VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

ETIOLOGIE PODVODŮ V KYBERPROSTORU

Autor práce: Martin Daniel, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Dr. Mgr. Josef Kříha, PhD., LL.M.

Katedra: Katedra právních oborů a bezpečnostních studií

2025

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Martin Daniel, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Etiologie podvodů v kyberprostoru

Název bakalářské práce v anglickém jazyce: Etiology of Fraud in Cyberspace

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
Dr. Mgr. Josef Kříha, PhD., LL.M.

Datum zadání bakalářské práce (měsíc, rok): listopad 2024

Cíl bakalářské práce: Hlavním cílem je s využitím teoreticko-praxeologického přístupu nalezení příčin kybernetických podvodů z pohledu teorie racionální volby s důrazem na finanční motivaci pachatelů a vliv technologického pokroku na jejich metody. Vedlejším cílem je objasnění nejčastějších forem a metod kybernetických podvodů v České republice a následné navržení účinných preventivních opatření, zaměřených na zvýšení povědomí uživatelů o těchto hrozbách.

Student: Martin Daniel, DiS.	26. 11. 2024	
Vedoucí práce: Dr. Mgr. Josef Kříha, PhD., LL.M.	6. 12. 2024	

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12. 12. 2024	
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11. 12. 2024	
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20. 1. 2025	

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ -2- ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Dr. Mgr. Josefu Kříhovi, PhD., LL.M. za cenné rady, připomínky, metodické vedení práce a zejména za jeho ochotu a vstřícnost. Dále bych chtěl poděkovat mé rodině za podporu během studia.

ABSTRAKT

DANIEL, M. *Etiologie podvodů v kyberprostoru: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 61 s. Vedoucí práce: Dr. Mgr. Josef Kříha, PhD., LL.M.

Klíčová slova: kybernetické podvody, motivace pachatelů, prevence, racionální volba, technologie.

Obsahové vymezení bakalářské práce se zabývá příčinami, formami a prevencí kybernetických podvodů v České republice. Využívá teorie racionální volby k analýze motivace pachatelů, přičemž hodnotí vliv technologického pokroku na metody páchání těchto trestných činů. Bakalářská práce vychází z kombinace teoretického přístupu, empirických dat Policie České republiky, Národního úřadu pro kybernetickou a informační bezpečnost a České bankovní asociace za období let 2021 až 2023. Výsledkem je identifikace nejčastějších typů kybernetických podvodů a návrh konkrétních preventivních opatření pro efektivnější ochranu jednotlivců a institucí.

ABSTRACT

DANIEL, M. *Etiology of Cyber Fraud: Bachelor Thesis*. České Budějovice: The College of European and Regional Studies, 2025. 61 pgs. Supervisor: Dr. Mgr. Josef Kříha, PhD., LL.M.

Key words: cyber fraud, offender motivation, prevention, rational choice, technology.

The content specification of the bachelor's thesis deals with the causes, forms, and prevention of cyber fraud in the Czech Republic. It utilizes rational choice theory to analyze offenders' motivations, while assessing the impact of technological advancements on the methods used to commit these crimes. The bachelor's thesis is based on a combination of theoretical approaches and empirical data from the Police of the Czech Republic, the National Cyber and Information Security Agency, and the Czech Banking Association, covering the period from 2021 to 2023. The outcome is the identification of the most common types of cyber fraud and a proposal of specific preventive measures to enhance the protection of individuals and institutions.

Obsah

Úvod

Informační a komunikační technologie se staly nedílnou součástí každodenního života současné společnosti. Jejich dostupnost i míra využití neustále roste napříč všemi generacemi. Každá nová technologická inovace však vedle nesporných přínosů přináší také určitá rizika. V důsledku probíhající digitalizace dochází k částečnému přesunu trestné činnosti do online prostředí, kde pachatelé využívají výhod kyberprostoru, zejména nízké pravděpodobnosti odhalení a možností značných finančních zisků.

Kybernetická kriminalita tak představuje jeden z nejzávažnějších bezpečnostních problémů současnosti. Podvody v digitálním prostředí jsou stále častější a ohrožují nejen jednotlivce, ale i firmy, instituce a celou kritickou infrastrukturu. S rostoucí komplexitou technologií se zvyšuje i sofistikovanost těchto útoků a jejich obtížná odhalitelnost, což podtrhuje naléhavost efektivní prevence a adekvátní reakce bezpečnostních složek. Kybernetické podvody dnes představují vážnou hrozbu pro stabilitu a důvěru v digitální prostředí.

Věcné vymezení bakalářské práce se zaměřuje na analýzu příčin a faktorů vedoucích k páchání kybernetických podvodů, přičemž klíčovým aspektem je teorie racionální volby. Tato teorie předpokládá, že pachatelé pečlivě zvažují rizika a přínosy svých činů, často jsou motivováni finančním ziskem. Díky tomuto přístupu lze lépe porozumět motivacím pachatelů i navrhnout účinná preventivní opatření. Práce rovněž zkoumá, jak technologický pokrok, včetně nových digitálních nástrojů a platforem, ovlivňuje metody a formy těchto podvodů.

Empirická část bakalářské práce se zaměřuje na kvantitativní analýzu dat získaných z policejních databází, statistik Národního úřadu pro kybernetickou a informační bezpečnost, České bankovní asociace a Europolu. Ambicí této analýzy je definovat současný stav kybernetických podvodů v České republice, identifikovat jejich nejčastější typy a analyzovat související trendy. Na základě získaných poznatků navrhnout konkrétní preventivní opatření a doporučení pro efektivnější řešení kybernetických incidentů.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce (dále jen „**práce**“) je s využitím teoreticko-praxeologického přístupu nalezení příčin kybernetických podvodů z pohledu teorie racionální volby, s důrazem na finanční motivaci pachatelů a vliv technologického pokroku na jejich metody. Vedlejším cílem je objasnění nejčastějších forem a metod kybernetických podvodů v České republice a následné navržení účinných preventivních opatření zaměřených na povědomí uživatelů o těchto hrozbách.

Při naplňování hlavního cíle práce je aplikována teorie racionální volby, přičemž důraz je kladen na motivace pachatelů ovlivněné technologickým vývojem – využívání umělé inteligence, anonymizačních nástrojů či globalizovaných platforem. Práce dále analyzuje proměny modus operandi pachatelů a jejich vývoj v období let 2021 až 2023. Metodologicky práce kombinuje teoreticko-praxeologický a fenomenologický přístup.

V kvalitativní části je použit fenomenologický přístup zaměřený na interpretaci motivací pachatelů a porozumění dynamice kybernetických podvodů z pohledu lidského rozhodování. Práce vychází z teoretických rámců racionální volby (Rational Choice Theory – dále jen “TRV”), rutinních aktivit (Routine Activity Theory – dále jen “TRA”) a psychologických modelů vnímání rizika. Tyto přístupy umožňují lépe porozumět faktorům ovlivňujícím rozhodování pachatelů i jejich vnímání rizik spojených s kybernetickou kriminalitou.

Empirická část práce zahrnuje kvantitativní analýzu statistických dat od Policie České republiky, Národního úřadu pro kybernetickou a informační bezpečnost a České bankovní asociace. Tyto údaje umožňují identifikovat trendy v incidenci a charakteru kybernetické kriminality, především podvodů. Výsledky kvantitativního šetření jsou doplněny kvalitativním posouzením determinantů technologického vývoje, komparací s vývojovými trendy kybernetické kriminality na základě zpráv Europolu.

Získaná data jsou vyhodnocena metodou obsahové analýzy, triangulace zdrojů, přičemž interpretace probíhá v kontextu teoretického rámce. Výsledky jsou následně syntetizovány v empirické části a v závěru práce konfrontovány s formulovanými výzkumnými cíli. Tato metodologická kombinace umožňuje komplexní pohled na problematiku kybernetických podvodů, jejich příčiny, vývojové trendy i možné způsoby efektivní prevence.

2 Vymezení základního pojmosloví a východisek zkoumané teoretické oblasti

V této kapitole budou vymezeny základní pojmy, které jsou nezbytné pro pochopení celkové problematiky kybernetických podvodů. Tato vymezení poskytnou teoretický základ pro další části práce a objasní klíčové aspekty, jako je kyberprostor, kybernetická kriminalita a právní definice protiprávního jednání souvisejícího s podvody v kyberprostoru.

2.1 Kyberprostor

Termín kyberprostor (cyberspace) poprvé použil americko-kanadský spisovatel William Ford Gibson v povídce "Vypálit Chrom"[1], později, v roce 1984, ve svém díle Neuromancer[2] uvedl první definici tohoto prostoru.

Podle Koloucha je kyberprostor **"*… virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.*"[3].**

Kyberprostor je v odborné literatuře definován jako: "*globální a vyvíjející se doména charakterizovaná užíváním elektrických sítí a elektromagnetického spektra, jejž smysl je vytvářet, uchovávat, zpracovávat, sdílet, selektovat, třídit, vybírat, používat či vymazávat informace*"[4]. Tato definice akcentuje nejen technickou podstatu kyberprostoru, ale také jeho funkční roli jako prostoru informačních a komunikačních toků, které mají zásadní význam při šíření podvodného chování a manipulaci s daty. Z hlediska kybernetických podvodů je důležité, že kyberprostor umožňuje anonymní a geograficky nedefinované jednání, čímž zásadně komplikuje právní i technické aspekty prevence a postihu.

[1] WIKISOFIA. *William Gibson* [online]. [cit. 2025-01-07]. Dostupné z WWW: <https://wikisofia.cz/wiki/William_Gibson>.
[2] GIBSON, W., *Neuromancer*. 1. vyd. Překlad Ondřej Neff. Plzeň: Laser, 1992.
[3] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019, s. 36.
[4] MAYER, M., MARTINO, L., MAZURIER, T., ZVETKOVA, G. *How Would You Define Cyberspace*. 2014. In: PORADA, V., RAIS, K. a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: Pocta Vladimíru Smejkalovi*. Plzeň: Aleš Čeněk, 2021, s. 323.

Kyberprostor je někdy mylně zaměňován s pojmem internet, ale to není přesné. Internet je pouze jednou z částí kyberprostoru, stejně jako je např. silnice součástí širší dopravní sítě. Kyberprostor představuje neustále se rozvíjející digitální prostředí, které zahrnuje všechny formy elektronické komunikace a výměny informací. Kybernetické útoky se mohou odehrát kdekoli v tomto komplexním systému.

Podle § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**zákon o kybernetické bezpečnosti**“) se kybernetickým prostorem rozumí **“*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*”**[5].

Rozvoj kybernetické bezpečnosti úzce souvisí s technologickým pokrokem v oblasti výpočetní techniky, procesem digitalizace a rostoucím počtem uživatelů pohybujících se v kyberprostoru. Tento fenomén by nebyl myslitelný bez vzniku a rozšíření internetu. Za počátky internetu lze považovat období od poloviny 20. století, kdy se začal prosazovat přechod od analogových systémů k digitálním technologiím.[6]

2.2 Kybernetická kriminalita

Kybernetická kriminalita představuje dynamickou a komplexní oblast trestné činnosti, ve které informační a komunikační technologie hrají klíčovou roli. Nejedná se pouze o digitální obdobu tradiční kriminality, ale o fenomén, který zahrnuje široké spektrum trestných činů s různou mírou sofistikovanosti. Klíčovým rysem kybernetické kriminality je zneužití digitálních technologií k nelegálním aktivitám, přičemž útočníci často využívají anonymitu, obtížnou dohledatelnost a globální charakter kyberprostoru.

Digitální prostředí nezná fyzické hranice, kybernetická kriminalita často přesahuje jurisdikční rámec jednotlivých států a vyžaduje mezinárodní spolupráci při jejím potírání. S rostoucím technologickým pokrokem se metody kybernetických útoků

[5] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů, Česká republika*. 2014, částka 77, s účinností od 1. ledna 2015.
[6] SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 34.

neustále vyvíjejí, což klade vysoké nároky na orgány činné v trestním řízení, bezpečnostní složky i legislativu.

V rámci odborné literatury lze na kybernetickou kriminalitu nahlížet jako na nedílnou součást širší agendy kybernetické bezpečnosti, jejíž klíčové prvky zahrnují kyberprostor, informační systémy, kritickou infrastrukturu a bezpečnostní opatření směřující k ochraně těchto prvků. Ucelený výklad základních pojmů, jako jsou kybernetický prostor, kybernetické hrozby, incidenty či ransomware, uvádí kolektiv autorů Policejní akademie ČR, přičemž akcentuje propojení kybernetické kriminality se strategickým řízením rizik a nutností aktivní obrany v prostředí digitálních technologií. Vymezení těchto pojmů je významné nejen z hlediska prevence a reakce na kybernetické útoky, ale i z pohledu právní klasifikace a určení odpovědnosti při páchání trestné činnosti v kyberprostoru[7].

Kybernetická kriminalita může být obecně rozdělena do dvou hlavních kategorií:

1. **Trestná činnost zaměřená na digitální infrastrukturu** – zahrnuje útoky na informační systémy, jako jsou hacking[8], distribuované útoky na dostupnost služeb (z anglického Distributed Denial of Service – dále jen "DDoS") či šíření škodlivého softwaru (malware, ransomware).

2. **Trestná činnost využívající digitální technologie k dosažení podvodného nebo jiného protiprávního zisku** – zahrnuje zejména kybernetické podvody, krádeže identity, neoprávněné platební transakce či zneužívání osobních údajů.

Vzhledem k zaměření této práce bude podrobně rozebrána druhá kategorie, tedy kybernetické podvody, které představují jednu z nejrozšířenějších forem digitální kriminality.

[7] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020, s. 33–35.
[8] HALAS, N. *Dokazovanie počítačovej kriminality*. Praha, 2023, s. 23-26.

2.3 Kybernetické podvody

Kybernetické podvody patří mezi nejčastější a zároveň nejzávažnější formy kybernetické kriminality. Pachatelé při nich využívají digitální technologie k manipulaci a oklamání jednotlivců či organizací s cílem finančního nebo jiného prospěchu. Motivací k tomuto jednání je nejen potenciál vysokého zisku, ale i široký dosah k obětem. Anonymita poskytovaná internetovým prostředím, relativní jednoduchost navázání kontaktu s obětí, činí z online podvodů mimořádně atraktivní a efektivní formou trestné činnosti.[9] Tyto podvody mohou mít různé podoby, od podvodných e-mailů a phishingových kampaní až po sofistikované manipulace s online bankovnictvím.

Kybernetické podvody jsou charakteristické několika klíčovými aspekty:

- **Využití psychologických technik** – pachatelé často cílí na lidskou důvěřivost, nedostatečné povědomí o bezpečnostních hrozbách či časový tlak, který oběti nutí jednat impulsivně.
- **Anonymita pachatelů** – díky využití sofistikovaných metod (např. falešných identit, šifrování nebo dark webu) je obtížné pachatele identifikovat a dopadnout.
- **Rychlost a globální dosah** – digitální podvody se šíří rychle a mohou zasáhnout velký počet obětí napříč různými státy, což komplikuje vyšetřování a právní postih.

2.3.1 Typy kybernetických podvodů

V rámci kybernetických podvodů lze identifikovat několik klíčových kategorií, které se odlišují svou metodikou i dopadem na oběti:

- **Phishing a sociální inženýrství** – techniky zaměřené na manipulaci obětí za účelem získání citlivých informací (hesla, bankovní údaje). Podle Kožíška a Píseckého se v případě sociálního inženýrství jedná o způsob manipulace lidí s cílem přimět je k určitému jednání nebo získat konkrétní informaci[10]. Ve většině případů útočník s obětí nevstupuje do osobního kontaktu a využívá prvky manipulace a přesvědčování. Tyto útoky mohou být prováděny nahodile nebo cíleně vůči konkrétním

[9] CLOUGH, J. *Principles of Cybercrime*. 2. vydání, Cambridge, 2015, s. 372-373.
[10] KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha, 2016, s. 37.

jednotlivcům. Sociální inženýři se navíc neustále učí ze svých chyb a své techniky průběžně zdokonalují a přizpůsobují aktuálnímu prostředí[11].

- **Podvody s falešnými webovými stránkami a e-shopy:** vytváření podvodných webů napodobujících webové stránky důvěryhodných institucí nebo e-shopů za účelem vylákání plateb nebo osobních údajů[12].
- **Podvody spojené s online bankovnictvím a platebními systémy:** neoprávněné převody financí, falešné platební transakce či zneužití digitálních měn.
- **Podvody na sociálních sítích a inzertních platformách:** například falešné investiční nabídky, vylákání peněz pod záminkou nouzové situace nebo zneužití platebních karet na podvržených stránkách dopravců.

Zmapování těchto forem podvodů včetně analýzy jejich dopadů bude klíčovou součástí této práce. Důraz bude kladen na faktory, které ovlivňují rozhodování pachatelů, přičemž jako hlavní analytický rámec bude použita teorie racionální volby.

[11] ŠULC, V. *Kybernetická bezpečnost*. Plzeň, 2018, s. 30-31.
[12] HALAS, N. *Dokazovanie počítačovej kriminality*. Praha, 2023, s. 29-31.

3 Právní rámec kybernetických podvodů

Kybernetická bezpečnost představuje širokou oblast, která se soustředí nejen na technická opatření a nástroje, ale také na strategické přístupy, metodické rámce a aktivní zapojení lidského faktoru[13]. Nedílnou součástí této oblasti je rovněž identifikace a ochrana klíčových objektů a struktur v kyberprostoru. Právní rámec pak určuje, jakým způsobem jsou tyto aspekty upraveny, jaká pravidla a odpovědnosti z nich vyplývají pro jednotlivé subjekty.

Kybernetické podvody představují významný problém současné digitální společnosti, proto je jejich právní úprava klíčovým nástrojem v boji proti tomuto fenoménu. Regulace kyberkriminality se v jednotlivých zemích liší, ale obecně se opírá o národní trestní zákoníky, mezinárodní úmluvy včetně právních předpisů Evropské unie. Tato kapitola se zaměřuje na právní vymezení kybernetických podvodů v České republice, jejich postižitelnost podle mezinárodních dokumentů a odpovědnost provozovatelů digitálních služeb.

3.1 Právní úprava kybernetických podvodů v České republice

V Českém právním řádu trestné činy primárně upravuje zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „**trestní zákoník**“). Pro účely této práce budou zohledněna vybraná ustanovení trestního zákoníku, která se vztahují k problematice kybernetických podvodů. Konkrétně jde o § 209 trestního zákoníku (trestný čin podvod), § 230 trestního zákoníku, § 230 trestního zákoníku (trestný čin neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací) a § 234 trestního zákoníku (trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku).

[13] KREMLING, J., SHARP PARKER, A. M. *Cyberspace, Cybersecurity, and Cybercrime*. Los Angeles, 2017, s. 23.

3.1.1 Podvod

Podle § 209 odst. 1 trestního zákoníku se trestného činu podvod obecně dopustí ten, „*kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci*“[14].

Podvod je trestný čin patřící mezi majetkové delikty, jehož smyslem je ochrana cizího majetku před neoprávněným obohacením pachatele nebo jiné osoby na úkor poškozeného. K naplnění skutkové podstaty dochází tehdy, pokud pachatel s cílem získat prospěch uvede jinou osobu v omyl, využije jejího omylu nebo zamlčí podstatné skutečnosti, v důsledku čehož dojde k neoprávněnému zásahu do majetku poškozeného, který utrpí majetkovou újmu[15].

Trestní zákoník rozlišuje různé formy podvodu v závislosti na výši způsobené škody a okolnostech jeho spáchání. Mezi přitěžující faktory patří například opakované spáchání podvodu, jednání v rámci organizované skupiny, zneužití postavení osoby, která má povinnost chránit majetkové zájmy poškozeného, nebo páchání podvodu za mimořádných okolností, jako je válečný stav či živelní pohroma. Výše trestu se odvíjí od společenské škodlivosti činu a rozsahu způsobené škody, přičemž zákon stanoví trestní sazby od několika měsíců až po deset let odnětí svobody.[16]

3.1.2 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

Trestného činu podle § 230 trestního zákoníku se obecně dopustí ten:

„*(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*

(2) Kdo zasáhne do počítačového systému nebo nosiče informací tím, že a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací, b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní

[14] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů, Česká republika*. 2009, částka 11, s účinností od 1. ledna 2010.
[15] ŠÁMAL, P. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 2638–2686.
[16] ŠÁMAL, P. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 2638–2686.

neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží nebo přenese data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci"[17].

Podle Gřivny a Dvořáka, autorů komentáře k § 230 trestního zákoníku[18], se neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací řadí mezi trestné činy ohrožující bezpečnost digitálních dat a systémů. Toto ustanovení chrání důvěrnost, integritu, dostupnost dat uložených v počítačových systémech a na nosičích informací, přičemž postihuje jak samotný neoprávněný přístup k těmto systémům, tak i různé formy manipulace s těmito daty.

Trestní zákoník stanoví několik forem tohoto trestného činu. Neoprávněným přístupem se rozumí situace, kdy pachatel překoná bezpečnostní opatření, čímž získá přístup k počítačovému systému nebo jeho části. Pokud následně neoprávněně užije, vymaže, poškodí či pozmění data, provede jiný zásah do technického nebo programového vybavení systému, dopouští se kvalifikované skutkové podstaty.

Zákon přihlíží i k závažnosti činu – přitěžující okolnosti zahrnují úmysl způsobit škodu, získání neoprávněného prospěchu, útoky na systémy strategického významu, způsobení rozsáhlé hospodářské škody. Výše trestních sazeb se pohybuje od několika měsíců až po osm let odnětí svobody v případě způsobení škody velkého rozsahu nebo spáchání organizovanou skupinou.

Ustanovení § 230 trestního zákoníku poskytuje právní základ pro postih široké škály kybernetických útoků, zejména neoprávněného přístupu do počítačových systémů (hacking), šíření škodlivého softwaru (malware), ransomware útoků, DDoS útoků či napadení kritické infrastruktury a strategických systémů.

[17] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů, Česká republika.* 2009, částka 11, s účinností od 1. ledna 2010.
[18] ŠÁMAL, P. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 2949-2970.

3.1.3 Neoprávněné opatření, padělání a pozměnění platebního prostředku

Trestného činu podle § 234 trestního zákoníku se obecně dopustí ten:

„*(1) Kdo sobě nebo jinému bez souhlasu oprávněného uživatele opatří, zpřístupní, přijme nebo přechovává platební prostředek, který umožňuje výběr hotovosti nebo převod peněžních prostředků anebo virtuálních aktiv používaných namísto peněžních prostředků (dále jen „platební prostředek“) a který náleží jinému, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*

(2) Kdo sobě nebo jinému opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek, bude potrestán odnětím svobody na jeden rok až pět let.

(3) Kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý nebo platný, nebo kdo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný, bude potrestán odnětím svobody na tři léta až osm let.

Kybernetické podvody často zahrnují zneužití platebních prostředků (např. podvody s kreditními kartami, neoprávněné převody z bankovních účtů). Tento trestný čin postihuje jak falšování platebních karet, tak zneužívání elektronických platebních údajů“[19].

Toto ustanovení chrání důvěryhodnost a bezpečnost platebního styku, a to jak v souvislosti s fyzickými, tak i elektronickými platebními prostředky. Mezi přitěžující okolnosti patří spáchání činu organizovanou skupinou nebo ve značném rozsahu, kdy se trestní sazba zvyšuje na pět až deset let odnětí svobody. Pokud se trestného činu dopustí organizovaná skupina působící ve více státech, nebo je čin spáchán ve velkém rozsahu, může trestní sazba dosáhnout osmi až dvanácti let odnětí svobody. Trestní zákoník tímto ustanovením postihuje různé formy kriminality v oblasti platebního styku, včetně neoprávněného přístupu k cizím finančním prostředkům, falšování platebních karet, zneužívání elektronických platebních systémů a podvodných transakcí[20].

[19] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů, Česká republika.* 2009, částka 11, s účinností od 1. ledna 2010.
[20] ŠÁMAL, P. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 3006-3051.

3.2 Mezinárodní a evropský právní rámec

3.2.1 Budapešťská úmluva o kyberkriminalitě (2001)[21]

Budapešťská úmluva o kyberkriminalitě (Cybercrime Convention) je první mezinárodní dohoda, která definuje a kriminalizuje určité činy v kyberprostoru. Mezi hlavní ustanovení patří:

- trestní postih **neoprávněného přístupu k počítačovým systémům,**
- postih **podvodného získání a zneužití osobních údajů,**
- povinnost signatářských států (včetně ČR) zavést právní nástroje umožňující vyšetřování kybernetických trestných činů napříč státními hranicemi.

Česká republika je signatářem této úmluvy, její ustanovení jsou implementována v českém trestním právu (např. zákon o kybernetické bezpečnosti).

3.2.2 Směrnice Evropského parlamentu a Rady 2019/713[22]

Tato směrnice o boji proti podvodům a padělání bezhotovostních platebních prostředků zavazuje členské státy EU ke kriminalizaci kybernetických podvodů souvisejících s:

- neoprávněným přístupem k bankovním účtům,
- krádeží digitálních identit a osobních údajů,
- zneužitím kryptoměn k trestné činnosti.

Státy EU, včetně České republiky, musely tuto směrnici implementovat do svých národních právních řádů.

[21] EUR-LEX. *Úmluva o kyberkriminalitě (Budapešťská úmluva)* [online]. Evropská unie, [cit. 2025-02-26]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=23>.

[22] EVROPSKÁ UNIE. *Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů a padělání bezhotovostních platebních prostředků a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV* [online]. EUR-Lex, [cit. 2025-02-26]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32019L0713>.

3.3 Odpovědnost provozovatelů digitálních platforem a institucí

Kybernetické podvody se často odehrávají **na digitálních platformách**, jako jsou sociální sítě, e-shopy nebo internetové bankovnictví. Z tohoto důvodu se legislativa zaměřuje i na **odpovědnost provozovatelů těchto služeb**.

3.3.1 Povinnosti bank a finančních institucí

Banky a platební instituce mají zákonnou povinnost chránit klienty před kybernetickými podvody. Mezi jejich hlavní povinnosti patří:

- **Dvoufaktorová autentizace (2FA)** – povinná při online platbách (nařízení PSD2)[23].
- **Monitorování podezřelých transakcí** – banky musí vyhodnocovat neobvyklé aktivity na účtech klientů.
- **Odpovědnost za podvodné transakce** – pokud dojde k neautorizované platbě a klient ji nahlásí včas, banky mají povinnost vrátit finanční prostředky.

3.3.2 Odpovědnost digitálních platforem

Digitální platformy, zejména sociální sítě, inzertní a video portály, hrají v oblasti kybernetických podvodů ambivalentní roli. Na jedné straně slouží jako prostředek ke sdílení informací a komunikaci, na straně druhé jsou často **zneužívány k šíření podvodných kampaní**, falešných reklam, deepfake videí, škodlivých odkazů.

Z bezpečnostně-právního hlediska se v posledních letech zvyšuje tlak na **aktivní odpovědnost provozovatelů platforem**. Směrnice a nařízení EU – zejména **Digital Services Act** (dále jen "DSA") – zavazují velké platformy k větší proaktivitě při odhalování a odstraňování škodlivého obsahu. V případě opakovaného porušování DSA mohou být uloženy sankce až do výše 6 % celosvětového obratu společnosti.[24]

[23] EUR-LEX. *Revidovaná pravidla pro platební služby v EU* [online]. [cit. 2025-02-27]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/revised-rules-for-payment-services-in-the-eu.html?fromSummary=24>.

[24] EUROPEAN COMMISSION. *The Digital Services Act package* [online]. [cit. 2025-02-27]. Dostupné z WWW: <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>.

Přesto praxe ukazuje, že odstranění podvodných příspěvků bývá často **pomalejší než šíření samotného obsahu**. Například podle Europolu jsou deepfake podvody či falešné investiční reklamy běžně zobrazovány i několik dní, než jsou staženy[25].

Z hlediska bezpečnostní praxe Policie ČR je spolupráce s platformami často zdlouhavá a nedostatečně operativní. V řadě případů je identifikace pachatele znemožněna anonymitou a mezinárodním rozměrem platformy, neboť pachatelé často využívají služeb anonymizérů a virtuálních privátních sítí[26] (dále jen "VPN") odkazujících se do zemí, které na žádosti o identifikaci uživatele IP adresy buď nereagují, nebo reagují velmi laxně.

Do budoucna lze očekávat:

- nárůst **automatizace detekce podvodného obsahu pomocí AI** (např. detekce vizuální manipulace),
- **zavádění standardů odpovědnosti** za ověřování identity zadavatelů reklam,
- zvýšenou podporu **preventivních informačních kampaní**, iniciovaných přímo platformami ve spolupráci s bezpečnostními složkami.

[25] EUROPOL. *Cybercrime: The risks of the digital age* [online]. European Union Agency for Law Enforcement Cooperation, 2023 [cit. 2025-02-27]. Dostupné z WWW: <https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-risks-of-digital-age>.
[26] MICROSOFT. *Co je VPN?* [online]. Microsoft Azure, [cit. 2025-02-27]. Dostupné z WWW: <https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-vpn>.

4 Motivace a strategie pachatelů kybernetických podvodů

Digitalizace a globální propojení prostřednictvím internetu přinesly nesčetné výhody, avšak zároveň otevřely nové příležitosti pro nelegální aktivity, mezi něž patří i kybernetické podvody. Tato kapitola se zaměřuje na analýzu motivací, které vedou pachatele k páchání kybernetických podvodů, a na strategie, jež tyto osoby využívají k dosažení svých cílů. Pochopení těchto aspektů je klíčové pro tvorbu účinných preventivních opatření a bezpečnostních protokolů, které mohou snížit riziko a následky útoků.

4.1 Motivace pachatelů kybernetických podvodů

4.1.1 Teorie racionální volby (Rational Choice Theory)

TRV vychází z předpokladu, že jednotlivci se rozhodují na základě kalkulace nákladů a přínosů, přičemž volí takové jednání, které jim přináší maximální užitek při minimálním riziku[27]. Tento přístup je široce využíván v ekonomii a kriminologii k analýze rozhodovacích procesů, včetně motivace pachatelů kybernetických podvodů.

V kontextu kyberkriminality lze chování pachatelů interpretovat jako **racionální kalkulaci očekávaných přínosů a rizik**. Při rozhodování zvažují zejména:

- **pravděpodobnost odhalení a postihu** – úroveň zabezpečení cíle, efektivitu vymáhání práva, mezinárodní spolupráci při stíhání kyberkriminality,
- **možné zisky** – nejen finanční, ale i informační (např. přístup k databázím, osobním údajům) či reputační (status v hackerské komunitě),
- **náklady na provedení podvodu** – požadované technologické nástroje, časovou náročnost, nutnou míru odborných dovedností.

Podle TRV se pachatelé rozhodují pro kybernetickou kriminalitu tehdy, pokud očekávaný zisk převyšuje riziko odhalení a související sankce. Nízká pravděpodobnost dopadení, možnost anonymního působení v přeshraničním prostředí a relativně vysoký

[27] ENCYCLOPAEDIA BRITANNICA. *Rational choice theory* [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.britannica.com/money/rational-choice-theory>.

potenciální výnos činí kybernetické podvody atraktivními ve srovnání s tradičními formami majetkové kriminality.

TRV poskytuje užitečný rámec pro návrh preventivních strategií v oblasti kybernetické kriminality. Z pohledu prevence a vymáhání práva lze na jejím základě formulovat účinná protiopatření, která snižují atraktivitu kybernetických podvodů:

- **zvyšování nákladů na spáchání podvodu** – například důslednější trestní postihy, vylepšené detekční mechanismy, mezinárodní spolupráce při stíhání kyberkriminality,
- **snižování očekávaného zisku** – lepší osvěta a školení uživatelů, implementace pokročilých bezpečnostních opatření, změna chování obětí (např. dvoufaktorová autentizace, opatrnost při sdílení údajů).

Přestože TRV nabízí cenné poznatky pro pochopení chování pachatelů kybernetických podvodů, **není jediným relevantním přístupem** k analýze kyberkriminality. Motivace pachatelů mohou být ovlivněny také **sociálními, psychologickými nebo ideologickými faktory**, které je nutné při prevenci zohlednit.

4.1.2 Teorie rutinních aktivit (Routine Activity Theory)

Podle této teorie kriminalita vzniká, když se setkají **motivovaný pachatel, vhodná oběť a nedostatečná ochrana.** Pachatelé zejména využívají:

- zranitelnosti v počítačových systémech nebo lidské chyby k získání neoprávněného přístupu,
- automatizované phishingové kampaně a malware umožňují oslovit velké množství obětí najednou.
- nedostatečnou prevenci či absenci právního postihu zvyšují počet kybernetických podvodů.

Teorie rutinních aktivit se zaměřuje na strukturu prostředí, kde se podvody odehrávají, na příležitosti, které zločincům umožňují úspěšně realizovat své útoky[28].

[28] SCIENCEDIRECT. *Routine Activity Theory* [online]. Elsevier, [cit. 2025-03-01]. Dostupné z WWW: <https://www.sciencedirect.com/topics/social-sciences/routine-activity-theory>.

4.1.3 Psychologické faktory kybernetických podvodů

Psychologické faktory hrají důležitou roli v tom, jak pachatelé vyhodnocují riziko a jakým způsobem oběti reagují na podvodné techniky. Mezi klíčové psychologické aspekty patří:

- **Kognitivní zkreslení** – například „optimismus bias“[29] způsobuje, že oběti podceňují riziko kyberpodvodu.
- **Emoční manipulace** – pachatelé využívají strach, časový tlak nebo pocit naléhavosti ke zvýšení pravděpodobnosti úspěchu podvodu.
- **Impulzivita** – některé oběti reagují impulzivně, aniž by si ověřily pravost zprávy či transakce.

Psychologický přístup pomáhá lépe pochopit, proč se některé oběti stávají terčem podvodů častěji než jiné a jak pachatelé využívají psychologických slabin k maximalizaci úspěšnosti svých útoků.

4.1.4 Propojení teorií a jejich aplikace na kybernetické podvody

Integrace teorie racionální volby, teorie rutinních aktivit a psychologických přístupů poskytuje komplexnější pohled na kybernetické podvody. Pachatelé nejen kalkulují náklady a přínosy (racionální volba), ale také těží z příležitostí a nedostatečné prevence (rutinní aktivity) a využívají psychologické slabiny obětí (kognitivní zkreslení, manipulace). Tento multidisciplinární pohled je klíčový pro efektivní prevenci při boji proti kyberkriminalitě.

Z hlediska behaviorální prevence je třeba zohlednit i klesající schopnost jednotlivců kriticky vyhodnocovat digitální informace, což úzce souvisí s fenoménem informačního přetížení. Porada a kol. upozorňují, že množství informací, kterým jsou uživatelé vystaveni, může vést k poklesu jejich schopnosti odlišit důvěryhodné zdroje od manipulativních a podvodných schémat[30].

[29] HORÁK, O. *Optimismus: kdy je výhodou, kdy nám škodí?* [online]. Praha: Psychologie.cz, 2012 [cit. 2025-03-01]. Dostupné z WWW: <https://psychologie.cz/optimismus-kdy-je-vyhodou-kdy-nam-skodi/>.
[30] PORADA, V., RAIS, K. a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: Pocta Vladimíru Smejkalovi*. Plzeň: Aleš Čeněk, 2021, s. 295-296.

Tab. 1: Srovnání teoretických přístupů

Teoretický přístup	Klíčové prvky	Aplikace na kybernetické podvody	Omezení
Teorie racionální volby	pachatelé kalkulují náklady a přínosy před spácháním trestného činu	pachatelé hodnotí rizika (odhalení, postihy) a výnosy (zisk z podvodu)	nezohledňuje emoční faktory a iracionální rozhodování
Teorie rutinních aktivit	Kriminalita vzniká, když se setká motivovaný pachatel, vhodná oběť, chybějící ochrana	Zvýšená online aktivita, slabá bezpečnost zvyšují pravděpodobnost úspěšného podvodu	Nezabývá se individuálním rozhodováním pachatelů
Psychologické faktory	Emoce, impulzivita, kognitivní zkreslení	Strach, důvěřivost a heuristiky mohou vést oběti k neuváženým rozhodnutím	Neřeší strukturální faktory kriminality (právní rámec, technická ochrana)

4.2 Strategie a taktiky pachatelů kybernetických podvodů

4.2.1 Sociotechnika a phishing

- Pachatelé manipulují obět tak, aby jim dobrovolně poskytla citlivé informace.
- Phishingové kampaně spočívají v rozesílání e-mailů s podvodným obsahem, jsou cíleny na široké spektrum příjemců (v řádech tisíců) s cílem oslovit co největší počet potencionálních obětí[31].
- Techniky jako vishing (hlasový phishing) a smishing (SMS phishing) jsou na vzestupu.

4.2.2 Technologické nástroje a exploatace zranitelností

- Pachatelé využívají zero-day zranitelnosti nebo neopravených systémových chyb k jejich následnému napadení.
- Automatizované skripty umožňují skenování webů a aplikací na slabiny.
- Škodlivý software umožňuje přímou manipulaci s daty nebo krádež informací.

4.2.3 Malware a ransomware

- Malware slouží ke krádeži přihlašovacích údajů nebo monitorování uživatelských aktivit.

- Ransomware zašifruje soubory (elektronické data) oběti a požaduje výkupné za jejich odemknutí. Podle Krále představuje specifickou formu škodlivého softwaru, jehož primárním cílem je vynucení finančního plnění od oběti prostřednictvím zastrašování či vydírání. Tento typ kybernetického útoku může mít různé podoby – v méně závažných případech je uživateli zobrazena výzva k úhradě údajné pokuty za domnělé porušení autorských práv nebo neoprávněné užívání softwaru. V kritičtějších scénářích ransomware šifruje soubory na infikovaném zařízení, čímž znemožňuje přístup k datům, přičemž neexistuje žádná

[31] HOLT, T. J., BOSSLER, A. M., SEIGFRIED-SPELLAR K. C. *Cybercrime and Digital Forensic: an introduction*.Third edition. London: 2022. s. 221.

jistota, že jejich zpřístupnění bude po zaplacení požadovaného výkupného skutečně umožněno[32].

Tyto útoky často cílí na instituce s kritickou infrastrukturou (nemocnice, úřady, firmy).

4.2.4 Distribuované útoky a botnety

DDoS je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a následnému pádu nebo nefunkčnosti a nedostupnosti služby nebo webové stránky pro uživatele[33].

Botnet je síť kompromitovaných zařízení (většinou počítačů) ovládaných útočníkem za účelem provádění kybernetických útoků. Takováto síť je často využívána k DDoS útoků, šíření spamu, malwaru, krádežím dat. Infekce zařízení probíhá pomocí škodlivého softwaru, přičemž majitel zařízení často netuší, že je jeho zařízení součástí botnetu. Mezi klíčová ochranná opatření patří aktualizace systému, použití silných hesel, antivirové ochrany[34].

Shrnutí:

- Útoky mohou vyřadit webové servery nebo poškodit infrastrukturu organizací.
- Často jsou využívány k vydírání (tzv. ransom DDoS útoky).
- Pachatelé rychle reagují na nová bezpečnostní opatření.
- Sdílení znalostí na dark webu umožňuje rychlou inovaci podvodných metod.
- Spolupráce v rámci hackerských komunit urychluje vývoj nových technik.

[32] KRÁL, M. *Bezpečný internet. Chraňte sebe i svůj počítač*. Praha, 2015, s. 14.
[33] MUDRÁKOVÁ, L. *Co je to DDoS útok a co o něm potřebujete vědět?* [online]. Dvojklik.cz, 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.dvojklik.cz/co-je-to-ddos-utok-a-co-o-nem-potrebujete-vedet/>.
[34] ESET. *Co je botnet?* [online]. ESET, 2015 [cit. 2025-03-01]. Dostupné z WWW: <https://www.eset.com/cz/botnet/>.

4.3 Příklady

4.3.1 Skupina Anonymous[35]

Skupina Anonymous, jejímž symbolem je maska Guye Fawkese, se řadí mezi nejznámější hackerská hnutí. Proslavila se řadou kybernetických útoků, mezi něž patří DDoS útoky, zveřejňování citlivých informací, neoprávněné zásahy do obsahu webových stránek nebo průniky do zabezpečených systémů. Její aktivity, kterými prosazuje své ideologické a politické cíle často balancují na hraně zákona.

4.3.2 WannaCry ransomware[36]

- Ransomware útok, který v roce 2017 infikoval stovky tisíc počítačů po celém světě, když využil zranitelnost systému Windows, kterou odhalila a zveřejnila skupina Shadow Brokers.
- Požadoval platby v bitcoinech výměnou za dešifrování souborů.

4.4 Shrnutí kapitoly

Motivace pachatelů kybernetických podvodů jsou rozmanité a zahrnují ekonomické, psychologické, ideologické i příležitostné faktory. Strategie pachatelů se neustále vyvíjejí a zahrnují jak technologické, tak sociální aspekty. Případové studie ukazují, že efektivní obrana proti kybernetickým podvodům vyžaduje kombinaci technických opatření, vzdělávání uživatelů, mezinárodní spolupráci.

[35] AKADEMIE VĚD ČESKÉ REPUBLIKY. *Hodní a zlí hackeři: Anonymous a hybridní válka* [online]. 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.avcr.cz/cs/fotoreportaze/Hodni-a-zli-hackeri-Anonymous-a-hybridni-valka/>.

[36] NÚKIB. *Ransomware WannaCry* [online]. Praha, 2017 [cit. 2025-03-01]. Dostupné z WWW: <https://nukib.gov.cz/cs/infoservis/hrozby/1455-ransomware-wannacry/>.

5 Preventivní přístupy a reakce na kybernetické podvody

Dynamický vývoj kybernetických podvodů vyžaduje komplexní preventivní přístup, který kombinuje legislativní opatření, pokročilé technologické nástroje, cílené vzdělávací programy zaměřené na uživatele i instituce.

5.1 Právní prevence

Striktnější regulace online platebních metod – zavedení přísnějších pravidel pro finanční transakce může snížit podvody spojené s platebními kartami a kryptoměnami.

Zvýšené postihy za kybernetické podvody – vyšší trestní sazby, efektivnější vymáhání práva mohou pachatelům zvýšit vnímané náklady podvodů, čímž sníží jejich atraktivitu.

Mezinárodní spolupráce – efektivní boj proti kybernetické kriminalitě vyžaduje spolupráci mezi státy, zejména v oblasti extradice a sdílení informací.

5.2 Technologická prevence

V oblasti technologické prevence je nutné reflektovat stále se vyvíjející spektrum kybernetických hrozeb, mezi které patří například sofistikované formy malwaru nebo ransomware. Tyto škodlivé kódy se v praxi zaměřují nejen na získání přístupu k citlivým datům, ale často vedou i k jejich zašifrování a následnému vydírání uživatelů. Závažným rizikem je také schopnost útočníků zneužít běžně používané technologie a jejich slabá místa k průniku do systémů organizací i jednotlivců. Vzhledem k této dynamice je klíčové zavádět komplexní bezpečnostní opatření, která zahrnují nejen antivirové a antimalwarové nástroje, ale také pravidelné aktualizace softwaru, omezení přístupových práv, segmentaci sítí jako klíčové obranné vrstvy[37].

[37] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020, s. 38–41.

Lze rozdělit na dvě hlavní témata:

- **Technické zabezpečení** – opatření na úrovni systémů a infrastruktury.
- **Uživatelská ochrana** – opatření související s chováním a bezpečnostními návyky uživatelů.

5.2.1 Technické zabezpečení

Firewally a systémy detekce narušení (IDS/IPS)[38]

- Moderní podnikové firewally umožňují detekci a blokování podezřelých síťových přenosů.
- Systémy IDS (Intrusion Detection Systems) a IPS (Intrusion Prevention Systems) analyzují síťový provoz a mohou v reálném čase detekovat neobvyklé vzory chování.

Umělá inteligence a strojové učení v detekci podvodů

- AI nástroje analyzují velké objemy dat a odhalují neobvyklé chování spojené s kyberpodvody.
- Bankovní instituce využívají algoritmy k detekci podvodných plateb na základě vzorců transakcí.
- AI systémy dokáží identifikovat podvodné e-maily dříve, než se dostanou k uživateli.

Biometrická autentizace a pokročilé identity management systémy

- Kromě hesel se stále častěji používají biometrické metody jako rozpoznání obličeje nebo otisků prstů.
- Multi-faktorová autentizace (MFA) s využitím biometriky snižuje riziko podvodného přihlášení.

Zero Trust Architecture (ZTA) a přístup na základě nejnižších oprávnění[39]

- Moderní bezpečnostní strategie Zero Trust předpokládá, že žádný uživatel nebo zařízení by neměl mít automatický přístup k síti bez ověření.

[38] VERSA NETWORKS. *What is IDS/IPS?* [online]. [cit. 2025-01-09]. Dostupné z WWW: <https://versa-networks.com/sd-wan/ids-ips/>.
[39] PALO ALTO NETWORKS. *What is a Zero Trust Architecture?* [online]. [cit. 2025-01-09]. Dostupné z WWW: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>.

- Omezení oprávnění znamená, že i při kompromitaci účtu útočník získá jen minimální přístup.

End-to-end šifrování a bezpečnost cloudových služeb

- Důraz na šifrování komunikace (např. TLS, E2EE) minimalizuje riziko odposlechu a manipulace s daty.
- Bezpečnostní opatření v cloudových službách, jako je zero-knowledge encryption, chrání data uživatelů před kompromitací na straně poskytovatele.

5.2.2 Uživatelská ochrana

Dvoufaktorová autentizace (2FA) a silná hesla

- Povinné používání 2FA (např. SMS kódy, autentizační aplikace) zásadně snižuje pravděpodobnost neoprávněného přístupu.
- Hesla by měla být dlouhá, unikátní a kombinovat znaky, čísla a speciální symboly.
- Používání správců hesel (password managers) eliminuje riziko opakovaného používání slabých hesel.

Ochrana proti phishingu a sociálnímu inženýrství

- Uživatelé by měli být pravidelně školeni v rozpoznávání phishingových e-mailů a podvodných webů.
- Webové prohlížeče mohou využívat rozšíření proti phishingu, která analyzují odkazy v reálném čase.
- Techniky jako **hover over links** (kontrola URL před kliknutím) a **e-mailová autentizace** (DMARC, SPF, DKIM) pomáhají omezit phishingové kampaně.

Ochrana proti malware a ransomware útokům

- Aktualizace softwaru a operačních systémů jsou klíčové pro ochranu před zneužitím zranitelností.
- Instalace **antimalwarových řešení**, která aktivně skenují a blokují podezřelé soubory nebo přílohy.
- Vytváření **záloh dat** offline i v cloudu, aby bylo možné obnovit informace v případě ransomware útoku.

Bezpečnost na sociálních sítích a ochrana osobních údajů

- Opatrnost při sdílení osobních údajů – kyberzločinci často využívají informace z veřejných profilů k cíleným útokům.
- Nastavení soukromí na sociálních sítích tak, aby nebyly osobní údaje snadno dostupné třetím stranám.
- Ověřování žádostí o přátelství a podezřelých zpráv (zejména ty obsahující odkazy nebo žádosti o finanční pomoc).

Simulované testování a školení zaměstnanců

- Společnosti by měly pravidelně provádět **phishingové testy**, aby zjistily, jak zaměstnanci reagují na podvodné e-maily.
- Interní bezpečnostní školení by mělo obsahovat praktické ukázky aktuálních kybernetických hrozeb.
- Podpora **kultury bezpečnosti** ve firmách, kdy zaměstnanci nejsou penalizováni za nahlášení podezřelých aktivit.

5.3 Vzdělávání a osvěta

Edukační kampaně – osvětové programy mohou uživatelům pomoci rozpoznat podvodné e-maily, falešné webové stránky a podvodné investiční nabídky.

Zvýšení povědomí o bezpečnostních hrozbách – firmy a organizace by měly školit své zaměstnance v oblasti kybernetické bezpečnosti.

Spolupráce s médii a sociálními sítěmi – šíření informací o nejnovějších hrozbách prostřednictvím veřejných kampaní.

Limity preventivních opatření

- **Adaptace kyberzločinců** – podvodníci neustále inovují své metody, čímž snižují efektivitu existujících bezpečnostních opatření.
- **Problém s osvětou** – mnoho uživatelů ignoruje doporučení o kybernetické bezpečnosti nebo podceňuje riziko.
- **Falešný pocit bezpečí** – implementace bezpečnostních opatření může vést ke snížení ostražitosti uživatelů.
- **Náklady na implementaci** – zavádění pokročilých bezpečnostních opatření je finančně náročné, zejména pro malé podniky.

Nárůst kybernetických útoků v EU: Podle analýzy společnosti BDO a dat Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) zaznamenala Evropská unie v první polovině roku 2023 třikrát více kybernetických útoků než ve druhé polovině předchozího roku.[40]

Nárůst kybernetických incidentů v ČR: NÚKIB evidoval v roce 2023 celkem 262 kybernetických incidentů, což představuje téměř dvojnásobný nárůst oproti 146 incidentům v roce 2022.[41]

Tyto údaje podtrhují rostoucí potřebu efektivního vzdělávání a osvěty v oblasti kybernetické bezpečnosti, aby se snížila zranitelnost organizací vůči stále častějším a sofistikovanějším útokům.

5.4 Dílčí a zevšeobecňující výstupy

Na základě předchozí analýzy jednotlivých forem a typologií kybernetických podvodů lze formulovat několik klíčových poznatků důležitých jak z hlediska bezpečnostně-právní teorie, tak aplikační praxe. V návaznosti na poznatky z teoretické části a empirického šetření byly identifikovány tyto dílčí výstupy:

Cílové skupiny pachatelů: Kybernetické podvody cílí na různé demografické skupiny. Zvlášť zranitelnými jsou senioři (vishing, spoofing), mladí dospělí (falešné investice, sociální sítě), a zaměstnanci institucí (BEC, CEO fraud). Je zřejmé, že pachatelé pečlivě selektují své cílové oběti podle jejich digitální gramotnosti a očekávané reakce.

Technologická versus behaviorální prevence: Technická opatření (dvoufaktorová autentizace, antiviry, síťové zabezpečení) zůstávají důležitá, avšak nestačí. Klíčová je behaviorální prevence: posílení schopnosti jednotlivce odolávat manipulaci a rozpoznat podvodné schéma. Efektivní ochrana vyžaduje kombinaci technických a psychosociálních nástrojů.

[40] BDO Czech Republic. *Vývoj kybernetických hrozeb v EU. Jakou roli hraje umělá inteligence?* [online]. [cit. 2025-01-19]. Dostupné z WWW: <https://www.bdo.cz/cs-cz/temata/digital/vyvoj-kybernetickych-hrozeb-v-eu-jakou-roli-hraje-umela-inteligence>.

[41] NÚKIB. *NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů* [online]. [cit. 2025-01-19] Dostupné z WWW: <https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu>.

Schopnost adaptace pachatelů: Kybernetická kriminalita má vysoce adaptivní charakter. Jakmile jsou určité formy podvodu široce medializovány, pachatelé přecházejí k sofistikovanějším metodám (např. z phishingu na quishing, z textové komunikace na deepfake video). Tato proměnlivost vyžaduje dynamický a prediktivní přístup v oblasti bezpečnosti.

Spolupráce institucí**:** Prevence kybernetických podvodů je efektivní pouze tehdy, je-li založena na **koordinaci mezi bezpečnostními složkami, bankovním sektorem a kybernetickými autoritami.** Kampaň #nePINdej![42] je ukázkou účinné meziinstitucionální osvěty.

Z výše uvedeného vyplývá, že úspěšná obrana proti kybernetickým podvodům nemůže být redukována na technické nástroje – vyžaduje propojení právních, bezpečnostních, psychologických a vzdělávacích přístupů.

5.5 Typové kazuistiky

5.5.1 Falešný bankéř (vishing)[43]

V roce 2023 obdržel seniorní klient jedné z předních českých bank telefonát z čísla, které bylo vizuálně shodné s oficiální zákaznickou linkou banky (tzv. spoofing čísla). Volající se představil jako pracovník bezpečnostního oddělení banky a uvedl, že byl detekován pokus o podvodný převod z klientova účtu. V důsledku navozeného dojmu urgentního ohrožení a profesionálně působící rétoriky volajícího klient postupně poskytl své přihlašovací údaje do internetového bankovnictví a následně, na žádost volajícího, nainstaloval program pro vzdálený přístup (např. AnyDesk), který umožnil útočníkovi převzít kontrolu nad jeho zařízením.

Během několika minut došlo k převodu finančních prostředků ve výši přesahující 780 000 Kč na zahraniční účet. Podvodník využil technik sociálního inženýrství, přičemž celý hovor působil jako standardní bezpečnostní proces banky. Případ byl vyšetřován Policií ČR, avšak pachatele se nepodařilo identifikovat.

Analýza případu: Jedná se o klasický případ kombinace spoofingu, sociální manipulace a zneužití technologií pro vzdálený přístup. Případ ilustruje zranitelnost

[42] ČBA. *Tisková zpráva: Kybertest a kampaň #nePINdej!*. Praha: ČBA, 2024.
[43] ČBA. *Tisková zpráva: Kybertest a kampaň #nePINdej!*. Praha: ČBA, 2024.

klientů vůči psychologickému nátlaku a nízkou informovanost o tom, že banka nikdy nepožaduje instalaci softwaru třetích stran. Z hlediska prevence je klíčová osvěta, implementace behaviorálních detekčních systémů a blokace známých nástrojů pro vzdálený přístup u klientských zařízení.

5.5.2 Deepfake investiční podvod s využitím AI a sociálních sítí[44]

V roce 2023 se na českých sociálních sítích začalo šířit video, ve kterém prezident republiky údajně veřejně doporučuje investici do nové státem podporované kryptoměnové platformy. Video využívalo technologie deepfake – tedy generativní umělou inteligenci, která dokáže věrně napodobit hlas i obličej konkrétní osoby. Vizuálně i jazykově působilo video autenticky, a mnozí uživatelé na jeho základě vstoupili na webové stránky odkazované v příspěvku.

Stránky byly vytvořeny tak, aby napodobovaly oficiální stránky vládní instituce a nabízely možnost registrace a investice. Uživatelé, kteří na stránky zareagovali, byli kontaktováni operátory, kteří s nimi vedli další komunikaci a přesvědčili je k převodu finančních prostředků. Škody se pohybovaly v řádech stovek tisíc korun. ČBA na případ oficiálně upozornila v rámci své osvětové kampaně a případ byl medializován.

Video bylo modifikováno a na možnost investování lákaly známí politici (např. Andrej Babiš, současný premiér vlády Petr Fiala apod.)

Analýza případu: Tento typ podvodu je ukázkou sofistikovaného zneužití důvěry a autority veřejně známých osob za využití technologií umělé inteligence. V bezpečnostně-právním kontextu se jedná o mimořádně obtížně postihnutelný čin, neboť je obtížné dohledat původce deepfake obsahu, a šíření je virální. Do budoucna bude nutné legislativně řešit odpovědnost za AI-generovaný obsah a podpořit vývoj nástrojů pro detekci deepfake.

[44] SEZNAM ZPRÁVY. *Prezident investuje do krypta? Deepfake video zneužívá jeho tvář* [online]. Praha: Seznam Zprávy, 2023 [cit. 2025-02-21]. Dostupné z WWW: <https://www.seznamzpravy.cz/clanek/deepfake-podvod-prezident>.

5.5.3 Ransomware útok na krajskou nemocnici[45]

Na podzim roku 2022 se krajská nemocnice v České republice stala obětí cíleného ransomwarového útoku. Útočníci pronikli do systému prostřednictvím nezabezpečeného e-mailového účtu zaměstnance a následně využili známé zranitelnosti v Exchange serveru, která nebyla aktuálně záplatována. V řádu hodin došlo k zašifrování rozsáhlé části IT infrastruktury nemocnice včetně přístupů k pacientským datům a dokumentaci. Útočníci zanechali výzvu k zaplacení výkupného v kryptoměně ve výši několika desítek tisíc eur s hrozbou zveřejnění citlivých dat. Incident způsobil vážné narušení provozu, bylo nutné dočasně omezit plánované operace a přejít na papírové vedení dokumentace. Zásah bezpečnostních složek a krizový štáb minimalizovaly dopady, avšak škody byly značné a následná obnova systémů trvala několik týdnů.

Analýza případu: Tento případ podtrhuje rizikovost kyberútoků na infrastrukturu kritické důležitosti, zejména v oblasti zdravotnictví. Ukazuje nutnost proaktivní správy aktualizací, školení zaměstnanců a zavedení technických opatření (segmentace sítí, zálohování, EDR nástroje). Z pohledu bezpečnostně-právního je klíčové, aby byly stanoveny minimální standardy zabezpečení pro instituce v kritické infrastruktuře.

[45] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti v České republice za rok 2022* [online]. Brno: NÚKIB, 2023 [cit. 2025-02-21]. Dostupné z WWW: <https://www.nukib.cz/cs/publikace-a-dokumenty/vyrocni-zpravy/>.

5.6 Syntéza doporučených opatření

Na základě analýzy jednotlivých forem kybernetických podvodů a rozboru nástrojů právní, technologické i behaviorální prevence lze formulovat soubor klíčových doporučení, která společně vytvářejí komplexní rámec ochrany před tímto druhem kriminality. Účinná prevence vyžaduje nejen dílčí technická řešení, ale především **koordinovanou strategii** zapojující státní instituce, soukromý sektor, vzdělávací systém i samotné uživatele.

Právní opatření:

- Posílení trestněprávní odpovědnosti za kybernetické podvody, včetně specifikace skutkových podstat a přísnějších sankcí.
- Legislativní ukotvení odpovědnosti digitálních platforem za obsah a chování uživatelů, především ve vztahu k podvodným reklamám a deepfake manipulacím.
- Rozšíření mezinárodní spolupráce v oblasti extradice, sdílení dat a jednotných postupů vyšetřování kybernetické kriminality.

Technologická opatření:

- Zavedení a standardizace víceúrovňové autentizace u všech finančních a citlivých digitálních služeb.
- Využití systémů umělé inteligence pro detekci anomálií, phishingu, deepfake a podvodného chování v reálném čase.
- Posílení infrastruktury veřejných institucí – segmentace sítí, pravidelné penetrační testy, školení zaměstnanců.

Edukace a osvěta:

- Povinné vzdělávání v oblasti kybernetické bezpečnosti na školách všech stupňů, s důrazem na rozpoznání podvodných schémat a správné digitální návyky.
- Cílené kampaně zaměřené na nejzranitelnější skupiny obyvatel (senioři, mladí dospělí), vedené ve spolupráci s bankami, policií a médii.
- Pravidelné testování zaměstnanců organizací formou simulovaných útoků (phishing, sociální inženýrství) a aktualizace vnitřních bezpečnostních směrnic.

Koordinační přístup:

- Zřízení specializovaných meziresortních pracovních skupin, které budou propojeny s odbornou veřejností, akademií a privátním sektorem.
- Sdílení dat o hrozbách a útocích v rámci národní bezpečnostní infrastruktury.
- Integrace preventivních nástrojů do digitálních platforem (automatizovaná upozornění, verifikace identity inzerentů, reporting škodlivého obsahu).

Tento rámec preventivních opatření reflektuje potřebu **multidisciplinární a adaptivní reakce** na měnící se podoby kybernetických podvodů. Pouze kombinací právní regulace, technologických inovací a systematické edukace lze efektivně čelit rizikům spojeným s digitalizací každodenního života.

Porada a kol. podtrhují význam aktivní role státu, který by měl přijmout odpovědnost za koordinaci prevence kybernetické kriminality napříč institucemi a zákonodárnou mocí[46].

[46] PORADA, V., RAIS, K. a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: Pocta Vladimíru Smejkalovi*. Plzeň: Aleš Čeněk, 2021, s. 296.

6 Kybernetická kriminalita na území ČR v letech 2021 až 2023

Empirická část práce vychází z principů fenomenologického přístupu, jehož cílem je hloubkové pochopení podstaty kybernetických podvodů prostřednictvím analýzy jejich projevů a determinant v konkrétním společenském a technologickém kontextu. Tato část bude kombinovat kvantitativní a kvalitativní rovinu poznání.

Na kvantitativní úrovni vychází analýza z údajů PČR, NÚKIB a ČBA, jež poskytují statisticky měřitelná data o četnosti, dynamice a strukturálních charakteristikách kybernetických podvodů v letech 2021–2023. Tyto informace reflektují nárůst incidentů, proměny v typu útoků a zasažených sektorů (včetně veřejné správy, zdravotnictví či finančního sektoru) i rozvoj metod používaných pachateli.

Zároveň bude uplatněna kvalitativní rovina přístupu, jejímž prostřednictvím je zkoumán vliv technologického vývoje – například nástupu umělé inteligence, dostupnosti nástrojů typu malware-as-a-service nebo rozšíření kryptoměn – na míru sofistikovanosti a podobu „modus operandi“ pachatelů. Empirická pozorování se tak zaměřují na způsob rozhodování pachatelů v kontextu teorie racionální volby a jejich motivaci, včetně ekonomického kontextu (např. inflace a zhoršení životní úrovně).

Cílem této části je nejen postihnout rozsah a charakter kybernetických podvodů v České republice, ale zároveň nabídnout aplikovaný vhled do způsobu, jakým technologický pokrok a socioekonomické faktory formují jejich incidence, strukturu a vývojové trendy.

Je však třeba dodat, že analýza byla omezena dostupností veřejných datových zdrojů, přičemž detailnější údaje od soukromých subjektů, zejména z bankovního sektoru, nebyly veřejně přístupné nebo nejsou systematicky zveřejňovány.

6.1 Kvantitativní analýza dat Policie ČR (2021–2023)

Tab. 2: Vývoj kybernetické kriminality (2021–2023)[47]

Rok	Celkový počet skutků	Meziroční změna (%)	Podvody (mezi osobami)	Padělání platebního prostředku	Neoprávněný přístup k počítačovému systému
2021	9 518	+ 17,8	4 087	—	1 682
2022	18 554	+ 94,9	7 727	4 283	2 575
2023	19 592	+ 5,6	8 495	5 515	1 687

V roce 2021 došlo k výraznému nárůstu kybernetické kriminality, kdy bylo zaznamenáno 9 518 skutků, což představovalo nárůst o 1 445 skutků (+17,8 %) oproti roku 2020, kdy bylo zaznamenáno 8 073 skutků. Mezi nejčastější formy patřily podvody mezi soukromými osobami (4 087 případů), neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla (1 682 případů). Dlouhodobě rostl počet případů hackingu (meziroční nárůst o 45 %) a pokračoval trend ransomwarových útoků. Zaznamenán byl také narůst počtu incidentů, které se jeví jako útoky cizí státní moci. Podle Zprávy o bezpečnostní situaci na území ČR za rok 2021[48] kybernetické kriminalitě nahrávalo nízké právní vědomí veřejnosti a nedostatečná regulace.

V roce 2022 pokračoval nárůst kybernetické kriminality, kdy bylo registrováno 10 965 skutků. Celkově pro rok 2022 byl charakteristický nárůst počtu registrovaných trestných činů o téměř 19 procent. Pachatelé v této oblasti využívali stále sofistikovanější softwarové nástroje k neoprávněnému získání finančních prostředků. Vláda v reakci na tento vývoj přijala koncepci rozvoje schopností Policie ČR v oblasti trestné činnosti páchané v kyberprostoru (2021–2025)[49].

V roce 2023 došlo k dalšímu nárůstu kybernetické kriminality, avšak tempo růstu se zpomalilo. Bylo zaznamenáno celkem 19 592 skutků (+1 038, +5,6 %). Nejčastěji

[47] zdroj: statistická data Ministerstva vnitra České republiky.
[48] MINISTERSTVO VNITRA ČR. *Statistiky kriminality – dokumenty* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://mv.gov.cz/clanek/statistiky-kriminality-dokumenty.aspx>.
[49] POLICIE ČESKÉ REPUBLIKY. *Dokumenty Policie České republiky* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://policie.gov.cz/clanek/dokumenty-policie-ceske-republiky.aspx>.

se jednalo o podvody mezi soukromými osobami (8 495 případů), neoprávněné opatření, padělání a pozměnění platebního prostředku (5 515 případů), neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla (1 687 případů). Kriminalita páchaná v kyberprostoru tvořila 10,8 % z celkové registrované kriminality v roce 2023, což je nárůst o 0,6 % oproti roku 2022. Významnou část incidentů tvořily DDoS útoky, v červnu 2023 došlo k nárůstu ransomware útoků. NÚKIB také registroval řadu phishingových kampaní. V reakci na rostoucí hrozby vznikla v roce 2023 pracovní komise (Republikový výbor pro prevenci kriminality)[50] pro koordinaci a spolupráci v prevenci kybernetické kriminality (Kyberkomise).

S rozvojem umělé inteligence lze předpokládat další nárůst sofistikovanější kybernetické kriminality. Z hlediska teorie racionální volby je patrná motivace pachatelů vidinou rychlého zisku s minimálním rizikem postihu.

6.2 Incidenty a aktivity podle NÚKIB[51]

V roce 2021 NÚKIB evidoval 157 kybernetických bezpečnostních incidentů (nárůst o 99 incidentů oproti roku 2020).

- Nejčastější typy útoků: phishing, podvodné e-maily, skenování sítí, s výrazným nárůstem ransomwaru.
- Klíčové incidenty: zneužití zranitelností ProxyLogon a ProxyShell, později Log4Shell (20 % všech incidentů roku 2021).
- Aktivní vzdělávání a osvěta: přes 33 800 proškolených uživatelů, spuštěn kurz „Kyber nemocnice!“.
- Došlo k prvnímu použití institutu ochranného opatření v historii úřadu.

V roce 2022 počet incidentů mírně klesl na 146, ale podíl incidentů v kritické infrastruktuře vzrostl téměř dvojnásobně.

- Phishing, spear-phishing, vishing a DDoS útoky patřily mezi hlavní vektory hrozeb.

[50] MINISTERSTVO VNITRA ČR. *Republikový výbor pro prevenci kriminality (RVPPK)* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://mv.gov.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx>.
[51] zdroj: statistická data NÚKIB

- Útoky v souvislosti s válkou na Ukrajině: DDoS útoky hacktivistických skupin (např. Killnet, Anonymous Russia).
- Incidenty převážně ve veřejném sektoru, zdravotnictví a soukromých organizacích.
- NÚKIB vydal 16 upozornění a 3 varování.

V roce 2023 došlo podle NÚKIB k 262 incidentům, což je 80% nárůst oproti předchozímu roku – historicky nejvíce.

- Nejčastější útoky: spear-phishing, vishing, quishing, DDoS, CEO podvody.
- Důvody nárůstu: hacktivismus, zejména proruské skupiny (NoName057(16)), a vyšší aktivita ransomwarových aktérů.
- NÚKIB detekoval také pokusy o průniky do sítí strategických institucí (pravděpodobně špionáž).
- Významná role AI: zneužívání generativní umělé inteligence v phishingových kampaních.
- Vzdělávací a osvětové aktivity: rekordních 67 997 proškolených uživatelů, školení, cvičení (např. TELCO23).

Dle statistik NÚKIB došlo mezi lety 2021–2023 k zdvojnásobení počtu incidentů (z 157 na 262), přičemž převládaly hrozby: ransomware, phishingové techniky a DDoS. Incidenty úzce souvisí s geopolitickou situací (válka na Ukrajině) a rozvojem technologií (zejména AI). Oslabení kapacit státu a nedostatek odborníků v oblasti kybernetické bezpečnosti nadále zůstává vážnou výzvou. NÚKIB zároveň realizuje penetrační testy, školení a kampaně zaměřené na zvyšování odolnosti veřejného sektoru. Četnost útoků ukazuje, že infrastruktura státu a samospráv je i nadále zranitelná.

Reakce NÚKIB: prevence, osvěta, strategická opatření (např. nový zákon o kybernetické bezpečnosti, projekt BIVOJ).

6.3 Zjištění České bankovní asociace

Podle údajů ČBA počet kybernetických útoků na klienty bank v roce 2024 vzrostl o 37 %. Za prvních sedm měsíců roku bylo napadeno více než 49 000 klientů, přičemž bankám se podařilo zachránit více než 4 miliardy korun. Přesto činily škody způsobené kyberpodvodníky přes 845 milionů Kč[52].

Typy útoků a techniky pachatelů:

- **Vishing**: podvodné telefonáty napodobující čísla banky.
- **Deepfake videa** a generativní AI: využívány k napodobení hlasu a tváře veřejně známých osob (např. prezident, politici) a jejich následné využití ve videu, které doporučuje investiční platfomu.
- **Investiční podvody**: cílené kampaně na sociálních sítích lákající na falešné výnosy.
- **Zneužití nástrojů pro vzdálený přístup**: např. AnyDesk, TeamViewer.

Reakce a aktivity ČBA:

- Společná kampaň **#nePINdej!** realizovaná s Policií ČR a NÚKIB: cílem je edukace veřejnosti, zejména zranitelných skupin (senioři, mladiství).
- Rozšíření edukace na nové platformy (Instagram, outdoor reklama, spoty v ČT a kinech).
- Nový obsah Kybertestu se zaměřením na **deepfake**, **phishing a AI** podvody. Test si dosud vyzkoušelo **360 000 lidí**, průměrné skóre bylo 73 %[53].

Role umělé inteligence

- AI je **oboustranným nástrojem**: využívána jak bankami k detekci rizik, tak podvodníky pro věrohodnější manipulaci.
- Banky analyzují **podezřelé chování klientů v reálném čase** díky AI algoritmům.

[52] zdroj: statistická data České bankovní asociace.
[53] ČESKÁ BANKOVNÍ ASOCIACE. *Kybertest 2023* [online]. [cit. 2025-03-04]. Dostupné z WWW: <https://www.cbaonline.cz/clanky/kybertest-2023>.

- AI je rovněž zapojena do preventivní edukace a marketingové komunikace kampaně #nePINdej!

Z dat a kampaní vyplývá, že bankovní sektor čelí stále sofistikovanějším útokům, přičemž zneužívání lidského faktoru zůstává klíčovým bodem. Pro efektivní prevenci je nezbytné propojit technická opatření s cílenou edukací veřejnosti.

- Varování před nárůstem tzv. vishingu – telefonických podvodů.
- Podvodníci využívají nástroje pro vzdálený přístup, kombinují je s kryptopodvody.
- Spolupráce ČBA s NÚKIB a Policií ČR na vzdělávacích kampaních a varování veřejnosti.

Bankovní sektor je klíčovým aktérem v oblasti prevence – kombinuje technologie s behaviorální analýzou a edukací klientů.

6.4 Europol – kybernetická kriminalita v mezinárodním kontextu

Problematika kybernetických podvodů je ve své podstatě transnacionální a je zřejmé, že četnost a proměna této trestné činnosti má nejen vnitrostátní dimenzi, ale je výrazně ovlivňována i širšími evropskými a globálními trendy. Cenným zdrojem poznatků je v tomto směru každoroční souhrnná zpráva Europolu Internet Organised Crime Threat Assessment (dále jen "IOCTA") a navazující tematické reporty.

Analýza zpráv IOCTA z let 2021[54], 2023[55] a 2024[56] ukazuje, že kybernetické podvody jsou stabilně klasifikovány jako jedna z nejzávažnějších a nejrozšířenějších forem kybernetické trestné činnosti v Evropě. Výrazným rysem současného vývoje je postupný přesun pachatelů k formám útoků, které vyžadují nízké technické dovednosti, avšak vykazují vysokou míru efektivity a zisku. Europol přitom konstatuje, že hlavními

[54] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2021* [online]. Haag: Europol, 2021 [cit. 2025-02-23]. Dostupné z WWW: <https://www.europol.europa.eu/publications-events/main-reports/iocta-2021>.
[55] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2023* [online]. Haag: Europol, 2023 [cit. 2025-02-25]. Dostupné z WWW: <https://www.europol.europa.eu/publications-events/main-reports/iocta-2023>.
[56] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2024* [online]. Haag: Europol, 2024 [cit. 2025-02-25]. Dostupné z WWW: <https://www.europol.europa.eu/publications-events/main-reports/iocta-2024>.

faktory jsou snadná dostupnost nástrojů (crime-as-a-service), anonymita prostředí a nízká pravděpodobnost odhalení.

Z hlediska konkrétních metod dominuje využití sociálního inženýrství, především v podobě investičních, pracovních či romantických podvodů. Europol opakovaně upozorňuje na výrazný vzestup takzvaného „pig butcheringu“ – dlouhodobých podvodných vztahů kombinovaných s falešnými investičními příležitostmi[57]. Významně se také prosazují podvody spojené s deepfake a umělou inteligencí, kdy jsou za účelem zvýšení důvěryhodnosti používány falešné vizuální a zvukové identity veřejně známých osob.

Zpráva IOCTA 2024 výslovně varuje před zneužitím generativních modelů (např. LLM – Large Language Models) v rámci phishingových a manipulačních kampaní. Například automatizovaně generované e-maily, personalizované podle cílové oběti, zásadně zvyšují účinnost podvodného jednání. S tímto trendem se lze již nyní setkat i na úrovni běžné trestné činnosti – např. při výslechu obětí podvodných výzev k převodům prostřednictvím mobilních aplikací, které působí velmi důvěryhodně.

Další oblastí, na kterou Europol upozorňuje, je růst affiliate modelů a brokerských služeb mezi pachatelskými skupinami. Například tzv. Initial Access Brokers prodávají přístup k napadeným systémům dalším subjektům, které následně realizují podvody, ransomware či zcizení údajů[58]. Dochází tak k fragmentaci pachatelů a větší profesionalizaci celého podvodného ekosystému. Tento trend odpovídá i zkušenostem z terénu, kdy oběti čelí kombinaci několika typů nátlaku – vishing, přesměrování na falešné stránky, vzdálený přístup, zcizení identity.

Europol zároveň konstatuje, že pachatelé ve většině případů volí racionálně nejvýhodnější způsob páchání trestné činnosti – s důrazem na ekonomický zisk, jednoduchost provedení a minimalizaci stopy. Tento závěr zcela koresponduje s předpoklady teorie racionální volby.

[57] EUROPOL. *Spotlight Report: Online Fraud Schemes*. Haag: Europol, 2023. [cit. 2025-03-11]. Dostupné z WWW: <https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023>.
[58] EUROPOL. *Spotlight Report: Cyber-attacks – The Apex of Crime-as-a-Service*. Haag: Europol, 2023. [cit. 2025-03-11]. Dostupné z WWW: <https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023>.

Z mezinárodního pohledu tedy lze potvrdit, že trendy identifikované v České republice (PČR, NÚKIB, ČBA) mají plnou relevanci i v rámci Evropské unie. Zároveň zůstává výzvou účinná předběžná identifikace a efektivní edukace potenciálních obětí, neboť techniky pachatelů se dynamicky vyvíjejí a překonávají tradiční bezpečnostní přístupy.

6.5 Shrnutí a interpretace zjištění

Z provedené analýzy dat čtyř relevantních zdrojů – PČR, NÚKIB, ČBA a Europolu – lze vysledovat několik jednotících prvků, které charakterizují současný stav kybernetických podvodů:

Motivace pachatelů je ve většině případů ryze ekonomická, přičemž pachatelé jednají na základě racionální volby, tj. poměřují potenciální zisk s rizikem odhalení a případného postihu.

Modus operandi se významně posunul od jednoduchých forem phishingu a podvodných e-shopů k pokročilým formám sociálního inženýrství – využívání deepfake, nástrojů vzdáleného přístupu a generativní umělé inteligence. Techniky pachatelů se stávají stále sofistikovanějšími.

Technologický vývoj (zejména nástup umělé inteligence, dostupnost nástrojů typu crime-as-a-service a zneužívání kryptoměn) umožňuje anonymnější a efektivnější útoky s minimálními vstupními náklady. Tím se snižuje prahová bariéra pro vstup do kyberkriminality a zvyšuje se konkurence mezi pachatelskými skupinami.

Rozdíly mezi sektory: data PČR a NÚKIB ukazují vyšší incidenci útoků ve veřejném sektoru a zdravotnictví, zatímco ČBA upozorňuje na zaměření pachatelů na bankovní klienty – zejména seniory a uživatele sociálních sítí. Europol tyto trendy potvrzuje v širším evropském měřítku.

Tyto zjištění potvrzují vhodnost zvoleného teoretického rámce práce (teorie racionální volby, teorie rutinních aktivit) a současně poskytují oporu pro návrh preventivních opatření, které budou představeny v závěru.

Tab. 3: Typické útoky podle zdrojů (PČR, NÚKIB, ČBA, Europol)

Typ útoku	PČR	NÚKIB	ČBA	Europol
Phising	✓	✓	✓	✓
Vishing	✓		✓	✓
Quishing				✓
Ransomware	✓	✓		✓
Deepfake		✓	✓	✓
BEC (Business Email Compromise)				✓

Tab. 4: Doporučená opatření dle cílových skupin

Cílová skupina	Technická opatření	Behaviorální opatření
Veřejnost	2FA, bezpečnostní software, aktualizace	Edukace, simulace útoků, rozpoznání rizik
Senioři	Zákaz instalací aplikací třetích stran, jednoduché návody	Pravidelní školení, nácvik reakcí na telefonní podvody
Instituce	Segmentace sítí, penetrační testy, školení zaměstnanců	Bezpečnostní politika, nastavení postupů krizové komunikace

6.6 Komparativní syntéza empirických zjištění

Porovnáním výstupů z jednotlivých analytických zdrojů lze identifikovat několik zásadních trendů a souvislostí:

Nárůst kvantity a kvality útoků: Jak vyplývá z údajů PČR a NÚKIB, mezi lety 2021–2023 došlo nejen k výraznému nárůstu počtu kybernetických incidentů (z 9 518 na téměř 20 000 ročně), ale zároveň ke zvýšení jejich technické i psychologické sofistikovanosti.

Posun od technických útoků k manipulaci oběti: Zatímco dříve převažovaly útoky na úrovni infrastruktury (např. DDoS), v současnosti dominuje zneužívání důvěry uživatelů. Tato změna je patrná ve statistikách všech zkoumaných subjektů a potvrzuje tezi, že nejslabším článkem bezpečnosti zůstává lidský faktor.

Zacílení na specifické cílové skupiny: Europol, stejně jako ČBA, uvádějí, že podvodníci volí oběti podle zranitelnosti – typicky jde o seniory, klienty bank, osoby s nižší digitální gramotností nebo oběti emocionální manipulace (např. romance scam, fake investments).

Globalizace kyberkriminality: Europol přináší důležitý kontext, podobné metody i cíle zaznamenávají členské státy EU napříč celým kontinentem. Formy podvodů jsou často sdíleny v rámci kybernetických tržišť a specializovaných skupin, což činí tradiční represivní opatření obtížně uplatnitelnými.

Z výše uvedeného vyplývá, že Česká republika není v oblasti kybernetických podvodů výjimkou – vývoj zde kopíruje evropské trendy. Z hlediska bezpečnostně-právní praxe je nutné akcentovat preventivní a vzdělávací strategie, které kombinují technická řešení s behaviorálním a psychologickým přístupem. Komparativní syntéza zároveň ukazuje, **že nejúčinnější prevencí je systémová odolnost, zvyšování digitální gramotnosti a schopnost adaptace bezpečnostních složek na nové metody útoků**.

Závěr

Ambicí předkládané práce bylo s využitím teoreticko-praxeologického přístupu detekovat příčiny kybernetických podvodů, a to zejména optikou teorie racionální volby s akcentem na finanční motivaci pachatelů a vliv technologického pokroku na jimi používané metody. Současně se práce zaměřila na objasnění nejčastějších forem a metod kybernetických podvodů v České republice, přičemž na základě provedené analýzy navrhla efektivní preventivní opatření orientovaná především na zvyšování povědomí uživatelů o těchto hrozbách.

Teoretická část práce primárně vymezila základní pojmy – kyberprostor, kybernetická kriminalita a právního rámce podvodného jednání v digitálním prostředí. Dále byly představeny tři teoretické přístupy – teorie racionální volby, teorie rutinních aktivit, psychologické modely chování pachatelů. Kombinace těchto přístupů poskytla multidimenzionální pohled na kybernetické podvody a umožnila lepší pochopení motivací pachatelů. Kybernetické podvody se jeví jako fenomén, který nelze interpretovat pouze z jedné perspektivy.

Hlavní empirická zjištění:

Empirická analýza kvantitativních dat od PČR, NÚKIB, České bankovní asociace a Europolu ukázala **výrazný nárůst kybernetických podvodů mezi lety 2021-2023**. Podvody prošly významnou evolucí, kdy tradiční phishingové útoky byly nahrazeny sofistikovanějšími metodami, včetně využití **deepfake technologií a generativní umělé inteligence**. Mezi hlavní závěry práce patří:

- **Rostoucí adaptabilita pachatelů**, kteří využívají anonymizační nástroje a rychle se přizpůsobují bezpečnostním opatřením.
- **Globalizace kyberkriminality**, kdy se metody podvodů sdílejí mezi skupinami pachatelů v různých státech.
- **Nedostatečná flexibilita právních a technologických opatření**, která často zaostávají za rychlostí inovací v oblasti kyberkriminality.

Úspěšnost pachatelů je ovlivněna nejen technologickým náskokem, ale především **nízkou úrovní bezpečnostního povědomí uživatelů**, kteří často nedokážou rozpoznat manipulační techniky. Digitální prostředí navíc vyžaduje vysokou úroveň kognitivního vnímání rizik, což pachatelé efektivně využívají.

Praktické dopady a doporučení:

Na základě kombinace teoretických a empirických poznatků byla formulována preventivní doporučení, která zahrnují **právní, technologická a edukační opatření**. Klíčovým prvkem těchto opatření je **posilování bezpečnostní gramotnosti občanů**, jež byla v rámci práce akcentována jako **jeden z nejslabších článků** obrany proti digitálním podvodům.

Práce nabídla teoreticky ukotvený a empiricky podložený pohled na dynamiku kybernetických podvodů v ČR, deskripci aktuální situace, spojila poznatky z teorie a praxe, nabídla konkrétní návrhy využitelné pro bezpečnostní praxi, tvorbu metodik i preventivní kampaně. Výsledky práce lze prakticky využít při prevenci kyberkriminality v bankovním sektoru, při školení bezpečnostních složek nebo vzdělávacích kampaních zaměřených na kybernetickou gramotnost.

Téma kybernetických podvodů je mimořádně aktuální a prakticky významné. Zpracování práce mi umožnilo propojit vlastní profesní zájem s hlubším odborným vhledem. Zkušenosti získané tvorbou práce považuji za cenný základ pro další profesní i studijní rozvoj v oblasti bezpečnostní politiky a kybernetické kriminality.

Seznam použitých zdrojů

Literární zdroje

1. CLOUGH, J. *Principles of Cybercrime*. 2. vydání. Cambridge: Cambridge University Press, 2015. 579 s. ISBN 978-11-0703-457-0.
2. GIBSON, W. *Neuromancer*. Překlad Ondřej Neff. 1. vydání. Plzeň: Laser, 1992. 234 s. ISBN 80-85601-27-3.
3. GŘIVNA, T., RICHTER, M., ŠIMÁNOVÁ, H. (ed.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. 440 s. ISBN 978-80-87284-95-7.
4. HALAS, N. *Dokazovanie počítačovej kriminality*. Praha: Leges, 2023. 140 s. ISBN 978-80-7502-681-1.
5. HOLT, T. J.; BOSSLER, A. M. a SEIGFRIED-SPELLAR, K. C. *Cybercrime and Digital Forensics: an introduction*. Third edition. London: Routledge, Taylor & Francis Group, 2022. 790 s. ISBN 978-0-367-36007-8.
6. KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. 330 s. ISBN 978-80-7251-505-9.
7. KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. 562 s. ISBN 978-80-88168-34-8.
8. KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3.
9. KRÁL, M. *Bezpečný internet. Chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. 184 s. ISBN 978-80-247-5453-6.
10. KREMLING, J., SHARP PARKER, A. M. *Cyberspace, Cybersecurity, and Cybercrime*. Los Angeles: Sage, 2017. 296 s. ISBN 978-1-5063-4725-7.
11. PORADA, V. a RAIS, K. a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. 1. vydání. Brno: CERM, akademické nakladatelství, 2021. 466 s. ISBN 978-80-7623-065-1.
12. SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. 429 s. ISBN 978-80-7623-068-2.
13. SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Aleš Čeněk, s.r.o., 2022. 1166 s. ISBN 978-80-7380-849-5.

14. ŠÁMAL, P. a kol. *Trestní zákoník: komentář*. 3. vydání. Praha: C. H. Beck, 2023. 4933 s. ISBN 978-80-7400-893-1.
15. ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, s.r.o., 2018. 148 s. ISBN 978-80-7380-737-5.

Elektronické zdroje

1. AKADEMIE VĚD ČESKÉ REPUBLIKY. *Hodní a zlí hackeři: Anonymous a hybridní válka* [online]. 2022 [cit. 2025-03-01]. Dostupné z WWW: <https://www.avcr.cz/cs/fotoreportaze/Hodni-a-zli-hackeri-Anonymous-a-hybridni-valka/>.
2. BDO Czech Republic. *Vývoj kybernetických hrozeb v EU. Jakou roli hraje umělá inteligence?* [online]. Praha [cit. 2025-01-19]. Dostupné z WWW: <https://www.bdo.cz/cs-cz/temata/digital/vyvoj-kybernetickych-hrozeb-v-eu-jakou-roli-hraje-umela-inteligence>.
3. ČESKÁ BANKOVNÍ ASOCIACE. *Kybertest 2023* [online]. [cit. 2025-03-04]. Dostupné z WWW: <https://www.cbaonline.cz/clanky/kybertest-2023>.
4. ENCYCLOPAEDIA BRITANNICA. *Rational choice theory* [online]. [cit. 2025-02-28]. Dostupné z WWW: <https://www.britannica.com/money/rational-choice-theory>.
5. ESET. *Co je botnet?* [online]. ESET, 2015 [cit. 2025-03-01]. Dostupné z WWW: <https://www.eset.com/cz/botnet/>.
6. EUR-LEX. *Revidovaná pravidla pro platební služby v EU* [online]. Evropská unie, [cit. 2025-02-27]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/revised-rules-for-payment-services-in-the-eu.html?fromSummary=24>.
7. EUR-LEX. *Úmluva o kyberkriminalitě (Budapešťská úmluva)* [online]. Evropská unie, [cit. 2025-02-26]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=23>.
8. EUROPEAN COMMISSION. *The Digital Services Act package* [online]. [cit. 2025-02-27]. Dostupné z WWW: <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>.

9. EUROPOL. *Cybercrime: The risks of the digital age* [online]. European Union Agency for Law Enforcement Cooperation, 2023 [cit. 2025-02-27]. Dostupné z WWW: <https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-risks-of-digital-age>.
10. EVROPSKÁ UNIE. *Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů a padělání bezhotovostních platebních prostředků a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV* [online]. EUR-Lex, [cit. 2025-02-26]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32019L0713>.
11. HORÁK, O. *Optimismus: kdy je výhodou, kdy nám škodí?* [online]. Praha: Psychologie.cz, 2012 [cit. 2025-03-01]. Dostupné z WWW: <https://psychologie.cz/optimismus-kdy-je-vyhodou-kdy-nam-skodi/>.
12. MICROSOFT. *Co je VPN?* [online]. Microsoft Azure, [cit. 2025-02-27]. Dostupné z WWW: <https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-vpn>.
13. MINISTERSTVO VNITRA ČR. *Republikový výbor pro prevenci kriminality (RVPPK)* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://mv.gov.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx>.
14. MINISTERSTVO VNITRA ČR. *Statistiky kriminality – dokumenty* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://mv.gov.cz/clanek/statistiky-kriminality-dokumenty.aspx>.
15. MUDRÁKOVÁ, L. Co je to DDoS útok a co o něm potřebujete vědět? In: *Dvojklik.cz* [online]. 20.4.2022, [cit. 2025-03-01]. Dostupné z WWW: <https://www.dvojklik.cz/co-je-to-ddos-utok-a-co-o-nem-potrebujete-vedet/>.
16. NÚKIB. *NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů* [online]. Praha [cit. 2025-01-19]. Dostupné z WWW: <https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/>.
17. NÚKIB. *Ransomware WannaCry* [online]. Praha, 2017 [cit. 2025-03-01]. Dostupné z WWW: <https://nukib.gov.cz/cs/infoservis/hrozby/1455-ransomware-wannacry/>.

18. PALO ALTO NETWORKS. *What is a Zero Trust Architecture?* [online]. [cit. 2025-01-09]. Dostupné z WWW: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>.
19. POLICIE ČESKÉ REPUBLIKY. *Dokumenty Policie České republiky* [online]. Praha [cit. 2025-03-03]. Dostupné z WWW: <https://policie.gov.cz/clanek/dokumenty-policie-ceske-republiky.aspx>.
20. SCIENCEDIRECT. *Routine Activity Theory* [online]. Elsevier, [cit. 2025-03-01]. Dostupné z WWW: <https://www.sciencedirect.com/topics/social-sciences/routine-activity-theory>.
21. VERSA NETWORKS. *What is IDS/IPS?* [online]. [cit. 2025-01-09]. Dostupné z WWW: <https://versa-networks.com/sd-wan/ids-ips/>.
22. WIKISOFIA. *William Gibson* [online]. [cit. 2025-01-07]. Dostupné z WWW: <https://wikisofia.cz/wiki/William_Gibson>.

Legislativní dokumenty

1. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 77, s účinností od 1. ledna 2015.
2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. 2009, částka 11, s účinností od 1. ledna 2010.

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- statistická data České bankovní asociace,
- statistická data Europolu,
- statistická data Národního úřadu pro kybernetickou a informační bezpečnost,
- statistická data Policie České republiky.

Seznam zkratek

AI	Artificial intelligece (umělá inteligence)
ČBA	Česká bankovní asociace
DDoS	Distributed Denial of Service
DSA	Digital Services Act
IOCTA	Internet Organised Crime Threat Assessment
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PČR	Policie České republiky
SMS	Short message service (služba krátkých textových zpráv)
TRA	Teorie rutinních aktivit
TRV	Teorie racionální volby
VPN	Virtuální privátní síť (z anglického Virtual Private Network)

Seznam tabulek

Seznam příloh

Příloha 1. STATISTICKÁ DATA POSKYTNUTÁ ČBA

	Q1 2023	Q2 2023	Q3 2023	Q4 2023
Počet napadených klientů	17 006	14 317	17 129	21 233
Celkový součet odčerpaných prostředků (včetně karetních transakcí), který představuje sumu škod banky a klientů. Do reálných škod nezahrnujeme platby zastavené na účtech dané instituce (vnitřní účty, účty money mules). Číslo zaokrouhlujeme na celé tisíce matematicky. (v Kč)	375 495 122	307 188 695	322 276 191	343 950 927

	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Počet napadených klientů	20 818	22 377	23 005	21 293
Celkový součet odčerpaných prostředků (včetně karetních transakcí), který představuje sumu škod banky a klientů. Do reálných škod nezahrnujeme platby zastavené na účtech dané instituce (vnitřní účty, účty money mules). Číslo zaokrouhlujeme na celé tisíce matematicky. (v Kč)	366 410 695	380 219 100	350 771 612	299 574 312

Sdělení ČBA k datům ze dne 7. 3. 2025: Vážený pane Danieli, veřejně dostupná data, která publikujeme na webu ČBA můžete pro potřeby své akademické práce využít. Pro přehlednost a kompletnost doplňujeme do přílohy dostupná a agregovaná data. K publikaci dochází kvartálně. A ačkoli jsme se na výměnu dat připravovali již od roku 2022, disponujeme daty od počátku roku 2023. Aktuální statistiky jsou složeny z výstupů 11 největších tuzemských bank, avšak mají spíše obecnou povahu. Detailnější kategorizaci výstupů nemáme jako Česká bankovní asociace k dispozici i například z důvodu odlišné metodologie jednotlivých bank, a tedy obtížné unifikaci

a shromažďování dat. Zajímavější analytiku dat budeme mít k dispozici pravděpodobně až v následujících letech díky plánovaným projektům v oblasti kybernetické bezpečnosti.

Lenka Trnková
Vedoucí sekretariátu výkonného ředitele

ČESKÁ BANKOVNÍ ASOCIACE I Budova Churchill II, Italská 69, 120 00 Praha 2