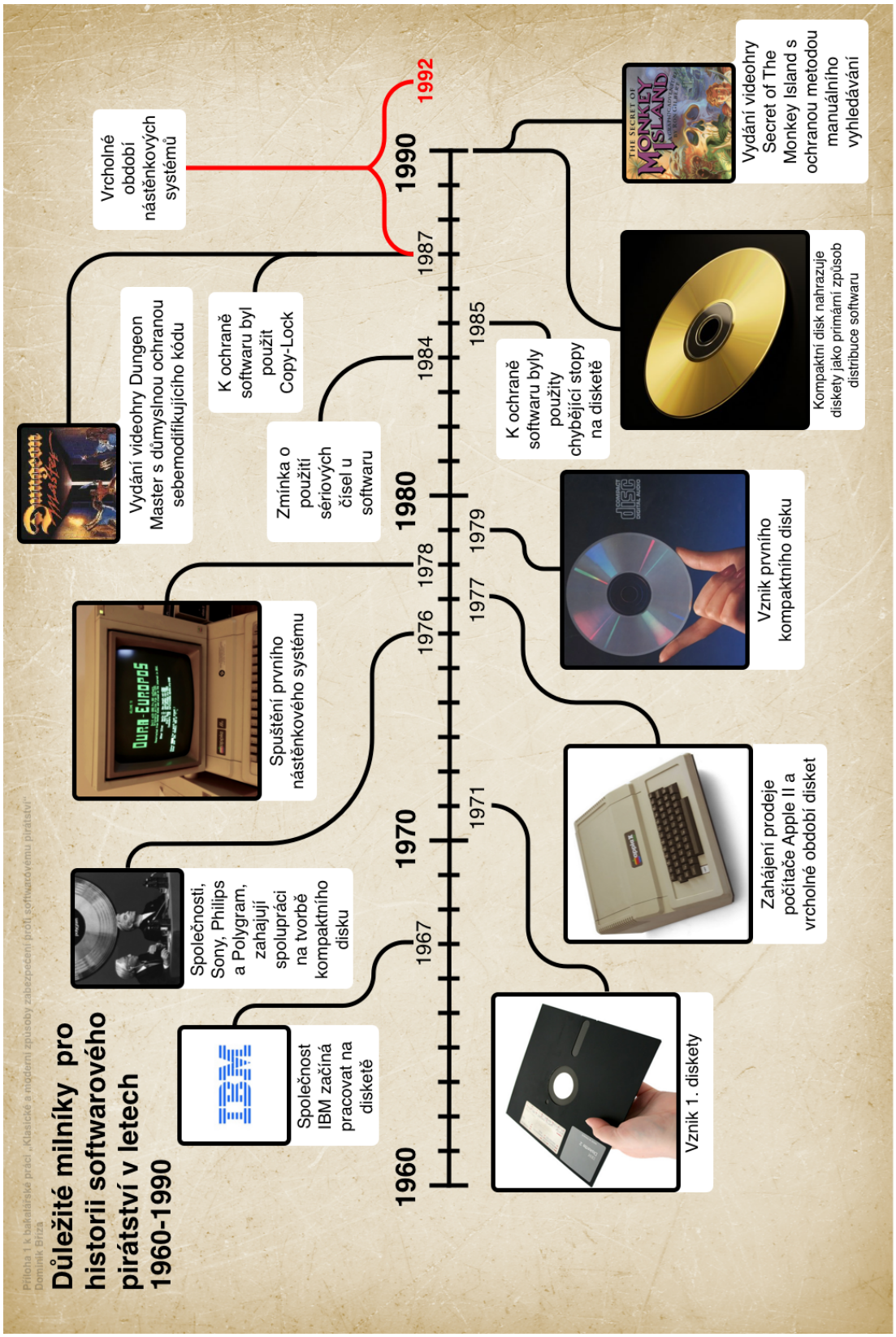
106. WILDE, Tyler a SAYER, Matt. The 19-year evolution of Steam. Online. In: PCgamer. 2022. Dostupné z: https://www.pcgamer.com/steam-versions/. [cit. 2025-07-31].

107. XIAOSONG, Lou a HWANG, Kai. Proactive Content Poisoning To Prevent Collusive Piracy in P2P File Sharing. Online. Dostupné z: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=78295c13354b74b42224a0d28edafb57bde97888. [cit. 2025-04-30].

108. YOON, Olivia. Always Online DRM and Video Games. Online. In: Cardozoaelj. 2021. Dostupné z: https://cardozoaelj.com/2021/09/27/always-online-drm-and-video-games/. [cit. 2025-07-31].

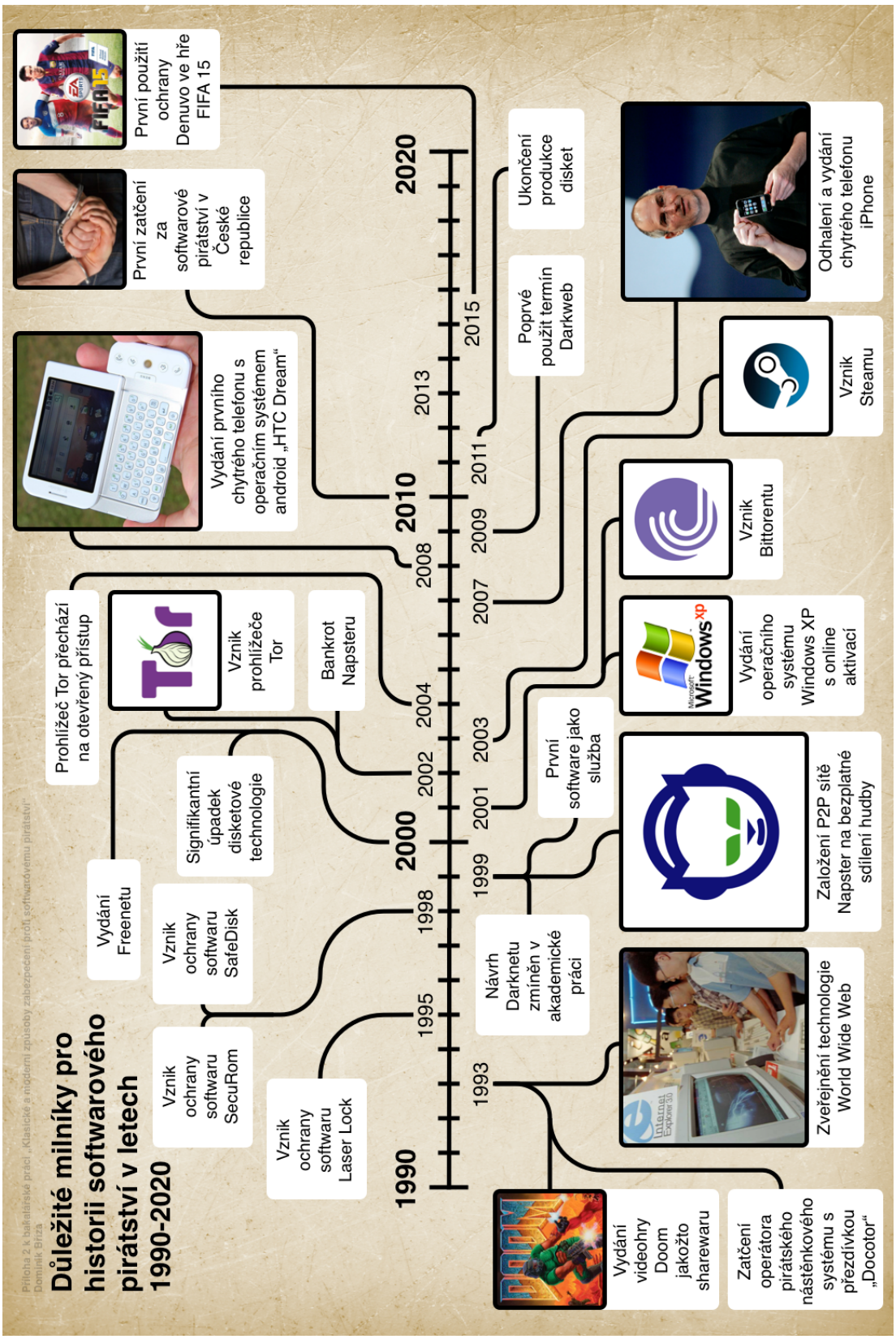
Seznam příloh

PŘÍLOHA 1: Vývoj softwarového pirátství v letech 1960-1990



Příloha 1 Vývoj softwarového pirátství mezi lety 1960-1990 (vlastní zdroj)

PŘÍLOHA 2: Vývoj softwarového pirátství v letech 1990-2020



Příloha 2 Vývoj softwarového pirátství mezi lety 1990-2020 (vlastní zdroj)