INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az Ukrán Országos Önkormányzat, az
Ukrán Országos Önkormányzat
Hivatala és a Magyar Ukrán Kulturális
és Dokumentációs Központ
együttes szabályzata
Leszja Ukrajinka Ukrán Kiegészítő Nemzetiségi
Nyelvoktató Iskola

2024.

Tartalomjegyzék

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Jogszabályi környezet:

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről
  41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

1. Az Informatikai Biztonsági Szabályzat célja

Az Ukrán Országos Önkormányzat az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatokat az alábbi szabályzat szerint határozza meg.

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésén keresztül az üzemeltetésig.
A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed az Ukrán Országos Önkormányzatra, az Ukrán Országos Önkormányzat Hivatalára, (továbbiakban: Hivatal), a Magyar Ukrán Kulturális és Dokumentációs Központ (továbbiakban: **MUKDK) és a** Leszja Ukrajinka Ukrán Kiegészítő Nemzetiségi Nyelvoktató Iskola alkalmazottjaira, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az Önkormányzat, a Hivatal, a **MUKDK és a** Leszja Ukrajinka Ukrán Kiegészítő Nemzetiségi Nyelvoktató Iskola tulajdonában lévő, illetve az általa használt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

Az Ukrán Országos Önkormányzat és Intézményei adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a Hivatal belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:
- Leltározási és értékelési szabályzattal,
- Számviteli politikával

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:

a környezeti infrastruktúra,
a hardver elemek,
az adathordozók,
a dokumentumok,
a szoftver elemek,
az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:
- az alkalmazott hardver eszközökre és azok működési biztonságára,

- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,

6.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

7. A védelem felelőse

Jelen szabályzatban foglaltak szakszerű végrehajtásáról az Ukrán Országos Önkormányzat, Hivatalának és Intézményeinek vezetői, mint adatvédelmi felelősek gondoskodnak.

Adatvédelmi felelős feladatai

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi feladatok ismertetése,
- ellenőrzi a szoftverek használatának jogszerűségét
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős az informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása a vezetők feladata.

8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

1. - közlésre szánt, bárki által megismerhető adatok,
2. - minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője az intézmény vezetője.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.
A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.
Az adatok védelmét, a feldolgozás - az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal biztosítani kell (szoftver, hardver adatvédelem). Ennek biztosítása a rendszergazda feladata.

9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

9.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.
- környezeti kár:
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,

- csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

10.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

10.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,

- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök környezetének védelme

11.1. Vagyonvédelmi előírások

- az informatikai eszközöket csak az Ukrán Országos Önkormányzat, az Önkormányzat intézményei és a Hivatal arra felhatalmazott alkalmazottai használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.2. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (pl. CD) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.3. Tűzvédelem

Az intézmények Tűzvédelmi Szabályzatai szerint.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
Az üzemeltetést, karbantartást és szervizelést az erre a feladatra megbízott szakember végzi.
A munkák szervezésénél figyelembe kell venni:
- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak az erre a feladatra megbízott szakember végezheti el.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
    - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).

12.3.2. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

12.3.3. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

12.3.4. Selejtezés, sokszorosítás, másolás

A selejtezést a Hivatal selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni.
Biztonsági illetve archív adatállomány előállítása másolásnak számít.

12.3.5. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.6. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a megbízott szakembernek kell készítenie, aki az archiválásban is segítséget nyújt.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

A Hivatal vezetőjének biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

12.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a Hivataloknak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.
A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.
A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

13. A munkaállomások működésbiztonsága

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén a megbízott informatikust azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
Az önkormányzat és intézményei informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását a Hivatal vezetője ellenőrzi.

15. Záró rendelkezések

Az Ukrán Országos Önkormányzat Közgyűlése az Ukrán Országos Önkormányzat, az Ukrán Országos Önkormányzat Hivatala a MUKDK és a Leszja Ukrajinka Ukrán Kiegészítő Nemzetiségi Nyelvoktató Iskola Informatikai Biztonsági Szabályzatát __/2024. (__.__.) **UOÖ sz. határozatával** elfogadta.

Jelen szabályzat 2024. január 02-napjától hatályos, mellyel egy időben a korábbi közérdekű adatok megismerése szabályzat hatályát veszti

Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Budapest, 2024. január 02.

Szabó Jaroszlava
Ukrán Országos Önkormányzat
elnök

UKRÁN ORSZÁGOS ÖNKORMÁNYZAT HIVATALA
Управління державного самоврядування українців Угорщини
1065 Budapest, Hajós u. 1.
Adószám: 15769118-1-42

Fotiadisz Szavvasz
Ukrán Országos Önkormányzat Hivatal
megbízott hivatalvezető

Magyarországi Ukrán Kulturális és Dokumentációs Központ
Центр Української Культури та Документації в Угорщині
1065 Budapest, Hajós u. 1.

Sipajlo Igor
Magyar Ukrán Kulturális
Dokumentációs Központ

Bernáth Viktória
Leszja Ukrajinka Ukrán Kiegészítő
Nemzetiségi Nyelvoktató Iskola

1. sz. melléklet

Az Ukrán Országos Önkormányzat és Intézményei biztonsági osztályba sorolása

1. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolása

1. Általános irányelvek

1.1. Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;

1.1.1. a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;

1.1.2. a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;

1.1.3. a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

2. Biztonsági osztályok

2.1. A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége. A 2.2.-2.6. pontok a döntéshez csak iránymutatást képeznek:

2.2. Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel

2.2.1. az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;

2.2.2. nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;

2.2.3. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;

2.3. A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel

2.3.1. személyes adat sérülhet;

2.3.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;

2.3.3. a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;

2.3.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.

2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel

2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;

2.4.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;

2.4.3. a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;

2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.

2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel

2.5.1. különleges személyes adat nagy mennyiségben sérülhet;

2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);

2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;

2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;

2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

2.6. Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel

2.6.1. különleges személyes adat kiemelten nagy mennyiségben sérülhet;

2.6.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban

következhetnek be;

2.6.3. a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;

2.6.4. az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;

2.6.5. a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

2.6.6. az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;

2.6.7. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

1. Biztonsági osztályok
Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerint a besorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége, az alábbiak a döntéshez csak szempontokat jelentenek:

Az Ukrán Országos Önkormányzat és Intézményei biztonsági osztályba sorolási szintje:
2. biztonsági osztály
A 2. biztonsági osztály esetében **csekély káresemény** következhet be, mivel
személyes adat sérülhet;
az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

2. sz. melléklet

2. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása

1. Az érintett szervezet biztonsági szintje 1., ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre - ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését - nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.1. Az 1. biztonsági szervezeti szint követelményei:

1.1.1. az érintett szervezet az érintett személyi kör részére biztosítja az 1.1.3. pont szerinti szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat);

1.1.2. az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;

1.1.3. az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre vagy szervezeti egységre;

1.1.4. a informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia;

1.1.5. a informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;

1.1.6. az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.

2. Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

2.1. A 2. biztonsági szervezeti szint követelményei az 1. szinthez rendelt követelményeken túl:

2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;

2.1.2. a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;

2.1.3. az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;

2.1.4. az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel;

2.1.5. a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.

3. Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.

3.1. A 3. biztonsági szervezeti szint követelményei a 2. szinthez rendelt követelményeken túl:

3.1.1. az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;

3.1.2. a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;

3.1.3. a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni vagy eseti eljárásokra;

3.1.4. a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;

3.1.5. a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;

3.1.6. a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

4. Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

4.1. A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:

4.1.1. az üzemeltetési vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;

4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;

4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is;

4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;

4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;

4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni;

4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;

4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.

5. Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.

5.1. A 5. biztonsági szervezeti szint követelményei a 4. szinthez rendelt követelményeken túl:

5.1.1. biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését;

5.1.2. biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát és továbbfejlesztését;

5.1.3. a szervezetnek rendelkeznie kell átfogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonságtudatosságának növelését;

5.1.4. a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;

5.1.5. a biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani;

5.1.6. a fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok felülvizsgálatával nyomon kell követni információbiztonsági környezet változását;

5.1.7. az információbiztonságot érintő külső vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni;

5.1.8. a szervezetnek ki kell alakítania az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meg kell határozni annak mutatóit és 5.1.7. pont szerinti esetben aktualizálnia kell azt.

3. melléklet

A Szabályzat 7. pontjához:

A védelem felelősei

1. Informatikai vezető: a Hivatal vezetője

2. A védelem felelőse az Ukrán Országos Önkormányzat által szerződéssel megbízott rendszergazdája