

## **Informacinės visuomenės plėtros komiteto kibernetinio saugumo skyriaus uždaviniai ir funkcijos**

Pagrindiniai skyriaus uždaviniai yra šie:

1. užtikrinti nepertraukiamą kibernetinio saugumo įvykių stebėjimą, kontrolę, reagavimą, paklausimų, incidentų ir kitų užklausų analizę, vertinimą, tyrimą, sprendimą arba jų priskyrimą ir sprendimo kontrolę, koordinavimą, rengti pranešimus ir ataskaitas, analizuoti ir kaupti įrodymus bei išvadas;
2. užtikrinti kibernetinį saugumą, vykdant debesijos paslaugų teikėjo funkcijas bei užtikrinti valstybės informacinių išteklių infrastruktūros konsolidavimą ir valstybės informaciniams ištekliams talpinti skirtų patalpų naudojimą, užtikrinti žmogiškuosius išteklius, kurių reikia informacinių technologijų paslaugoms (toliau – IT paslaugos) teikti;
3. užtikrinti konsoliduotos valstybės informacinių išteklių infrastruktūros (toliau – IRT infrastruktūra) kibernetinį saugumą.

Skyrius, įgyvendindamas jam pavestus uždavinius, siekdamas ir užtikrinti kibernetinį saugumą teikiant IT paslaugas, atlieka šias funkcijas:

1. pagal skyriaus kompetenciją užtikrina kibernetinį saugumą, vykdant IT paslaugų nepertraukiamą teikimą ir palaikymą, vadovaujantis paslaugų teikimo sutartyse (angl. Service Level Agreement) nustatytais kriterijais, kiekybiniais bei kokybiniais rodikliais;
2. renka, apdoroja ir analizuoja informaciją, būtiną teikiamų IT paslaugų ir IRT infrastruktūros nepertraukiamo veikimo, administravimo bei saugos užtikrinimui, nedelsiant reaguoja į aptiktus incidentus, problemas, trikdžius bei grėsmes, nuolat vykdo IT paslaugų ir IRT infrastruktūros efektyvumo bei saugumo gerinimo prevenciją;
3. visų skambučių ir elektroninių užklausų (incidentų, problemų, trikdžių, pokyčio prašymų ir pan.) priėmimas, valdymas, klasifikavimas, prioretizavimas, pagal kompetenciją sprendimas ir/arba nukreipimas trečio lygio specialistams, informavimas apie užklausų sprendimo eigą, užklausų uždarymas;
4. užklausų (incidentų, problemų, trikdžių, pokyčio prašymų ir pan.) sprendimas/atsakymas ir/arba nukreipimas kitų lygių specialistams, informavimas apie priskirtų užklausų sprendimo eigą, užklausų eskalavimas ir uždarymas;
5. pagal skyriaus kompetenciją teikia IT paslaugų gavėjams konsultacijas, prireikus organizuoja IT paslaugų gavėjų mokymus;
6. pagal skyriaus kompetenciją dirba su kibernetinio saugumo ir IT paslaugų valdymo sistemomis (angl. SIEM, PAM, ITSM) ir su ją susijusių veiklos procesų: analizavimą, planavimą, diegimą, administravimą, priežiūrą ir plėtrą;
7. pagal skyriaus kompetenciją nuolat renka ir analizuoja informaciją apie kibernetinio saugumo įvykius, paklausimus ir incidentus, registruoja, sprendžia, koordinuoja ir eskaluoja užklausas, analizuoja ir inicijuoja technines ir organizacines priemones, teikia Komiteto direktoriui, siūlymus dėl kibernetinio saugumo užtikrinimo;
8. pagal skyriaus kompetenciją nuolat renka ir analizuoja informaciją dėl kibernetinio saugumo ir IT paslaugų valdymo sistemų plėtros, tobulinimo bei tam skirtų lėšų efektyvesnio panaudojimo;
9. pagal skyriaus kompetenciją užtikrina teikiamų IT paslaugų ir IRT infrastruktūros kibernetinį saugumą, rengia ataskaitas (kibernetinio saugumo, IT paslaugų kokybės, reagavimo į užklausas bei jų sprendimo ir pan.), teikia pasiūlymus dėl gerinimo;

10. pagal skyriaus kompetenciją rengia kibernetinio saugumo užtikrinimui būtinos įrangos ir paslaugų pirkimo technines specifikacijas bei dalyvauja vykdant viešuosius pirkimus;
11. pagal skyriaus kompetenciją dalyvauja Komiteto komisijų, darbo grupių veikloje;
12. pagal skyriaus kompetenciją teisės aktų nustatyta tvarka rengia ir skleidžia informaciją apie Komiteto veiklą;
13. pagal skyriaus kompetenciją atstovauja Komitetui priskirtais klausimais;
14. užtikrina, kad skyriaus gaunami ir rengiami dokumentai būtų tinkamai saugomi;
15. sudaro skyriui pagal dokumentacijos planą priskirtas bylas;
16. pagal skyriaus kompetenciją vykdo kitas teisės aktais Komitetui nustatytas funkcijas ir Komiteto direktoriaus pavedimus.