**Vysoká škola ekonomická v Praze**
Fakulta managementu

# Pojmová matice 7. Z

semestrální práce z předmětu 6MMOD1

**Autor semestrální práce:** [redacted]
**Vyučující předmětu:** Ing. Adriana Krištůfková
doc. Dr. Ing. Jan Voráček, CSc.
**Rok:** LS 2020/2021

# Obsah

# Seznam obrázků

# Anotace a klíčová slova

V rámci závěrečné zprávy se zabývám tvorbou pojmové matice (nástroje terminologické unifikace). Na základě této metody vytvářím matici věnující se kybernetické bezpečnosti organizací. Díky těmto technikám dochází ke zjednodušení prvního modelu. V druhém jsou témata více kompaktní a výsledná matice přehlednější. Výhoda kombinace kvalitativního a kvantitativního modelování je zřejmá a značně usnadňuje práci s danou problematikou.

Klíčová slova: pojmová matice, kybernetická bezpečnost, Role Construct Repertory Grid

# Pojmová matice kybernetické bezpečnosti

## 1.1 Úvod

V rámci této závěrečné zprávy se zabývám tvorbou pojmové matice na téma kybernetická bezpečnost organizace. Touto zprávou navazuji na tu předchozí věnující se kybernetické bezpečnosti kritické infrastruktury, kde byla tato tématika podrobněji rozebrána: „Kybernetická bezpečnost je součástí výpočetní techniky. Jejím cílem je hlavně ochrana informací a dat a zabránění jejich zveřejnění, neoprávněného zacházení či jiného zneužití. Jedná se o mechanismy a kolektivní postupy, které tuto ochranu vykonávají. Obor je to ale poměrně nový. V posledních letech nabíral na závažnosti s rostoucím významem informačních a komunikačních technologií. Jde o ryze virtuální oblast, kde jsou data přenášena výhradně v elektronické podobě (Kybernetická bezpečnost a ochrana, 2017 & Hrůza, 2015)“.

Cílem tohoto úkolu je osvojení nástroje terminologické unifikace, kterým je právě pojmová matice a vytvoření takového modelu, který co nejlépe a nejkompaktněji popisuje danou oblast a její problematiku. Kybernetická bezpečnost patří v dnešní době zajisté k jednomu ze stěžejních témat každé společnosti. Ochrana firemních dat či dat svých klientů je klíčová a měl by být na ni kladen velký důraz. Obecně se tvrdí, že informace a data jsou v dnešní době jedno z nejdražších „zboží“ na světě. Zabezpečení kybernetické bezpečnosti, která je zasazena do firemní strategie, se stává neodmyslitelným krokem podnikání.

## 1.2 Metody

Výraz pojmová matice a způsob jejího tvoření pochází již z 40.–50. let 19. století. Jejím tvůrcem byl psycholog George Alexander Kelly (Pancratz, 2016). Jedná se o metodu diferenciální psychologické diagnostiky, která je založená na teorii osobních konstruktů. Výsledný model se skládá ze čtyř hlavních bodů:

- téma – kybernetická bezpečnost organizace;
- elementy – právní rámec, výpověď zaměstnance, únik informací a dat a další níže uvedené;
- konstrukty – jsou tvořeny dvěma póly, např. dlouhodobé vs. krátkodobé škody a další níže uvedené;
- hodnocení – klasifikace zvolených elementů na škále konstruktů, například na škále 1–5 a další níže uvedené (Ilea Institute, nedatováno).

Na základě tohoto kvantitativního rozdělení nabízí např. program WebGrid různé analytické nástroje, které umožňují identifikaci významově podobných pojmů a jejich sloučení. Hlavním cílem této metody je pohled a nalezení jeho řešení

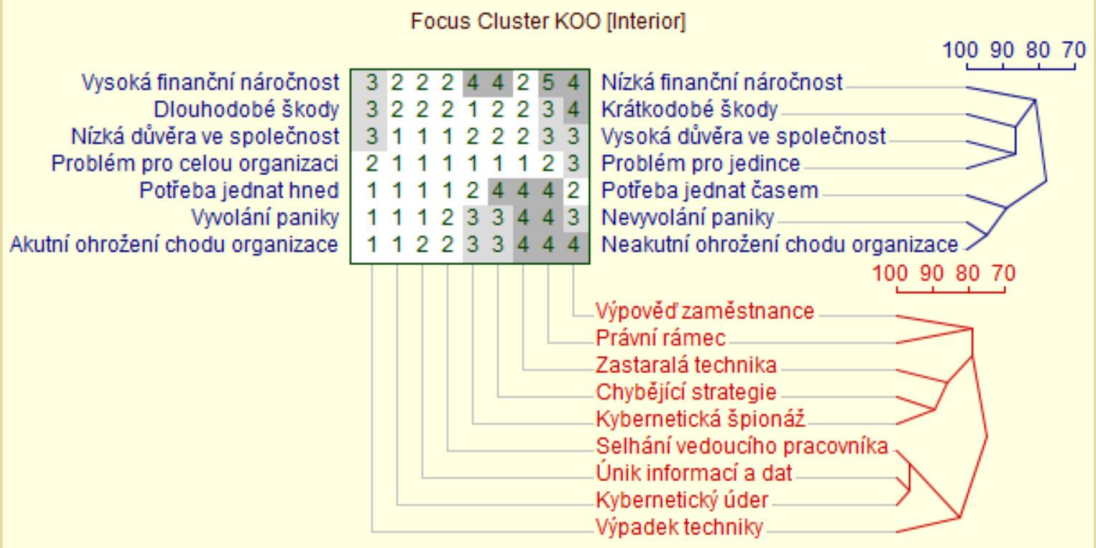
kompaktním, ale zároveň co nejpřehlednějším a nejjednodušším způsobem. Výsledná matice může obsahovat všechny původně zařazené pojmy, ale také poukazuje na možnost jejich sloučení a tím vést k vyšší přehlednosti.

## 1.3 Výsledky

Na obrázku číslo 1 je vyobrazena původní pojmová matice kybernetické bezpečnosti organizace. U první pojmové matice byly zahrnuty následující pojmy:

- výpověď zaměstnance; právní rámec; zastaralá technika; chybějící strategie; kybernetická špionáž; selhání vedoucího pracovníka; únik informací a dat; kybernetický úder; výpadek techniky.

**Obrázek 1 Kybernetická bezpečnost organizace – původní pojmová matice**

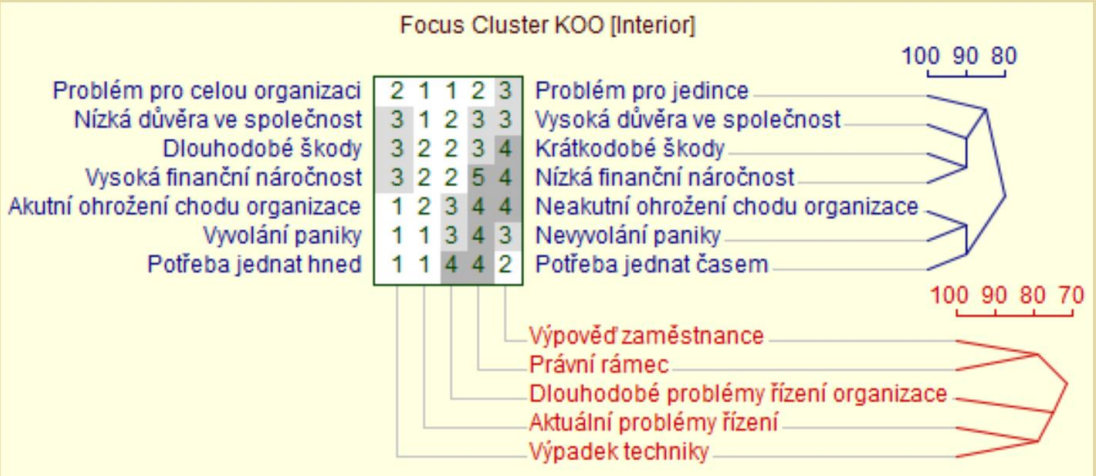



Zdroj: vlastní zpracování v programu WebGrid

Na obrázku číslo 2 je znázorněna upravená pojmová matice kybernetické bezpečnosti organizace. U druhé pojmové matice došlo na základě shlukové analýzy ke sloučení významově podobných pojmů:

- zastaralá technika + chybějící strategie + kybernetická špionáž = **dlouhodobé problémy řízení**;
- únik informací + kybernetický úder + selhání vedoucího = **aktuální problémy řízení**.

**Obrázek 2 Kybernetická bezpečnost organizace – původní pojmová matice**




Zdroj: vlastní zpracování v programu WebGrid

## 1.4 Diskuse

Metoda pojmové matice a její využití pro mě byla novinkou a příjemně mě překvapilo její poměrně jednoduché využití. I když se na první pohled zdá, že vybrané faktory nemají žádnou spojitost a každý z nich má v tabulce své oprávnění, je zajímavé pozorovat, jak se tento názor může rychle změnit. Detailnější pohled na faktory a jejich bodové ohodnocení poskytuje naprosto nový pohled na danou problematiku. Z prvotních devíti ukazatelů se povedlo vytvořit pouze pět, které lépe reprezentují větší uskupení, nikoliv jednotlivé „menší“ problémy.

První model pojmové matice vychází z poznatků myšlenkové mapy na téma kybernetická bezpečnost kritických infrastruktur. Z ní vychází několik základních faktorů, které mohou být problémem pro kybernetickou bezpečnost organizace. Plynou z ní též hrozby, které na bázi těchto faktorů mohou vzniknout. Jedná se jak o faktory lidské, tak i technologické či strukturální. Nejlepší ochranou je samozřejmě předcházení takovým událostem, ale to není vždy možné. Po vytvoření pojmové matice a zvolení „clusteru“ se díky zobrazení velmi přehledné tabulky a z ní plynoucí shlukové analýzy dají dobře odvodit podobná témata. I tam, kde by původně nebyl důvod hledat spojení, je možné při bližším pohledu a zamyšlení najít pojítko.

V mém případě se nabízelo spojení pojmů zastaralá technika, chybějící strategie a kybernetická špionáž. Na první pohled nulová souvislost, ale opak je pravdou. Jedná se totiž o dlouhodobé problémy řízení. Ať už chybějící strategie, zastaralá technika či kybernetická špionáž se projevují spíše v dlouhodobém horizontu a jsou následkem delšího zanedbávání a nepozornosti organizace. Podobně je tomu u druhého uskupení, kde došlo ke spojení pojmů únik informací, kybernetický úder a selhání vedoucího. Zde se ale jedná o problémy, která jsou velmi aktuální a vyžadují

rychlé a okamžité řešení. Jde o aktuální problém řízení. Jednoduchým způsobem zde došlo ke zjednodušení problémových faktorů, které jsou nyní sloučeny do reprezentativních skupin.

Přímo pro mou osobu se tato metoda jeví jako ideální. Často mám potíže s uskupováním témat do menších a kompaktních celků a zabývám se maličkostmi, což mě stojí mnoho času. Zde je možné poměrně snadno na základě kombinace kvalitativního a kvantitativního hodnocení rozpoznat vazby jednotlivých faktorů a díky tomu zjednodušit daný problém. To směřuje k uchopení problému jako celku, což spíše povede k úspěšnému řešení.

# Seznam literatury

Hrůza, Petr, 2015. Kritická informační infrastruktura a významné informační systémy. *Univerzita obrany.* [online]. [cit. 2021-04-12]. Dostupné z: https://moodle.unob.cz/pluginfile.php/72163/mod_resource/content/2/Kybernetick%C3%A1%20bezpe%C4%8Dnost%20T8.pdf

Ilea Institut, nedatováno. Repertory Grid-Verfahren. [online]. [cit. 2021-04-12]. Dostupné z: https://ilea-institut.de/leistungen/kultur-entwickeln/repertory-grid-verfahren/

Kybernetická bezpečnost a ochrana, 2017. *Kybernetická bezpečnost (Cyber Security). [*online]. [cit. 2021-04-12]. Dostupné z: https://www.cybersecurity.cz/basic.html

Pancratz, Nils, 2016. Repertory Grids als Methode zur Untersuchung von Schülervorstellungen im Bereich Computer und Internet. *Universität Oldenburg*. [online]. [cit. 2021-04-12]. Dostupné z: http://oops.uni-oldenburg.de/2854/1/RepertoryGridsSchu%CC%88lervorstellungenInternet.pdf