Možné důsledky teroristického ohrožení elektrizační soustavy ČR

Bc. Lenka Brehovská

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta technologická

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ

Fakulta technologická
Institut bezpečnostních technologií
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	Bc. Lenka BREHOVSKÁ
Studijní program:	N 2808 Chemie a technologie materiálů
Studijní obor:	Řízení technologických rizik
Téma práce:	Možné důsledky teroristického ohrožení na elektrizační soustavu České republiky

Zásady pro vypracování

1. Zpracujte teoretickou část diplomové práce - popis terorismu a kritické infrastruktury s ohledem na ochranu elektrizační soustavy.
2. Popište důsledky výpadku elektroenergetické soustavy pro ČR.
3. Analyzujte prvky elektrizační soustavy jako teroristicky zajímavé a důsledky zasazeni elektrizační soustavy z teroristického hlediska.
4. Identifikujte elektrizační prvky, které by mely podléhat zvýšené ochraně.
5. Analýzou zranitelnosti vyhledejte slabá místa v elektrizační soustavě, která mohou byt teroristy využita a mohou vest k nežádoucim následkům.
6. Vysvětlete předpokládané využití v praxi.
7. Zpracujte souhrn typických zranitelných míst elektrizační soustavy České republiky a návrh nejzranitelnějších prvků k ochraně celé soustavy.

Rozsah práce: 107 stran

Rozsah příloh: 9 stran

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

Seznam odborné literatury:

Dle doporučení vedoucího práce.

Vedoucí diplomové práce: **doc. Ing. Janošec Josef, CSc.**

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **18. května 2009**

Ve Zlíně dne 9. března 2009

doc. Ing. Petr Hlaváček, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta technologická

prof. PhDr. Vladimír Šefčík, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce pojednává o možných důsledcích teroristického ohrožení elektrizační soustavy ČR. Práce je rozdělena do dvou částí. Podrobněji se popisuje problematika spojená s terorismem a možnými ohroženími elektrizační soustavy. Zaobírá se důsledky, následky a ochranou kritické infrastruktury zaměřenou na elektrizační soustavu. Pro vyhodnocení výsledků je použita metoda AKIS. Ve výsledcích jsou ukázány nejcitlivější místa elektrizační soustavy a prvky s reálnou možností napadení teroristy.

Klíčová slova: Terorismus, Kritická infrastruktura, Energetika, Elektrizační soustava

ABSTRACT

The thesis discusses deals about the possible consequences of terrorist threat of the electricity systém of the Czech republic. It is dividend into two sections. It is described more detail issues related to terrorism and protectial threats to the elektricity system. It is dealed with the implications, consequences and porotections critical infrastructure amen at elektricity grid. For the evaluation it is used of the method AKIS. The results shown the most sensitive places of the elektricity systém and elementts with realistic posibility of attack by terrorists.

Keywords: Terrorism, Kritical infrastructure, Energetics, Power system

Motto*:*

„Účinek úderu nezávisí na tom, jak často a jakou silou udeříme, ale kam.“

Honoré de Balsac

Poděkování:

Za cenné rady a náměty děkuji Doc. Ing. Josefu Janoščovi CSc., řediteli z Institutu ochrany obyvatelstva, MV GŘ HZS Lázně Bohdaneč.

Prohlášení:

Prohlašuji, že jsem na diplomové práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků, je-li to uvedeno na základě licenční smlouvy, budu uvedena jako spoluautorka.

V Uherském Hradišti

.....

Podpis diplomanta

OBSAH

ÚVOD

Kritická infrastruktura je nejcitlivější oblastí státu. Poškození kritické infrastruktury má za následek ochromení části území, celého státu či několika států. Do roku 2004 se nepočítalo s radikálnějším ohrožením kritické infrastruktury. 11. března 2004 po útocích v Madridu se ukázalo více než pravděpodobné napadení jakékoliv části kritické infrastruktury teroristy. Rok po útocích v Madridu teroristé opět zaútočili. 7. července 2005 vybuchlo několik bomb v londýnském metru. Je známo mnoho útoků na kritickou infrastrukturu jak v Evropě, tak v USA. Útoky v Madridu a Londýně však ukázaly, jaké následky mohou být při napadení kritické infrastruktury. Začala se zdůrazňovat hrozba teroristických útoků na kritickou infrastrukturu. Evropská rada na svém zasedání v červnu 2004 požádala Komisi o přípravu celkové strategie na ochranu kritické infrastruktury. Komise přijala 20. října 2004 sdělení „Ochrana kritické infrastruktury v boji proti terorismu“ ve kterém předložila jasné návrhy, jak by se v rámci EU měla zlepšit prevence, připravenost a schopnost reakce na teroristické útoky zasahující kritickou infrastrukturu.

Nejcitlivější částí kritické infrastruktury je elektrizační soustava. Elektrická energie nemá možnost jakéhokoliv ukládání a hromadění energie pro případ výpadku. V rámci elektrizační soustavy je třeba dbát na vyváženou výrobu a spotřebu. Menší nevyvážení mezi výrobou a spotřebou má za následek výpadek elektrické energie.

V dnešní elektrizační době je nemožné fungovat delší dobu bez elektrické energie. Zkušenosti z velkých blackoutů během posledních jedenácti let ukázaly, že čím je výpadek elektroenergetické soustavy delší tím větší má následky a tím hůře se zasažené území vzpamatovává. Příkladem je výpadek elektrické energie na Novém Zélandě v roce 1998. Výpadek trval 5 týdnů a oblast kolem městečka Auckland se stále nevyrovnala s ekonomickými ztrátami.

Ukázalo se, že pravděpodobnost teroristického napadení na elektrizační soustavu stále stoupá. Již několik teroristických skupin v Evropě i v Americe se pokusilo elektrizační soustavu napadnout. Důsledky však nebyly velké. Jednalo se převážně o menší výpadky bez ztrát na životech či velkých ekonomických ztrát. Nyní je jen otázkou času kdy se uskuteční první velký teroristický útok na dodávky elektrické energie a jaké důsledky a následky vyvolá.

I. TEORETICKÁ ČÁST

1 TERORISMUS

V dnešní době se jen velice málo lidí na Západě setkalo s terorismem a přesto má každý díky médiím o terorismu určitou představu. Masmédia nás každý den bombardují zprávami o teroristických útocích, desítkách mrtvých a zraněných. Pohled na tuto hrozbu se v průběhu několika málo let radikálně změnil. Na počátku 90. let se na terorismus pohlíželo jako na bezpečnostní riziko. Později díky různým nárazovým akcím jak v Evropě tak ve Spojených státek se začal pohled měnit. Zlomovým okamžikem se staly útoky na World Trade Center z 11. září 2001. Terorismus již nebyl rizikem, ale celosvětovou hrozbou a lidé se začali terorismu obávat. Díky tomu se terorismus stal smutnou a nedílnou součástí každodenního života.

1.1 Charakteristika terorismu

1.1.1 Definice

Terorismus není výlučnou problematikou počátku 21. století. Různé projevy v Irsku, španělském Baskitsku, na Blízkém východě nebo v Turecku jsou zaznamenány ve všeobecné historické paměti soudobé populace. Přesto ucelená definice pojmu není dokončená. Největším problémem však není vytvoření samotné definice, ale její uplatnění v praxi[1].

O vytvoření ucelené definice se pokoušeli odborníci již od 30. let minulého století. První definice terorismu byla publikována až v roce 1980 v USA a stala se výchozím standardem pro posuzování a hodnocení teroristických činů. Zní: *„Terorismus je propočítané použití násilí nebo hrozby násilí, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen.“*(BRZYBOHATÝ [1], 1999).

1.1.2 Guerilla, terorismus a válka

V dnešní době nastává velký problém ve vymezení pojmu válka, guerilla a terorismus. Příčinou může být velké medializování tohoto problému či dnešní charakter válek. Zaměňují se pojmy jako terorismus a guerilla což je snahou i různých extrémistických proudů s cílem zakrýt skutečný charakter připravovaného násilí. Spojují se

[1] SCHEU, ŠULCOVÁ (op. cit.)[1], 2004. s 3.

pojmy terorismus a válka hlavně ve spojení s bezpečnostní politikou v Iráku či Afghánistánu. Proto je důležité řádné vymezení těchto pojmů v dalším pochopení terorismu.

Válka

Ve významovém slovníku je válka chápána jako konflikt mezi relativně velkými skupinami lidí, kteří v boji používají fyzické násilí a zbraně[2]. Ve slovníku spisovné češtiny je válka označena jako organizovaný ozbrojený boj mezi dvěmi stranami (státy aj.).

Jestliže vyjdeme z těchto dvou definic, lze říci, že válka je násilný masový konflikt, ve kterém se na bojích bezprostředně podílí dvě nebo více ozbrojených sil. Z toho alespoň jednu stranu tvoří regulérní ozbrojené síly. Na obou stranách existuje přinejmenším centrálně řízená organizace těch, co vedou válku a boje. Ozbrojené operace vykazují jistou kontinuitu, což znamená, že obě strany sledují určitou strategii.

Část expertů označuje válkou pouze ozbrojený konflikt určité intenzity. Měřítkem často bývá počet obětí. Samotné ozbrojené konflikty jsou rozděleny do tří kategorií (MAREŠ [2], 2006).

- Menší ozbrojený konflikt: počet mrtvých 25 až 1000 obětí.
- Střední ozbrojený konflikt: počet mrtvých nad 1000, ale bylo to méně jak 1000 v každém roce konfliktu.
- Válka, kde počet mrtvých přesahuje 1000 v každém roce konfliktu.

Guerilla

Guerilla a partyzánská válka je specifickou kategorií války. Někdy jsou tyto pojmy zaměňovány.

Pojem partyzánská válka byl poprvé použit v polovině 18. století ve francouzských instrukcích pro vedení války s malými částmi oddílů[3]. Podle významového slovníku je partyzánská válka formou vedení ozbrojeného konfliktu, která se vyhýbá velkým a rozhodujícím bitvám a soustředí se na drobné dílčí přepadové akce [3]. Partyzánská válka je systematická bojová a záškodnická činnost, vedená zpravidla malými skupinami (nestátními aktéry) domácího odboje, proti vojskům agresora, který území okupuje. Partyzánská činnost může být součástí různých válek.

---

[2] http://cs.wikipedia.org/wiki/V%C3%Allka, Prosinec 25, 2006.

[3] MAREŠ (opakovaná citace) [18], 2006.

Pojem guerilla byl používán k vyjádření odboje proti Napoleonovi. Guerilla je člověk, který bojuje v neoficiální armádě. Existují tři základní vysvětlení guerilly:

- *guerilla jako strategie boje za frontovou linií*. Ve válce činnost jednotlivců v neoficiální armádě oslabuje a vyčerpává jednu z bojujících stran a prospívá druhé.
- *guerilla jako hlavní strategie boje.* Je součástí strategie neoficiální armády, která velkým množstvím malých střetů chce vojensky porazit protivníka.
- *guerilla jako etapa války*. Nebyl-li neoficiální armádou poražen protivník, pak válka pokračuje a guerilloví bojovníci vytvářejí regulérní armádu.

Odlišení pojmů válka, guerilla a terorismus

I když jsou tyto pojmy podobné svým významem, existují v nich rozdíly. Následující tabulka pojmy porovnává podle charakteristik.

Tabulka 1: Charakteristiky války, guerilly a terorismu (zdroj [2])

Charakteristika	***Konvenční válka***	***Guerilla***	***Terorismus***
Jednotky nasazené do boje	Velké (armády, sbory, divize)	Střední (čety, roty, prapory)	Malé (obvykle méně než deset osob)
Zbraně	Plný rozsah vojenské bojové techniky (letecké síly, obrněná technika, dělostřelectvo)	Většinou pěchotní typy lehkých zbraní, někdy též část dělostřelectva	Ručí zbraně, ruční granáty, pušky a specializované zbraně, např. bomby odpalované na dálku, tlakové bomby
Taktika	Obvykle kombinované operace zahrnující několik druhů vojenských sil	Taktika komand	Speciální taktika: únosy, atentáty, výbuchy aut, braní rukojmí atd.
Terče	Většinou vojenské jednotky, průmyslová a dopravní infrastruktury	Většinou vojenský, policejní a administrativní personál jakož i političtí oponenti	Státní symboly, političtí oponenti a obecně veřejnost
Zamýšlený účinek	Fyzické zničení	Především vojenské oslabení nepřítele	Psychický nátlak
Kontrola teritoria	Ano	Ano	Ne
Uniforma	Nošení uniformy	Časté nošení uniformy	Nenošení uniformy
Rozeznatelnost válečných zón	Geograficky rozeznatelná válka	Vála omezena na zemi sporu	Nerozeznatelné válečné zóny
Mezinárodní legislativa	Ano, pokud je vedena podle pravidel	Ano, pokud je vedena podle pravidel	Ne
Domácí legalita	Ano	Ne	Ne

1.1.3 Druhy terorismu

Terorismus se dělí na jednotlivé druhy podle různých kritérií (cíl, rozsah, metody provedení, ideologie a jiné).

Státní terorismus

Rozlišovány jsou tři typy státního terorismu. První představuje použití násilí vládou proti svým občanům. Je používán k udržení moci vládou v daném státě. Druhý je státem podporovaný terorismus. Vláda kontroluje a podporuje teroristické skupiny doma i v zahraničí. Třetí typ představuje podporování nezávislé teroristické skupiny v zahraničí. Druhý a třetí typ státního terorismu jsou zaměřeny proti vládám cizích států [4]. Terorismus, který je prováděný vládou nebo představiteli vlády vede zpravidla k útlaku nebo zastrašování obyvatelstva. Je zaměřen buď na jednotlivé skupiny, nebo celé obyvatelstvo. Takové vlády ovlivňují vydávání zákonů a jiných právních předpisů, které legalizují mučení, bití a umožňují zabíjení občanů represivními složkami státu (policií, ale i armádou).

Státní terorismus většinou používají diktátoři. Příkladem můžou být plynové útoky Saddáma Husajna na kurdské obyvatele, Stalinovy čistky a mnoho jiných [4].

Mezinárodní terorismus

Definice, která by říkala co přesně mezinárodní terorismus je, neexistuje. Jedna definice, která se používá ve vládních kruzích USA, definuje mezinárodní terorismus jako terorismus zasahující občany nebo majetek více než jedné země.[4]

Některé teroristické skupiny se zaměřují pouze na činnost ve své zemi, některé na opak, pracují na mezinárodní úrovni. Nechávají se podporovat jinou zemí či na území jiné země pracují. Díky této činnosti se terorismus nedaří vymítit. Existují tři aspekty, které proměnily terorismus na mezinárodní. Prvním aspektem je rozpad kolonií. Mnoho států podporovalo teroristy za ukončení kolonialismu. Například Maroko podporovalo Alžírské teroristy. Druhým aspektem byla studená válka. Obě strany, jak demokratický západ, tak komunistický východ, podporovaly teroristickou činnost, aby ukázaly druhé straně svou sílu. Třetím aspektem se stala situace v Izraeli, který vznikl uprostřed arabského světa. Díky tomu arabský svět podporoval teroristy v boji proti Izraelitům [4].

---

[4] PERL [10], 2005, s. 7.

V dnešní době je mezinárodní terorismus považován za velkou hrozbu domácí i zahraniční bezpečnosti. Trendem terorismu je organizovaná, samostatně se financující mezinárodní síť. Terorismus se spojuje a různé skupiny spolu začínají spolupracovat. Spojují se výcviky, financování i technologie. Proto stojí nad celou otázkou mezinárodního terorismu šíření zbraní hromadného ničení. Některé státy podporující terorismus se zaměřují na obohacování uranu a tvrdí, že mají i jaderné zbraně. Objevily se již náznaky, že al-Kaida se pokusila získat chemické, biologické, radiologické a jaderné zbraně. Terorismus se díky internacionalitě stává nebezpečnější a proto je důležité proti němu účinně a přesně bojovat, s co nejmenšími chybami.[5]

Náboženský terorismus

Náboženský terorismus se v dnešní době dá považovat za hrozbu 21. století. Rozděluje se na dvě části. Fundamentalistický terorismus a eschatologický terorismus.

Fundamentalistický terorismus je násilná forma náboženského extremismu usilující o prosazení víry do státních struktur. V dnešní době je za nejnebezpečnější variantu považován islámský fundamentalismus. Prvkem islámského terorismu je motiv msty za příkoří, způsobené neislámským světem [5].

Eschatologický terorismus je specifickou částí náboženského terorismu. Jedná se o terorismus zahrnující sekty zastávající apokalyptický názor, že dnešní svět je špatný a musí být zničen. Nejznámější teroristickou sektou eschatologického terorismu je japonská sekta Óm Šinrikjó [5].

Kybernetický terorismus

Hrozba použití internetu jako prostředku teroristických aktivit je stále reálnější a možnější. Internet denně používají miliony lidí na celém světě. Díky této síti jsou propojeny počítače celého světa od domácností po firmy, banky a státní organizace. Je proto reálné napadení státních organizací pomocí internetu. Internet je jedno z nejsilnějších médií na světě a bohužel velice zranitelné. Kybernetický terorismus by se dal rozdělit na dva směry.

Propagandistický a informativní směr. Jedná se o propagaci terorismus, teroristických akcí, idejí skupin a cílů skupin.

---

[5] PERL (op. cit.) [10], 2005, s. 7.

Druhý směr již realizuje přímé napadení počítačových sítí. Likviduje služby a je podstatně nebezpečnější. Likvidací služby či celé jedné sítě dosáhl hacker sice zmenšení svého operačního prostředí, ale je to pro něj největší výhra.

1.2 Formy terorismu

Pro snadnější členění forem terorismu se požívají tři: konvenční, superterorismus a nekonvenční.

1.2.1 Konvenční terorismus

Konvenční terorismus je historickým typem, který přetrvává do současnosti. Tato forma terorismu používá klasické (konvenční) prostředky, jako např. výbušniny, střelné zbraně, hořlaviny, stejně jako násilné metody: atentáty, únosy, držení rukojmí. Teroristé používají střelbu, sečné a bodné zbraně, ubití [6], organizují bombové útoky, sabotáže, vraždy významných osob, zadržují rukojmí, zastrašují, vydírají, vyhrožují (BRZYBOHATÝ (op. cit.) [1], 1999).

V následujícím textu budou stručně charakterizovány jednotlivé prostředky konvenčního terorismu.

Střelba, sečné a bodné zbraně, ubití

Používá se při teroristických akcích namířeních proti nezúčastněným osobám v davu, nebo na konkrétní cílené osoby jako jsou politici, umělci, novináři a další. Užívá se rovněž jako postup proti konkrétním národům, nebo skupinám osob jako jsou například Američané, Izraelci atd.

Pumové atentáty

Bombové útoky jsou nejpoužívanější prostředky teroristických akcí. Teroristé je považují za účinný nástroj, který lze úspěšně využít pro malé i velké cíle s poměrně nízkou pravděpodobností včasného odhalení. Použití bombových útoků umožňuje i malým skupinám zabít mnoho lidí a vyvolat strach, paniku a nejistotu.

Cílem bombových útoků se stávají osoby, významné cíle nebo symbolické cíle. Bombové útoky proti osobám jsou mířeny na veřejné cíle (nahodilé skupiny) nebo prominentní osoby, státní činitele, vojenské představitele. Pumové atentáty státních představitelů vyžadují pečlivé plánování. Snad proto nejsou tak četné. Z prominentních osob jsou často terčem útoků lidé veřejnosti dobře známí (vědci, finančníci, lidé z průmyslu nebo státní správy). Vojenskými cíli teroristických útoků jsou vojáci ve službě

i mimo službu, vojenské kolony, stacionární i pohyblivé objekty. V neposlední řadě se stávají oběťmi i nahodilí občané na nádražích, v obchodních centrech, letadlech a jinde (mimo jiné: SHARPE [4], 2001).

Bombové útoky na významné a symbolické cíle mají vytvořit nejistotu a strach, jejich cílem není zabíjení osob. Takovými cíli jsou elektrárny, budovy, symboly konkrétního státu nebo skupiny obyvatel (BRZYBOHATÝ (op. cit.) [1], 1999).

Bomby jsou různých typů. Dopisové, balíčkové, v automobilech, specifické a bomby při sebevražedných atentátech. Nejmenší z nich jsou dopisové a balíčkové bomby. Tyto bomby jsou určeny pro významné osoby, ale obvykle jsou oběťmi další lidé. Proti takovým útokům se dá snadno a rychle vybudovat účinná opatření.

Specifické bomby jsou rozměrnější než dopisové či balíčkové. Lze je snadno přepravit a dají se použít téměř všude. Mohou se odložit na veřejných místech, jako jsou telefonní budky, odpadkové koše, nebo mohou být přeneseny do letadla v kufru.

Teroristé používají i bomby v osobních nebo nákladních automobilech. Tyto bomby mohou způsobit velké škody jak na životech tak majetku. Jsou velice mobilní a účinné.

Sebevražedné pumové atentáty

Sebevražedné atentáty jsou specifickým prostředkem terorismu, který má mnoho taktických výhod. Jde o sebeobětování a odpadá příprava únikových cest a možné ohrožení dopadením. Takové jednání snižuje náklady a zjednodušuje útok. Takové jednání zvyšuje bezpečnost skupiny. Zvyšuje se účinnost útoku, jeho přesnost a psychologický dopad na obou stranách. Sebevražedný atentátník je většinou člověk mladý, svobodný se solidním vzděláním a dobře společensky postavený. Nejedná se tedy o nevzdělance nebo jedince, který nemá co ztratit (MIKA [7], 2003).

První sebevražedné atentáty jsou zaznamenány za druhé světové války. Japonští „*kamikadze*“ používali letadla naplněného výbušninou proti americkým letadlovým lodím. Takové jednání mělo své výhody. Útoky mohli provádět i nezkušení piloti a obrana proti fanatickému nepříteli byla obtížná. Jediným možným řešením bylo celkové zničení letounu dříve, než dopadlo na letadlovou loď. Takové jednání vzbuzovalo strach a hrůzu z nepřítele [4].

Sebevražedné atentáty se znovu objevily až na Blízkém východě. Používají je především islámští teroristé. V 70. letech se objevují jen sporadicky, ale od roku 1982 se objevili jako odpověď na izraelskou invazi do Libanonu. Teroristická skupina Hizballáh začala používat sebevražedné atentáty proti Izraelcům. Ideologii Hizballáhu silně ovlivnil duchovní vůdce ajatolláh Chomejní, který přehodnotil kult mučednictví. Islám zakazuje sebevraždu, ale smrt ve válce zaručuje pravověrným místo v nebi. Muslimský duchovní Šejch Fadlalah prohlásil: „*Není rozdílu mezi smrtí se zbraní v ruce nebo s bombou na těle.*“ [4].

Sebevražedným atentátům se brzy na to začala věnovat další teroristická skupina Islámský džihád a v 90. letech začala i islámská fundamentalistická skupina Hamás. Sebevražední atentátníci jsou nejčastěji mladiství ve věku do 20 let. Tyto lidi společnost považuje za dost staré na to, aby nesli odpovědnost za své činny, ale ne dost staré na vlastní rodiny. Hamás prohlašuje, že se neustále hlásí další a další dobrovolníci. Tito dobrovolníci strávili roky na modlitbách v mešitách Hamánu, které vedly k přesvědčení, že jako mučedníci padlí za Palestinu půjdou rovnou do nebe [4].

Únosy lidí a letadel

Únos je překvapivé zajetí osoby nebo osob, většinou provedené s použitím zbraní, za účelem dosažení cílů organizace, skupiny nebo určité osoby [1]. Únosy lidí a letadel jsou nejdůležitější teroristické činnosti již od 60. let. Nejsou však novodobou činností. Objevovali se již od dob řecko římských. Únosy měli dopomoci teroristům k dosažení svých cílů. Byly to nátlaky na vlády za účelem propuštění vězňů, dosažení politických ústupků, ale také k dosažení finančních částek na další činnost [4].

Únosy jsou směřovány na významné i anonymní osoby. Teroristé požadují vyplnění svých požadavků.[6] Jedním ze společenských prvků únosů je prodlužování jejich zajetí, výhružky smrtí či zraněním. Je to jeden z možných donucovacích prostředků pro třetí stranu. Pokud by výhrůžka nesplnila svůj účel, přiklánějí se teroristé ke stupňování výhružek, dohodě či v neposlední řadě k postupnému zabíjení rukojmí. Zkušenosti ukázaly, že teroristé obvykle nechtějí zabít většinu rukojmí, protože jim dávají šanci k úniku z krizové situace.

Počátkem 70. let se začaly objevovat únosy letedel. Znamenaly velký počet ohrožených osob na palubě letedla. Od roku 1982 počet únosů letadel klesl na 20 za rok.

[6] http://www.mvcr.cz/rs_atlantic/project/article.php?id=4857, Leden 2, 2007

Byl to jednak důsledek změny v taktice teroristů, kteří se přeorientovali hlavně na pumové atentáty, střílení a únosy lidí [4], ale i rozvoj ochranných opatření ze strany leteckých společností, legislativy a zvýšené připravenosti specializovaných složek protiteroristických sil států.

Atentáty

Atentátem je označován útok na život významné osoby, obvykle z politických důvodů. Je to forma násilí a účinná zbraň teroristů. Atentáty jsou většinou pečlivě promyšlené a dlouhodobě plánované činy.

Atentátníci jsou obvykle součástí skupiny. Jedinci, kteří atentáty plánují ze soukromých důvodů, mohou být k takovému činu dovedeni díky pomatení mysli. Jsou přesvědčeni, že vraždou jediné osoby je možné změnit budoucnost. Předpokládají, že atentát obrátí pozornost na jejich přístupy a vládní autority se začnou jejich problematikou zabývat. Při jakémkoliv úspěšném atentátu platí, že čím vyšší je symbolická hodnota cíle, tím silnější je dopad na společnost. Dopady atentátů jsou různé. Z pohledů vládnutí nepřinesly nic. Zatím co z pohledu teroristů přinesly daleko větší úspěch, než tomu je ve skutečnosti. Pravdou je, že každý takový teroristický čin má hluboký vliv na celou organizaci, která atentát prováděla [4].

Zastrašování a vydírání

Výhružky použití násilí mohou být stejně účinné jako samotná akce. Existuje mnoho možností, jak zastrašování použít. Jednou z nich je odlákání pozornosti na falešnou bombu. To je taktický tah, který může přinést fatální následky. Pro bezpečnostní složky je důležité si vždy uvědomovat možnost existence reálného zařízení [1].

Vydírání je jednou z možných metod kdy teroristické skupiny získávají finanční prostředky. Může jít o bankovní loupeže či vydírání významných podnikatelů. Problémem je fakt, že hranice mezi terorismem a kriminálním činem je velice nezřetelná [1].

1.2.2 Superterorismus

Tento typ terorismu využívá zbraní netradičních. Jedná se o zbraně způsobující hromadné ztráty čili zbraně hromadného ničení. Mezi zbraně hromadného ničení patří chemické, biologické, radiologické a jaderné zbraně. Do roku 1995 se pouze uvažovalo o možném zneužití zbraní hromadného ničení v rámci teroristických útoků. Roku 1995 sekta Óm Šinrikjó provedla historicky první útok v Tokijském metru. Od roku 1995 se považuje konvenční terorismus za reálný [5].

Chemické zbraně

Chemické zbraně jsou zbraně, které na objekt útoku působí anorganickými a organickými sloučeninami, jejich účelem je působit buď dráždivě nebo toxicky na různé organismy. Chemické zbraně jsou velice účinné a efektivní při použité proti civilnímu obyvatelstvu.[7]

Chemické zbraně se člení podle povahy působení na nervově paralytické látky (tabun, sarin, soman, VX) ovlivňující cholinergní přenos nervového vzruchu cestou ireverzibilní inhibice acetylcholinesterázy. Zpuchýřující látky (yperit, lewisit) charakteristické devastujícím a špatně se hojícím efektem na tkáních, založený na jejich cytotoxicitě. Psychicky a fyzicky zneschopňující látky (BZ látka, kyselina d-lysergová) vyvolávající již v malých koncentracích psychické nebo fyzické zneschopnění. Dráždivé otravné látky (Adamsit, Clark, CS látka) mají charakter oslabujících látek používající se za účelem snížení bojeschopnosti. Všeobecně jedovaté (oxid uhelnatý, nitráty, nitrity) jsou látky účinkující na úrovni jako inhibitory dýchacího řetězce. Dusivé otravné látky (fosgen, difosgen, chlorpikrin) vyvolávají změny v dýchacích orgánech[8].

Biologické zbraně

Biologické zbraně jsou živé organismy nebo z nich odvozený infekční materiál, který je určen pro vyvolání nemoci nebo usmrcení osob, zvířat nebo rostlin. Podle infekčního onemocnění rozdělujeme biologické zbraně do šesti základních skupin: bakterie (antrax, mor, cholera), rickettsie (tyfus, Q-horečka), viry (Ebola, neštovice, hemoragické horečky), plísně (mykózy), toxiny (botulotoxin, ricin, saxitocin), geneticky modifikované organismy [9].

Radiologické zbraně

Radiologické zbraně jsou isotopické zbraně způsobující kontaminaci prostředí radioaktivními látkami bez jaderné detonace. Nejvýznamnějším zástupcem této skupiny je špinavá bomba. Jedná se o zařízení obsahující jakoukoliv radioaktivní látku a konvenční výbušninu. Při výbuchu dojde k rozptylu radioaktivní látky[10].

Nukleární zbraně

Nukleární zbraně obsahují nadkritické množství materiálu. Mezi zbraně nukleární řadíme zbraně štěpné (obsahují ^{235}U, ^{239}Pu) projevující se charakteristickým hřibovitým

[7] http://cs.wikipedia.org/wiki/Chemick%C3%A9_zbran%C4%9B

mrakem. Termonukleární zbraň (vodíková puma) a Neutronové zbraně (jedná se o kombinaci štěpné a fúzní zbraně) [10].

1.2.3 Nekonvenční terorismus

Pro nekonvenční terorismus je typické použití netypických prostředků. Takové zbraně nevyvolávají primárně ničivé účinky, ale sekundární jev má katastrofální následky. Mezi nekonvenční terorismus se řadí informační terorismus a psychologický terorismus.

Informační terorismus

Informační technologie nabízejí možnost rychle a efektivně před zrakem mnoha lidí zasáhnout. S rozvojem informačních technologií stále stoupá riziko informačního terorismu. Prostředky informačního terorismu jsou snadno dostupné. Jedná se převážně o sdělovací prostředky, digitální informační systémy a jiné. Útok na informační prostředky je relativně méně nákladné. S vybavením za několik tisíc se dají způsobit obrovské miliónové až miliardové ztráty, jak ve finančním sektoru tak dopravě, bankovnictví a mnoha jiných.

Psychologický terorismus

Psychologický terorismus je plánované použití propagandy v mírovém období, za účelem šíření strachu. Je zaměřen a ovlivnění lidského myšlení. Základním nástrojem psychologické války je propaganda. Terorismus propagandu využívá a je na ní existenčně závislí.

1.3 Teroristické ohrožení

V dnešní době je terorismus považován za jednu z nejvýznamnějších hrozeb dnešního světa. Jedná se o hrozbu globální, nezaměřující se pouze na určitě oblasti jako tomu bylo do ruku 2001. Po útocích na Spojené státy 11. září 2001 se radikálně zhoršila mezinárodně-bezpečnostní situace. O několik let později se však tato situace nezlepšila. Možnosti teroristických aktivit narůstají a státy se musejí s touto hrozbou vypořádat.

V souvislosti s teroristickým ohrožením je nutno nadefinovat pojmy hrozba a riziko.

Hrozba *je objektivní skutečnost, která může znamenat negativní dopad*[8]. Hrozbě lze čelit protiopatřeními. S ohledem na konkrétní cíl je odstupňována intenzita opatření.

Riziko *je to co stát podstupuje, aby jeho snaha redukovat hrozby nepřekročila únosnou míru*[8].

[8] http://aplikace.mvcr.cz/archiv2008/rs_atlantic/data/files/aon.pdf

V této souvislostí platí, že čím je chráněný zájem střelenější, tím je úspěch útoku méně pravděpodobný. Pokud se ale vysoce střežený zájem povede napadnout, znamená to pro teroristy vyšší efekt. V úvahu přicházejí ztráty na životech, hmotné škody, snížení důvěryhodnost republiky, škody v ekonomickém sektoru státu i přidružených ekonomik států.

1.3.1 Teroristické ohrožení ve světě

Prezident USA Georgie Bush podepsal v listopadu 2002 zákon o protiteroristickém ohrožení (Terrorism Risk Insurance Act, TRIA). Cílem tohoto zákona bylo znovu nastartovat ekonomiku USA. V rámci tohoto zákona je zvažování možných rizik a to s ohledem na to jaké riziko teroristického útoku v které zemi je. Jedna z předních pojišťovacích společností firma AON začala vydávat materiál *TerrorismRisk Insurance Expertise*[9]. Základem této analýzy je známkování jednotlivých zemí. Země jsou firmou AON známkovány podle škály barevných stupňů Homeland Adisory Systém Ministerstva vnitřní bezpečnosti USA. Rozlišuje 5 stupňů.

Tabulka 2: Homeland Security Advisory Systém (zdroj [11])

Severe risk of terrorist attacks	Naprosté riziko	Irák, Indie, Pákistán, Izrael/Palestina, Saudská Arábie, Kolumbie, Nepál, Somálsko
High risk of terrorist attacks	Vysoké riziko	Ruská federace, Alžírsko, Turecko, Kypr apod.
Elevated risk of terrorist attacks	Zvýšené riziko	Egypt, USA, Německo, Francie, Súdán, Austrálie, Velká Británie aj.
Guarded risk of terrorist attacks	Riziko vyžadující ostražitost	Kanada, Mexiko, Kazachstán, Írán apod.
Low risk of terrorist attacks	Nízké riziko	ČR, Dánsko, Grónsko, Norsko Finsko, Libye apod.

Podobným problematikám se věnují i jiné ústavy (World Market Analysis; WMRC Global Terrorism index). Obě tyto studie zahrnují údaje o povaze potenciálních útočníků, jejich ideologickému profilu apod. Dochází ke známkování jak zemí, tak měst[11].

[9] http://www.aon.com

Tabulka 3: Hodnocení nebezpečnosti (zdroj [11])

5	Velmi nebezpečná místa, často zmítaná válkou. Velké nebezpečí úmrtí
4	Nebezpečná místa, konflikty převážně regionální. Možnost úmrtí
3	Nebezpečí převážně lokálního charakteru. Možnost ohrožení
2	Méně nebezpečná místa, možnost ohrožení pouze lokálně
1	Incidenty pouze izolovaně, nízká možnost ohrožení

1.3.2 Teroristické ohrožení v ČR

I když česká republika zatím nebyla dějiště žádné teroristické akce, riziko uskutečnění útoku stále roste.

Česká republika je v rámci mezinárodního terorismu považována za zem aktivně se účastnící protiteroristického snažení. Je tudíž považována za potenciální terč teroristů. Na přelomu září a října roku 2006 obdrželi bezpečnostní složky České republiky informaci o možném teroristickém činu na území státu. Přijatá informace byla vyhodnocena jako mimořádně závažná a proto byla podniknuta nezbytná opatření k eliminaci rizik vyplývající z této hrozby, včetně přijetí mimořádných bezpečnostních opatření. Z pohledu terorismu je největším rizikem fakt, že Česká republika je tranzitním místem pro pobyt osob podezřelých z napojení na teroristické skupiny. Od roku 2001 byly zadrženy desítky osob podezřelých z terorismu, které získaly víza České republiky. V rámci teroristického ohrožení se zájem musí ohlížet i na zájmy České republiky v zahraničí, kde došlo již k několika útokům na cíle spojené s Českou republikou. Jedná se převážně o území Iráku a Afghánistánu. V červenci 2005 zemřel jeden občan České republiky při útocích v egyptském Šarm al-Šejku. V České republice se již vyskytly i některé incidenty spojené se zneužitím internetového bankovnictví. Proto by se Česká republika měla postarat o snížení pravděpodobnosti vzniku takovýchto událostí.[12]

Místa ohrožena teroristickými útoky:

- Místa s vlekou koncentrací lidí (metro, stadiony, nádraží, letiště)
- Strategické objekty (mosty, tunely, elektrárny, zásobárny pitné vody)
- Vládní objekty a osoby (Prezident, sídlo vlády, ministerstva)

1.4 Dopady terorismu

Každý teroristický čin sebou přináší určité dopady. Jedná se zejména o psychologické důsledky významné politické, ekonomické a sociální následky. Podružné jsou již důsledky na infrastrukturu a medializaci teroristů. Dopady terorismu se dají rozlišovat do čtyř oblastí lidské činnosti:

- oblast ekonomiky
- oblast psychologická
- oblast bezpečnosti
- oblast infrastruktury

1.4.1 Oblast ekonomiky

Terorismus ekonomiku Západní Evropy zatím výrazně nepoškodil. Evropské finanční trhy a burzy reagovaly na zprávy o atentátech pouze drobným zakolísáním v trvání několika minut. Teroristé vědí, že růst ekonomiky je dán i očekáváním veřejnosti ohledně budoucnosti. Pokud se teroristům podaří veřejnosti vštípit očekávání strachu a nejistoty, dosáhne se tím k oslabení spotřebitelské poptávky a investic. Z toho vyplývá, že strach z terorismu může mít ničivější následky než válka. Ekonomové Zvi Eckstein a Daniel Tsidonn ukazují ve svém výzkumu Makroekonomické důsledky teroru. Ukazují, že teror má velký dopad na ekonomiku a pokud teror přetrvává vyžádá si větší počet obětí a může snížit úroveň spotřeby zhruba o pět procent. Kdyby Evropa byla vystavena vlně terorismu s větší délkou a intenzitou, mohly by škody dosahovat až stovek miliard euro ročně [13].

1.4.2 Oblast psychiky

Teroristé uplatňují násilí formou úderů bez vyhlášení války a tím dosahují obrovských psychologických dopadů. Šíření strachu patří mezi jedu z teroristických cílů. V atmosféře strachu lze snadněji vynutit splnění požadavků. Terorismus je tudíž považován za psychologický boj[14].

1.4.3 Oblast bezpečnosti

Největší obrat v oblasti bezpečnosti nastal po útocích 11. září 2001. Státy začaly přijímat opatření pro minimalizaci následků teroristických akcí a vlády schvalovaly zákony týkající se bezpečnostního prostředí. Přijímají se protiteroristická opatření a vyprofilovaly se dva přístupy v boji proti terorismu.

Válka proti terorismu

Válku proti terorismu prosazuje hlavně Bushova administrativa. Spočívá v použití vojenských sil. Tak je možné poměrně rychle zničit armády diktátorských států a svrhnou režim.

Takový přístup má několik silných stránek. Jsou to vojenské schopnosti USA. Spojené státy mají nejmodernější armádu světa. Jsou schopny zasahovat i na velké vzdálenosti. Platformou války proti terorismu je „***Národní bezpečnostní strategie*“**, která vymezuje základní strategické zájmy USA. Klade důraz na *preempci*, přisuzuje menší význam multilaterálním přístupům v oblasti bezpečnosti a udržuje stávající vojenskou převahu. Významným pilířem války proti terorismu je rekonfigurace sítě vojenské přístupnosti ve světě nazvané „*Global Posture Review“*. Týká se to převážně snižování základen ve světě a zvýšení schopnosti rychlého nasazení armády kdekoliv ve světě do 4 dnů [15].

Slabými stránkami je hlavně přímá odpověď na nepřímou strategii. Tato válka se nevede na konkrétní stát či koalici. Terorismus nerespektuje hranice. A to vyvolává řadu negativních odpovědí. Příkladem byl 11. březen 2003, teroristický útok v Madridu jako reakce na invazi do Iráku (20. března 2003).

Boj proti terorismu

Boj proti terorismu, tedy ne válku, hájí zejména státy Evropské unie. Tato metoda se zaměřuje na postižení základních kořenů terorismu a na preemptivní strategii. Vojenské zásahy proti terorismu jsou předpokládány až jako krajní řešení.

Tato metoda má své silné stránky. Neomezuje se na následky a vnější projevy terorismu, ale na jeho kořeny a příčiny. Zaměřuje se na hledání dlouhodobých východisek a jejich řešení. Důležitým kladem je, že se nezaměřuje na vrchol pomyslné pyramidy terorismu, ale na její základnu. Zastává názor, že vrchol pyramidy je snadno doplnitelný, ale základna pyramidy nikoliv a její doplnění trvá roky [15].

Slabou stránkou je pomalé řešení problému. Boj proti terorismu není otázkou okamžiku, ale problémem mnoha let. Vyžaduje značné investice a mnoho času.

1.4.4 Oblast Infrastruktury

Mezi nejvýznamnější dopady v oblasti infrastruktury patří bezpečnostní opatření, která jsou přijímána. Primárně se zájem zaměřuje na místa s velkou koncentrací lidí.

V dopravě nelze přijmout stejná opatření. Jiná opatření jsou v automobilové a železniční dopravě, jiná v dopravě letecké. Potenciálním cílem jsou supermarkety. Potenciální ohrožení se nachází i v napadení rozvodů či plynovodů. Elektrizační sítě, pitné vody atd.[5]

2 KRITICKÁ INFRASTRUKTURA

2.1 Infrastruktura

S termínem infrastruktura se poprvé setkáváme v 19. století, kdy termín označoval vojenská zařízení. Poté se pojem znovu objevil v 80. letech 20. století v knize America in Ruins, kde se začalo jednat o infrastrukturální krizi zapříčiněnou desetiletími nedostatečných investic do veřejných komunikací a staveb ve Spojených státech. Pojem infrastruktura byl ale nedostatečně chápán a proto Národní výzkumná rada U.S. (National research council) zavedla definici: Veřejná infrastruktura se vztahuje jak ke specifickým funkcím - dálnice, ulice, silnice a mosty; hromadná doprava, letiště a letecká síť; vodárny a vodní zdroje; čistírny odpadních vod; zpracování komunálního odpadu; výroba a přenos elektrické energie; telekomunikace a zpracování nebezpečného odpadu – tak i ke složeným polyfunkčním systémům [16].

V nezákladnějším smyslu slova lze infrastrukturu pojmenovat jako množinu propojených strukturálních prvků, které udržují celou strukturu pohromadě. Z pravidla se jedná o prvky, které jsou uměle vytvořené. S termínem infrastruktura se seznámíme v řadě různých odvětví. Nejvíce se používá v ekonomii, kdy infrastrukturu popisuje třeba budovy nebo silnice[16].

Pojem „infrastruktura“ je odvozen od latinského výrazu *infra* znamenající vespod něčeho. Často se ve spojení s infrastrukturou užívá označení veřejná infrastruktura. V České republice se veřejnou infrastrukturou rozumí pozemky, stavby a zařízení.

2.2 Kritická infrastruktura

Kritická infrastruktura by se dala označit za část infrastruktury, která je životně důležitá pro chod a bezpečnost státu a obyvatelstva. Její napadení by mělo katastrofální následky na chod státu a života v něm.

Pojem kritická infrastruktura se objevil poprvé v roce 1997 v amerických článcích zaměřující se na tuto problematiku. Za základ ochrany kritické infrastruktury se však považuje rok 1962, kdy se datuje tzv. Kubánská krize. Po této krizi se začal řešit problém

bezpečnosti telekomunikační sítě a poprvé se vzala v úvahu zranitelnost tohoto systému [17].

„Kritická infrastruktura jsou fyzické, kybernetické a organizační systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimálního chodu ekonomiky a správy státu“[18]

Tabulka 4: Oblasti kritické infrastruktury (zdroj [19])

	Oblast KI	Produkt nebo služba	Gestor
1	Energetika	1.1. Elektřina	MPO/ ERÚ
		1.2. Plyn	MPO/ ERÚ
		1.3. Tepelná energie	MPO/ ERÚ
		1.4. Ropa a ropné produkty	SSHR/MPO
2	Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou	MZe
		2.2. Zabezpečení a správa povrchových vod a podzemních zdrojů vody	MZe/MŽP
		2.3. Systém odpadních vod	MZe
3	Potravinářství a zemědělství	3.1. Produkce potravin	MZe
		3.2. Péče o potraviny	
		3.3. Zemědělské výroba	
4	Zdravotní péče	4.1. Přednemocniční a neodkladná péče	MZ
		4.2. Nemocniční péče	
		4.3. Ochrana veřejného zdraví	
		4.4. Výroba, skladování a distribuce léčiv a zdravotních prostředků	
5	Doprava	5.1. Silniční	MD
		5.2. Železniční	
		5.3. Letecká	
		5.4.Vnitrozemská	
6	Komunikační a informační systémy	6.1. Služby pevných telekomunikačních sítí	MI/ČTU
		6.2 Služby mobilních komunikačních sítí	
		6.3 Rádiová komunikace a navigace	
		6.4 Satelitní komunikace	
		6.5 Televizní a rádiové vysílání	
		6.6 Přístup k internetu a datovým službám	
		6.7 Poštovní a kurýrní služby	MI
7	Bankovní a finanční sektor	7.1 Správa veřejných financí	MI
		7.2 Bankovnictví	ČNB
		7.3 Pojišťovnictví	MF
		7.4 Kapitálový trh	MF/KCP
8	Nouzové služby	8.1 Policie ČR	MV
		8.2 Hasičský záchranný sbor ČR	MV
		8.3 Zdravotnické záchranné služby	MZ
		8.4 Letecká zdravotnická záchranná služba	MZ
		8.5 Armáda ČR	MO
		8.6 Radiační monitorování	SÚJB
		8.7 Předpovědní, varovná a hlásná služba	MŽP
9	Veřejná správa	9.1 Sociální ochrana a zaměstnanost	MPaSV
		9.2 Diplomacie	MZ

		9.3 Výkon justice a vězeňství	MS
		9.4 Státní správa a samospráva	MV
10	Odpadové hospodářství	10.1 Nakládání s odpady	MŽP
		10.2 Radioaktivní odpady	MPO/SÚRAO

Vysvětlivky:
KCP – Komise pro cenné papíry SSHR – Správa státních hmotných rezerv
ERÚ – Energetický regulační úřad SÚRAO - Správa úložišť radioaktivních odpadů

Na kritickou infrastrukturu nahlížíme jako na komplexní systém. Má síťové uspořádání, které se skládá z jednotlivých prvků sítě a spojnic. Jako v každé síti se i zde nacházejí místa, kde se schází více prvků spojnic – „*uzel*“. Některé z těchto uzlů jsou málo významné a jiné více. Poškození, či narušení strategicky významného uzlu by vedlo ke zhroucení celé kritické infrastruktury. Zájmem ochrany kritické infrastruktury by mělo být tyto strategicky významné uzly chránit.

Ochrana kritické infrastruktury by se měla zaměřit na prevenci. Úroveň ochrany je závislá na množství financí, které jsem ochotni investovat. Je nutné říci, že žádný stát nemá dostatek financí, aby mohl stoprocentně zabezpečit ochranu celé infrastruktury. Proto je nutné stanovit si míru rizika, kterou jsme ochotni, či nuceni respektovat. Ekonomika tedy hraje v této problematice klíčovou roli.

Kritická infrastruktura je velice rozsáhlá a očekává se, že stát ji bude kontinuálně chránit. Prvky kritické infrastruktury však nepatří všechny do majetku státu. Některé patří soukromím subjektům, které mají na paměti prvotně zisk, před bezpečností obyvatel. Což je opak státu. Jedná se například o energetiku, telekomunikace, zásobovaní vodou apod. Díky tomu se bezpečnost kritické infrastruktury stává složitějším procesem. V dnešní době neexistuje žádný legální způsob jak vkládat peníze státu do ochrany kritické infrastruktury, která se nachází v soukromých rukou. A naopak stát nemůže přinutit soukromý subjekt, aby vkládal peníze do preventivních opatření. Je proto nutné najít způsob, jak sdílet informace vedoucí k ochraně kritické infrastruktury, což by vedlo k posílení bezpečnosti.

V dnešní době již máme zkušenosti s útoky na kritickou infrastrukturu. Jedná se o napadení náhodná (mimořádné události) či úmyslná (teroristické útoky).

2.2.1 Ochrana kritické infrastruktury

Ochrana kritické infrastruktury zaznamenala v posledních několika desítek let pár změn v prioritách její ochrany. Nejdříve byla ochrana infrastruktury zaměřena na možné

ohrožení jaderným napadením, po té se změnilo na ohrožení živelnými pohromami. Zásadní zlom nastal po teroristickém útoku 11. září 2001. Ochrana se začala radikálně zaměřovat na teroristické napadení. Příkladem můžou být i teroristické útoky v Madridu či Londýně, kde došlo k napadení dopravní sítě jako jedné ze součástí kritické infrastruktury.

Otázky ochrany kritické infrastruktury se poprvé začaly řešit ve Spojených státech kde byla vydaná tzv. Bílá kniha. Jednalo se o směrnici 63, kterou vydal president Bill Clinton jako presidentské rozhodnutí. Bílá kniha pojímá kritickou infrastrukturu jako základní systém, který má vliv na funkce ekonomiky státu. O několik let později vydala Evropská unie tzv. Zelenou knihu jako obdobu Bílé knihy. Ta pojednává o evropském programu na ochranu kritické infrastruktury. Byla vydaná v Bruselu 17. listopadu 2005. Zelená kniha uvádí, že: „Účinná ochrana kritické infrastruktury vyžaduje komunikaci, koordinaci a spolupráci, jak na národní tak na evropské úrovni, a to mezi všemi zainteresovanými subjekty – vlastníky a provozovateli infrastruktur, regulačními orgány, profesními organizacemi a odvětvovými sdruženími, stejně jako všech úrovní státní a veřejné správy a také veřejnosti.“[19]

Ochrana kritické infrastruktury je proces zaměřený na ochranu subjektů i objektů kritické infrastruktury aby nedošlo k jejich selhání. Smyslem ochrany kritické infrastruktury je minimalizace dopadů výpadků činností těchto struktur, s co nejmenším zasažením obyvatelstva[20].

Subjektem kritické infrastruktury jsou vybrané subjekty výrobní i nevýrobní sféry provozující zařízení a objekty nebo poskytující služby popř. vytvářející produkty ve stanovených oblastech kritické infrastruktury[10].

Objekty kritické infrastruktury jsou stavby zařízení a prvky, které vlastní nebo provozují subjekty kritické infrastruktury.Uznávají se tři základní skupiny objektů[18]:

- veřejné, soukromé a vládní objekty infrastruktury a vzájemně propojené kybernetické a fyzikální sítě
- procedury a relevantní jednotlivost mající kontrolu nad funkcemi kritické infrastruktury
- objekty s kulturním nebo tzv. „měkké cíle“ v podobě masových akcí (sportovních, kulturních apod.)

[10] 21. schůze VCNP ze dne 23.9.2003, usnesení č. 179 – materiál „Aktuální seznam subjektů kritické infrastruktury“

Cílem ochrany kritické infrastruktury je zabezpečit strategické a životní zájmy dotýkající se obyvatelstva. Stát musí za všech okolností zabezpečit provozuschopnost základních prvků, vazeb a toků zabezpečující chod státu a udržet za každé situace jeho stabilitu a zabezpečit další rozvoj [20].

Na ochraně kritické infrastruktury se podílí několik aktérů. Prvořadně se jedná o stát, který představuje vůli lidu. O stát a soukromé subjekty, které jsou vlastníky jednotlivých objektů a dále o stát a obyvatelstvo, kde stát garantuje přežití a stabilitu.

V České republice má problematiku ochrany kritické infrastruktury nestarosti Výbor pro civilní nouzové plánování Bezpečnostní rady státu. Jeho řízení patří do gesce MV GŘ HZS.

Problematika řešení kritické infrastruktury a její ochrana lze rozdělit na tři části [19]:

- mapování kritické infrastruktury v ČR
- inventura přístupu subjektů řešící problematiku kritické infrastruktury jejich jednotlivých oblastech
- rozbor situace v jednotlivých odvětvích ČR s vazbou na postupy mezinárodních organizací a institucí (NATO, EU, …)

Ochrana Kritické infrastruktury musí být zajištěna pomocí preventivních opatření. Vzhledem k tomu že význam kritické infrastruktury je definovaný v mezinárodním měřítku dá se předpokládat, že zasažení části kritické infrastruktury v jednom regionu bude mít dopad i na sousední regiony. Proto by se měla ochrana řešit jak v problematice národní tak nadnárodním.

2.2.2 Ochrana kritické infrastruktury v ČR

Základním cílem ochrany kritické infrastruktury je snížení zranitelnosti systému před možnými ohroženími, jako jsou živelné pohromy, nehody, teroristické útoky a jiná nebezpečná jednání. Lidské sídla se stávají čím dál více zranitelnějšími a každý stát by se měl

Jestliže v dnešní době dojde k ohrožení jednoho z prvků kritické infrastruktury, začne se problematikou zaobírat Policie ČR, která v případě potřeb bude posilována Armádou ČR. Díky provedené profesionalizaci Armády ČR již není v silách Armády vyhovět všem požadavkům Policie na posílení. Proto se začalo jednat o vzniklém

problému a jak ho vyřešit. Jednou z variant je přenechat střežení v případě potřeb „Dobrovolným aktivním zálohám“. Další možnou variantou je vznik „Národních brigád“ podle vzoru národních brigád ve Spojených státech. Otázkou je však, zda se tyto možnosti legislativně přijmou. Jinou variantou by bylo vznik nových vojensky specializovaných policejních jednotek. Takovou to zkušenost mají jiné státy EU jako je Francie a „žandarmerie“, Itálie a „karabiniéři“ či Rakouské četnictvo a jiné [21].

V rámci ochrany kritické infrastruktury by mělo být provedeno několik kroků [17]:

a) Hlavní úkoly ochrany kritické infrastruktury pracovníka na úrovni státu jsou:
    i. Provedení analýzy zranitelnosti kritické infrastruktury vůči mimořádným událostem.
    ii. Do systému ochrany kritické infrastruktury zapojit právnické i fyzické osoby.
    iii. Zpracovat plán na odstranění primárních rizik.
    iv. Zpracovat plán kontinuity.
    v. Zajistit systém detekce živelných pohrom a možných útoků.
    vi. Zajisti plán odezvy na ztrátu funkčnosti kritické infrastruktury.
    vii. Připravit plán obnovy kritické infrastruktury.
    viii. Zajistit spolupráci mezi veřejnou správou, právnickými a fyzickými osobami.
    ix. Zajistit výzkum ochrany kritické infrastruktury.
    x. Zajistit zpravodajské analýzy.
    xi. Zajistit mezinárodní spolupráci.
    xii. Zajistit legislativní a finanční požadavky.
b) Je důležité propojení ochrany kritické infrastruktury mezi státem a soukromími subjekty. Některé prvky kritické infrastruktury spadají do soukromého vlastnictví, a proto je důležité najít účinný nástroj spolupráce.
c) Je třeba respektovat zásady:
    i. Zaměřovat činnost na důležité aspekty.

ii. Včasně varování před živelnou pohromu sníží ztráty na životech.

iii. Řízení ochrany kritické infrastruktury postavit tak aby byl zajištěn udržitelný rozvoj.

iv. Věnovat pozornost nejzranitelnějšímu systému.

v. Zvládání nouzových situací zaměřit na ochranu lidí a kritických prvků.

vi. Věnovat velkou pozornost prevenci.

vii. Občané mají právo na pomoc.

viii. Občané do systému odezvy patří jako potenciální oběti, ale i jako aktivní prvky odezvy.

ix. Zajistit informovanost občanů o krizových plánech a plánech odezvy.

x. Systém řízení bezpečnosti i krizové řízení musí být musí být přizpůsoben místním podmínkám.

xi. Systém řízení bezpečnosti musí mít legitimitu.

d) Na základě stanovených kritérií se hodnotí stav jednotlivé části kritické infrastruktury podle kvalitativní stupnice:

i. Velmi dobrý stav: prvek je v bezvadném stavu a plní své funkce. Náklady na údržbu jsou v souladu s normami. Nejsou provozní problémy

ii. Dobrý stav: prvek je v dobrém stavu a plní své funkce. Náklady jsou v souladu s normami ale postupně rostou. Prvek je v polovině své životnosti. Provozní problémy jsou občas.

iii. Přijatelný stav: Prvek je opotřebován a má nižší výkonnost. Náklady na údržbu překračují normy a stále rostou. Časté jsou provozní problémy.

iv. Špatný stav: prvek je významnou měrou opotřeben a své funkce plní na nízké úrovni. Náklady na údržbu výrazně překračují normy. Prvek se blíží ke konci životnosti.

v. Kritický stav: Prvek je ve špatném stavu a nepracuje jak by měl. Náklady na údržbu jsou nepřiměřeně vysoké. Je nutná výměna.

2.2.3 Legislativa

Česká legislativa pojem „kritická infrastruktura nezná“ a však se touto problematikou zaobírá. Probíhají práce spojené s ochranou kritické infrastruktury a postupně se připravuje legislativní prostředí. Avšak ochrana kritické infrastruktury probíhá podle zákonů, které lze použít. Jedná se například o zákony na ochranu dodávek ropy a elektřiny.

a) Zákon č. 189/1999 Sb. o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů.

b) Zákon č. 458/2000 Sb. o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů.

c) Zákon č. 406/2000 Sb. o hospodaření energií.

Z hlediska řízení státu je absence zákonu, který by koordinoval jednotlivé právní předpisy a bude upravovat jednotlivé oblasti. Selhání kritické infrastruktury může mít dopad i na okolní státy a proto byly úkoly pro státní správu definovány takto[22]:

a) prosazovat národní a mezinárodní koncepci

b) zpracovat potřebnou legislativu

c) vyměňovat si informace s mezinárodními organizacemi, vládami a soukromím sektorem

d) vyzývat k přijetí příslušných opatření

e) hodnotit hrozby a zranitelnost a sdílet tyto informace

f) aplikovat krizová opatření

g) stanovit finanční zatížení soukromého sektoru

h) pro soukromý sektor se vytyčily úkoly[22]:

   a. uskutečňovat státní koncepci

   b. uskutečňovat nadnárodní koncepci

   c. hodnotit vlastní zranitelnost a závislost

   d. realizovat krizová opatření

e. rozdělit odpovědnost

f. vyměňovat informace s vládou a jinými organizacemi

Ukazuje se, že stav ochrany není dobrý a existují velké nedostatky.

Legislativní podklad řízení bezpečnosti[23, 24]:

a) Zákon č. 1/1993 Sb., Ústava ČR

b) Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR

c) Zákon č. 238/2000 Sb., o HZS

d) Zákon č. 239/2000 Sb., o IZS

e) Zákon č. 240/2000 Sb., o krizovém řízení

f) Zákon č. 241/2000 Sb., o HOPKS

g) Nařízení vlády č. 462/2000 Sb., k zákonu 240/2000

h) Vyhláška č. 498/2000 Sb., o plánování a provádění hospodářských opatření při krizové stavy

i) Zákon č. 12/2002 Sb., o státní pomoci při obnově území postiženého živelní nebo jinou pohromou

j) Zákon č. 59/2006 Sb., o prevenci závažných havárií

k) Zákon č. 18/1997 Sb., atomový zákon

l) Zákon č. 254/2001/8 Sb., o vodách

2.2.4 Evropské nástroje řešení kritické infrastruktury

a) **Evropský program pro ochranu kritické infrastruktury (EPCIP)**: tento program by měl zajistit ochranu s nejmenší pravděpodobností selhání v rámci celé EU. Měl by minimalizovat negativní dopady. Pro EPCIP je charakteristické zajištění hrozeb vyplývající z teroristického ohrožení. Ochrana bude zaměřena na sblížení všech rizik, aby zainteresované subjekty mohli své úsilí zaměřit na ta rizika proti kterým jsou stále zranitelnější[25].

b) **ARGUS**: jedná se bezpečný a obecný systém rychlé výměny informací. Jedná se systém, který bude logickým rozhraním zajišťující rychlý tok informací mezi stávajícími systémy. Cílem bude maximální ochrana a bezpečnost včetně sítě donucovacích orgánů [26].

c) **Výstražná informační síť kritické infrastruktury (CIWIN)**: je zaveden jako součást EPCIP. CIWIN bude napojen na ARGUS.

d) **Evropská agentura pro informační a síťovou bezpečnost (ENISA)**: hlavním cílem je dosáhnutí vysoké informační a síťové bezpečnosti mezi členskými státy.

3 ELEKTRICKÁ ENERGIE

Elektrická energie *je schopnost elektromagnetického pole konat elektrickou práci. Čím větší energii má elektromagnetické pole, tím více elektrické práce může vykonat*[11].

Elektrická energie se získává přeměnou jiné energie. V dnešní době se využívá energie z přírodních zdrojů jako je uhlí, ropa, plyn voda a jiné. Výroba, přenos, rozvod a spotřeba elektrické energie je soubor označovaný jako elektrizační soustava. Rozvodná síť elektrizační soustavy v průběhu několika desítek let zažila velký rozmach. Na počátku minulého století bylo jen několik kilometrů rozvodné sítě. Nyní je rozvodná síť dlouhá v řádově tisíce kilometrů, napojená na okolní státy a neustále modernizovaná[27].

3.1 Elektrizační soustava

Elektrizační soustava *je část energetické soustavy a zahrnuje všechny silnoproudá zařízení sloužící k získání elektrické energie a k její přenosu a rozvodu až po jednotlivé spotřebiče. Je tvořena alternátory ve výrobnách elektrické energie, přenosovou soustavou a rozvodnými soustavami*[12].

S objevem elektrické energie začala éra elektrifikace. Po druhé světové válce se začaly propojovat elektrické sítě států. Dělo se tak na celém světě. V Evropě došlo ke vzniku dvou mezinárodních soustav. Západoevropská síť (UCPTE) a síť „socialistického bloku“ (MIR). Na našem území se začala elektrizační soustava propojovat s NDR v oblasti Krušných hor kdy jsem dodávali elektrickou energii do Karl-MarxStadtu, dnešní Chemnitz. U polských hranic jsem dodávali elektrickou energii do Polska a z Polska byla z oblasti Katowic dodávaná energie pro Ostravu a Slovensko. Díky tomuto systému se zkracovaly dodávky a snižovaly ztráty ve vedení. Později byla tato soustava rozšířena v Mukačevu na ukrajinskou elektroenergetickou síť Sovětského svazu a v Maďarsku, které bylo napojeno na Bulharsko a Rumunsko[28].

---

[11] http://cs.wikipedia.org/wiki/Elektrick%C3%A1_energie

[12] http://www.cez.cz/edee/content/file/_static/encyklopedie/vykladovy_slovnik_energetiky/hesla/elektriz_soust.html

Rozvodné soustavy UCPTE a MIR se od sebe liší a nastával problém s jejich propojením. Soustavy se liší rozdílnými metodami a technickými prostředky regulace kmitočtu a každá síť pulzuje jiným tepem. Koncem padesátých let se začaly obě soustavy propojovat. První propojení vzniklo s Rakouskem tzv. vyděleným provozem. Rakousko nám dodávalo energii v letních měsících kdy z vodních elektráren a my jsme ji vraceli z uhelných elektráren. Později se obě soustavy propojily přes tzv. stejnosměrnou spojku. Střídavý proud se usměrňuje pomocí polovodičů a po té opět pomocí polovodičů mění na střídavý. Výhodou je nezávislost sítí. Každá síť může pracovat nezávisle na druhé a není ovlivněna případnou poruchou v jedné síti. V roce 1995 se Česká republika připojila na soustavu UCPTE mezi bavorským Weidenem a českým Rozvadovem. Vybudovala se nová měnírna a vedení o napětí 400kV. Jedná se o přímé napojení, které mohlo být realizované díky mnoha technickým změnám provozu elektrizační soustavy a změnám principu regulace turbín v elektrárnách[28].

3.1.1 Požadavky na elektrizační soustavu

Elektrizační soustava je vybudovaná a vyprojektovaná tak aby vyhověla několika požadavkům[29]:

a) **Spolehlivost dodávky elektrické energie**: jakékoliv přerušení toku energie může vyvolat velké finanční škody a ohrozit lidské životy. Proto je nutné zajistit spolehlivost systému
   i. Vysokou kvalitou jednotlivých prvků systému
   ii. Dostatečnou rezervou ve výrobě energie
   iii. Bezpečností systému
   iv. Využíváním rozsáhlých sítí k zásobování odběratelů více cestami

b) **Dobrá kvalita dodané energie**:
   i. Udržování napětí na definovaných hladinách
   ii. Udržování kmitočtu na definované hladině

c) **Hospodárná výroba a rozvod**: Je třeba z hlediska účinnosti a nákladů optimalizovat náklady na výrobu a přenos energie.

d) **Dopad na životní prostředí**: Důležité je co nejmenší znečištění životního prostředí. Proto jsou podniky nuceny nejdříve vyhledávat efektivní využití stávajícího zařízení. Získání stavebního povolení v takovém rozsahu začíná být stále těžší.

3.2 Prvky elektrizační soustavy

3.2.1 Elektrárny

Elektrárna *je technologické zařízení sloužící k výrobě elektrické energie. Ta se získává přeměnou z energie vázané v nějakém zdroji. Nejčastěji je tato energie nejdříve přeměněna na energii mechanickou, kterou je následně poháněn elektrický generátor. Další alternativou může být využití fotovoltaického jevu nebo termoelektrického jevu, ale obě možnosti jsou prakticky nepoužitelné pro větší elektrické výkony*[13].

Většina elektrické energie se v Česku vyrábí v tepelných elektrárnách, jaderných a vodních. Tři čtvrtiny elektrické energie vyrábí gigantická společnost ČEZ, která vlastní 15 uhelných, 2 jaderné, 12 vodních, 1 větrnou a 1 sluneční elektrárnu[30].

V tepelných elektrárnách se voda ohřívaná v kotli přeměňuje na páru, která roztáčí turbínu. Turbína pohání alternátor, který vyrábí elektrickou energii. Ta je rozváděna vedením vysokého napětí. Teplo se v tepelných elektrárnách vytváří spalováním fosilních paliv (uhlí, ropa, oleje, mazut, zemní plyn). Příkladem tepelné elektrárny je i jaderná elektrárna. Ta se liší od klasické tepelné elektrárny přítomností reaktoru místo kotle. V reaktoru probíhá řízená štěpná reakce. Palivem bývá nejčastěji uran či plutonium. Dalším příkladem elektrárny je vodní elektrárna. Ta je poháněna vodou z řek, přehrad, přílivem či odlivem nebo energií z mořských vln. Obsluha je poměrně jednodušší a na její spuštění a zastavení není třeba tolika lidí. Ve světě procují i jiné elektrárny jako jsou sluneční, větrné ty však na našem území neplní tu hlavní funkci při výrobě elektrické energie. Slouží jen jako demonstrativní ukázky alternativní elektrárny[31].

Uhelná elektrárna

Principem této elektrárny je přeměna tepelné energie na mechanickou a mechanické na elektrickou. Teplo které je postupně uvolňováno z kolte ohřívá vodu a mění jí v páru. Pára naráží na lopatky turbíny, rozpohybuje jí. Turbína je pevně spojena s generátorem, který otáčivými pohyby vytváří elektřinu. V generátoru rotuje magnet, který indikuje napětí a proud. Vše se otáčí rychlostí 3 000 otáček za minut. Pára jde do kondensátoru, kde

[13] http://encyklopedie.seznam.cz/heslo/128046-elektrarna

se přemění zpět na kapalinu a vrací se do oběhu. Pára která je vyrobena v kotli nemusí soužit pouze k výrobě elektřiny ale i k vytápění měst či obcí. Na takové principu jsou založeny městské teplárny. Uhelné elektrárny jsou uspořádány do tzv. výrobních bloků. Výrobní blok znamená samostatnou jednotku skládající se z kotle, turbíny a příslušenství, z generátoru,odlučovače popílku, chladící věže, blokového transformátoru a odsiřovací zařízení[32].

Jaderná elektrárna

Jaderná elektrárna a uhelná elektrárna mají mnohé společné. Oba typy elektráren jsou tzv. tepelné elektrárny. Rozdíl mezi nimi je ve zdroji tepelné energie. V jaderné elektrárně je tepelná energie uvolňovaná při řízené štěpné reakci probíhající v jaderném reaktoru. Většina jaderných elektráren pracuje na tříokruhovém systému. Primární (jaderný), sekundární (nejaderný) a terciární (chladící)[33].

Primární okruh jaderné energie slouží k získávání tepelné energie z řízené štěpné řetězové reakce. Pomocí chladiva se získaná tepelná energie odvádí a přeměňuje na jinou formu tepelné energie využitou v parní turbíně. V sekundárním okruhu dochází k přeměně tepelné energie páry na mechanickou energii rotoru parní turbíny. Úloha terciárního okruhu je vytvoření co největšího podtlaku v kondensátoru turbíny. Čím bude nižší teplota chladící vody v terciálním okruhu, tím větší bude vytvořený podtlak a bude vytvořena větší účinnost turbíny[34].

Vodní elektrárna

Princip vodní elektrárny je založen na roztáčení turbíny pomocí vody. Turbína je na společné hřídeli s generátorem a tvoří tzv. turbogenerátor. Mechanická energie proudící vody se tak mění na elektrickou. Vodné elektrárny v ČR vyrábí celkem 17% veškeré energie[36].

Výhodou vodních elektráren je, že dokáží vyrobit elektrickou energii zadarmo. To platí tehdy, jestliže náklady na výstavbu elektrárny a vodního díla zaručují dostatečný přívod vody[31].

3.2.2 Přenos elektrické energie

Přenos a rozvod elektrické energie se děje pomocí elektrických sítí. Ty mají za úkol propojení elektráren a přepravu velkých výkonů přenosovou soustavou (napětí 400 kV a 220 kV) a přepravu elektrické energie na nižší napětí (110 kV a 22 kV) distribuční

soustavou k odběratelům. U odběratelů distribuční transformační stanice sníží napětí na 3x380/220 V[28].

Elektrické sítě dělíme z několika hledisek [31]

a) Z hlediska parametrů

i. Sítě s prostorově soustředěnými parametry (sítě VN a NN)

ii. Sítě s prostorově rozloženými parametry (sítě VVN)

b) Z hlediska hladiny napětí

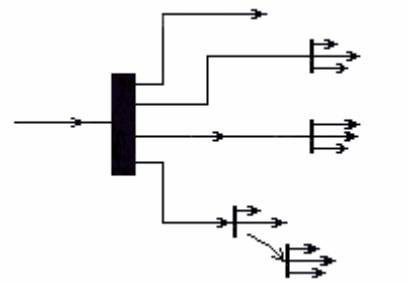
i. Přenosová síť (400kV, 220kV a částečně 110kV)

ii. Distribuční sítě (částečně 110kV, 25kV, 22kV, 10kV, 6kV, 0.4kV)

c) Z hlediska topologie

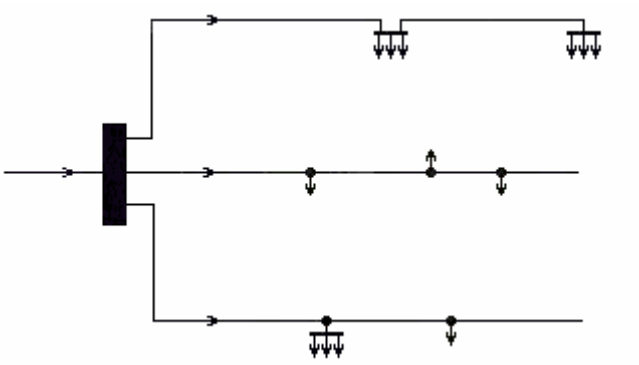
i. Paprskové sítě (obrázek 1). Snadno se udržují, jsou jednoduché a snadno se vyhledávají poruchy. Nemá rezervní napájení, výpadek jednoho prvku sítě má za následek výpadek napájení jednoho nebo i více odběrných míst.

Obrázek 1: Paprsková síť



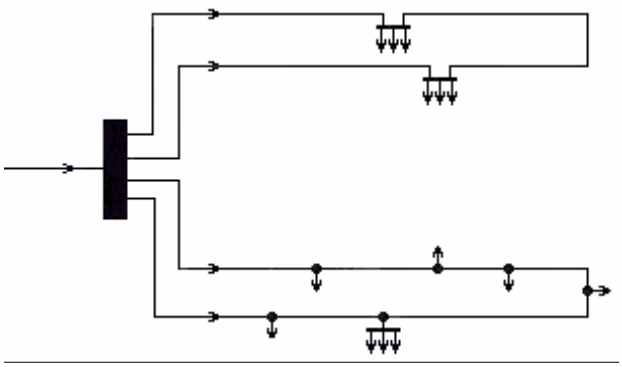
ii. Průběžné sítě (obrázek 2). Průběžné sítě jsou přehledné, ale díky své konfiguraci musejí mít větší průřezy kabelů z napájecí rozvodny.

Obrázek 2: Průběžné sítě



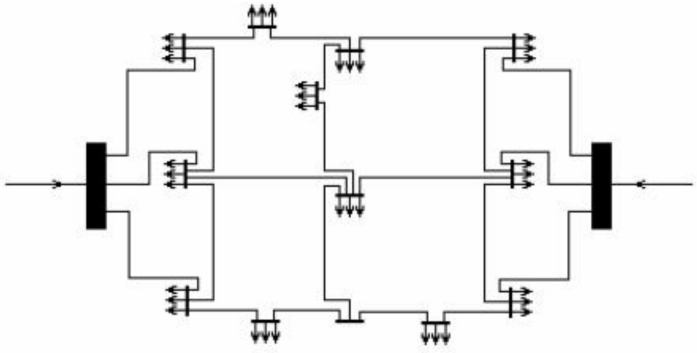
iii. Okružní sítě (obrázek 3). Každé odběrné místo má napájení ze dvou stran. Tím je zvýšena spolehlivost napájení

Obrázek 3: Okružní sítě



iv. Mřížové sítě (obrázek 4). Jednotlivá vedení sítě se stýkají v uzlech, které tvoří pojistkové sítě či rozvodnice. Při poruše je pojistkami odpojeno vedení, ale uzel je napájen z ostatních větví.

Obrázek 4: Mřížová síť



Pro přenos energie o vysokém napětí slouží převážně venkovní vedení. To musí čelit nepřízní počasí. Jako vodiče se používají bronzové vodiče do průřezu 25 mm^2 nebo lana. Soustředěná lana mají v ose duši, drát a určitý počet drátů stejného průřezu. Lana bývají kombinovaná z různých drátů. Nejběžnější je Al-Fe. Za vlhkého počasí se na lanech malého průměru objevuje pozorovatelné napětí tzv. korona. Projevuje se výboji rušící televizi a rozhlas. Pro minimalizování korony se vedení o napětí 4 000 kV a vyšší používají svazkové vodiče (vedení několika lan). Na stožárech jsou vodiče upevněny pomocí izolátorů. Izolátory mohou být podpěrné nebo závěsné. Konce izolátorů jsou vybaveny speciálními svorkami vytvořenými tak, aby se vodiče a izolátory nepoškodily. Izolátory musejí odolávat velké mechanické a fyzikální zátěži. Jsou vyráběny z porcelánu nebo skla. Nejviditelnějším zařízením rozvodu elektrické energie jsou stožáry. Na vršku stožáru je slabší zemnící vodič, zabezpečující ochranu proti bleskům. Konstrukce stožárů

zabezpečuje, že se svazky lan k sobě ani v největších vichřicích nepřiblíží. Čím jsou stožáry vyšší, tím mohou být od sebe vzdálenější. Stožáry jsou nosné a výztužné. Výztužné stožáry se nesmějí zřítit. [28].

3.2.3 Přenosová soustava

Elektrická přenosová soustava je systém zařízení, která zajišťuje přenos elektrické energie od výrobců k odběratelům, čímž se míní přenos ve velkých měřítkách, od velkých zdrojů k velkým rozvodnám[14].

Přenosová soustava je převážně tvořena soustavou nadzemních vedení vysokého napětí. Dále je tvořena kabely, transformátory, odpojovači, vypínači, bleskojistkami kompenzačními prvky systémem řízení a regulace sítě. Na výstupu z přenosové soustavy jsou transformátory dodávající elektřinu do distribuční sítě [37].

V České republice provozuje přenosovou soustavu státní společnost ČEPS, a.s. Přenosová soustava ČEPS propojuje všechny významné subjekty soustavy a zajišťuje významný podíl na zahraniční spolupráci. ČEPS, a.s. zajišťuje přenos elektřiny, provoz, údržbu a rozvoj přenosové soustavy a dispečerské řízení. Dále zpracovává plán obrany přenosové soustavy proti šíření poruch a plán obnovy elektrizační soustavy po rozsáhlých poruchách. Z technického hlediska řídí systémové služby, jako je regulace výkonu, kmitočtu a napětí [38].

Přehled zařízení přenosové soustavy

Tabulka 5: Zařízení přenosové soustavy(zdroj [38])

Popis zařízení	Celkem ČR	Jednotky
Trasy vedení 400 kV	2 900	Km
Trasy vedení 220 kV	1 440	Km
Trasy vedení 110 kV	106	Km
Délka vedení 400 kV	3 383	Km
Délka vedení 220 kV	1 912	Km
Délka vedení 110 kV	161	Km
Zahraniční vedení 400 kV	10	Ks
Zahraniční vedení 220 kV	6	Ks

[14] http://encyklopedie.seznam.cz/heslo/460358-prenosova-soustava

Zahraniční vedení 110 kV	0	Ks
Rozvodny 420 kV	24	Ks
Rozvodny 245 kV	14	Ks
Rozvodny 123 kV	2	Ks
Transformační výkon 400/220 kV	1 900	MVA
Transformační výkon 400/110 kV	11 290	MVA
Transformační výkon 220/110 kV	4 000	MVA
Transformační vazby 400/220 kV	4	Ks
Transformační vazby 400/110 kV	41	Ks
Transformační vazby 220/110 kV	20	Ks
Kompenzační výkon 400 kV	660	MVAr
Kompenzační výkon 35 kV	367	MVAr
Kompenzační výkon 10 kV	409	MVAr
Kompenzační uzly (tlumivky) 400 kV	4	Ks
Kompenzační uzly (tlumivky) 35 kV	6	Ks
Kompenzační uzly (tlumivky) 10 kV	9	Ks

3.2.4 Distribuční soustava

Distribuční soustava je rozvod elektřiny z přenosové soustavy nebo ze zdrojů zapojených do ní ke koncovým uživatelům. Součástí je řídící, ochranné, zabezpečovací a informační systémy. Jedná se o zařízení s napětím 110 kV a nižším [40].

Provozovatelem distribuční soustavy je právnická či fyzická osoba, která je držitelem licence na distribuci elektrické energie. Provozovatel distribuční sítě je povinen zabezpečit plynulý a bezpečný provoz přiměřený životnímu prostředí a její rozvoj. Provozovatel je povinen na vymezeném území distribuovat elektřinu konečným zákazníkům a dodávat elektřinu všem kdo o to požádá a splňuje podmínky dané energetickým zákonem[41].

V České republice jsou tři firmy zajišťující distribuci elektrické energie odběratelům. Jedná se o ČEZ Distribuce, a.s., E.ON Distribuce, a.s., Pražská energetika, a.s.

Tabulka 6: Technické údaje distribuční sítě EO.N Distribuce, a.s.(zdroj [42])

	Počet	Jednotky
Zásobovací oblast	26 499	Km^2
Vedení VVN – 110 kV	3 976,1	Km
Vedení VN – 22 kV	21 745	Km
Vedení NN – 0,4 kV	38 837,1	Km
Transformátorovy VVN/VN	78	Ks
Počet transformátorů VVN/VN	145	Ks

Tabulka 7: Technické údaje distribuční sítě ČEZ Distribuce, a.s. (zdroj [43])

	Počet	Jednotky
Zásobovací oblast	52 697	Km^2
Vedení VVN – 110 kV	9 540	Km
Vedení VN – 22 kV	50 136	Km
Vedení NN – 0,4 kV	94 102	km

Tabulka 8: Technické údaje distribuční sítě PRE, a.s (zdroj[44])

	Počet	Jednotky
Vedení VVN – 110 kV	196,4	Km
Vedení VN – 22 kV	3 584	Km
Vedení NN – 0,4 kV	7 557,2	Km
Transformátorovy VVN/VN	20	Ks

3.2.5 Elektrické stanice

K přenosu elektrické energie z místa výroby do místa spotřeby pomáhají elektrické sítě, elektrické vedení a elektrické stanice. Elektrické stanice se dělí na transformátorovy, ve kterých se napětí mění na jiné, spínací stanice, z nichž se rozvádí elektrická energie při tomtéž napětí a měnírny pro usměrnění střídavého proudu na stejnosměrný a kompenzovány sloužící k vyrovnání jalových složek proudu. Podle velikosti a provozu jsou stanice malé, střední a velké, s obsluhou a bezobslužné. Velkou částí stanic jsou rozvodny, u menších stanic jsou to rozvaděče, u malých stanic rozvodnice. Rozvodny jsou

zařízení pro přivádění a odvádění elektrické energie téhož napětí. Mají samostatnou budovu nebo samostatný prostor. Elektrickou část rozvoden tvoří vodiče, izolátory, přístroje spínací, ochranné, řídící a návěstní. Kryté se používají pro napětí do 35 kV, venkovní jsou pro VVN [39].

Každá elektrická stanice má své části. Jedná se o části elektrické, společná a pomocná a stavební[31].

a) elektrická část
    i. rozvodná zařízení, jedná se o hlavní část elektrické stanice sloužící k rozvádění, měření, jištění a kontrole elektrické energie a pro spínání a přepínání elektrických obvodů
    ii. transformátory
    iii. kompenzační zařízení
b) společná a pomocná část
    i. slouží k zabezpečení provozu a údržbě elektrických stanic
c) stavební část
    i. budovy, pozemky, komunikace aj.

3.3 Stabilita elektrizační sítě

Stabilita elektrizační soustavy je problematika velice náročná. S velkou přesností lze stanovit zda soustava byla v minulosti stabilní či nikoliv, ale již nelze říci jak bude elektrizační soustava náchylná na výpadky elektrické energie v budoucnosti. Musíme předpokládat, že soustava má přiměřené rezervy jak ve zdrojích, tak v přenosových linkách aby došlo k vyrovnání potřeb odběratelů a případným nepředvídatelným událostem. Mezi nepředvídatelné události řadíme rozsáhlé neřízené výpadky elektrické energie způsobené počasím či teroristickými útoky[46].

Velkou nevýhodou elektrické energie je, že se nedá akumulovat. Proto se musí řídit jednoduchým vztahem VÝROBA = SPOTŘEBA. Výsledkem toho je pružné reagování na spotřebu energie, po které je v daném čase poptávka. Výroba elektrické energie je rozdělena do pásem (základní a regulační)[47].

V základním pásmu pracují tepelné a jaderné elektrárny, které dodávají většinou konstantní výkon. Po těchto elektrárnách se požaduje nemněný výkon dodávek elektrické energie[47].

Do regulačního pásma se řadí takové zdroje, které lze v krátkém čase uvést do provozu a doplnit chybějící výkon, či je bezproblémově odstavit. Do tohoto pásma se ředí vodní elektrárny, paroplynové, parné elektrárny[47].

Přenos energie každoročně roste a tím roste riziko poruchovosti toku elektrické energie. V roce 2002 činil přenos elektrické energie přenosovou soustavou 58 018 GWh. V roce 2006 to bylo již 61 216 GWh. S tokem energie rostou u ztráty energie i celkový instalovaný výkon transformátorů. V roce 2006 bylo zaznamenáno 83 výpadků, co je oproti roku 2005 o 22 výpadků více. Z celkových 83 výpadků v roce 2006 bylo celkem 20 v souvislosti s omezením výroby či přerušením dodávek elektrické energie. Jednalo se o 69 výpadků přenosových vedení a 14 výpadků transformátorů. 25. července 2006 poprvé v historii vyhlásil ČEPS v důsledku narušení celistvosti přenosové soustavy stav nouze pro ČR. Stalo se tak v důsledku vysokých teplot a zvýšené zátěže přenosových soustav při omezení výroby elektrické energie. To se projevilo atypickým rozložením toku elektrické energie. 4. listopadu 2006 postihla Evropu vlna kaskádovitých výpadků, která ovlivnila i elektrizační síť ČR. Došlo k vypnutí přenosového vedení v Německu a postupnému navazování dalších států[48].

Elektrizační soustava je jedním z nejsložitějších „organismů“. Musí být správě vyživována, chráněna, trénována, rozvíjena a obnovována. Musí být dokonale modelována. To umožňuje řádně připravit její provoz a správně identifikovat poruchy a sjednávat nápravy. Velmi důležitá je správná interpretace výsledků vycházející z modelových výpočtů. Elektrizační soustava ČR pracuje v synchronním provozu se soustavami Evropy. To vyžaduje modelování celého celku. Lze tohoto docílit díky spolupráci provozovatelů přenosových soustav sdružených v organizaci UCTE[46].

3.4 Energetická bezpečnost

Energetická bezpečnost *je zajištění kontinuity nezbytných dodávek energie a energetických služeb pro zajištění chráněných zájmů státu*[15].

[15] BENEŠ, Ivan, *Energetická bezpečnost*, CITYPLAN, spol, s.r.o., 2007, 36.str, ISBN 978-80-254-1244-2

Energetická bezpečnost se dělí na 3 témata[49]:

a) Bezpečnostní zajištění energetických zdrojů

b) Bezpečnost energetických transformací a dopravy energie

c) Energetická bezpečnost konečných uživatelů energie

V subsystému energetických transformací a dopravy energie je největším bezpečnostním problémem privatizace a liberalizace. Dochází k rozchodu přístupu veřejného sektoru a přístupu soukromého sektoru. Odpovědnost vlád vychází ze zajištění spolehlivého a bezpečného toku energie ke spotřebiteli. Odpovědnost soukromého sektoru vede ke zvyšování tržní hodnoty energetických podniků. Může docházet ke střetům. Tam kde jsou tržby malé není zajištěna míra spolehlivosti dodávek, neboť zásobování je ekonomicky málo motivované. Z hlediska bezpečnosti je subsystém konečných uživatelů nejkritičtější. Přerušení dodávek energie spotřebitelům dá vzniknout krizovým situacím a ohrožením chráněných zájmů ČR[49].

3.4.1 Zajištění energetických zdrojů

Subsystém zajištění energetických zdrojů má dvě rozdělení. Jedná se o vlastní naleziště a o dopravní cesty z producentských zemí do zemí importérů. Členění zdrojů znamená volbu mezi primárními zdroji energie (ropa, uhlí, zemní plyn, uran). Členění dovozních cest znamená volbu v dopravě přístupových zdrojů[49].

Tabulka 9: Hlavní zdroje neobnovitelné energie

Neobnovitelná zdroj	Kolik	Kde
Ropa	59,3% zásob na území 5 států	Saudská Arábie, Írán, Irák, Kuvajt, Spojené Arabské Emiráty
Zemní plyn	55,7% zásob na území 3 států	Rusko, Írán, Katar
Uhlí	¾ zásob na území 5 států	USA, Rusko, Čína, Indie, Austrálie
Uran	50,7% zásob na území 3 států	Austrálie, Kazachstán, Kanada

Zásobování primárních energetických zdrojů v ČR jsou tvořeny hnědým uhlím, černým uhlím a uranovou rudou. Ve spotřebě uhlí je ČR soběstačná. Ve spotřebě zemního plynu však soběstačná není. Celková těžba zemního plynu tvoří pouhých 1,5%. 75% spotřeby zemního plynu se dováží z Ruska a 24% z Norska. V dlouhodobém horizontu

bude ČR odkázána pouze na dodávky z jiných zemí. Dá se proto předpokládat, že získání neobnovitelných zdrojů bude předmětem mezistátních vztahů.

3.4.2 Bezpečnost energetické distribuce

Elektrizační soustava je nejranitelnějším prvkem kritické infrastruktury. Ve vyspělých zemí je elektrizační soustava nejcentralizovanějším a nejtechničtějším prvkem ve státě. Elektrická síť je navrhována podle pravidla N-1, což znamená, že je schopna se vyrovnat s výpadkem jednoho prvku soustavy. Síť však nemá žádné zásobníky na uchování elektrické energie a při nerovnováze mezi potřebou a výrobou by mohlo dojít k selhání systému během několika málo sekund. Není fyzicky možné zajistit ochranu elektrizační sítě. Proto se musejí hledat taková opatření, která by zmírňovala následky blackoutu při vypadnutí jednoho či více prvků soustavy. V nedávně minulosti byly zaznamenány velké výpadky trvající i několik dnů. Je tedy nasnadě, aby elektrizační síť byla chráněna jako celek[49].

Díky změně lidských sídel a závislosti na energetice se lidská společnost stává čím dál zranitelnější na výpadky elektrické energie. Jedná se o surovinu, která je již nezbytně nutná k přežití a jakékoliv napadnutí elektrizační soustavy ochromí celou společnost.

3.5 Blackout

Blackout je totální výpadek elektrické energie. Jedná se o jedno z nejzávažnějších ohrožení ekonomického vývoje. Ve zprávě Global Risks 2006 byla hodnocena pravděpodobnost evropsko výpadku elektřiny na 5 stupňové stupnici hodnotou 3 s ekonomickým dopadem 2. Specifickou vlastností blackoutu je skutečnost, že dopady na okolí jsou mnohem větší než škody na zařízení. Příčinou jsou domino efekty šíření krizové situace. Výsledkem je ohrožení chráněných zájmů státu. Důležité je zabývat se opatřeními, než příčinami. Ze zahraničních zkušeností vyplývá, že blackout je reálně nebezpečí[50].

Dopady nežádoucích situací jsou členěny do několika kategorií: zdraví a životy, majetek a ekonomika, životní prostředí. V případě blackoutu jsou dopady zařazovány do kategorie, zdraví, životy a ekonomika[50].

Blackout je sled velmi rychlých událostí vzniklých v elektrizační soustavě. Příčinou vzniku blackoutu bývá špatné zvládnutí nabídky a poptávky po elektrické energii. Vzniká během několika málo sekund a nelze proti němu vytvářet strategické rezervy. V budoucnu se dá předpokládat zvýšené riziko vzniku blackoutu. Přibývají extrémní klimatické jevy, objevuje se hrozba teroristického útoku v ČR díky zapojení ČR do akcí na

Středním Východě. Dlouhotrvající blackout může rozložit jakoukoliv průmyslově vyspělou společnost. Vzniklá chaotická situace by se jen velice těžce zvládala.

3.5.1 Kdyby nešel proud

Každá moderní sopečnost je na elektřině naprosto závislá. Nepřipouští si možnost jakéhokoliv velkého zkolabování elektrické sítě. Elektřina se bere jako samozřejmost a život bez ní si neumíme představit. Jak by ale vypadal svět po následku dlouhotrvajícího blackoutu?

První minuty

Vypadne vše, co je na elektřině závislé, kromě zařízení vlastnící záložní baterie či agregát. Došlo by k:

a) vyřazení dopravní signalizace

b) vyřazení železniční dopravy

c) ochromení letecké dopravy

d) výpadku mobilní sítě, kabelové televize, internetu

Lidé by uvízli ve:

a) výtazích

b) metrech

c) vlacích

d) autech na ucpaných komunikacích

Hodiny a dny

Většina výrobních zařízení by uzavřela své podniky. Jednak z důvodů absence náhradních zdrojů, jednak díky tomu že se lidé nedostanou do práce. Ochromil by se finanční trh, bankovnictví elektronický platební styk. Nebylo by možné vybírat peníze z bankomatů. Kolabovalo by zásobování pitnou vodu. Nebylo by možné k čerpání vody do systému. Přestalo by fungovat topení a klimatizace. Zavřely by krámy a restaurace. Nebylo by možné nakupovat potraviny. Vznikly by požáry díky svícení svíčkami. Ochromila by se ambulantní péče[49].

Týdny a měsíce

Jediná zkušenost blackoutu trvající týdny má jediné město – Auckladn na Novém Zélandě. Malým podnikům začnou vznikat ztráty, které nebudou schopny pokrýt. Značná část velkých obchodů ztratí nedůvěru v infrastrukturu a přesune své podniky jinam. Ekonomické důsledky několika týdenního výpadku ponese stát několik let[49].

3.5.2 Příklady velkých blackoutů

a) Výpadek proudu trvající 5 týdnu (20. února – 27. března 1998) ochromil městečko Auckland na Novém Zélandě. Blackout byl způsoben opakovanými poruchami na vysokonapěťových kabelech[49]

b) 14. srpna 2003 došlo ke kaskádovitému rozvoji poruch na elektrizační síti. Počáteční impulz dal zkrat způsobený větvemi stromů. Zasaženo bylo 50 milionů lidí v Kanadě a USA[49].

c) 27. – 28. září 2003 nastal blackout postihující celkem 56 milionů lidí v Itálii, Sardinii. Díky bouřce, která vyřadila mezistátní vedení elektrické energie zásobující Itálii ze Švýcarska. Díky kaskádovitým poruchám se během 4 sekund zhroutil systém zásobování elektřinou[49].

d) Dosud největší výpadek elektrické energie nastal v Indii, kde postihl přes 100 milionu lidí. Blackout byl opět způsoben vícenásobnými poruchami, které vyřadily 2 700 MW výkonu[49].

e) 4. listopadu 2006 došlo k rozsáhlému výpadku elektrické energie v Německu, Francii, Itálii, Španělsku, Belgii a Portugalsku. Výpadek nastal díky vypnutí proudu přes řeku Ems, aby mohla bezpečně proplout velká loď. Důsledky vypnutí však nebyly správně vyhodnoceny a evropská elektrizační síť se rozpadla na tři části[49].

II. PRAKTICKÁ ČÁST

4 ELEKTRIZAČNÍ SOUSTAVA

Za krizových stavů je obvyklé omezování poskytování výrobků a služeb obyvatelstvu. Služby a výrobky se dodávají v množství nutném k přežití krizového stavu. To se ale nedá praktikovat v oblasti elektrizační soustavy. Elektrická energie se nedá uchovávat v zásobníkách. Aby mohla být odebírána spotřebitelem, je nutné ji vyrobit a ihned transportovat. Jakákoliv nerovnováha mezi výrobou a spotřebou spouští celou řadu systémových ochran a automatik. Pokud se nezabrání v nerovnováze ztrácí se kontrola nad celým systémem. Pokud jsou dodávky elektrické energie delší jak 24 hodin nastává velký problém u spotřebitelů energie a život společnosti se značně naruší. Čím delší je přerušení dodávek elektrické energie tím větší nastává problém v běžném životě. Po rozboru distribuční společnosti se ukázalo, že jsou, až na hlavní město Praha, ve všech ostatních regionech podmínky pro nouzové zásobování elektřinou pokrývající 40% – 100% zatížení dané sítě. Objevuje se zde zásadní legislativní problém, na který se odvolávají distribuční společnosti. Jedná se o zákon č. 458/2000 Sb., energetický zákon. Energetici mají tak únikovou cestu vyhlášením stavu nouze v energetice a koneční spotřebitelé se tak nedoví, kdy bude po výpadku proudu zásobování opět obnoveno[52].

Tak jako každá soustava má i elektrizační soustava své silné a slabé stránky. Ohrožují ji určitě hrozby a účelně by se proti nim mělo bojovat.

4.1 Silné stránky ES[52]

a) Česká republika je výkonově soběstačná, ale vyváží i cca 20% výkonu v poměru k maximálnímu zatížení soustavy.

b) Vzhledem k vysokému podílu jaderné energetiky a vlastním zdrojům uhlí jsou mezní náklady na výrobu poměrně malé

c) Přenosová soustava je výborně navržena a provozována a zajišťuje spolehlivý přenos elektrické energie

d) Česká republika je elektrifikována

e) Více jak třetina zdrojů elektřiny je vyvedena do distribučních soustav a mohou se tak stát zdroji místních ostrovních systémů k nouzovému zásobování elektřinou

f) V České republice je vysoký znalostní potenciál pracovníků v energetice

4.2 Slabé stránky ES[52]

a) energetická a krizová legislativ nejsou propojeny. Doposud není naplněn úkol energetické koncepce.

b) Liberalizace trhu s energií nadřazují ekonomické ukazatele provozu elektrizačních soustav nad ukazatele spolehlivosti a energetické bezpečnosti

c) Díky privatizaci energetických podniků se stát zbavil možnosti přímého ovlivnění energetiky a zbývají pouze legislativní nástroje.

d) Riziko z nedodávky elektrické energie nese prvotně spotřebitel. Dodavatel je oprávněn v případě nutnosti vyhlásit stav nouze a tím je ze zákona vyvázán z odpovědnosti za způsobené škody.

e) V současně době není požadováno, aby veřejné elektrizační soustavy byly schopny zajistit zásobování elektřinou v ostrovních provozech. Tento fakt dělá z elektrizační soustavy nejzranitelnější systém kritické infrastruktury

f) Nejsou zpracovány scénáře odezvy na dlouhodobý výpadek zásobování elektřinou velkého rozsahu včetně vyhodnocení nároků na IZS

g) Od subjektů kritické infrastruktur nejsou vyžadovány plány krizové připravenosti na zajištění kontinuity v případě blackoutu

h) Neexistuje systém přípravy obyvatelstva jak se zachovat v případě blackoutu

4.3 Hrozby ES[52]

a) Ve druhé polovině 20. století nastal investiční boom ve výstavbě elektrárenských zdrojů, který postupně upadl. Ten se začal v současnosti opět oživovat díky společnosti ČEZ i nezávislých výrobců

b) Vysoká zisková marže z prodeje elektrické energie není přiměřeně využita pro obnovu elektrárenského parku

c) Nedostatek globálních surovin vede ke zvyšování ceny elektřiny

d) Přenosová soustava je dimenzována podle zásady n-1. Znamená to, že odolá proti výpadku jednoho důležitého prvku soustavy. V případě vyššího počtu výpadků může nouzový stav přejít do rozsáhlé poruchy - blackoutu

e) Distribuční soustavy nejsou schopny pracovat nezávisle na přenosové soustavě.

f) Nelze vyloučit hrozbu útoku na přenosovou soustavu. I minimální počet útočníků může způsobit vyřazení několika prvků a způsobit blackout trvající týdny až měsíce

4.4 Nouzové dodávky elektrické energie

Elektrizační soustava je nejzranitelnější částí kritické infrastruktury z mnoha ohledů. Jedná se o nejcentralizovanější infrastrukturu. Je dimenzovaná na n-1 poruch. Systém zvládne jednu vážnou poruchu nikoliv však dvě a více. Elektrická energie nelze uchovávat v zásobnících jako ropu či uhlí. Výpadek elektrické energie je otázkou okamžiku. Při nerovnováze mezi výrobou a spotřebou dojde k selhání systému během 5 sekund[52].

Vícenásobná porucha v jednom časovém úseku vede k rozpadu elektrizační soustavy. Rozpad přenosové soustavy vyvolá národní blackout, který postihne 10 milionu lidí. Čtyřnásobná porucha distribuční soustavy postihne tisíce až statisíce lidí. Nejcitlivějším článkem elektrizační soustavy je přenosová soustava. Po rozpadu přenosové soustavy budou odpojeny i systémové elektrárny. Jedná se o jaderné a uhelné elektrárny, které jsou pečlivě střeženy a v případě nutnosti lze ostrahu zvýšit. Po rozpadu přenosové soustavy však systémové elektrárny nemají kam dodávat elektrickou energii a musí být neprodleně odstaveny z provozu. V takovém případě mohou elektrickou energii dodávat systémy ostrovních provozů založených na místních zdrojích. To však nelze docílit dokud neexistuje legislativa nařizující distribučním soustavám zajistit nouzové ostrovní provozy. V případě rozpadu přenosové soustavy by se tak zvýšila bezpečnost zásobování až 100krát. Ostrovní provozy tak mohou výrazně snížit důsledky blackoutu[52].

Je třeba připravit a schválit soubor krizových a energetických zákonů, které by ukládali povinnost provozovatelům elektronických systémů vytvořit ostrovní provozy a energetické inspekci prověření reálné funkce ostrovních provozů.

5 DŮSLEDKY PŘERUŠENÍ DODÁDVEK ELEKTRICKÉ ENERGIE

5.1 Obecné zásady

a) Dopady na životy a zdraví osob. Jedná se o přímě ohrožení života a zdraví provozního personálu zajišťující chod přenosové, distribuční soustavy. Dochází k ohrožení života a zdraví pracovníků likvidující následky poškození. Ohrožení zdraví a života obyvatelstva v důsledku omezení nebo přerušení dodávek energií.

Zahrnují se sem hlavně zdravotnická zařízení, ústavy sociální péče a jiné. Ohrožení života a zdraví v důsledku vzniku sekundárních krizových situací (epidemie, narušení dodávek pitné vody…)

b) Zničení nebo poškození majetku. Zahrnuje se zde převážně zničení, poškození nebo omezení využití nemovitého a movitého majetku. Poškození nebo zničení objektů chráněných památkovou péčí a další jinak významné objekty, muzea aj.

c) Poškození životního prostředí. Znečištění životního prostředí. Poškození životního prostředí v důsledku vzniku sekundárních krizových situací.

d) Mezinárodní dopady. Riziko omezení nebo nemožnosti plnění mezinárodních smluvních závazků, závazků v rámci NATO, nemožnosti plnění hospodářských a obchodních závazků se zahraničím na úrovni podnikatelských subjektů. Nutnost vyžádání a organizování humanitární pomoci

e) Ekonomické dopady. Vyvolané rizikem narušení či celkového ochromení hospodářství s významnými ekonomickými ztrátami ve všech sektorech.

f) Sociální dopady. Sociální dopady na běžný život obyvatelstva. Rychlý nárůst nezaměstnanosti v důsledku redukce hospodářských činností, snížení kapacitních možností a značných ekonomických ztrát hospodářských subjektů. Omezení nebo nemožnost zajištění základních sociálních služeb obyvatelstvu.

5.2 Dopady na obyvatelstvo

Každá průměrná domácnost spotřebuje ročně kolem 2 750 kWh energie, kterou nemůže nahradit žádným jiným druhem energie. Je využita na osvětlení, praní, žehlení, chlazení a mrazení. Spotřeba ostatní energie činí kolem 1 360 kWh. Připadá na vaření, ohřev teplé vody, vytápění. Vyřazením elektrizační soustavy budou nejvíce postihnuty plně elektrizované domácnosti. Obyvatelstvo pro zachování života potřebuje čisté ovzduší, teplo, vodu a potraviny. Přerušením zásobování elektřinou se vyřadí do určité míry i neelektrické zdroje. Pro zajištění informovanosti občanů v krizových situací je důležité, aby se chovali podle postupů, které byly dříve zpracovány, ale aby byla i poskytována aktuální sdělení rozhlasem nebo televizí. V případě výpadku energie je tento způsob informovanosti ohrožen. Nejohroženější skupinou obyvatelstva jsou obyvatelé měst. Z pohledu nouzového plánování a krizového řízení musí být zpracovány scénáře odezvy na možné havárie velkého rozsahu a na krizové situace, při kterých bude nutno použít městské

veřejné teplárny a po vyhodnocení požadavků na provozuschopnost musí být realizována opatření nutná pro zajištění provozuschopnosti městských tepláren.

5.3 Dopady poruchy zásobování na výrobní podniky a podniky služeb

Největším spotřebitelem elektřiny je průmysl.

5.3.1 Zpracovatelský průmysl

Energeticky náročné podniky bývají vybavovány vlastními zdroji elektřiny a tepla. Jsou samovýrobci elektřiny. Někdy jsou přebytky elektřiny a tepla vyrobené nad rámec spotřeby podniku vyvedeny do veřejné elektrické a teplárenské sítě. U některých těchto podniků více než vlastní útok na systém zásobování energiemi, je největší hrozbou útok na vlastní technologii (zejména u podniků chemického průmyslu), kterým lze proměnit podnik na zbraň hromadného ničení se zamořením složek životního prostředí (ovzduší, voda půda).

Zdroje elektřiny nezávislých výrobců pracují většinou v propojení s elektrizační soustavou, ale v případě poruchy sítě jsou schopny obvykle provozu izolovaně, tj. v ostrovním režimu. Vlastní zdroj energie v průmyslovém závodě pak zajišťuje zásobování energiemi nezávisle na veřejných sítích v případě jejich poruch. Tyto zdroje současně plní funkci nouzových zdrojů elektřiny. Pokud závodní zdroj není dimenzován na celý výkon spotřeby závodu, lze pak v případě přerušení napájení ze sítě uplatnit omezení na straně spotřeby pomocí vypínacího plánu tak, aby mohly být zachovány v provozu nejdůležitější technologické procesy. Zabraňuje se tím rozsáhlým škodám, které by mohly vzniknout v provozu v případě přerušení dodávek energie z veřejných sítí. Dodávka elektřiny je tím zajištěna ze dvou vzájemně nezávislých zdrojů. Jako palivo se většinou používá uhlí a zemní plyn, někde se vyskytuje i TTO a v papírnách i dřevní odpad. Technicky jsou závodní elektrárny řešeny obvykle jako:

- parní kotel s parní turbinou na pohon generátoru.
- plynová spalovací turbina se spalinovým kotlem na výrobu technologického tepla, případně v kombinovaném cyklu s parní turbinou.
- spalovací pístový motor pro pohon generátoru a výrobu teplé nebo horké vody (některé motory umožňují i výrobu páry).
- malá vodní elektrárna.

Spalovací turbinu a pístový motor lze vybavit dvoupalivovým systémem pro spalování zemního plynu a lehkého topného oleje s možnosti okamžitého přechodu z jednoho paliva na druhé. Takovéto řešení podstatně zvyšuje nezávislost zdroje na dodávkách paliva.

5.3.2 Doprava

Silniční doprava je závislá na spolehlivém zásobování benzínů a nafty. Vzhledem ke stovkám čerpacích stanic je dopravní infrastruktura ohrožena mnohem více teroristickým útokem na vlastní dopravní stavby, než na zdroj energie pro silniční dopravu. Kritickými místy jsou důležité mosty a dálnice. Tyto problémy se mohou projevit nejen ve zvýšení času na dopravy, ale přinesou sebou značné zvýšení spotřeby pohonných hmot.

Železniční doprava je závislá na kapalných palivech a na elektřině. Při poruše elektrické ho napájení elektrifikovaných tratí mohou být sice elektrické lokomotivy nahrazeny dieselelektrickými lokomotivami. I v případě železniční dopravy nejcitlivější částí jsou železniční uzly, mosty a tunely, jejichž zničení vyřadí celé části železnice.

Náhrada elektrických lokomotiv dieselelektrickým provozem vyvolá značné zvýšení spotřeby nafty, což se projeví nejen v urychlení spotřeby zásob, ale též sníží dopravní kapacity pro ostatní účely.

Městská doprava je závislá na kapalných palivech a na elektřině (metro, tramvaje, trolejbusy) a v menší míře na zemním plynu či LPG (autobusy). Vlastní útok na zásobování MHD energiemi nezpůsobí takové ochromení městské dopravní infrastruktury, k jakému by došlo v případě teroristického útoku přímo na dopravní stavby. Nejzranitelnějšími místy jsou metro, mosty a tunely.

5.3.3 Obchod a služby

Spotřebu energie v obchodech a službách tvoří vytápění, osvětlení, příprava teplé užitkové vody, chlazení a mrazení, příprava pokrmů a zejména spotřeba nejrůznější kancelářské techniky a dalších elektrických spotřebičů.

Banky, telekomunikace, obchodní komplexy jsou velmi citlivé na přerušení dodávky elektřiny, které by znemožnilo jejich provoz, případně způsobilo i značné škody při ztrátě datových údajů. Proto jsou elektronická zařízení často vybaveny zařízením pro nepřerušený přechod z jednoho systému napájení na jiný. Z pohledu nouzového plánování a krizového řízení musí být důležitá elektronická zařízení u bank, telekomunikací a obchodních komplexů vybavena náhradním zdrojem napájení a musí být zajištěn

automatický přechod z jednoho systému na druhý. Důležitá data musí být pravidelně zálohována na vhodných vnějších médiích.

Pro zvýšení spolehlivosti a nezávislosti bývá jako vhodný zdroj elektrické energie instalován nouzový zdroj elektřiny se spalovacím motorem v administrativních budovách, bankách, nemocnicích, hotelech, na letištích a všude tam, kde úplné přerušení dodávky elektřiny není přípustné. Z pohledu nouzového plánování a krizového řízení musí být administrativní budovy, banky, nemocnice, hotely, letiště, kina, divadla a jiná společenská centra vybavena náhradním zdrojem napájení a musí být zajištěn automatický přechod z jednoho systému na druhý.

5.3.4 Zemědělství

Zemědělství je závislá na kapalných palivech a elektřině. Nafta je nejen důležitou pohonnou hmotou pro pohon zemědělských strojů, ale též pro technologické účely. Přerušení dodávky elektřiny může ohrozit velkovýrobní provozy, kdy v důsledku výpadku pohonu ventilátorů může dojít k úhynu většího množství zvířat a drůbeže. Kontaminace zemědělské půdy, vody i ovzduší, může narušit soběstačnost státu v zásobování potravinami. Terčem útoku se mohou stát samozřejmě i potraviny a zdroje pitné vody – jejich ničení nebo kontaminace. Z pohledu nouzového plánování a krizového řízení musí být provedena opatření na zajištění ochrany zdrojů pitné vody, skladů a distribučních center potravin proti útoků teroristů.

5.4 Dopady poruch zásobování na činnost veřejných institucí a služeb

Mezi nejdůležitější státní a veřejné organizace, na které se nevztahují elektroenergetické regulační stupně, patří obrana státu, objekty a zařízení Ministerstva vnitra, Policie České republiky, hasičské záchranné sbory a dále subjekty hospodářské mobilizace.

Veřejné instituce a organizace zřízené veřejným sektorem mají význam pro správu území v dobách míru a větší v krizových situacích. Veřejný sektor řídí integrované záchranné systémy, odpovídá za politické a organizační zvládnutí krizových situací

Do veřejného sektoru patří kromě činnosti úřadů, policie a armády také provoz nemocnic, škol a školských zařízení, sociálních zařízení atd. V sociálních zařízeních se nachází většinou handicapovaní spoluobčané, děti a staří lidé. Přerušení zásobování elektřinou může být nejen nebezpečné (operační sály, nemocniční přístroje), ale může

způsobit u těchto občanů i větší paniku. Důležité je také zachování informační funkce veřejného rozhlasu a televize.

Největší hrozbou může být v krizové situace takové narušení energetického systému a informačního systému, které by spolupůsobily při vzniku co největší paniky a omezení akceschopnosti záchranných sborů i politických orgánů samosprávy a státní správy.

6 KRIZOVÉ SITUACE A MOŽNOST JEJICH VÝSKYTU V ČR

Elektrizační soustava je nejcitlivějším a nejzranitelnějším místem kritické infrastruktury. Může být poškozena, zničena nebo narušena úmyslnými teroristickými činy, přírodními pohromami, nedbalostí, nehodami nebo kyberterorismem, trestnou činností a chováním se zlým úmyslem. Elektrizační soustavu rozdělujeme do třech sektorů.

Tabulka 10: Sektory ES

	Sektor 1 Výroba el. energie	**Sektor 2 ČEPS**	**Sektor 3 Distribuce**
	ČEZ (62 011,5 GWh)	Transformátorovny	Vedení 110 kV
	Ostatní výrobci (22 349,4 GWh)	Vedení 400 kV	Vedení 22 kV
		Vedení 220 kV	Vedení 0,4 kV
			Transformátorovny
ČEZ	Plynné elektrárny = 33 713,7 GWh		
	Jaderné elektrárny = 26 046,5 GWh		
	Vodné elektrárny = 2 251,0 GWh		
Ostatní	Plynné elektárny = 18 681,7 GWh		
	Paroplynné a spalovací = 2 480,0 GWh		
	Větrné elektrárny = 49,2 GWh		
	jiné = 132,3 GWh		

ES je systém citlivý na správnou funkci a interakci prvků, které na sebe navazují a vzájemně se ovlivňují. Elektřinu nelze skladovat. Proto musí být udržována rovnováha mezi výrobou a spotřebou. ES jako celek musí kontinuálně zabezpečovat požadavky na zajištění velikosti spotřeby elektřiny, která se v čase mění[54].

Některé události mohou vzhledem k závažnosti, rozsahu území, které zasahují, a četnosti výskytu způsobit poškození nebo ztrátu funkce některého prvku nebo několika prvků ES a vést k haváriím regionálního nebo celostátního charakteru. Ze světa jsou známy události, jejichž důsledkem byl úplný výpadek dodávek elektřiny. Roku 2003 USA a Kanada, Dánsko a Švédsko, Itálie, roku 2004 Řecko. Havárie velkého rozsahu mohou přesáhnout reálné možnosti provozovatelů zajistit okamžité obnovení provozu nebo si mohou vyžádat odstavení systému, a způsobit tak krizovou situaci v zásobování odběratelů[54].

6.1 Příčiny a původci vzniku a trvání KS [54]

6.1.1 Výrobny elektřiny mohou být odstaveny z těchto příčin:

a) přímé poškození výrobního zařízení (z důvodu technické poruchy, vady materiálu, zanedbání údržby, živelní události, teroristického útoku, války),

b) chybná funkce řídicího systému,

c) nevhodný dispečerský zásah nebo manipulace (selhání lidského činitele),

d) rozpad elektrické sítě napájené výrobnou,

e) nedostatek paliva nebo jiných provozních hmot.

Každá výrobna má technologické uzly, jejichž vyřazení z provozu má za následek odstavení. Vyřazení ostatních technologických zařízení způsobí jen přechodné obtíže.

Nejvíce odolné proti účinkům pohrom (včetně teroristických útoků) jsou jaderné elektrárny. Větší poškození hlavního výrobního bloku však může elektrárnu odstavit z provozu na dlouhou dobu či trvale. Vyřazení jaderné elektrárny z provozu může být příčinou rozsáhlejších výpadků ES.

Elektrárny na různá fosilní paliva jsou z hlediska zranitelnosti technologie srovnatelné s jadernými elektrárnami. Důsledky jednotlivých druhů poškození mohou být velmi rozdílné. Poškození určitých uzlů výrobny spalující kapalná paliva může být spojeno s rozsáhlým požárem a ekologickou havárií, u výrobny spalující plyn může dojít k požáru nebo výbuchu, jejichž následkem může být úplná devastace výrobny. Relativně nejmenší poškození lze očekávat u výroben spalujících pevná paliva.

Vodní elektrárny, jsou při povodni vyřazeny z činnosti, neboť se změní výškový rozdíl hladin, který umožňuje výrobu elektřiny. Tyto elektrárny jsou také citlivé na zalití výrobních prostor vodou.

Všechny parní (uhelné i jaderné) elektrárny potřebují ke svému chlazení vodu, průtočnou do kondenzace nebo na doplnění odpařené vody do chladicích věží. Všechny elektrárny tohoto typu proto stojí blízko zdroje vody. Citlivost elektráren na dlouhodobé důsledky zatopení není velká, choulostivé jsou v této části motory a ovládací a ochranná zařízení.

Do úvah o možném ohrožení systému musí být zahrnuta i problematika paliva a velikosti jeho zásob. Z tohoto hlediska jsou nejméně zranitelné jaderné elektrárny a elektrárny vodní. Elektrárny na pevná a kapalná paliva udržují jen omezenou zásobu paliva. Přerušení přepravních tras může mít za následek odstavení výrobny. U výroben spalujících plyn znamená přerušení přepravní cesty okamžité odstavení zdroje.

Specifickou otázkou je opětovné uvedení odstaveného výrobního zařízení do provozu, především v případě, že k odstavení došlo v důsledku rozpadu elektroenergetického systému.

Přenosová soustava a distribuční soustavy mohou být odstaveny z těchto příčin:

a) přímé poškození určitého prvku vedení,

b) chybná funkce řídicího systému nebo automaticky působících ochran,

c) nevhodný dispečerský zásah

d) nerovnováha mezi poptávkou a nabídkou v systému, přesahující určitou mez.

Závažnější než vlastní poškození vedení přenosové soustavy a distribučních systémů je rozpad ES jako celku, tedy i odstavení výroben. Obnova provozu celého systému je složitá. Velmi zranitelným prvkem jsou rozvody vysokého a velmi vysokého napětí.

6.1.2 Přenosová soustava

Venkovní vedení nejsou ohrožena působením povodní, s výjimkou odplavení půdy v okolí základů podpěrných stožárů. K tomu došlo v roce 2002 na vedení u dálnice D8 u Veltrus. Důsledek takového poškození je plně kompenzován propojením systému vedení tak, aby výpadek kteréhokoliv vedení neznamenal přerušení chodu soustavy. Přenosová soustava je koncipována a realizována tak, aby nedošlo k jejímu rozpadu v případě vyřazení jednoho prvku soustavy z provozu a v některých případech i dvou prvků. Obtíže působí silný vítr, o rychlosti větší než 100 km/h, který může způsobit pád stožárů vedení

a dlouhodobé přerušení provozuschopnosti přenosového vedení. Podobné účinky mohou mít i sesuvy půdy, které jsou ale v trasách vedení přenosové soustavy málo pravděpodobné. Vážným rizikem je tvorba námrazy na vedení při kombinaci deště a nízkých teplot; jejím důsledkem je stržení lan pod tíhou ledu. Významně může venkovní vedení poškodit teroristický útok provedený v určitém místě určitým způsobem.

Rozvodny400 kV a 220 kV jsou zařízení ve venkovním provedení, takže jsou choulostivé na zatopení vodou a znečištění izolace. Rozvodny jsou málo odolné proti teroristickému útoku.

6.1.3 Distribuční soustavy

Distribuční soustavy jsou nejrozsáhlejší částí ES. Poškození jednoho prvku má zpravidla za následek přerušení dodávky v části soustavy. Trvání tohoto přerušení závisí na místě a rozsahu poškození zařízení.

Vedení jsou ve venkovním provedení, takže jsou poměrně snadno přístupná, a tedy snadno zranitelná. Významně zabezpečená nejsou ani kabelová vedení, protože jsou zaústěna do nadzemních objektů.

Nejcitlivějším a nejzranitelnějším místem kabelového vedení distribuční sítě jsou transformovny a četné propojovací skříně, které jsou umístěny na stěnách budov do výšky asi 1 m nad zemí.

6.1.4 Funkčnost dispečerského informačního a řídicího systému může narušit:

a) přímé poškození určitých prvků systému,

b) chybná funkce prvků systému (zkreslení dat, chybné vyhodnocení dat, nedostatek v softwarovém vybavení apod.),

c) selhání lidského činitele,

d) úmyslné přetížení systému.

Systém je tvořen soustavou propojení, k nimž patří telefonní spoje, radioreléové spoje, elektronické systémy pro přenos dat, automatiky aj. Jednotlivé spojové trasy jsou zálohovány. Poškození jednoho prvku nepředstavuje téměř žádné riziko. Vznik poruchy dispečerského řízení však vždy znamená prodloužení doby obnovení dodávky elektřiny. Kolaps celého řídicího systému by měl pro elektroenergetiku zásadní význam.

7 ANALÝZA RIZIK

Nejdůležitějším krokem ke snížení rizika je analýza rizik. Analýza rizik je proces, který stanovuje pravděpodobnost uskutečnění hrozeb a dopadu na aktiva. Jde o stanovení rizik a jejich závažnosti. Jakékoliv účinné řešení problému je založeno na kvalitní analýze rizik[51].

Analýza rizik zahrnuje čtyři důležité kroky:

a) identifikaci aktiv,
b) stanovení hodnoty aktiv,
c) identifikaci hrozeb a slabin,
d) stanovení závažnosti hrozeb a míry zranitelnosti.

Správné pochopení vztahů je pro správné provedení analýzy klíčové. Mechanismus uplatnění rizika probíhá způsobem, kdy hrozba využije zranitelnosti, překoná protiopatření a začne působit na aktivum, kde způsobí škodu. Aktivum motivuje útočníka k aktivaci hrozby. Aktivum se vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními. Protiopatření chrání aktiva, detekuje hrozby a zabraňuje jejich působení částečně či úplně. Samotná protiopatření zároveň odrazují od aktivování hrozby. Hrozba působí buď na aktivum nebo na protiopatření. Aby hrozba mohla působit, musí být aktivována, a k tomu jsou nezbytné zdroje[51].

Riziko většinou neexistuje izolovaně, ale jedná se o kombinaci několika rizik, které mohou představovat hrozbu. Je třeba určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměřit se na klíčové rizikové oblasti. V průběhu analýze rizika se provádí některé obecné činnosti[51].

a) Stanovení hranice analýzy rizik: ta odděluje aktiva, která budou zahrnuta do analýzy, od aktiv ostatních. Při stanovení hranice analýzy se vychází ze záměrů managementu. Aktiva, která mají vztah ke snižování rizik, budou zahrnuta do analýzy a budou ležet uvnitř hranice analýzy. Ostatní budou ležet mimo hranici.

b) Identifikace aktiv: spočívá ve vytvoření soupisu všech aktiv, ležící uvnitř hranice analýzy rizik.

c) Stanovení hodnoty a seskupování aktiv: Hodnota aktiva je založena na velikosti škody způsobené zničením či ztrátou aktiva. Důležité je rozlišit zda se jedná o jedinečné aktivum nebo aktivum jednoduše nahraditelné.

Do hodnoty se promítá závislost subjektu na existenci, ale i na správném fungování aktiva, tedy k jakým škodám dojde omezením funkčnosti nebo ztrátou aktiva, než se aktivum obnoví.

d) Identifikace hrozeb: Identifikují se hrozby, které připadají pro analýzu v úvahu. Provádí se tak, že se vybírají ty, které by mohly ohrozit alespoň jedno aktivum subjektu. K identifikaci hrozeb lze použít seznam hrozeb, sestavených podle literatury, vlastních zkušeností, průzkumů dříve provedených analýz.

e) Analýza hrozeb a zranitelností: Každá hrozba se hodnotí vůči jednotlivému aktivu. U aktiv, na které se může hrozba uplatnit se určí úroveň hrozby a úroveň zranitelnosti. Při stanovení hrozby se vychází z nebezpečnosti, motivace a přístupu. Při stanovení zranitelnosti se vychází z faktorů jako je citlivost a kritičnost. Při analýze hrozeb a zranitelností se berou v úvahu realizovaná protiopatření. Protiopatření mohou snížit úroveň hrozby i úroveň zranitelnosti. Výsledným stavem je seznam dvojic hrozba-aktivum se stanovenou úrovní hrozby a zranitelnosti.

f) Pravděpodobnost jevu: K popisu určitého jevu doplňujeme údaj, s jakou pravděpodobností může jev nastat.

g) Měření rizika: Výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva.

7.1 Analýza rizik v kritické infrastruktuře

Analýza má za úkol identifikovat pravděpodobnost nějaké mimořádné události. Identifikovat možné dopady a škody. Je mnoho metodik k provádění analýzy rizik jak v oblasti bezpečnosti informačních technologií, tak i v oblastech jiných. Výsledkem metod je očekávaná výše škody nebo kategorizace rizika. Analýza rizik v kritické infrastruktuře je poněkud problematická. Bylo zjištěno, že aplikace klasických metod analýzy rizik nevede k žádoucímu cíli. Důvodem jsou nedostatečně silné vypovídací statistiky pro výpadky infrastruktur. Pro analýzu rizik v kritické infrastruktuře byla vytvořena metoda na bázi posouzení kritičnosti.[17]

Výchozím bodem analýzy jsou provozní procesy, které probíhají. V zájmu nejí prioritně kým anebo čím jsou funkční schopnosti procesů ohroženy, ale pouze to zda může

být proces narušen nebo končit výpadkem. V této analýze se musí podkládat otázka „Jaké dopady bude mít v příslušném procesu to, že něco nebude fungovat.“[17]

V analýze rizik u kritické infrastruktury se setkáváme s pojmem kritičnost. Kritičnost je vyjádřena odstupňovaným hodnocením. Jedná se o vykazování nízké či vysoké kritičnosti. U kritičnosti se vyhodnocuje pravděpodobnost a očekávaný dopad poruchy. K posouzení výpadku určitého celého procesu je třeba zvláštního posouzení. Může dojít k bezvýznamnému výpadku, či výpadek může být katastrofální.

7.1.1 Metoda AKIS

Nástrojem k získání rychlého hodnocení jednotlivých sektorů infrastruktury je metoda AKIS. Vytvoří se přehled o jednotlivých sektorech infrastruktury, které se dále rozčlení. Identifikují se kritické procesy a zhodnotí se kritičnost. Jednotlivé body s vysokou kritičností se dále posuzují na závislost na informačních technologiích. Po ukončení vznikne matice kritičnosti.

V prvním korku je nutné posuzovaný sektor zobrazit ujasnit, jak sektor funguje, jak pracuje a jaký má význam pro ekonomiku, jaké vůdčí podniky v sektoru jsou. Sektory můžeme dále rozdělit na jednotlivá odvětví či služby. Pro jednotlivá odvětví či služby je nutné identifikovat provozní procesy. Posuzují se ty procesy, které mají z hlediska kritičnosti význam. K identifikaci procesů jsou k dispozici různé pomůcky. Pokud se jedná o sektor s vysokým národohospodářským významem, je vhodné pracovat v součinnosti s experty. Důležitým předpokladem úspěšné analýzy kritičnosti je věrohodné zacházení s obdrženými informacemi.

V hodnocení kritičnosti je nejpodstatnější práce s odborníky. Pokud je to možné, dotazuje se více odborníků, může se tak zhodnotit různá subjektivní hodnocení. Aby mohlo být hodnocení srovnatelné je nutná existence možnosti výsledky analyzovat a srovnávat mezi jednotlivými sektory. Je sestavována několika stupňová škála. Např. pro pravděpodobnost výpadku od „velmi řídký“ do „téměř jistý“. Následně kombinujeme dopad a pravděpodobnost výpadku což představuje kritičnost procesu. Podle hodnocení kritičnosti a provedení hodnocení výsledků anket experty můžeme jednotlivé procesy uspořádat do matice kritičnosti.[17]

Na základě této metody nejsou výsledky dostatečně detailní, aby sloužily jako základ ke konkrétním opatřením. Metoda AKIS umožňuje získat rychlý přehled o kritické

infrastruktuře a vytvořit tím dobré znalosti, které napomůžou k zachování spolehlivosti infrastruktury na bázi spolupráce mezi státem a hospodářstvím.[17]

7.2 Výsledky metody AKIS

Tabulka 11: Rozdělení sektorů Elektrizační soustavy metodou AKIS

Elektrizační soustava

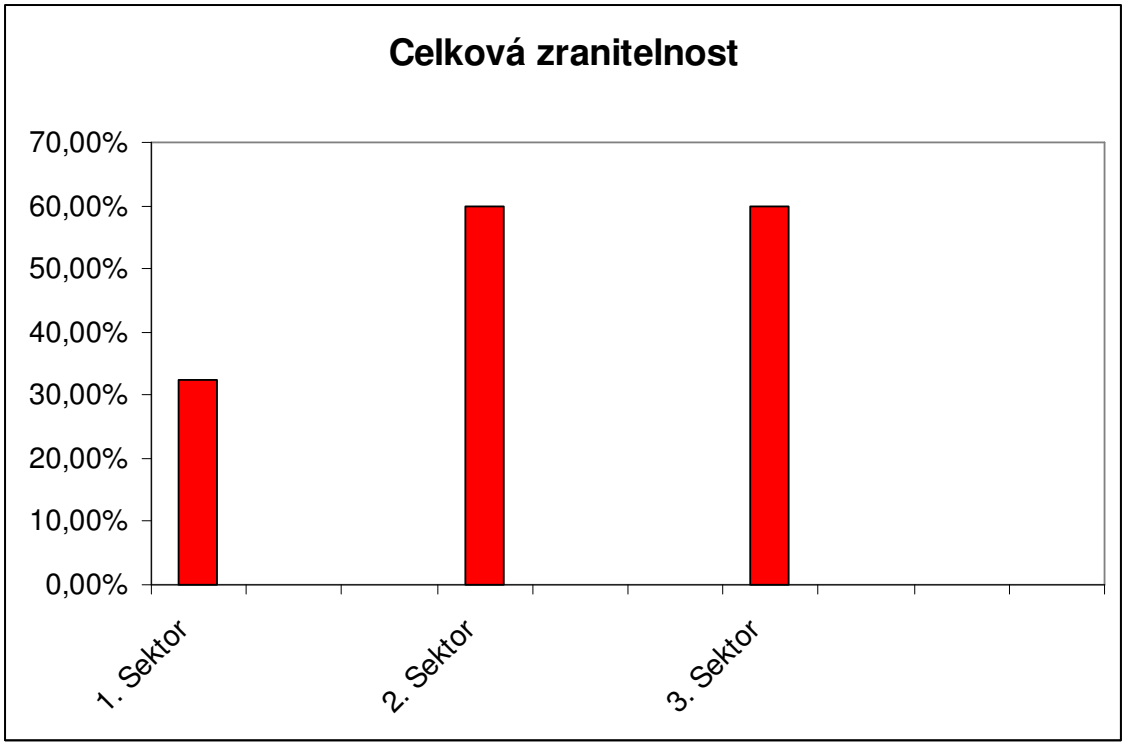
	Sektor 1 Výroba el. energie	**Sektor 2 ČEPS**	**Sektor 3 Distribuce**
	ČEZ (62 011,5 GWh)	Transformátorovny	Vedení 110 kV
	Ostatní výrobci (22 349,4 GWh)	Vedení 400 kV	Vedení 22 kV
		Vedení 220 kV	Vedení 0,4 kV
			Transformátorovny
ČEZ	Plynné elektrárny = 33 713,7 GWh		
	Jaderné elektrárny = 26 046,5 GWh		
	Vodné elektrárny = 2 251,0 GWh		
Ostatní	Plynné elektárny = 18 681,7 GWh		
	Paroplynné a spalovací = 2 480,0 GWh		
	Větrné elektrárny = 49,2 GWh		
	jiné = 132,3 GWh		

Tabulka 12: Dotazník 1

DOTAZNÍK OHROŽENÍ ELEKTRIZAČNÍ SOUSTAVY										
Jméno:	**Ing.**	**Josef**	**Šarapatka**			Datum:			27.3.2009	
Firma:	**ČEZ, a.s.**									
	1. Sektor			**2. Sektor**			**3. Sektor**			
	Elektrárna			Vedení 400 kV	Vedení 220 kV	Transformátorovny přenosové soustavy	Vedení 110 kV	Vedení 220 kV	Vedení 0,4 kV	Transformátorovny distribuční soustavy
	Jaderná	Uhelná	Vodní							
Zranitelnost	0	50	15	60	60	60	60	60	60	60
Riziko poškození člověkem KOORDINOVANĚ	max 5	50	15	60	60	60	60	60	60	60
Riziko poškození člověkem JEDNORÁZOVĚ	0	25	5	60	60	60	60	60	60	60
Riziko poškození člověkem ÚMYSLNĚ	0	25	5	60	60	60	60	60	60	60
Riziko poškození člověkem NEDBALOSTNĚ	0	10	0	15	15	15	15	15	15	15
Bezpečnostní opatření provozovatele	100	80	80	40	40	40	40	40	40	40
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ES	30	30	30	15	15	15	15	15	15	15

Tabulka 13: Celková zranitelnost Dotazníku 1

CELKOVÁ ZRANITELNOST				
			v %	
1. Sektor	Elektrárna	Jaderná	0	**32,50%**
		Uhelná	50	
		Vodní	15	
2. Sektor	Vedení 400 kV		60	**60%**
	Vedení 220 kV		60	
	Transformátorovny		60	
3. Sektor	Vedení 110 kV		60	**60%**
	Vedení 22 kV		60	
	Vedení 0,4 kV		60	
	Transformátorovny		60	



Tabulka 14: Celkové riziko poškození Dotazníku 1

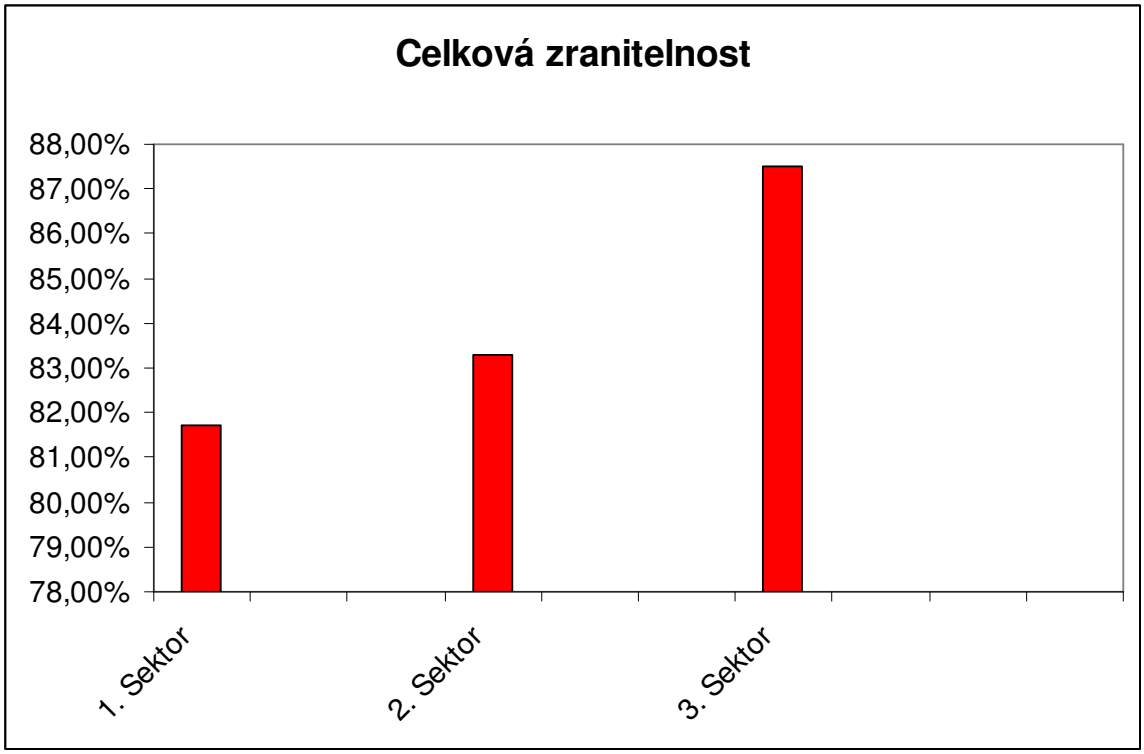
CELKOVÉ RIZIKO POŠKOZENÍ				
			v %	
1. Sektor	Elektrárna	Jaderná	5	**13,70%**
		Uhelná	28	
		Vodní	8	
2. Sektor	Vedení 400 kV		49	**49%**
	Vedení 220 kV		49	
	Transformátorovny		49	
3. Sektor	Vedení 110 kV		49	**49%**
	Vedení 22 kV		49	
	Vedení 0,4 kV		49	
	Transformátorovny		49	

Tabulka 15: Dotazník 2

DOTAZNÍK OHROŽENÍ ELEKTRIZAČNÍ SOUSTAVY										
Jméno:			**Bílek**			Datum:			5.4.2009	
Firma:	**ČEPS, a.s.**									
	1. Sektor			**2. Sektor**			**3. Sektor**			
	Elektrárna			Vedení 400 kV	Vedení 220 kV	Transformátorovny přenosové soustavy	Vedení 110 kV	Vedení 220 kV	Vedení 0,4 kV	Transformátorovny distribuční soustavy
	Jaderná	Uhelná	Vodní							
Zranitelnost	95	60	90	90	90	70	90	90	90	80
Riziko poškození člověkem KOORDINOVANĚ	95	60	85	90	90	90	90	90	90	80
Riziko poškození člověkem JEDNORÁZOVĚ	50	40	40	30	30	40	40	40	40	35
Riziko poškození člověkem ÚMYSLNĚ	50	60	85	40	40	50	40	40	40	45
Riziko poškození člověkem NEDBALOSTNĚ	50	45	40	20	20	35	20	20	20	30
Bezpečnostní opatření provozovatele	100	45	30	30	30	95	25	25	20	45
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ES	100	25	60	50	50	60	90	80	70	80

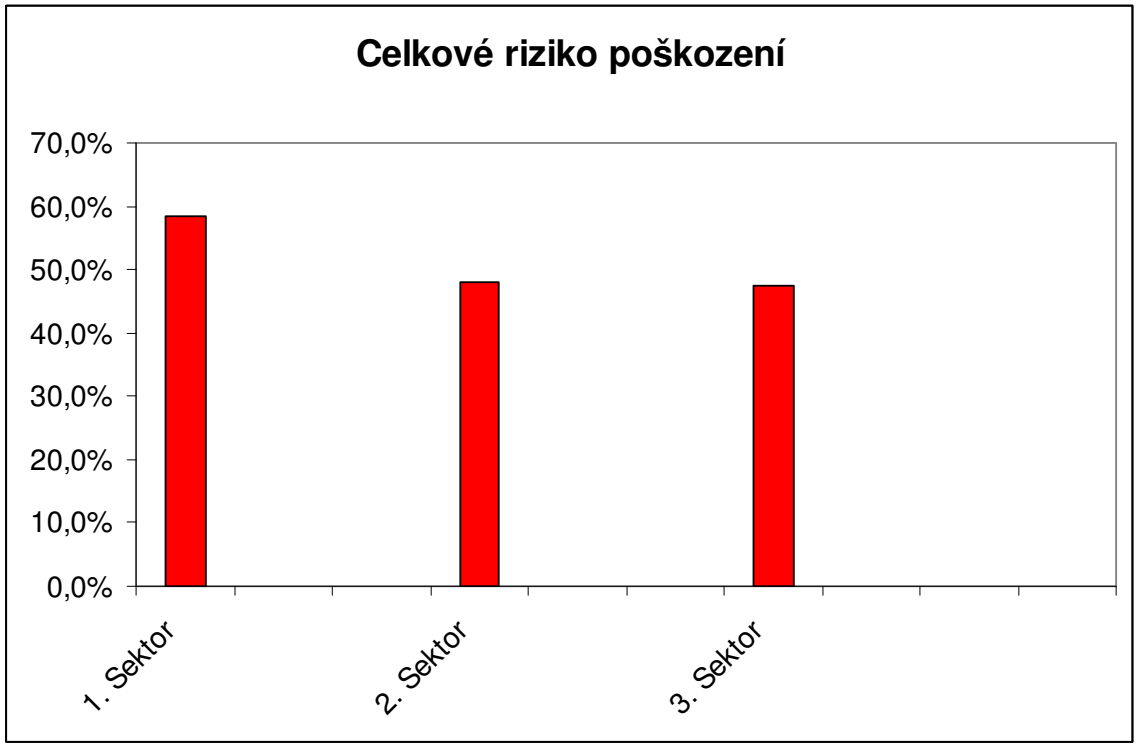
Tabulka 16: Celková zranitelnost Dotazníku 2

CELKOVÁ ZRANITELNOST				
			v %	
1. Sektor	Elektrárna	Jaderná	95	**81,70%**
		Uhelná	60	
		Vodní	90	
2. Sektor	Vedení 400 kV		90	**83%**
	Vedení 220 kV		90	
	Transformátorovny		70	
3. Sektor	Vedení 110 kV		90	**88%**
	Vedení 22 kV		90	
	Vedení 0,4 kV		90	
	Transformátorovny		80	



Tabulka 17: Celkové riziko poškození Dotazníku 2

CELKOVÉ RIZIKO POŠKOZENÍ				
			v %	
1. Sektor	Elektrárna	Jaderná	61	**58,3%**
		Uhelná	51	
		Vodní	63	
2. Sektor	Vedení 400 kV		45	**47,9%**
	Vedení 220 kV		45	
	Transformátorovny		54	
3. Sektor	Vedení 110 kV		48	**47,5%**
	Vedení 22 kV		48	
	Vedení 0,4 kV		48	
	Transformátorovny		48	



Tabulka 18: Dotazník 3

DOTAZNÍK OHROŽENÍ ELEKTRIZAČNÍ SOUSTAVY										
Určeno a poskytnuto pro účely Diplomové práce Bc. Lenky Brehovské										
Jméno:		**Zdeněk**	**Bauer**			Datum:			7.4.2009	
Firma:	**E.ON Distribuce, a.s.**									
	1. Sektor			**2. Sektor**			**3. Sektor**			
	Elektrárna			Vedení 400 kV	Vedení 220 kV	Transformátorovny přenosové soustavy	Vedení 110 kV	Vedení 220 kV	Vedení 0,4 kV	Transformátorovny distribuční soustavy
	Jaderná	Uhelná	Vodní							
Zranitelnost							50	60	70	50
Riziko poškození člověkem KOORDINOVANĚ							50	60	70	50
Riziko poškození člověkem JEDNORÁZOVĚ							30	40	50	30
Riziko poškození člověkem ÚMYSLNĚ							40	60	70	40
Riziko poškození člověkem NEDBALOSTNĚ							20	40	50	20
Bezpečnostní opatření provozovatele							provoz monitorovaný ochranami vedení	provoz monitorovaný ochranami vedení		vstupy do objektů dálkově monitorované
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ES							50	30	15	60

Tabulka 19: Celková zranitelnost Dotazníku 3

CELKOVÁ ZRANITELNOST				
			v %	
1. Sektor	Elektrárna	Jaderná	x	
		Uhelná	x	
		Vodní	x	
2. Sektor	Vedení 400 kV		x	
	Vedení 220 kV		x	
	Transformátorovny		x	
3. Sektor	Vedení 110 kV		50	**57,5%**
	Vedení 22 kV		60	
	Vedení 0,4 kV		70	
	Transformátorovny		50	

Tabulka 20: Celkové riziko poškození Dotazníku 3

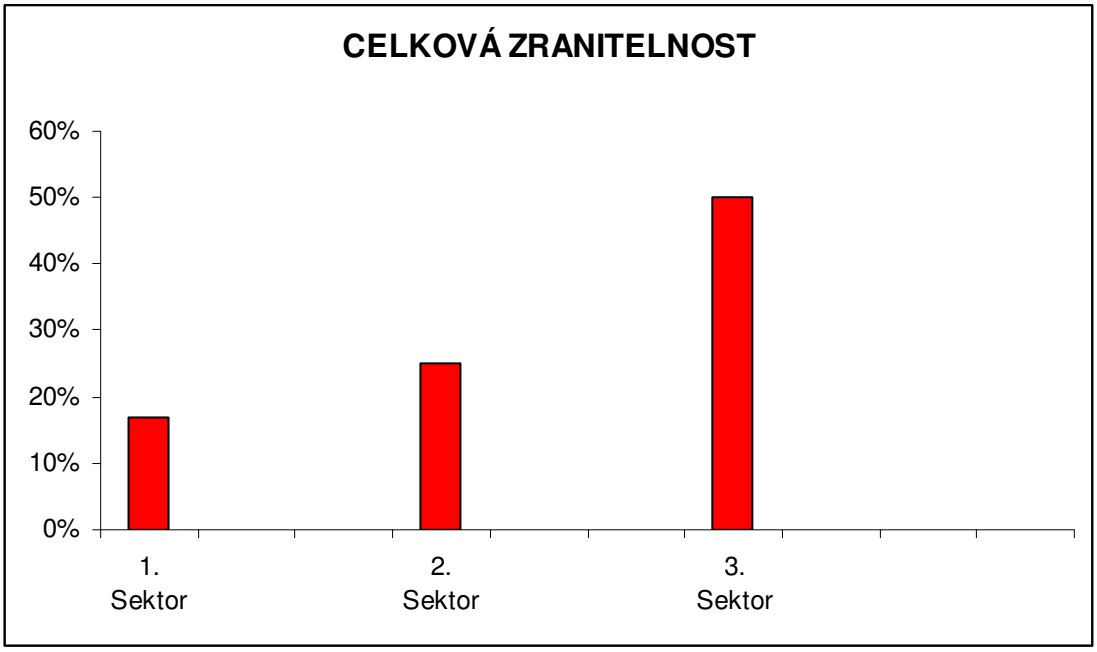
CELKOVÉ RIZIKO POŠKOZENÍ				
			v %	
1. Sektor	Elektrárna	Jaderná	x	
		Uhelná	x	
		Vodní	x	
2. Sektor	Vedení 400 kV		x	
	Vedení 220 kV		x	
	Transformátorovny		x	
3. Sektor	Vedení 110 kV		35	**45,0%**
	Vedení 22 kV		50	
	Vedení 0,4 kV		60	
	Transformátorovny		35	

Tabulka 21: Dotazník 4

DOTAZNÍK OHROŽENÍ ELEKTRIZAČNÍ SOUSTAVY										
Jméno:		**Radovan**	**Kožíšek**			Datum:			14.4.2009	
Firma:	**E.ON ČR**									
	1. Sektor			**2. Sektor**			**3. Sektor**			
	Elektrárna			Vedení 400 kV	Vedení 220 kV	Transformátorovny přenosové soustavy	Vedení 110 kV	Vedení 220 kV	Vedení 0,4 kV	Transformátorovny distribuční soustavy
	Jaderná	Uhelná	Vodní							
Zranitelnost	1	25	25	25	35	25	50	50	75	25
Riziko poškození člověkem KOORDINOVANĚ	25	10	10	5	5	5	5	5	5	5
Riziko poškození člověkem JEDNORÁZOVĚ	1	1	1	5	5	5	10	50	75	50
Riziko poškození člověkem ÚMYSLNĚ	20	10	10	5	5	5	5	5	5	5
Riziko poškození člověkem NEDBALOSTNĚ	1	1	1	5	5	5	10	50	75	50
Bezpečnostní opatření provozovatele	100	50	35	50	50	50	50	35	10	50
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ES	100	25	10	100	75	100	35	10	5	35

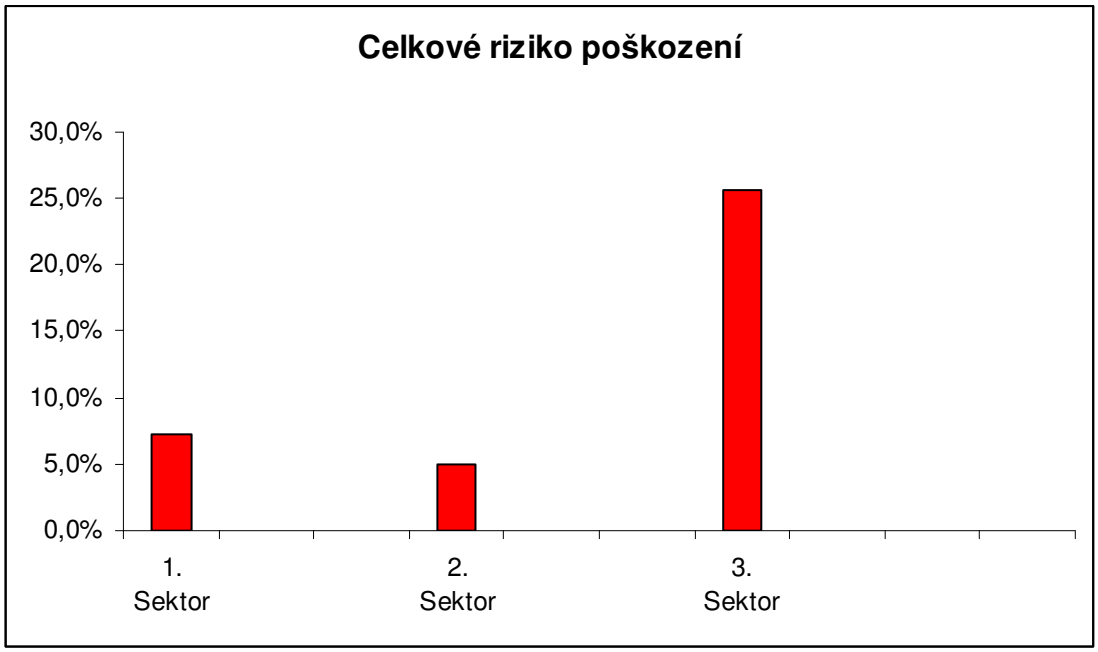
Tabulka 22: Celková zranitelnost Dotazníku 4

CELKOVÁ ZRANITELNOST				
			v %	
1. Sektor	Elektrárna	Jaderná	1	**17%**
		Uhelná	25	
		Vodní	25	
2. Sektor	Vedení 400 kV		25	**25%**
	Vedení 220 kV		35	
	Transformátorovny		25	
3. Sektor	Vedení 110 kV		50	**50%**
	Vedení 22 kV		50	
	Vedení 0,4 kV		75	
	Transformátorovny		25	



Tabulka 23: Celkové riziko poškození Dotazníku 4

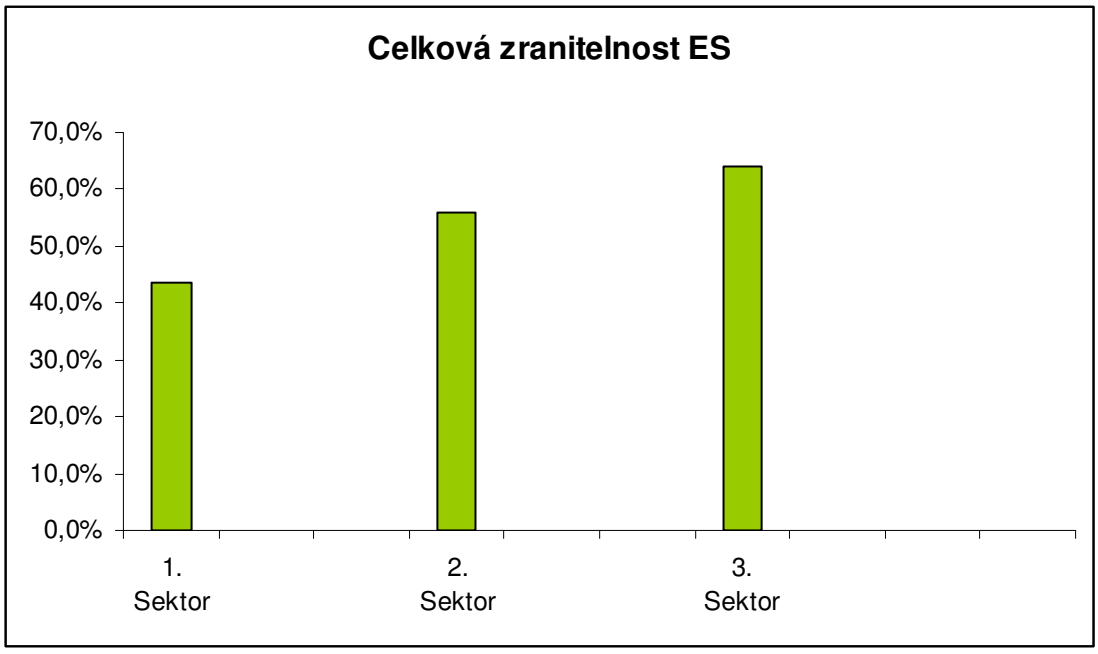
CELKOVÉ RIZIKO POŠKOZENÍ				
			v %	
1. Sektor	Elektrárna	Jaderná	10,5	**7,2%**
		Uhelná	5,5	
		Vodní	5,5	
2. Sektor	Vedení 400 kV		5	**5%**
	Vedení 220 kV		5	
	Transformátorovny		5	
3. Sektor	Vedení 110 kV		7,5	**25,6%**
	Vedení 22 kV		27,5	
	Vedení 0,4 kV		40	
	Transformátorovny		27,5	



7.3 Výsledky

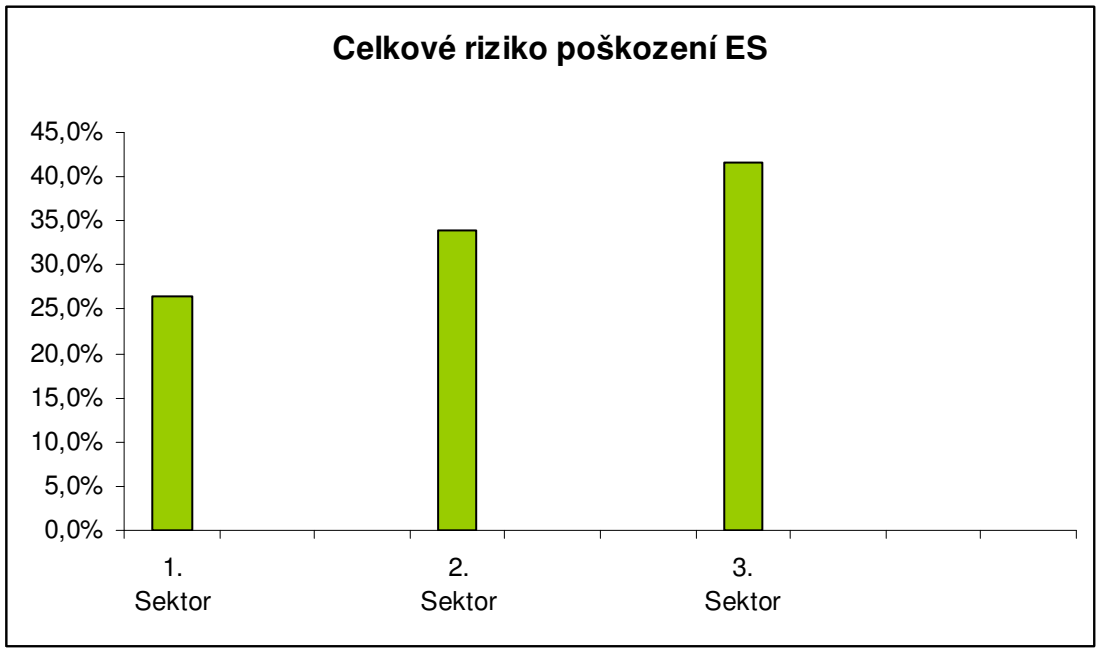
Tabulka 24: Celková zranitelnost ES

CELKOVÁ ZRANITELNOST ES							
			1. Dotazník	2. Dotazník	3. Dotazník	4. Dotazník	**Výsledky**
1. Sektor	Elektrárna	Jaderná	32,5%	81,7%	x	17,0%	43,7%
		Uhelná					
		Vodní					
2. Sektor	Vedení 400 kV		60,0%	83,0%	x	25,0%	56,0%
	Vedení 220 kV						
	Transformátorovny						
3. Sektor	Vedení 110 kV		60,0%	88,0%	57,5%	50,0%	63,9%
	Vedení 22 kV						
	Vedení 0,4 kV						
	Transformátorovny						



Tabulka 25: Celkové riziko poškození ES

CELKOVÉ RIZIKO POŠKOZENÍ ES							
			1. Dotazník	2. Dotazník	3. Dotazník	4. Dotazník	**Výsledky**
1. Sektor	Elektrárna	Jaderná	13,7%	58,3%	x	7,2%	26,4%
		Uhelná					
		Vodní					
2. Sektor	Vedení 400 kV		49,0%	47,9%	x	5,0%	33,9%
	Vedení 220 kV						
	Transformátorovny						
3. Sektor	Vedení 110 kV		49,0%	47,5%	45,0%	25,60%	41,6%
	Vedení 22 kV						
	Vedení 0,4 kV						
	Transformátorovny						



K vyplnění dotazníků byli osloveni odborníci ze všech tří sektorů. V prvním sektoru byli osloveni lidé z elektrárny Temelín (jako zástupce jaderné elektrárny), teplárna Strakonice (jako nezávislý dodavatel elektrické energie), skupina ČEZ a vodní dílo Lipno I. Z druhého sektoru byl osloven bezpečnostní ředitel ze společnosti ČEPS, a.s. Ze třetího sektoru byli osloveni odborníci z E.ON ČR a E.ON Distribuce.

K posuzování možného napadení elektrizační soustavy byla zvolena kritéria: zranitelnost, riziko poškození a bezpečnostní opatření provozovatele. Pro vyplnění dotazníků bylo zvoleno hodnocení od 0-100%. Kde 100 je pro maximum.

7.3.1 Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Z výsledků vyplývá vzrůstající zranitelnost od sektoru 3 po sektor 1. Je to dáno vzrůstajícími bezpečnostními opatřeními od odběratelů elektrické energie, kteří jsou nejméně chránění po samotné elektrárny, které mají vysoká zabezpečovací opatření. Distribuční soustava je na rozdíl od přenosové hustěji rozvětvena. Možnost přerušení dodávek je více reálná. A však zasažená oblast při poškození distribuční soustavy nebude natolik rozsáhlá jako při zasažení přenosové soustavy.

7.3.2 Riziko poškození

Hodnotícími body bylo poškození elektrizační soustavy člověkem koordinovaně, jednorázově, úmyslně a nedbalostně.

Tabulka 26: Riziko poškození člověkem

Riziko poškození člověkem					
		Koordinovaně	Jednorázově	Úmyslně	Nedbalostně
1. Sektor	Jaderná	41,7%	25,5%	35,0%	25,5%
	Uhelná	40,0%	22,0%	31,7%	18,7%
	Vodní	36,7%	15,3%	33,3%	20,5%
2. Sektor	Vedení 400 kV	51,7%	31,7%	35,0%	13,3%
	Vedení 220 kV	51,7%	31,7%	35,0%	13,3%
	Transformátorovny	51,7%	35,0%	35,0%	18,3%
3. Sektor	Vedení 110 kV	51,3%	35,0%	36,3%	16,3%
	Vedení 22 kV	53,8%	47,5%	41,3%	31,3%
	Vedení 0,4 kV	56,3%	56,3%	43,8%	40,0%
	Transformátorovny	49,0%	43,8%	37,5%	28,8%

Nejcitlivějším prvkem ES na poškození je vedení 0,4 kV. Výsledek vyplývá ze zranitelnosti. Vedení 0,4 kV je nejnižším prvkem v celé ES a nejméně chráněný. Vedení směřuje již ke koncovým odběratelům a narušení tohoto vedení má za následek jen minimální výpadek proudu, který se dá snadno nahradit.

Z výsledků vyplývá jako jeden z nejcitlivějších bodů ES transformátorovny přenosové soustavy. Tyto transformátorovny jsou nenahraditelnou součástí přenosu elektrické energie. Jsou to prvky, které jsou „vyráběny na míru“ a neexistuje náhrada. Jakékoliv narušení transformátorovny má za následek výpadek přenosu proudu a je nutná okamžitá oprava. Přenosová soustava pracuje v provozu n-1. Výpadek jednoho transformátoru by soustava zvládla. Výpadek dvou a více je pro přenos energie katastrofální a ES se hroutí na ostrovní provozy. Náhrada transformátoru trvá měsíce a je velice nákladná. Napadením tohoto prvku by teroristé dosáhli největších výsledků. Transformátorovny přenosové soustavy by měly být nejvíce chráněny ze sektorů 2 a 3.

8 OCHRANA KRITICKÉ INRASTRUKTURY

Ochrana kritické infrastruktury se stala po útocích ze dne 11. března 2004 v Madridu a 7. července 2005 jednou z hlavních priorit státu Evropské unie. Ukázalo se, že hrozba teroristických útoků na evropskou infrastrukturu, je více než reálná. Evropská rada na zasedání v červnu 2004 požádala Komisi o přípravu celkové strategie na ochranu kritické infrastruktury. Na základě toho bylo 20. října 2004 přijato sdělení „Ochrana kritické infrastruktury v boji proti terorismu“. Jsou zde stanoveny návrhy, jak by se měla zlepšit prevence, připravenost a schopnost reakce na teroristické útoky zasahující EU. Na zasedání Rady EU v prosinci 2004 bylo podpořeno záměr Komise předložit Evropský program na ochranu kritické infrastruktury (EPCIP) a byla zřízena Výstražná informační síť kritické infrastruktury (CIWIN).

8.1 Sdělení komise radě a evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu [55]

V Bruselu dne 20. října 2004 bylo přijato sdělení komise radě a evropskému parlamentu. Toto sdělení obsahuje přehled opatření, která komise provádí a navrhuje další opaření pro posílení stávajících nástrojů a splnění úloh.

Kritické infrastruktury musejí být vymezeny na úrovni členských států a na evropské úrovni. Kritické infrastruktury jsou vysoce propojeny a navzájem vysoce závislé. Díky vzájemnému propojení může docházet k řetězovému hromadění problémů, které mohou způsobovat neočekávané a vážnější selhávání nezbytných služeb. Pro určení kritické infrastruktury lze použít tři faktory:

a) **Rozsah** – ztráta prvku kritické infrastruktury se hodnotí podle velikosti zeměpisné oblasti, která by mohla být jeho ztrátou nebo nedostupností postižena.

b) **Závažnost** – stupeň dopadu nebo ztráty může být hodnocen jako žádný, minimální, mírný nebo velký.

c) **Vliv času** – kdy by mohla mít ztráta prvku vážný dopad

Ne všechny infrastruktury je možné chránit před všemi hrozbami. Některé infrastruktury jako např. elektrizační soustava jsou natolik rozsáhlé a plošné, že je není možno kontinuálně hlídat. Ochrana infrastruktur vyžaduje kooperativní partnerství mezi vlastníky a provozovateli kritických infrastruktur a orgány členských států. Odpovědnost za řízení rizika spočívá zejména na vlastnících a provozovatelích.

8.2 Zelená kniha

Dne 17. listopadu 2005 přijala Komise Zelenou knihu o Evropském programu na ochranu kritické infrastruktury, která stanovila politické možnosti. Odpovědi získané ze Zelené knihy zdůraznily přidanou hodnotu rámce Společenství týkající ho se ochrany kritické infrastruktury. Byla zde uznána potřeba zvýšit schopnost ochrany kritické infrastruktury v Evropě a pomoci snížit zranitelnost kritických infrastruktur. Byla zdůrazněna důležitost klíčových zásad subsidiarity, proporcionaliy a komplementarity[56].

8.3 EPCIP

Cílem EPCIP je zajistit, aby v rámci celé Evropské unie existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření. Úroveň ochrany by neměla být stejná pro všechny kritické infrastruktury, ale měla by být odvozená od dopadu, jenž by mohl způsobit jejich možné selhání [56].

EPCIP má co nejvíce minimalizovat veškeré negativní dopady, které zvýšené investice na ochranu mohou mít na konkurenceschopnost příslušného odvětví. Při výpočtu přiměřenosti nákladů nesmíme opomíjet potřebu udržovat stabilitu trhů, která je rozhodující zejména u dlouhodobého investování, ani vliv, jenž taková ochrana má na vývoj akciových trhů a na makroekonomické prostředí[56].

8.3.1 EPCIP by měl chránit před [56]

a) **veškerá ohrožení** – komplexní přístup, který počítá jak s hrozbami úmyslných útoků, tak přírodních pohrom.

b) **veškerá ohrožení, ale se zaměřením na terorismus** – pružný přístup, který by zajistil návaznost na další druhy ohrožení, jako je hrozba úmyslných útoků či přírodních pohrom, ale s prioritním zaměřením na terorismus.

c) **zaměřený na terorismus** – přístup orientovaný na terorismus, bez jakékoliv zvláštní pozornosti vůči běžnějším ohrožením.

8.3.2 Základní principy EPCIP[56]

a) **Subsidiarita** – základem EPCIP by měl být princip subsidiarity, kdy ochrana kritické infrastruktury je v odpovědnosti subjektů především na národní úrovni. Hlavní odpovědnost za ochranu kritické infrastruktury by spadala pod členské státy a vlastníky/provozovatele jednající ve společném rámci. Komise by se naopak zaměřila na aspekty spojené s ochranou kritických infrastruktur s přeshraničním dosahem v rámci EU. Odpovědnost za rozhodnutí a plány na ochranu vlastního majetku by měla zůstat na vlastnících a provozovatelích.

b) **Doplňkovost –** společný rámec EPCIP by doplňoval již existující opatření. Zavedené komunitární mechanizmy by měly být nadále využívány, aby přispívaly k zajištění celkové implementace EPCIP.

c) **Důvěrnost** – sdílení informací o ochraně kritické infrastruktury by zůstalo zachováno v důvěrném prostředí. To je nezbytné zejména proto, že konkrétní údaje o kritické infrastruktuře by mohly být zneužity a způsobit tak její selhání nebo jiné nepřijatelné důsledky. Informace o ochraně kritické infrastruktury by byly jak na úrovni EU, tak na úrovni členských států utajovány a přístup k nim by byl povolen jen v potřebných případech.

d) **Spolupráce zainteresovaných subjektů –** svou roli při ochraně kritické infrastruktury mají všechny zainteresované subjekty včetně členských států, Komise, průmyslových/obchodních sdružení, normalizačních orgánů, vlastníků, provozovatelů a uživatelů („uživatel“ je definován jako organizace užívající danou infrastrukturu pro obchodní účely a pro poskytování služeb). Všichni by měli v rámci své odpovědnosti a specifické úlohy spolupracovat a přispívat tak k rozvoji a implementaci EPCIP. Vůdčí a koordinační úlohu při rozvoji a implementaci

přístupu při ochraně kritické infrastruktury v rámci daného území, by měly orgány členských států. Takový přístup by měl být vždy konzistentní v celostátním měřítku. Vlastníci, provozovatelé a uživatelé by byli aktivně zapojeni jak na národní úrovni, tak na úrovni EU. Tam, kde neexistují odvětvové normy nebo ještě nebyly zavedeny normy mezinárodní, mohou normalizační orgány přijmout vhodné společné normy.

e) **Proporcionalita** – vzhledem k tomu, že by nebylo opodstatněné chránit veškerou infrastrukturu před všemi hrozbami (např. rozvodné sítě elektrické energie jsou příliš rozsáhlé na to, aby je bylo možné oplotit nebo hlídat), měly by být ochranné strategie a opatření úměrné úrovni daného nebezpečí. S pomocí vhodných technik řízení rizik lze soustředit pozornost na nejrizikovější oblasti, přičemž je nutno brát v úvahu danou hrozbu, její relativní význam pro infrastrukturu, poměr nákladů a výnosů, stávající úroveň bezpečnostní ochrany a účinnost dostupných zmírňujících strategií.

8.3.3 Společný rámec EPCIP

Jakékoliv poškození jedné infrastruktury v jednom členském státě může negativně ovlivnit ostatní státy a evropskou ekonomiku jako celek. K takovým případům může docházet častěji nové technologie a liberalizace trhu způsobují, že mnoho infrastruktur je součástí širší sítě. Ochranná opatření budou silná pouze tak, jak v jejich nejslabším článku. Společná úroveň ochrany je nezbytná. Účinná ochrana vyžaduje komunikaci, koordinaci a spolupráci na národní, evropské i mezinárodní úrovni mezi všemi zainteresovanými subjekty. Na úrovni EU by mohl být zaveden společný rámec na ochranu kritické infrastruktury, který by zajistil, že každý členský stát bude poskytovat přiměřenou a stejnou úroveň ochrany týkající se vlastní kritické infrastruktury[57].

Společný rámec EPCIP by obsahoval opatření definující pravomoci a odpovědnosti všech subjektů podílejících se na ochraně kritické infrastruktury. Společný rámec by měl doplnit existující opatření na úrovni Společenství a členských států, tak aby poskytoval maximální možnou úroveň bezpečnosti kritické infrastruktury v EU.

Navrhuje se, aby posílení kritické infrastruktury bylo dosaženo zavedením společného rámce EPCIP, který by umožňoval výměnu nejlepších postupů a kontrolních mechanismů. Některé z prvků, které by měly být součástí společného rámce[56]:

a) společné principy CIP;

b) společně dohodnuté kódy/standardy;

c) obecné definice, na základě kterých mohou být vytvořeny odvětvově specifické definice

d) společný seznam odvětví s kritickou infrastrukturou

e) prioritní oblasti CIP;

f) popis odpovědností zúčastněných subjektů;

g) dohodnuté referenční ukazatele;

h) metody pro srovnávání a stanovení prioritních infrastruktur u jednotlivých odvětví.

8.4 Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

Tato směrnice představuje první etapu přístupu, jehož cílem je určit a označit EKI a posoudit potřebu zvýšit jejich ochranu. Směrnice se soustředí na energetiku a dopravu. Doplňuje stávající odvětvová opatření na úrovni Společenství a členských států. U všech označených EKI by měli být zavedeny plány bezpečnosti provozovatele nebo rovnocenná opatření zahrnující určení důležitých prostředků, posouzení rizik a určení, výběr a stanovení priorit protiopatření a postupů. Pro každou EKI by měl být jmenován styčný bezpečnostní úředník s cílem usnadnit spolupráci a komunikaci s vnitrostátními orgány příslušnými pro ochranu kritické infrastruktury[58].

9 TERORISMUS A ELEKTRIZAČNÍ SOUSTAVA

Mnoho teroristických organizací nepovažuje za hlavní terč svých akcí energetické zásobovací řetězce. Nepovažují je však ani za něco zcela zbytečného. Existují četné případy útoků na ropovody a plynovody, elektrické transformátory a stožáry. Takovéto útoky jsou však součástí řady útoků zaměřené na několik různých cílů[59].

Přibližně asi 4% všech teroristických útoků zaznamenaných od roku 2004 jsou namířené na energetickou infrastrukturu (uvedené číslo vychází z databáze WITS kde z 35 707 všech útoků bylo jen 1 597 útoků provedeno na energetický sektor)[59].

V letech 1999 – 2008 bylo nejvíce útoku na elektrizační soustavu provedeno

a) výbušným systémem a žhářskými útoky na transformační stanice

b) výbušným zařízením vedeným na elektrárnu a rozvodnou stanici

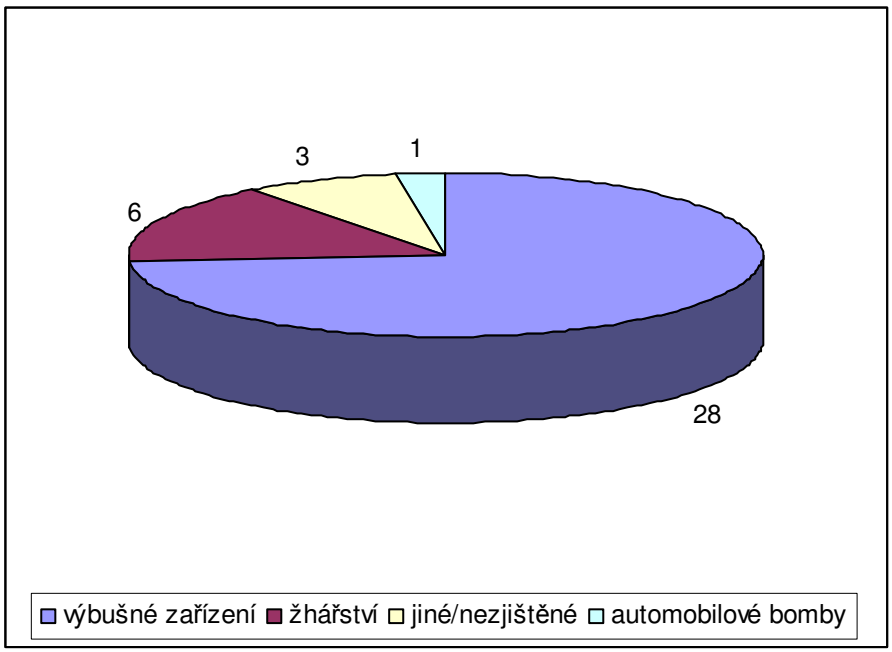
c) žhářským útokem na elektrárnu

d) výbušným zařízením na stožáry elektrického vedení.

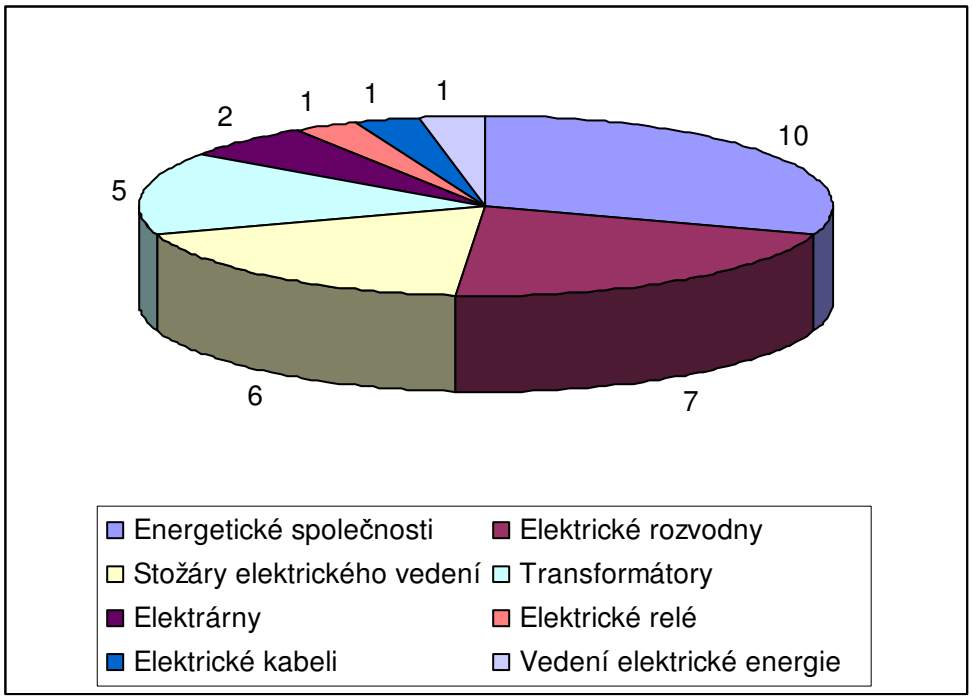
e) ozbrojeným útokem na rozvodny

Evropské elektrické zásobování je mnohem více napadáno než jiné energetické zásobování. Ze světového měřítka se však jedná o podprůměr. Ve světě převládá nejvíce útoků na společnosti přepravující ropu a plyn[59].

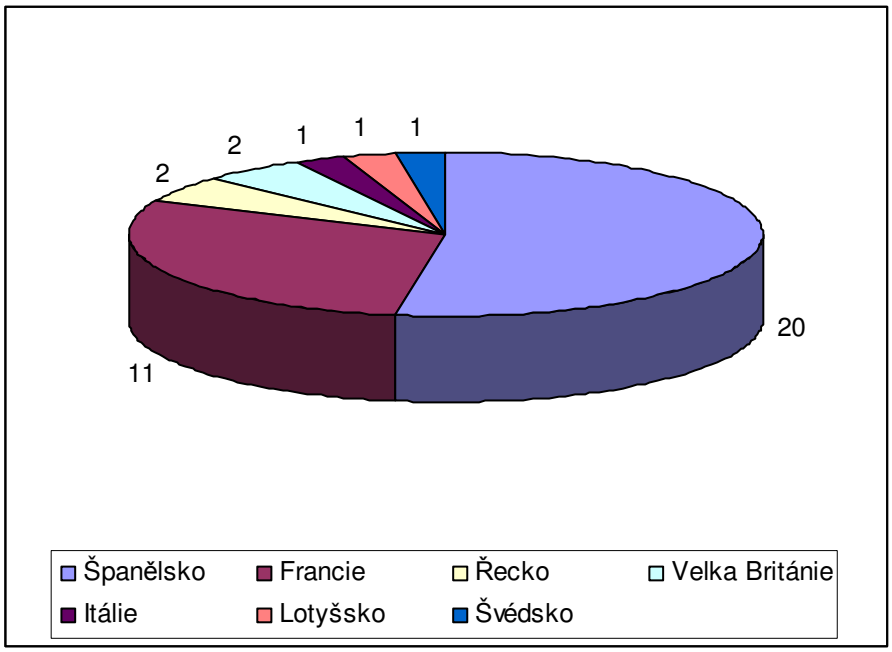
Obrázek 5: Nejčastěji použité zbraně v útocích na ES v Evropě v letech 1999-2008[59]



Obrázek 6: Evropské cíle teroristických útoků na ES v letech 1999-2008[59]



Obrázek 7: Nejčastější útoky v zemích EU na ES[59]



Teroristické útoky vedené na elektrizační soustavu, které proběhly v Evropě v letech 1999–2008 nevedly k smrtícím účinkům. Žádný člověk nezemřel v rámci útoků vedených na jakýkoliv prvek elektrizační soustavy. Neobjevili se velké škody spojené s takovými útoky. Z toho vyplývá téměř neexistence významného narušení dodávek

elektrické energie. Pachatelé takových to teroristických útoků jsou převážně dobře známi. Pocházejí z levicových či separatistických skupin. Jedná se převážně o skupiny ETA ve Španělsku, FLNC ve Francii, PIRA ve Velké Británii, „Revoluční buňky“ v Řecku a podobně[59].

Al-Kájda

Hlavní motivací Al-Kájdy na ohrožení dodávek elektrické energie je způsobit co největší hospodářské škody[59].

Al-Kájda má dvě hlavní motivace v teroristických útocích:

a) „Zastavte plenění muslimské ropy“,

b) „Poškození ekonomiky USA a oslabení západního světa.

Avšak v muslimském světě je jakékoliv napadení energetického sektoru velice kontroverzní otázkou. Samotný Bin Ládin vyzývá k útokům na zahraniční ropná zařízení, ale již dříve varoval, proti takovým útokům[59].

ZÁVĚR

Kritická infrastruktura je jedna z nejdůležitějších prvků, které zabezpečují chod státu. Její ohrožení či napadení se nedotýká pouze státu, ale i jeho obyvatel. Elektrizační soustava je jednou z velice důležitých součástí kritické infrastruktury.

V dnešní době se již bez elektrické energie neobejdeme. Vše je na ni závislé počínaje televizorem a konče proudící vodou z vodovou. Elektrická energie má jako jediná část kritické infrastruktury nevýhodu. Nelze vytvořit její zásoby pro případ nedostatku. Při nevyvážené výrobě a spotřebě dochází k výpadkům elektroenergetické soustavy. Snahou státu je proto omezit ztráty, které při výpadku nastaly. Přijímají se opatření na úrovni distribuční soustavy, přenosové soustavy i výrobního sektoru. Nemalou úlohu sehrává i stát přijímáním zákonů a vyhlášek, které se týkají ochrany ES jak v národní tak nadnárodní úrovni.

Po útocích ve Španělsku se ukázaly útoky na kritickou infrastrukturu velice pravděpodobné. I elektrizační soustava se teroristickým útokům nevyhne. Útoky vedené proti elektrizační soustavě zatím nedosáhly takových rozměrů, jako útoky zaměřené na obyvatelstvo, ale postupně se teroristé stávají více agresivnější. Elektrizační soustava je velice citlivá a cílená teroristická akce může vyvolat i několikaměsíční narušení normálního chodu státu nebo postiženého území. Je proto vhodné zaměřit pozornost ochrany elektrizační soustavy i na nejcitlivější místa, jako jsou transformátorovny. Nevýhodou elektrizační soustavy je její rozsáhlost a možnost ochrany celé soustavy je prakticky nereálná. Ochrana nejdůležitějších částí představuje přístup, který může snížit riziko teroristického útoku na elektroenergetickou soustavu.

SEZNAM POUŽITÉ LITERATURY

[1] BRZYBOHATÝ, Marian. *Terorismus I.* 1. vyd. Praha: Police history, 1999. 141 s. ISBN 80-902670-1-7

[2] MAREŠ, Miroslav. *Vymezení pojmů terorismus, válka a guerilla v soudobé bezpečnostní terminologii.* In: Obrana a strategie 1/2004, s. 19 – 32. ISSN1214-6463[online][cit. 2006-10-19]. Dostupný z WWW:<http://www.army.cz/mo/obrana_a_strategie/1-2004cz/mares.pdf>

[3] http://cs.wikipedia.org/wiki/Guerilla

[4] SHARPE, M.E., *Encyklopedie světový terorismus od starověku po útok na USA*, Překl. P. Tůma, Z. Hurník Praha: Svojka & CO, 2001 (1. vydání), 536 s. ISBN 80-7237-340-4

[5] FOLTIN,Pavel, ŘEHÁK,David, STOJAR, Richard, *Vybrané aspekty soudobého terorismu,* 1. vyd. Ministerstvo obrany ČR-AVIS, 2008. 143 s. ISBN 978-80-7278-443

[6] ŠEDIVÝ, Jiří. *Nové paradigma terorismu*. In: Mezinárodní politika. ÚMV Praha, 2003, roč. 4, č. 1, s. 4 – 7. ISSN 0543-7962.

[7] MIKA, O. J., *Současný terorismus*, 1. vyd., Praha: Triton, 2003, 92 s. ISBN 80-7254-409-8

[8] PATOČKA,Jiří, *Vojenská toxikologie*, 1. vyd., Grada Publishing, a.s. 2004, 180 s. ISBN 80-247-0608-3

[9] STŘEDA, Ladislav, *Šíření zbraní hromadného ničení,* 1. vyd., MV-generální ředitelství Hasičského záchranného sboru ČR, 2003, 245 s. ISBN 80-86640-03-5

[10] ÖSTERREICHER, Jan, VÁVROVÁ,Jiřina, *Přednášky z radiobiologie*, 1. vyd., Spoltisk s.r.o., 2003, 116 s. ISBN 80-86571-01-7

[11] *Je možné měřit míru ohrožení země terorismem?*[online][cit. 2008-11-9]Dostupný z WWW: < http://aplikace.mvcr.cz/archiv2008/rs_atlantic/data/files/aon.pdf>

[12] *Národní akční plán boje proti terorismu aktualizované znění pro léta* 2007-2009[online][cit. 2008-11-9] Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/dokument/2008/nap_2007_cze.pdf>

[13] *Ekonomické souvislosti terorismu*[online][cit. 2008-11-10] Dostupný z WWW: <zdroj:http://pavelkohout.blogspot.com/2005/07/ekonomick-souvislosti-terorismu.html>

[14] EICHLER,Jan, *terorismus a války na počátku 21. století,* 1. vyd., Karolinum, 2007, 352 s. ISBN 978-80-246-1317-8

[15] EICHLER, Jan. *Jak dál v boji proti globálnímu terorismu*. In: Obrana a strategie. Brno: 2005, roč. 5, č. 1, s. 21-32. ISSN 1214-6463

[16] http://cs.wikipedia.org/wiki/Infrastruktura

[17] ŠENOVSKÝ, Michail, ADAMEC, Vilém, ŠENOVSKÝ, Pavel, *Ochrana kritické infrastruktury,* 1.vyd. 2008,

[18] http://www.uvr.cz/images/publikace/uvr/2007-04/08_kriticka.pdf, Listopad 8, 2008

[19] KOVAŘÍK, Jaroslav, *Kritická infrastruktura a ochrana obyvatelstva*, In: Ochrana obyvatel 2007 Ochrana kritické infrastruktury, s. 145-153, ISBN 80-86634-51-5, [online][cit. 2008-11-8] Dostupný z WWW: <http://www.btv.cz/download/Ochrana_kriticke_infrastruktury_2007.pdf>

[20] *Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020* [online][cit. 2008-11-12] Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/hasici/ochrobyv/koncepce/3.pdf>

[21] ZELINKA,Jan, *Možné způsoby fyzické ochrany důležitých objektů a kritické infrastruktury, historie a současnost*, In: Ochrana obyvatel 2007 Ochrana kritické infrastruktury, s. 453-456, ISBN 80-86634-51-5, [online] [cit.2008-11-12] Dostupný z WWW: <http://www.btv.cz/download/Ochrana_kriticke_infrastruktury_2007.pdf>

[22] PROCHÁZKOVÁ, Dana, *Bezpečnost je základní prioritou bezpečnosti*, In: Environmentální aspekty podnikání 3/2004, s. 6-11[online][cit. 2008-11-15] Dostupný z WWW: <http://www.cemc.cz/aspekty/vyber_z_clanku/rizeni/dokumenty/11.pdf>

[23] Úvod do krizové legislativy a řízení [online][cit. 2008-11-19] Dostupný z WWW: <http://www.cityplan.cz/%C3%9Avod-do-krizove-legislativy-a-rizeni-342.html>

[24] ŠAMAL, Kamil, ADAMEC, Vilém, *Analýza právních předpisů vztahujících se ke krizovému a havarijnímu plánování v ČR* [online][cit.2008-11-20] Dostupný z WWW: <http://labrisk.vsb.cz/cz/kmvp2007/SAMAL.pdf>

[25] *Zelená kniha*,[online][cit.2008-11-20] Dostupný z WWW:<http://ec.europa.eu/research/era/pdf/era_gp_final_cs.pdf>

[26] HORÁK, R., SALIGER, T., NAVRÁTIL, J., *Řešení kritické infrastruktury s možností využité nástrojů EU*[online][2008-11-15] Dostupný z WWW: <http://www.btv.cz/download/Ochrana_kriticke_infrastruktury_2007.pdf>

[27] Elektrická energie, [online][cit. 2008.11.21] Dostupný z WWW: <http://www.eon.cz/cs/info/el_power.shtml>

[28] *Elektrizační soustavy*, [online][cit.2008-11-21] Dostupný z WWW: <zdroj:http://www.cez.cz/edee/content/file/_static/encyklopedie/encyklopedie_energetiky/05/soustavy_3.html>

[29] Dostupný z WWW: <k315.feld.cvut.cz/download/ape/kap1.doc>

[30] *Encyklopedie* [online][cit.2008-11-25]<http://encyklopedie.seznam.cz/heslo/501762-elektrarny-v-cesku>

[31] skripta elektroenergetika

[32] *Proces výroby v uhelných elektrárnách*. [online][cit.2008-11-22] Dostupný z WWW: <http://www.cez.cz/cs/energie-a-zivotni-prostredi/uhelne-elektrarny/flash-model-jak-funguje-uhelna-elektrarna.html>

[33] *Technologie výroby energie v JE* [online][cit.2008-11-23]Dostupný z WWW: <http://www.jaderna-energie.cz/technologie-vyroby-energie.htm>

[34] *Technologie a bezpečnost*. [online][cit.2008-11-23] Dostupný z WWW: <http://www.cez.cz/cs/energie-a-zivotni-prostredi/jaderna-energetika/jaderne-elektrarny-cez/edu/technologie-a-zabezpeceni.html#p1>

[35] *Výroba elektrické energie*, [online][cit.2008.11.23] Dostupný z WWW: <:www.ped.muni.cz/wtech/elearning/ELE/Vyroba_elektricke_energie.ppt>

[36] *Vodní elektrárny v ČR*, [online][cit.2008-11-23] Dostupný z WWW: <http://www.vodni-tepelne-elektrarny.cz/vodni-elektrarny-cr.htm>

[37] *Přenosová soustava*. [online][cit.2008-12-5] Dostupný z WWW: <http://encyklopedie.seznam.cz/heslo/460358-prenosova-soustava>

[38] *Údaje o PS*. [online][cit.2008-12-5] Dostupný z WWW: <http://www.ceps.cz/detail.asp?cepsmenu=3&IDP=32&PDM2=0&PDM3=0&PDM4=0>

[39] *Elektrizační soustava*. [online][cit.2008-12-5] Dostupný z WWW: <http://www.powerwiki.cz/attach/PES/cv08.pdf>

[40] *Slovník pojmů*. [online][cit.2008-12-5] Dostupný z WWW: <http://www.eon.cz/cs/info/terms_dictionary.shtml>

[41] *Pravidla provozování distribučních soustav* [online][cit.2008-12-5] Dostupný z WWW: <http://www.cezdistribuce.cz/edee/content/file-other/distribuce/energeticka_legislativa/PPDS/2008/PPDS_2008_2801.pdf>

[42] *popis distribuční soustavy E.ON Distribuce, a.s.* [online][cit.200-12-5] Dostupný z WWW: <http://www.eon.cz/file/cs/distribution/technical_information/EON-popis_ds.pdf>

[43] *Výroční zpráva 2007* [online][cit.2008-12-5] Dostupný z WWW: <http://www.cezdistribuce.cz/edee/content/file-other/distribuce/o_spolecnosti/Vyroc_zprava_2007_CJ.pdf>

[44] *Rozsah rozvodného zařízení* [online][cit.2008-12-5] Dostupný z WWW: <http://www.predistribuce.cz/distribuce/distribucni-sit/technicke-informace/rozsah-rozvodneho-zarizeni.html>

[45] *ZEL_11.Notebook* [online][cit.2008-12-7] Dostupný z WWW: <http://is.sssep9.cz/podklady/bransovsky/Z%C3%A1klady%20elektrotechniky%20-%20pdf/Zel_11.pdf>

[46] *Stabilita elektrizační soustavy* [online][cit.2008-12-7] Dostupný z WWW: <http://www.vesmir.cz/clanek.php3?CID=7053>

[47] *Stabilita sítě* [online][cit.2008-12-7] Dostupný z WWW: <http://proatom.luksoft.cz/view.php?cisloclanku=2006021501>

[48] *Trh s elektrickou energií v Evropě* [online][cit.2008-12-7] Dostupný z WWW:< (zdroj:http://www.pxe.cz/pxe_downloads/Info/pxe_analyza.pdf>

[49] BENEŠ, Ivan, *Energetická bezpečnost*, CITYPLAN, spol, s.r.o., 2007, 36.str, ISBN 978-80-254-1244-2

[50] Městské teplárny-základ ochrany proti blackoutu [online][cit.2008-12-8] Dostupné z WWW: <http://ww.cityplan.cz/index.php?id_document=994>

[51] SMEJKAL,V.,RAIS,K.;*Řízení rizik*; 1.vyd.; Praha: Grada Publishing, 2003, 272s.; ISBN 80-247-0198-7

[52] BENEŠ, I.,ROSA. J.;*Systémové řešení nouzového zásobování elektřinou v případě krizových stavů*; CITYPLAN s.r.o. 2008

[53] *Typové plány pro řešení krizových situací* [online][cit. 2009-3-1] Dostupný z WWW: <http://www.volny.cz/casopis.energetika/e_0306_1.html>

[54] KOM(2004)702, [online][cit.2009-3-3] Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:CS:HTML>

[55] KOM(2005)576 Zelená kniha [online][cit.2009-3-3] Dostupný z WWW: < http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf>

[56] EPCIP [online][cit.2009-2-24] Dostupný z WWW: <http://www.europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477&format=PDF&aged=1&language=EN&guiLanguage>

[57] Směrnice rady 2008/114/ES [online][cit.2009-3-4] Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF>

[58] *The Terrorism Threat to Energy Supply Chains* Presentation in Brussels, March 3rd, 2009, Brynjar Lia PhD.,

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

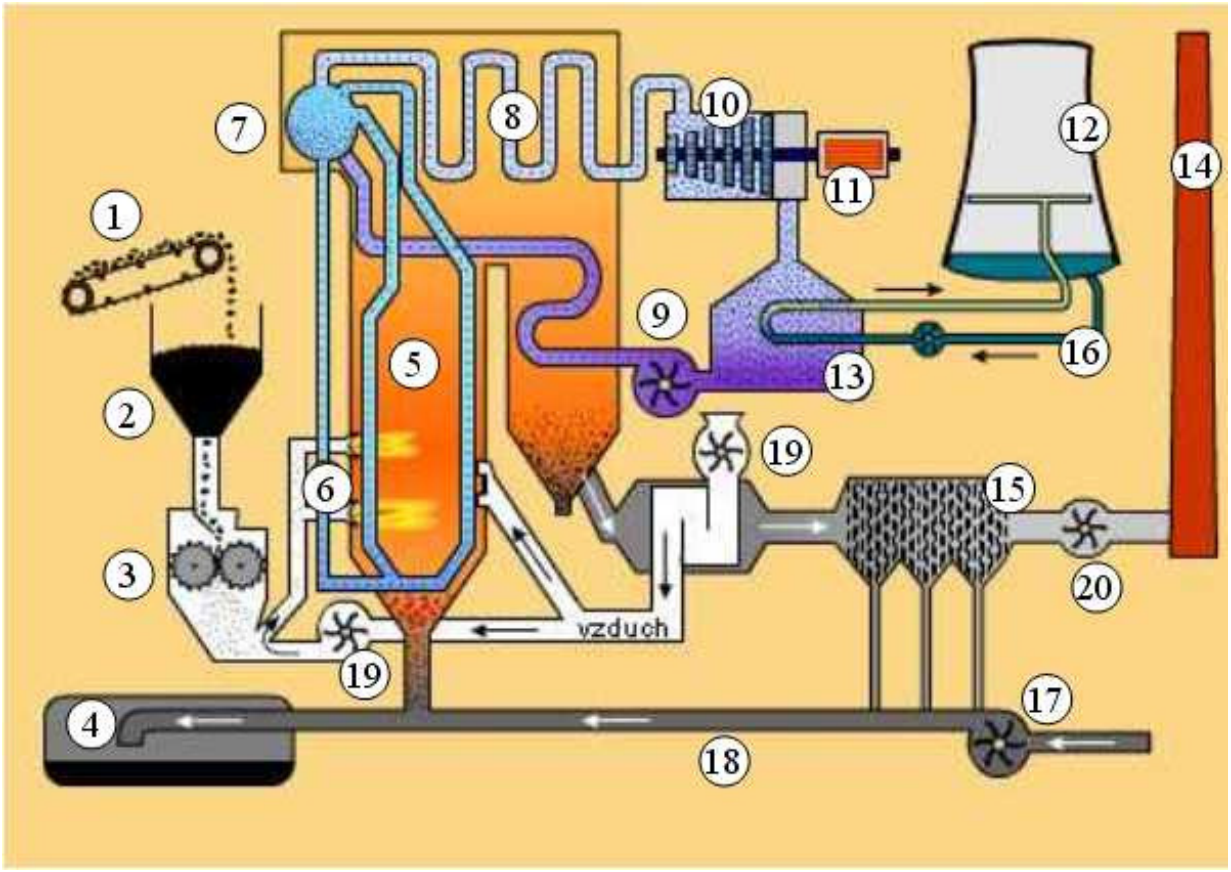
MV GŘ HZS	Ministerstvo vnitra generální ředitelství hasičského záchranného sboru
IZS	Integrovaný záchranný systém
HOPKS	Hospodářská opatření pro krizové stavy
EPCIP	Evropský program pro ochranu kritické infrastruktury
ARGUS	Systém rychlé výměny informací
CIWIN	Výstražná informační síť kritické infrastruktury
ENISA	Evropská agentura pro informační a síťovou bezpečnost
UCPTE	Západoevropská síť Svazu pro koordinaci
MIR	Síť socialistického bloku
VVN	Velmi vysoké napětí
VN	Vysoké napětí
NN	Nízké napětí
UCTE	The Union for the Co-ordination of Transmission of Elektricity
ES	Elektrizační soustava
EU	Evropská Unie
EPCIP	Evropský program na ochranu kritické infrastruktury
CIWIN	Výstražná informační síť kritické infrastruktury
EKI	Evropská kritická infrastruktura

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

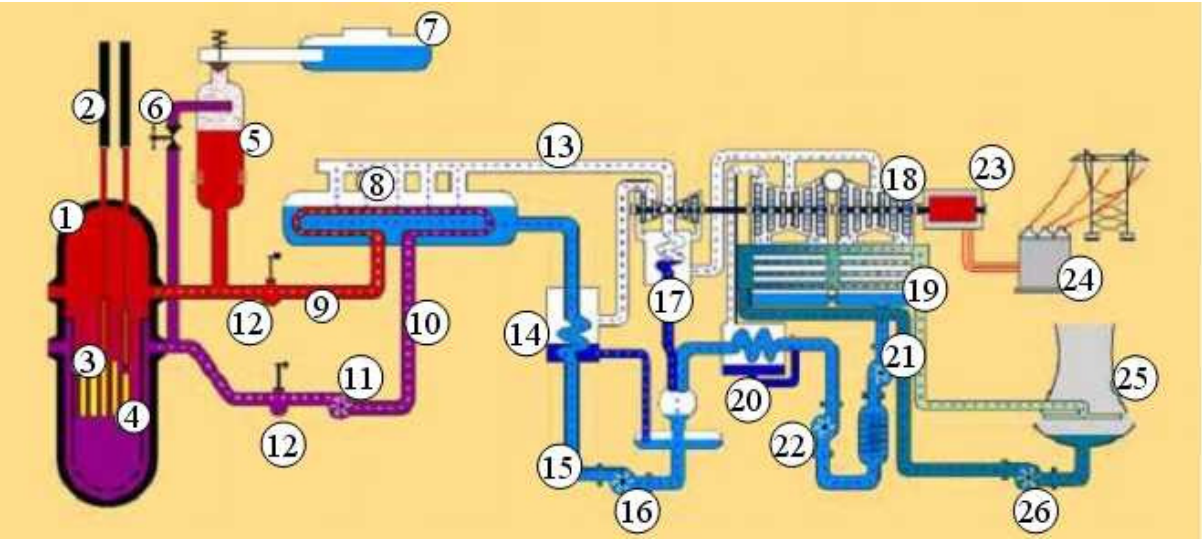
PŘÍLOHA P I: SCHÉMA UHLENÉ ELEKTRÁRNY



1	Pásový dopravník	8	Přehřívač páry	15	Elektrostatický odlučovač popílku
2	Zásobník uhlí	9	Napájecí čerpadlo	16	Chladící voda
3	Mlecí zařízení	10	Turbína	17	Čerpadlo
4	Úložiště popílku	11	Elektrický generátor	18	Technologická voda spalovací
5	Kotel	12	Chladící věž	19	Ventilátor
6	Hořáky	13	Kondensátor	20	Dýmový ventilátor
7	Parní buben	14	Komín		

Zdroj: [35]

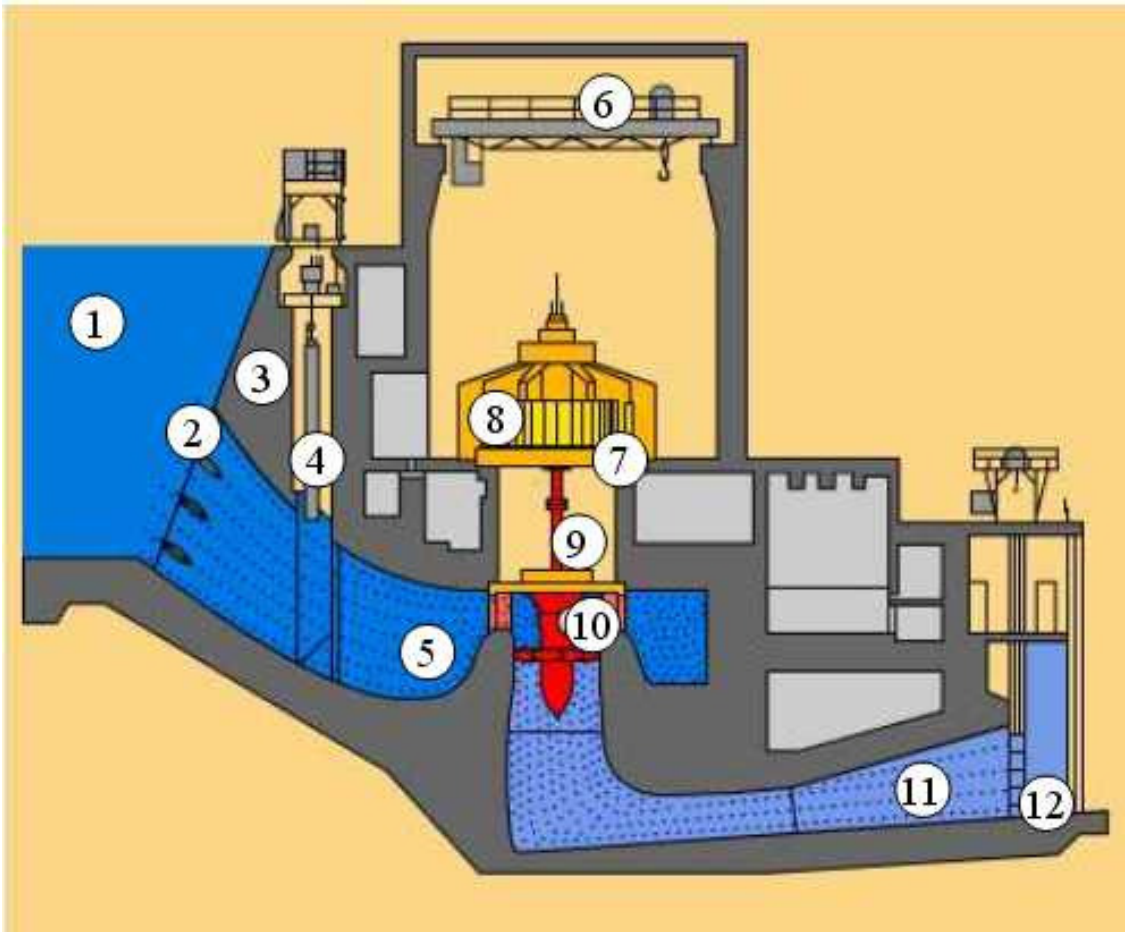
PŘÍLOHA P II: SCHÉMA JADERNÉ ELEKTRÁRNY



1	Jaderný reaktor	9	Horká část cirkulační slučky primárního okruhu	17	Separátor a přehřívač páry
2	Regulační kazety	10	Studená část cirkulační slučky primárního okruhu	18	Turbína
3	Jaderné palivo	11	Hlavní cirkulační čerpadlo	19	Kondensátor
4	Štěpná reakce	12	Hlavní uzavírací armatura	20	Nízkotlaká regenerace
5	Kompenzátor objemu	13	Hlavní parní potrubí	21	Kondenzační čerpadlo 1. stupně
6	Sprchy kompenzátoru objemu	14	Vysokotlaká regulace	22	Kondenzační čerpadlo 1. stupně
7	Barbotážní nádrž	15	Hlavní napájecí potrubí	23	Elektrický generátor
8	Parogenerátor	16	Napájecí zařízení	24	Transformátor

Zdroj: [35]

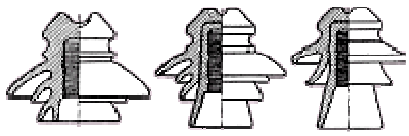
PŘÍLOHA P III: SCHÉMA VODNÍ ELEKTRÁRNY



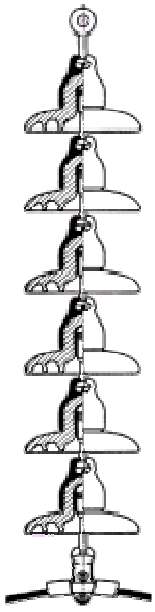
1	Přívodní kanál	5	Tlakový přivaděč	9	Hřídel
2	Česle	6	Montážní jeřáb	10	Vodní turbína
3	Vzdouvací zařízení-hráze	7	Generátor	11	Sací roura
4	Vtoková hradidla	8	Rotor	12	Odpadní kanál

Zdroj: [35]

PŘÍLOHA P IV: IZOLÁTORY

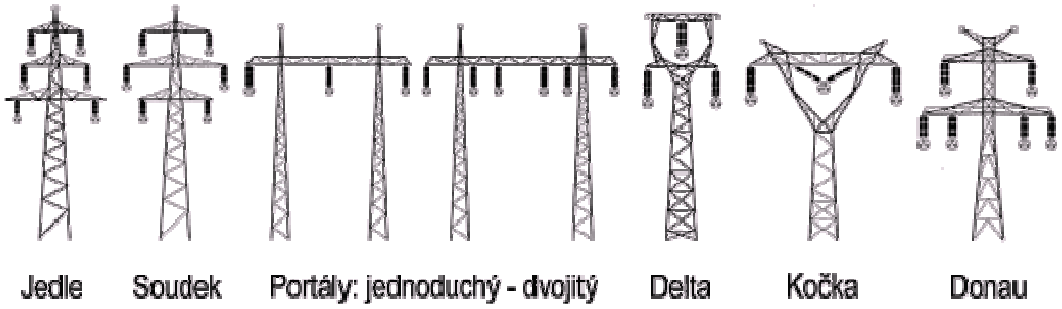


Delta izolátory a řetězce izolátorů



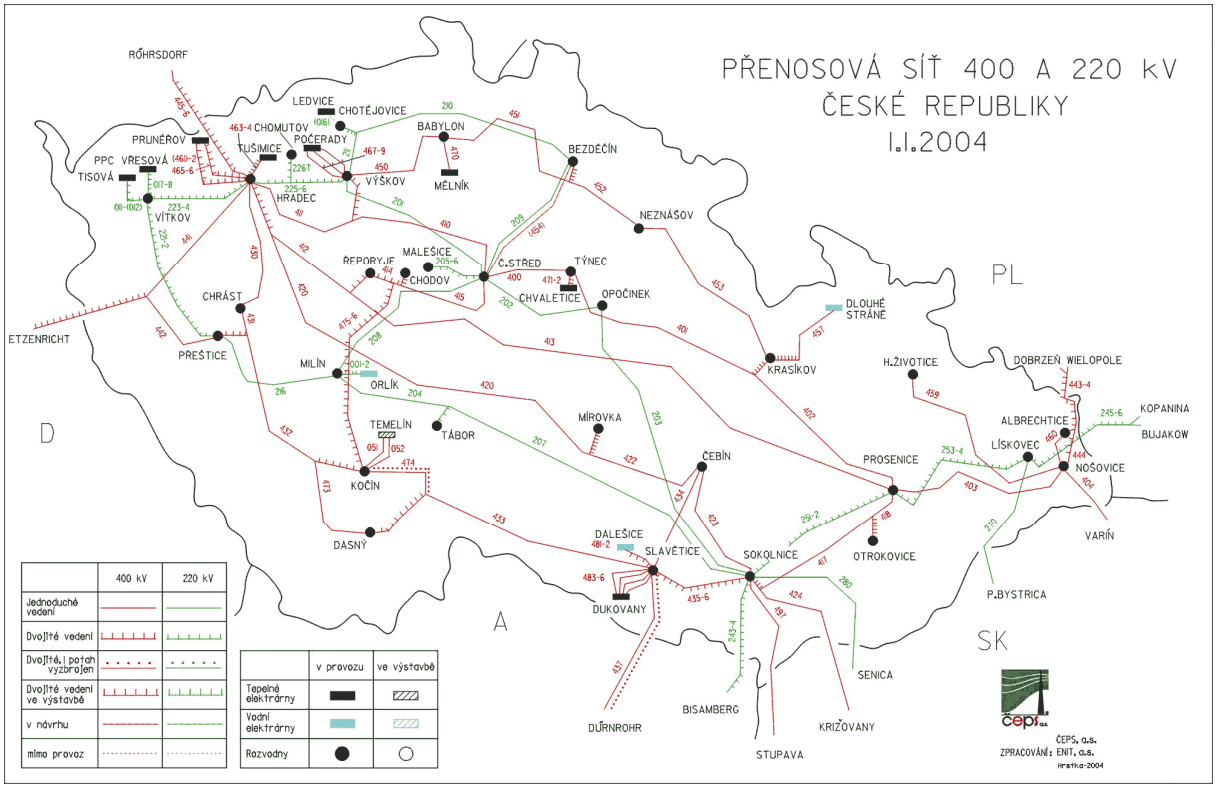
Zdroj: [28]

PŘÍLOHA P V: STOŽÁRY



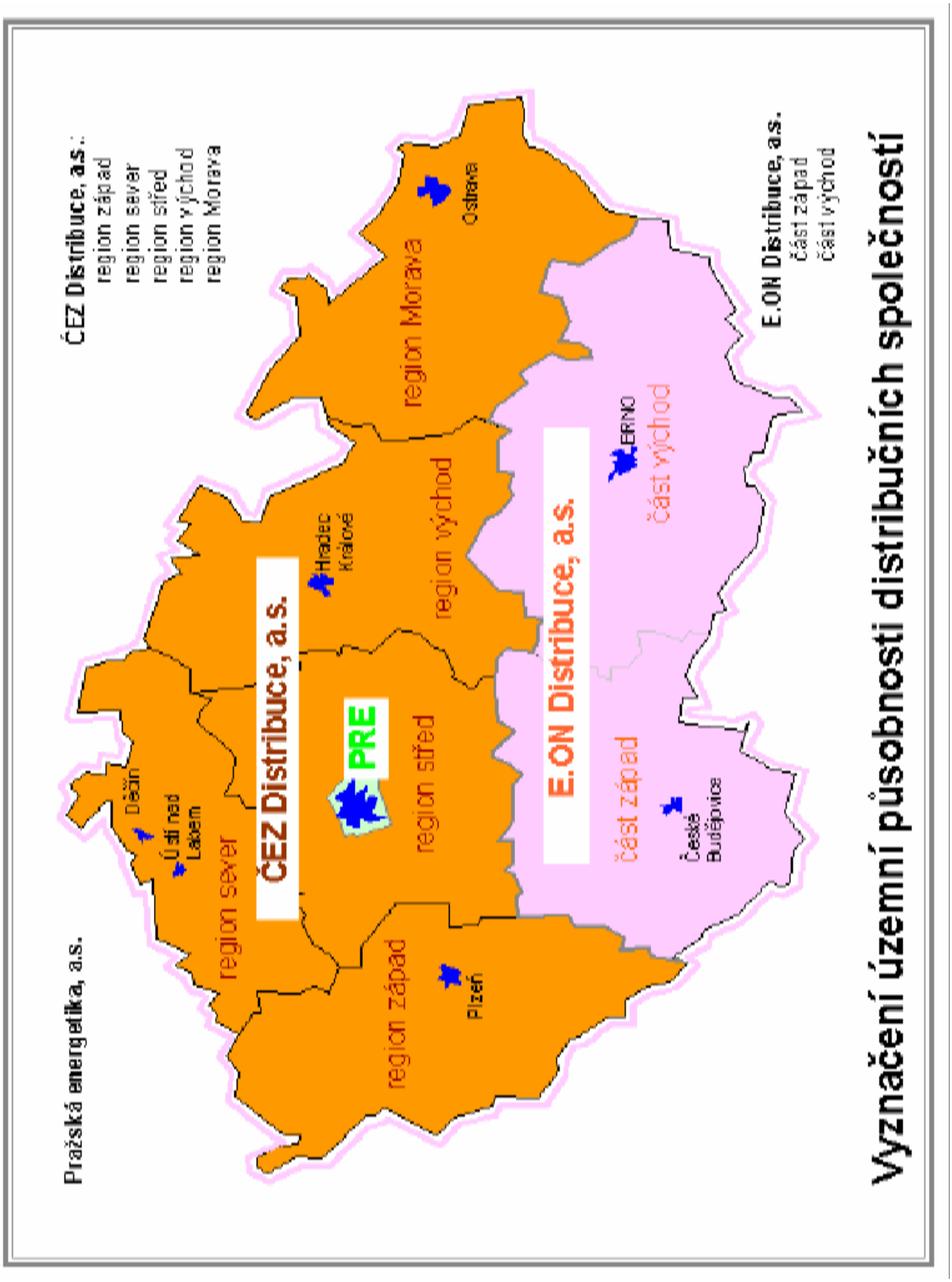
Zdroj: [28]

PŘÍLOHA P VI: SCHÉMA PŘENOSOVÉ SOUSTAVY ČR



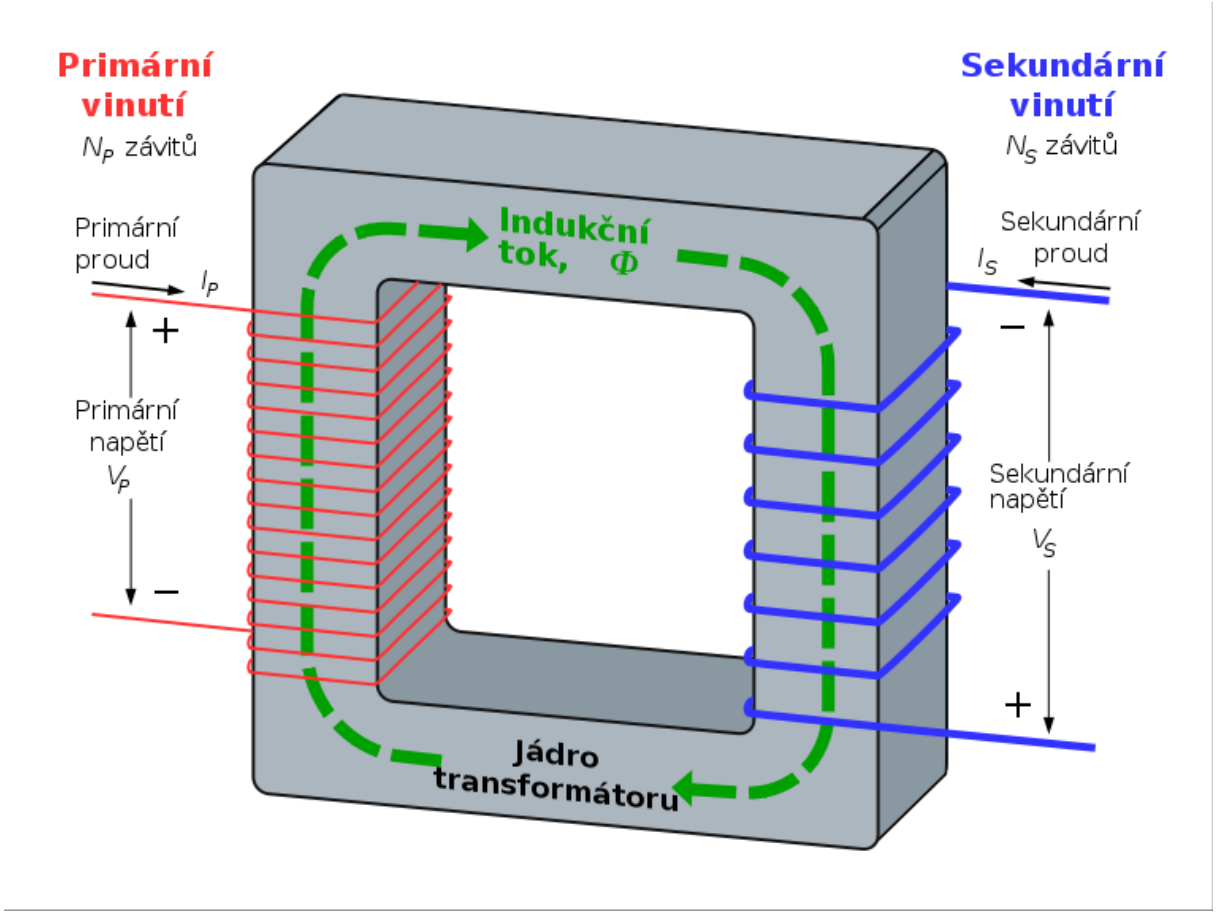
Zdroj: [38]

PŘÍLOHA P VII: DISTRIBUČNÍ SPOLEČNOSTI ČR



Zdroj: [39]

PŘÍLOHA P VIII: TRANSFORMÁTOR



PŘÍLOHA P VIIII: ZÁSOBOVACÍ ŘETĚZEC ELKTŘINY