LATVIJAS REPUBLIKAS
AIZSARDZĪBAS MINISTRIJA

NACIONĀLO BRUŅOTO SPĒKU KIBERAIZSADZĪBAS VIENĪBAS (KAV) KONCEPCIJA

Rīga
2013

Ievads

Saskaņā ar Nacionālās drošības koncepciju viens no aktuālākajiem nacionālās drošības apdraudējuma faktoriem ir informācijas tehnoloģiju apdraudējums jeb pret nacionālās drošības interesēm vērstas darbības elektroniskās informācijas telpā. Apstākļos, kad valsts pārvalde, sabiedrība un ekonomika ir atkarīga no informācijas tehnoloģiju nodrošinātajiem un atbalstītajiem pakalpojumiem, to nelikumīga izmantošana, bojāšana, paralizēšana vai iznīcināšana var radīt draudus valsts un sabiedrības drošībai, sabiedriskajai kārtībai, kā arī var negatīvi ietekmēt valsts ekonomiku.[1]

Valsts aizsardzības koncepcija norāda, ka nākotnē, visticamāk, valsts apdraudējumu radīs uzbrukumi, kas būs dažādi pēc formas un rakstura, savstarpēji saistīti un grūti paredzami. Šie uzbrukumi būs saistīti gan ar tradicionālo karadarbību, gan ar nestandarta karadarbības metodēm, tostarp ar teroristiskām, organizētām noziedzīgām darbībām, kā arī ar uzbrukumiem informācijas tehnoloģijām, informatīvu karu un psiholoģisku iedarbību. Pretinieks spēs darboties, ietekmējot gan fiziski, gan virtuāli, darbojoties uz sauszemes, jūrā, gaisā, kā arī kosmiskajā un elektroniskās informācijas telpā.[2]

Kiberdrošības jautājumi iegūst arvien lielāku aktualitāti arī NATO un ES, kas izstrādā vienotu politiku kiberapdraudējumu izpētei, identificēšanai un novēršanai un pilnveido organizāciju kiberaizsardzības spējas. 2011.gadā NATO apstiprināja Alianses Kiberaizsardzības politiku un izstrādāja detalizētu plānu spēju attīstībai. Starptautiskā prakse liecina, ka, ņemot vērā informācijas tehnoloģiju klātesamību ikvienā nozarē un plašo pielietojamību, valsts resursi ir ierobežoti un nepietiekami liela apjoma draudu novēršanā un krīzes pārvarēšanā. Gan Latvijas kaimiņvalstis, gan pārējās ES un NATO dalībvalstis veido dažādus valsts un privātā jeb civili-militārās sadarbības formātus, lai nodrošinātu rezerves ekspertu iesaisti informācijas tehnoloģiju drošībā un aizsardzībā.

[1] Nacionālās drošības koncepcija, 3.7.pants.
[2] Valsts aizsardzības koncepcija, 11-12.pants.

Latvijā ir izveidota nacionālā informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV, kas ikdienā sniedz atbalstu valsts un pašvaldību iestādēm, komersantiem un fiziskām personām incidentu novēršanā un uztur vienotu valsts elektroniskās informācijas telpā notiekošo darbību atainojumu. Informācijas tehnoloģiju drošības likums nosaka svarīgākās prasības valsts un pašvaldību institūcijām un komersantiem, kā arī CERT.LV pienākumus un uzdevumus miera laikā. Valsts apdraudējuma gadījumā Ministru kabinets var pieņemt lēmumu par CERT.LV uzdevumu, tiesību un resursu nodošanu Nacionālajiem bruņotajiem spēkiem.

Valsts drošības iestādes ir identificējušas kibertelpas kritisko infrastruktūru un īsteno to aizsardzības sistēmas izveidi un uzraudzību saskaņā ar valsts normatīviem aktiem.

Lai arī Latvijā ir izveidotas institūcijas, kas nodrošina nacionālās kiberdrošības spējas, ir izstrādāti un regulāri tiek pilnveidoti plāni rīcībai paaugstināta apdraudējuma gadījumā un sadarbībā ar privāto sektoru ir pieejama ekspertu iesaiste, taču esošo resursu un pasākumu kopums nav pietiekami liels un organizēts, lai efektīvi un ātri rīkotos nopietnos un plašu kiberincidentu jeb kiberuzbrukumu gadījumos.

Ņemot vērā jauno drošības vidi, tajā esošos apdraudējumus un valsts pārvaldes ierobežotos resursus, nepieciešams izveidot ekspertu kopumu kā rezerves vienību, kas apvienotu privātajā sektorā nodarbinātos un iesaistīties gribošus ekspertus, un sadarbībā ar CERT.LV krīzes situācijā vai kara laikā sniegtu atbalstu valstij un privātam sektoram. Zemessarga dienests nodrošina juridisko bāzi un ir veids kā organizēti iesaistīt privātā sektora augsta kvalifikācijas speciālistus valsts aizsardzības uzdevumu izpildei. Patriotiski noskaņotiem informācijas tehnoloģiju ekspertiem ir iespēja brīvprātīgi iesaistīties un, saņemot valsts atbalstu, veidot sadarbību, pilnveidot zināšanas, piedalīties un organizēt kiberuzbrukumu novēršanas mācības un nepieciešamības gadījumā sniegt atbalstu valsts un privātām struktūrām. Šādas vienības izveide gan stiprinātu valsts spējas reaģēt krīzes un kara situācijās, gan arī veicinātu sadarbību starp valsts pārvaldi un privāto sektoru kiberdrošības jomā.

Mērķis, funkcijas un uzdevumi

Lai nodrošinātu rezerves kiberaizsardzības spēju veidošanu valstī, kas būtu izmantojamas, gan civilajiem, gan militārajiem uzdevumiem**, mērķis** ir izveidot Kiberaizsardzības vienību (KAV), kura spētu piesaistīt augsti kvalificētus informācijas tehnoloģijas ekspertus valsts aizsardzības uzdevumu izpildei brīvajā laikā no to pamatdarba.

Kiberaizsardzības vienības **pamatfunkcijas** ir:

1. Sniegt atbalstu CERT.LV un NBS vienībām krīzes un kara situācijās informācijas tehnoloģiju drošības incidentu novēršanā un radušos seku pārvarēšanā kibertelpā, ja CERT.LV rīcībā esošie resursi ir nepietiekami un vienības piesaiste paātrina neatliekamo pasākumu īstenošanu, vai ja tās rīcībā ir speciāli resursi šo darbību veikšanai.
2. Gatavot un nodrošināt zemessargus, kas veido vienību un var sniegt atbalstu CERT.LV un NBS vienībām krīzes un kara situācijās.

Lai sasniegtu mērķi un nodrošinātu funkciju īstenošanu, Kiberaizsardzības vienība veic sekojošus **uzdevumus**:

1. Apzina un rekrutē informācijas tehnoloģiju ekspertus dalībai Kiberaizsardzības vienībā, izstrādā vienības attīstības un darba plānu.
2. Nodrošina piesaistīto zemessargu sākotnējo militāro un tālāko profesionālo apmācību.
3. Plāno, organizē un nodrošina dalību nacionālās un starptautiskā līmeņa mācībās. Regulāri piedalās kiberaizsardzības apmācību procesos NATO, ES, divpusējā un reģionālā formātā, tajā skaitā NATO Izcilības centrā Kiberdrošības jautājumos un organizē regulāru apmācību nacionālajā līmenī.
4. Sadarbībā ar NBS militārā CERT ekspertiem un CERT.LV veido ekspertīzi, piedalās jaunu drošības risinājumu testēšanā un novērtēšanā un sniedz priekšlikumus kiberaizsardzības uzlabošanai.
5. Gatavojas un piedalās NATO, ES vai reģionālo kiberaizsardzības vienību sastāvā vai rezervē.
6. Veicina civili-militāro sadarbību jeb publisko un privāto partnerību kiberaizsardzības jautājumos.

7. Veicina informācijas tehnoloģiju ekspertu un sabiedrības izpratni un zināšanas par kiberapdraudējumiem. Iesaista Jaunsardzi, veicinot jauniešu izglītību un tālāku interesi iesaistīties informācijas tehnoloģiju drošības un aizsardzības jomā.

Vienības izveide

Ņemot vērā esošo normatīvo bāzi, vienību administratīvi vispiemērotāk veidot Zemessardzes ietvaros, bet tās operacionālo pakļautību un darbību organizēt atbilstoši resursu konsolidētai un efektīvai izmantošanai, tajā skaitā maksimāli veicinot pieejamo speciālistu izmantošanu un sadarbību.

Vienības izveidei ir piesaistāmi IT speciālisti, kas atbilst šādiem kritērijiem:

- Zināšanas un prasmes, kas nepieciešamas vienības uzdevumu izpildei;
- Patriotisms un vēlme sniegt ieguldījumu valsts drošības stiprināšanā;
- Atbilstība darbam ar valsts noslēpumu (t.sk. NATO, ES);
- Inovatīvs domāšanas veids, spēja pielāgoties ātri mainīgajai informācijas tehnoloģiju videi;
- Spējas veltīt 1-3 dienas mēnesī apmācībai un dienesta uzdevumu izpildei dienesta vietā vai virtuālā telpā.

IT ekspertu iesaisti vienībā motivēs iespējas:

1) piedalīties starptautiskās mācībās un pasākumos NATO, ES, divpusējos un reģionāla formāta ietvaros un paplašināt savas profesionālās zināšanas;
2) iegūt zināšanas un praktizēt spējas aizsardzības resora informācijas tehnoloģiju vidē sadarbībā ar NBS militārā CERT ekspertiem un piedalīties kiberoperācijās;
3) iepazīties un sadarboties ar starptautiskajiem ekspertiem aizsardzības un drošības jautājumos kibertelpā.

Šādā veidā tiks veicinātas ne tikai valsts struktūru kiberdrošības spējas, bet arī privātajam sektoram būs iespēja pilnveidot savu speciālistu kvalifikāciju un stiprināt uzņēmumu kiberdrošību.

Tālākie soļi, lai uzsāktu vienības izveidi:

1. Izveidot vienības projekta grupu, kuru veido 2–3 eksperti, kuri izstrādā vienības operacionālās spējas un to ieviešanas rīcības plānu.

2. Balstoties uz atlasīto ekspertu ieteikumiem un IT profesionāļu vides vērtējumu, izveidot vismaz 5 augsti kvalificētu informācijas tehnoloģiju speciālistu kopu, kuru papildus savam pamatdarbam piekrīt konsultēt un komentēt vienības izveidošanas rīcības plānu un iecerētos pasākumus.

3. Organizēt tikšanās un prezentācijas augstskolās un lielajos uzņēmumos ar IT specializāciju vai nozīmīgu IT darbības uzturēšanas sektoru, informējot par vienības izveidi, tās uzdevumiem un potenciālajiem ieguvumiem vienības dalībniekiem.

4. Izveidot tiešus un nepārtrauktus kontaktus jeb regulāru sadarbību ar lielajiem uzņēmumiem, kuru tīkliem un sistēmām tradicionāli ir augsts apdraudējums un līdz ar to arī strādā augstākas kvalifikācijas speciālisti (bankas, elektronisko sakaru pakalpojumu sniedzēji, transporta uzņēmumi u.c.), aicinot iesaistīties vienības darbībā un piedāvājot mācību scenārijos iekļaut ar konkrētā uzņēmuma darbības sfēru saistītos riska faktorus.

5. Apzināt un iesaistīt no profesionālā militārā dienesta atvaļinātos speciālistus, piedāvājot iespēju saglabāt saikni ar militāro vidi, kas saistīta ar viņu pamatprofesiju.

6. Iesaistīt vienības darbībā Latvijas augstskolu IT programmu studentus, piedāvājot militāro kiberapmācību, tādējādi gatavojot potenciālos vienības IT speciālistus.

Vienības izveide un dalībnieku piesaiste tiek organizēta sadarbībā ar CERT.LV un tās ietvaros izveidoto IT/IS Drošības ekspertu grupu.

Vienības darbība

Vienības darbs tiek organizēts gan virtuālā telpā, gan regulāri tiekoties, kā arī organizējot un piedaloties nacionālās vai starptautiskās apmācībās.

Atkarībā no operacionālās nepieciešamības jeb specializācijas, vienības eksperti tiks sadalīti grupās, piemēram, pildot ātrās reaģēšanas grupas, kiberlaboratorijas

personāla vai grupu līderu pienākumus. Ņemot vērā nelielo plānoto profesionālā dienesta (pilna laika) karavīru skaitu vienībā, tās iekšējā struktūra un pienākumu sadale jābalsta uz ekspertiem, kas ir viedokļu un ekspertīzes līderi savā jomā un spējīgi ap sevi pulcināt IT profesionāļus ar līdzīgu specializāciju. Šāda koncepta piemērošana ir sevi pierādījusi citu valstu vienībās, kad noteikta uzdevuma pildīšanai tiek komplektēta ar formālo struktūru nesaistīta grupa, kas sevī iekļauj visu nepieciešamo ekspertīzi un atbalstu.

Lai gan nozīmīgākā IT ekspertu atrašanās vieta ir Rīga, tomēr vienības elementus plānots attīstīt arī reģionu centros, izskatot iespējas par bāzi izmantot augstākās mācību iestādes, kas piedāvā IT specialitāšu programmas.

KAV spēju izveide ir plānota piecu gadu periodā, kur:

- 2015.gada sākumā vienība sasniegs sākotnējās operacionālās spējas;
- 2018.gada sākumā vienība sasniegs pilnas operacionālas spējas.

Tālākās darbības:

1. Uzsākt īstenot dokumentā noteiktos soļus vienības izveidošanai.

2. Apzināt un piesaistīt starptautisko un nacionālo pieredzi, lai vienības veidošanas laikā detalizēti izstrādātu un tālāk attīstītu kiberaizsardzības vienības rezervistu ideju.