



## МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Повітрофлотський пр-т, 6, м. Київ, 03168, тел.: (044) 234-71-52, факс: (044) 226-20-15  
E-mail: kabmin\_doc@mil.gov.ua, сайт: www.mil.gov.ua, код згідно ЄДРПОУ 00034022

від \_\_\_\_\_ 20 \_\_ р. № \_\_\_\_\_

На № \_\_\_\_\_ від \_\_\_\_\_ 20 \_\_ р.

Голові Верховної Ради України  
Дмитру РАЗУМКОВУ

На № 11/10-748 від 05.06.2020

Шановний пане Дмитре!

У Міністерстві оборони України розглянуто лист Першого заступника Голови Верховної Ради України щодо депутатського запиту народного депутата України Федієнка О.П. стосовно надання інформації про стан проведення аудиту інформаційної безпеки та стану кіберзахисту на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління, а саме телекомунікаційних та інформаційно-телекомунікаційних мереж (систем), які як взаємодіють з публічними мережами, так і не підключені до мережі Інтернет або інших глобальних мереж передачі даних.

За результатами опрацювання надаю інформацію згідно із запитом (додаток 1).

Водночас повідомляю, що незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури Міністерства оборони України та Збройних Сил України, передбачений Законом України "Про основні засади забезпечення кібербезпеки України", не проводився у зв'язку з відсутністю нормативно-правових актів Кабінету Міністрів України, якими мав би регламентуватися порядок його проведення.

Аудит інформаційної безпеки елементів інформаційно-телекомунікаційних систем Збройних Сил України постійно проводиться Департаментом внутрішнього аудиту Міністерства оборони України (додаток 2).

Також у листопаді 2019 року Державною службою спеціального зв'язку та захисту інформації України проводилася цільова перевірка стану технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-телекомунікаційних системах Генерального штабу Збройних Сил України, за результатами якої отримано Акт



перевірки від Адміністрації Держспецзв'язку (гриф обмеження доступу – таємно).

З метою підвищення ефективності забезпечення кібербезпеки у Міністерстві оборони України та Збройних Силах України Командуванням Військ зв'язку та кібербезпеки Збройних Сил України організовано проведення внутрішнього аудиту інформаційної безпеки військових частин (підрозділів). Внутрішній аудит проводився визначеним особовим складом підрозділів, які безпосередньо відповідальні за забезпечення кібербезпеки у Збройних Силах України (додаток 3).

Народного депутата України поінформовано.

Додаток: 1. Інформація про стан проведення аудиту інформаційної безпеки та стану кіберзахисту на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління на 2 арк., відкрита інформація.

2. Відомості щодо аудиту інформаційної безпеки елементів інформаційно-телекомунікаційних систем Збройних Сил України на 1 арк., відкрита інформація.

3. Відомості щодо особового складу, який проводив внутрішній аудит інформаційної безпеки військових частин (підрозділів) на 1 арк., відкрита інформація.

З повагою

Міністр оборони України



Андрій ТАРАН



## ІНФОРМАЦІЯ

про стан проведення аудиту інформаційної безпеки та стану кіберзахисту на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління

## 1. Перелік мереж, призначення та основні сервіси.

## 1.1. Інформаційна система з доступом до мережі Інтернет (ІСД-Інтернет).

Призначення: ІСД-Інтернет призначена для доступу посадових та службових осіб Міністерства оборони України та Збройних Сил України до інформаційних ресурсів мережі Інтернет, оприлюднення в мережі Інтернет інформації про діяльність Міністерства оборони України та Збройних Сил України, обміну відкритою інформацією через мережу Інтернет у службових цілях.

Основні сервіси: mail, web.

## 1.2. Автоматизована система управління Збройних Сил України "Дніпро".

Призначення: АСУ "Дніпро" призначена для забезпечення роботи командирів, начальників і службових осіб Міністерства оборони України та Збройних Сил України по управлінню підпорядкованими органами управління, військовими частинами та організаціями за рахунок автоматизації процесів приймання, обробки, відображення, документування та передачі інформації в повсякденній діяльності Збройних Сил України, а також для виконання покладених завдань і функцій. Основними завданнями АСУ "Дніпро" є забезпечення: автоматизації ведення діловодства та електронного документообігу відповідно до вимог чинних нормативних документів; обміну повідомленнями, в тому числі документальними; вирішення завдань планування окремих видів забезпечення; вирішення окремих завдань інформаційно-аналітичної підтримки діяльності органів військового управління; організації та управління функціонуванням АСУ "Дніпро"; контролю за виконанням завдань відповідними органами військового управління.

Основні сервіси: mail, web.

## 1.3. Мережі ЗСУ001, ЗСУ002.

Мережі ЗСУ001 та ЗСУ002 належать до систем спеціального зв'язку. Порядок створення та підтвердження відповідності комплексних систем захисту інформації в цих системах відбувається згідно з Порядком створення комплексних систем захисту інформації в системах спеціального зв'язку, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.10.2018 № 141/ДСК.

## 2. Класифікація та функціональні профілі захищеності та їх семантики відповідно до НД ТЗІ 2.5-005-99.

Функціональні профілі захищеності інформації в АРМ ІСД-Інтернет від несанкціонованого доступу включають такий набір послуг:

КД-2, КО-1, ЦД-1, ЦО-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2.



Функціональні профілі захищеності інформації в АРМ АСУ ЗС України "Дніпро" від несанкціонованого доступу мають включати набір послуг, не нижчий, ніж:

КД-2, КО-0, ЦД-1, ЦО-1, ЦВ-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2.

3. Перелік документів на підставі яких мережі (системи) класифіковано та визначено профілі:

Типове технічне завдання на створення комплексної системи захисту інформації автоматизованого робочого місця інформаційної системи з доступом до мережі Інтернет, що призначене для обробки відкритої інформації, яка належить до державних інформаційних ресурсів, затверджене начальником Генерального штабу – Головнокомандувачем Збройних Сил України 24.03.2015;

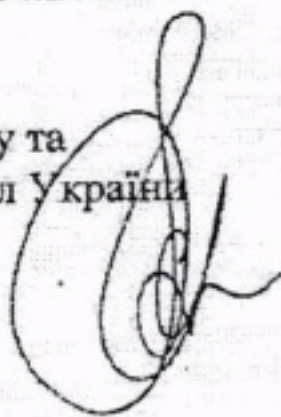
Типове технічне завдання на створення КСЗІ автоматизованих робочих місць автоматизованої системи управління Збройних Сил України "Дніпро", що призначене для обробки відкритої інформації, затверджене начальником Генерального штабу – Головнокомандувачем Збройних Сил України 27.12.2010.

4. Методики, за якими здійснювався аудит, його результати та списки осіб, які безпосередньо проводили аудит:

Міжнародне керівництво по аудиту (COBIT Audit Guideline), яким визначаються правила щодо використання концептуального ядра і основних принципів управління COBIT під час проведення аудиту в сфері інформаційних технологій;

Тимчасова методика проведення аудиту інформаційної безпеки військових частин (підрозділів) щодо ефективності забезпечення кібербезпеки, розроблена Військовим інститутом телекомунікацій та інформатизацій імені Героїв Крут та затверджена Командувачем Військ зв'язку та кібербезпеки Збройних Сил України 24.04.2020.

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор



Євген СТЕПАНЕНКО



**ВІДОМОСТІ**  
щодо аудиту інформаційної безпеки елементів інформаційно-  
телекомунікаційних систем Збройних Сил України

№ п/п	Найменування структурного підрозділу (військової частини)	Хто здійснював перевірку	Номер акту та дата
1.	Головне управління зв'язку та інформаційних систем Генерального штабу Збройних сил України		234/6/40/1 від 26.02.2019
2.	Управління розвитку та автоматизації Збройних сил України		
3.	Центральна телерадіостудія		234/40/1 від 30.01.2019
4.	Центральний друкарський орган Міністерства оборони України газета "Народна армія"		234/6/40/2 від 28.02.2019
5.	Центральний спортивний клуб		234/6/40/15 від 16.07.2019
6.	Центральний друкарський орган Міністерства оборони України журнал "Військо України"		234/6/40/2 від 16.07.2019
7.	Військова частина А3519		234/3968 від 04.11.2019
8.	Національний військово-медичний клінічний центр "ГВКІ"		234/4631 від 21.12.2019
9.	Військова частина А0351		2187/3 від 10.02.2020
10.	Військова частина А4362		234/3968 від 04.11.2019

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор

Євген СТЕПАНЕНКО

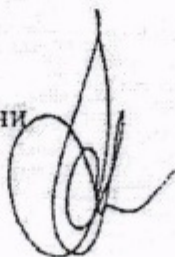


## ВІДОМОСТІ

щодо особового складу, який проводив внутрішній аудит інформаційної безпеки військових частин (підрозділів)

№ п/п	Військове звання	Прізвище, ім'я, по батькові	Посада
1.	полковник		Начальник центру кібернетичної безпеки інформаційно-телекомунікаційних систем – заступник командира військової частини А0334
2.	підполковник		Начальник центру безпеки інформації військової частини А0334
3.	підполковник		Начальник 3 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
4.	підполковник		Начальник 7 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
5.	підполковник		Начальник 8 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
6.	підполковник		Начальник 4 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
7.	підполковник		Начальник 6 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
8.	підполковник		Начальник 9 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор



Євген СТЕПАНЕНКО



## ІНФОРМАЦІЯ

про стан проведення аудиту інформаційної безпеки та стану кіберзахисту на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління

## 1. Перелік мереж, призначення та основні сервіси.

## 1.1. Інформаційна система з доступом до мережі Інтернет (ІСД-Інтернет).

Призначення: ІСД-Інтернет призначена для доступу посадових та службових осіб Міністерства оборони України та Збройних Сил України до інформаційних ресурсів мережі Інтернет, оприлюднення в мережі Інтернет інформації про діяльність Міністерства оборони України та Збройних Сил України, обміну відкритою інформацією через мережу Інтернет у службових цілях.

Основні сервіси: mail, web.

## 1.2. Автоматизована система управління Збройних Сил України "Дніпро".

Призначення: АСУ "Дніпро" призначена для забезпечення роботи командирів, начальників і службових осіб Міністерства оборони України та Збройних Сил України по управлінню підпорядкованими органами управління, військовими частинами та організаціями за рахунок автоматизації процесів приймання, обробки, відображення, документування та передачі інформації в повсякденній діяльності Збройних Сил України, а також для виконання покладених завдань і функцій. Основними завданнями АСУ "Дніпро" є забезпечення: автоматизації ведення діловодства та електронного документообігу відповідно до вимог чинних нормативних документів; обміну повідомленнями, в тому числі документальними; вирішення завдань планування окремих видів забезпечення; вирішення окремих завдань інформаційно-аналітичної підтримки діяльності органів військового управління; організації та управління функціонуванням АСУ "Дніпро"; контролю за виконанням завдань відповідними органами військового управління.

Основні сервіси: mail, web.

## 1.3. Мережі ЗСУ001, ЗСУ002.

Мережі ЗСУ001 та ЗСУ002 належать до систем спеціального зв'язку. Порядок створення та підтвердження відповідності комплексних систем захисту інформації в цих системах відбувається згідно з Порядком створення комплексних систем захисту інформації в системах спеціального зв'язку, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.10.2018 № 141/ДСК.

## 2. Класифікація та функціональні профілі захищеності та їх семантики відповідно до НД ТЗІ 2.5-005-99.

Функціональні профілі захищеності інформації в АРМ ІСД-Інтернет від несанкціонованого доступу включають такий набір послуг:

КД-2, КО-1, ЦД-1, ЦО-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2.



Функціональні профілі захищеності інформації в АРМ АСУ ЗС України "Дніпро" від несанкціонованого доступу мають включати набір послуг, не нижчий, ніж:

КД-2, КО-0, ЦД-1, ЦО-1, ЦВ-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2.

3. Перелік документів на підставі яких мережі (системи) класифіковано та визначено профілі:

Типове технічне завдання на створення комплексної системи захисту інформації автоматизованого робочого місця інформаційної системи з доступом до мережі Інтернет, що призначене для обробки відкритої інформації, яка належить до державних інформаційних ресурсів, затверджене начальником Генерального штабу – Головнокомандувачем Збройних Сил України 24.03.2015;

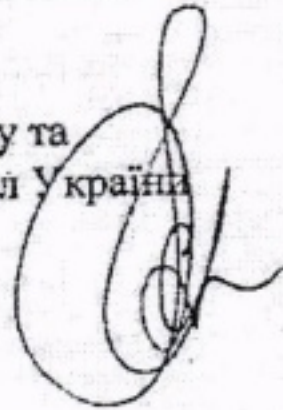
Типове технічне завдання на створення КСЗІ автоматизованих робочих місць автоматизованої системи управління Збройних Сил України "Дніпро", що призначене для обробки відкритої інформації, затверджене начальником Генерального штабу – Головнокомандувачем Збройних Сил України 27.12.2010.

4. Методики, за якими здійснювався аудит, його результати та списки осіб, які безпосередньо проводили аудит:

Міжнародне керівництво по аудиту (COBIT Audit Guideline), яким визначаються правила щодо використання концептуального ядра і основних принципів управління COBIT під час проведення аудиту в сфері інформаційних технологій;

Тимчасова методика проведення аудиту інформаційної безпеки військових частин (підрозділів) щодо ефективності забезпечення кібербезпеки, розроблена Військовим інститутом телекомунікацій та інформатизацій імені Героїв Крут та затверджена Командувачем Військ зв'язку та кібербезпеки Збройних Сил України 24.04.2020.

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор



Євген СТЕПАНЕНКО



**ВІДОМОСТІ**  
щодо аудиту інформаційної безпеки елементів інформаційно-  
телекомунікаційних систем Збройних Сил України

№ п/п	Найменування структурного підрозділу (військової частини)	Хто здійснював перевірку	Номер акту та дата
1.	Головне управління зв'язку та інформаційних систем Генерального штабу Збройних сил України		234/6/40/1 від 26.02.2019
2.	Управління розвитку та автоматизації Збройних сил України		
3.	Центральна телерадіостудія		234/40/1 від 30.01.2019
4.	Центральний друкарський орган Міністерства оборони України газета "Народна армія"		234/6/40/2 від 28.02.2019
5.	Центральний спортивний клуб		234/6/40/15 від 16.07.2019
6.	Центральний друкарський орган Міністерства оборони України журнал "Військо України"		234/6/40/2 від 16.07.2019
7.	Військова частина А3519		234/3968 від 04.11.2019
8.	Національний військово- медичний клінічний центр "ГВКГ"		234/4631 від 21.12.2019
9.	Військова частина А0351		2187/3 від 10.02.2020
10.	Військова частина А4362		234/3968 від 04.11.2019

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор

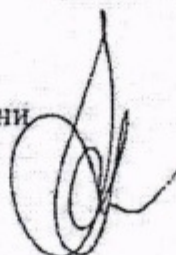
Євген СТЕПАНЕНКО



**ВІДОМОСТІ**  
щодо особового складу, який проводив внутрішній аудит інформаційної  
безпеки військових частин (підрозділів)

№ п/п	Військове звання	Прізвище, ім'я, по батькові	Посада
1.	полковник		Начальник центру кібернетичної безпеки інформаційно-телекомунікаційних систем – заступник командира військової частини А0334
2.	підполковник		Начальник центру безпеки інформації військової частини А0334
3.	підполковник		Начальник 3 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
4.	підполковник		Начальник 7 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
5.	підполковник		Начальник 8 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
6.	підполковник		Начальник 4 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
7.	підполковник		Начальник 6 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
8.	підполковник		Начальник 9 центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах

Командувач Військ зв'язку та  
кібербезпеки Збройних Сил України  
генерал-майор



Євген СТЕПАНЕНКО



Апарат Верховної Ради України  
КАРТКА ДОКУМЕНТА



155588

Кореспонденти Таран А. В. Міністерство оборони України (всього 1)  
Вид документа Відповідь на депутатський запит  
Вих. № та дата 220/4386 від 25.07.2020  
кореспондента № ДСК  
Реєстр. № та 119042 від 27.07.2020  
дата реєстрації  
Арк./прим. 10/1  
Стислий зміст На №11/10-748 05.06.2020 Відповідь на запит н.д. Федієнка О.П. щодо результатів розгляду питання стосовно проведення аудиту діяльності у сфері кібербезпеки

Проходження документа (особа, у якої є позначка «Оригінал»)	Дата передачі оригіналу ВСК	Дата отримання оригіналу	Підпис