VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY

INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS

STANOVENÍ HODNOTY INFORMACÍ V PRŮMYSLOVÉM PODNIKU PRO AUDIT ISMS

DETERMINATION OF THE VALUE OF INFORMATION IN AN INDUSTRIAL ENTERPRISE FOR AUDIT ISMS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Šimon Orviský

AUTHOR

VEDOUCÍ PRÁCE — Ing. Jana Rozehnalová, M.Sc.

SUPERVISOR

BRNO 2026

Zadání bakalářské práce

Ústav:	Ústav výrobních strojů, systémů a robotiky
Student:	**Šimon Orviský**
Studijní program:	Strojírenství
Studijní obor:	Kvalita, spolehlivost a bezpečnost
Vedoucí práce:	**Ing. Jana Rozehnalová, M.Sc.**
Akademický rok:	2025/26

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Stanovení hodnoty informací v průmyslovém podniku pro audit ISMS

Stručná charakteristika problematiky úkolu:

Informace jsou vždy podstatnou komoditou podniku a tvoří velkou část podnikového know–how. Význam informace je stále pro podnik nepopíratelný. Podoba informace a množství generované jednotlivými podnikovými procesy se postupně vyvíjí se vrůstající digitalizace. K informaci je třeba přistupovat jako k podnikovému aktivu. Práce si klade za cíl identifikovat podnikové informace, přiřadit k nim vlastníka a zvolit nejlepší způsob jejich ohodnocení. Výstupem bude metodika hodnocení podnikových informačních aktiv.

Cíle bakalářské práce:

Popis současného stavu vědy v oblasti informační/kybernetické bezpečnosti.
Rešerše relevantních norem a legislativy EU / ČR.
Systémový rozbor řešené problematiky.
Návrh metodiky stanovení a ohodnocení informačních aktiv.
Vlastní závěry a/nebo doporučení pro další rozvoj řešené problematiky.

Seznam doporučené literatury:

ČERMÁK, Miroslav. Řízení informačních rizik v praxi, Brno: Tribun EU, 2009. ISBN 978-80-7399-731-1.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724.

ČSN ISO 55000. Management aktiv – Přehled, zásady a terminologie. 1. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2025/26

V Brně, dne

L. S.

doc. Ing. Petr Blecha, Ph.D., FEng. ředitel ústavu	doc. Ing. Jiří Hlinka, Ph.D. děkan fakulty

BSTRAKT

Bakalářská práce se zabývá stanovením hodnoty informací v průmyslovém podniku pro audit systému řízení bezpečnosti informací. Cílem práce je popis současného stavu vědy v oblasti informační a kybernetické bezpečnosti, rešerše relevantních norem a legislativy Evropské unie a České republiky, systémový rozbor řešené problematiky a návrh metodiky pro stanovení a ohodnocení informačních aktiv. Teoretická část popisuje aktuální stav kybernetické bezpečnosti v České republice, vymezuje základní pojmy podle zákona č. 264/2025 Sb., představuje principy systému řízení bezpečnosti informací, legislativní rámec transpozice směrnice NIS2 a relevantní mezinárodní normy řady ISO/IEC 27000 a ISO 55000. Praktická část přináší vlastní návrh metodiky založené na hodnocení informačních aktiv podle pětistupňové škály a tří atributů CIA, jejíž funkčnost je demonstrována na modelovém průmyslovém podniku. Robustnost metodiky je ověřena citlivostní analýzou. V závěrečné části jsou identifikovány limity navrženého řešení a formulována doporučení pro praktické nasazení metodiky v rámci auditu ISMS.

ABSTRACT

This bachelor's thesis deals with the valuation of information in an industrial enterprise for the purpose of an Information Security Management System audit. The aim of the thesis is to describe the current state of the art in the field of information and cybersecurity, to provide a review of relevant standards and legislation of the European Union and the Czech Republic, to conduct a systemic analysis of the subject matter, and to propose a methodology for the identification and valuation of information assets. The theoretical part describes the current state of cybersecurity in the Czech Republic, defines basic terms in accordance with Act No. 264/2025 Coll., presents the principles of the Information Security Management System, the legislative framework resulting from the transposition of the NIS2 Directive, and the relevant international standards of the ISO/IEC 27000 family and ISO 55000. The practical part introduces an original methodology based on the valuation of information assets using a five-point scale and the three CIA attributes, whose functionality is demonstrated on a model industrial enterprise. The robustness of the methodology is verified through a sensitivity analysis. The final part identifies the limitations of the proposed solution and formulates recommendations for the practical implementation of the methodology within the framework of an ISMS audit.

KLÍČOVÁ SLOVA

informační bezpečnost, kybernetická bezpečnost, ISMS, hodnocení aktiv, CIA triáda, NIS2, audit, průmyslový podnik

KEYWORDS

information security, cybersecurity, ISMS, asset valuation, CIA triad, NIS2, audit, industrial enterprise

BIBLIOGRAFICKÁ CITACE

ORVISKÝ, Šimon. *Stanovení hodnoty informací v průmyslovém podniku pro audit ISMS*. Online, bakalářská práce. Jana ROZEHNALOVÁ (vedoucí práce). Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2026. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/174326.

PODĚKOVÁNÍ

V první řadě mi dovolte poděkovat paní Ing. Janě Rozehnalové, M.Sc. za trpělivost, cenné rady, přátelský přístup při celé tvorbě této bakalářské práce. Rád bych také poděkoval rodině a přátelům za plnou podporu jak u studia, tak při psaní této bakalářské práce.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Jany Rozehnalové, M.Sc. a s použitím literatury uvedené v seznamu. V souladu se zásadami VUT uvádím, že jsem při zpracování práce použil nástroje generativní AI; použití je transparentně popsáno v části „Využití generativní AI“

V Brně dne 22. května 2026 ……

Orviský Šimon

OBSAH

1 ÚVOD 11

2 POPIS SOUČASNÉHO STAVU VĚDY V OBLASTI INFORMAČNÍ/KYBERNETICKÉ BEZPEČNOSTI 13

2.1 Vývoj informační bezpečnosti 13
2.2 Hrozby kybernetické bezpečnosti 13
2.3 Základní pojmy a názvosloví 14
2.4 Bezpečnost informací a CIA triáda 15
2.5 ISMS (Systém řízení bezpečnosti informací) 16
2.6 Legislativní rámec 17
2.7 Normy ISO 17
2.8 Aktiva a jejich klasifikace 18
2.9 Dělení aktiv 18
2.10 Hodnocení aktiv 19
2.11 Evidence aktiv 19
2.12 Garanti aktiv 19
2.13 Metody hodnocení aktiv 20
2.14 Nástroje pro hodnocení aktiv 20
2.15 Shrnutí 21

3 NÁVRH METODIKY STANOVENÍ A HODNOCENÍ INFORMAČNÍCH AKTIV 22

3.1 Úvod do navržené metodiky 22
3.2 Charakteristika vzorového průmyslového podniku 22
3.3 Postup hodnocení 22
3.4 Hodnotící stupnice a třídy aktiv 23
3.5 Aplikace metodiky na modelový průmyslový podnik 25
3.6 Citlivostní analýza 28
3.7 Souhrn výsledků aplikace metodiky 31

4 DISKUZE A DOPORUČENÍ 32

4.1 Diskuze výsledků aplikace metodiky 32
4.2 Limity navržené metodiky 33
4.3 Doporučení pro praktické nasazení 34

5 ZÁVĚR 37

6 SEZNAM POUŽITÝCH ZDROJŮ 41

7 SEZNAM ZKRATEK, SYMBOLŮ, OBRÁZKŮ A TABULEK 43

7.1 Seznam zkratek 43
7.2 Seznam tabulek 44
7.3 Seznam obrázků 44

1 ÚVOD

Informace patří mezi klíčové zdroje každé organizace a tvoří podstatnou součást jejího know-how. S postupující digitalizací podnikových procesů narůstá nejen objem zpracovávaných dat, ale také jejich strategická hodnota a citlivost. Informace již nelze chápat pouze jako podporu provozu, ale jako samostatné podnikové aktivum, které vyžaduje cílenou ochranu a systematickou správu.

S významem informací roste také počet a závažnost kybernetických hrozeb. Pravidelné zprávy Evropské agentury pro kybernetickou bezpečnost a Národního úřadu pro kybernetickou a informační bezpečnost ukazují, že v posledních letech dochází k posunu od plošných útoků k cíleným incidentům s vážnými dopady na chod organizací. V reakci na tento vývoj přijala Evropská unie směrnici NIS2, která byla v České republice transponována zákonem č. 264/2025 Sb. o kybernetické bezpečnosti, jenž společně s navazujícími vyhláškami výrazně rozšiřuje okruh povinných osob a zpřísňuje požadavky na bezpečnostní opatření.

Důležitou součástí systému řízení bezpečnosti informací (ISMS) je správné stanovení hodnoty jednotlivých informačních aktiv. Bez něj nelze efektivně prioritizovat bezpečnostní opatření ani provést kvalitní audit ISMS. Pro průmyslový podnik je tato problematika obzvláště významná, neboť kombinuje běžné kancelářské systémy se specifickými technologickými aktivy a know-how, jehož ztráta nebo narušení může mít fatální následky.

Cílem této bakalářské práce je popis současného stavu vědy v oblasti informační a kybernetické bezpečnosti, rešerše relevantních norem a legislativy Evropské unie a České republiky, systémový rozbor řešené problematiky, a především návrh metodiky stanovení a ohodnocení informačních aktiv pro průmyslový podnik. V závěru jsou formulovány vlastní závěry a doporučení pro další rozvoj řešené problematiky.

Práce je rozdělena do tří hlavních kapitol. Kapitola 2 se věnuje současnému stavu vědy v oblasti informační a kybernetické bezpečnosti, vymezuje základní pojmy podle aktuální legislativy, popisuje koncept ISMS a Demingova PDCA cyklu, představuje legislativní rámec na úrovni Evropské unie i České republiky a normy řady ISO/IEC 27000 a ISO 55000. Závěr teoretické kapitoly se věnuje klasifikaci a hodnocení informačních aktiv a existujícím nástrojům pro analýzu rizik, jako jsou CRAMM, EBIOS Risk Manager a Průvodce řízením aktiv a rizik vydaný NÚKIB.

Kapitola 3 představuje vlastní návrh metodiky pro hodnocení informačních aktiv průmyslového podniku. Obsahuje popis modelového podniku, na kterém je metodika demonstrována, postup hodnocení, hodnotící stupnice a třídy aktiv, aplikaci metodiky na konkrétní příklady aktiv a citlivostní analýzu, která ověřuje robustnost navrženého řešení.

Kapitola 4 obsahuje diskuzi dosažených výsledků, identifikaci limitů navržené metodiky a praktická doporučení pro její nasazení v reálném prostředí průmyslového podniku při auditu systému řízení bezpečnosti informací.

VYUŽITÍ GENERATIVNÍ AI

Při zpracování této bakalářské práce jsem využil nástroje generativní umělé inteligence.
Použité nástroje a jejich účel:

- Claude (Anthropic; model/verze: Opus 4.6; URL: https://claude.ai/), období: 2026-02-20–2026-05-22. Účel: Jazyková korektura / stylistické přeformulování mého textu

Rozsah a charakter použití:

- AI byla použita pouze jako podpůrný nástroj (inspirace/korektura/návrhy), bez přímého vložení výstupů.

Ověření a odpovědnost:

Výstupy generativní AI jsem kriticky ověřoval (Konzultace s vedoucím; Porovnání s odbornými zdroji / literaturou; Kontrola pomocí norem, legislativy, odborných článků a vedoucí.) a plnou odpovědnost za obsah práce nesu já.

2 POPIS SOUČASNÉHO STAVU VĚDY V OBLASTI INFORMAČNÍ/KYBERNETICKÉ BEZPEČNOSTI

V dnešní době, kdy se téměř veškerá komunikace a práce s daty přesouvá do digitálního prostředí, bezpečnost informací se stala jedním z nejdůležitějších témat. Firmy si sice uvědomují, že jejich data a informace mají velkou hodnotu, ale ne vždy jim věnují dostatečnou ochranu. Abychom mohli informace chránit, musíme vědět co chráníme a jakou to má hodnotu. Tato kapitola popisuje normy, legislativu, přístupy k identifikaci a hodnocení informačních aktiv.

2.1 Vývoj informační bezpečnosti

Firmy 20 let zpátky ukládaly dokumenty do šanonů, všechna data na jeden počítač. Informace se sdílely telefonicky nebo poštou. Doba se však posouvá rychle. Je třeba držet krok. Dnes se stává standardem, že se data ukládají v cloudu, zaměstnanci pracují z domova, všechny systémy jsou napojené na internet a navzájem propojené. Ať už se jedná o komunikaci účetních systémů se sklady, sklady s dodavateli nebo přístup dodavatelů do firemních systémů, firmy jsou na IT závislé. Když spadne systém, je zasažen provoz celé firmy. Digitalizace přináší firmám řadu výhod. Na druhou stranu s sebou také nese nechtěná rizika. Otevírá totiž více míst, kudy se útočník může dostat dovnitř. Zde však nestačí staré praktiky jako zamknout kancelář nebo najmout hlídače. Je potřeba zaměřit se na systémový přístup.

2.2 Hrozby kybernetické bezpečnosti

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) ve své výroční zprávě za rok 2025 analyzovala celkem 4 875 bezpečnostních incidentů. Útočníci využívají phishing jako primární metodu průniků. Phishing tedy tvoří přibližně 60 % pozorovaných případů. S pokroky v automatizaci vznikají služby jako Phishing-as-a-Service (PhaaS). Díky nim si i méně zkušený útočník může pořídit hotovou sadu a napadat slabá místa firem. Ransomware je ve zprávě označen za hrozbu s největším dopadem v EU. Útočník při něm zašifruje firemní data a za jejich odemčení požaduje výkupné. [1]

Pokud z evropské úrovně přejdeme ke konkrétní situaci v České republice, lze vycházet z měsíčního přehledu NÚKIB. Mezi hrozbami, kterým čelí české subjekty, jednoznačně dominují průniky, tedy případy, kdy se útočník neoprávněně dostane do systému, většinou přes prolomený uživatelský účet nebo zranitelnost v aplikaci. V březnu na ně připadla více než polovina všech incidentů a jejich převaha trvá již druhý měsíc po sobě. Zatímco průniky vedou statistikám, útoky na dostupnost, především DoS a DDoS, jejichž cílem je zahltit a vyřadit online služby, se po lednovém nárůstu drží na nízkých hodnotách. Kromě toho NÚKIB eviduje i méně časté, zato závažnější případy: neoprávněný přístup k datům, jejich úniky, nasazení škodlivého kódu a phishing. Pozitivním zjištěním je, že ransomware již třetí měsíc po sobě nezpůsobil žádný úspěšný útok [2], ačkoli ENISA jej označuje za hrozbu s největším dopadem v EU. [1]

Z hlediska celkového trendu počet incidentů sice klesá a blíží se dlouhodobému průměru, jejich závažnost ale roste. NÚKIB eviduje čtyři významné incidenty, což je nejvíce

za poslední rok. Tato kombinace naznačuje, že útočníci útočí méně často, zato cíleněji. Varovným signálem zůstávají i zranitelné systémy a neúspěšné pokusy o průnik. [2]

I když počet incidentů klesá, jejich rostoucí závažnost ukazuje, že firmy potřebují vědět, co chrání a jakou to má hodnotu.

2.3 Základní pojmy a názvosloví

Abychom problematiku kyberbezpečnosti dokázali pochopit, je třeba porozumět základním pojmům. Zákon č. 264/2025 Sb., o kybernetické bezpečnosti (nový) a norma ČSN EN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník, nám poskytují definice základních pojmů v okruhu ICT.

IT (Information Technology) = Informační technologie

ICT (Information and Communication Technology) = Informační a komunikační technologie

IS (Information System) = Informační systém

ISMS (Information Security Management System) = Systém řízení informační bezpečnosti

Data = "Záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů a metadat, zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa" [3]

Informace = "Zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext." [3]

Aktivum = "Fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě" [3]

Primární aktivum = "Aktivum v podobě zpracovávané informace nebo poskytované služby." [3]

Podpůrné aktivum = "Aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby." [3]

Technické aktivum = " Technický nebo programový prostředek anebo vybavení." [3]

Bezpečnost informací = "Zajištění důvěrnosti, integrity a dostupnosti informací a dat." [3]

Hrozba = " Jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby. " [3]

Zranitelnost = "Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito hrozbou." [3]

Riziko = "Účinek nejistoty na dosažení cílů. Riziko bezpečnosti informací je spojeno s možností, že hrozby využijí zranitelností informačního aktiva nebo skupiny informačních aktiv, a tak způsobí organizaci škodu." [5]

Tyto pojmy tvoří základ celé problematiky bezpečnosti informací. V dalších kapitolách budou dále rozvedeny zejména pojmy aktivum a metody jeho hodnocení, které jsou klíčové pro tuto práci.

2.4 Bezpečnost informací a CIA triáda

Bezpečnost informací stojí na třech pilířích, často označovaných jako CIA triáda.

CIA = Confidentiality, Integrity, Availability (Důvěrnost, Integrita, Dostupnost)

Je důležité, aby k informaci měli přístup pouze oprávněné osoby, informace byly správné, úplné a přístupné oprávněným uživatelům v okamžiku potřeby. [4]

Důvěrnost = "Vlastnost, že informace není dostupná nebo není zpřístupněná neoprávněným jednotlivcům, entitám nebo procesům." [5]

Jako příklad pro důvěrnost můžeme uvést, že např. firemní mzdová data by měl vidět pouze HR a vedení, ne všichni zaměstnanci. Zdravotní dokumentace pacienta by měla být přístupná pouze jeho lékaři atd. Selže-li důvěrnost, mohou pak data uniknout ven, konkurence získá strategické plány, hacker zveřejní osobní údaje klientů. Selhání důvěrnosti často otevírá dveře k dalším útokům, včetně narušení integrity nebo dostupnosti.

Integrita = "Zajištění přesnosti a úplnosti" [5]

Integrita je klíčovým atributem informací. I drobná neoprávněná změna dat může způsobit, že informace ztratí svou hodnotu. Příkladem může být útok, kdy je změněna částka na faktuře, nebo selhání systému, při kterém virus poškodí databázi.

Dostupnost = "Vlastnost vyjadřující přístupnost a použitelnost na žádost oprávněné entity" [5]

Dostupnost znamená, že je potřeba zajistit přístup k datům oprávněným osobám, když je potřebují. Bez klíčových dat nemůže firma pracovat. Příkladem narušení dostupnosti je výpadek serveru nebo ransomware, který data zašifruje.

2.5 ISMS (Systém řízení bezpečnosti informací)

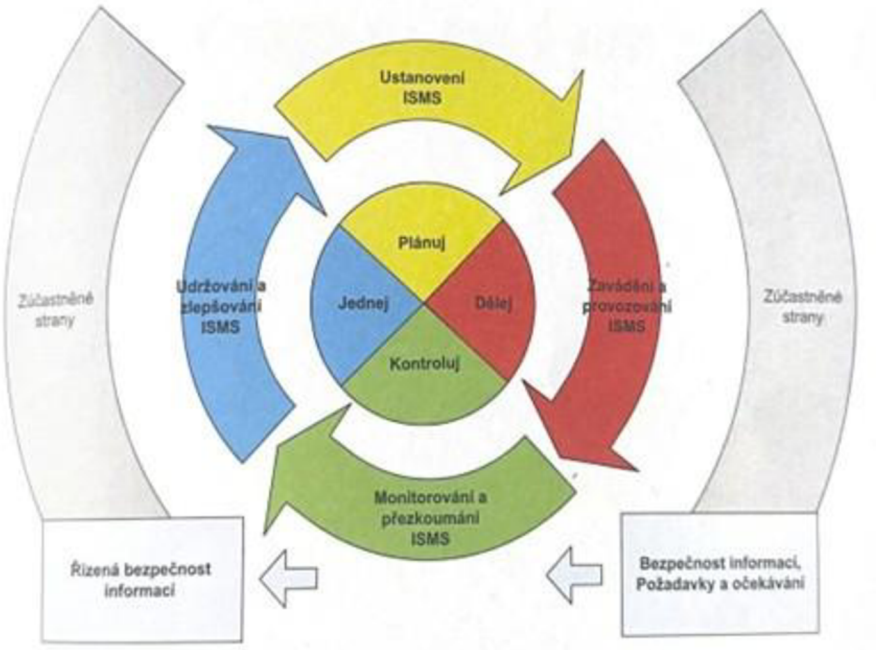
Pojem ISMS, tedy Information Security Management System, vyjadřuje systémový přístup k řízení bezpečnosti informací v rámci organizace. Vystihuje skutečnost, že bezpečnost informací není izolovanou činností, ale tvoří integrální součást celkového systému řízení organizace. [4]
ISMS se na základě modelu PDCA (Demingův model) viz Obr. 1) rozděluje na čtyři etapy.

Ustavení ISMS, tedy určení rozsahu a odpovědnosti. Zavedení samotného ISMS. Monitorování a následné přezkoumání ISMS. Díky zpětné vazbě a hodnocení pak můžeme provádět soustavné zlepšování a pravidelnou údržbu. [4]

Samotný model PDCA, nazývaný také Demingův cyklus, je metodou postupného zlepšování kvality výrobků, služeb, dat atd. Dosahuje toho systematickým intervalovým zpracováním čtyř základních činností.

- "Plan (plánuj) – naplánování zamýšleného zlepšení
- Do (dělej) – realizace plánu
- Check (kontroluj) – ověření výsledku
- Act (jednej) – úpravy a plošná implementace do praxe " [4]

Cyklus je třeba neustále opakovat, abychom mohli dosáhnout požadovaných výsledků. [4]



Obr. 1) "Model PDCA v ISMS (někdy také označovaný jako životní cyklus ISMS) " [4]

2.6 Legislativní rámec

EU představila na konci roku 2020 novou strategii pro kybernetickou bezpečnost, která pokrývá bezpečnost klíčových služeb nemocnic, energetických sítí a železnic, ale i pokrytí připojených zařízení v domácnostech a továrnách. [6]

Klíčovým předpisem v této oblasti je směrnice NIS2. Jedná se o nástupce původní směrnice NIS. Členské státy EU ji měly povinně implementovat do svých zákonů do října 2024. Oproti první směrnici rozšiřuje okruh organizací, které musí plnit bezpečnostní požadavky, a zpřísňuje pravidla. [6]

Vedle směrnice NIS2 vznikly i další předpisy. Akt o kybernetické bezpečnosti, přijatý v roce 2019, posílil agenturu ENISA a zavedl certifikační rámec ECCF. Komise navrhla v lednu 2026 nové rozšíření aktu pro posílení odolnosti EU. Balíček obsahuje snahu o zjednodušení dodržování pravidel kyberbezpečnosti a požadavků na řízení rizik pro firmy. Nová iterace aktu také usiluje o snížení rizik v dodavatelském řetězci ICT ze strany dodavatelů ze třetích zemí. [6; 7]

V návaznosti na směrnici NIS2 od 1. listopadu 2025 nabyl účinnosti zákon č. 264/2025 Sb., který rozšiřuje okruh regulovaných subjektů. Cílem úpravy je nejen větší odolnost českých podniků, ale i přenesení odpovědnosti na vrcholové vedení podniku. Povinností firem je nyní samo identifikovat, zda spadají do vyššího či nižšího režimu povinností, provést analýzu rizik, zavést ISMS a procesy pro detekci a hlášení incidentů. Při vážném porušení předpisů může sankce dosáhnout výše 250 milionů korun, případně 2 % z celkového obratu. [3]

K zákonu č. 264/2025 Sb. [3] byla vydána vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách, která stanovuje rozdělení poskytovatelů regulovaných služeb do daných režimů. [8] Dále vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností stanovuje bezpečnostní opatření pro poskytovatele v režimu vyšších povinností. Vyhláška definuje metodiku pro hodnocení aktiv a jejich dělení na primární a podpůrná aktiva. Primární aktiva se hodnotí z hlediska CIA. [9] Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností dále vymezuje procesy zavádění bezpečnostních opatření a klasifikaci závažnosti kybernetických incidentů. [10]

Kromě zákona o kybernetické bezpečnosti existují v ČR i další předpisy, které ovlivňují ochranu informací. GDPR (Nařízení EU 2016/679) upravuje ochranu osobních údajů fyzických osob a platí v celé EU. Při hodnocení informačních aktiv je proto nutné zohlednit, zda dané aktivum obsahuje osobní údaje, protože jejich únik může mít pro organizaci závažné důsledky. Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce upravuje elektronické podpisy, pečetě a důvěryhodné služby pro elektronické transakce. Zákon č. 499/2004 Sb. Zákon o archivnictví a spisové službě stanovuje pravidla pro archivaci a skartaci dokumentů. Při zavádění ISMS je potřeba brát v potaz všechny tyto předpisy. [11; 12; 13]

2.7 Normy ISO

Pro řízení bezpečnosti informací existuje rodina mezinárodních norem ISO/IEC řady 27000. Jejím základním slovníkem je norma ČSN EN ISO/IEC 27000:2020. [5] Tyto normy pomáhají organizacím zavést a provozovat systém řízení bezpečnosti informací

(ISMS). Díky nim mohou organizace také nezávisle ohodnotit svá informační aktiva. [4]

Nejdůležitější normou z celé řady je ČSN EN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Systémy, která specifikuje požadavky na vybudování, zavedení, provoz a monitorování ISMS. Norma také stanovuje požadavky na výběr bezpečnostních opatření chránících informační aktiva. Podle této normy se organizace mohou certifikovat. [4]

Norma ČSN EN ISO/IEC 27005:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti se zabývá řízením rizik bezpečnosti informací. Norma podporuje koncepty specifikované v normě ISO/IEC 27001:2023. Nejsou zde však uvedeny konkrétní metody pro řízení rizik bezpečnosti. Samotný přístup k řízení rizik pak záleží na dané organizaci. [4]

ČSN ISO 55000:2025 Management aktiv – Slovník, přehled a zásady poskytuje definice termínů, přehled zásad a výsledků managementu aktiv. Popisuje také přínosy a vztahy mezi managementem, systémem a portfoliem aktiv. Zabývá se rovněž zlepšováním a vyspělostí managementu aktiv. Lze ji aplikovat na všechny typy aktiv napříč organizacemi různých druhů a velikostí. [14]

2.8 Aktiva a jejich klasifikace

Aktivum tvoří elementární jednotku, na níž je celá kybernetická bezpečnost postavena. Rozumí se jím cokoli, co má pro daný subjekt, ať už jde o organizaci, či obchodní společnost, určitou hodnotu, a co si proto zaslouží odpovídající ochranu. Význam aktiva přesahuje samotnou oblast řízení rizik a plnění zákonných požadavků; promítá se rovněž do každodenního provozu organizace. [15]

Zákon definuje aktivum jako „fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě" (§ 2 odst. 1 písm. c) zákona č. 264/2025 Sb.) [3] Aktivum tak v žádném případě nelze redukovat pouze na server či aplikaci. Patří sem i konkrétní pracovník, postup, jímž je služba poskytována, know-how organizace nebo budova, ve které je umístěna infrastruktura nezbytná pro chod regulované služby, a řada dalších prvků. [15]

2.9 Dělení aktiv

Zákon vymezuje tři kategorie aktiv:

1. Primární aktiva představují to nejcennější, na čem stojí samotný smysl existence organizace. Spadají sem zejména poskytované služby nebo informace. V prostředí advokátní kanceláře jimi mohou být uzavřené smlouvy s klienty a samotné poskytování právních služeb, zatímco u výrobního podniku půjde spíše o výrobní dokumentaci a vlastní výrobní postup. [15]

2. Podpůrná aktiva v sobě slučují vše, co umožňuje primárním aktivům plnit jejich funkci. Řadí se sem lidské zdroje, dodavatelské vztahy, prostory, v nichž organizace působí, a také jednotlivé organizační postupy a procesy. [15]

3. Technická aktiva tvoří specifickou podmnožinu aktiv podpůrných a rozumí se jimi technické či programové prostředky a vybavení. Konkrétně se jedná například o servery,

prvky síťové infrastruktury, koncové počítače, software a další technologie, bez nichž by primární aktiva nemohla řádně fungovat. [15]

2.10 Hodnocení aktiv

Identifikace aktiv, jež představují předmět ochrany, představuje výchozí krok celého procesu řízení kybernetické bezpečnosti. Bez jasné představy o tom, co konkrétně je potřeba zabezpečit, organizace není schopna účelně volit bezpečnostní opatření ani rozumně rozhodovat o tom, jaké finanční či časové zdroje má do ochrany vložit. Jakmile jsou aktiva určena, hodnotí se v praxi jejich význam ze tří základních úhlů pohledu: důvěrnosti, integrity a dostupnosti. [15]

- **Důvěrnost** vyjadřuje požadavek, aby k aktivu (typicky k informaci) měli přístup pouze oprávnění uživatelé. Příkladem mohou být strategické obchodní smlouvy, jejichž obsah je vyhrazen úzkému okruhu vedení a nikdo mimo tento okruh do nich nemá nahlížet. [15]

- **Integritou** se rozumí, že aktivum (opět například informace) zůstává v původním, nepozměněném a věcně správném stavu. Lze si to představit na složení léčiv, které musí být zachováno beze změn; jakýkoli neoprávněný zásah by mohl vést k tomu, že přípravek přestane plnit svůj účel. [15]

- **Dostupnost** znamená, že oprávněný uživatel se k aktivu (například k informaci) dostane právě ve chvíli, kdy je to potřeba. Praktickým příkladem může být situace, kdy v rozhodující okamžik nelze pracovat s účetním nebo výrobním systémem, takže není možné odeslat platbu faktury či pozastavit běh výrobní linky. [15]

2.11 Evidence aktiv

Nový zákon ukládá povinným osobám vést průběžně aktualizovaný přehled vlastních aktiv (§ 12 odst. 1–5 a § 14 odst. 1 písm. a) bod 5 a odst. 2 písm. c)). [3] Obsah takové evidence musí věrně odrážet skutečný stav toho, čím organizace disponuje nebo co při své činnosti využívá. Jen na tomto základě lze efektivně určit, která aktiva mají pro fungování organizace klíčový význam a jakým způsobem k jejich ochraně přistupovat. Pokud tyto podklady chybějí, není možné řádně dostát ani navazujícím zákonným požadavkům. Typicky při ohlašování bezpečnostního incidentu ve smyslu § 19. [3]

2.12 Garanti aktiv

Typicky bývá garantem aktiva pracovník, který s daným systémem přichází do kontaktu při své každodenní činnosti. Roli garanta řídicího systému výrobní linky tak může zastávat například vedoucí provozu, jenž má díky pravidelné práci s tímto systémem dostatečný přehled na to, aby rozpoznal i méně nápadné odchylky od standardního chování. Obdobně lze za garanta účetního softwaru určit vedoucího ekonomického úseku. Software denně spouští, ověřuje výstupy svých podřízených, přiděluje jim v něm úkoly a podobně. Díky této každodenní zkušenosti rozumí konkrétnímu podpůrnému aktivu detailněji než manažer kybernetické bezpečnosti, který nemá možnost sledovat jeho fungování v takové míře. Pravděpodobněji proto zachytí, že aplikace vykazuje nestandardní projevy nebo že došlo ke ztrátě určitých dat.

Jakmile k takové situaci dojde, je povinností garanta aktiva informovat manažera kybernetické bezpečnosti a poskytnout mu součinnost při dalším šetření. [15]

2.13 Metody hodnocení aktiv

Pro usnadnění celého procesu oceňování se doporučuje využít vhodnou softwarovou podporu, jako je například nástroj vycházející z metodiky CRAMM. Následně je nezbytné definovat jasná kritéria a škálu, podle které se bude majetek klasifikovat. Toto hodnocení lze vyjádřit buď konkrétními finančními částkami, nebo pomocí kvalitativních kategorií. Často se volí například pětistupňová škála, kde první stupeň představuje situaci zcela bez dopadu a pátý stupeň znamená vážné problémy pro firmu. [4]

Základem pro určení hodnoty aktiv je odhad škod, které by organizaci vznikly při narušení jejich dostupnosti, důvěrnosti nebo integrity. Tato tři bezpečnostní kritéria slouží jako hlavní stavební kámen pro celkové ocenění. K samotnému výpočtu se nabízí více cest, ale tou nejběžnější a nejjednodušší je metoda průměrování. Výsledná hodnota aktiva se jednoduše získá sečtením jednotlivých hodnocení pro všechna tři kritéria a jejich následným vydělením třemi viz vzorec (*1*). [4]

$$\frac{(C + I + A)}{3} \tag{1}$$

C – Důvěrnost, I – Integrita, A – Dostupnost

2.14 Nástroje pro hodnocení aktiv

Pro systematické hodnocení informačních aktiv a navazující analýzu rizik existuje řada specializovaných metodik a softwarových nástrojů, které byly vyvíjeny v průběhu posledních desetiletí. Mezinárodní přehled těchto nástrojů spravuje Evropská agentura pro kybernetickou bezpečnost (ENISA) ve své databázi Risk Management Inventory. [16]

Jednou z metodik uvedených v této databázi je CRAMM (CCTA Risk Analysis and Management Method). Vznik metodiky se datuje do roku 1985 a stojí za ní britská vládní agentura CCTA (Central Computer and Telecommunications Agency). Poslední verze 5 byla uvolněna v roce 2003. CRAMM se distribuuje formou komerčního softwarového nástroje a jeho metodický rámec odpovídá normě ISO/IEC 17799. Cílovou skupinou jsou velké organizace a státní instituce. Mezi jazyky, ve kterých je metodika dostupná, patří kromě angličtiny i čeština. [16; 17]

Metodický základ CRAMM vycházel z bezpečnostních postupů uplatňovaných v britské státní správě. Práce s metodikou bez příslušného softwaru je obtížně proveditelná. Z hlediska procesu pokrývá tři klíčové oblasti řízení rizik: identifikaci, analýzu a vyhodnocení. [17]

Jako další významnou metodiku lze uvést EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). První verze byla vydána ve Francii v roce 1995 agenturou DCSSI. V současnosti metodiku spravuje a rozvíjí francouzská Agence nationale de la sécurité des systèmes d'information (ANSSI), která v roce 2018 publikovala radikálně přepracovanou verzi nazvanou EBIOS Risk Manager. Tato moderní verze je dostupná zdarma a je v souladu s normami ISO 27000, ISO 27005 a ISO 31000. [18]

Postup EBIOS Risk Manager je rozdělen do pěti pracovních ateliérů. Atelier 1 vymezuje rozsah a kontext studie, identifikuje obchodní aktiva a definuje obávané události. Atelier 2 zkoumá zdroje rizik a jejich cíle. Atelier 3 definuje strategické scénáře útoku, Atelier 4 rozpracovává operační scénáře a Atelier 5 se věnuje zvládání rizik a definici bezpečnostních opatření. [18]

V českém prostředí poskytuje praktickou podporu při hodnocení aktiv a rizik Průvodce řízením aktiv a rizik vydaný Národním úřadem pro kybernetickou a informační bezpečnost. [19] Nejedná se o softwarový nástroj, ale o ucelený metodický dokument se šablonami pro identifikaci primárních aktiv, jejich klasifikaci a hodnocení podle CIA atributů a pro navazující řízení rizik. Součástí jsou katalogy typových hrozeb, zranitelností a doporučených bezpečnostních opatření.

2.15 Shrnutí

Tato kapitola představila současný stav v oblasti informační a kybernetické bezpečnosti se zaměřením na české prostředí. Z analýzy aktuálních hrozeb vyplynulo, že v České republice dlouhodobě dominují průniky do informačních systémů. Přestože celkový počet incidentů klesá k dlouhodobému průměru, jejich závažnost roste. To naznačuje posun směrem k cíleným útokům s vážnějšími dopady.

V navazujících podkapitolách byly vymezeny základní pojmy a názvosloví podle aktuální legislativy, zejména zákona č. 264/2025 Sb., a popsána CIA triáda (důvěrnost, integrita, dostupnost) jako základní rámec hodnocení bezpečnosti informací. Představen byl rovněž koncept systému řízení bezpečnosti informací (ISMS) a Demingův PDCA cyklus, který tvoří jeho metodický základ.

Dále byla zpracována rešerše legislativního rámce, jenž v České republice zahrnuje zákon č. 264/2025 Sb. a jeho prováděcí vyhlášky č. 408, 409 a 410/2025 Sb. Tato úprava je výsledkem transpozice evropské směrnice NIS2 a navazuje na další předpisy, jako jsou GDPR či zákon o archivnictví. Z mezinárodních norem byla popsána zejména řada ISO/IEC 27000, která stanovuje požadavky na vybudování a provoz ISMS, a ISO 55000 zaměřená na management aktiv.

Klíčovým tématem této práce je identifikace, klasifikace a hodnocení informačních aktiv. Aktiva byla rozdělena do tří kategorií podle zákona: primární, podpůrná a technická, a byla popsána povinnost vést jejich evidenci, přiřazovat odpovědné garanty a hodnotit je z hlediska CIA. Představeny byly rovněž existující metody hodnocení, zejména pětistupňová škála se součtovým algoritmem viz (1), a dále nástroje pro hodnocení aktiv a analýzu rizik. Mezi popsané nástroje patří britská metodika CRAMM, francouzský EBIOS Risk Manager spravovaný agenturou ANSSI a v českém prostředí Průvodce řízením aktiv a rizik vydaný NÚKIB. Tyto teoretické poznatky tvoří základ pro praktickou část, ve které je navržena vlastní metodika hodnocení informačních aktiv pro průmyslový podnik.

3 NÁVRH METODIKY STANOVENÍ A HODNOCENÍ INFORMAČNÍCH AKTIV

3.1 Úvod do navržené metodiky

Předchozí kapitola popsala teoretický rámec problematiky řízení bezpečnosti informací, vymezila základní pojmy, představila platnou legislativu a normy a popsala existující přístupy k hodnocení informačních aktiv. Navazující kapitola představuje vlastní návrh metodiky pro stanovení a hodnocení informačních aktiv v prostředí průmyslového podniku.

Cílem navržené metodiky je poskytnout jednoznačný a opakovatelný postup, který umožní systematicky určit hodnotu jednotlivých aktiv a zařadit je do tříd podle jejich významnosti pro organizaci. Metodika je koncipována tak, aby ji bylo možné použít při auditu systému řízení bezpečnosti informací (ISMS), při interním řízení rizik nebo jako podklad pro rozhodování o investicích do bezpečnostních opatření.

Návrh vychází z platné české legislativy, konkrétně ze zákona č. 264/2025 Sb. [3], který vymezuje pojem aktivum a jeho dělení na primární, podpůrná a technická, a z prováděcí vyhlášky č. 409/2025 Sb. [9] stanovující povinnost hodnotit primární aktiva podle atributů důvěrnosti, integrity a dostupnosti. Pro samotný výpočet hodnoty aktiva je převzat součtový algoritmus popsaný v odborné literatuře [4], podle kterého se výsledná hodnota získá jako prostý průměr hodnocení tří CIA atributů.

V následujících podkapitolách je nejprve charakterizován vzorový průmyslový podnik 3.2, dále popsán pětistupňový postup hodnocení v kapitole 3.3, představeny hodnotící stupnice a třídy aktiv v kapitole 3.4 a navržená metodika je aplikována na vzorový průmyslový podnik v kapitole 3.5. Závěr kapitoly tvoří citlivostní analýza kapitola 3.6.

3.2 Charakteristika vzorového průmyslového podniku

V této kapitole je metodika aplikována na modelový průmyslový podnik. Jde o fiktivní organizaci, která neodpovídá žádné konkrétní firmě. Slouží pouze k tomu, aby na ní bylo možné ukázat postup hodnocení v praxi.

Modelový podnik má střední velikost, tedy 50 až 250 zaměstnanců, a zabývá se výrobou průmyslových komponentů. Pro samotnou metodiku není rozhodující, o jaký typ výroby přesně jde. Postup je navržen tak, aby ho bylo možné použít v různých výrobních podnicích.

Při hodnocení jsou uvažovány běžné informační systémy, se kterými se ve výrobních podnicích lze setkat. Patří mezi ně systém řízení podniku (ERP), systém řízení výroby (MES) a systém správy produktových dat (PLM). Konkrétní výčet aktiv a jejich hodnocení je uveden v sekci 3.5, kde k tomu existuje vhodný kontext.

3.3 Postup hodnocení

Navržená metodika se opírá o pětikrokový postup, který lze aplikovat při auditu ISMS i při interním řízení rizik. Jednotlivé kroky na sebe logicky navazují a v praxi je doporučeno provést je vždy v uvedeném pořadí.

Krok 1: Identifikace primárních aktiv

Prvním krokem je sestavení přehledu primárních aktiv podniku, tedy informací a služeb,

na nichž stojí samotná existence organizace. V průmyslovém podniku se typicky jedná o výrobní dokumentaci, technologické postupy, receptury, výrobní procesy nebo plánování výroby. Identifikace by měla probíhat ve spolupráci s vedením a vedoucími jednotlivých úseků, neboť právě oni mají nejlepší přehled o tom, co je pro chod podniku skutečně klíčové.

Krok 2: Mapování podpůrných a technických aktiv

Pro každé primární aktivum je nutné dohledat související podpůrná a technická aktiva, která zajišťují jeho fungování. Mezi podpůrná aktiva patří zejména zaměstnanci, dodavatelé, prostory a organizační procesy. Technická aktiva tvoří hardware, software a další technologické prostředky, jako jsou servery, řídicí systémy či databázové aplikace.

Krok 3: Přiřazení garantů

Každému aktivu je přiřazena odpovědná osoba, garant. Garantem by měl být pracovník, který s aktivem přichází do kontaktu při své každodenní činnosti a je schopen rozpoznat odchylky od standardního chování. U výrobní dokumentace to může být vedoucí technologického úseku, u účetního systému vedoucí ekonomického oddělení.

Krok 4: Hodnocení podle atributů CIA

V tomto kroku jsou primární aktiva ohodnocena z hlediska tří bezpečnostních atributů a těmi jsou: důvěrnosti (C), integrity (I) a dostupnosti (A). Hodnocení probíhá na pětistupňové škále, kde stupeň 1 odpovídá nulovému dopadu a stupeň 5 dopadu kritickému. Detailní popis stupnice je uveden v následující podkapitole.

Krok 5: Výpočet hodnoty a zařazení do třídy

Výsledná hodnota aktiva se získá jako prostý průměr hodnocení tří CIA atributů podle vzorce viz (1). [4] Na základě této hodnoty je aktivum zařazeno do jedné ze čtyř tříd: nízká (1,00–1,99), střední (2,00–2,99), vysoká (3,00–3,99) a kritická (4,00–5,00). Třída pak slouží jako podklad pro volbu vhodných bezpečnostních opatření.

3.4 Hodnotící stupnice a třídy aktiv

Pro hodnocení primárních aktiv byla zvolena pětistupňová kvalitativní škála vycházející ze součtové metody popsané v odborné literatuře. [4] Hodnocení primárních aktiv probíhá podle pětistupňové škály uvedené v Tab 1) Konkrétní podoba stupnice je vlastním návrhem této práce, který respektuje rámec stanovený vyhláškou č. 409/2025 Sb. [9]. Vyhláška ponechává volbu konkrétní hodnotící stupnice na povinné osobě a požaduje pouze, aby umožňovala zařazení aktiv do jednotlivých úrovní podle jejich významnosti.

Konkrétní popisy jednotlivých stupňů byly inspirovány Tabulkou 9 z Průvodce řízením aktiv a rizik vydaného NÚKIB [19], která obsahuje stupnici pro hodnocení důvěrnosti, integrity a dostupnosti. V této práci byla původní čtyřúrovňová stupnice rozšířena na pět stupňů přidáním úrovně bez dopadu pro detailnější rozlišení.

Hodnotitel přiřadí každému aktivu pro každý ze tří atributů důvěrnosti (C), integrity (I) a dostupnosti (A) stupeň od 1 do 5 podle očekávaného dopadu narušení daného atributu na chod organizace. Stupeň 1 představuje situaci bez dopadu, stupeň 5 dopad kritický.

Pětistupňová škála byla zvolena jako kompromis mezi dostatečně jemným rozlišením významnosti aktiv a praktickou použitelností. Kratší škála (například třístupňová) by neumožnila dostatečné rozlišení mezi aktivy, zatímco delší škála (například desetistupňová) by zvyšovala subjektivitu hodnocení a snižovala opakovatelnost výsledků.

Tab 1) Hodnotící stupnice pro atributy CIA

Stupeň	Označení	Důvěrnost (C)	Integrita (I)	Dostupnost (A)
1	**Bez dopadu**	Aktivum je veřejně dostupné nebo bylo určeno ke zveřejnění. Únik informace neohrozí žádné zájmy organizace.	Změna aktiva neovlivní chod organizace ani její oprávněné zájmy. Aktivum nevyžaduje ochranu z hlediska integrity.	Nedostupnost aktiva nezpůsobí žádné komplikace. Tolerovatelná doba výpadku je v řádu týdnů.
2	**Nízký**	Aktivum tvoří interní know-how organizace, jeho ochrana není vyžadována zákonem ani smluvně. Únik způsobí drobné komplikace.	Drobná chyba v aktivu způsobí nepříjemnosti, ale dají se odstranit. Provoz organizace pokračuje bez podstatného omezení.	Krátkodobý výpadek aktiva (do jednoho pracovního dne) je akceptovatelný. Dlouhodobější výpadek by mohl ohrozit zájmy organizace.
3	**Střední**	Únik aktiva vede k poškození oprávněných zájmů organizace. Patří sem například obchodní informace nebo data, jejichž ochranu vyžaduje legislativa.	Neoprávněná změna aktiva má citelný dopad na chod organizace. Hrozí finanční nebo provozní ztráty, které lze ale řešit.	Výpadek aktiva by neměl trvat déle než několik hodin. Delší nedostupnost vede k přímému ohrožení provozu organizace.
4	**Vysoký**	Únik aktiva vede k vážnému poškození organizace. Mezi tato aktiva patří citlivé osobní údaje, obchodní tajemství nebo strategické informace.	Změna aktiva vede k vážnému narušení činnosti organizace. Hrozí poškození reputace, narušení smluvních vztahů nebo právní odpovědnost.	Nedostupnost aktiva má vážné dopady na provoz. Tolerovatelná doba výpadku je v řádu minut až jednotek hodin.
5	**Kritický**	Únik aktiva může ohrozit existenci organizace. Patří sem strategické obchodní tajemství nebo zvláštní kategorie osobních údajů.	Neoprávněná změna aktiva má fatální dopad. Vede ke ztrátě klíčových informací, právní odpovědnosti nebo zastavení činnosti.	Aktivum musí být dostupné prakticky nepřetržitě. I krátká nedostupnost ohrožuje existenci organizace.

Výsledná hodnota aktiva se vypočítá jako prostý průměr hodnocení tří atributů podle vzorce viz (1) [4] a nabývá hodnoty v rozmezí 1,00 až 5,00. Na základě této hodnoty je aktivum zařazeno do jedné ze čtyř tříd, které odrážejí jeho významnost pro chod organizace a podle nichž se odvíjí intenzita aplikovaných bezpečnostních opatření. Rozsah průměrů viz Tab 2)

Tab 2) Třídy aktiv podle výsledné hodnoty

Třída	Rozsah průměru	Charakteristika a doporučená ochrana
Nízká	**1,00 – 1,99**	Aktivum s nízkou hodnotou pro organizaci. Postačují běžná bezpečnostní opatření odpovídající standardní praxi.
Střední	**2,00 – 2,99**	Aktivum se střední hodnotou. Vyžaduje standardní bezpečnostní opatření, pravidelný monitoring a kontrolu přístupů.
Vysoká	**3,00 – 3,99**	Aktivum s vysokou hodnotou. Vyžaduje posílená bezpečnostní opatření, řízený přístup, zálohování a zvýšenou pozornost při auditu.
Kritická	**4,00 – 5,00**	Aktivum s kritickou hodnotou pro chod organizace. Vyžaduje nejvyšší úroveň zabezpečení, redundanci, plán kontinuity provozu a pravidelný audit.

Při použití navržené metodiky je třeba zohlednit, že prostý aritmetický průměr neodráží extrémní hodnoty jednotlivých atributů. Pokud má aktivum, byť jen jeden z atributů důvěrnosti, integrity nebo dostupnosti ohodnocen nejvyšším stupněm 5, jeho narušení by mělo kritický dopad na chod organizace. V takovém případě nelze aktivum zařadit do tříd Nízká či Střední, i kdyby výsledný průměr odpovídal nižší kategorii. Takové aktivum musí být zařazeno minimálně do třídy Vysoká.

Zařazení aktiva do třídy slouží jako podklad pro volbu konkrétních bezpečnostních opatření a pro prioritizaci jejich zavádění. Aktiva ve vyšších třídách vyžadují přísnější ochranu a častější kontrolu, zatímco aktiva ve třídě nízké lze pokrýt běžnými standardními opatřeními.

3.5 Aplikace metodiky na modelový průmyslový podnik

Tato podkapitola představuje praktickou aplikaci navržené metodiky na modelový průmyslový podnik představený v kapitole 3.2. Cílem je demonstrovat funkčnost metodiky na konkrétních příkladech informačních aktiv a ukázat, jak lze postupovat při hodnocení v reálném prostředí.

Při výběru primárních aktiv byl jako orientační rámec použit Průvodce řízením aktiv a rizik vydaný NÚKIB [19], který popisuje strukturu primárních aktiv tvořenou službou a souvisejícími informacemi. Konkrétní výběr aktiv byl přizpůsoben specifikům výrobního průmyslového podniku a jeho hlavních činností.

Pro modelový podnik bylo identifikováno celkem osm primárních aktiv: jedna hlavní služba a sedm souvisejících informací. Každé aktivum bylo ohodnoceno podle pětistupňové škály uvedené v kapitole 3.4 z hlediska důvěrnosti (C), integrity (I) a dostupnosti (A). Výsledná hodnota aktiva byla vypočtena jako prostý průměr a aktivum bylo zařazeno do odpovídající třídy.

Tab 3) Identifikace a hodnocení primárních aktiv modelového podniku

ID	Primární aktivum	Typ	C	I	A	Hodnota	Třída
S1	Služba výroby a dodávky komponentů	služba	4	5	5	**4,67**	**Kritická**
P1	Výrobní dokumentace a technologické postupy	informace	5	5	4	**4,67**	**Kritická**
P2	Plán výroby a evidence zakázek	informace	3	4	4	**3,67**	**Vysoká**
P3	Skladová evidence surovin a hotových výrobků	informace	2	4	4	**3,33**	**Vysoká**
P4	Účetní a finanční evidence	informace	4	5	3	**4,00**	**Kritická**
P5	Personální evidence zaměstnanců	informace	5	4	2	**3,67**	**Vysoká**
P6	Klientské smlouvy a obchodní dokumentace	informace	4	4	3	**3,67**	**Vysoká**
P7	Evidence kvality a měření	informace	3	5	3	**3,67**	**Vysoká**

Při interpretaci výsledků je třeba zohlednit, že pokud má aktivum jakýkoli z atributů CIA ohodnocen nejvyšším stupněm 5, je automaticky zařazeno minimálně do třídy Vysoká bez ohledu na výslednou průměrnou hodnotu. Toto pravidlo zajišťuje, že aktiva s alespoň jedním kriticky důležitým atributem nebudou podhodnocena vlivem aritmetického průměrování.

Z tabulky Tab 3) je patrné, že všechna identifikovaná aktiva spadají do tříd Vysoká nebo Kritická, což odpovídá skutečnosti, že se jedná výhradně o primární aktiva podporující hlavní činnost podniku. Žádné z aktiv nedosáhlo nižší třídy, neboť všechna mají přímý vliv na chod organizace.

Odůvodnění hodnocení jednotlivých aktiv

Následující text uvádí odůvodnění hodnocení každého z osmi identifikovaných primárních aktiv. U každého aktiva je vysvětleno, proč byly konkrétní atributy CIA ohodnoceny právě daným stupněm.

S1: Služba výroby a dodávky komponentů

Služba výroby představuje hlavní činnost modelového podniku a její narušení by mělo přímý dopad na všechny obchodní aktivity. Důvěrnost byla ohodnocena stupněm 4, neboť údaje o probíhajících zakázkách jsou citlivé z konkurenčního hlediska, avšak nejedná se o strategické tajemství v pravém smyslu slova. Integrita byla ohodnocena nejvyšším stupněm 5, protože

narušení správnosti údajů o průběhu výroby a expedici by vedlo k vážnému poškození smluvních vztahů a mohlo by způsobit zastavení dodávek klíčovým odběratelům. Dostupnost byla také ohodnocena stupněm 5, neboť bez fungování této služby není podnik schopen plnit své zakázky a každá hodina prostoje má přímé finanční dopady. Celková hodnota 4,67 řadí toto aktivum do třídy Kritická.

P1: Výrobní dokumentace a technologické postupy

Výrobní dokumentace tvoří know-how podniku a představuje jeden z nejcennějších informačních zdrojů. Důvěrnost byla ohodnocena nejvyšším stupněm 5, protože únik dokumentace ke konkurenci by znamenal trvalou ztrátu konkurenční výhody a obsah dokumentace lze považovat za strategické obchodní tajemství. Integrita byla rovněž ohodnocena stupněm 5, neboť neoprávněná změna technologického postupu může vést k výrobě vadných produktů, ohrožení bezpečnosti uživatelů, reklamacím a vzniku právní odpovědnosti. Dostupnost byla ohodnocena stupněm 4, jelikož krátkodobý výpadek lze obvykle překlenout, dokumentace existuje v záložních kopiích a klíčové postupy znají zkušení pracovníci. Celková hodnota 4,67 řadí toto aktivum do třídy Kritická.

P2: Plán výroby a evidence zakázek

Plán výroby propojuje obchodní část podniku s výrobním provozem a zajišťuje plnění zakázek v dohodnutých termínech. Důvěrnost byla ohodnocena stupněm 3, protože plán obsahuje informace o objednávkách a kapacitě, jejichž únik by sice škodil konkurenční pozici, ale neměl by fatální dopad. Integrita byla ohodnocena stupněm 4, neboť chybný plán (nesprávné množství, špatné priority, chybné termíny) způsobí zmatek ve výrobě, opožděné dodávky a hrozící smluvní pokuty. Dostupnost byla rovněž ohodnocena stupněm 4, protože bez plánu nelze efektivně řídit výrobu a delší výpadek vede k zastavení provozu. Celková hodnota 3,67 řadí toto aktivum do třídy Vysoká.

P3: Skladová evidence surovin a hotových výrobků

Skladová evidence zajišťuje přehled o zásobách materiálu a hotových výrobků a tvoří klíčovou součást logistických procesů. Důvěrnost byla ohodnocena stupněm 2, neboť informace o stavu zásob nejsou strategicky důvěrné a jejich případný únik nemá pro podnik fatální dopad. Integrita byla ohodnocena stupněm 4, protože nepřesná evidence vede k chybám v dodávkách, inventurním rozdílům, ztrátám materiálu a může způsobit prostoje výroby kvůli nedostatku surovin. Dostupnost byla také ohodnocena stupněm 4, neboť bez fungující evidence nelze efektivně skladovat ani vychystávat a logistika podniku se prakticky zastaví. Celková hodnota 3,33 řadí toto aktivum do třídy Vysoká.

P4: Účetní a finanční evidence

Účetní evidence zahrnuje veškeré finanční záznamy podniku, smluvní podmínky, mzdy zaměstnanců a evidenci pohledávek a závazků. Důvěrnost byla ohodnocena stupněm 4, jelikož finanční data jsou citlivá. Únik informací o marži, smluvních podmínkách s odběrateli nebo o mzdové struktuře by způsobil poškození reputace a oslabení vyjednávací pozice. Integrita byla ohodnocena nejvyšším stupněm 5, protože neoprávněná změna účetních záznamů znamená porušení zákona o účetnictví a může vést k pokutám od finanční správy, neplatné účetní závěrce a soudním sporům. Dostupnost byla ohodnocena stupněm 3, neboť účetní systém nemusí

fungovat nepřetržitě, krátkodobý výpadek je nepříjemný, ale řešitelný. Celková hodnota 4,00 řadí toto aktivum do třídy Kritická.

P5: Personální evidence zaměstnanců

Personální evidence obsahuje osobní údaje všech zaměstnanců, smluvní podmínky a mzdové informace. Důvěrnost byla ohodnocena nejvyšším stupněm 5, neboť osobní údaje podléhají ochraně podle obecného nařízení o ochraně osobních údajů (GDPR) [11] a jejich únik může vést k vysokým pokutám, žalobám ze strany zaměstnanců a trvalému poškození reputace podniku. Integrita byla ohodnocena stupněm 4, protože chybné údaje ve mzdách nebo v evidenci pojištění mohou způsobit právní spory, pokuty a dohady se zaměstnanci. Dostupnost byla ohodnocena stupněm 2, neboť HR systém nemusí fungovat nepřetržitě, výpadek v délce několika dnů je řešitelný, jelikož mzdy se zpracovávají měsíčně a další personální agenda počká. Celková hodnota 3,67 řadí toto aktivum do třídy Vysoká.

P6: Klientské smlouvy a obchodní dokumentace

Klientské smlouvy a obchodní dokumentace tvoří právní základ obchodních vztahů podniku s jeho odběrateli a dodavateli. Důvěrnost byla ohodnocena stupněm 4, protože smlouvy obsahují citlivé obchodní podmínky, ceny, marže a slevové úrovně, jejichž únik by oslabil vyjednávací pozici podniku. Integrita byla rovněž ohodnocena stupněm 4, neboť neoprávněná změna smluvních podmínek by mohla vést k právním sporům, poškození obchodních vztahů a finančním ztrátám. Dostupnost byla ohodnocena stupněm 3, jelikož při výpadku elektronického přístupu ke smlouvám lze komunikovat s partnery alternativními kanály a krátkodobá nedostupnost není kritická pro chod podniku. Celková hodnota 3,67 řadí toto aktivum do třídy Vysoká.

P7: Evidence kvality a měření

Evidence kvality obsahuje výsledky kontrol, měření a certifikací výrobků a slouží jako podklad pro reklamace, audity a obchodní jednání. Důvěrnost byla ohodnocena stupněm 3, neboť údaje o kvalitě jsou důležité pro vnitřní procesy a certifikace, ale nejsou strategicky tajné. Integrita byla ohodnocena nejvyšším stupněm 5, protože neoprávněná manipulace s daty o kvalitě by mohla vést k expedici vadných výrobků, vážným reklamacím, ztrátě certifikace či dokonce ohrožení bezpečnosti uživatelů. Dostupnost byla ohodnocena stupněm 3, jelikož krátkodobý výpadek lze překlenout, pracovníci mohou zapisovat měření na papír a do systému je zadat dodatečně. Celková hodnota 3,67 řadí toto aktivum do třídy Vysoká.

3.6 Citlivostní analýza

Navržená metodika hodnocení informačních aktiv vychází z kvalitativního hodnocení tří atributů CIA na pětistupňové škále a z prostého aritmetického průměru těchto hodnot. Toto zjednodušení je výhodné z hlediska srozumitelnosti a snadné aplikace, avšak nese s sebou určitá rizika, která je třeba ověřit. Z toho důvodu byla provedena citlivostní analýza, jejímž cílem je posoudit, jak stabilní jsou výsledky hodnocení vůči drobným změnám vstupních hodnot a jakou roli hraje volba metody zprůměrování.

Hodnocení atributů CIA je svou povahou subjektivní. Různí hodnotitelé mohou totéž aktivum klasifikovat mírně odlišně, případně se jednotlivá hodnocení mohou měnit v čase v důsledku nové zkušenosti, změny prostředí organizace nebo aktualizace bezpečnostních

požadavků. Pokud by drobná změna v hodnocení vedla k zásadnímu posunu výsledné třídy aktiva, ztrácela by metodika svou praktickou hodnotu, neboť by každé nové hodnocení mohlo přinést jiný závěr.

Druhým motivem analýzy je ověření vhodnosti prostého aritmetického průměru jako způsobu výpočtu výsledné hodnoty. Tento přístup přiřazuje všem třem atributům stejnou váhu, což v praxi nemusí odpovídat skutečné významnosti jednotlivých vlastností aktiv. Některé typy aktiv mohou v daném prostředí silně preferovat například dostupnost (typicky výrobní procesy) nebo důvěrnost (typicky aktiva podléhající ochraně osobních údajů). Citlivostní analýza umožňuje posoudit, zda by zavedení váženého průměru zásadně změnilo výsledky hodnocení.

V následující části jsou analyzována tři reprezentativní aktiva, která byla vybrána tak, aby pokryla různé situace: aktivum na hranici mezi třídami (P3), aktivum s výraznou disperzí mezi atributy (P5) a aktivum hluboko v třídě Kritická (P1). Pro každé aktivum byl proveden výpočet při změně hodnocení o jeden stupeň a při použití váženého průměru. Výsledky jsou interpretovány s ohledem na praktické důsledky pro hodnotitele i pro organizace, které by metodiku použily v reálném prostředí.

Aktivum P3: Skladová evidence surovin a hotových výrobků (C=2, I=4, A=4, průměr 3,33, třída Vysoká)

Aktivum P3 bylo zvoleno jako reprezentant aktiv, jejichž výsledná hodnota se pohybuje blízko hranice mezi třídami. Skladová evidence byla původně ohodnocena průměrnou hodnotou 3,33, což ji řadí do třídy Vysoká, avšak relativně blízko spodní hranice rozsahu 3,00–3,99.

Při změně hodnocení kteréhokoli atributu o jeden stupeň směrem dolů klesá průměr na 3,00, což odpovídá přesné hranici třídy Vysoká. Pokud by se hodnocení snížilo u dvou atributů současně, průměr klesá na 2,67 a aktivum přechází do třídy Střední. Tab 4) shrnuje vliv jednotlivých změn na výslednou třídu.

Tab 4) Citlivost aktiva P3 na změnu hodnocení

Scénář	C	I	A	Průměr	Třída
Původní hodnocení	2	4	4	**3,33**	**Vysoká**
C snížena o 1	1	4	4	**3,00**	**Vysoká (hranice)**
I snížena o 1	2	3	4	**3,00**	**Vysoká (hranice)**
A snížena o 1	2	4	3	**3,00**	**Vysoká (hranice)**
C a I sníženy o 1	1	3	4	**2,67**	**Střední**
I a A sníženy o 1	2	3	3	**2,67**	**Střední**

Aplikace váženého průměru s váhami 0,2 pro důvěrnost, 0,3 pro integritu a 0,5 pro dostupnost (odrážející důraz na dostupnost ve výrobním podniku) dává hodnotu 3,6, což aktivum stabilizuje ve třídě Vysoká s vyšší rezervou od hraniční hodnoty 3,00.

Z analýzy vyplývá, že skladová evidence je citlivá na změnu hodnocení, ale zavedení váženého průměru s důrazem na dostupnost její zařazení stabilizuje. Pro praxi to znamená, že u hraničních aktiv je vhodné provést hodnocení opakovaně nebo zvážit konzervativnější přístup s vyšší klasifikací.

Aktivum P5: Personální evidence zaměstnanců (C=5, I=4, A=2, průměr 3,67, třída Vysoká)

Aktivum P5 reprezentuje skupinu aktiv s výraznou disperzí mezi atributy. Důvěrnost je ohodnocena nejvyšším stupněm 5 (citlivé osobní údaje podléhající ochraně podle GDPR), zatímco dostupnost stupněm 2 (HR systém nemusí fungovat nepřetržitě). Prostý aritmetický průměr 3,67 řadí aktivum do třídy Vysoká, ale tato hodnota rozředí extrémní význam důvěrnosti průměrováním s nižšími atributy.

Při změně hodnocení o jeden stupeň zůstává aktivum stabilně v třídě Vysoká. Mnohem zajímavější je však vliv vah. Tab 5) ukazuje, jak se výsledek mění při použití různých sad vah.

Tab 5) Vliv vah na hodnocení aktiva P5

Metoda výpočtu	Výpočet	Hodnota	Třída
Prostý průměr	(5 + 4 + 2) / 3	**3,67**	**Vysoká**
Průmyslová váha (0,2·C + 0,3·I + 0,5·A)	1,0 + 1,2 + 1,0	**3,20**	**Vysoká**
GDPR váha (0,5·C + 0,3·I + 0,2·A)	2,5 + 1,2 + 0,4	**4,10**	**Kritická**

Při průmyslové váze s důrazem na dostupnost klesá hodnota na 3,20 a aktivum zůstává v třídě Vysoká. Při použití váhy odrážející význam ochrany osobních údajů (s důrazem na důvěrnost) roste hodnota na 4,10 a aktivum spadá do třídy Kritická. Volba vah tedy zásadně mění výsledné zařazení.

Pro praxi z toho plyne, že personální evidence a další aktiva spadající pod regulace ochrany osobních údajů by měla být hodnocena s ohledem na požadavky GDPR. Použití váženého průměru s důrazem na důvěrnost lépe odráží skutečné riziko spojené s únikem osobních údajů, který může vést k vysokým pokutám a trvalému poškození reputace.

Aktivum P1: Výrobní dokumentace a technologické postupy (C=5, I=5, A=4, průměr 4,67, třída Kritická)

Aktivum P1 reprezentuje stabilní aktiva s vyrovnaným vysokým hodnocením všech tří atributů. Výrobní dokumentace je hluboko v třídě Kritická s průměrnou hodnotou 4,67, což je téměř na maximální hodnotě stupnice.

Při změně hodnocení o jeden stupeň zůstává aktivum stabilně v třídě Kritická. Pouze plošné snížení všech tří atributů o jeden stupeň by aktivum přesunulo do třídy Vysoká. Tab 6) shrnuje vliv změn.

Tab 6) Citlivost aktiva P1 na změnu hodnocení

Scénář	C	I	A	Průměr	Třída
Původní hodnocení	5	5	4	**4,67**	**Kritická**
C snížena o 1	4	5	4	**4,33**	**Kritická**
I snížena o 1	5	4	4	**4,33**	**Kritická**
A snížena o 1	5	5	3	**4,33**	**Kritická**
C a I sníženy o 1	4	4	4	**4,00**	**Kritická (hranice)**
Všechny sníženy o 1	4	4	3	**3,67**	**Vysoká**

Aplikace váženého průměru s průmyslovými váhami dává hodnotu 4,50, což aktivum drží v třídě Kritická. Použití váhy s důrazem na důvěrnost by dalo hodnotu 4,70, opět Kritická.

Z analýzy vyplývá, že výrobní dokumentace patří mezi nejstabilnější aktiva. Výsledné zařazení je vůči drobným chybám hodnocení odolné a zachovává si stejnou klasifikaci jak při prostém, tak při váženém průměru. Pro praxi to znamená, že u takových aktiv lze metodice plně důvěřovat bez nutnosti doplňkové analýzy.

3.7 Souhrn výsledků aplikace metodiky

Aplikace navržené metodiky na modelový průmyslový podnik ukázala, že všech osm identifikovaných primárních aktiv spadá do třídy Vysoká nebo Kritická. Tři aktiva (S1 Služba výroby, P1 Výrobní dokumentace a P4 Účetní evidence) byla zařazena do třídy Kritická, zbývajících pět aktiv do třídy Vysoká.

Tento výsledek odpovídá očekávání, neboť všechna posuzovaná aktiva mají přímý vliv na chod podniku a jeho hlavní obchodní činnost. Pro praktický audit ISMS to znamená, že u všech těchto aktiv je nutné zavést přiměřená bezpečnostní opatření a věnovat jim odpovídající pozornost při řízení rizik.

4 DISKUZE A DOPORUČENÍ

Předchozí kapitola popsala návrh metodiky pro hodnocení informačních aktiv průmyslového podniku a její aplikaci na modelový případ. Cílem této kapitoly je kriticky zhodnotit dosažené výsledky, identifikovat silné a slabé stránky navrženého řešení a formulovat doporučení pro jeho praktické využití.

Diskuze vychází z hodnocení provedeného v kapitole 3.5 a z citlivostní analýzy v kapitole 3.6. Pozornost je věnována především otázce, zda navržená metodika splňuje cíle definované v zadání práce a jakým způsobem by mohla být uplatněna v reálném prostředí průmyslového podniku při auditu systému řízení bezpečnosti informací.

Kapitola je rozdělena do tří částí. Podkapitola 4.1 shrnuje a interpretuje výsledky aplikace metodiky na modelový podnik a vyvozuje obecnější závěry. Podkapitola 4.2 se věnuje limitům navržené metodiky, tedy aspektům, ve kterých je metodika omezena nebo by mohla vést k nepřesným výsledkům. Podkapitola 4.3 formuluje konkrétní doporučení pro praktické nasazení metodiky v organizacích a pro její další rozvoj.

4.1 Diskuze výsledků aplikace metodiky

Aplikace navržené metodiky na modelový průmyslový podnik vedla k identifikaci osmi primárních aktiv, která byla na základě hodnocení podle pětistupňové škály zařazena do dvou tříd. Tři aktiva se ocitla v třídě Kritická, zbylých pět v třídě Vysoká. Žádné aktivum nedosáhlo nižších tříd Střední ani Nízká.

Tento výsledek odpovídá očekávání plynoucímu z povahy zvolených aktiv. Všech osm aktiv představuje služby a informace přímo podporující hlavní činnost podniku. Z tohoto důvodu mají všechna aktiva vysokou významnost pro chod organizace, což se promítá do jejich klasifikace. Nepřítomnost aktiv v nižších třídách neukazuje na chybu v metodice, ale na skutečnost, že do hodnocení nebyla zařazena aktiva, která by typicky dosahovala nižších hodnot.

Mezi aktivy ve třídě Kritické patří služba výroby a dodávky komponentů (S1), výrobní dokumentace a technologické postupy (P1) a účetní a finanční evidence (P4). Společným rysem těchto aktiv je vysoké hodnocení napříč všemi třemi atributy CIA. Služba výroby a výrobní dokumentace představují samotnou podstatu obchodní činnosti podniku, jejich narušení by mělo přímý dopad na schopnost plnit zakázky a chránit konkurenční výhodu. Účetní evidence pak podléhá zákonným požadavkům a její integrita má fatální dopad na právní pozici organizace.

Aktiva ve třídě Vysoké zahrnují plánovací, skladové, personální, obchodní a kvalitativní informace. Tato aktiva podporují provoz podniku, avšak jejich krátkodobý výpadek nebo dílčí narušení nepředstavuje bezprostřední ohrožení existence organizace. Přesto vyžadují řízený přístup, pravidelné zálohování a kontrolu integrity.

Citlivostní analýza provedená v kapitole 3.6 ukázala, že stabilita zařazení aktiv do tříd se mezi jednotlivými aktivy výrazně liší. Výrobní dokumentace představuje stabilní aktivum, jehož klasifikace zůstává konstantní i při změně hodnocení o jeden stupeň nebo při použití váženého průměru. Naproti tomu skladová evidence se nachází blízko hranice tříd a její zařazení může ovlivnit i drobná změna hodnocení. Personální evidence poté ukázala, že volba vah zásadně mění výsledek u aktiv s výraznou disperzí mezi atributy. Při zohlednění požadavků na ochranu osobních údajů by aktivum spadalo do třídy Kritická, nikoli pouze Vysoká.

Z provedeného hodnocení vyplývá několik obecnějších závěrů. Navržená metodika umožňuje systematicky a transparentně klasifikovat primární aktiva podle jejich významnosti pro organizaci. Použití pětistupňové škály poskytuje dostatečnou jemnost pro rozlišení mezi aktivy bez toho, aby byl proces hodnocení neúměrně složitý. Zavedení override pravidla pro aktiva s hodnocením 5 v některém z atributů zajišťuje, že kriticky důležité atributy nejsou rozředěny aritmetickým průměrováním. Současně se ukázalo, že u aktiv blízko hranic tříd je třeba věnovat zvláštní pozornost interpretaci výsledku.

4.2 Limity navržené metodiky

Žádná metodika hodnocení aktiv není dokonalá a navržené řešení není výjimkou. Identifikace limitů je důležitým krokem, který umožňuje uživatelům metodiky správně interpretovat výsledky a předem počítat s jejím omezením. V této podkapitole jsou rozebrány hlavní oblasti, kde má navržená metodika své slabiny.

Subjektivita kvalitativního hodnocení představuje obecný limit všech kvalitativních metod, navrženou metodiku nevyjímaje. Hodnocení atributů CIA na pětistupňové škále vychází z odborného úsudku hodnotitele, který interpretuje popisy jednotlivých stupňů a aplikuje je na konkrétní aktivum. Různí hodnotitelé mohou téže aktivum klasifikovat odlišně podle své zkušenosti, znalosti prostředí organizace nebo aktuálního pohledu na rizika. Tento limit lze částečně zmírnit hodnocením v týmu, opakováním hodnocení nebo využitím podrobnějších popisů jednotlivých stupňů.

Omezení prostého aritmetického průměru se projevuje zejména u aktiv s výraznou disperzí mezi jednotlivými atributy CIA. Citlivostní analýza ukázala, že personální evidence s hodnocením 5, 4, 2 dostává průměr 3,67 a spadá do třídy Vysoká, ačkoli z hlediska ochrany osobních údajů by mohla být klasifikována jako Kritická. Aritmetický průměr rozřeďuje extrémní hodnoty a může vést k podhodnocení aktiv s jedním kritickým atributem. Override pravidlo, podle kterého aktivum s alespoň jedním atributem ohodnoceným stupněm 5 spadá minimálně do třídy Vysoká, tento limit částečně řeší. Nepokrývá však několik dalších situací:

- Aktiva s atributem hodnoty 4 (nikoli 5), která mají vážné dopady, ale prostý průměr je zařadí do nižších tříd. Například aktivum s hodnocením C=4, I=2, A=2 (vážné poškození při úniku) dostane průměr 2,67 a spadá do třídy Střední.
- Odvětvové priority atributů, kdy v daném prostředí jeden atribut převažuje nad ostatními (například dostupnost ve výrobě nebo důvěrnost u osobních údajů). Prostý průměr s tímto pravidlem nepočítá.
- Kombinovaný efekt dvou středně vysokých atributů, kdy aktivum s hodnocením C=4, I=4, A=2 dostane průměr 3,33 (Vysoká), ale logicky by mělo mít vyšší prioritu než aktivum se stejnou průměrnou hodnotou, ale rozloženou jinak.
- Regulační požadavky (GDPR, oborové normy), které mohou požadovat klasifikaci do vyšší třídy bez ohledu na výslednou hodnotu průměru.

Pro pokrytí těchto situací by bylo vhodné rozšířit metodiku o vážený průměr s odvětvově specifickými váhami nebo o doplňková override pravidla zohledňující regulační požadavky.

Citlivost u hraničních aktiv se vyskytuje u aktiv, jejichž průměrná hodnota se nachází blízko hranice mezi dvěma třídami. Skladová evidence s průměrem 3,33 leží blízko spodní hranice třídy Vysoká a pouhá změna hodnocení o jeden stupeň u dvou atributů by ji přesunula do třídy Střední. Metodika v takových případech vyžaduje od hodnotitele zvýšenou pozornost a případně opakované hodnocení s ověřením výsledku.

Generický charakter metodiky je jejím záměrem, ale zároveň i omezením. Metodika byla navržena tak, aby byla použitelná v různých typech průmyslových podniků, a nezohledňuje specifika jednotlivých odvětví. Konkrétní organizace by mohla potřebovat upravit popisy stupňů, přidat odvětvově specifická aktiva nebo zohlednit regulační prostředí, ve kterém působí. Pro reálné nasazení je proto nezbytné metodiku přizpůsobit konkrétním podmínkám.

Závislost na zkušenosti hodnotitele je posledním významným limitem. Kvalitní hodnocení aktiv vyžaduje znalost informačních systémů organizace, jejích obchodních procesů a regulačního prostředí. Hodnotitel bez dostatečné zkušenosti může nesprávně interpretovat popisy stupňů nebo přehlédnout významné aspekty hodnoceného aktiva. Tento limit nelze zcela odstranit, lze jej však zmírnit zapojením více odborníků z různých částí organizace do procesu hodnocení.

4.3 Doporučení pro praktické nasazení

Na základě poznatků z aplikace metodiky a identifikovaných limitů jsou v této podkapitole formulována praktická doporučení pro organizace, které by metodiku chtěly použít při hodnocení svých informačních aktiv a při auditu systému řízení bezpečnosti informací. Doporučení jsou rozdělena do čtyř oblastí: postup při zavedení metodiky, řešení specifických typů aktiv a možnosti dalšího rozvoje metodiky.

Postup při zavedení v organizaci by měl začínat fází přípravy, ve které je sestaven tým hodnotitelů složený z pracovníků různých odborných oblastí. Doporučuje se zapojit zástupce IT oddělení, vedení podniku, právního oddělení a klíčových provozních útvarů. Před samotným hodnocením je vhodné popisy jednotlivých stupňů na pětistupňové škále přizpůsobit konkrétnímu prostředí organizace. Hodnocení by mělo probíhat formou společných pracovních setkání, na kterých jednotliví členové týmu prezentují svůj návrh hodnocení a společně dospějí ke shodě. Tento přístup omezuje subjektivitu hodnocení a využívá expertní znalost jednotlivých členů týmu.

Hodnocení sporných a hraničních aktiv vyžaduje zvýšenou pozornost. U aktiv, jejichž průměrná hodnota se pohybuje blízko hranice mezi třídami (například mezi 2,90 a 3,10), je doporučeno provést hodnocení opakovaně s odstupem několika dnů nebo s jiným složením týmu. Pokud se výsledky liší, je vhodné přiřadit aktivu konzervativně vyšší třídu, neboť důsledky podhodnocení jsou v praxi závažnější než důsledky mírného nadhodnocení.

Aktiva podléhající regulačním požadavkům je vhodné hodnotit s ohledem na specifické předpisy. U aktiv obsahujících osobní údaje by se měla zvážit aplikace váženého průměru s důrazem na důvěrnost, který lépe odráží požadavky obecného nařízení o ochraně osobních údajů. Doporučená sada vah pro tato aktiva je 0,5 pro důvěrnost, 0,3 pro integritu a 0,2 pro dostupnost. U aktiv kritických z hlediska výrobních procesů lze naopak použít váhy s důrazem na dostupnost (0,2 pro důvěrnost, 0,3 pro integritu a 0,5 pro dostupnost), které lépe vystihují skutečné dopady výpadku.

Využití metodiky v rámci auditu ISMS představuje jeden z hlavních cílů jejího návrhu. Výsledná tabulka klasifikovaných aktiv slouží auditorovi jako podklad pro posouzení přiměřenosti zavedených bezpečnostních opatření. Aktiva ve třídě Kritická musí být chráněna nejpřísnějšími opatřeními včetně redundance, plánu kontinuity provozu a pravidelného nezávislého auditu. Aktiva ve třídě Vysoká vyžadují posílená opatření s důrazem na řízený přístup, zálohování a monitoring. Pro každé aktivum by měla existovat dokumentace popisující aplikovaná opatření a způsob jejich kontroly.

Doporučení pro další rozvoj metodiky zahrnují několik směrů, kterými by mohla být metodika rozšířena. Prvním z nich je propojení s konkrétními bezpečnostními opatřeními tak, aby výsledná třída aktiva automaticky generovala doporučená opatření z katalogu (například z

katalogu NÚKIB). Druhým směrem je rozšíření o kvantitativní hodnocení rizik, které by k třídě aktiva doplnilo odhad pravděpodobnosti a finančních dopadů jednotlivých scénářů. Třetím směrem je vytvoření odvětvově specifických verzí metodiky, které by zohledňovaly specifika různých typů průmyslových podniků (potravinářský, strojírenský, chemický, energetický). Posledním směrem je integrace s existujícími nástroji pro řízení rizik, zejména s EBIOS Risk Manager nebo s nástroji uvedenými v databázi ENISA.

5 ZÁVĚR

Tato bakalářská práce se věnovala stanovení hodnoty informací v průmyslovém podniku pro audit systému řízení bezpečnosti informací. Cílem práce bylo popsat současný stav vědy v oblasti informační a kybernetické bezpečnosti, provést rešerši relevantních norem a legislativy Evropské unie a České republiky, zpracovat systémový rozbor řešené problematiky a navrhnout metodiku pro stanovení a ohodnocení informačních aktiv, doplněnou o vlastní závěry a doporučení pro další rozvoj řešené problematiky.

Teoretická část přinesla rozbor aktuální situace v oblasti kybernetické bezpečnosti. Z analýzy zpráv Evropské agentury pro kybernetickou bezpečnost (ENISA) a Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) vyplynulo, že přestože počet incidentů klesá k dlouhodobému průměru, jejich závažnost roste. To naznačuje posun směrem k cíleným útokům s vážnějšími dopady, na který reaguje nová evropská i česká legislativa. Byly vymezeny základní pojmy podle zákona č. 264/2025 Sb. a popsány principy CIA triády, systému řízení bezpečnosti informací a Demingova PDCA cyklu. Legislativní rámec zahrnoval transpozici směrnice NIS2 do českého právního řádu novým zákonem o kybernetické bezpečnosti a jeho prováděcími vyhláškami č. 408, 409 a 410/2025 Sb. Z mezinárodních norem byla popsána řada ISO/IEC 27000 a norma ISO 55000. Závěr teoretické části byl věnován klasifikaci a hodnocení informačních aktiv a existujícím nástrojům pro analýzu rizik, mezi něž patří metodiky CRAMM, EBIOS Risk Manager a Průvodce řízením aktiv a rizik vydaný NÚKIB.

Hlavním přínosem práce je vlastní návrh metodiky pro hodnocení informačních aktiv průmyslového podniku. Metodika vychází z pětikrokového postupu zahrnujícího identifikaci primárních aktiv, mapování podpůrných a technických aktiv, přiřazení garantů, hodnocení podle atributů CIA a výpočet výsledné hodnoty s následným zařazením do tříd. Pro hodnocení byla zvolena pětistupňová kvalitativní škála navržená s ohledem na rámec vyhlášky č. 409/2025 Sb. a inspirovaná metodikou NÚKIB. Výsledná hodnota se počítá jako prostý aritmetický průměr tří atributů CIA. Metodika byla doplněna o pravidlo zajišťující, že aktivum s alespoň jedním atributem ohodnoceným nejvyšším stupněm 5 nebude zařazeno do nižších tříd než Vysoká.

Funkčnost metodiky byla demonstrována její aplikací na modelový průmyslový podnik. Bylo identifikováno osm primárních aktiv tvořených jednou službou výroby a sedmi souvisejícími informacemi. Tři aktiva, konkrétně služba výroby a dodávky komponentů, výrobní dokumentace a účetní evidence, byla zařazena do třídy Kritická. Zbývajících pět aktiv spadlo do třídy Vysoká. Tento výsledek odpovídal očekávání, neboť všechna posuzovaná aktiva podporují hlavní činnost podniku.

Robustnost metodiky byla ověřena citlivostní analýzou provedenou na třech reprezentativních aktivech. Analýza prokázala, že výrobní dokumentace představuje stabilní aktivum odolné vůči drobným změnám hodnocení i vůči volbě metody zprůměrování. Skladová evidence se ukázala jako citlivá z důvodu blízkosti hranice mezi třídami, kde i drobná změna hodnocení může vést k posunu do nižší třídy. Personální evidence pak demonstrovala, že volba vah zásadně mění výsledek u aktiv s výraznou disperzí atributů. Při použití váženého průměru s důrazem na důvěrnost, který lépe odpovídá požadavkům GDPR, by toto aktivum spadalo do třídy Kritická místo Vysoká.

V rámci diskuze byly identifikovány limity metodiky, mezi něž patří subjektivita kvalitativního hodnocení, omezení prostého aritmetického průměru u aktiv s disperzí atributů, citlivost u hraničních aktiv, generický charakter metodiky a závislost na zkušenosti hodnotitele. Pro praktické nasazení byla formulována doporučení zahrnující sestavení mezioborového týmu hodnotitelů, opakované hodnocení sporných a hraničních aktiv, aplikaci váženého průměru s

konkrétními sadami vah u aktiv podléhajících regulačním požadavkům a využití výsledků jako podkladu pro audit ISMS.

Cíle stanovené v zadání bakalářské práce byly splněny. Současný stav vědy v oblasti informační a kybernetické bezpečnosti byl popsán v kapitole 2, ve které byla rovněž zpracována rešerše relevantních norem a legislativy Evropské unie a České republiky. Systémový rozbor problematiky a návrh metodiky stanovení a ohodnocení informačních aktiv jsou obsaženy v kapitole 3. Vlastní závěry a doporučení pro další rozvoj řešené problematiky tvoří kapitolu 4.

Možné směry dalšího rozvoje navržené metodiky zahrnují propojení s konkrétními bezpečnostními opatřeními tak, aby výsledná třída aktiva automaticky generovala doporučená opatření z katalogu hrozeb a opatření vydaného NÚKIB, rozšíření o kvantitativní hodnocení rizik s odhadem pravděpodobnosti a finančních dopadů, vytvoření odvětvově specifických verzí metodiky pro různé typy průmyslových podniků a integraci s existujícími nástroji pro řízení rizik, zejména s EBIOS Risk Manager. Navržená metodika představuje použitelný nástroj pro malé a střední průmyslové podniky, které potřebují systematicky hodnotit svá informační aktiva v souladu s požadavky nové české legislativy v oblasti kybernetické bezpečnosti.

.

6 SEZNAM POUŽITÝCH ZDROJŮ

1] ENISA. *ENISA Threat Landscape 2025*. Online. 2025. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025. [cit. 2026-03-22].

2] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Kybernetické incidenty pohledem NÚKIB: Březen 2026*. Online. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2026. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-brezen2026.pdf. [cit. 2026-04-30].

3] Zákon č. 264/2025 Sb., o kybernetické bezpečnosti. In: *Sbírka zákonů České republiky*. 2025, částka 264. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-264. [cit. 2026-04-07].

4] ONDRÁK, Viktor; SEDLÁK, Petr a MAZÁLEK, Vladimír. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

5] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN ISO/IEC 27000, *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Česká agentura pro standardizaci, 2020.

6] EUROPEAN COMMISSION. *EU cybersecurity policies*. Online. 2026. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. [cit. 2026-04-04].

7] EUROPEAN COMMISSION. *Akt EU o kybernetické bezpečnosti*. Online. Shaping Europe's digital future. 2026. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/cybersecurity-act. [cit. 2026-04-30].

8] Vyhláška č. 408/2025 Sb. o regulovaných službách. In: *Sbírka zákonů České republiky*. 2025. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-408. [cit. 2026-05-17].

9] Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. In: *Sbírka zákonů České republiky*. 2025. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-409. [cit. 2026-04-22].

10] Vyhláška č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. In: *Sbírka zákonů České republiky*. 2025. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-410. [cit. 2026-05-17].

11] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR). In: *Úřední věstník Evropské unie*. 2016. Dostupné z: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [cit. 2026-04-07].

12] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. In: *Sbírka zákonů České republiky*. 2016. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297. [cit. 2026-04-07].

13] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2004. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499. [cit. 2026-04-07].

14] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN ISO 55000, *Management aktiv – Slovník, přehled a zásady*. Online. Praha: Česká agentura pro standardizaci, 2025. [cit. 2026-04-21].

15] CYBRELA S.R.O. *Aktivum v kybernetické bezpečnosti*. Online. AION CS, S. R. O. Zákony pro lidi. 2025. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-264. [cit. 2026-05-03].

16] EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Risk Management - Risk Assessment Methods*. Online. ENISA. 2022. Dostupné z: https://tools.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/. [cit. 2026-05-17].

17] EUROPEAN UNION AGENCY FOR CYBERSECURITY. *CRAMM*. Online. ENISA. 2022. Dostupné z: https://tools.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [cit. 2026-05-17].

18] AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. *La méthode EBIOS Risk Manager*. Online. Cyber.gouv.fr. 2024. Dostupné z: https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/. [cit. 2026-05-17].

19] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. Online. 2022. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf. [cit. 2026-05-17].

7 SEZNAM ZKRATEK, SYMBOLŮ, OBRÁZKŮ A TABULEK

7.1 Seznam zkratek

ANSSI	Agence nationale de la sécurité des systèmes d'information
CCTA	Central Computer and Telecommunications Agency
CIA	Confidentiality, Integrity, Availability (Důvěrnost, Integrita, Dostupnost)
CRAMM	CCTA Risk Analysis and Management Method
ČSN	Česká technická norma
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ECCF	European Cybersecurity Certification Framework
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
EU	Evropská unie
GDPR	General Data Protection Regulation
HR	Human Resources
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MES	Manufacturing Execution System
NIS	Network and Information Security
NIS2	Druhá směrnice o bezpečnosti sítí a informací
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan-Do-Check-Act
PhaaS	Phishing-as-a-Service
PLM	Product Lifecycle Management

7.2 Seznam tabulek

TAB 1) HODNOTÍCÍ STUPNICE PRO ATRIBUTY CIA 24
TAB 2) TŘÍDY AKTIV PODLE VÝSLEDNÉ HODNOTY 25
TAB 3) IDENTIFIKACE A HODNOCENÍ PRIMÁRNÍCH AKTIV MODELOVÉHO PODNIKU 26
TAB 4) CITLIVOST AKTIVA P3 NA ZMĚNU HODNOCENÍ 29
TAB 5) VLIV VAH NA HODNOCENÍ AKTIVA P5 30
TAB 6) CITLIVOST AKTIVA P1 NA ZMĚNU HODNOCENÍ 31

7.3 Seznam obrázků

OBR. 1) MODEL PDCA V ISMS (NĚKDY TAKÉ OZNAČOVANÝ JAKO ŽIVOTNÍ CYKLUS ISMS)[4]16