

Державна служба України з надзвичайних ситуацій  
Львівський державний університет безпеки життєдіяльності  
Навчально-науковий інститут цивільного захисту  
Кафедра управління інформаційною безпекою

«Допущено до захисту»  
Начальник кафедри управління  
інформаційною безпекою, д.т.н.,  
полковник служби цивільного захисту

\_\_\_\_\_ Ростислав ТКАЧУК  
“ \_\_\_\_ ” \_\_\_\_\_ 2021 року

## ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Аналіз та забезпечення інформаційного захисту приміщення  
засідань ГУ ДСНС у Миколаївській області від витоку інформації  
технічними каналами

Виконав:  
здобувач IV курсу, групи КБ-41  
спеціальності (освітньої програми)  
125 «Кібербезпека» (Управління  
інформаційною безпекою)  
(шифр і назва спеціальності (освітньої програми))  
Олександра ГОРЖІЄВСЬКА  
(прізвище та ініціали)

Керівник Ростислав ТКАЧУК  
(прізвище та ініціали)

Рецензент Наталя ЛИСА  
(прізвище та ініціали)

Львів – 2021 року

## АНОТАЦІЯ

Мета даної дипломної роботи - дослідження інформаційного захисту приміщення залу засідань ГУ ДСНС у Миколаївській області від витоку інформації технічними каналами.

У першому розділі опис теоретичної частини, що стосується інформації, каналів її витоку та технічного захисту.

У другому розділі розглядається інформаційний захист приміщення залу засідань від витоку інформації технічними каналами, згідно нормативних документів та засвоєного матеріалу під час навчання.

У третьому розділі розглядаються необхідні заходи та засоби для забезпечення інформаційного захисту приміщення залу засідань.

За результатами дипломної роботи зроблено висновки та пропозиції. З метою покращення інформаційного захисту приміщення залу засідань, необхідно вжити такі заходи: підвищення звукоізоляції та створити комплекс технічного захисту інформації, який обов'язково повинен пройти атестацію.

## **ABSTRACT**

The purpose of this thesis is to study the information protection of the meeting room of the State Emergency Service in the Nikolaev region from information leakage through technical channels.

The first section describes the theoretical part concerning information, its sources of leakage and technical protection.

The second section considers the information protection of the meeting room from information leakage through technical channels, according to regulations and the material learned during training.

The third section discusses the necessary measures and tools to ensure information security of the meeting room.

Based on the results of the thesis, conclusions and suggestions were made. In order to improve the information protection of the meeting room, it is necessary to take the following measures: increase sound insulation and create a complex of technical protection of information, which must be certified.

## ЗМІСТ

ВСТУП..... **Помилка! Закладку не визначено.**

1.2. ЗАСОБИ ДЛЯ ВИЯВЛЕННЯ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ.....9

1.3. ЗАСОБИ ЗАХИСТУ АКУСТИЧНОГО КАНАЛУ.. **Помилка! Закладку не визначено.**

РОЗДІЛ 2. АНАЛІЗ ПРИМІЩЕННЯ ЗАЛУ ЗАСІДАНЬ . **Помилка! Закладку не визначено.**

2.1. ДЕТАЛЬНИЙ ОПИС ОБ'ЄКТУ ЗАХИСТУ І ВИДІВ ІНФОРМАЦІЇ, ЩО ОПРАЦЬОВУЄТЬСЯ І ЗБЕРІГАЄТЬСЯ НА ОБ'ЄКТІ . **Помилка! Закладку не визначено.**

2.2. ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ..... **Помилка! Закладку не визначено.**

ПЛАН-СХЕМИ ОІД:..... **Помилка! Закладку не визначено.**

2.3. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ..... **Помилка! Закладку не визначено.**

2.4. КАЛЕНДАРНИЙ ПЛАН РОБІТ ЩОДО СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ..... **Помилка! Закладку не визначено.**

2.5. ЗДІЙСНЕННЯ КАТЕГОРІЮВАННЯ ПРИМІЩЕННЯ ЗАЛУ ЗАСІДАНЬ ..... **Помилка! Закладку не визначено.**

2.6. ЗДІЙСНЕННЯ ОБСТЕЖЕННЯ ПРИМІЩЕННЯ ЗАЛУ ЗАСІДАНЬ ..... **Помилка! Закладку не визначено.**

2.7. МОДЕЛЬ ЗАГРОЗ ..... **Помилка! Закладку не визначено.**

2.8. МОЖЛИВІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ У ПРИМІЩЕННІ ЗАЛУ ЗАСІДАНЬ ..... **Помилка! Закладку не визначено.**

РОЗДІЛ 3. ВИБІР НЕОБХІДНИХ ЗАХОДІВ ТА ЗАСОБІВ ЗАХИСТУ ПРИМІЩЕННЯ ЗАЛУ ЗАСІДАНЬ ..... **Помилка! Закладку не визначено.**

3.1. ПРОВЕДЕННЯ РОБІТ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ .. **Помилка! Закладку не визначено.**

3.2. РОЗРОБЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ ..... **Помилка! Закладку не визначено.**

3.3. ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ ЗАХОДІВ ЗАХИСТУ НА  
ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ..... **Помилка! Закладку не визначено.**

3.4. ПЕРЕЛІК ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЗАХИСТУ НА ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.....	<b>Помилка! Закладку не визначено.</b>
3.5. ПЕРЕЛІК ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ НА ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ. ....	<b>Помилка! Закладку не визначено.</b>
3.5.1. ВИБІР ФІЗИЧНОГО ЗАХИСТУ. ФОТО, КОРОТКИЙ ОПИС, ЗАСТОСУВАННЯ.....	<b>Помилка! Закладку не визначено.</b>
3.5.2. ВИБІР КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ФОТО, КОРОТКИЙ ОПИС, ЗАСТОСУВАННЯ .....	<b>Помилка! Закладку не визначено.</b>
3.6. ВВЕДЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЮ ТА ОБСЛУГОВУВАННЯ.....	<b>Помилка! Закладку не визначено.</b>
3.7. РОЗРАХУНОК ВАРТОСТІ ЗАГАЛЬНИХ ВИТРАТ НА ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.....	<b>Помилка! Закладку не визначено.</b>
ВИСНОВОК.....	7
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	9

## ВИСНОВОК

Дипломна робота присвячена інформаційному захисту приміщення залу засідань ГУ ДСНС України у Миколаївській області від можливого витоку інформації через технічні канали.

На основі проведених досліджень розроблено проект комплексної системи захисту інформації на об'єкті інформаційної діяльності, проаналізовано види інформації, що озвучуються і зберігається на об'єкті. Оцінено канали витоку інформації та побудовано модель загроз. Також описано організаційний і технічних захист на об'єкті інформаційної діяльності, а саме виділеному приміщенні - зал засідань.

У першому розділі розглянуто інформацію, що стосується акустичної інформації, каналів її витоку та технічного захисту. Для захисту мовної інформації від витоку технічними каналами на об'єктах інформаційної діяльності, де циркулює інформація з обмеженим доступом, створюється комплекс технічного захисту інформації, який являє собою сукупність організаційних, інженерних і технічних заходів та засобів

У другому розділі розглянуто інформаційний захист приміщення залу засідань від витоку інформації технічними каналами, згідно нормативних документів та засвоєного матеріалу під час навчання. На об'єкті інформаційної діяльності циркулює різного типу інформація, як відкрита, так і з обмеженим доступом. Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності.

У третьому розділі розглянуто необхідні заходи та засоби для забезпечення інформаційного захисту приміщення залу засідань. Так як на об'єкті інформаційної діяльності інформація з обмеженим доступом, що

озвучується є державною таємницею, то до системи захисту входить комплекс технічного захисту інформації та фізичний захист.

Розробляючи проект технічного захисту інформації з обмеженим доступом на даному об'єкті, складено кошторис, в який входить вартість обраних технічних засобів захисту інформації, а саме фізичних засобів та технічних пристроїв. Усі засоби були взяті з переліку сертифікованих приладів ТЗІ на сайті Держспецзв'язку.

Вартість захисту інформації технічними та фізичними засобами захисту, на об'єкті інформаційної діяльності, ГУ ДСНС України в місті Миколаїв, становить 59 405,00 грн.



### Список використаних джерел

1. Введение в безопасность предпринимательства. Учебное пособие. – С – Пб.: Высшая административная школа мэрии, 1996. – 99 с.
2. Конкурентная разведка в компьютерных сетях / Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. - К. : ИПРИ НАН Украины, 2013. — 248 с.
3. Закон України «Про інформацію» від 2.10.1992 //Відомості Верховної Ради. – 1992 - №44 - ст.650.
4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. - К.: ТИД ДиаСофт, 2002. - 668с.
5. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2016. - 104 с.
6. Барсуков В.С. Сучасні технології безпеки / В.С. Барсуков, В.В. Водолазський. - М.: Нолидж, 2000. - 496 с.
7. Положення «Про Державну службу України з надзвичайних ситуацій»// Постанова Кабінету Міністрів України від 16 грудня 2015 р. №1052-м. Київ
8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5.07.1994 //Відомості Верховної Ради. - 1994 - №31 - ст.№286.
9. Закон України «Про державну таємницю» від 21.01.1994//Відомості Верховної Ради. - 1994 - №16 – ст. № 93.
10. Ярочкин В.И. Информационная безопасность. – М.: Академический Проект. Мир. 2004. – 544 с.
11. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» від 08.11.2005 // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України – м. Київ: 2005.

12. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 21–22.

13. Бурнашов С. В. Проектування та розроблення відкритих wіfі-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

14. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

15. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. *Information Technology and Security*. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

16. Н.Масюк, О.Полотай Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур. Актуальні проблеми управління інформаційною безпекою держави: Збірник тез наукових доповідей XII Всеукраїнської науково-практичної конференції – К. 2021. – С. 92-96.

17. Полотай О., Мороз Ю., Великий В. Методи технічного захисту інформації у сфері інформаційної безпеки. Інформаційна безпека інформаційні технології: Збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. – Львів, 2020. – С. 40-41.

18. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. *Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing*, vol 1293, Springer, Cham. – pp.1101-1115.

19. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

20. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.

21. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

22. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.