



Львівський державний  
університет безпеки  
життєдіяльності



КІБЕР  
ПОЛІЦІЯ  
НАЦІОНАЛЬНА ПОЛІЦІЯ  
УКРАЇНИ

softserve



UnderDefense

# ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей  
V Міжнародної науково-практичної  
конференції  
ІБІТ 2024

27 листопада 2024 року

Міністерство освіти і науки України  
Державна служба України з надзвичайних ситуацій  
Львівський державний університет безпеки життєдіяльності  
Національний університет “Львівська політехніка”

# **ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024**

Збірник доповідей  
V Міжнародної науково-практичної конференції

**27 листопада 2024 року**

Львів – 2024

**ББК 32.81+78.362**

*Інформаційна безпека та інформаційні технології: збірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с.*

**ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ:**

**Ростислав Львович ТКАЧУК** – доктор технічних наук, професор, начальник кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності;

**Олександр Володимирович ПРИДАТКО** – кандидат технічних наук, доцент, проректор з навчальної та методичної роботи Львівського державного університету безпеки життєдіяльності;

**Богдан Васильович ДУРНЯК** – доктор технічних наук, професор, в.о. ректора Української академії друкарства;

**Роман Святославович ЯКОВЧУК** – доктор технічних наук, доцент, начальник факультету цивільного захисту, Львівський державний університет безпеки життєдіяльності;

**Ольга Володимирівна МЕНЬШИКОВА** – кандидат фізико-математичних наук, доцент, заступник начальника факультету цивільного захисту, Львівський державний університет безпеки життєдіяльності;

**Іван Романович ОПІРСЬКИЙ** – доктор технічних наук, професор, завідувач кафедри захисту інформації Національний університет «Львівська політехніка»;

**Sofia KUTAS**

team lead of security and access management department in NBS, United Kingdom and Ireland

**Ярослав Васильович ІЛЬЧИШИН**

кандидат педагогічних наук, начальник науково-дослідного центру, Львівський державний університет безпеки життєдіяльності

**Назарій Євгенович БУРАК**

кандидат технічних наук, доцент, заступник начальника кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності

**Тарас Євгенович РАК**

доктор технічних наук, доцент, професор кафедри інформаційних технологій ПЗВО «ІТ СТЕП Університет»

**Ігор Михайлович ЖУРАВЕЛЬ**

доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»

**Zbigniew KOKOSIŃSKI**

dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki

**Volodymyr SAMOTYY**

prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki

**Sergii TELENYK**

prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology

**Володимир Афанасійович РОМАКА**

доктор технічних наук, професор, професор кафедри захисту інформації Національного університету «Львівська політехніка»

**Валерій Богданович ДУДИКЕВИЧ**

доктор технічних наук, професор, професор кафедри захисту інформації Національного університету «Львівська політехніка»

**Любомир Степанович СІКОРА**

доктор технічних наук, професор, професор кафедри автоматизованих систем управління Національного університету «Львівська політехніка»

**Наталя Корнеліївна ЛИСА**

доктор технічних наук, професор, доцент кафедри автоматизованих систем управління Національного університету «Львівська політехніка»

**Тетяна Олександрівна ГОВОРУЩЕНКО**

доктор технічних наук, професор, декан факультету інформаційних технологій Хмельницького національного університету

**Amiran SHARADZE**

PhD student, Assistant of the Department of computer sciences, Batumi Shota Rustaveli State University

**РЕДКОЛЕГІЯ:**

**Ростислав ТКАЧУК** – д.т.н., професор, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

**Олександр ПРИДАТКО** – к.т.н., доцент, проректор з навчальної та методичної роботи Львівського державного університету безпеки життєдіяльності;

**Іван ОПРСЬКИЙ** – д.т.н., професор, професор, завідувач кафедри захисту інформації Національного університету “Львівська політехніка”;

**Валерій ДУДИКЕВИЧ** – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”;

**Zbigniew KOKOSIŃSKI** – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki;

**Volodymyr SAMOTYU** – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki;

**Sergii TELENYK** – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology;

**Володимир РОМАКА** – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”;

**Любомир СІКОРА** – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету “Львівська політехніка”;

**Наталя ЛИСА** – д.т.н., доцент, доцент кафедри кафедри автоматизованих систем управління Національного університету “Львівська політехніка”;

**Тетяна ГОВОРУЩЕНКО** – д.т.н., професор, декан факультету інформаційних технологій Хмельницького національного університету;

**Ольга МЕНЬШИКОВА** – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

**Андрій ІВАНУСА** – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

**Валентина ЯЩУК** – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

**Орест ПОЛОТАЙ** – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

**Валерія БАЛАЦЬКА** – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

**Ігор МАЛЕЦЬ** – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

**Назарій БУРАК** – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

**Ольга СМОТР** – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

**Юрій БОРЗОВ** – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

**Роман ГОЛОВАТИЙ** – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

**Олександр ХЛЕВНОЙ** – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

# З М І С Т

## СЕКЦІЯ 1

---

### ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

#### *НАПРЯМ 1.*

#### *УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ*

<b>Балацька В., Побережник В.</b> ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА NFT ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДЕРЖАВНИХ РЕЄСТРІВ	6
<b>Фединець Н., Синиця О.</b> МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В СУЧАСНИХ РЕАЛІЯХ	9
<b>Полотай О.</b> ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ БАНКІВСЬКОЇ УСТАНОВИ	12
<b>Ткаченко А.</b> ВІРУСИ-ДРОППЕРИ: ТЕХНІКИ ДОСТАВКИ ШКІДЛИВОГО ПЗ ТА ОБХІД ЗАХИСНИХ СИСТЕМ	16
<b>Ящук В., Ошурко Б.</b> СУЧАСНІ ВИКЛИКИ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УМОВАХ ВІЙНИ	17
<b>Ящук В., Столярчук В.</b> ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМУ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ	20
<b>Виглазов В.</b> ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ВОЄННИЙ ЧАС	23
<b>Паньків А-М-І., Хлевной О.</b> КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ: ТАКТИКИ, МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ	27
<b>Бик Е., Бурак Н.</b> ДОСЛІДЖЕННЯ СУЧАСНИХ КОМУНІКАЦІЙНИХ ПЛАТФОРМ ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПОВСЯКДЕННОЇ ДІЯЛЬНОСТІ ДСНС УКРАЇНИ	29
<b>Водоніс Я., Полотай О.</b> ПРОЦЕСНИЙ ПІДХІД В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВАХ, ЯКІ НАДАЮТЬ ІТ-ПОСЛУГИ	32
<b>Литвиненко Р., Лучик В.</b> ЦИФРОВА КРИМІНАЛІСТИКА	36
<b>Мукан І., Котовська О.</b> КРИМІНАЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У КІБЕРПРОСТОРІ ТА ЕКСПЕРТНА РОЛЬ ГРОМАДСЬКИХ (НЕУРЯДОВИХ) ОРГАНІЗАЦІЙ	40

<b>Ящук В., Водніцька О., Sharadze A.</b> АНАЛІЗ СВІТОВИХ ПРАКТИК УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ	44
<b>Дем'янчук Ю.</b> МОДЕЛЬ ПОВЕДІНКИ «АГЕНТІВ» ВОЄННОЇ КОМУНІКАЦІЇ: ФОРМАЛЬНО-СИНТАКСИЧНА ІЄРАРХІЯ	48
<b>Харчук А.І., Харчук А.А.</b> ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ	52
<b>Бундус В., Лучик В.</b> РОЗСЛІДУВАННЯ КІБЕРАТАК У ВОЄННИХ УМОВАХ	54

### **НАПРЯМ 2.**

#### **ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ**

<b>Борматов Р.</b> ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ	57
<b>Пилипенко В., Тимчишин О., Федець Н.</b> ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ	60

### **НАПРЯМ 3.**

#### **БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ**

<b>Savchuk K.</b> AI IN ACTION: DEFENDING AGAINST EVOLVING CYBER THREATS	64
<b>Орощук Х., Маслоva Н., Любименко О.</b> ЗАГРОЗИ CLOUD COMPUTING: ВИКЛИКИ ТА МЕТОДИ ЗАХИСТУ	68
<b>Івануса А., Ткаченко А., Петрович А.</b> ВДОСКОНАЛЕННЯ АРХІТЕКТУРИ ЗАСОБІВ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ	73
<b>Кондратюк М.</b> ЗАХИСТ КРИПТОВАЛЮТНИХ ГАМАНЦІВ	76
<b>Івануса А., Брич Т., Ткач М.</b> РОЗРОБКА МОДУЛІВ І ФУНКЦІОНАЛЬНОСТІ ЗАСОБУ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ	79
<b>Грабченков Б., Лучик В.</b> СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЇХ ЗАСТОСУВАННЯ	83
<b>Івануса А., Сорока А., Ланчевич А.</b> АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ У WEB-ДОДАТКАХ	86

#### **НАПРЯМ 4.**

##### **ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ**

<b>Сабадах І., Лучик В. РОЛЬ ШИФРУВАННЯ У ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ</b>	91
<b>Гордієнко Т. АНАЛІЗ ЗАГРОЗ У КАНАЛАХ ЗВ'ЯЗКУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОПЕРАТИВНОЇ ПОЛІГРАФІЇ</b>	94
<b>Світличний В., Шестаков В. МЕТОДИ ЗАХИСТУ ІоТ-ПРИСТРОЇВ ВІД КІБЕРЗАГРОЗ</b>	98
<b>Клименко Т. АКТУАЛЬНІСТЬ ЗАХИСТУ Й БЕЗПЕКИ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ І МЕСЕНДЖЕРАХ В УМОВАХ ВІЙСЬКОВОГО СТАНУ</b>	103
<b>Ящук В., Кутник Н. ОЦІНЮВАННЯ ВРАЗЛИВОСТЕЙ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ З ВИКОРИСТАННЯМ ПЛАТФОРМИ TRYNACKME</b>	106
<b>Любімов О., Іовенко І. РОЗУМІННЯ МАЙБУТНІМИ ОФІЦЕРАМИ ЗАХИЩЕНОГО ЗВ'ЯЗКУ З ОРБІТАЛЬНИМИ НАНОСУПУТНИКАМИ</b>	109
<b>Остапець Д., Сухомлин О. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ</b>	117
<b>Остапець Д., Мотиленко В. МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОКАЗІВ НУЛЬОВОГО РОЗГОЛОШЕННЯ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ</b>	120
<b>Курінний І., Світличний В. АНТИВІРУСНІ ПРОГРАМИ: ЇХ ЗНАЧЕННЯ ТА ЕФЕКТИВНІСТЬ У ЗАХИСТІ ДАНИХ</b>	123
<b>Лучик В., Прокопчук Н. ЗАХИСТ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМИ ПРОЦЕСАМИ (SCADA)</b>	127
<b>Полотай О. ДОСЛІДЖЕННЯ СПОСОБІВ ЗАХИСТУ WEB-САЙТІВ ВІД МЕРЕЖЕВИХ АТАК</b>	129
<b>Одерій Н., Світличний В. ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ: МОТИВАЦІЯ ЗЛОВМИСНИКІВ</b>	133
<b>Федоренко А. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВУ ЕПОХУ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ</b>	135
<b>Полотай О., Гуменюк М. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN</b>	138
<b>Пільов К. ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</b>	142
<b>Лучик В., Гончаров Д. ОСНОВНІ ПРОТОКОЛИ МЕРЕЖЕВОЇ БЕЗПЕКИ</b>	144
<b>Рошинець І., Полотай О. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ</b>	



В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ VPN	148
<b>Лучик В., Гуменюк І.</b> БРАНДМАУЕРИ ТА ЇХ ВИКОРИСТАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ	152
<b>Світличний В., Колода Я.</b> БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ: МЕТОДИ ЗАХИСТУ ВІД СПАМУ ТА ШКІДЛИВИХ ВКЛАДЕНЬ	156
<b>Ориник С., Полотай О.</b> ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД АТАК VLAN HOPPING	159
<b>Курило Д., Світличний В.</b> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІЇ ІНТЕРНЕТ ПІРАТСТВУ	162
<b>Назаров В.</b> ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІЖНАРОДНОЇ РЕКЛАМНОЇ АГЕНЦІЇ В УМОВАХ ДЕЦЕНТРАЛІЗОВАНОГО СЕРЕДОВИЩА	164
<b>Ranovuk U., Ranovuk R., Rajesh N., Fedyna B.</b> SECURE DOCUMENT MANAGEMENT VIA VPN IN CORPORATE INFORMATION SYSTEMS	170
<b>Філіпчук Б., Ткачук Р.</b> ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАХИЩЕНИХ КАНАЛІВ, ПОБУДОВАНИХ НА ПРОТОКОЛАХ WireGuard ТА OpenVPN	175
<b>Світличний В., Ковтун І.</b> СУЧАСНІ МЕТОДИ БОРОТЬБИ З АТАКАМИ ТИПУ SQL-ІН'ЄКЦІЙ	179
<b>Кугот В., Сабат В.</b> ОПЕРАТИВНЕ УПРАВЛІННЯ В ІЄРАРХІЧНО-СТРУКТУРОВАНИХ СИСТЕМАХ ТА ВИБІР МОДЕЛЕЙ СТРАТЕГІЙ ЦІЛЕОРІЄНТОВАНИХ ДІЙ В УМОВАХ ЗАГРОЗ	182
<b>Гончарук І., Манжай О.</b> ЗАХИСТ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ПРАКТИКИ ТА ПЕРСПЕКТИВИ В УКРАЇНІ	186
<b>Руденко М.</b> ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ	188
<b>Нечипорук В., Лучик В.</b> АНАЛІЗ ВРАЗЛИВОСТЕЙ В ПОПУЛЯРНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ТА ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ	191

#### **НАПРЯМ 5.**

##### **ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

<b>Яхно Н., Лучик В.</b> ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	195
<b>Шевців Ю., Костишин Е.</b> ВПЛИВ ВІЙНИ НА ГЕНДЕРНУ ПАРИТЕТНІСТЬ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ	198
<b>Яремко Р., Ткачик О.</b> ПОНЯТТЯ ПРО ГЕНДЕРНІ СТЕРЕОТИПИ ТА ЇХ ВПЛИВ НА ПОВСЯКДЕННЕ ЖИТТЯ ЛЮДЕЙ	200
<b>Коваль І., Лакіш В.</b> ГЕНДЕРНІ ВІДМІННОСТІ У ПІДГОТОВЦІ РЯТУВАЛЬНИКІВ	203

## НАПРЯМ 6.

### КРИПТОГРАФІЧНІ ТА СТЕГANOГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

- Grytsiuk P., Sikora L.** THE MECHANISM OF GENERATING FIBONACCI AND LUCAS POLYNOMIALS 206
- Чорненька С., Манжай О.** КРИПТОГРАФІЧНІ МЕТОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ 211
- Кобилкіна О., Ровецький І.** СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ 215
- Остапець Д., Дзюба В.** АПАРАТНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ 218
- Галицький І., Лаврик Т.** ІНТЕГРАЦІЯ КРИПТОГРАФІЇ ТА СТЕГANOГРАФІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: АНАЛІЗ ПРОГРАМНИХ РІШЕНЬ 221
- Горячий О., Журавель І.** ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОСТИХ СТЕГANOГРАФІЧНИХ МЕТОДІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ 225
- Малець О.-С., Смотр О.** СТАН ДОСЛІДЖЕНЬ У СФЕРІ ЦИФРОВОГО МАРКУВАННЯ ДЛЯ АУДІОФАЙЛІВ 230
- Олег Г., Захар Я.** АНАЛІЗ ЕФЕКТИВНОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КВАДРАТНОГО КОРЕНЯ ПРОСТОГО ЧИСЛА 234

## НАПРЯМ 7.

### КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ

- Танчин І.** СТРАТЕГІЇ РЕАЛІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ В АРХІТЕКТУРІ ІІoT ПОЛІГРАФІЧНОГО ПІДПРИЄМСТВА 238
- Чепурной К., Тимошенко Л.** ЗАХИСТ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ 243
- Weigang G., Myronchuk K.** DATA ENCRYPTION ALGORITHMS IN MASS SERVICE SYSTEMS 246
- Балацька В., Опірський І.** ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОВІРИ ТА ПРОЗОРОСТІ У ДЕРЖАВНИХ РЕЄСТРАХ 251
- Demudova A., Маслова Н., Кіс Т.** ЗАСТОСУВАННЯ МЕТОДІВ ШИФРУВАННЯ В СИСТЕМАХ ЗАХИСТУ МЕДИЧНИХ ДАНИХ 254
- Піх І., Браташ С.** ВІДМОВОСТІЙКІСТЬ ЯК КРИТЕРІЙ ЯКОСТІ

ВЕБЗАСТОСУНКУ	258
<b>Побережник В., Балацька В., Опірський І.</b> КОНЦЕПЦІЯ САМОСУВЕРЕННОЇ ІДЕНТИЧНОСТІ ЯК АЛЬТЕРНАТИВА ТРАДИЦІЙНИМ МЕТОДАМ АВТЕНТИФІКАЦІЇ	262
<b>Ротань К.</b> КРИТИЧНА ІНФРАСТРУКТУРА ПІД ЧАС ВІЙНИ: ЗАХИСТ ВІД КІБЕРАТАК ТА ВІДНОВЛЕННЯ СИСТЕМ	265
<b>Коробейнікова Т., Одінцов Б.</b> ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ	268
<b>Дейнека О., Гарасимчук О.</b> МОДЕЛЬ КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ ЗГІДНО З ВИМОГАМИ SOC 2 TYPE 2	273
<b>Ranovuk U., Hidey R.</b> HARDWARE-SOFTWARE APPROACH TO ENSURING INFORMATION SECURITY IN AUTOMATED METROLOGICAL CONTROL SYSTEMS FOR PRODUCTION PROCESSES	277
<b>Ranovuk U., Kutas S., Qureshi A.</b> SECURE ACCESS TO ENTERPRISE INFORMATION SYSTEMS IN THE MODERN DIGITAL ENVIRONMENT	282
<b>Сафронов О., Лучик В.</b> ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ	286
<b>Рак М.</b> ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ: КРИМІНАЛЬНА ТА ЦИВІЛЬНА. СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ	289
<b>Скориневич Б., Кулик Ю., Гавриляк В.</b> АНАЛІЗ БЕЗПЕКИ ПІДХОДУ “ІНФРАСТРУКТУРА ЯК КОД” (INFRASTRUCTURE AS CODE) В ХМАРНИХ ОБЧИСЛЕННЯХ	291
<b>Дорогий Я., Цуркан В., Дорога-Іванюк О.</b> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ОСВІТНЬОЇ ГАЛУЗІ	296
<b>Бердиченко І., Дорогий Я., Дорога-Іванюк О.</b> ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОНОДАВСТВА ЄС ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ	299
<b>Сороченко М., Лаврик Т.</b> БЕЗПЕКА БЛОКЧЕЙН: АНАЛІЗ АТАК ТА ВРАЗЛИВОСТЕЙ	304
<b>Тульвїнський С.</b> КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ПРИНЦИП ФУНКЦІОНУВАННЯ ПІДРОЗДІЛУ	307
<b>Коробейнікова Т., Бодак А., Бороденко Д.</b> НУЛЬОВА ДОВІРА: ПРИНЦИПИ, ВИКЛИКИ ТА ВПРОВАДЖЕННЯ	310
<b>Токар В., Лучик В.</b> РОЛЬ НАВЧАННЯ СПІВРОБІТНИКІВ У ЗА-	

ПОБІГАННІ КІБЕРАТАКАМ	315
<b>Помаза-Пономаренко А., Тарадуда Д.</b> КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	318
<b>Щербина А.</b> КІБЕРБЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: СУЧАСНІ ВИКЛИКИ ТА РІШЕННЯ	322
<b>Іщенко А., Марич В.</b> ПІГ-КОНТРАКТ, ЯК ПРАВОВЕ ПОЛЕ З ОХОРОНИ ПРАЦІ ДЛЯ ПРАЦІВНИКІВ ІТ-КОМПАНІЙ	326
<b>Яшук В., Мисько Р.</b> ЗАХИСТ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ	328
<b>Дришлюк Д., Лучик В.</b> МЕТОДИ РОЗСЛІДУВАННЯ ТА ДОКУМЕНТУВАННЯ КІБЕРАТАК НА ДЕРЖАВНІ УСТАНОВИ	331
<b>Сафронов О., Лучик В.</b> ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ	334
<b>Сиротенко Б., Лучик В.</b> ЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ	336
<b>Шведов В., Рудик Ю.</b> АПАРАТИ ЗАХИСТУ В СИСТЕМАХ SMART HOUSE	338
<b>Кутняк М., Куперштейн Л.</b> СИСТЕМА ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА ОСНОВІ ПЛАТФОРМИ ARDUINO	342

## **НАПРЯМ 8. ІНФОРМАЦІЙНІ ВІЙНИ**

<b>Кісіль Р.</b> ФЕЙКОВІ НОВИНИ ЯК ІНСТРУМЕНТ СУЧАСНОГО ПРОТИСТОЯННЯ	346
<b>Сабат В., Мацюк В.</b> ФІШИНГ ЯК ЗАГРОЗА ОНЛАЙН СЕРЕДОВИЩА	349
<b>Снапкова Н.</b> РОЗУМІННЯ МАЙБУТНІМИ ОФІЦЕРАМИ ЗНАЧУЩОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНИ У ПРОЦЕСІ ЦИВІЛЬНО-ВІЙСЬКОВОЇ ВЗАЄМОДІЇ	353

**СЕКЦІЯ 2****ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ  
ТЕХНОЛОГІЙ В УМОВАХ ВІЙНИ****НАПРЯМ 9.****ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ**

- Milianets T., Pukach A.** SERVER LOAD BALANCING MATHEMATICAL MODEL BASED ON AUTOMATIC NODE'S RATING EVALUATION 360
- Вілык V.** SURVEY OF DSL GENERATORS FOR THE JAVA PLATFORM 363
- Кісіль О.** РОЗРОБЛЕННЯ ПРОГРАМНОЇ СИСТЕМИ ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ СИЛ ТА ЗАСОБІВ ДЛЯ ГАСІННЯ ПОЖЕЖИ В ФОРМАТІ ЧАТ-БОТА 366
- Літовська О.** ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ СИГНАЛУ RRG ДЛЯ ВИЯВЛЕННЯ ТА УСУНЕННЯ ВИКИДІВ 368
- Павлюк О., Заболотна А., Міщук М.** СИСТЕМА ЗБОРУ ТА ПРЕПРОЦЕСИНГУ ДАНИХ ТРИОСЬОВИХ АКСЕЛЕРОМЕТРА ТА ПІРОСКОПА ОТРИМАНИХ ЗА ДОПОМОГОЮ СМАРТ-ГОДИННИКІВ 373
- Шопський О., Малець І.** АНАЛІЗ І ВДОСКОНАЛЕННЯ МОДЕЛІ КЛАСТЕРИЗАЦІЇ ДАНИХ ДЛЯ ФОРМУВАННЯ ВИБІРКИ З МЕТОЮ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ 379
- Ровецький І.** АРХІТЕКТУРНІ ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПРОГРАМНИХ СЕРВІСІВ З ПАРАЛЕЛЬНИМИ ОБЧИСЛЕННЯМИ 381
- Малець Б., Заболоцький Т.** СИСТЕМА АНАЛІЗУ ДАНИХ ДЛЯ КУРСУ «МОДЕЛІ СТАТИСТИЧНОГО НАВЧАННЯ» 384
- Мотульський В., Хлевной О.** ОНЛАЙН-СЕРВІС ДЛЯ ОПЕРАТИВНОГО РОЗРАХУНКУ СИЛ ТА ЗАСОБІВ ПОЖЕЖНО-РЯТУВАЛЬНИХ СЛУЖБ У ЖИТЛОВИХ БУДИНКАХ ПІДВИЩЕНОЇ ПОВЕРХОВСТІ 387
- Льба О., Головатий Р.** СИСТЕМА БРОНЮВАННЯ ЖИТЛА ДЛЯ ВОЛОНТЕРІВ 390
- Поглод П., Смотри О.** СТВОРЕННЯ ІНТЕГРОВАНОЇ МОБІЛЬНОЇ СИСТЕМИ ДЛЯ КООРДИНАЦІЇ ГУМАНІТАРНОЇ ДОПОМОГИ ТА ЕВАКУАЦІЙНИХ ЗАХОДІВ 393
- Гапанович В., Смотри О.** РОЗРОБКА МОБІЛЬНОГО СЕРВІСУ НАДАННЯ ПСИХОЛОГІЧНОЇ ДОПОМОГИ 396

<b>Близнюк Т. РОЗРОБКА ПЗ ДЛЯ СТВОРЕННЯ ПОРТАЛУ АВТОСПОРТИВНИХ НОВИН</b>	400
<b>Шпак З., Шувар М. ПАНЕЛЬ КЕРУВАННЯ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ НА БАЗІ ЧАТ-БОТУ МЕСЕНДЖЕРА</b>	403

### ***НАПРЯМ 10.***

#### ***МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ***

<b>Білик О., Мартинчук О. ВИЯВЛЕННЯ БПЛА ЗА ДОПОМОГОЮ SDR HACKRF ONE</b>	407
<b>Гнатюк В., Горбачов І. АНАЛІЗ СУЧАСНИХ ПРОГРАМНО-АПАРАТНИХ РІШЕНЬ ДЛЯ ІР-ТЕЛЕФОНІЇ</b>	410
<b>Гнатюк В., Батрак О., Головань М. МЕТОДИ ОПТИМІЗАЦІЇ РОБОТИ КОНТАКТ ЦЕНТРУ</b>	414
<b>Гамрецький Р., Гнатюк В. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ І МОДЕЛЕЙ ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ</b>	417
<b>Паньків Т., Борзов Ю. РОЗРОБЛЕННЯ СЕРВІСУ ПОШУКУ НАЙБЛИЖЧИХ МЕДЗАКЛАДІВ НА ОСНОВІ ГЕОЛОКАЦІЇ</b>	422
<b>Громик О. АВТОМАТИЗАЦІЯ В РЕСТОРАННОМУ БІЗНЕСІ: СУЧАСНІ РІШЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ТА СЕРВІСУ</b>	425
<b>Острроверхий В., Молошний В. ВДОСКОНАЛЕННЯ УПРАВЛІННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ ІНТЕРНЕТ ПРОВАЙДЕРА</b>	429
<b>Пилипенко В., Борзов Ю. ФУНКЦІОНУВАННЯ ЗАСОБІВ (СИСТЕМ) ЗВ'ЯЗКУ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ</b>	432

### ***НАПРЯМ 11.***

#### ***3D МОДЕЛЮВАННЯ ТА 3D ДРУК***

<b>Духнич Н., Хлевной О. 3D МОДЕЛЮВАННЯ ТА 3D ДРУК – МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ</b>	436
<b>Івановський М., Кусій М. ВИКОРИСТАННЯ UNITY ДЛЯ 3D-МОДЕЛЮВАННЯ З ЕЛЕМЕНТАМИ ЛІНІЙНОГО ШИФРУВАННЯ</b>	439

### ***НАПРЯМ 12.***

#### ***МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ***

<b>Semenyuk S. APPLICATION OF THE STOCHASTIC SIR MODEL TO CYBERSECURITY THREATS MODELING</b>	444
--	-----

3. Конференції Державного університету «Житомирська політехніка».  
URL: <https://conf.ztu.edu.ua/wp-content/uploads/2019/12/27-2.pdf> (дата звернення: 17.11.2024).

**УДК 621.396**

## **ФУНКЦІОНУВАННЯ ЗАСОБІВ (СИСТЕМ) ЗВ'ЯЗКУ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ**

**Володимир ПИЛИПЕНКО  
Юрій БОРЗОВ**

**Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.**

***Abstract.** Sustainable functioning and implementation of modern communication systems and means in the bodies and subdivisions of the SES of Ukraine is one of the strategic directions of the service and the State as a whole. The author analyzes the directions of development of information and communication technologies that facilitate the introduction of digital communication systems and the use of modern solutions to provide reliable communication channels for the bodies and subdivisions of the SES of Ukraine.*

***Keywords:** State Emergency Service of Ukraine (SESU), communication channels, radio communication, digital communications, information system.*

***Анотація.** Стале функціонування та запровадження сучасних систем та засобів зв'язку в органах та підрозділах ДСНС України є одним із стратегічних напрямків роботи служби і держави в цілому. Проаналізовано напрямки розвитку інформаційно-комунікаційних технологій, які сприяють впровадженню цифрових систем зв'язку і використання сучасних рішень для забезпечення надійними каналами зв'язку органи та підрозділи ДСНС України.*

***Ключові слова:** ДСНС України, канали зв'язку, радіозв'язок, цифрові комунікації, інформаційна система.*

З початком повномасштабного вторгнення російських окупаційних військ на територію України перед Державною службою України з надзвичайних ситуацій (далі – ДСНС України) постало багато нових викликів, у тому числі ліквідації наслідків влучань російських ракет по житлових будовах, кварталах. Це у свою чергу потребує не тільки використання пожежної та спеціальної рятувальної техніки, але й сучасних, надійних систем забезпечення сталого зв'язку як на місці ліквідації надзвичайних ситуацій, так і до прийому і обробки викликів на спецлінії 101 та Системи 112.

В умовах тотальних блекаутів і введення погодинних графіків відключень електропостачання, перед ДСНС України виникла гостра потреба в

забезпеченні безперебійного та стабільного функціонування ІТ-інфраструктури, що включає надійне оброблення та зберігання даних, оперативне реагування на надзвичайні ситуації, а також захист критичних інформаційних систем від потенційних загроз і технічних збоїв. Фахівцями центрів оперативного зв'язку запроваджено ряд організаційних та технічних заходів щодо сталого й безперебійного зв'язку на всіх рівнях, починаючи від державного пожежно-рятувального поста до апарату ДСНС України, а саме:

- забезпечення усіх критичних вузлів відомчої мережі гарантованим резервним живлення (серверні кімнати, ЦОДи, ретранслятори радіозв'язку);
- налаштування та використання кількох каналів зв'язку (підключення декількох незалежних один від одного інтернет-провайдерів);
- використання супутникових комплектів Інтернет-доступу типу «Starlink»;
- налаштування та використання каналів зв'язку від Державної служби спеціального зв'язку та захисту інформації України;
- впровадження резервних схем маршрутизації викликів на спецлінії 101, використовуючи ресурси операторів стільникового зв'язку, АТ «Укртелеком» та надавачів послуг із SIP-транкінгу.

Одним із ключових засобів зв'язку в умовах воєнного стану є забезпечення ДСНС України сучасним радіозв'язком, яке полягає у побудові відомчої цифрової радіомережі. Активне впровадження цифрового радіозв'язку дозволило повністю перебудувати логіку радіомереж ДСНС України, а також удосконалити взаємодію із іншими службами на всіх рівнях. Цифровий радіозв'язок забезпечив високу захищеність радіопередачі сигналу, відстежування та моніторинг місцезнаходження за допомогою GPS. На прикладі впровадження цифрового радіозв'язку у місті Львові та Львівській області охоплення зони покриття становить близько 90%, з яких покриття стаціонарних радіостанцій – 99%, автомобільних і переносних – близько 80%. Менше охоплення, зазвичай, є у гірській місцевості, де за особливістю рельєфу, не завжди є можливість проходження радіохвиль. Надійність та охоплення великої зони покриття здійснено за рахунок встановлення базових станцій (радіоретрансляційного обладнання) та ретрансляторів. Кожний ретранслятор створює навколо себе «СOTУ» покриття, а «СОТИ» об'єднуються, створюючи територію покриття (рис 1).



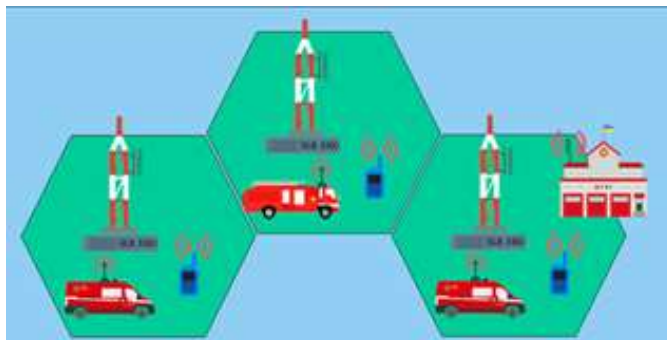


Рисунок 1 – Схематичний вигляд «Сот»

Системою цифрового радіозв'язку можна керувати за допомогою серверу та спеціалізованого програмного забезпечення, яке називається «SMART PTT» (Рис 2.). Загалом PTT означає «Push-To-Talk», комунікаційну технологію, яка дозволяє користувачам натискати кнопку, щоб передавати свій голос через двосторонню радіостанцію або інший пристрій зв'язку. Smart PTT відноситься до версії цієї технології, яка містить додаткові функції та можливості, такі як відстеження місцезнаходження GPS, обмін миттєвими повідомленнями, групові виклики та інтеграція з іншими системами зв'язку.

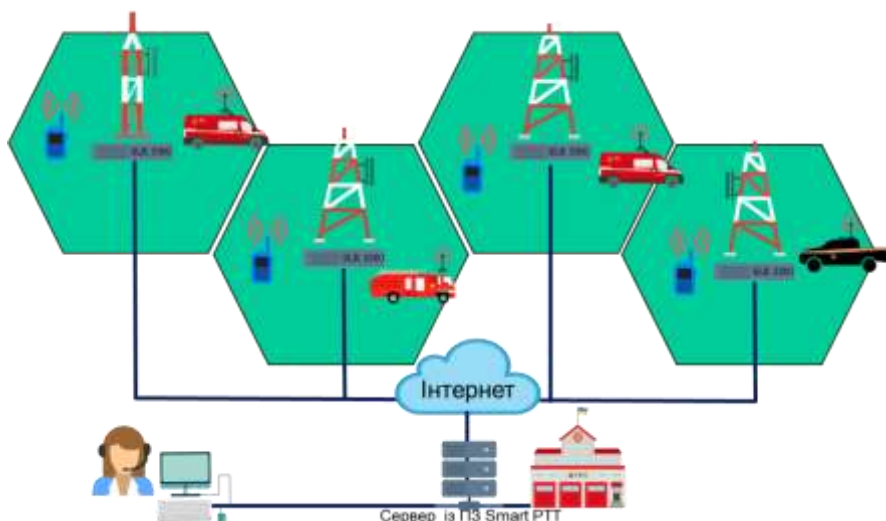


Рисунок 2 – Схематичний вигляд «SMART PTT»

ДСНС України активно впроваджує багаторівневу систему безперервного прийому та обробки викликів на лінії 101 із використанням новітніх методів побудови систем, які базуються на цифрових процесах доставки голосових дзвінків до кінцевого абонента. Використання цифрових IP АТС та SIP-транків провайдерів зв'язку в органах та підрозділах ДСНС України дозволяє гнучко налаштовувати під конкретні потреби того чи іншого підрозділу. Ця система включає в себе розділення серверної та мережевої інфраструктури географічно, а також забезпечення одночасно кількох незалежних каналів зв'язку, що мінімізує виведення з ладу спецлінії 101. У випадках локального пошкодження чи відсутності зв'язку із основними системами здійснюється автоматичне переключення на аналогові лінії центрального вузла АТ «Укртелеком». На сьогодні відмовитись повністю від використання мереж загального користування не можливо, так як це залишається зв'язком «останньої надії».

Упровадження нових схем прийому і обробки екстрених викликів на лінії 101 дозволило забезпечити безперебійну роботу в умовах війни та тотальних відключень електроенергії, а використання волоконно-оптичних ліній зв'язку є сучасним і надійним рішенням.

Також, активно здійснюється впровадження сучасних інформаційно-аналітичних систем таких як: МІА: Облік і звіт, МІА: Здоров'я, Система автоматизованого документообігу АСКОД, Інтерактивний інспектор, Логістична інформаційна система. Всі ці системи створюють єдину екосистему в автоматизації робочих процесів, планування, обліку, контролю та аналізу ділових процесів управлінської, виробничої, фінансової та господарської діяльності.

Таким чином, на основі викладеного матеріалу, можна стверджувати, що ефективно впровадження та використання сучасних засобів (систем) зв'язку в умовах війни в органах та підрозділах ДСНС України, забезпечує кращу взаємодію під час ліквідації наслідків ракетних влучань та надзвичайних ситуацій, а також гарантує сталий, безперебійний зв'язок та дозволяє ефективно використовувати сили та засоби за призначенням.

#### *Інформаційні джерела*

1. Дії підрозділів ДСНС України в умовах воєнного стану : навч. посіб. / ред. М. С. Коваль. Львів : ЛДУБЖД, 2023. 306 с.
2. Сайко В.Г., Амірханов Е.Д. Основи мереж цифрового радіозв'язку і радіодоступу нового покоління. К.: ДУТ, 2015. 77 с.
3. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 8 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
4. Gonçalves F. E. Configuration guide for Asterisk PBX. 2nd ed. 2007. 370 p.