**NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti**

**NIS2 and its causes on healthcare and other departments, new Cybersecurity law**

Projekt 4.

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D.

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2022/2023

**Z a d á n í P r o j e k t IV**

Student: **Šimon Kochánek**

Obor: Informatika a kybernetika ve zdravotnictví

Téma: **NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti**

Téma anglicky: **NIS2 and its causes on healthcare and other departments, new Cybersecurity law**

Z á s a d y p r o v y p r a c o v á n í :

Student představí NIS2 a také nový ZoKB. Poté zpracuje rešerši na změny řízení Kybernetické bezpečnosti ve zdravotních zařízeních, které budou podléhat novémeu zákonu. NIS2 začne platit od roku 2024 a výrazně zasáhne do oblast IT bezpečnosti.

Seznam odborné literatury:

1. <https://osveta.nukib.cz/course/view.php?id=145>
2. <https://www.isvs.cz/smernice-nis-2-koho-se-tyka-a-jak-ji-aplikovat-v-praxi/>
3. <https://www.epravo.cz/top/clanky/nis2-nova-regulace-kyberneticke-bezpecnosti-veu-115691.html>
4. <https://nis2.tech/>

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 12.3.2023

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedry

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 14.5.2023 …...….………...………………...

Jméno autora vč. titulů

**PODĚKOVÁNÍ**

Rád bych vyjádřil upřímné poděkování doktorce Brechlerové za její vedení mého semestrálního projektu. Cením si jejího přístupu, který mi umožnil pracovat na projektu s větší svobodou a bez přísných pravidel. Děkuji jí za vedení a motivaci, které mi pomohly rozvíjet své schopnosti a mé pracovní příležitosti v oblasti kyberbezpečnosti. Její přístup k mému zpracování byl otevřený a konstruktivní, a jsem jí za to velmi vděčný.

**ABSTRAKT**

NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti

Tato semestrální práce se zaměřuje na detailní průzkum a analýzu nově implementovaných směrnic NIS2 a ZoKB, s důrazem na jejich dopad na řízení kybernetické bezpečnosti ve zdravotnických zařízeních. Nové směrnice představují zásadní změny v oblasti IT bezpečnosti, které budou mít významný dopad na zdravotnická zařízení. Směrnice NIS2, která začne platit od roku 2024, přináší řadu nových požadavků a standardů týkajících se kybernetické bezpečnosti. Souběžně s tím, práce zkoumá novou ZoKB, jež představuje další klíčový legislativní nástroj v tomto kontextu. Práce nabízí rešerši těchto změn a diskutuje jejich potenciální dopady na zdravotnická zařízení, která budou muset tyto nové požadavky splnit.

**Klíčová slova**

NIS2, ZoKB, Směrnice NIS2, nový ZoKB, NIS2 zdravotnictví

**ABSTRACT**

NIS2 and its causes on healthcare and other departments, new Cybersecurity law

This term paper focuses on detailed research and analysis of the newly implemented NIS2 and ZoKB guidelines, with an emphasis on their impact on cybersecurity management in healthcare facilities. The new directives represent major changes in IT security that will have a significant impact on healthcare facilities. The NIS2 Directive, which will come into force in 2024, introduces several new requirements and standards relating to cyber security. In parallel, the thesis examines the new ZoKB, which represents another key legislative instrument in this context. The thesis offers an exploration of these changes and discusses their potential impact on healthcare facilities that will have to comply with these new requirements.

**Keywords**

NIS2, ZoKB,Directive NIS2, new ZoKB, NIS2 healthcare

Obsah

[Seznam symbolů a zkratek 8](#_Toc137569358)

[1 Úvod 9](#_Toc137569359)

[1.1 Přehled současného stavu 10](#_Toc137569360)

[1.2 Cíle práce 10](#_Toc137569361)

[2 Metody 11](#_Toc137569367)

[2.1 Současný stav NIS1 a ZoKB 11](#_Toc137569368)

[2.1.1 NIS 1 11](#_Toc137569369)

[2.1.2 Zákon o Kybernetické Bezpečnosti č. 181/2014 11](#_Toc137569370)

[3 Výsledky 12](#_Toc137569371)

[4 Diskuse 14](#_Toc137569372)

[5 Závěr 15](#_Toc137569373)

[Seznam použité literatury 16](#_Toc137569374)

[Příloha A: Požadavky na formátování práce 17](#_Toc137569375)

[Příloha B: Základní typografické zásady 18](#_Toc137569376)

[Příloha C: Další doporučení pro přehlednost textu 19](#_Toc137569377)

[Příloha D: Obsah přiloženého CD 20](#_Toc137569378)

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| ALI | Akutní plicní selhání (*Acute Lung Injury*) |
| PID | Proporcionálně-integračně-derivační |

# Úvod

V digitálním věku, kdy společnosti stále více závisí na informačních a komunikačních technologiích, se otázka kybernetické bezpečnosti stala neoddělitelnou součástí našeho života. Direktiva o bezpečnosti sítí a informačních systémů (NIS1), která byla v roce 2016 přijata Evropskou unií, představovala první pokus o vytvoření soudržného rámcového práva pro zajištění kybernetické bezpečnosti v celé EU. Cílem bylo dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů v celé Unii, aby tak byla zajištěna její digitální rezistence.

Nicméně, jak se technologie rychle vyvíjejí a kybernetické hrozby se stávají sofistikovanějšími a diverzifikovanějšími, stává se jasné, že NIS1 již není schopna dostatečně řešit současné výzvy v oblasti kybernetické bezpečnosti. Důležité je zdůraznit, že od doby, kdy byla NIS1 implementována, došlo k dramatickým změnám v digitální krajině. Digitální technologie se staly integrální součástí našeho každodenního života a fungování ekonomiky, což znamená, že potenciální dopady kybernetických útoků jsou nyní mnohem větší než kdy dříve.

Vzhledem k těmto novým výzvám a příležitostem bylo nezbytné provést revizi NIS1. Cílem této revize bylo zajistit, že regulace EU v oblasti kybernetické bezpečnosti zůstane aktuální a efektivní vzhledem k rychlým změnám v digitální krajině.

Tato semestrální práce se proto zaměří na zkoumání NIS2, navrhované revize NIS1, s cílem zhodnotit její potenciál pro zlepšení kybernetické bezpečnosti v EU. Kromě toho se budu věnovat také analýze nového zákona o kybernetické bezpečnosti v České republice, který představuje náši národní odpověď na NIS2 a je klíčový pro integraci této evropské směrnice do našeho právního systému.

## Přehled současného stavu

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., v platném znění, představuje klíčový právní dokument pro řízení a zajišťování kybernetické bezpečnosti v České republice. Byl přijat s cílem ochránit kritickou infrastrukturu země a zajišťovat bezpečnost informačních systémů a sítí.

Tento zákon stanovuje rámec pro identifikaci a ochranu kritických informačních infrastruktur, stanovení bezpečnostních standardů a postupů a koordinaci mezi různými subjekty v oblasti kybernetické bezpečnosti. Zákon také zřizuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako hlavní regulační orgán v této oblasti.

Nicméně, i přes jeho význam, zákon čelí kritice za některé jeho aspekty. Někteří kritici poukazují na to, že zákon může být příliš obecný v některých svých ustanoveních, což může vést k nejednoznačnosti v jeho interpretaci a aplikaci. Dalšími oblastmi, které vyvolávají diskusi, jsou například otázky soukromí a ochrany osobních údajů v kontextu kybernetické bezpečnosti.

Je důležité poznamenat, že tento zákon byl přijat v roce 2014, a od té doby se digitální prostředí výrazně změnilo. Nové technologie, jako je cloud computing, Internet věcí (IoT) a umělá inteligence, přinášejí nové výzvy v oblasti kybernetické bezpečnosti, které tento zákon nemusí plně pokrýt. Proto je aktuální revize a aktualizace tohoto zákona klíčovou otázkou pro zajištění efektivní ochrany kybernetické bezpečnosti v České republice.

## Cíle práce

* Zjistit současný stav NIS1 a ZoKB.
* Nastudovat NIS2, pochopit důvody zavedení, a její význam.
* Projít si změny navrhované NÚKIBem a pochopit změny týkající se nového ZoKB
* Zanalyzovat změny a nové subjekty pro řízení Kybernetické bezpečnosti
* Zhodnotit změny pro zdravotnické subjekty

# Metody

## Současný stav NIS1 a ZoKB

Tři základní dokumenty pro Kybernetickou Bezpečnost v ČR:

- NIS1 – směrnice od EU 2016/1148

- ZoKB – Zákon o Kybernetické Bezpečnosti č.181/2014

- Vyhláška 82/2018 – Vyhláška o Kybernetické bezpečnosti

Pojďme si každý dokument představit:

### NIS 1

Směrnice o síťové a informační bezpečnosti (NIS), známá také jako NIS1, je první legislativní krok Evropské unie v oblasti kybernetické bezpečnosti. Byla přijata v červenci 2016 s cílem zvýšit celkovou úroveň kybernetické bezpečnosti v EU. NIS1 se zaměřuje na poskytování právních rámců pro zajištění bezpečnosti sítí a informací, zvláště u operátorů základních služeb (například v energetice, dopravě, bankovnictví a zdravotní péči) a poskytovatelů digitálních služeb (jako jsou online tržiště, cloudové služby a vyhledávače).

Směrnice stanovuje minimální bezpečnostní standardy a požadavky na oznámení incidentů pro tyto společnosti. Dále také požaduje, aby všechny členské státy EU zřídily nezávislý národní úřad pro kybernetickou bezpečnost, který by měl dostatečné zdroje na to, aby mohl reagovat na incidenty a monitorovat uplatňování těchto bezpečnostních opatření. Tento rámec také podporuje spolupráci mezi členskými státy EU v oblasti sdílení informací a nejlepších postupů.

### Zákon o Kybernetické Bezpečnosti č. 181/2014

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., který byl vyhlášen dne 29. srpna 2014 a nabyl účinnosti od 1. ledna 2015, je klíčovým předpisem České republiky, který se zabývá bezpečností kyberprostoru.

Tento zákon je úzce spojen s několika prováděcími předpisy, včetně Vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, Vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích a Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury1.

Základním cílem tohoto zákona je zvýšit bezpečnost kybernetického prostoru, zejména ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Tento zákon se však nesnaží řešit všechna rizika v kyberprostoru, jako je porušování autorských práv, různé podvodné aktivity, úniky elektronických dat či šíření závadného elektronického obsahu.

Pro orgány a osoby, které určuje zákon, přibude řada nových povinností v oblasti zajištění bezpečnosti informačních a komunikačních systémů a komunikace s určenými kontaktními místy. Zákon také stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu.

Povinnosti plynoucí ze zákona se dotýkají jen vymezeného okruhu právnických osob, orgánů a podnikajících fyzických osob. To ale neznamená, že ostatních subjektů se potřeba chránit své informační a komunikační systémy před neustále narůstajícími kybernetickými hrozbami nijak netýká. Pro tyto subjekty může zákon a zejména vyhláška sloužit jako vhodná inspirace nebo metodika.

Zákon také zavádí několik nových pojmů, včetně:

- "Kybernetický prostor" jako digitální prostředí umožňující zpracování informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.

- "Kritická informační infrastruktura" jako prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.

- "Významný informační systém" jako informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

# Výsledky

Věnujte kapitolu pouze přehlednému podání výsledků, nikoliv jejich diskusi. Data uvádějte zejména v grafech a tabulkách. Preferovány jsou grafy – tabulky se všemi naměřenými hodnotami, ze kterých grafy vycházejí, lze umístit do příloh práce.

Výsledky mají vždy obsahovat hlavní text, který zasadí prezentované obrázky a tabulky do souvislosti s předchozím textem a čtenáře prezentovanými daty provede. Prezentování výsledků ve formě nekomentovaného obrázkového alba je v drtivé většině případů nevhodné.

Na každý obrázek musí být uveden odkaz v textu, který má formát jako v následující větě. Obrázek se vždy čísluje a popisuje pod obrázkem, viz příklad na Obr. 3.1.



**Obr. 3.1:** Tulipány před ozářením kryptonitem. Fotografie: autor.

Obrázky číslujte podle hlavní kapitoly, ve které se vyskytují. Podkapitoly se již neuvažují. To znamená, že obrázky v úvodu (typicky kap. 1) budou: Obr. 1.1, Obr. 1.2 atd. V metodách (typicky druhá velká kapitola) budou číslovány Obr. 2.1, Obr. 2.2, Obr. 2.3 atd.

Popis tabulky, na rozdíl od obrázku, je zpravidla nad tabulkou, viz Tabulka 3.1. Není nutné v něm opisovat celý obsah záhlaví tabulky, které následuje hned vzápětí. Jednotlivé proměnné v tabulce jsou řazeny do sloupců. V tabulce jsou nezávislé proměnné, kategorie probandů apod. řazeny vlevo, závislé proměnné vpravo. Jednotky uvádějte v kulatých závorkách v záhlaví tabulky, ne u každého čísla zvlášť. Vysvětlující poznámky (např. dosažená hladina významnosti, zda jsou data udávána jako průměr + směrodatná chyba průměru, jaký statistický test byl použit apod.) jsou umisťovány pod tabulku a odkaz na ně se udává jako horní index (symboly, čísla, písmena) na příslušném místě tabulky. Na každý obrázek a tabulku je třeba odkazovat z hlavního textu.

**Tabulka 3.1:** Reakční čas *T*20 signálu periferní saturace kyslíkem, *Sp*O2, měřený třemi různými přístroji.

|  |  |  |  |
| --- | --- | --- | --- |
|  | *T*20 (s) | | |
| Fáze | Root Radical-7 | Nellcor N-600 | Carescape B650 |
| Hypoxická | 52±15\* | 65±19\* | 56±15 |
| Hyperoxická | 43±14 | 55±28 | 49±15 |
| Hyperkapnická | 75±23 | 119±47# | 73±41# |

Data byla měřena pro shodnou skupinu 14 probandů a jsou uvedena jako aritmetický průměr ± směrodatná odchylka. Symboly \* a # značí statisticky významný rozdíl (*p*<0,05) časů pro shodnou fázi.

# Diskuse

V této části shrňte získané výsledky (hlavní zjištění práce) a následně tyto výsledky interpretujte s ohledem na cíle práce. Lze též získané výsledky a výstupy konfrontovat s výsledky a výstupy jiných autorů, výrobky jiných společností apod. Nezbytné je správné uvádění zdrojů (citace prací, které jsou zde porovnávány a diskutovány). Diskutují se rovněž limitace práce. Nakonec lze nastínit další směřování práce do budoucna, opatrně spekulovat o klinickém významu práce apod.

# Závěr

Závěr stručně shrnuje splnění vytyčených cílů práce.

Shrnutí splněných (nebo snad v menší míře nesplněných) cílů práce navazuje na úvod práce. Z dalších částí práce (metody, výsledky a diskuse) je přebíráno jen to nejpodstatnější a v minimální nutné míře – závěr práce nemá být zopakováním abstraktu, výsledků nebo diskuse. Konec závěru může obsahovat podložené spekulace o významu práce do budoucna nebo výrazná doporučení pro další výzkum nebo praxi, pokud z výsledků předkládané práce přímo vyplývají.

# Seznam použité literatury

[1] s.r.o, Pixelfield, and Jana Blehová. “Co přináší zákon o kybernetické bezpečnosti.” T-SOFT, 13 Jan. 2015, https://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/.

# Příloha A: Požadavky na formátování práce

* Pro hlavní text práce používejte patkové písmo (Times New Roman, Georgia, Garamond apod.), velikost 12. Rovnice, matematické symboly apod. by měly být sázeny stejným, nebo alespoň co nejpodobnějším písmem stejné velikosti. Popisy obrázků a tabulek sázejte stejným písmem se zmenšenou velikostí. Nadpisy, čísla stránek, případné záhlaví či zápatí apod. mohou být sázeny buď stejným písmem jako hlavní text, nebo písmem bezpatkovým (např. Calibri). **V celé práci musí být použity maximálně dvě různá písma.**
* Řádkování práce, odsazení odstavců, velikosti písma v nadpisech apod. definují přímo jednotlivé styly použité v této šabloně.
* Okraje stránek práce jsou vždy 2,5 cm na každé straně plus 1 cm u hřbetu práce (levá strana).
* Práce je tištěna jednostranně, na papír formátu A4.
* Stránky se číslují arabskými číslicemi počínaje první (titulní) stranou. Číslování stránek se zobrazuje až od první stránky obsahu, což znamená, že na titulní straně, v zadání, prohlášení, poděkování a abstraktech se číslo stránky neuvádí.
* Hlavní kapitoly práce, počínaje Úvodem a konče Závěrem, jsou číslovány arabskými číslicemi. Seznam použité literatury číslo nemá. Přílohy označujte velkými písmeny anglické abecedy.
* Každou hlavní kapitolu práce (nadpis 1. úrovně) začínejte na samostatné stránce.

# Příloha B: Základní typografické zásady

* Fyzikální a fyziologické veličiny a matematické proměnné se sázejí proloženě (kurzívou). Zkratky a symboly, pod kterými se neskrývá číselná hodnota, jsou sázeny normálním písmem – stejně jako označení fyzikálních jednotek.
* Jednotky veličin a symboly (například procenta) se v textu od číselných údajů oddělují nezlomitelnou mezerou. Zápis bez mezery má význam přídavného jména. Např. „10 Ω“ čteme „deset ohmů“ a „10Ω“ čteme „desetiohmový“.
* Nezlomitelnou mezeru je nutné v editoru textu vyznačit. Např. v aplikaci Microsoft Word se použije kombinace <Shift> + <Ctrl> + <mezerník>.
* Neslabičné předložky a spojky (netýká se „a“) nesmí zůstat na konci řádku. Proto za nimi používejte nezlomitelnou mezeru.
* Rozlišujte spojovník a pomlčku. Spojovník je krátká čára používaná ke spojení dvou slov (např. česko-anglický slovník). Pomlčka slouží k vyznačení prodlevy v textu, pak ji obvykle píšeme s mezerami, nebo k vyznačení rozsahu (5–10), kdy se píše bez mezer.

# Příloha C: Další doporučení pro přehlednost textu

* Obrázky a tabulky sázejte v textu samostatně, bez obtékání textu po stranách. Nevkládejte obrázky a tabulky na stránku před skončením odstavce. Zkontrolujte, že popis obrázku nebo tabulky zůstal na stejné straně jako vlastní obrázek nebo tabulka.
* První řádek odstavce by neměl zůstat sám na konci řádky (tzv. vdova) a poslední řádek odstavce by neměl zůstat sám na začátku nové stránky (tzv. sirotek).
* Veškeré zkratky, s výjimkou těch nejznámějších jako DNA, by měly být v práci vysvětleny při prvním výskytu v hlavním textu a současně také v abstraktu, pokud je nutné je v něm použít.
* Na rovnice odkazujte jejich číslem, a to až za jejich uvedením v textu práce.
* Všechny obrázky a tabulky v práci musí být odkazovány z hlavního textu pomocí svých čísel.

# Příloha D: Obsah přiloženého CD

Poslední přílohou práce je obsah přiloženého datového nosiče. Typ a povinný obsah datového nosiče je specifikován na stránkách FBMI ČVUT v Praze. Pro odevzdávané práce v předmětech typu Projekt X není odevzdání této přílohy nutné.

Dále na datový nosič umístěte přílohy, které není možné pro jejich rozsah nebo charakter umístit do výtisku práce, ale které mohou být důležité pro posouzení úplnosti a kvality splnění zadání práce, jako jsou různé konstrukční výkresy, zdrojový kód programů pro zpracování naměřených dat apod.