Český telekomunikační úřad
se sídlem Sokolovská 219, Praha 9
poštovní přihrádka 02, 225 02 Praha 025

Čj.: ČTÚ - 23 417/2018–604
V Praze 9. května 2018
Počet listů: 21

Typový plán

„Narušení funkčnosti významných systémů elektronických komunikací“

Zpracovatel dokumentu: Samostatné oddělení bezpečnosti a krizového řízení

OBSAH Strana

T y p o v ý p l á n

Typ krizové situace: Narušení funkčnosti významných systémů elektronických komunikací

---

1. Základní část

Typový plán „Narušení funkčnosti významných systémů elektronických komunikací“ je dokument, kterým Český telekomunikační úřad (dále jen „ČTÚ“), ve spolupráci s dalšími ústředními správními úřady, stanovil typové postupy, zásady a opatření pro řešení konkrétního druhu krizové situace. Narušení významných systémů elektronických komunikací je identifikováno v „Analýze hrozeb pro Českou republiku“ jako nebezpečí s nepřijatelným rizikem, pro které lze předpokládat vyhlášení krizového stavu.

Vnitrostátní podmínky pro řešení krizových situací v komunikačních systémech tvoří soubor opatření vyplývajících z příslušných legislativních norem a plánů k zajištění poskytování služeb elektronických komunikací za havarijních nebo krizových situací, které jsou vytvářeny a realizovány prostřednictvím orgánů státní a veřejné správy a subjekty vykonávajícími komunikační činnosti, zejména operátory[1)].

Zajišťování veřejné komunikační sítě, poskytování veřejně dostupné služby elektronických komunikací, zavádění vysokorychlostních sítí elektronických komunikací podle zákona o opatřeních ke snížení nákladů na budování vysokorychlostních sítí elektronických komunikací a zajišťování sítí elektronických komunikací pro účely bezpečnosti státu se uskutečňují ve veřejném zájmu.

Za významné systémy elektronických komunikací jsou považovány veřejné komunikační sítě, jejichž prostřednictvím jsou poskytovány veřejně dostupné služby elektronických komunikací a narušení jejich funkčnosti by mělo za následek závažný dopad na bezpečnost a obranu státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Prostřednictvím veřejných sítí a služeb elektronických komunikací jsou zajišťovány hlasové a datové služby, jejichž prostřednictvím se poskytují i důležité informace pro řešení krizových situací. Kromě uvedených veřejných sítí a služeb jsou zřizovány sítě pro neveřejné účely, jejichž provoz a využití zajišťuje zřizovatel (např. Ministerstvo vnitra ČR síť PEGAS pro integrovaný záchranný systém)[2)].

1.1. Popis krizové situace

Veřejně dostupné služby elektronických komunikací se poskytují nebo se k nim zajišťuje přístup prostřednictvím veřejných sítí elektronických komunikací provozovaných provozovatelem – operátorem. Sítě elektronických komunikací jsou tvořeny přenosovými systémy, popřípadě spojovacími nebo směrovacími zařízeními a jinými prostředky umožňujícími přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, popřípadě sítí pro rozvod elektrické energie bez ohledu na druh přenášené informace. Protože služby elektronických komunikací spočívají převážně v přenosu signálů po sítích elektronických komunikací, včetně sítí používaných pro

---

[1)] Vyhláška č. 241/2012 Sb., o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů.

[2)] Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.

rozhlasové a televizní vysílání a sítí kabelové televize, je popis krizové situace zaměřen jak na část postižených síťových technologických prvků, tak i část nedostupných služeb elektronických komunikací.

Při popisu krizové situace v oblasti narušení funkčnosti významných systémů elektronických komunikací, je potřeba se zaměřit na přesný název subjektu podnikajícího v elektronických komunikacích postiženého poruchou, popis příčiny, rozsah jeho nefunkčnosti (částečná nefunkčnost – popis funkcionalit které jsou neprovozuschopné, anebo celková nefunkčnost) a pokud je to možné, i předpoklad odstranění poruchy. Při závažném narušení sítě elektronických komunikací se postupuje v souladu se ZEK[3)].

1.1.1. Příčiny narušení funkčnosti významných systémů elektronických komunikací

Poskytování služeb elektronických komunikací z hlediska síťových přenosů probíhá v převážné míře v těchto sítích elektronických komunikací:

- pevné sítě,
- mobilní sítě (buňkové rádiové sítě),
- rádiové sítě,
- družicové sítě,
- sítě pro rozhlasové a televizní vysílání.

V případech, kdy hrozí závažné snížení bezpečnosti a integrity sítě z důvodů poškození nebo zničení komunikačního zařízení může podnikatel, zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, přijmout opatření k přerušení poskytování služby nebo odepření přístupu ke službě. Toto opatření musí být omezeno pouze na dobu nezbytně nutnou, a je-li to technicky možné, musí být zachován přístup k číslům tísňového volání. O přijatých opatřeních, důvodech přerušení poskytování služby nebo odepření přístupu k ní a o předpokládaném termínu odstranění příčiny, je povinen bezprostředně informovat ČTÚ a vhodným způsobem i uživatele a subjekty provozující pracoviště pro příjem tísňového volání.[4)]

1.1.2. Narušení bezpečnosti a integrity veřejných sítí a služeb mohou způsobit zejména následující příčiny

- přímé poškození provozních zařízení (provozní havárií, technickou poruchou, zanedbáním údržby, neodborným servisním zásahem, živelní pohromou, teroristickým nebo jiným cíleným útokem, mechanickým poškozením),
- výpadky v důsledku prudkého nárůstu provozu v síti a následného přetížení nebo v důsledku výpadku jiné sítě elektronických komunikací,
- disfunkční chování nebo kybernetické napadení řídících systémů sítí elektronických komunikací,
- narušení dodávky elektrické energie včetně narušení dodávky ze záložního zdroje,
- rozsáhlé omezení činnosti obsluhy provozních zařízení (epidemie, živelní pohroma, sociální příčiny, vznik nebo nebezpečí ozbrojeného konfliktu),
- úmyslným nebo neúmyslným elektromagnetickým rušením.

Propojovací vedení je chráněno vůči negativním vlivům izolací a pláštěm v závislosti na prostředí, ve kterém je umístněné. Ze všech prvků přenosové soustavy je obvykle nejméně chráněno proti mechanickému poškození a doba obnovy propojení je závislá od umístění a typu kabelu. Vhodným způsobem obnovy kabelového propojovacího vedení je odpovídající

---

3) Například § 98 ZEK.

4) § 98 odst. 3,4 ZEK.

topologie sítě počítající s využitím náhradních a obchozích cest například formou radioreleového propojení zařízení pro zpracování signálu.

Pevné sítě elektronických komunikací jsou nejodolnějším systémem vůči elektromagnetickému rušení a vůči nepříznivým povětrnostním podmínkám.

Méně odolné jsou vůči mechanickým poškozením vlivem havárií, stavebním a výkopovým pracím, nebo jiným záměrným činnostem. Z hlediska působení živelních pohrom jsou nejzranitelnější vlivem záplav z důvodu umístnění technologických prvků v suterénních nebo přízemních částech budov nebo přímo v terénu v záplavových oblastech, případně v mostních konstrukcích.

Mobilní sítě elektronických komunikací jsou kombinací pevných a rádiových sítí. Přístup uživatelů ke službám je realizován tzv. buňkovým systémem, kde buňka je geografický prvek, který obsahuje základnovou stanici s rádiovým vysílačem/přijímačem, prostřednictvím kterého každý uživatel nacházející se uvnitř buňky komunikuje s ostatními uživateli pevných nebo mobilních telekomunikačních systémů. Přenos ze základnových stanic se předává systémem řídících stanic po pevných sítích elektronických komunikací propojených s jinými sítěmi nebo jinými základnovými stanicemi.
Z hlediska výše uvedené architektury sítě je pravděpodobnost přetížení mobilní sítě vyšší než u jiných sítí zejména v případě nárůstu počtu volajících a počtu volání v jedné buňce (zejména v místech s vysokou koncentrací obyvatel při společenských akcích nebo mimořádných situacích). Tato síť je energeticky značně náročná z důvodu poměrně vysokého počtu základnových stanic potřebných k pokrytí daného území. K zajištění provozuschopnosti sítě v případě výpadku sítě elektrické energie je nutné zajistit adekvátní počet náhradních zdrojů elektrické energie včetně jejich doplňování pohonnými hmotami.
Zvýšení spolehlivosti mobilních sítí lze dosáhnout, obdobně jako u pevných sítí, vhodnou topologií sítě, která může eliminovat výpadek některé z ústředen. Dosahuje se toho směrováním volání střídavě na tzv. duální ústředny, které odbavují provoz vznikající na tomto území.
Stejně jako rádiové sítě (např. typu Wi-Fi) i tyto sítě jsou značně citlivé na úmyslné, či neúmyslné elektromagnetické rušení (např. z důvodu solární bouře). Jejich výhodou je snadnější nahrazení v případě poškození základnové stanice nebo možnost pokrytí buňky signálem sousedních stanic v případě hustějšího osazení daného území.
Technologické prvky sítě, zejména vysílací, jsou energeticky náročné, a proto je nutné, pro případ výpadku energetické soustavy, zálohovat tato zařízení náhradním zdrojem elektrické energie s trvalým provozem a s odpovídajícím výkonem. Obnova provozu při haváriích zařízení záleží na rozsahu poškození a zejména na přístupnosti k anténním systémům (např. v zaplaveném území nebo v zimních podmínkách). Doporučovaným technickým řešením je realizace zálohování vysílacích stanic mobilními elektro energetickými prostředky.

Typické příčiny narušení bezpečnosti a integrity sítí a služeb elektronických komunikací:

- poškození technologicko-provozních zařízení pro rozhlasové a televizní vysílání způsobené např. technickou poruchou, neprovedením či zanedbáním servisních prací, dopady při vzniku živelní pohromy, teroristický nebo jiný úmyslný útok apod.,
- poškození kabelových sítí určených pro přenos rozhlasového a televizního signálu DVB-C,
- kybernetické napadení řídících systémů sítí pro rozhlasové a televizní vysílání,
- narušení dodávky elektrické energie včetně jejího přerušení ze záložního zdroje,
- rozsáhlé omezení činnosti obsluhy provozních zařízení sítí pro rozhlasové a televizní vysílání z důvodů sociálních nebo epidemiologických,
- úmyslné nebo neúmyslné elektromagnetické rušení rozhlasového nebo televizního signálu.

Rozhlasové a televizní vysílání je zajišťováno prostřednictvím rádiových sítí rozhlasových (DAB) a televizních vysílačů (DVB-T), dále prostřednictvím kabelových sítí (DVB-C) nebo prostřednictvím satelitních přenosů (DVB-S). Příčiny narušení uvedených služeb mají obdobný charakter jako příčiny uvedené v tomto článku. Výjimku tvoří satelitní systémy, jejichž provoz je ovlivněn specifickým umístěním v kosmickém prostoru a to kosmickým počasím (solární bouře), kosmickým odpadem, neočekávanou změnou polohy satelitu, elektromagnetickým rušením atd.

1.1.3. Zákonné povinnosti pro všechny uvedené sítě a služby

Za rozhodující při posuzování oblasti „Bezpečnost a integrita veřejných komunikačních sítí elektronických komunikací“ členy krizového štábu je potřeba dle ZEK považovat:

- podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinen zajišťovat bezpečnost a integritu své sítě a bezpečnost služeb, které poskytuje,
- podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací může v případech, kdy hrozí nebo dojde k závažnému narušení bezpečnosti a integrity jeho sítě z důvodů poškození nebo zničení elektronického komunikačního zařízení, zejména vlivem velkých provozních havárií nebo živelních pohrom, přerušit poskytování služby nebo odepřít přístup ke službě. Přerušení nebo odepření musí být omezeno pouze na dobu nezbytně nutnou, a je-li to technicky možné, musí být zachován přístup k číslům tísňového volání,
- o závažném narušení bezpečnosti a ztrátě integrity sítě, rozsahu a důvodech přerušení poskytování služby nebo odepření přístupu k ní, přijatých opatřeních a o předpokládaném termínu odstranění příčiny podle odstavce 3 je podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinen bezodkladně informovat ČTÚ, subjekty provozující pracoviště pro příjem tísňového volání a vhodným způsobem i uživatele.

Za rozhodující při posuzování oblasti „Bezpečnost, integrita a poskytování služeb za krizových stavů“**,** EK, je potřeba považovat:

- podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je za krizového stavu povinen podle svých technicko-organizačních pravidel zabezpečit bezpečnost a integritu své sítě a interoperabilitu poskytovaných služeb. Náležitosti uvedených technicko-organizačních pravidel je stanoveno ČTÚ prováděcím právním předpisem,[5)]
- podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou telefonní službu je oprávněn při nebezpečí vzniku krizové situace a za krizového stavu [6)] na žádost Ministerstva vnitra poskytovat přednostně připojení k veřejné komunikační síti a přístup k veřejně dostupné telefonní službě účastníkům krizové komunikace podle zvláštního právního předpisu.[7)] Za tímto účelem je v rozsahu nezbytně nutném oprávněn omezit nebo přerušit poskytování veřejně dostupné telefonní služby. O omezení nebo přerušení poskytování veřejně dostupné telefonní služby, včetně jeho rozsahu, je povinen bezodkladně informovat ČTÚ. Toto omezení může trvat pouze po dobu nezbytně nutnou a musí být zachován přístup k číslům tísňového volání.

[5)] Vyhláška č. 241/2012 Sb., o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů.

[6)] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

[7)] § 18 zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.

1.1.4. Modelové scénáře možného vývoje krizových situací

1.1.4.1. Popis skutečností indikujících, že může vzniknout krizová situace

Příčiny, které vedou ke vzniku krizové situace a mohou narušit funkčnost komunikačního systému:

- živelní pohromy (např. zvyšování hladiny toků, bouřková činnost, vichřice a silné větrné poryvy, svahové pohyby a sesuvy půdy, lesní požáry, solární bouře, následky seismických vln atd.),
- epidemie – hromadné nákazy osob a zvířat,
- technické, technologické havárie (např. radiační výrony škodlivin, exploze, požáry, omezení nebo přerušení dodávek elektrické energie, plynu, vody, havárie způsobené přepětím nebo účinkem silného elektromagnetického pole atd.),
- kybernetické útoky na komunikační a informační systémy (SCADA systémy apod.)
- narušení funkčnosti ekonomických vztahů (např. insolvence právnických osob, ale i platební neschopnost uživatelů služeb elektronických komunikací apod.),
- narušení sociálních vztahů (např. stávky zaměstnanců, etnické vnitrostátní nepokoje apod.),
- narušení mezinárodních vztahů (ozbrojené konflikty, narušení smluvních vztahů, technologická ztráta integrity mezinárodních sítí elektronických komunikací, nefunkčnost národních domén Internetu apod.),
- disfunkce systémů elektronických komunikací (např. rozsáhlé výpadky řídících systémů, klíčových technologických zařízení a systémů apod.),
- narušení dodržování právních předpisů státu velkého rozsahu (např. terorismus, rozsáhlá organizovaná kriminalita, masivní porušování ZEK).

1.1.4.2. Popis skutečností indikujících, že vzniklá situace je krizová

- přetrvávající působení příčin krizové situace, jejich zintenzivnění a prostorové rozšíření,
- rozsáhlé kybernetické útoky na komunikační a informační systémy,
- nedostatečná účinnost protikrizových opatření,
- rozsáhlý výpadek dodávek elektrické energie,
- dlouhodobé přerušení dodávek služeb elektronických komunikací,
- rozsah narušení sítí elektronických komunikací neumožňuje dodávky služeb ani účastníkům krizové komunikace s přednostním právem (přednostní spojení),
- reálné nebezpečí vzniku sekundárních krizových situací (kaskádový efekt), postupný nárůst ohrožení základních funkcí státu a kritické infrastruktury.

1.1.4.3. Popis skutečností indikujících, že vzniklá situace přestává být krizová

- slábne (přestává působit) vliv příčin vzniku krizové situace,
- eliminace kybernetických útoků na komunikační a informační systémy,
- obnovení dodávek elektrické energie odběratelům,
- obnovení dodávek služeb elektronických komunikací vybraným účastníkům (čísla tísňového volání, orgány krizového řízení),
- obnova funkčnosti narušených prvků sítě elektronických komunikací.

1.1.5. Sekundární události, které mohou vzniknout jako důsledek vzniku krizové situace (přerušení poskytování služeb elektronických komunikací)

- technické a technologické havárie velkého rozsahu vlivem výpadku řídících systémů (SCADA),
- možné narušení dodávek ropy, plynu a elektrické energie velkého rozsahu u dalších

kritických infrastruktur vlivem narušení řídících systémů,
- narušení ekonomiky a finančního hospodářství (bankovnictví) velkého rozsahu,
- narušení funkčnosti dopravní soustavy velkého rozsahu (zejména v oblasti letecké přepravy),
- narušení funkčnosti veřejných informačních vazeb velkého rozsahu,
- možné narušení zákonnosti velkého rozsahu,
- narušení poskytování zdravotnické péče závislé na službách elektronických komunikací (např. telemedicína),

1.2. Následky krizové situace

Následkem vzniku krizových situací může dojít k narušení/přerušení kontinuity provozu veřejné komunikační sítě a v důsledku toho k narušení/přerušení poskytování služeb elektronických komunikací, které může mít vliv na:

- narušení (znemožnění) koordinovaného postupu mezi orgány krizového řízení, orgány veřejné správy a samosprávy a mezi složkami integrovaného záchranného systému,
- narušení činnosti bezpečnostních, obranných a zpravodajských orgánů státu,
- omezení nebo ochromení činnosti orgánů státu a organizací pověřených výkonem veřejné správy,
- ztrátu informační podpory v krizové situaci,
- narušení řídících a monitorovacích systémů provozovatelů veřejných sítí závislých na přístupu k datovým zdrojům a přenosu informací,
- omezení nebo ochromení činnosti subjektů kritické infrastruktury státu,
- četnost a nepřetržitost poskytování informační podpory pro veřejnost včetně volání na čísla tísňového volání (omezení přístupu veřejnosti k informacím poskytovaným veřejnou správou),
- výpadky tísňových volání, omezená informovanost obyvatelstva, možné nepokoje,
- informování obyvatelstva o mimořádných událostech a krizových situacích.

1.2.1. Dopady na životy a zdraví osob

Dopady na život a poškození zdraví osob v důsledku působení krizových stavů v oblasti komunikačních systémů mohou být přímé a nepřímé.

K nepřímému dopadu na život, zdraví a bezpečnost osob dochází v důsledku selhání poskytování služeb elektronických komunikací, např. tísňového volání, varovného systému obyvatelstva nebo v důsledku disfunkce zdravotnických informačních systémů. Mezi nepřímé dopady rovněž patří vznik a eskalace disfunkce řídících a informačních systémů vlivem přerušení toku dat, která vyvolává takové stavy, při kterých mohou vzniknout škody na životech a zdraví osob, např. výpadky monitorovacího systému životního prostředí, řídícího a informačního systému petrochemických produktovodů, řídících a informačních systémů integrovaného záchranného systému.

1.2.2. Dopady na environmentální prostředí

Dopady na environmentální prostředí v důsledku působení krizových stavů v oblasti komunikačních systémů mohou být přímé a nepřímé.

K nepřímému ohrožení, poškození nebo devastaci životního prostředí v důsledku krizových situací v oblasti komunikačních systémů může dojít při přerušení přenosů příslušných datových souborů řídících systémů s havarijními důsledky ovlivňujícími životní prostředí jako je např. únik nebezpečných látek.

Krizové situace způsobené jinými negativními vlivy, které mají přímý dopad na životní prostředí, může dále prohloubit:

- disfunkce monitorovacích systémů dopravního informačního systému,
- disfunkce monitorovacích systémů životního prostředí,
- disfunkce řídících, informačních a komunikačních systémů krizového řízení a integrovaného záchranného systému.

1.2.3. Mezinárodní dopady při narušení významných systémů elektronických komunikací

- omezení nebo zastavení mezinárodního provozu ve veřejných sítích elektronických komunikací, a to i s možným dopadem na další státy EU,
- omezení nebo znemožnění plnění mezinárodních hospodářských, politických a vojenských závazků,
- omezení nebo znemožnění mezinárodní spolupráce při odstraňování příčin a důsledků krizových situací.

1.2.4. Ekonomické dopady

Patří sem především omezení nebo ochromení řídících a komunikačních procesů ve výrobní i nevýrobní sféře národního hospodářství, zejména v oblasti bankovnictví a finančních služeb.

1.2.5. Sociální dopady

- omezení nebo znemožnění poskytování sociálních služeb obyvatelstvu vázaných na poskytování služeb elektronických komunikací,
- omezení nebo znemožnění přístupu obyvatelstva k peněžním zdrojům vázaným v bankách a spořitelnách závislém na poskytování služeb elektronických komunikací,
- omezení přístupu obyvatelstva k informacím a omezení komunikace s veřejnou správou,
- omezení nebo znemožnění zásobování obyvatelstva v důsledku výpadku výroby a distribuce závislé na poskytování služeb elektronických komunikací.

1.2.6. Dopady na kritickou infrastrukturu

Vznik krizové situace v komunikačních systémech v závislosti na rozsahu má místní, národní nebo nadnárodní dopady na funkčnost přímo nebo nepřímo postižených odvětví kritické infrastruktury přerušením nebo snížením kvality přenosu potřebných informací.

V důsledku působení krizových situací v oblasti komunikačních systémů dochází k nepřímým škodám na majetku. Jedná se zejména o:

- disfunkci varovného informačního systému,
- omezení možností použití služeb elektronických komunikací a technických prostředků při situačním monitorování stavu krizových situací,
- výpadek nebo ochromení komunikačních systémů užívaných k záchraně majetku a k výkonu prací pro minimalizaci škod,
- disfunkci systémů tísňového volání.

Přehled v minulosti řešených krizových situací

V předchozím období nedošlo k rozsáhlému narušení funkčnosti významných systémů elektronických komunikací, v jehož důsledku by vznikla krizová situace s nutností vyhlášení krizových stavů na území ČR. Příčinou vzniku krizových situací s nutností vyhlášení

krizových stavů byly zejména přírodní pohromy typu záplavy s dlouhodobými dešti a bouřemi v letech 1997 až 2013. Tyto krizové situace měly rovněž dopad na kvalitu, bezpečnost a integritu veřejných sítí a služeb elektronických komunikací. Projevovaly se dlouhodobějšími (cca 1 až 2 dny) lokálními výpadky služeb elektronických komunikací zejména v postiženém (zaplaveném) území.

Nejvíce postižená území:

1997 – povodí řek Moravy, Odry a Bečvy,
2002 – povodí řek Lužnice, Vltavy, Berounky, Ohře, Labe a Jizery.

Dílčí analýza situace z hlediska elektronických komunikací:

- v roce 1997 neúplné pokrytí území ČR signálem pro mobilní komunikaci, značná část komunikace byla zajištěna přes pevné sítě elektronických komunikací. V procesu dostavby se nacházely sítě dvou mobilních operátorů,
- služba mobilní komunikace byla poskytována koncovým uživatelům pouze v omezeném rozsahu.

Mezi hlavní příčiny výpadků služeb elektronických komunikací zejména patřily:

- zaplavené technologické celky v suterénech a nižších podlažích budov,
- přerušené kabelové trasy umístěné v blízkosti řečišť a mostních konstrukcí,
- poškozené anténní systémy v důsledku prudkých větrů a deště,
- přerušení dodávek elektrické energie do zaplavených území,
- narůstající počet volání v důsledku, kterého docházelo k přetížení komunikačních kanálů,
- špatná organizační opatření a neznalost používání krizových mobilních telefonů.

Přijímaná opatření a nezbytné potřeby:

- aktivovat systém přednostního připojení ke službám elektronických komunikací orgánům krizového řízení,
- zajistit dodávky elektrické energie prostřednictvím záložních elektrocentrál,
- zajistit kontinuální doplňování pohonných hmot pro provoz elektrocentrál,
- mít připravené servisní skupiny a náhradní technologie pro obnovu provozu,
  zvýšená potřeba čerpadel a vysoušecích zařízení pro obnovu provozu zaplavených technologií,
- zajistit přístup oprávněných osob za účelem udržování anebo obnovy provozu do postižených území, která jsou policejně uzavřena, včetně jejich vybavení funkčními komunikačními prostředky.

2. Operativní část

2.1. Zásady pro řešení krizové situace

Mezinárodní podmínky řešení krizových situací předpokládají nejen plnění mezinárodně platných opatření technického a technologického charakteru, ale i úzkou součinnost orgánů států při provozování komunikačních systémů v příhraničních oblastech. Pro komunikační systémy se jedná zejména o:

- realizaci Tamperské úmluvy[8)] ke zmírňování dopadů katastrof a poskytováním humanitární pomoci (např. v oblasti elektronických komunikací),
- uskutečňování mezinárodních sankcí v oblasti spojů podle zvláštního zákona[9)].

Vnitrostátní podmínky pro řešení krizových situací v komunikačních systémech tvoří soubor opatření vyplývajících z příslušných právních předpisů a plánů k zajištění poskytování služeb elektronických komunikací za havarijních nebo krizových situací zpracovaných podnikateli[1)].

Požadovaným stavem je zachování a rychlá obnova dostupnosti služeb elektronických komunikací v plném rozsahu.

Těžiště prováděných činností:

- zabezpečení integrity a bezpečnosti veřejných komunikačních sítí a služeb elektronických komunikací a na nich závislé činnosti subjektů kritické infrastruktury státu,
- zachování dostupnosti služeb ve veřejných sítích elektronických komunikací stanoveným subjektům a obyvatelstvu za krizových stavů na čísla tísňového volání,
- zajištění koordinace činností při likvidaci následků havarijních nebo krizových situací mezi havarijními složkami provozovatelů sítí a poskytovatelů služeb elektronických komunikací a složkami integrovaného záchranného systému,
- stanovení priorit obnovy činnosti komunikačních systémů ve vazbě na hospodářsko-politické požadavky a výstupy z krizového plánování,
- minimální doba na obnovu dodávek služeb elektronických komunikací po případném výpadku v důsledku krizových situací, periodická kontrola bezpečnostních opatření subjektů kritické infrastruktury a objektivizace havarijních plánů, plánů zabezpečení kontinuity činnosti a plánů obnovy.

Spolupráce mezi orgány státní správy:

Výkon státní správy v oblasti elektronických komunikací zajišťuje MPO ČR a ČTÚ.

Za provoz sítí přenos informací, včetně údržby a obnovy služeb a jejich obnovu za krizových situací v sítích elektronických komunikací určených pro neveřejné účely odpovídají jejich provozovatelé. Výstavbu a provoz komunikačních sítí a služeb integrovaného záchranného systému řídí Ministerstvo vnitra ČR[10)].
Mezi subjekty státní správy, u kterých se předpokládá úzká spolupráce při závažném narušení bezpečnosti a integrity veřejných sítí a služeb elektronických komunikací, především patří:

- ČTÚ
- MPO
- Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR (dále jen „GŘ HZS“.

ČTÚ

Působnost ČTÚ je dána zejména:

[8)] Mezinárodní úmluva o poskytování telekomunikačních zdrojů pro zmírňování katastrof a záchranné práce v gesci OSN.
[9)] § 6 odst. 2 zákona č. 69/2006 Sb., o mezinárodních sankcích, ve znění pozdějších předpisů.
[10)] § 7 zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.

- zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů,

- zákonem č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů,

- zákonem č. 206/2005 Sb., o ochraně některých služeb v oblasti rozhlasového a televizního vysílání a služeb informační společnosti, ve znění pozdějších předpisů

- zákonem č. 194/2017 Sb., o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací a o změně některých souvisejících zákonů

- zákonem č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,

- zákonem č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů.

Plní specifické úkoly v oblasti zajišťování bezpečnosti a integrity veřejných sítí a služeb elektronických komunikací zaměřené na oznamovací a kontrolní činnost, uvedené v části 1.2. tohoto dokumentu.

ČTÚ dále zabezpečuje:

- vydává všeobecná oprávnění, rozhoduje o jejich změně nebo zrušení a vede evidenci podnikatelů v elektronických komunikacích,

- vydává opatření obecné povahy, v nichž uvádí náležitosti technicko-organizačních pravidel podnikatelů zajišťujících veřejnou komunikační síť a provádí jejich kontrolu,

- stanovuje poskytovatele univerzální služby v elektronických komunikacích a přezkoumává poskytování univerzální služby,

- spolupracuje s příslušnými národními regulačními orgány členských států a s Komisí Evropských společenství,

- ověřuje odbornou způsobilost k obsluze vysílacích rádiových zařízení,

- vykonává kontrolu elektronických komunikací,

- vykonává správu rádiových kmitočtů a čísel včetně vedení jejich databáze, i pro potřeby ozbrojených sil, ozbrojených bezpečnostních sborů a záchranných sborů,

- zabezpečuje harmonizaci využívání rádiového spektra a harmonizaci číslovacích plánů,

- předkládá MPO návrhy právních předpisů v oblasti elektronických komunikací a spolupracuje s ním na jejich přípravě,

- vydává prováděcí právní předpisy v oblasti elektronických komunikací v rozsahu zmocnění podle platné legislativy,

- zabezpečuje oznamovací a informační povinnost ve vztahu ke Komisi EU v otázkách patřících do jeho působnosti,

- zabezpečuje mezinárodní vztahy v oblasti elektronických komunikací v případech stanovených vládou.

MPO

Působnost MPO vztažená k elektronickým komunikacím je vymezena v § 105 ZEK:

MPO ve spolupráci s ČTÚ určuje prvky kritické infrastruktury za oblast elektronických komunikací a k tomu vydává opatření obecné povahy.

MPO dále:

- zpracovává návrhy hlavních zásad státní politiky v elektronických komunikacích,
- zabezpečuje v oblasti elektronických komunikací plnění závazků vyplývajících z mezinárodních smluv, kterými je Česká republika vázána (požaduje zdroje k řešení krizových situací v oblasti elektronických komunikací v souladu s Tamperskou úmluvou),
- zpracovává krizový plán, který obsahuje souhrn krizových opatření a postupů k řešení krizových situací,
- poskytuje na požádání podklady z oblasti elektronických komunikací ústředním správním úřadům a Ústřednímu krizovému štábu.

GŘ HZS

GŘ HZS ČR se podílí na zajišťování bezpečnosti České republiky plněním a organizováním úkolů požární ochrany, ochrany obyvatelstva, civilního nouzového plánování, integrovaného záchranného systému, krizového řízení a dalších úkolů, v rozsahu a za podmínek stanovených právními předpisy.

GŘ HZS ČR je organizační součást Ministerstva vnitra ČR, která má přímý vztah k oblastem elektronických komunikací jako jsou bezpečnost, integrita a poskytování služeb za krizových stavů, uvedených v § 99 odst. 3 ZEK, s důrazem na zabezpečení služby přednostního přístupu k veřejné telefonní službě.

Ministerstvo vnitra ČR je vlastníkem a provozovatelem sítě integrovaného záchranného systému PEGAS. Síť PEGAS je neveřejná obdoba veřejných digitálních sítí mobilních telefonních operátorů, ovšem s podstatně jiným určením, a tedy i s podstatně jiným vybavením, které nelze funkcemi veřejných sítí nahradit.

Zásady monitorování stavu, přenos informací, vyrozumění o hrozbě vzniku krizových situací a způsob varování

Provozovatelé sítí elektronických komunikací trvale monitorují jejich provoz prostřednictvím dohledových center. V případě závažného narušení bezpečnosti a integrity sítě a následného přerušení poskytování služeb elektronických komunikací, operátor informuje o této skutečnosti ČTÚ, subjekty provozující pracoviště pro příjem tísňového volání a vhodným způsobem i uživatele poskytovaných služeb[11)].

Způsob vyrozumění a varování uživatelů služeb o realizaci krizových opatření v sítích elektronických komunikací a realizaci následných dodávek služeb je nutné zajistit v rámci smluv o dodávkách služeb.

Zásady monitorování stavu, přenosu informací, vyrozumění o hrozbě vzniku krizové situace a způsoby varování včetně vyhodnocování krizové situace zajišťují:

[11)] § 98 ZEK.

- dohledová centra, havarijní a krizové orgány operátorů,
- odborné útvary a krizové orgány určené podle krizového zákona,[12)]
- odborné útvary (odbor bezpečnosti a krizového řízení a odbor elektronických komunikací) a odborná pracovní skupina Krizového štábu MPO,
- odborné útvary a krizový štáb ČTÚ.

2.2. Opatření pro řešení krizové situace – karty opatření (příloha č. 1)

Tabulka opatření pro oblast narušení funkčnosti významných systémů elektronických komunikací

Označení opatření	Opatření	Zajišťuje	Spolupracuje
1.	*Aktivace přednostního připojení k veřejné komunikační síti a veřejně dostupné telefonní službě účastníkům krizové komunikace. (Příloha č. 1)*	Podnikatel zajišťující veřejnou komunikační síť	HZS kraje, OPIS MV-GŘ HZS ČR

2.3. Činnosti poskytovatelů služeb elektronických komunikací a provozovatelů sítí elektronických komunikací

V oblasti veřejných sítí elektronických komunikací podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen poskytovat tuto službu nepřetržitě po všechny dny v roce, nestanoví-li zákon jinak, a v kvalitě stanovené podle zákona o elektronických komunikacích[13)]. Je povinen zajišťovat bezpečnost a integritu veřejných komunikačních sítí a služeb, a to i za krizových stavů[14)].

Postupy, které krizové situaci mohou zabránit nebo zmírnit její dopady

Typické a předpokládané postupy (pracovní režimy) při krizových situacích a při jejich předcházení jsou popsány v havarijních plánech poskytovatelů služeb elektronických komunikací a provozovatelů sítí elektronických komunikací.

Návrhy vhodných technologických a organizačních postupů k řešení krizových situací

Principy technologických a organizačních postupů jsou obsaženy ve vyhlášce č. 241/2012 Sb., o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů.

Technicko-organizační pravidla podnikatelů v oboru elektronických komunikací

a) organizaci, strukturu a prvky systému krizového řízení, zásady jeho aktivace a koordinace postupů, včetně organizačního a personálního zajištění řešení krizových situací, odborné přípravy příslušných pracovníků provozu, údržby a obnovy sítí a služeb,

b) opatření k řízení a zachování integrity a bezpečnosti sítě a zajištění její průchodnosti a interoperability služeb, monitorování provozu sítě, detekce vzniklých závad,

[12)] Zákon číslo 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon).
[13)] § 61 ZEK.
[14)] § 98 a 99, ZEK.

sledování průběhu a nárůstu závad a odstraňování závad v síti, včetně možností řešení a základní opatření pro obnovu sítě a poskytování služeb,

c) opatření k zajištění přednostního připojení k síti a přednostního přístupu k veřejně dostupné telefonní službě,

d) zásady rozvoje, plánování a výstavby sítě s ohledem na krizové situace a odolnost sítě proti narušení a možnosti její obnovy,

e) způsob zajištění logistické podpory pro obnovu integrity sítě (provozní materiál, technologie, rozmístění zařízení, energie, služby), včetně zajištění finančních zdrojů pro obnovu sítě,

f) stanovení způsobu vyhlašování začátku a ukončení omezení nebo přerušení poskytování veřejně dostupné telefonní služby,

g) zásady a organizaci vnější a vnitřní komunikace podnikatele podle § 99 odst. 1 ZEK.

Činnost poskytovatelů služeb elektronických komunikací, provozovatelů sítí elektronických komunikací v době hrozby vzniku a při vzniku krizové situace

na základě vyvíjející se hrozby analyzují situaci vzniklou v komunikačním systému (elektronická komunikační zařízení, síťové prvky, zdroje energie),
- určují možnou příčinu, charakter, rozsah, důsledky a možný vývoj narušení komunikačních systémů,
- přijímají bezodkladná opatření s cílem minimalizovat rozsah narušení komunikačních systémů a stabilizovat situaci,
- připravují evakuaci obsluh a technologií komunikačních systémů,
- vyhodnocují odezvu realizovaných opatření a rozhodují o dalším postupu a opatřeních,
- v nezbytném případě přijímají návrhy k přerušení poskytování služby elektronických komunikací, popřípadě k odepření nebo omezení přístupu ke službě,
- o přijatých opatřeních informují ČTÚ, subjekty provozující pracoviště pro příjem tísňového volání a uživatele,
- neprodleně přistupují k likvidaci možných příčin a následků přerušení poskytování služeb,
- v případě potřeby mohou vyžadovat potřebnou součinnost prostřednictvím MPO a ČTÚ.

Činnost poskytovatelů služeb elektronických komunikací, provozovatelů sítí elektronických komunikací při řešení krizové situace a v etapě likvidace následků krizové situace

Podnikatelé poskytující veřejně dostupnou službu elektronických komunikací v době krize:

- průběžně vyhodnocují vývoj situace a postup při obnově poskytování služeb,
- v nezbytném případě provedou evakuaci ohrožených technologií a pracovníků,
- provádí pro odstranění následků narušení funkčnosti významných systémů elektronických komunikací činnosti a v případě potřeby zajišťují náhradní technologie,
- oznamují stav obnovy ČTÚ.

2.4. Činnost ČTÚ

Činnost ČTÚ v době hrozby vzniku a při vzniku krizové situace

- samostatné oddělení bezpečnosti a krizového řízení ČTÚ analyzuje získané informace obdržené od orgánů krizového řízení, ostatních složek státní správy a poskytovatelů služeb elektronických komunikací,
- při vyhodnocování situace přihlíží především k následujícím skutečnostem:

- je-li překonání a likvidace následků krizové situace plně v možnostech poskytovatelů služeb elektronických komunikací,
- průběžně analyzuje předpokládaný čas, po který bude trvat likvidace následků přerušení poskytování služeb elektronických komunikací,
- shromažďuje a analyzuje informace o územním rozsahu, jak velké území státu je postiženo,
- analyzuje informace o rozsahu omezení nebo přerušení dodávek služeb elektronických komunikací,
- samostatné oddělení bezpečnosti a krizového řízení ČTÚ zpracovává informaci, pro předsedu Rady ČTÚ, podává návrh na svolání Krizového štábu ČTÚ a vytváří odbornou pracovní skupinu pro řešení krizové situace v elektronických komunikacích.

- odborná pracovní skupina:

- vyhodnocuje, odborné důsledky a zároveň předpoklady řešení krizové situace,
- navrhuje nezbytná technická a organizační opatření pro zajištění chodu ČTÚ a plnění úkolů vyplývajících z jeho působnosti,
- s poskytovateli veřejných služeb elektronických komunikací a provozovateli veřejných sítí elektronických komunikací projednává potřebnou součinnost a možnosti zkrácení doby likvidace následků krizové situace,
- sleduje postup poskytovatelů veřejných služeb elektronických komunikací a provozovatelů veřejných sítí elektronických komunikací při likvidaci následků krizové situace,
- předkládá Krizovému štábu ČTÚ informaci o vzniklé krizové situaci a návrh na její řešení,
- po projednání a vyhodnocení informace Krizovým štábem ČTÚ jsou v případě potřeby informovány veřejnost, Ústřední krizový štáb a případně další orgány krizového řízení.

Činnost ČTÚ při řešení krizové situace a v etapě likvidace jejích následků

- sleduje postup poskytovatelů služeb elektronických komunikací a provozovatelů sítí při likvidaci následků krizové situace a obnově poskytování služeb,
- průběžně vyhodnocuje vývoj situace a postup při likvidaci následků krizové situace,
- v případě potřeby předkládá Ústřednímu krizovému štábu informace o vývoji situace a návrhy krizových opatření (např. zajištění náhradních zdrojů elektrické energie, potřebná součinnost ostatních resortů),
- ve spolupráci s dalšími ministerstvy[15)] zajišťuje poskytování komunikačních zdrojů pro zmírňování následků katastrof a záchranné práce ze zahraničí,
- shromažďuje a analyzuje informace předávané podnikatelskými subjekty v oblasti elektronických komunikací,
- Krizový štáb ČTÚ spolu s odbornými útvary ČTÚ analyzuje průběžně vývoj situace a navrhuje opatření k jejímu řešení a eliminaci následků,
- podává průběžně aktuální informace o vývoji situace a přijatých opatřeních předsedovi Rady ČTÚ a podle stanovených regulí informuje Ústřední krizový štáb a MPO.

Kromě uvedených úkolů vykonává ČTÚ následující činnosti:

- zabezpečuje za krizových stavů výkon státní správy včetně regulace ve věcech elektronických komunikací v oblastech stanovených zákonem,
- koordinuje za krizových stavů ve spolupráci s MPO procesy a postupy podnikatelů v oblasti elektronických komunikací, přípravu a zabezpečení regulace v oblasti veřejně dostupných služeb elektronických komunikací,

[15)] Bod IV. usnesení vlády ze dne 10. dubna 2002 č. 378.

- podporuje zachování integrity a bezpečnosti veřejných komunikačních sítí,
- v případech, kdy je ohroženo nebo přerušeno nepřetržité poskytování veřejně dostupné služby elektronických komunikací, je oprávněn rozhodovat o opatřeních nezbytných k udržení nebo obnovení tohoto poskytování. Ukládá v době krizového stavu v případě nebezpečí z prodlení podnikateli zajišťujícímu veřejnou komunikační síť nebo poskytujícímu veřejně dostupnou službu elektronických komunikací povinnost zabezpečovat veřejně dostupnou službu elektronických komunikací,
- podílí se na tvorbě a organizaci komunikační podpory pro řešení krizových situací a na ovlivňování výstavby infrastruktury elektronických komunikací pro potřeby obrany a bezpečnosti státu.

2.5. Činnost orgánů krizového řízení

- kontaktují smluvní subjekty, které jim poskytují služby elektronických komunikací,
- v případě potřeby žádají o spolupráci oblastní odbory ČTÚ (viz kontakty uvedené v bodě 3.1. tohoto dokumentu),
- analyzují informace obdržené od poskytovatelů služeb elektronických komunikací,
- při vyhodnocování situace a výpadku služeb elektronických komunikací přihlížejí především k následujícím skutečnostem:
  - jak dlouho bude trvat obnova dodávek služeb elektronických komunikací,
  - jak velké území regionu a počet účastníků je postiženo,
  - v jakém rozsahu jsou omezeny nebo přerušeny dodávky služeb elektronických komunikací,
- vyhodnocují důsledky a předpoklady řešení zajištění náhradní komunikace,
- prověřují funkčnost komunikačních vazeb s orgány krizového řízení ve vazbě na krizový plán,
- průběžně vyhodnocují vývoj situace, možnosti zabránění vzniku sekundárních krizových situací a postup při likvidaci následků krizové situace,
- ve spolupráci s operátory zabezpečí přístup servisních týmů do postižených lokalit a objektů za účelem podrobné specifikace škod a postupů k jejich odstranění,
- zajišťují přístup do ohrožených prostor osobám zajišťujícím obnovu poskytování služeb elektronických komunikací,
- realizují mimořádná opatření k zajištění pohonných hmot pro provoz náhradních zdrojů elektrické energie,
- zajišťují ochranu důležitých objektů komunikační infrastruktury,
- plní další úkoly jako za stavu nebezpečí,

2.6. Požadavky na mimořádné síly, prostředky a mimořádné zdroje

<u>Požadavky na mimořádné síly a prostředky</u>

- zásah složek integrovaného záchranného systému podle požadavků operátorů,
- prostředky pro obnovu provozu a zajištění komunikačních činností z pohotovostních zásob, které se nacházejí ve správě Správy státních hmotných rezerv (např. kalová čerpadla, vysoušeče, elektrocentrály apod.),
- spolupracuje s policejními orgány při zajišťování vstupu do uzavřených oblastí.

<u>Požadavky na mimořádné zdroje</u>

- náhradní zdroje elektrické energie ze státních hmotných rezerv,
- pohonné hmoty ze státních hmotných rezerv pro zajištění provozu náhradních zdrojů elektrické energie,
- věcné zdroje podle reálné situace (v souladu s Metodikou vyžadování věcných zdrojů

za krizové situace[16)] včetně přepravních kapacit).

3. Pomocná část

3.1. Informace o zpracovateli Typového plánu

Kontaktní spojení:

Český telekomunikační úřad, Sokolovská 219, 225 02 Praha 025
telefon: 224 004 111, fax: 224 004 830
e-mail: podatelna@ctu.cz
datová schránka ID: **a9qaats**

Vedoucí samostatného oddělení bezpečnosti a krizového řízení ČTÚ
telefon: 224 004 723, fax: 224 004 815

Zástupce vedoucího samostatného oddělení bezpečnosti a krizového řízení ČTÚ
telefon: 224 004 717, fax: 224 004 815

Český telekomunikační úřad – odborné útvary a odbor krizového řízení
Sokolovská 219, Praha 9, poštovní přihrádka 02, 225 02 Praha 025
telefon: 224 004 111, fax 224 004 830
e-mail: podatelna@ctu.cz

Český telekomunikační úřad, odbor pro oblast Praha
Sokolovská 219, Praha 9, poštovní přihrádka 02, 225 02 Praha 025
telefon: 224 004 503, fax: 224 004 828

Český telekomunikační úřad, odbor pro jihočeskou oblast
Žižkova tř. 1321/1, 370 01 České Budějovice 6
telefon: 386 104 111, fax: 386 104 120

Český telekomunikační úřad, odbor pro západočeskou oblast
Husova 2727/10, poštovní přihrádka 273, 305 73 Plzeň
telefon: 377 925 911, fax: 377 236 693

Český telekomunikační úřad, odbor pro severočeskou oblast
Mírové náměstí 3097/37, 400 01 Ústí nad Labem
telefon: 475 309 311, fax. 475 210 572

Český telekomunikační úřad, odbor pro východočeskou oblast
Velké náměstí 1, 500 03 Hradec Králové
telefon: 495 279 311, fax: 495 279 315

Český telekomunikační úřad, odbor pro jihomoravskou oblast
Šumavská 35, 602 00 Brno
telefon: 541 428 611, fax: 541 428 631

Český telekomunikační úřad, odbor pro severomoravskou oblast
Havlíčkovo nábřeží 2728/38, 702 00 Ostrava-Moravská Ostrava
telefon: 595 138 551, fax: 595 138 568

Ministerstvo průmyslu a obchodu, Na Františku 32, 110 15 Praha 1
telefon: 224 851 111, fax: 224 811 089
e-mail: posta@mpo.cz
datová schránka ID: **bxtaaw4**

[16)] Usnesení vlády ze dne 4. ledna 2012 č. 14.

Identifikační údaje o zpracovateli Typového plánu:

Název a adresa zpracovatele typového plánu

Poštovní adresa:

Český telekomunikační úřad
Sokolovská 219, poštovní přihrádka 02
Praha 9
225 02 Praha 025

Sídlo:

Český telekomunikační úřad
Sokolovská 219, Praha 9 (metro B, stanice Vysočanská)

Kontaktní údaje osob, které se podílely na zpracování Typového plánu.

Samostatné oddělení bezpečnosti a krizového řízení ČTÚ
Sokolovská 219, Praha 9
Tel: 224 004 723, 224 004 718

Přílohy: (Karty opatření)

Příloha č.1

KARTA OPATŘENÍ					
Opatření					**Označení opatření**
Aktivace přednostního připojení k veřejné komunikační síti a veřejně dostupné telefonní službě účastníkům krizové komunikace					**1**
Nařizuje (schvaluje)	MV	**Provádí**	Podnikatel zajišťující veřejnou komunikační síť	**Spolupracuje**	HZS kraje, OPIS MV-GŘ HZS ČR
Související právní předpisy					
Zákon č. 127/2005 Sb., o elektronických komunikacích Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů					
Mimořádné zdroje, síly a prostředky					
Další potřebné informace související s plněním opatření					
Seznam účastníků krizové komunikace, pro které byla služba přednostního připojení zřízena					

Popis činností k realizaci opatření

P. č.	Činnosti na ústřední úrovni	Nařizuje	Provádí	Spolupracu
1.	Odeslání žádosti o poskytnutí přednostního připojení na podnikatele zajišťující veřejnou komunikační síť	MV	OPIS MV-GŘ HZS ČR	
2.	Aktivace přednostního připojení		Podnikatelé zajišťující veřejnou komunikační síť	
3.	Podání zpětné informace o aktivaci přednostního připojení		Podnikatelé zajišťující veřejnou komunikační síť	OPIS MV-GŘ HZS ČR

4.	Podání informace o omezení nebo přerušení poskytování veřejně dostupné služby na ČTÚ		Podnikatelé zajišťující veřejnou komunikační síť	
P. č.	**Činnosti na krajské úrovni**	**Nařizuje**	**Provádí**	**Spolupracu**
1.	Zaslání požadavku na aktivaci přednostního připojení na OPIS MV-GŘ HZS ČR	Hejtman	HZS kraje	OPIS MV-GŘ HZS ČR
P. č.	**Činnosti na úrovni obce s rozšířenou působností**	**Nařizuje**	**Provádí**	**Spolupracu**