Univerzita Pardubice

Fakulta ekonomicko-správní

Počítačová kriminalita

Michaela Pšeničková

Bakalářská práce
2016

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michaela Pšeničková**
Osobní číslo:	**E13751**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Počítačová kriminalita**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce bude pomocí metod shlukové analýzy provést komparaci vybraných zemí v oblasti počítačové kriminality na základě dostupných parametrů. Výsledky budou patřičně vizualizovány.
Osnova:
- Úvod do počítačové kriminality.
- Druhy počítačové kriminality.
- Shluková analýza.
- Komparace vybraných zemí v oblasti počítačové kriminality na základě dostupných parametrů.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.
JIROVSKÝ, Václav. Kybernetická kriminalita. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
MATĚJKA, Michal. Počítačová kriminalita. Praha: Computer Press, 2002. ISBN 80-7226-419-2.
ŘEZANKOVÁ, Hana, Dušan HÚSEK a Václav SNÁŠEL. Shluková analýza dat. 2. vyd. Praha: Professional Publishing, 2009. ISBN 978-80-8694-681-8.

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **29. září 2015**
Termín odevzdání bakalářské práce: **29. dubna 2016**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 29. září 2015

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, 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.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 29. 4. 2016 Michaela Pšeničková

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala své vedoucí práce, Ing. Renátě Máchové, Ph.D., za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato práce bude sloužit studentům pro pochopení oblasti počítačové kriminality. Zabývá se jejím vymezením, dělením a konkrétními formami počítačové kriminality. Poukáže na složitost tohoto tématu a přiblíží jeden z možných způsobů hodnocení počítačové kriminality pomocí vybraných parametrů.

KLÍČOVÁ SLOVA

Počítačová kriminalita, shluková analýza, analýza, dendrogram

TITLE

Cyber crime

ANNOTATION

This bachelor thesis will help students to understand a phenomena of cyber crime. It deals with its definition, partition and particular forms of cyber crime. It points out a complexity of the topic and specifies one of the possible ways of rating cyber crime by selected parameters.

KEYWORDS

Cybercrime, cluster analysis, analysis, dendrogram.

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

BBS	Bulletin Board System
BÚ	Běžný účet
CD	Compact Disc
CPCC	Cophenetic Correlation Coefficient
	Kofenetický korelační koeficient
DoS	Denial of Service
ENIAC	Electronic Numerical Integrator And Computer
HDP	Hrubý domácí produkt
HNP	Hrubý národní produkt
IBM	International Business Machines Corporation
IC3	Internet Crime Complain Center
IP	Internet Protocol
LICRA	Ligue Internationale Centre le Racisme et l´Antisémitisme
	Mezinárodní liga proti rasismu a antisemitismu
OSN	Organizace spojených národů
P2P	Peer-To-Peer
PC	Personal Computer
PDA	Personal Digital Assistant
PDF	Portable Document Format
PHP	Hypertext Preprocessor
	Hypertextový preprocesor
RIAA	Recording Industry Association of America
	Asociace amerického nahrávacího průmyslu
SW	Software
WWW	World Wide Web

ÚVOD

S lehkou nadsázkou je možné říci, že základem dnešní společnosti, ale také ekonomiky, jsou informační technologie a jejich vzájemné propojení do sítí. Jedním z rysů současnosti, je jejich velmi rychlý vývoj a s tím související vývoj počítačové kriminality. Dnes existuje mnoho publikací věnujících se tomuto tématu.

Pod pojmem počítačová kriminalita si lze představit mnoho aktivit, jako například útok zaměřený na zničení počítače, dat, útok zaměřený na zneužití dat nebo porušení autorských práv apod. Přesněji vymezit počítačovou kriminalitu není snadné. Pod nejobecnější definicí si lze představit každou „nečestnou“ činnost páchanou pomocí počítače. Toto vymezení je ale příliš široké. Lze si pod ním vybavit i manipulaci s daty na úřadech, ve firmách či jiných institucích, což je možná důvodem, proč je v mnoha zemích počítačová kriminalita zahrnována do hospodářské kriminality a neexistují o ní samostatné statistické údaje.

Toto téma bylo zvoleno, neboť se počítačová kriminalita týká celé společnosti. Počítač lze v dnešní době nalézt v každé domácnosti, organizaci, zkrátka je využíván téměř v každé oblasti lidské činnosti. Faktorů, které ovlivňují počítačovou kriminalitu, je možné nalézt mnoho, záleží však na formě počítačové kriminality. Měla by se tedy věnovat větší pozornost, vzdělávání v této oblasti. V této práci se pokusím o stručnou charakteristiku počítačové kriminality a jejích možných forem.

Hlavní body, kterým se tato práce bude věnovat, jsou úvod do počítačové kriminality, vymezení jejích nejběžnějších forem, dále úvod do shlukové analýzy a nakonec komparace vybraných zemí v oblasti počítačové kriminality na základě dostupných parametrů.

Cílem práce je pomocí metod shlukové analýzy provést komparaci vybraných zemí v oblasti počítačové kriminality na základě dostupných parametrů. Výsledky budou patřičně vizualizovány.

1 POČÍTAČOVÁ KRIMINALITA

Počítačovou kriminalitou lze rozumět takovou činnost, kterou je porušován zákon, nebo je v rozporu s morálními pravidly společnosti. Jde o skupinu společensky nebezpečných jednání páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení, databází a výpočetní techniky.[15][19]

Pod pojmem počítačová kriminalita si lze představit činnost, ve které určitým způsobem figuruje počítač, jako souhrn teoretického a programového vybavení (včetně dat, komponent) nebo i větší množství počítačů, v těchto formách[15]:

a) počítač, jako předmět trestné činnosti,

b) počítač, jako nástroj trestné činnosti.

1.1 Příčiny vzniku

Mezi základní kriminogenní faktory, které přispěly ke vzniku počítačové kriminality, nebo ji usnadňují, patří tyto[29]:

- složitost informačních technologií,
- důvěra uživatelů ve výstupy z informačních technologií,
- objem dat,
- páchání trestné činnosti „od obrazovky“ je snazší než v reálném životě,
- nízké právní vědomí populace,
- nedokonalost legislativy.

1.2 Netiketa

Netiketa, neboli správné chování na internetu jsou podobně jako etiketa nepsaná pravidla chování, která rozhodně nejsou povinná. Užíváním těchto doporučení vypovídá o nás, jako o uživatelích internetu.[2][14]

Mezi tyto pravidla patří[14]:

- chovejte se tak, abyste nepoškozovali ostatní uživatele,
- neomezujte ostatní při jejich vlastní práci na síti,
- nenahlížejte do souborů ostatních uživatelů,

- nevyužívejte počítače ke krádežím,
- nevyužívejte síť ke zveřejnění falešných údajů, falešného svědectví,
- nevyužívejte ani si nekopírujte software, za který jste nezaplatili,
- nevyužívejte zdroje ostatních uživatelů bez autorizace,
- nepřisvojujte si duševní bohatství ostatních,
- uvažujte o společenských důsledcích programu, který tvoříte,
- používejte počítač s úctou, s respektem a ohleduplně.

2 HISTORIE POČÍTAČOVÉ KRIMINALITY

Jak se může zdát, počítačová kriminalita vznikla společně se vznikem počítačů, opak je ale pravdou. K opravdovému rozmachu počítačové kriminality však došlo až ke konci 20. století, po rozšíření PC mezi uživatele. V rozvoji počítačové kriminality lze sledovat určitá vývojová stádia, která zpravidla odpovídají i vývoji počítačových technologií[23]:

- období od vynálezu telefonů, po uvedení prvního PC na trh lze nazvat ***pravěk***,
- období od roku 1981 po případ Citibank v roce 1994 lze nazvat ***středověk***,
- období od roku 1994 po současnost lze označit jako ***novověk***.

2.1 Pravěk

Za první „počítačový" zločin je považován případ z roku 1801, kdy ve Francii tkadlec Jacquard sestrojil jednoduchý tkalcovský stav s automatizací některých kroků. Ale zaměstnanci jeho manufaktury se báli, že kvůli přístroji ztratí svá pracovní místa a pomocí stávek byl Jacquard od vývoje dalšího tkalcovského stavu odrazen.[29][23]

S pozvolným vývojem komunikačních technologií docházelo k sériím nevinných žertíků ze strany obsluhy telefonních ústředen. Pracovníci hovory cíleně přerušovali a spojovali dva k sobě nepatřící.[23]

K velkému posunu došlo v roce 1946, konkrétně 14. února. Na pennsylvánské univerzitě byl sestrojen první elektronický počítač, nazvaný ENIAC. Počítače, jako ENIAC a jeho nástupci však ještě zabírali celou místnost. Vzhledem k jejich nákladovosti, je vlastnily pouze velké firmy, nelze tedy ještě mluvit o jejich kriminálním využití.[23]

Programátoři si při práci s těmito počítači museli umět poradit s mnohdy zcela nedokonalými programy. Bylo nutné tyto programy doupravit svépomocí. Zásahy do programu, které měly zefektivnit jejich funkci a programy tak mohly být lépe využívány, se nazývaly *„hack"*. Jejich zásahy je však nutné chápat jako pozitivní, ne jako v dnešním slova smyslu.[23]

Dalším důležitým momentem byl rok 1971, který proslul případem *Cap 'n' Crunch*. Jméno případu je stejné, jako cereálie, do kterých se přidávala hračka v podobě píšťalky. Veterán Jonh Draper zjistil, že tato píšťalka vydává zvuk o frekvenci 2600 Hz. S využitím zvuku o této frekvenci lze v telefonní lince uskutečňovat hovory zdarma. Po zveřejnění toho triku se rozmohla telefonie, která dostala název *„phreaking"*.[23][42]

2.2 Středověk

V 80. letech, konkrétně 12. 8. 1981, uvedla společnost IBM svůj první počítač typu IBM PC. Umožnila tak, aby se počítač stal dostupný obyčejným domácnostem. V souvislosti právě s těmito počítači došlo ke slučování telefonních linek a počítačů prostřednictvím modemů. Vzniklé sítě lze považovat za předchůdce dnešního internetu v podobě systémů Bulletin Board System (BBS).[23]

V tomto období se díky vzniklým filmům, hackerským časopisům a hrám rozrůstalo množství fandů. Tyto publikace mnohdy až neuváženě zveřejňovaly návody, jak se zdokonalit v oblasti phreakingu, jak získat číslo cizí kreditní karty a další aktivity. Nejprve šlo jen o fandy, kteří si chtěli dokázat, že sami proniknou do systému. Později však tyto činnosti směřovaly pouze k vlastnímu obohacení a poškození druhých.[23]

Pro toto období je také příznačný vznik prvních virů. První virus pravděpodobně vytvořila v roce 1986 Pákistánská softwarová firma, aby jim pomáhala chránit programy, které vyvinula. Virus nazvala *„Brain“* a šířila ho mezi uživateli prostřednictvím diskety. K jeho spuštění došlo po vložení diskety do PC.[23][22][42]

V roce 1988 se nechvalně zapsal do dějin počítačové kriminality Kevin Mitnick, když zaútočil na počítač společnosti Equipment Digital. Dostal se tak na seznam FBI „Most Wanted“. Dalším známým hackerem je Robert Morris, který v roce 1988 vypustil rychle se šířícího červa, který se vymkl kontrole a napadl přes 6000 počítačů. V neposlední řadě je nutné zmínit i Kevina Poulsena. Ten se roku 1993 naboural do telefonních linek kalifornské rozhlasové stanice, aby vyhrál automobil značky Porsche.[15][23][42]

Dalším milníkem tohoto období je vznik kompatibilního disku, tedy CD. Tento disk napomohl vzniku nové oblasti počítačové kriminality, *počítačovému pirátství*. CD se nejprve používalo v oblasti hudebních nahrávek, vcelku rychle se ale začalo používat k uchovávání dat. K tomuto účelu byla vytvořena mechanika CD-ROM, která se používala ke čtení CD. Zařízení pro digitální záznam bylo zpočátku velmi drahé, ke změně došlo v 90. letech. Na trh se dostala mechanika CD-R. Ta uměla zaznamenávat, neboli vypalovat data na CD.[23]

2.3 Novověk

Období středověku ukončily dva případy. Prvním z nich byl *Orchard Street Finger-Hackers* (1993). Jednalo se o technologicky málo zdatné hackery, kteří prodávali ukradené přístupové kódy pro telefonní spojení. V druhém, známější, případě *Citibank* (1994) ruská

skupina pronikla do systému Citibank a převedla si na své vlastní účty 10 milionů dolarů.[15][23][42]

Pro období novověku je charakteristické masové rozšíření počítačů s operačním systémem Microsoft Windows. S růstem rozšíření počítačů rostl i vývoj software (SW), rozšíření sítí typu internet a grafického prostředí World Wide Web (www). Docházelo k zneužívání hesel pro přístup do vládních počítačů, k první průmyslové špionáži, exponenciálnímu růstu počtu virů, apod.[23]

Novým distribučním kanálem počítačových virů se stala elektronická pošta. Prvním známým virem, který se velmi rychle rozšířil do celého světa, byla *Melissa* (1999). Tento virus se sám rozesílal 50 prvním kontaktům v adresáři. Nešlo o destruktivní virus, ale ukázal, kam až se lze zajít. Dalším takovým případem byl virus *I love you* (2000), který byl skrytý za milostným vzkazem.[23][42]

Novinkou této doby se staly *Denial of Service* (DoS) útoky, nebo také útoky odepření přístupu. Jedním z nejznámějších DoS útoků, byl útok, který postihl v roce 2000 servery eBay, Yahoo, Amazon a další. Rozdíl mezi počítačovými viry a DoS útoky je takový, že DoS útok se nesnaží cílový počítač infikovat, ale zahltit ho sérií opakovaných požadavků.[15][23]

Za další milník lze označit období, kdy vznikl systém pro výměnu hudebních nahrávek, Napster. Byl vyvinut studentem Shawnem Flanningem a otevřel zcela novou problematiku. Do této doby byl internet organizován na principu *klient-server* (tedy uživatel se přihlašoval na server a odtud stahoval potřebná data). Napster fungoval na principu *peer-to-peer* (P2P, uživatel se přihlásil přímo k dalšímu uživateli poskytujícímu obsah). Došlo k obrovskému nárůstu uživatelů, kteří sdíleli až stovky terabajtů dat. Na toto reagovala americká organizace nahrávacích společností RIAA žalobou.[23][42]

V souvislosti s rozšířením počítačové kriminality a s jejím vnímáním se v mnoha zemích začalo diskutovat o možnostech monitorování internetu státními institucemi. Vlády mnoha zemí začaly vytvářet systém, kde by všichni poskytovatelé internetu byli povinni poskytnout státním orgánům monitorování dat a to nejen na základě soudního příkazu. Součástí systému byl také zákaz šifrování dat či jakýkoliv prostředek proti monitorování.[23]

V roce 2000 byl internetový portál Yahoo žalován francouzským soudem za šíření nacistických materiálů. Yahoo soud ve Francii prohrálo. Pobočka francouzské ligy v USA (LICRA) žalovala Yahoo u soudu na výkon rozhodnutí (zamezení přístupu k těmto materiálům). Soud v USA ale shledal, že rozsudek je v rozporu s ústavou USA, konkrétně s dodatkem o svobodě projevu.[23]

O rok později vyvinul ruský pracovník firmy ElconSoft, Dimitrij Skljarov, program, který převáděl elektronické knihy z chráněného formátu Adobe E-Book do nechráněného formátu Portable Document Format (PDF). To je podle ruského práva zcela legální, ale v USA jeto považováno za trestný čin. Po návštěvě konference DefCon v USA byl proto Skljarov zatčen a byl obžalován z toho, že jeho program firma nabízela na internetu, kde se k němu mohli dostat i občané USA a tím byl páchán trestný čin. Zatčení okamžitě vyvolalo protesty v celém světě. Po několika protestech byl Skljarov propuštěn, ale spor proti společnosti stále trvá. Ukončení tohoto sporu bude mít zásadní vliv na trestnost činu na internetu. Pokud soud uzná postup amerických orgánů, bude to znamenat, že trestnost činnosti na internetu se bude posuzovat podle toho, odkud se na obsah dívají uživatelé.[23]

Situace 11. září 2001 ovlivnila i oblast informačních technologií. Mnoho lidí požadovalo bezprostředně po útoku zpřísnění pravidel, zejména co se týče elektronické komunikace. Ukázalo se, že pachatelé dokáží použít takové metody, které jsou neodhalitelné. Proto tyto omezení mají vliv pouze na obyčejné občany, kterým je zasahováno do soukromí.[23]

V roce 2007 pronikla čínská skupina hackerů do počítačové sítě Ministerstva obrany USA. Pentagon tento útok přiznal a potvrdil, že hackeři se dostali k e-mailovým adresám asistentů tehdejšího ministra obrany Roberta Gatese. Čína tento útok dodnes popírá.[3][42]

V roce 2007 se také poprvé objevil tzv. *Zeus botnet*. Ten pracoval na principu, jako phishing- lákal příjemce e-mailové zprávy na kliknutí na odkaz, který infikuje počítač. Jeho cílem bylo okrást majitele o peníze tím, že zachytí jeho stisky na klávesnici při zadávání bankovních údajů. Zloději se zaměřili na malé a střední podniky a podařilo se jim ukrást téměř 70 000 $. Mezinárodní vyšetřování vedlo k zatčení více než 100 osob ve Velké Británii, USA a na Ukrajině.[3]

Při volbě amerického prezidenta v roce 2008 bylo odhaleno, že síť počítačů Obamovy kampaně byla napadena cizí vládou, která odcizila data. Stejně byla napadena také McCainova kampaň. Po zvolení Obamy na post prezidenta byla zveřejněna zpráva, že za tímto útokem se skrývá Čína, která shromažďovala data o těchto dvou politicích.[3]

Dne 12. ledna 2010, Google detekoval na své podnikové síti vysoce sofistikovaný útok, původem v Číně. Cílem byly účty g-mail několika aktivistů za lidská práva. Šetření odhalilo, že bylo poškozeno přinejmenším dalších 20 velkých společností, které tento útok nezaregistrovaly.[3]

V roce 2010 se nový druh červa, *Stuxnet*, zaměřil na software průmyslově řídících počítačů německé firmy Siemens. Jeho infekční schopnosti vedly v Íránu ke spekulacím o národní bezpečnosti. Z vytvoření Stuxnetu byli podezříváni USA a Izrael, kvůli údajné sabotáži íránského jaderného programu.[3]

3 DRUHY POČÍTAČOVÉ KRIMINALITY

Počítačová kriminalita se postupem času rozvíjela, její množství rostlo a vznikla potřeba ji rozdělit. Různí autoři dělí počítačovou kriminalitu různými způsoby a těmto způsobům se budu v této kapitole věnovat.

3.1 Dělení počítačové kriminality

Prof. Smejkal a kol. rozčleňuje počítačovou kriminalitu do dvou základních skupin[19]:

a) delikty, kde počítač, program, data, informační systém apod. jsou nástrojem trestné činnosti pachatele,

b) delikty, kde počítač, program, data, informační systém atd. jsou cílem zločinného útoku, přičemž se může jednat o tyto trestné činy:

- fyzický nebo logický útok na počítač nebo komunikační zařízení,
- neoprávněné užívání počítače nebo komunikačního zařízení,
- neoprávněné užívání nebo distribuci počítačových programů,
- změnu v programech a datech, okrajově i v technickém zapojení počítače nebo komunikačního zařízení,
- neoprávněný přístup k datům, získávání utajovaných informací (tzv. počítačová špionáž) nebo jiných informací o osobách (osobní údaje),
- trestné činy, předmětem jejichž útoku je počítač jako věc movitá.

Rada Evropy dělí počítačovou kriminalitu do čtyř oblastí[19]:

- trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů (neoprávněný přístup, neoprávněné odposlouchávání, narušování dat, narušování systémů, zneužívání zařízení),
- trestné činy se vztahem k počítači (počítačový podvod, padělání počítačem),
- trestné činy se vztahem k obsahu počítače (dětská pornografie),
- trestné činy související s porušováním autorského práva a souvisejících práv.

Podle vzniku lze počítačovou kriminalitu rozdělit do dvou oblastí[23]:

- tradiční počítačová kriminalita,

– nová počítačová kriminalita.

3.2 Formy počítačové kriminality

Počítačovou kriminalitu tedy lze rozdělit na[23]:

1 tradiční počítačovou kriminalitu,

2 novou počítačovou kriminalitu.

Tyto dále rozdělím na protiprávní jednání proti počítači a protiprávní jednání s využitím počítače.

3.2.1 Tradiční protiprávní jednání proti počítači

Tradiční jednání, které lze považovat za počítačovou kriminalitu. Oblasti počítačové kriminality se dotýká pouze okrajově.

- *Průmyslová špionáž*

Jedná se o průnik do systému konkurence a využití jejich dat. K tomu se využívají různé hackerské útoky nebo infikování hostitelského počítače virem. Účelem je získání důvěryhodných informací z hostitelského počítače.[23]

- *Krádež a loupež*

O krádeži lze mluvit, dojde-li k odcizení počítače. Nemusí dojít pouze k odcizení počítače samého, ale také jeho součástí, záznamových médií a dalších příslušenství.[23]

O loupež se jedná tehdy, bude-li například při přepadení odcizen notebook nebo jiný předmět.[23]

- *Zpronevěra*

Zpronevěrou lze nazvat například, když zaměstnanec podniku po rozvázání pracovní smlouvy neodevzdá veškerou výpočetní techniku zapůjčenou zaměstnavatelem. Mnohem větší význam má však zpronevěra u protiprávního jednání s využitím počítače.[23]

3.2.2 Tradiční protiprávní jednání s využitím počítače

Jedná se o tradiční jednání, které společně s novými informačními technologiemi nabyly nových forem.[23]

- *Podvody*

Na internetu se vyskytuje mnoho podvodných e-shopů, pachatelé se snaží vylákat peníze z lidí pomocí neexistujících služeb, především v souvislosti s pornografickými stránkami. Obchodníci se se svými podvodnými stránkami pohybují zejména na freewebech a snaží se nalákat oběti na příslib velkého zisku na obchodech s komoditami, cennými papíry apod.[23]

Jedním druhem internetového podvodu je *phishing*. Jedná se o vylákání přístupových údajů k účtům z uživatelů internetového bankovnictví pro své vlastní obohacení.[12]

K získání těchto údajů využívají zejména podvodné e-maily, které vypadají, že jsou odeslány přímo z banky. Pokud uživatelé tento e-mail otevřou a dostanou se na podvodnou odkazovanou stránku, kde jsou po něm požadovány přístupové údaje k účtu, údaje o platební kartě či jiné důvěrné informace. Pokud uživatel tyto informace vyplní, získají data podvodníci, kteří je následně využijí ve svůj prospěch.[12]

- *Padělání a penězokazectví*

Už odedávna se padělalo cokoliv, co mohlo padělateli přinést nějaký prospěch. Zatímco dříve bylo potřeba nejzručnějších kreslířů a rytců, dnes je padělání otázkou ovládání softwaru a investice do kvalitního tisku. Dnešní grafické programy a nejmodernější laserové a sublimační tiskárny dokáží doslova zázraky. Vše potom zůstává otázkou správného druhu papíru. Ochranné prvky peněz proto procházejí neustálým vývojem, aby odolaly zdokonalujícím se padělatelům.[23][27][6]

Nejde pouze o padělání peněz, ale také o padělání a pozměňování známek, padělání a pozměňování nálepek k označení zboží nebo předmětů dokazujících plnění poplatkové povinnosti, padělání a pozměňování veřejných listin, padělání občanských průkazů, cestovních dokladů a dalších.[23][6]

- *Útoky na čest a pověst, elektronická msta, pomluvy*

Sociální sítě jsou dnes velkým fenoménem a je velice obtížné najít někoho, kdo zůstal bez profilu na některé z nich. Lidé tyto sítě využívají při pořádání společenských akcí, různých srazů apod. Ke svému profilu mají připojeny jen své „přátele“ a domnívají se, že když něco prostřednictvím těchto sítí (Facebook, Twitter,…) sdílí, zjistí to jen jejich kamarádi. Sociální sítě tedy vytvářejí dojem, že je možné říci cokoliv komukoliv a nikdo jiný kromě okruhu jejich známých se o tom nedozví.[22]

Šíření pomluv dostalo v elektronické podobě mnohem větší rozměr. Tuto činnost může páchat každý s přístupem k internetu. Jedním způsobem páchání takového činu je zanesení osobních údajů do různých seznamek. Oběť je potom po určitou dobu obtěžována nepříjemnými telefonáty a návštěvami v místě bydliště. Dalším způsobem může být rozšiřování nepravdivých informací o oběti po internetu.[23]

- *Vydírání, elektronické výpalné*

Majitelé systémů připojených k internetu jsou zastrašováni zničením systému, zničením dat a v neposlední řadě jejich zneužitím. Jelikož žádný systém nemá 100% zabezpečení, mnohé firmy elektronické výplatné zaplatí. Tento způsob vydírání je velice nebezpečný a předpokládá se jeho další vývoj.[23]

V dnešní době se rozšiřuje tzv. *Ransomware*. Jedná se o škodlivý kód, který se zabydlí v počítači, zašifruje uložená data a po uživateli požaduje výkupné. Útočníci se snaží v majiteli napadeného stroje vzbudit dojem, že se k zašifrovaným datům dostane po zaplacení pokuty. Ta byla údajně vyměřena například za používání nelegálního softwaru. Ani po zaplacení výkupného však uživatelé nemají jistotu, že se ke svým datům doopravdy dostanou.[26]

- *Šíření pornografie*

Šíření pornografie je vedle hackingu a warezu tou nejrozšířenější nelegální aktivitou v souvislosti s počítači. Ještě v dobách před internetem se pornografie šířila jen díky časopisům, které se předávaly spíše „z ruky do ruky“ nebo na černém trhu, později díky videokazetám, rozšiřovaným tím samým způsobem. Dnes si však s tímto konzumenti nemusejí dělat starosti. Šíření pornografie je v mnoha státech nelegální, to však přináší problém v souvislosti s celosvětovou přístupností internetu. Obsah pornografických stránek je viditelný i ve státech, kde je šíření pornografie trestnou činností. Právo zatím tento problém velice dobře neřeší.[23]

- *Extremismus na Internetu*

Internet je ideálním místem pro aktivity extremistických skupin[1]. Na internetu nalezneme nespočet webových stránek s tématikou Ku-Klux-Klanu apod. Po vzniku internetu se komunikace těchto nelegálních skupin velice ulehčila. U extremismu vždy platí, že odpovědnost za něj nese autor, jeho dohledání je ale vzhledem k jejich

[1] *„Jako extremismus lze označit vyhraněné jednání či ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance a útočí proti základním demokratickým ústavním principům, které jsou definovány například v českém ústavním pořádku.“[5]*

šikovnosti a možnosti přesměrování internetového protokolu (IP adresy) velice složité. Problémem při odhalování extremismu je i fakt, že velkou část materiálů obsahují webové stránky, jejichž poskytovatelé nesídlí na území státu, kde je šíření těchto materiálů nelegální. Orgány příslušného státu se pak musí obrátit na úřady státu, kde autor sídlí. Častým problémem ale zůstává, že legislativa daného státu problematiku chápe jinak.[23][5]

- *Hoaxes a fámy*

Jedním z možných nebezpečí na internetu je šíření nepravdivých poplašných řetězových zpráv, hoaxů. Důvěryhodně napsaná zpráva dokáže ovlivnit chování mnoha lidí. Hoax se snaží vzbudit u čtenáře důvěru, přimět ho k tomu, aby zprávu rozeslal všem známým i neznámým lidem, na které má kontakt. Hoax se tak dále šíří světem. Díky internetu opět došlo k masovému rozšíření těchto zpráv. Jako příklad mohu uvést varování před počítačovými viry, varování před nastrčenými infikovanými injekčními stříkačkami, varování před koncem světa apod.[23][1][13]

3.2.3 Nová protiprávní jednání proti počítači

- *Hacking*

Jinak také průnik do systému nestandardní cestou. V počátku se jednalo o zjištění, jak systém funguje a následné odstranění chyb. Dnes se jedná o zneužití a poškození záznamu na nosiči informací. Hacking provádí hacker, který si vytváří vlastní programy nebo speciální PHP skripty, které mu slouží k prolomení funkčnosti zabezpečení systému.[15][23][25]

- *Carding*

Zneužívání platebních karet. Platební karta se stala převažujícím platebním nástrojem a má mnohdy nedostačující zabezpečení. Ke zneužití může dojít několika způsoby. Jedním z nich je krádež čísla platební karty, nebo krádež karty přímo.[23]

Dalším způsobem je využití metody *sociálního inženýrství*. Tyto metody spolu s phreakingem využíval americký hacker Fry Guy, když zneužíval úvěrové družstvo Western Union. Ta poskytovala vybírání hotovosti z účtu pomocí telefonních služeb. S pomocí získaných informací právě metodou sociálního inženýrství kontaktoval pobočku a požádal o vybrání peněz z účtu. Tato služba však vyžadovala opětovné zavolání na číslo klienta a potvrzení transakce. Fry Guy tento hovor přesměroval pomocí nabourání se do telefonní ústředny na jemu vybranou telefonní budku.[23]

Pachatelé cadringu získávají osobní údaje majitelů účtů různými způsoby, například se vydávají za pracovníky banky, prohledávají odpadky a hledají vyhozené výpisy z bankovních účtů apod. Postupem času se tyto techniky stále zlepšují a vyvíjejí. Jde například o nainstalování kamery do bankomatu nebo nainstalování celého falešného bankomatu, který funguje jako čtečka informací na kartě.[23]

- *Krádeže, ničení dat a zneužití osobních údajů*

V tomto případě se jedná o zjištění osobních údajů, dat, které se pachatel chystá využít k poškození této osoby, nebo k vlastnímu prospěchu. Jako příklad lze uvést zneužití osobních údajů k vydírání, obtěžování či šíření pomluv. Jako trestný čin se považuje i jakákoliv manipulace s těmito informacemi- zničení, vymazání, formátování, apod.[23]

3.2.4 Nová protiprávní jednání s využitím počítače

Jedná se o zcela nové činy, které vznikly s nástupem vyvíjejících se informačních technologií.[23]

- *Spamming*

Pod pojmem spamming si lze představit zasílání nevyžádané elektronické pošty, která se hromadně šíří internetem. Spam může obsahovat reklamu, počítačový vir, trojského koně apod. Spammeři získávají elektronické adresy nejrůznějšími způsoby. Nejčastějšími zdroji jsou registrační stránky pro služby zdarma, ICQ, Facebook a další stránky, kde bývá elektronická adresa jednou z přenášených informací. Pro filtraci spamu se používají tzv. Bayesovské filtry. Ty vyhodnocují pravděpodobnost spamu pomocí analýzy struktury přijaté správy. Co se týče České republiky, spamming jako takový není trestným činem, ale sběrem elektronických adres může být spáchán trestný čin neoprávněného zacházení s osobními údaji.[15][23][13]

- *Warez*

Warez je moderní počítačové pirátství, většinou skupinového charakteru. Jedna část skupiny se věnuje prolamování bezpečnostních prvků a druhá část se specializuje na šíření pomocí www serverů a získáváním financí na provoz, což často provádí umisťováním reklam na stránky s erotickou tématikou. Tyto reklamy uživatele zahltí množstvím samovolně se otevírajících oken, aniž by se k software dostali. Dnes se warez používají k šíření tzv. cracků (programů, které umožňují zrušit bezpečnostní zajištění u programových produktů).[15][23]

V současné době jsou rozšířené programy pro sítě peer-to-peer, které umožňují výměnu hudebních soborů, videí a dalších. Postihnutí nelegálního souboru šířeného v síti peer-to-peer je mnohem těžší než, když je soubor šířený servery warez.[15]

- *Phreaking*

Phreaking, nebo také zneužívání telefonních služeb. Původní telefandové se jen bavili na úkor telefonních společností, ale postupem času se pokusili proniknout do počítačových systémů. Dnes jsou phreakeři vesměs studenti, kteří zúročují své znalosti výrobou tzv. věčných čipových telefonních karet, nebo jen tak „napíchnou" telefonní ústředny či automaty. Mohou tak zdarma telefonovat, surfovat zdarma po internetu a odposlouchávat cizí telefonní hovory.[23]

- *Cracking*

Cracking je prolamování nebo obcházení bezpečnostních prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití. Cracking používá rozmanitou řadu metod, jednou z nich je například debugování spuštěného programu a reverse engineering[2]. Osoba odstraňující tyto bezpečnostní prvky programu se nazývá cracker. Crack je program, který slouží k odstranění nebo omezení funkčnosti bezpečnostních prvků programu či softwaru. Cracking se často používá k průniku do systému s cílem zjištění informací pro umožnění neoprávněného přístupu do systému (nejčastěji jde o tzv. password cracking[3]).[15][23][13]

- *Sniffing*

Sniffing neboli neoprávněné monitorování elektronické komunikace na síti, především na internetu. Existuje mnoho programů, tzv. snifferů, které umožňují monitorovat komunikaci, která prochází přes určitý uzel sítě. Sniffer tak může zachytávat hesla, přístupová jména, čísla platebních karet apod. Ty ukládá do logovacích souborů nebo je odesílá přes internet. Informace získané tímto způsobem se nejčastěji využívají k průniku do systému, k vydírání nebo k dalšímu zneužití například v hackingu. Jako obrana je proto nutné komunikaci dostatečně zašifrovat.[15][23][13]

- *Cybersquatting*

Za tímto názvem se ještě nedávno schovávalo legální blokování internetových domén. Dnes je cybersquatting, neboli doménové pirátství trestným činem. Svůj vrchol

[2] Zpětná dekompilace (získání zdrojového kódu)programu.
[3] Zjišťování hesla pro přístup do systému.

cybersquatting zažíval, když velké firmy vstupovaly na internet. Cybersquatteři si zaregistrují doménu známého subjektu a snaží se tuto doménu dotyčnému subjektu prodat za mnohdy astronomickou částku. Další formou doménového pirátství může být nekalá soutěž, například parazitování na pověsti (cybersquatter si založí stránku se jménem známé firmy a provozuje na ní svůj internetový obchod).[15][23]

4 INTERNET CRIME COMPLAIN CENTER

Internet Crime Complain Center neboli IC3 je centrum, které se snaží poskytnout veřejnosti spolehlivé informace a data Federálního úřadu pro vyšetřování týkající se podezření na Internetovou kriminalitu, usnadnit její vyšetřování a vyvinout účinná spojenectví spolu s donucovacími orgány. Tyto informace analyzují, poskytují veřejnosti, poskytují k vyšetřování a pro zpravodajské účely činné v trestním řízení.[8]

Od roku 2000 získává IC3 stížnosti napříč spektrem kybernetické kriminality, které zahrnují online podvody v mnoha podobách, hacking, hospodářskou špionáž (krádež obchodního tajemství), online vydírání, praní špinavých peněz, krádež identity apod. Aby lépe odrážel široký charakter počítačové kriminality, byl IC3, dříve známé, jako Internet Fraud Complain Center, přejmenován.[8]

4.1 IC3 Internet Crime Report

IC3 každoročně vydává report z minulých let. Tento report obsahuje analýzy varování, analýzy internetové kriminality a to hned z několika úhlů. Z genderového úhlu (počet procent ženských obětí, počet procent mužských obětí, počet obětí mezi věkem 20-29 let apod.) a z geografického úhlu (počet stížností podle států, finanční ztráta jednotlivých států apod.).

Jelikož je kybernetická kriminalita v České republice zahrnována do Hospodářské kriminality a tudíž o ní samotné nejsou vedeny žádné statistiky, využila jsem tyto reporty pro splnění cíle mé bakalářské práce. Dle reportu z roku 2013 jsem vybrala 42 nejpostiženějších států, jak je možno vidět v Tabulce 1. Tyto státy budu porovnávat s vybranými ukazateli.

Tabulka 1:Přehled vybraných států

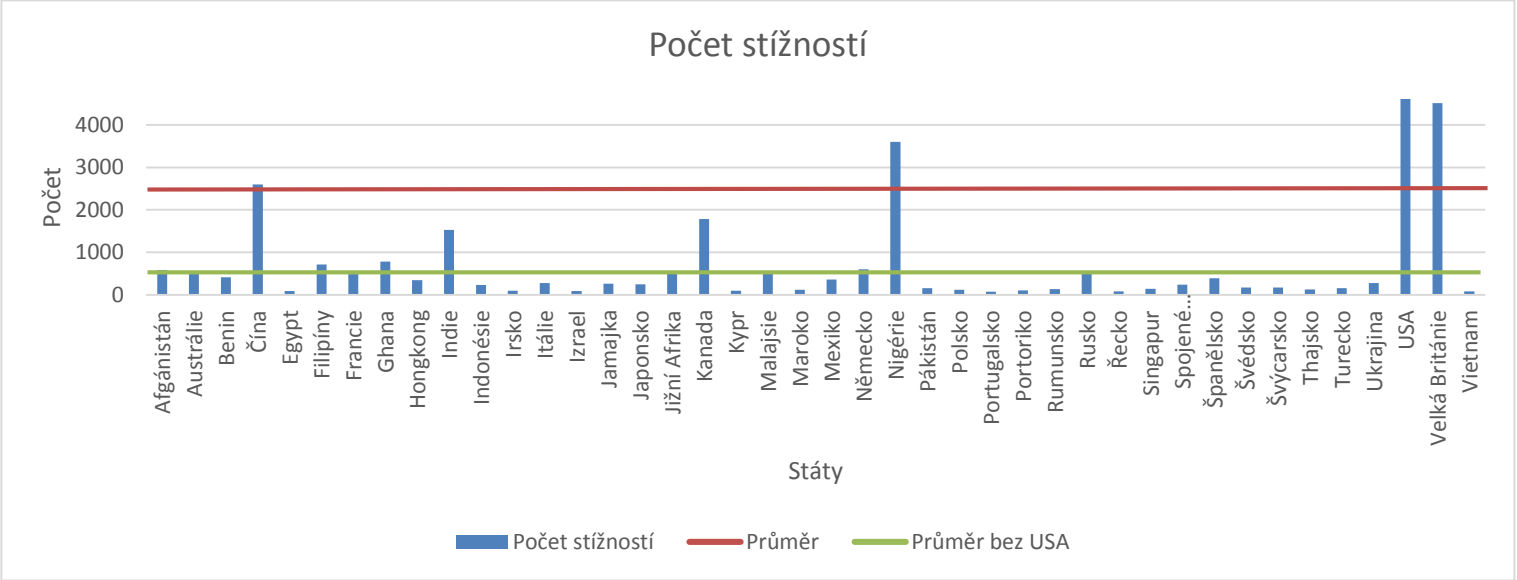
	Počet stížností	**Počet stížností přesahujících ztrátu 100.000 $**		**Počet stížností**	**Počet stížností přesahujících ztrátu 100.000 $**
Afghánistán	578	267	Mexiko	361	207
Austrálie	500	251	Německo	603	181
Benin	409	148	Nigérie	3598	1984
Čína	2601	2237	Pákistán	152	78
Egypt	89	51	Polsko	118	54
Filipíny	714	398	Portugalsko	76	45
Francie	486	164	Portoriko	101	57
Ghana	782	559	Rumunsko	130	78
Hongkong	344	278	Rusko	533	258
Indie	1529	919	Řecko	77	44

	Počet stížností	Počet stížností přesahujících ztrátu 100.000 $		Počet stížností	Počet stížností přesahujících ztrátu 100.000 $
Indonésie	229	186	Singapur	140	78
Irsko	93	48	Spojené Arabské Emiráty	239	92
Itálie	273	160	Španělsko	386	223
Izrael	86	44	Švédsko	168	49
Jamajka	260	160	Švýcarsko	167	68
Japonsko	242	91	Thajsko	128	84
Jižní Afrika	534	281	Turecko	154	74
Kanada	1782	1006	Ukrajina	273	125
Kypr	94	51	USA	83799	49128
Malajsie	524	312	Velká Británie	4511	2464
Maroko	120	55	Vietnam	78	43

Zdroj: Zpracováno podle[9]

4.2 Počet stížností na internetovou kriminalitu

Z Obrázku 1 je patrné, že počet stížností na internetovou kriminalitu většiny vybraných států leží pod průměrem (2572,9 stížností). Vysoko nad průměrem se pohybuje USA, které se s 83799 stížnostmi nevešly do grafu. Nad průměrem také leží Nigérie a Velká Británie. Kolem průměru se pohybuje Čína. Naopak nejméně stížností má z vybraných zemí Portugalsko (76 stížností). Ovšem, kdybychom USA vyřadili z výběru, jakožto odlehlou hodnotu, potom by Čína, Kanada, Indie, Filipíny a Ghana měly nadprůměrné množství stížností na internetovou kriminalitu.[9]



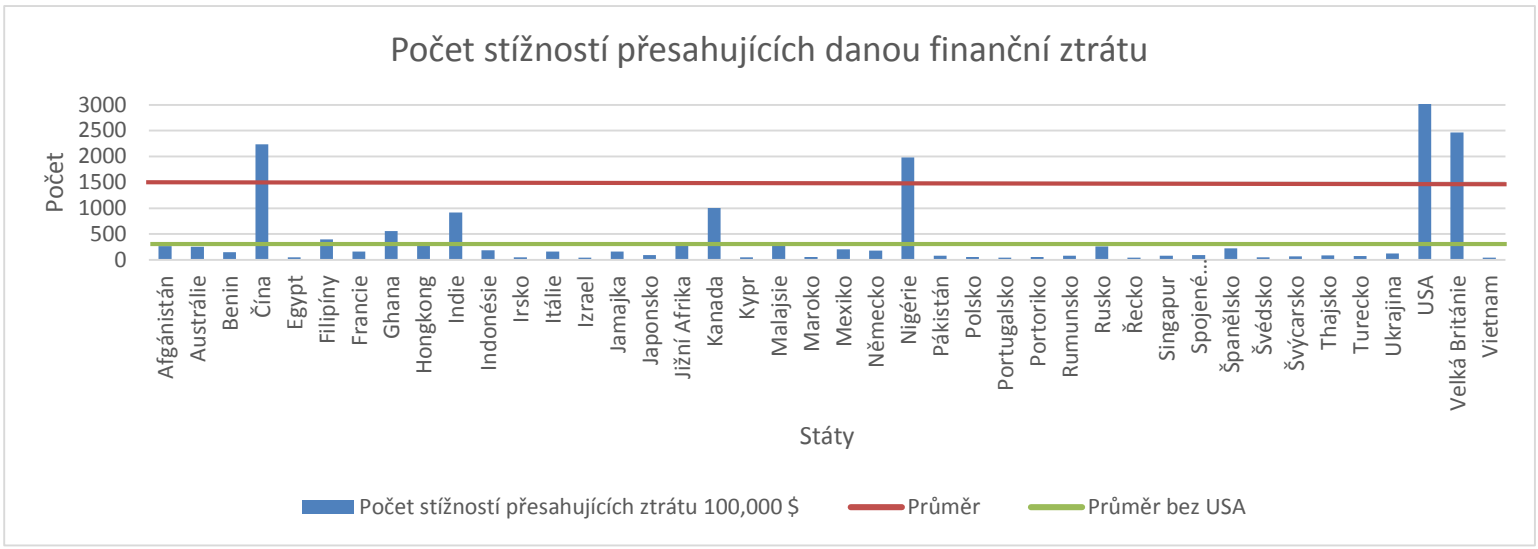
Obrázek 1: Graf počtu stížností na počítačovou kriminalitu

Zdroj: zpracováno podle[9]

4.3 Počet stížností přesahujících finanční ztrátu 100.000 USD

V Obrázku 2 můžeme vidět, že počet stížností na počítačovou kriminalitu, které přesahují finanční ztrátu 100.000 USD většiny vybraných států, opět leží pod průměrem (1501,9). Vysoko nad průměrem se nachází USA, které kvůli svým hodnotám přesahuje rozsah grafu. Nad průměrem se nachází Čína, Nigérie a Velká Británie.[9]

Průměr stížností států s danou minimální finanční ztrátou opět zvedá USA s 49128 stížnostmi. Po vyřazení USA z výběru se nad průměrem (340,3) pohybuje Čína, Filipíny, Ghana, Indie, Kanada, Nigérie a Velká Británie. Naopak nejnižší počet stížností má z výběru Vietnam, pouhých 43 stížností.[9]



Obrázek 2: Graf počtu stížností na počítačovou kriminalitu přesahujících finanční ztrátu 100.000 USD

Zdroj: zpracováno podle[9]

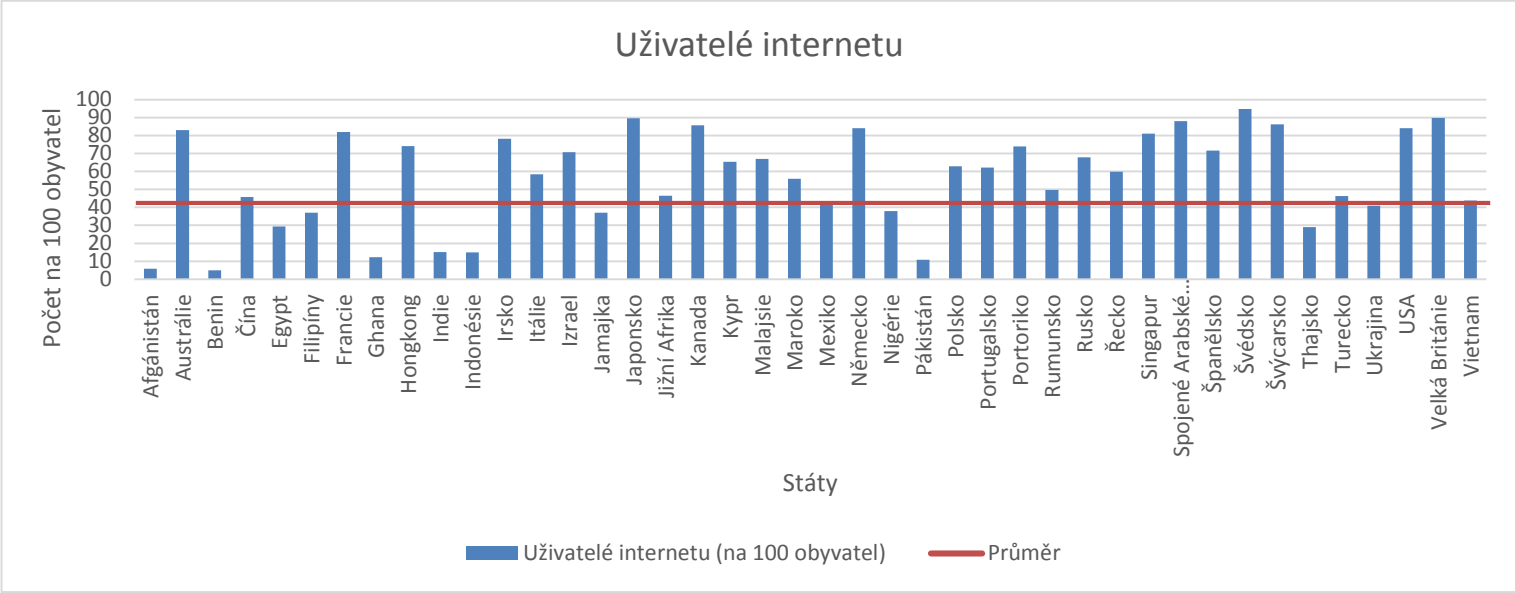
5 UKAZATELÉ HODNOCENÍ

Podle stránek The WorldBank bylo prostudováno několik oblastí průzkumů a byly zvoleny indikátory, jež lze použít k ohodnocení počítačové kriminality. Jelikož jsou data hodnotící počítačovou kriminalitu uvedena z roku 2013, veškeré zmíněné ukazatele se vztahují k témuž roku. Jedná se o hrubý domácí produkt, hrubý národní produkt, počet uživatelů internetu, počet ekonomicky aktivních obyvatel, počet % připojených domácností k elektrickému napětí, běžný účet platební bilance, import, export, zaměstnanost a nezaměstnanost obyvatel. Každý ukazatel je popsán, vysvětlen a doplněn o graf vytvořený z přístupných dat.

5.1 Uživatelé internetu

Prvním ukazatelem je počet uživatelů na Internetu. Internet je celosvětově přístupná síť. Poskytuje přístup k mnoha komunikačním službám, včetně e-mailových služeb, World Wide Web (www), datům, zábavě a zpravodajství bez ohledu na použité zařízení (PC, mobilní zařízení, digitální TV, PDA atd.). Přístup k němu může být z pevné nebo mobilní sítě.[39]

Z Obrázku 3 lze vyčíst, že z vybraných zemí je nejvyšší počet uživatelů internetu ve Švédsku, ve Velké Británii, Japonsku a Spojených Arabských Emirátech. Naopak nejméně uživatelů internetu je v Beninu, Afghánistánu, Ghaně, Indii, Indonésii a v Polsku. Kolem celosvětového průměru (42,5 uživatelů)se pohybují Čína, Jižní Afrika, Mexiko, Turecko, Nigérie a Vietnam. Počet uživatelů internetu také závisí na kvalitě internetového pokrytí, které v Ghaně není zdaleka tak kvalitní, jako například ve Švédsku.[39]



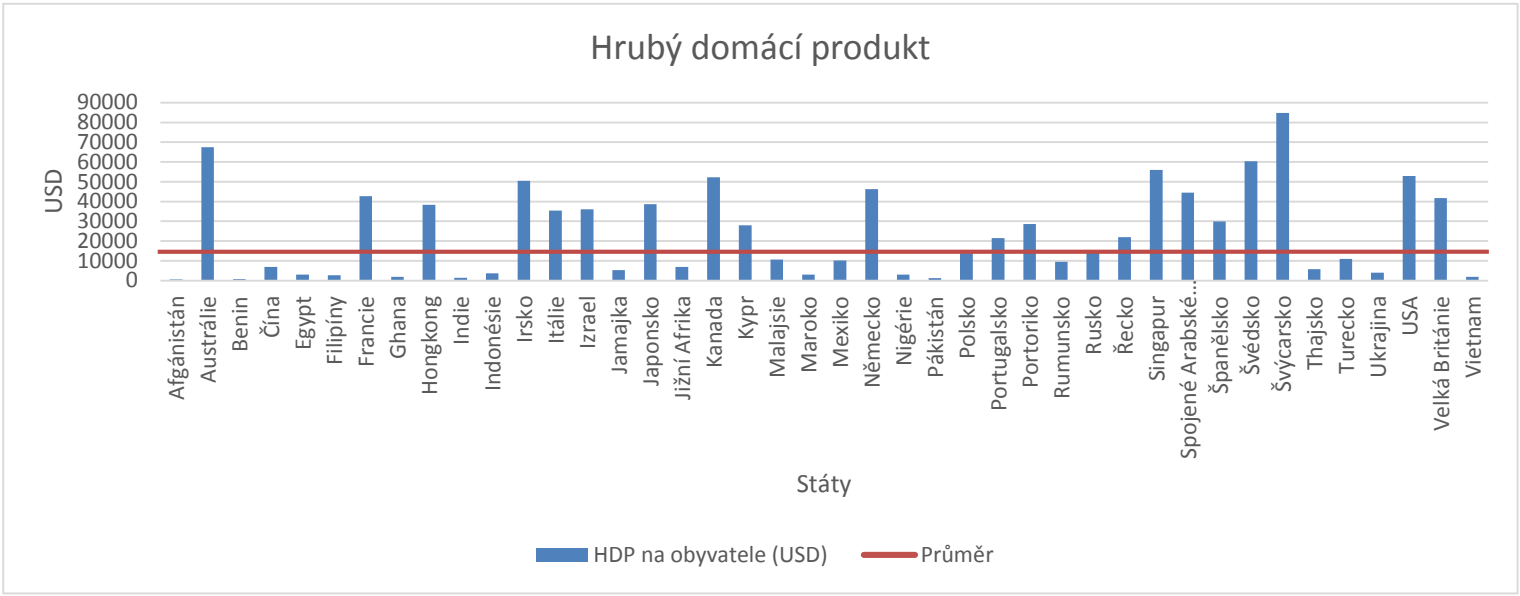
Obrázek 3: Graf počtu uživatelů internetu

Zdroj: zpracováno podle[39]

5.2 Hrubý domácí produkt

Druhým ukazatelem je hrubý domácí produkt (HDP). HDP je ukazatelem výkonnosti ekonomiky a vyjadřuje se v peněžních jednotkách. HDP je měřeno ze systémů národních účtu, které se zpracovávají podle metodik OSN. To umožňuje i mezinárodní srovnávání jednotlivých zemí. Zjednodušeně se jedná o těchto pět typů účtů: podnikový, domácností, státní, styku s cizinou a kapitálové účty. V rámci každého účtu se porovnávají příjmy a výdaje.[10]

Data v Obrázku 4 představují HDP v Amerických dolarech na obyvatele. Z grafu je patrné, že většina zemí má v porovnání se světovým průměrem (14670,46 USD) stejné nebo vyšší HDP. Nejnižších hodnot nabývají Afghánistán, Benin, Ghana, Indie, Pákistán a Vietnam. Naopak nejvyšší HDP má Švýcarsko (84732,96 USD), jehož hodnota pro vysoké hodnoty přesahuje rozsah grafu. Vysoko nad průměrem se také pohybuje Austrálie, Švédsko, Singapur a USA.[34]



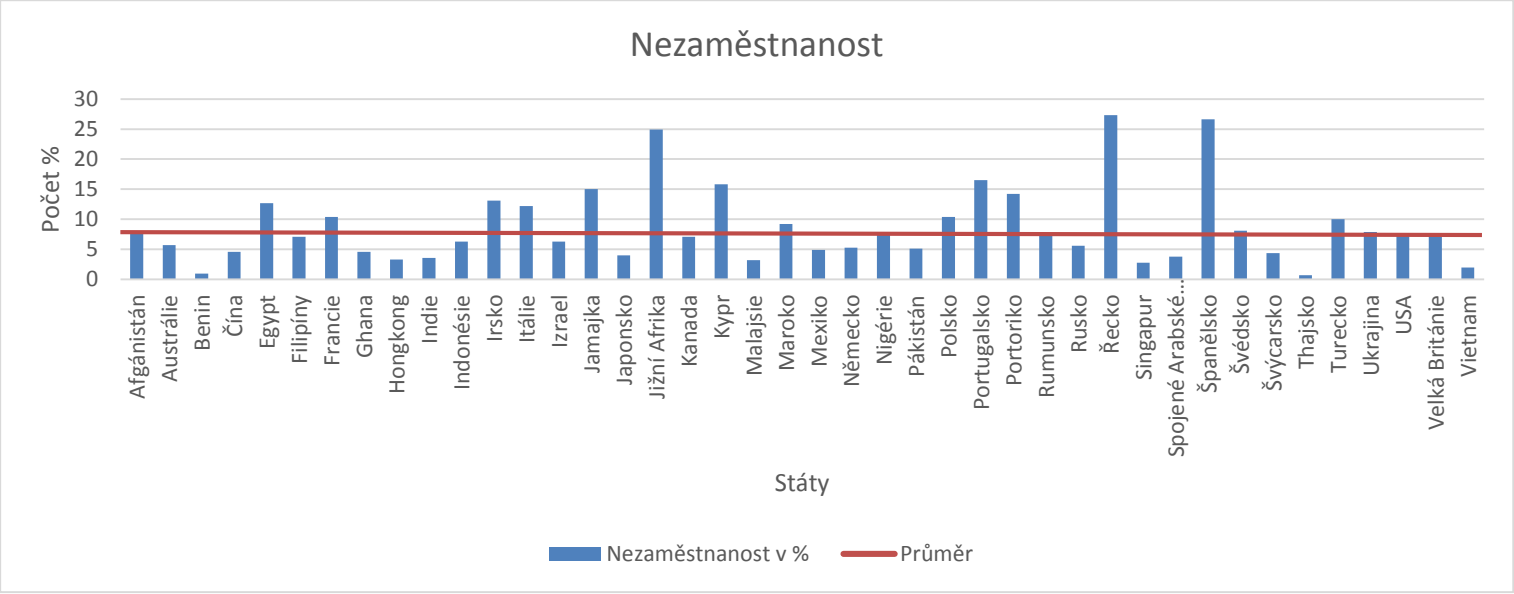
Obrázek 4: Graf HDP na obyvatele

Zdroj:zpracováno podle[34]

5.3 Nezaměstnanost

Třetím ukazatelem je celková nezaměstnanost. Jedná se o obyvatele, kteří jsou bez práce, a právě si práci hledají. Osoby, které práci nehledají, se do nezaměstnanosti nepočítají. Celkově se tedy jedná o osoby, které práci hledají, jsou ji schopni, ale nemohou ji najít. Jako základ tohoto indikátoru slouží ekonomicky aktivní obyvatelé. [38][11]

Z Obrázku 5 je patrné, že se nezaměstnanost ve většině vybraných států pohybuje pod světovým průměrem. Tento průměr zvedají státy Řecko (27,29%), Španělsko a Jižní Afrika. Naopak nejnižší nezaměstnanost je v Beninu (1%) a v Thajsku (0,69%). Nezaměstnanost většiny zbývajících států se pohybuje kolem světového průměru (8,59%).[38]



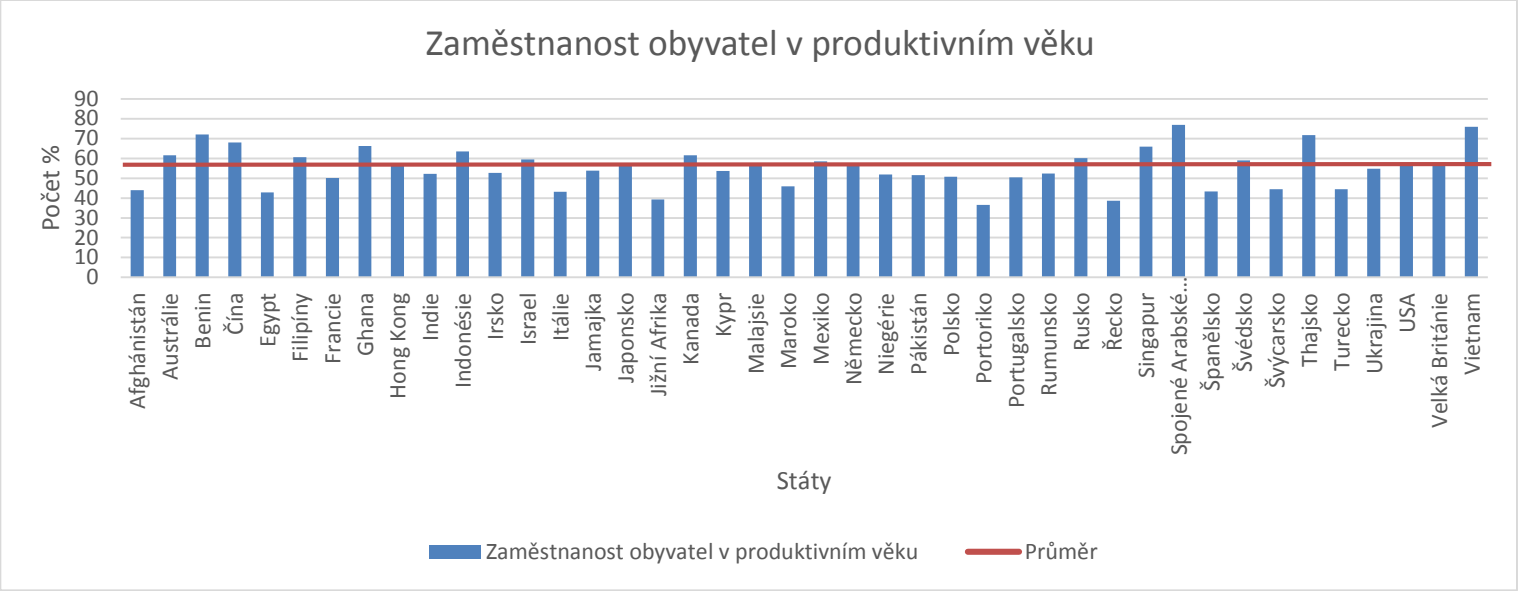
Obrázek 5: Graf nezaměstnanosti

Zdroj: zpracováno podle [38]

5.4 Zaměstnanost obyvatel v produktivním věku

Čtvrtým ukazatelem je zaměstnanost obyvatel v produktivním věku. Do skupiny zaměstnaných jsou bráni obyvatelé žijící v domácnostech, které v daném týdnu vykonaly práci za mzdu, zisk, či rodinný zisk po dobu nejméně jedné hodiny, nebo ač zrovna v práci nebyli, pak jsou zaměstnáni nebo podnikají. Za obyvatele v produktivním věku lze zahrnout osoby starší 15 let.[32]

Z Obrázku 6 je patrné, že zaměstnanost obyvatel v produktivním věku se ve většině vybraných států pohybuje kolem světového průměru (58,5%). Tento průměr zvedá Vietnam, Thajsko a Spojené Arabské Emiráty.[32]



Obrázek 6: Graf zaměstnanosti obyvatel v produktivním věku

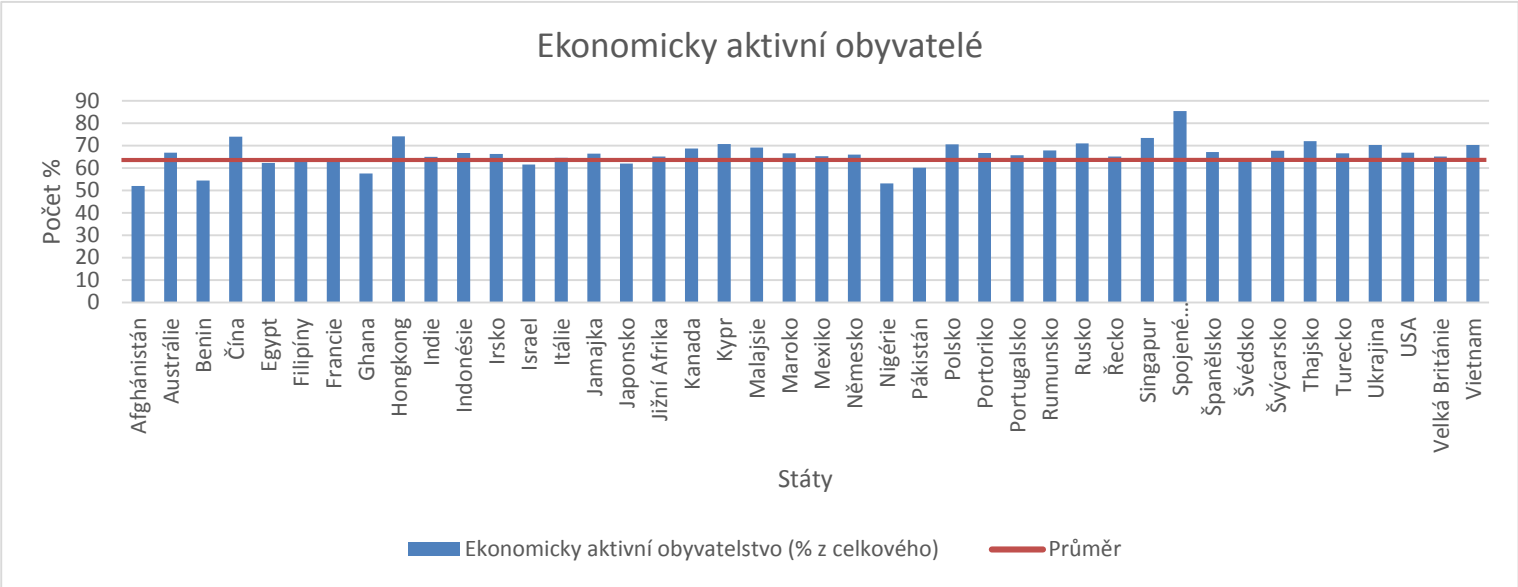
Zdroj: Zpracováno podle[32]

5.5 Počet ekonomicky aktivních obyvatel

Počet obyvatel ve věku 15-64 let, je považován za počet lidí, kteří jsou ekonomicky aktivní. Ekonomicky aktivní obyvatelstvo, čili pracovní sílu, tvoří zaměstnaní a nezaměstnaní.

Za zaměstnané jsou považovány všechny osoby starší 15-ti let, které patří mezi placené zaměstnance nebo osoby zaměstnané ve vlastním podniku. Za nezaměstnané jsou považovány osoby 15leté a starší, které ve sledovaném období souběžně splňují tři podmínky. Neměly placené zaměstnání, zaměstnání aktivně hledaly a byly připraveny k nástupu do práce.[37][7]

V Obrázku 7 je možné vidět, že počet procent ekonomicky aktivních obyvatel je ve všech vybraných zemích vysoký, lze z toho odhadovat, že populace těchto států stárne. Světový průměr je 63,7% ekonomicky aktivních obyvatel. Pod tímto průměrem se pohybuje Afghánistán, Benin, Ghana, Nigérie a Pákistán.[37]



Obrázek 7: Graf počtu % ekonomicky aktivních obyvatel

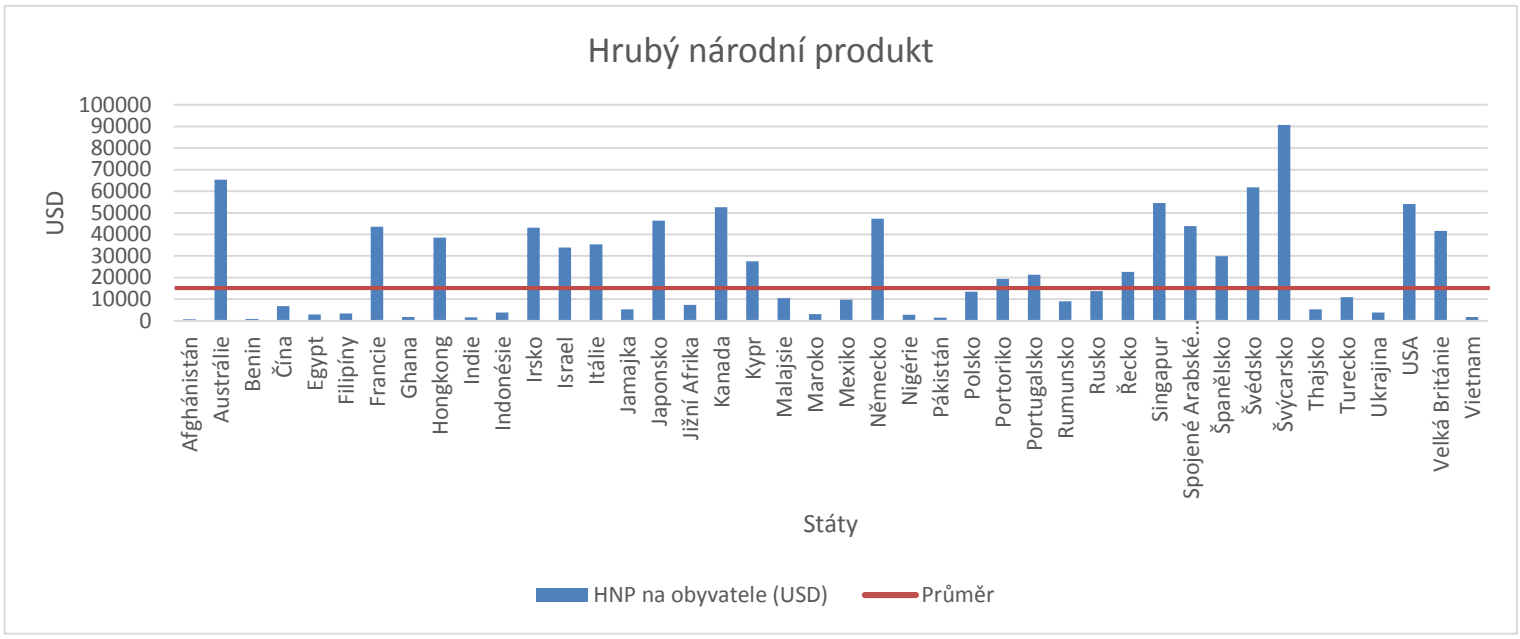
Zdroj: zpracováno podle[37]

5.6 Hrubý národní produkt

Dalším ukazatelem je hrubý národní produkt (HNP). Ten zahrnuje všechny nové statky a služby vytvořené za dané období příslušníky určitého státu. HNP nesleduje, na jakém území bylo zboží vyrobeno, ale zaměřuje se právě na národnostní hledisko. Například v HNP České republice není zahrnut například počítač vyrobený německým podnikem na území ČR. Naopak jsou v něm zahrnuty výrobky vyrobené českými podniky, které sídlí v zahraničí.[35][40]

Pokud je HDP daného státu vyšší než HNP, znamená to, že podniky ze zahraničí, které vyrábí na území daného státu, vyrábějí zboží a služby o větší celkové hodnotě, než jakou hodnotu mají zboží a služby vyrobené podniky daného státu v zahraničí.[40]

Z Obrázku 8 je patrné, že téměř polovina vybraných zemí se pohybuje nad světovým průměrem (14 142,5 USD), tento průměr z vybraných zemí zvedá hlavně Švýcarsko (90670 USD) a Austrálie (65410 USD). Nejnižší HNP má Afghánistán, pouhých 690 USD. Zbytek zemí má velice rozdílné HNP.[35]



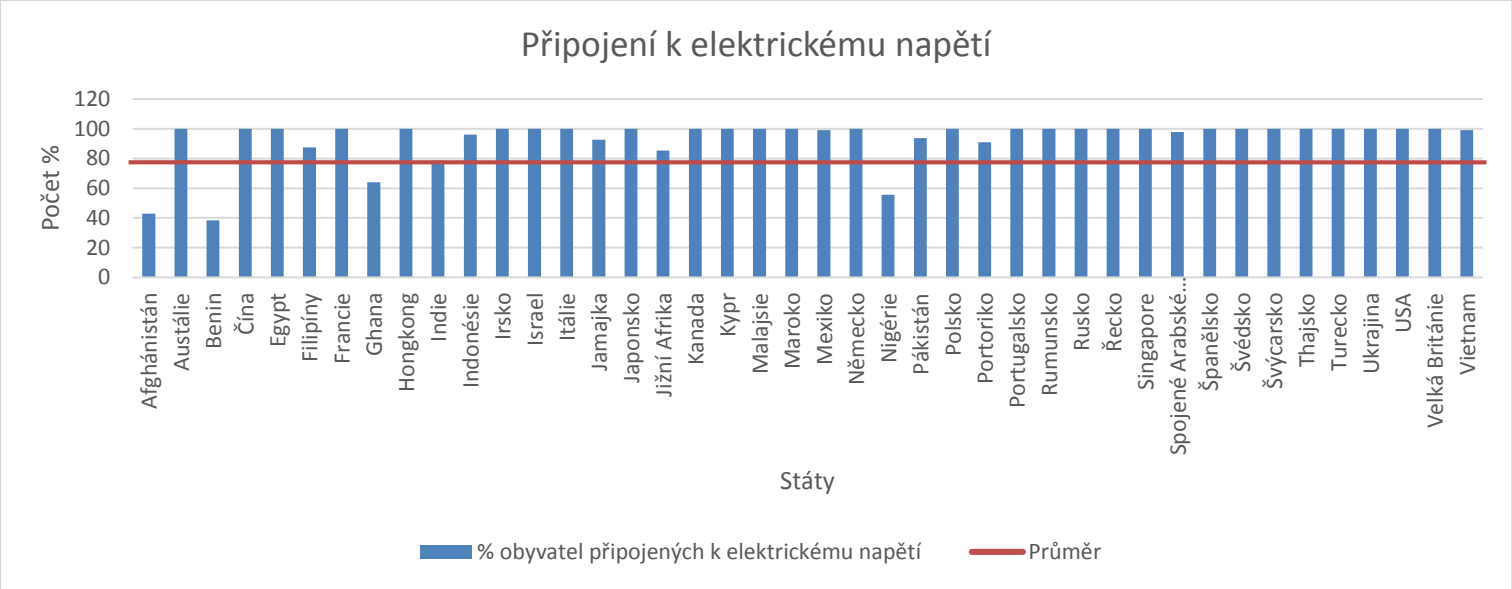
Obrázek 8: Graf HNP na obyvatele

Zdroj: zpracováno podle [35]

5.7 Připojení k elektrickému napětí

Připojení k elektrickému napětí je počítáno jako procento obyvatel, mající přístup k elektrickému napětí. Tyto údaje byly shromažďovány z průmyslu, národních průzkumů a mezinárodních zdrojů.[30]

Z Obrázku 9 je patrné, že většina vybraných států má 100% obyvatel, připojených k elektrickému napětí. Tyto státy se tedy pohybují nad světovým průměrem, 78% obyvatel připojených k elektrickému napětí. Nejméně obyvatel připojených k elektrickému napětí má Afghánistán, Benin, Ghana a Nigérie.[30]



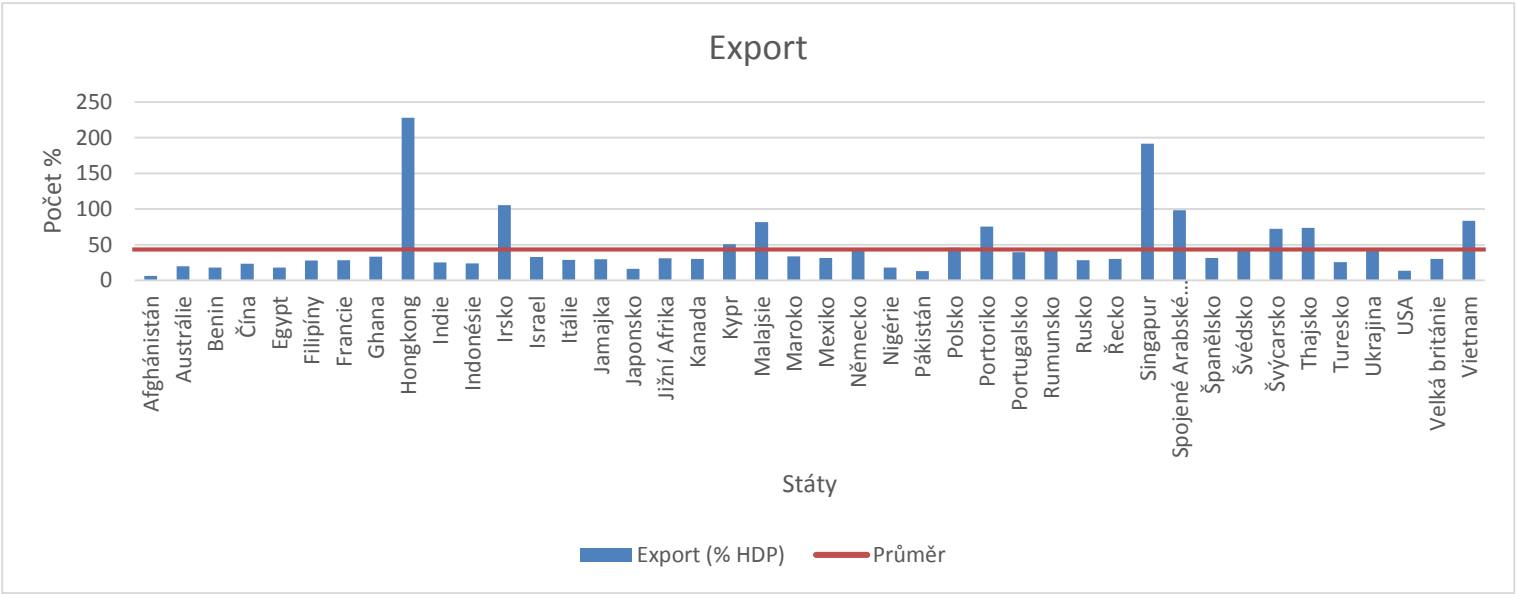
Obrázek 9: Graf počtu % připojených obyvatel k elektrickému napětí

Zdroj: zpracováno podle [30]

5.8 Export

Dalším ukazatelem je export neboli vývoz. Export je celkový objem produktů a služeb nakupovaný zahraničními subjekty vyjádřený ve finanční hodnotě. V teorii lze rozlišovat ještě pojem čistý export, což je rozdíl mezi vývozem a dovozem. Pokud export převyšuje import, má to z dlouhodobého hlediska pozitivní dopad na ekonomiku státu. Znamená to přebytek platební bilance a nárůst HDP státu. Z dlouhodobého hlediska je žádoucí, aby měl stát import i export vyrovnaný.[33][20]

V Obrázku 10 lze vidět, že export jednotlivých zemí je velice nerovnoměrný, světový průměr je 42% HDP. Nad tímto průměrem se pohybuje jen Hongkong, Irsko, Malajsie, Portoriko, Singapur, Spojené Arabské Emiráty a Vietnam. Okolo světového průměru se pohybují Ghana, Izrael, Maroko, Mexiko, Německo, Polsko, Portugalsko, Rumunsko, Španělsko, Švédsko a Ukrajina. Naopak nejméně vyvážejí Afghánistán, Benin, Čína, Nigérie, Pákistán a USA.[33]



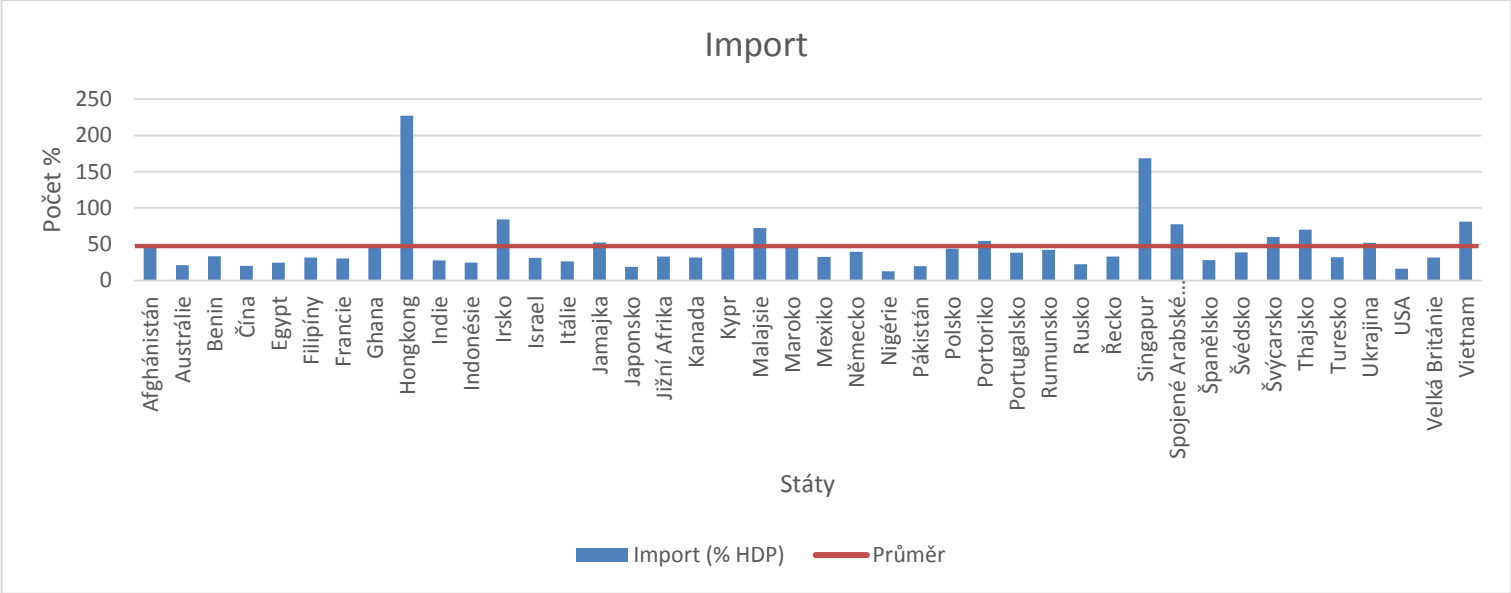
Obrázek 10: Graf exportu v % z HDP

Zdroj: zpracováno podle [33]

5.9 Import

Devátým indikátorem je import. Import neboli dovoz je část produkce nakupovaná domácími subjekty v zahraničí. Je opakem exportu. Organizace a podniky využívají import produktů a služeb z důvodů finanční výhodnosti nebo proto, že produkt, služba není v dané zemi k dispozici. U některých surovin je import nevyhnutelný. Dovozce (importér) musí počítat s proclením dováženého zboží a s riziky změn měnových kurzů.[21][36]

V Obrázku 11 lze vidět, že nad světovým průměrem se pohybují pouze Hongkong, Irsko, Malajsie, Singapur, Spojené Arabské Emiráty, Švýcarsko, Švédsko a Vietnam. Kolem světového průměru, 48% z HDP se pohybují Afghánistán, Ghana, Jamajka, Kypr, Maroko, Německo, Polsko, Portoriko, Portugalsko, Rumunsko a Ukrajina. Nejmenší dovoz má Nigérie a USA, naopak nejvíce dováží Hongkong.[36]



Obrázek 11: Graf importu v % z HDP

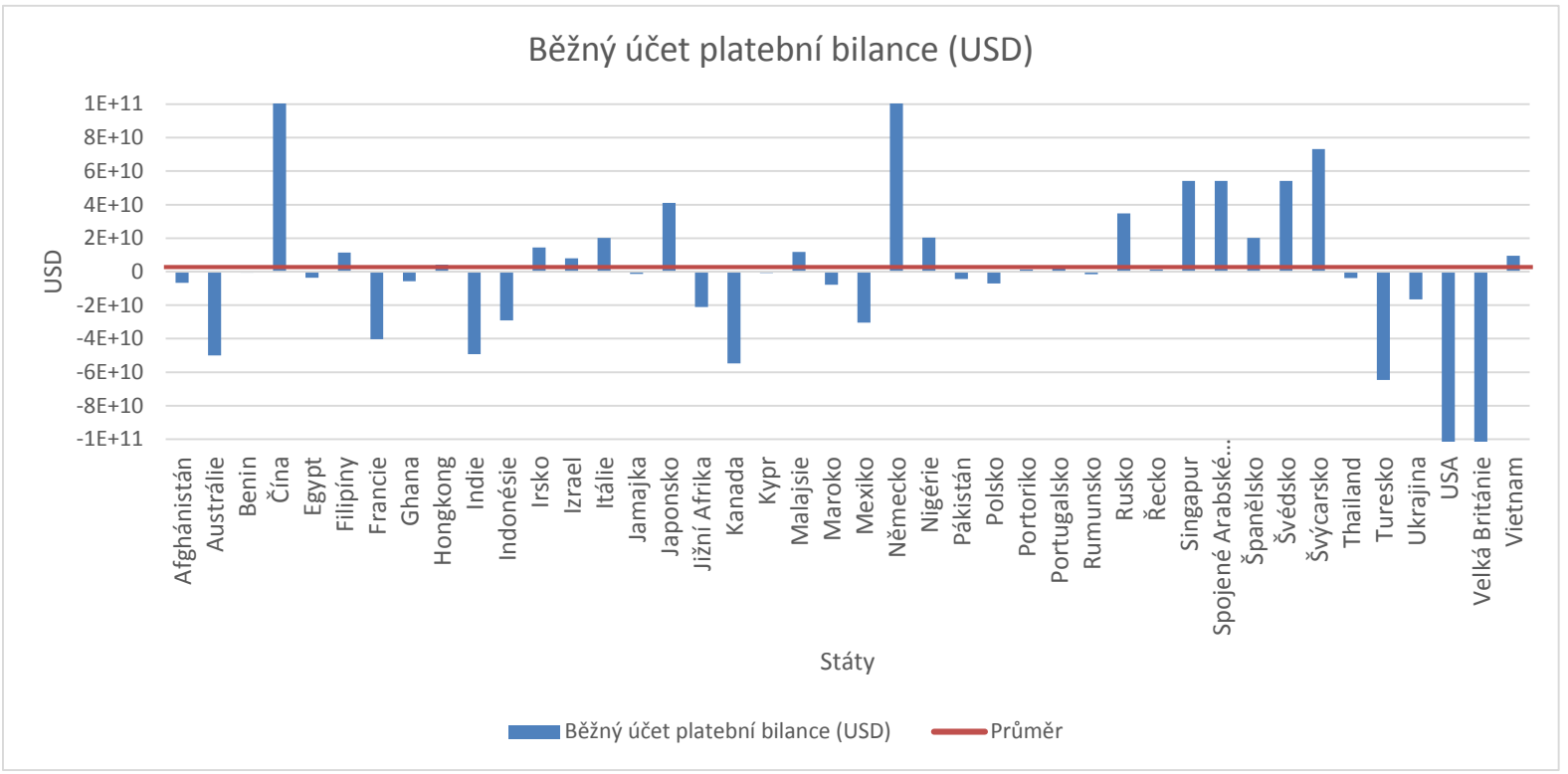
Zdroj: zpracováno podle [36]

5.10 Běžný účet platební bilance

Posledním indikátorem je platební bilance. Platební bilance vyjadřuje peněžní hodnotu všech ekonomických transakcí mezi zemí a ostatními zeměmi v průběhu určitého období, zpravidla za kalendářní rok. Platební bilance má podobu účtu a zahrnuje běžný, kapitálový a finanční účet a v neposlední řadě změnu rezerv. [24][38][31]

V běžném účtu (BÚ) jsou zachyceny toky zboží (vývoz a dovoz) a služeb (příjmy a výdaje z dopravních služeb, cestovního ruchu a ostatních obchodních a neobchodních služeb), výnosy z kapitálu, investic a práce (úroky, dividendy, reinvestované zisky, pracovní příjmy) i kompenzující položky k reálným a finančním zdrojům poskytnutým či získaným bez protihodnoty (běžné jednostranné převody jako např. dary, výživné, penze, zahraniční pomoc, příspěvky aj.).[31]

Z Obrázku 12 je patrné, že platební bilance vybraných zemí se velmi liší. Kvůli velkému rozdílu hodnot jsem nastavila menší rozpětí. Největší platební bilanci má z vybraných zemí Německo, 242 mil. USD. Naopak nejmenší platební bilanci má USA, -377 mil. USD. Světový průměr je 1,6 mil. USD. Kolem tohoto průměru se pohybují Hongkong, Izrael, Portoriko, Portugalsko a Řecko.[31]



Obrázek 12: Graf běžného účtu platební bilance v USD

Zdroj: zpracováno podle [31]

6 SHLUKOVÁ ANALÝZA

Hlavním cílem shlukové analýzy je zařadit objekty do shluků, takovým způsobem, aby dva objekty stejného shluku byly více podobné než dva objekty jiného shluku. Tyto objekty však mohou mít různý charakter jako například živočichové, rostliny, ale také textové dokumenty nebo webové stránky. K dosažení cíle je ale třeba vyřešit řadu dílčích úkolů. Prvním z nich je určení podobnosti dvou objektů. Podobnost měříme pomocí charakteristických vlastností objektů.[28][18]

Vzhledem k velkému množství vědních oborů se v oblasti analýzy vyvinuly i rozličné metody, které lze použít. Podle literatury lze rozlišit[28]:

- tradiční metody a jejich modifikace,
- novější přístupy.

6.1 Tradiční metody a jejich modifikace

V rámci těchto metod jsou v literatuře nejčastěji uváděny dvě základní skupiny. Tyto skupiny jsou tvořeny *metodami rozkladu (partitioning) a hierarchickými metodami*.[28]

U metod rozkladu jde o zařazení objektů do předem stanoveného počtu shluků. Tyto metody lze dělit na *metody pevného shlukování* (objekt je či není ve shluku) a na *fuzzy shlukovou analýzu* (objektům je přiřazena příslušnost ke shluku). Na dělení metod rozkladu však existuje velké množství pohledů. Patří sem například *iterativní relokační algoritmy, metody matematického programování, zobrazování pomocí minimální kostry* apod. Těmto metodám se však dále věnovat nebudu.[28]

Naopak výsledkem hierarchických metod je hierarchie skupin objektů. Tyto metody lze dělit na *aglomerativní* (postupné shlukování objektů) a *divizní* (postupné rozdělování skupin objektů na podskupiny). Těmto metodám se budu podrobněji věnovat níže. Dalším možným dělením hierarchických metod je rozdělení podle způsobu přihlížení na proměnné při vytváření shluků na *monotetické* a *polytetické* shlukování. Metody je možné také dělit na *jednorozměrné*, kdy se shlukují pouze objekty a na *dvourozměrné*, kdy se shlukují současné kategorie dvou proměnných.[28][18]

Hierarchická shluková analýza

Jak už jsem výše zmínila, při tomto způsobu shlukování lze rozlišit dva přístupy, monotetický a polytetický. Při monotetickém přístupu se shluky v určité úrovni vytvářejí

pouze podle jednoho atributu a při polytetickém přístupu se berou v úvahu vždy všechny atributy současně.[28]

Dalším možným členěním je na aglomerativní a divizní přístup.[28][18]

a) *Aglomerativní přístup* vychází ze stavu, kdy každý objekt představuje samostatný shluk. Shluky se postupně po dvojicích spojují od nejvíce po nejméně podobné, až vznikne jediný shluk.

b) *Divizní přístup* vychází z toho, že na začátku tvoří všechny objekty jediný shluk. Ten se postupně rozděluje, až do té doby, dokud každý objekt netvoří jeden shluk.

Polytetické shlukování

Jak jsem již uvedla, u tohoto přístupu je možné rozlišit aglometarivní a divizní shlukování. Já dále budu vycházet z aglomerativního přístupu, tedy, že na počátku je každý objekt jedním shlukem. V prvním kroku se spojí dva objekty na základě matice (ne)podobnosti. Dále je nepodobnost shluků určována podle různých aglomerativních algoritmů. V programových systémech lze nalézt [28]:

- *Metoda průměrné vazby pro mezishlukové vzdálenosti*, která počítá vzdálenost mezi dvěma shluky jako aritmetický průměr vzdáleností všech dvojic objektů, z nichž každý patří do jiného shluku.
- *Metoda průměrné vazby pro vnitroshlukové vzdálenosti*, kde se nejprve spojí dva uvažované objekty do jednoho shluku a teprve potom je počítán aritmetický průměr všech vzdáleností.
- *Metoda nejbližšího souseda* rozčleňuje objekty do shluků s minimální vzdáleností objektů patřících do jednoho shluku.
- *Metoda nejvzdálenějšího souseda* rozčleňuje objekty do shluků s maximální vzdáleností objektů patřících do jednoho shluku.
- *Centroidní metoda* počítá vzdálenost mezi shluky jako euklidovskou vzdálenost mezi dvěma centroidy. To jsou vektory aritmetických průměrů jednotlivých proměnných počítané na základě všech objektů obsažených ve shluku.
- *Mediánová metoda* je založena na stejném principu jako metoda centroidní, s tím rozdílem, že jsou brány v úvahu i velikosti shluků (počty objektů v jednotlivých shlucích).

- *Wardova metoda* spočívá ve spojení shluků, jejichž přírůstek celkového vnitroskupinového součtu čtverců odchylek jednotlivých hodnot je od shlukového průměru minimální.

6.2 Novější přístupy

K nejnovějším přístupům lze zařadit *metody založené na mřížce*, ale také *metody založené na modelu* nebo *metody založené na hustotě*. Déle je možné sem zařadit metody odvozené z výše uvedených metod, jako jsou *metody smíšené*, které využívají všechny uvedené přístupy a *shlukování podprostorů*, jehož základ tvoří metody založené na mřížce a metody založené na hustotě.[28]

Metody založené na mřížce spočívají v rozdělení datového prostoru do konečného počtu pravoúhlých buněk, které vytvářejí mřížkovou strukturu. Všechny operace jsou prováděny na této struktuře. Výhodou těchto metod je nízká časová náročnost, která je závislá na počtu buněk v jednotlivých dimenzích.[28]

Příkladem může být algoritmus STING (STatistical INformation Grid). Ten v první fázi rozdělí datový prostor na pravoúhlé buňky. Buňky tvoří několik úrovní a vytvářejí hierarchickou strukturu. Každá buňka je rozštěpena v nižší úrovni na určitý počet buněk, přičemž pro každou buňku jsou uchovávány statistické charakteristiky (počet objektů, průměr, směrodatná odchylka, minimum, maximum).[28]

Naopak u shlukování podprostorů jde o zkoumání podprostorů původního prostoru. Tyto metody jsou určeny pro soubory s velkým množstvím proměnných.[28]

6.3 Měření podobnosti

Ve shlukové analýze má velmi důležitou roli také měření podobnosti, pro které existuje mnoho koeficientů. Použití jednotlivých koeficientů však závisí na rozhodnutí, zda shlukovat objekty, atributy nebo kategorie, ale také na typech použitých atributů. Podobnost objektů lze zkoumat pomocí míry podobnosti, častěji jsou však používány míry nepodobnosti.[28]

V případě kvantitativních dat, což jsou data použitá v této analýze, se pro vyjádření vztahu objektů používají míry vzdálenosti. Ty jsou založeny na reprezentaci objektů v prostoru, jehož souřadnice představují jednotlivé proměnné. Mezi nejpoužívanější typy vzdáleností patří *euklidovská* D_E, *vážená euklidovská* D_{EW}, *čtvercová euklidovská* D_{ES}, *manhattanská* D_B, *Čebyševova* D_C, *Minkovského* D_M a *Lanceyho-Williamsova* D_{LW}.[28][18]

Výpočet Euklidovské vzdálenosti, jež je použita v analýze, vyjadřuje vzorec (1).[28]

$$D_{E(x_i,x_j)}=\sqrt{\sum_{l=1}^{m}(x_{il}-x_{jl})^2}=\|x_i-x_j\| \quad (1)$$

Hodnota x_{il} představuje hodnotu l-tého pozorování i-tého prvku a hodnota x_{jl} představuje hodnotu l-tého pozorování j-tého prvku.[28]

6.4 Transformace

Jelikož jsou kvantitativní data, použita v této analýze v odlišných měrných jednotkách, bylo nutné provést transformaci dat, která tento problém odstraní. Jedním z předpokladů analýzy je nezávislost proměnných na měrných jednotkách. Kdybychom neprovedli transformaci dat, mohlo by se stát, že některé znaky by mohly ovlivňovat shlukování více než jiné.[28][18]

Pro transformaci kvantitativních dat existuje mnoho postupů. V práci byla data standardizována a následně převedena do normovaného stavu.[28]

Při výpočtu normovaných hodnot, z-skórů, se od každé *i*-té hodnoty *l*-té proměnné odečítá aritmetický průměr hodnot proměnné a výsledek je následně dělen výběrovou směrodatnou odchylkou.[28]

$$z_{il} = \frac{x_{il}-\bar{x}_l}{s_l}, \quad (2)$$

kde $\bar{x}_l$ je aritmetický průměr a s_l značí směrodatnou odchylku. Ty lze vypočítat z následujících vztahů (3), (4).[28]

$$\bar{x}_l = \frac{1}{n}\sum_{i=1}^{n} x_{il} \quad (3)$$

$$s_l = \sqrt{\frac{\sum_i (x_{il}-\bar{x}_l)^2}{n-1}} \quad (4)$$

Nově vzniklá proměnná z_l má střední hodnotu rovnu 0 a směrodatnou odchylku 1.[28][18]

6.5 Rozdělení do shluků a jejich vlastnosti

Shlukování bylo provedeno všemi výše zmíněnými hierarchickými shlukovými metodami. Dendrogramy těchto metod jsou uvedeny v Příloze. Dále bylo rozhodnuto o nejvhodnější metodě na základě *Kofenetického korelačního koeficientu* a *koeficientu Delta*.[18]

Kofenetický korelační koeficient *(CPCC)* je korelační koeficient vzdálenosti mezi prvky matice vzdálenosti (matice (ne)podobnosti) a prvky kofenetické matice. Kofenetická matice je

tvořena prvky, které představují vzdálenost mezi shlukovanými objekty v okamžiku jejich prvního zařazení do shluku. Čím vyšší je hodnota koeficientu, tím kvalitnějšího shlukování bylo dosaženo. Koeficienty dosahující hodnot >0,75 značí „užitečné“ shlukování. Lze ho vypočítat jako Pearsonův korelační koeficient (viz vzorec (5)) mezi skutečnou a predikovanou vzdáleností.[18]

$$\rho_{X,Y} = \frac{E(XY)-E(X)E(Y)}{\sqrt{E(X^2)-E^2(X)}\sqrt{E(Y^2)-E^2(Y)}} \tag{5}$$

Koeficient Delta (ΔA) měří stupeň přetvoření struktury. Čím nižší koeficient, tím došlo k menší ztrátě informací. Je tedy vhodné, aby se koeficient blížil k 0. Koeficient Delta lze vypočítat podle vzorce (6), kde d_{jk} je vzdálenost dvou objektů matice vzdálenosti a d^*_{jk} značí vzdálenost dvou objektů z iterační matice vzdálenosti. Delta se počítá pro A=1 a A=0,5.[18]

$$\Delta_A = \left[\frac{\sum_{j<k}^{N}\left|d_{jk}-d^*_{jk}\right|^{\frac{1}{A}}}{\sum_{j<k}^{N}\left(d^*_{jk}\right)^{\frac{1}{A}}}\right]^A \tag{6}$$

Hodnoty koeficientů je možné vidět v Tabulce 2. Na základě výsledků byla pro analýzu zvolena metoda průměrné vazby pro vnitroshlukové vzdálenosti, která dosahuje nejvyšších hodnot koeficientu CPCC a zároveň nejnižších hodnot koeficientu ΔA.[18]

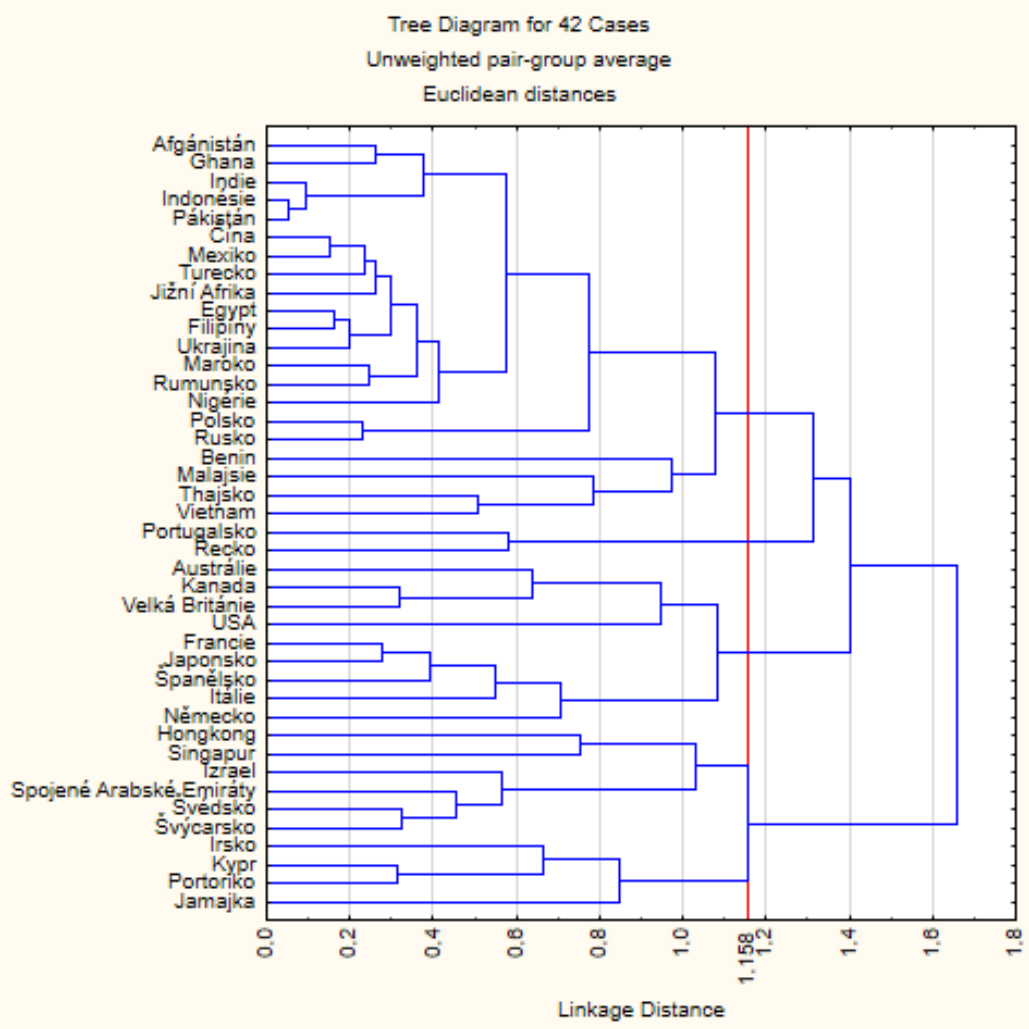
Tabulka 2:Přehled koeficientů kvality shlukování

Metrika	Metoda shlukování	Delta A=0,5	Delta A=1	CPCC
Euklidovská	Metoda nejbližšího souseda	1,08	0,98	0,69
Euklidovská	Metoda nejvzdálenějšího souseda	0,30	0,24	0,73
Euklidovská	Metoda průměrné vzdálenosti	0,16	0,13	0,89
Euklidovská	Centroidní metoda	1,00	0,90	0,82
Euklidovská	Mediánová metoda	1,15	1,02	0,70
Euklidovská	Wardova-Wishartova metoda	0,87	0,85	0,73

Zdroj: zpracováno podle[16][17]

Postup shlukování přehledně zobrazuje speciální stromový graf, dendrogram. Ten zobrazuje postupné shlukování objektů a shluků již vytvořených v předešlých krocích. Lze ho vytvořit v horizontální (objekty uvedeny na ose y) nebo vertikální (objekty uvedeny na ose x) podobě.[28]

Pro analýzu byla zvolena horizontální podoba diagramu. Vybraná metoda průměrné vzdálenosti má celkem 41 iteračních kroků. Na základě jejích výsledků bylo rozhodnuto o rozdělení postižených států do 4 shluků, jak je možné vidět v Obrázku 13.



Obrázek 13: Dendrogram metody průměrné vzdálenosti

Zdroj: vlastní zpracování

Výsledné rozdělení do shluků je možné vidět v Tabulce 3.

Tabulka 3: Rozdělení zemí do shluků

Shluk 1	**Shluk 2**	**Shluk 3**	**Shluk 4**
Hongkong, Singapur, Švédsko, Švýcarsko, Spojené Arabské Emiráty, Izrael, Kypr, Portoriko, Irsko, Jamajka	Kanada, Velká Británie, Austrálie, USA, Francie, Japonsko, Španělsko, Itálie, Německo	Portugalsko, Řecko	Benin, Malajsie, Vietnam, Thajsko, Rusko, Polsko, Nigérie, Rumunsko, Maroko, Ukrajina, Filipíny, Egypt, Jižní Afrika, Turecko, Mexiko, Čína, Indie, Pákistán, Indonésie, Ghana, Afghánistán

Zdroj: zpracováno podle[17]

V následujícím textu budou specifikovány vlastnosti jednotlivých shluků. Přehled popisných statistik všech shluků lze nalézt v Příloze.

Shluk1

Tento shluk se skládá z 10 objektů. Těmi jsou Hongkong, Singapur, Švédsko, Švýcarsko, Spojené Arabské Emiráty, Izrael, Kypr, Portoriko, Irsko a Jamajka.

Z Tabulky 4 je patrné, že tyto státy mají podprůměrné množství stížností na počítačovou kriminalitu a také podprůměrné množství stížností s finanční ztrátou nad 100.000 USD. Státy Shluku1 se vyznačují druhým nejnižším průměrným počtem stížností, který činí 169,2 stížností a také druhým nejnižším průměrným množstvím stížností s finanční ztrátou na 100.000 USD, 92,5 stížností. Ukazatel nezaměstnanosti vykazuje druhou nejnižší průměrnou hodnotu, 8,6% a současně druhou nejvyšší zaměstnanost 55,6%. HDP se pohybuje okolo 43 235 USD na obyvatele a HNP okolo 42 194 USD na obyvatele. V porovnání s ostatními shluky je Shluk1 význačný nejvyšším průměrným exportem, importem a také má nejvíce ekonomicky aktivních obyvatel. Export činí 88,8% z HDP a import 82,3% z HDP.

Tabulka 4: Popisná statistika Shluk1

Shluk1		
Indikátor	**Průměr**	**směrodatná odchylka**
Běžný účet platební bilance	27545564164,61	28285257125,38
Ekonomicky aktivní obyvatelstvo	69,78	6,52
Export	88,83	69,53
HDP na obyvatele	43235,24	21586,19
HNP na obyvatele	42194,00	23492,62
Import	82,30	64,88
Nezaměstnanost	8,68	5,29
Obyvatelé připojení k elektrickému napětí	99,03	2,36
Počet stížností	169,20	86,64
Počet stížností s finanční ztrátou nad 100.000 USD	92,50	73,77
Uživatelé internetu	74,98	15,93
Zaměstnanost obyvatel v produktivním věku	55,67	9,97

Zdroj: vlastní zpracování

Shluk2

Do tohoto shluku bylo roztříděno 9 států, kterými jsou Kanada, Velká Británie, Austrálie, USA, Francie, Japonsko, Španělsko, Itálie a Německo.

V porovnání s ostatními shluky se tento shluk vyznačuje nadprůměrným počtem stížností a vysokým množstvím stížností s finanční ztrátou nad 100.000 USD. Tento shluk obsahuje

USA, které tuto hodnotu značně ovlivňují. Ale i kdybychom vyřadili USA jako odlehlou hodnotu, tento shluk by stále vykazoval nejvyšší průměrnou hodnotu jak v počtu stížností (1 097,8 stížností), tak v množství stížností s finanční ztrátou na 100.000 USD (1 464,5 stížností). Státy Shluku2 jsou typické druhou nejvyšší nezaměstnaností s průměrnou hodnotou 9,8%, nejvyšším HDP a HNP, jejichž průměrná hodnota činí 44 303,7 USD (HDP na obyvatele) a 45 071,25 USD (HNP na obyvatele). V porovnání s ostatními shluky mají státy Shluku2 nejnižší import, export a platební bilanci běžného účtu. Tyto státy mají také 100% obyvatel připojených k elektrickému napětí. Všechny průměrné hodnoty lze vidět v Tabulce 5.

Tabulka 5: Popisná statistika Shluk2

Shluk2		
Indikátor	**Průměr**	**směrodatná odchylka**
Běžný účet platební bilance	5805752989,13	108339871773,06
Ekonomicky aktivní obyvatelstvo	65,05	2,56
Export	29,36	8,84
HDP na obyvatele	44303,70	11538,25
HNP na obyvatele	45071,25	10978,83
Import	29,22	6,59
Nezaměstnanost	9,85	7,29
Obyvatelé připojení k elektrickému napětí	100,00	0,00
Počet stížností	1097,88	1464,53
Počet stížností s finanční ztrátou nad 100.000 USD	567,50	820,55
Uživatelé internetu	80,57	10,60
Zaměstnanost obyvatel v produktivním věku	55,84	6,22

Zdroj: vlastní zpracování

Shluk3

Shluk3 je tvořen 2 objekty, kterými jsou Řecko a Portugalsko.

V porovnání s ostatními shluky je Shluk3 typický nejnižším průměrným počtem stížností (76,5 stížností) a také nejnižším průměrným množstvím stížností s finanční ztrátou nad 100.000 USD (44,5), hned po Shluku1. Státy tohoto shluku, mají také nejvyšší nezaměstnanost, která v průměru činí 21,9% obyvatel a také je v těchto státech zaměstnáno 37,65% obyvatel, což je nejméně z vytvořených shluků. Export a import těchto států patří hned po Shluku1 k nejvyšším. Export dosahuje průměrně 52,89% z HDP a import 43,93% z HDP. Stejné pořadí vykazuje také ukazatel ekonomicky aktivních obyvatel, který průměrně

dosahuje 65,83% z celkového počtu obyvatel. HDP a HNP patří hned po Shluku4a Shluku1 na třetí místo ze všech shluků. HDP průměrně činí 21 736,84 USD na obyvatele a HNP dosahuje průměrně 20 960 USD na obyvatele. Všechny průměrné hodnoty je možné vidět v Tabulce 6.

Tabulka 6: Popisná statistika Shluk3

Shluk3		
Indikátor	**Průměr**	**směrodatná odchylka**
Běžný účet platební bilance	1408526609,00	403,05
Ekonomicky aktivní obyvatelstvo	65,83	1,10
Export	52,89	32,05
HDP na obyvatele	21736,84	324,03
HNP na obyvatele	20960,00	2333,45
Import	43,93	15,19
Nezaměstnanost	21,90	7,64
Obyvatelé připojení k elektrickému napětí	95,44	6,45
Počet stížností	76,50	0,71
Počet stížností s finanční ztrátou nad 100.000 USD	44,50	0,71
Uživatelé internetu	60,98	1,58
Zaměstnanost obyvatel v produktivním věku	37,65	1,48

Zdroj: vlastní zpracování

Shluk4

Shluk4 je tvořen z 21 objektů. Těmi jsou Benin, Malajsie, Vietnam, Thajsko, Rusko, Polsko, Nigérie, Rumunsko, Maroko, Ukrajina, Filipíny, Egypt, Jižní Afrika, Turecko, Mexiko, Čína, Indie, Pákistán, Indonésie, Ghana a Afghánistán.

Tento shluk je typický druhým nejvyšším průměrným počtem stížností a s tím souvisejícím počtem stížností s finanční ztrátou nad 100.000 USD na počítačovou kriminalitu, hned za Shlukem2. Státy tohoto shluku jsou typické nejnižší průměrnou nezaměstnaností, která činí 6,98% obyvatel a současně je v těchto státech zaměstnáno v průměru 56,38% obyvatel ve věku 15-64 let, což je nejvyšší hodnota. Tato hodnota však může být ovlivněna faktem, že státy tohoto shluku mají nejmenší počet ekonomicky aktivních obyvatel. V porovnání s ostatními shluky, mají státy tohoto shluku průměrně nejnižší HDP a HNP, které dosahují 5 560,98 USD na obyvatele (HDP) a 5 443,33 USD na obyvatele (HNP). Mají také nejslabší export, 34,67% z HDP a slabý import, 39,18% z HDP. Nejhorší

výsledek má tento shluk také u počtu uživatel internetu (36,56), počtu ekonomicky aktivních obyvatel (64,88) a počtu obyvatel připojených k elektrickému napětí (87,64). Všechny průměrné hodnoty si lze opět prohlédnout v následující Tabulce 7.

Tabulka 7: Popisná statistika Shluk4

Shluk4		
Indikátor	**Průměr**	**směrodatná odchylka**
Běžný účet platební bilance	870577904,09	47287234041,64
Ekonomicky aktivní obyvatelstvo	64,88	6,32
Export	34,67	21,19
HDP na obyvatele	5560,98	4389,96
HNP na obyvatele	5443,33	4249,63
Import	39,18	18,30
Nezaměstnanost	6,98	5,14
Obyvatelé připojení k elektrickému napětí	87,64	19,97
Počet stížností	649,24	895,63
Počet stížností s finanční ztrátou nad 100.000 USD	399,90	606,70
Uživatelé internetu	36,56	19,73
Zaměstnanost obyvatel v produktivním věku	56,38	10,43

Zdroj: vlastní zpracování

ZÁVĚR

Touto prací, zabývající se počítačovou kriminalitou, jsem chtěla přiblížit jeden způsob, jak pohlížet na tuto problematiku. K jejímu hodnocení lze použít mnoho různých metod, které poskytují různou představu o dané situaci. Pomocí metod shlukové analýzy bylo posuzováno 42 vybraných států, konkrétně 42 států s nejvíce stížnostmi na počítačovou kriminalitu a s nejvyšším množstvím stížností s finanční ztrátou nad 100.000 USD spojenou s touto kriminalitou. Pomocí grafů byla znázorněna data jednotlivých ukazatelů a bylo vyobrazeno, v jakých hodnotách se jednotlivé státy pohybují. Pomocí těchto grafů, si čtenář mohl udělat názor o vybraných státech.

Práce je rozdělena do 6 částí. První část je věnována definici počítačové kriminality a jejímu rozčlenění. Dále příčinám jejího vzniku a správnému chování na internetu.

Druhá část je zaměřena na historii počítačové kriminality. Historie je rozdělena do 3 částí od roku 1801 až do roku 2010, nazývaných starověk, středověk a novověk. Jsou zde zmíněny nejzávažnější milníky, co se počítačové kriminality týče.

V třetí části je počítačová kriminalita dělena podle různých autorů a přístupů. Dále jsou zde popsány konkrétní formy počítačové kriminality. Ty jsou rozděleny jako tradiční a nová protiprávní jednání.

Čtvrtá část pojednává o Internet Crime Complain Center (IC3): stručné charakteristice, zaměření činnosti a reportech, které každoročně vydává. Na základě reportu z roku 2013 byly vybrány země s nejvíce stížnostmi na počítačovou kriminalitu a nejvyšším počtem stížností na počítačovou kriminalitu přesahujících finanční ztrátu 100.000 USD. Oba tyto ukazatelé jsou popsány přiloženým grafem. Data z tohoto reportu jsou dále použita ke shlukové analýze.

Pátá, předposlední část práce je věnována vybraným ukazatelům hodnocení. Každý ukazatel je popsán přiloženým grafem a popisem situace ve vybraných zemích na základě dat pořízených ze stránek The WorldBank.

Šestá, poslední část, je věnována shlukové analýze, která rozděluje státy do výsledného počtu shluků. Každý shluk je popsán a celý proces vyobrazen v přiloženém dendrogramu.

Cílem této práce bylo pomocí metod shlukové analýzy provést komparaci vybraných zemí v oblasti počítačové kriminality na základě dostupných parametrů. Na základě těchto parametrů jsem porovnávala 4 shluky, vzniklé pomocí metody průměrné vzdálenosti. Shluky jsou názorně vizualizovány pomocí přiložených dendrogramů.

POUŽITÁ LITERATURA

[1] *Absolut Beginner on WWWeb*. Čeho se nebát- HOAX, fámy, atd. [online]. 2003, 2004 [cit. 2015-10-18]. Dostupné z: http://www.abowe.brbla.net/1-kapitola-uzivatelske-minimum/bezpecnost-zaklady/hoax.php

[2] *Bezpečně-online.cz.* Netiketa. [online]. [cit. 2015-11-11]. Dostupné z: http://www.bezpecne-online.cz/surfuj-bezpecne/komunikace-se-svetem/netiketa.html

[3] *Bloomberg.* Cyber crime and information warfare: 30-year history. [online]. 2010 [cit. 2015-12-02]. Dostupné z: http://www.bloomberg.com/ss/10/10/1014_cyber_attacks/1.htm

[4] *Businessinfo.* Hlavní měnové a fiskální ukazatele. [online]. 2011-06-30 [cit. 2015-12-02]. Dostupné z: http://www.businessinfo.cz/cs/clanky/hlavni-menove-a-fiskalni-ukazatele-cr-3113.html#pb

[5] *Cz.nic.* Extremismus na Internetu. [online]. 2012, 2014 [cit. 2015-10-18]. Dostupné z: http://www.jaknainternet.cz/page/1693/extremismus-na-internetu/

[6] DOLEŽAL, Ivan. *Svět tisku.* Padělání tiskovin. [online]. 2004 [cit. 2015-11-14]. Dostupné z: http://www.svettisku.cz/buxus/generate_page.php?page_id=7003&buxus_svettisku

[7] *Else international.* Ekonomicky aktivní obyvatelstvo. [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://www.elseaz.cz/slovnik/ekonomicky-aktivni-obyvatelstvo/

[8] *Federal Bureau of Investigation.* Internet Crime Complain Center. [online]. 2000 [cit. 2015-11-11]. Dostupné z: http://www.ic3.gov/about/default.aspx

[9] *Federal Bureau of Investigation.* Internet Crime Complaint Center. 2013 Internet Crime Report. [online]. 2014 [cit. 2015-11-11]. Dostupné z: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

[10] *Finance.cz.* Hrubý Domácí Produkt (HDP). [online]. 2015-10-13 [cit. 2015-11-03]. Dostupné z: http://www.finance.cz/makrodata-eu/hdp/informace/

[11] *Finance.cz.* Nezaměstnanost. [online]. 2015-11-14 [cit. 2015-11-14]. Dostupné z: http://www.finance.cz/makrodata-eu/trh-prace/nezamestnanost/

[12] *Ho@x.cz.* Phishing. [online]. 2015-09-21 [cit. 2015-11-14]. Dostupné z: Phishing. http://www.hoax.cz/phishing/

[13] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu*. 1. Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8

[14] *Chování.eu.* Netiketa. [online]. [cit. 2015-11-11]. Dostupné z: http://www.chovani.eu/netiketa/c56

[15] JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[16] JONÁŠOVÁ H. *Modul pro kvalitu významnosti hierarchického shlukování*. Dostupné z: http://jonasova.upce.cz

[17] JONÁŠOVÁ H., LOHYNSKÝ J. *Modul pro hierarchické shlukování.* Dostupné z: http://jonasova.upce.cz

[18] JONÁŠOVÁ, Hana. *Zpracování dat metodami shlukové analýzy*. Univerzita Pardubice, 2014.

[19] MACHÁČEK, Miroslav. Počítačová kriminalita a bezpečnost. *Internet pro všechny*. [online]. 2013 [cit. 2015-11-14]. ISSN 1801-1160. Dostupné z: http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/

[20] *ManagementMania.* Export. [online]. 2013 [cit. 2015-12-02]. Dostupné z: https://managementmania.com/cs/export-v-ekonomice

[21] *ManagementMania.* Import. [online]. 2013 [cit. 2015-12-02]. Dostupné z: https://managementmania.com/cs/import

[22] MAŠKOVÁ, Martina. První virus osobních počítačů vznikl před dvaceti lety. *BBCCZECH.com.* [online]. 2006, 2006-01-23 [cit. 2015-10-17]. Dostupné z: http://www.bbc.co.uk/czech/scitech/story/2006/01/060123_pc_virus_pckg.shtml

[23] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

[24] *Miraslebl.* Obchodní a platební bilance. [online]. 2000 [cit. 2015-12-02]. Dostupné z: http://www.miras.cz/seminarky/makroekonomie-07-platebni-bilance.php

[25] *Mozektevidi.cz.* Hacking, hacker. [online]. 2010-12-30 [cit. 2015-11-10]. Dostupné z: http://mozektevidi.cz/hacking-hacker/

[26] *Novinky.cz.* Vyděračský virus terorizuje už i uživatele Linuxu. [online]. 2015-11-09 [cit. 2015-11-09]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/385814-vyderacsky-virus-terorizuje-uz-i-uzivatele-linuxu.html

[27] *Papírová platidla, bankovky*. Padělky. [online]. 2012 [cit. 2015-11-14]. Dostupné z: http://www.papirovaplatidla.cz/informace/padelky

[28] ŘEZANKOVÁ, Hana, HÚSEK, Dušan, SNÁŠEL, Václav. *Shluková analýza dat*. 2. Praha: Professional Publishing, 2009. ISBN 978-80-8694-681-8.

[29] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

[30] *The WorldBank.* Access to electricity (% of population). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/EG.ELC.ACCS.ZS

[31] *The WorldBank.* Current account balance (BoP, current US$). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/BN.CAB.XOKA.CD

[32] *The WorldBank.* Employment to population ratio, 15+, total (%). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/SL.EMP.TOTL.SP.ZS

[33] *The WorldBank.* Export of goods and services (% of GDP). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/NE.EXP.GNFS.ZS

[34] *The WorldBank.* GDP. [online]. 2014, [cit. 2015-11-9]. Dostupné z: http://search.worldbank.org/quickview?name=%3Cem%3EGDP%3C%2Fem%3E+per+capita+%28current+US%24%29&id=NY.GDP.PCAP.CD&type=Indicators&cube_no=2&qterm=GDP

[35] *The WorldBank.* GNI. [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/NY.GNP.PCAP.CD

[36] *The WorldBank.* Import of goods and services (% of GDP). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/NE.IMP.GNFS.ZS

[37] *The WorldBank.* Population ages 15-64 (% of total). [online]. 2015 [cit. 2015-12-02]. Dostupné z: http://data.worldbank.org/indicator/SP.POP.1564.TO.ZS

[38] *The WorldBank.* Unemployment. [online]. 2014 [cit. 2015-11-10]. Dostupné z: http://databank.worldbank.org/data/reports.aspx?Code=SL.UEM.TOTL.ZS&id=af3ce82b&report_name=Popular_indicators&populartype=series&ispopular=y

[39] *The WorldBank.* Internet users. [online]. 2014, 2014-11-12 [cit. 2015-11-13]. Dostupné z: http://databank.worldbank.org/data/reports.aspx?Code=IT.NET.USER.P2

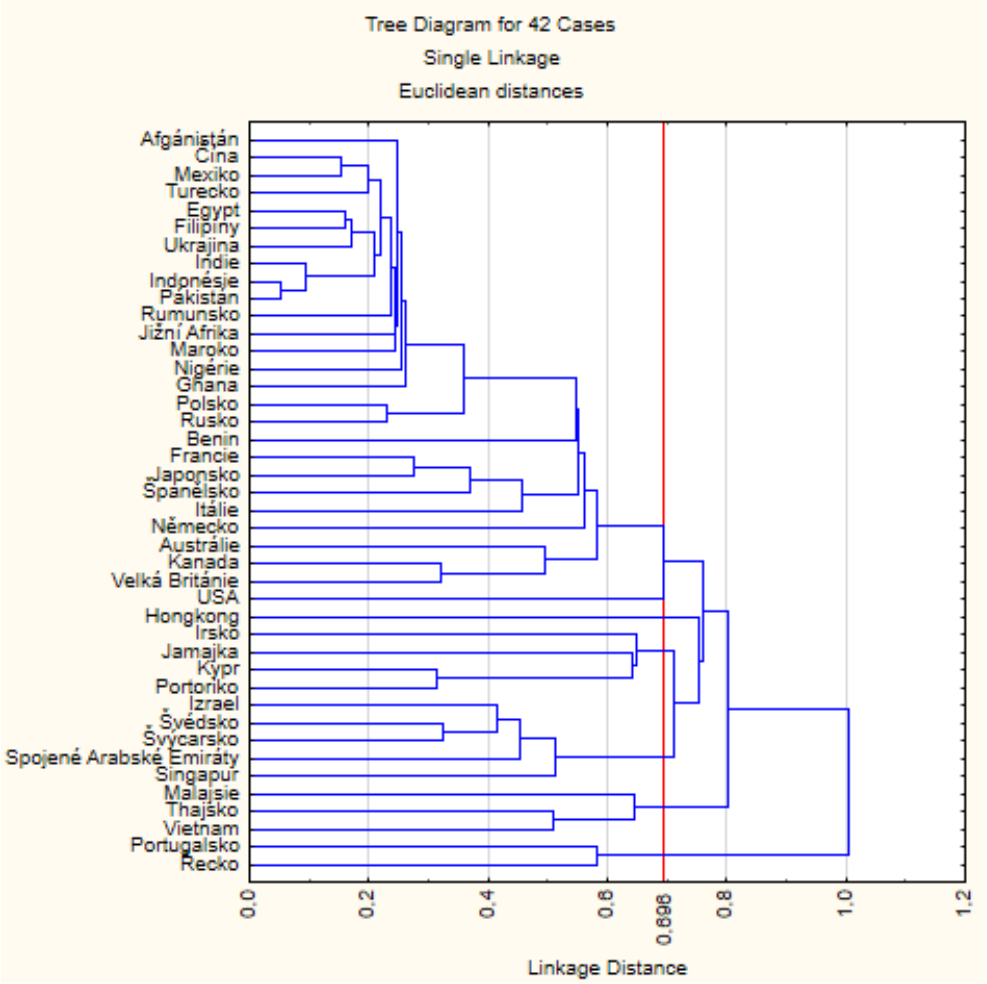
[40] *Vítejte na Zemi.* HNP. [online]. 2013 [cit. 2015-12-02]. Dostupné z: http://vitejtenazemi.cz/cenia/index.php?p=hnp&site=spotreba

[41] VOJTOVÁ, Tereza. *Firemnifinance.cz.* Pomluva na Facebooku vás může vyjít pěkně draho. [online]. 2011-08-02 [cit. 2015-11-14]. Dostupné z: http://firmy.finance.cz/zpravy/finance/320049-pomluva-na-facebooku-vas-muze-vyjit-pekne-draho/

[42] *Wavefront consulting group certified information security consultants.* A brief history of cybercrime. [online]. 2008 [cit. 2015-12-02]. Dostupné z: http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html

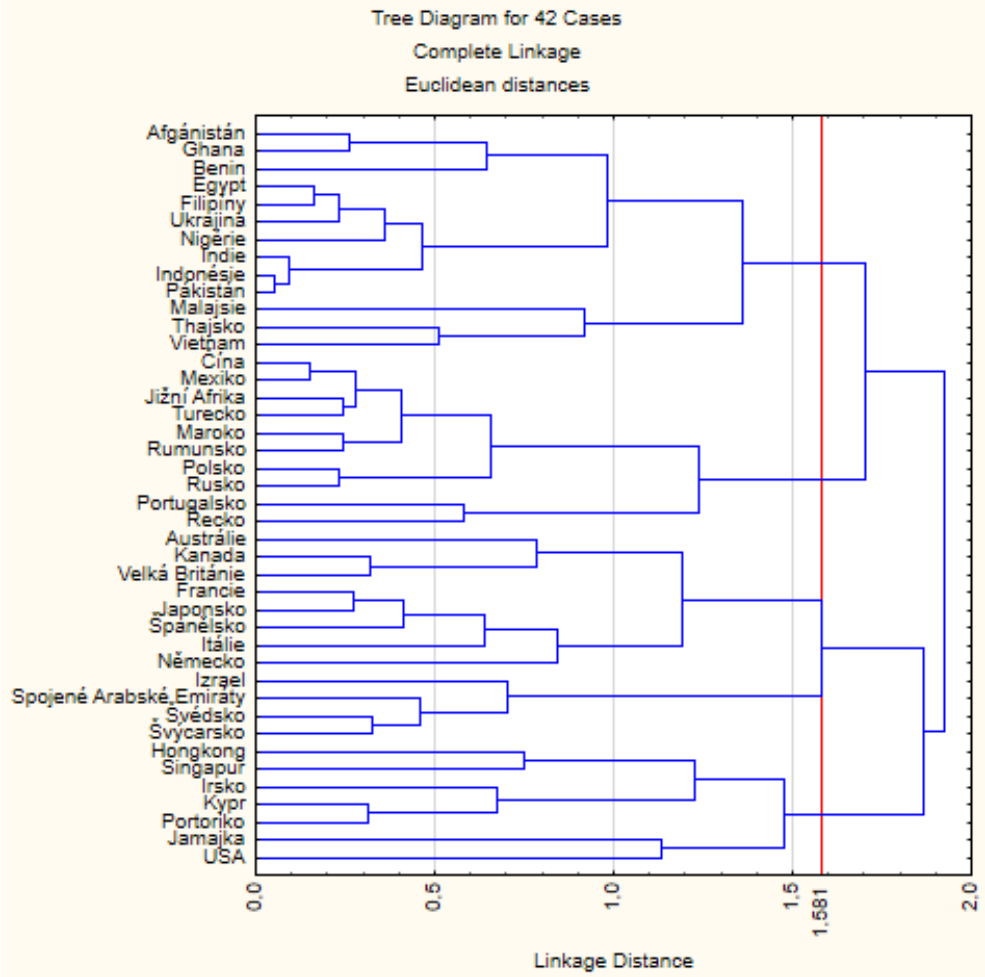
SEZNAM PŘÍLOH

Příloha A



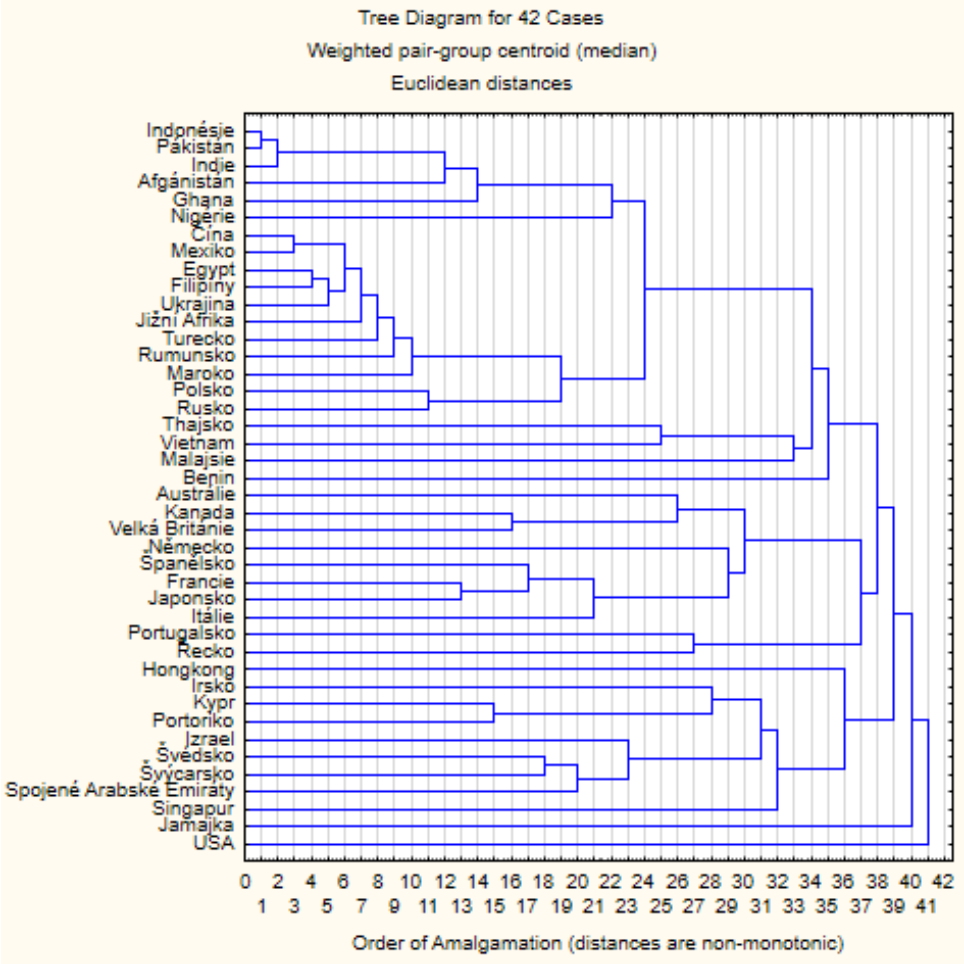
Zdroj: vlastní zpracování

Příloha B



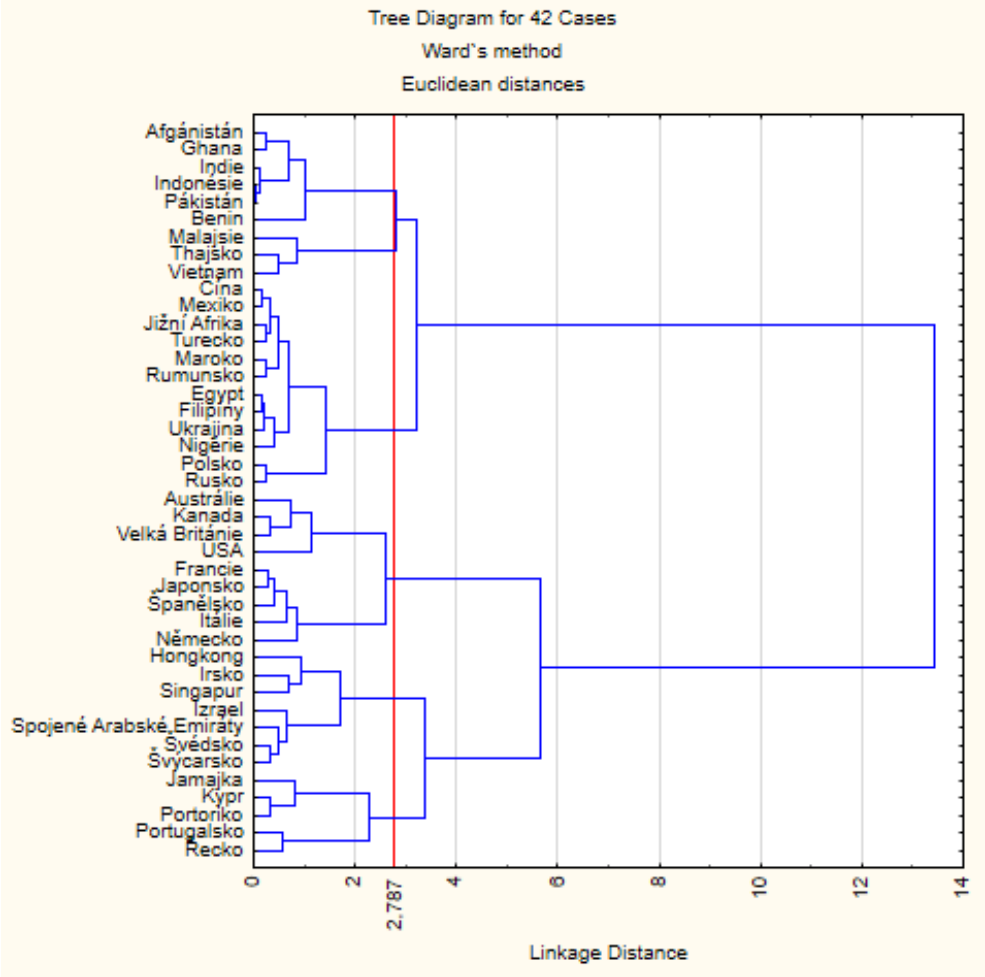
Zdroj: vlastní zpracování

Příloha C



Zdroj: vlastní zpracování

Příloha D



Zdroj: vlastní zpracování

Příloha E

Indikátor	Shluk1	Shluk2	Shluk3	Shluk4
Běžný účet platební bilance	27545564164,61	5805752989,13	1408526609,00	870577904,09
Ekonomicky aktivní obyvatelstvo	69,78	65,05	65,83	64,88
Export	88,83	29,36	52,89	34,67
HDP na obyvatele	43235,24	44303,70	21736,84	5560,98
HNP na obyvatele	42194,00	45071,25	20960,00	5443,33
Import	82,30	29,22	43,93	39,18
Nezaměstnanost	8,68	9,85	21,90	6,98
Obyvatelé připojení k elektrickému napětí	99,03	100,00	95,44	87,64
Počet stížností	169,20	1097,88	76,50	649,24
Počet stížností s finanční ztrátou nad 100.000 USD	92,50	567,50	44,50	399,90
Uživatelé internetu	74,98	80,57	60,98	36,56
Zaměstnanost obyvatel v produktivním věku	55,67	55,84	37,65	56,38

Zdroj: vlastní zpracování