МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра «Інформаційна безпека та наноелектроніка»
(повне найменування кафедри)

Пояснювальна записка

до дипломної роботи
магістр
(ступінь вищої освіти)

на тему Дослідження захищеності комунікаційного центру «Служби 112»
(назва теми)

Виконав: студент 2 курсу, групи БК-814м
Спеціальності 125 Кібербезпека та захист інформації
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
ПРИЙМЕНКО А.С
(ПРІЗВИЩЕ та ініціали)
Керівник КОЗІНА Г.Л.
(ПРІЗВИЩЕ та ініціали)
Рецензент МОРОЗ Г. В.
(ПРІЗВИЩЕ та ініціали)

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ

Завідувач кафедри ІБтаН, к. ф.-м. н., доцент
Андрій КОРОТУН
«_____» _____2025 р.

З А В Д А Н Н Я

НА ДИПЛОМНИЙ РОБОТУ СТУДЕНТА

ПРИЙМЕНКО Артема Сергійовича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження захищеності комунікаційного центру «Служби112» (Security assessment of the «112 Service» communication centr)
керівник проєкту (роботи) к.ф-м.н., доцент кафедри ІБтаН КОЗІНА Галина Леонідівна ,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові,)
затверджені наказом закладу вищої освіти від «26» листопада 20 25 року № 530
2. Строк подання студентом проєкту (роботи) 22.12.2025р.
3. Вихідні дані до проєкту (роботи) документація служби 112, нормативні акти
щодо захисту інформації, стандарти кібербезпеки, технічні вимоги до комуні-каційних
центрів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз нормативної бази служби 112, оцінка вразливостей комунікаційного центру, пропозиції щодо підвищення захищеності, аналіз ризиків кібербезпеки, розробка пропозицій захисту інформації.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 11 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	КОЗІНА Г.Л., доцент кафедри ІБтаН	04.09.2025	19.12.2025
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН	20.12.2025	20.12.2025

7. Дата видачі завдання » 04 » вересня 2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз літературних джерел за тематикою дослідження.	04.09.25-20.09.25	Виконано
2	Опис предметної області та структури КЦ 112.	21.09.25-30.09.25	Виконано
3	Аналіз вразливостей, поверхні атаки та ризиків.	01.10.25-10.10.25	Виконано
4	Розробка пропозицій з підвищення захисту.	11.10.25-20.11.25	Виконано
5	Оформлення пояснювальної записки та відповідної документації.	21.11.25-10.12.25	Виконано
6	Нормоконтроль та рецензування.	11.12.25-19.12.25	Виконано

Студент _____ Артем ПРИЙМЕНКО
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Галина КОЗІНА
(підпис) (Ім’я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 82 с., 1 табл., 5 рис., 1 дод., 37 джерел.

КОМУНІКАЦІЙНИЙ ЦЕНТР 112, КІБЕРБЕЗПЕКА, ЗАХИЩЕНІСТЬ ІНФОРМАЦІЇ, ЕКСТРЕНА ДОПОМОГА, ВРАЗЛИВОСТІ, ЗАГРОЗИ

Об’єкт дослідження – комунікаційний центр служби 112 як елемент критичної інфраструктури.

Предмет дослідження – захищеність інформаційно-комунікаційної системи центру 112.

Мета роботи – аналіз функціонування, структури, інформаційно-комунікаційних процесів, визначення загроз і вразливостей, формування рекомендацій щодо посилення кіберзахисту.

Методи дослідження: аналіз наукових і нормативних джерел, системний і структурно-функціональний аналіз, моделювання загроз і атак, порівняння підходів до безпеки. Встановлено функції та структуру центру, визначено ризики, запропоновано заходи захисту (SSH-ключі, 2FA, RBAC).

Практична цінність: посилення кіберстійкості для ефективної екстреної допомоги.

ABSTRACT

Explanatory note to the master's thesis: 82 p., 1 table, 5 figures,1 appendix, 37 sources.

COMMUNICATION CENTER 112, CYBERSECURITY, INFORMATION SECURITY, EMERGENCY AID, VULNERABILITIES, THREATS

The object of research is the communication center of service 112 as an element of critical infrastructure.

The subject of research is the security of the information and communication system of center 112.

The purpose of the work is to analyze functioning, structure, information-communication processes, identify threats and vulnerabilities, form recommendations for enhancing cyber protection.

Research methods: analysis of scientific and normative sources, system and structural-functional analysis, modeling of threats and attacks, comparison of security approaches. The functions and structure of the center are established, risks are identified, protection measures are proposed (SSH keys, 2FA, RBAC).

Practical value: enhancing cyber resilience for effective emergency aid.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АМТС — автоматична міжміська телефонна станція;

АРМ — автоматизоване робоче місце;

БС — базова станція (стільникового зв’язку);

ВСС — вузол спеціальних служб;

ГІС — геоінформаційна система;

ДП — державне підприємство;

ЄІС МВС — Єдина інформаційна система Міністерства внутрішніх справ України;

ІКС — інформаційно-комунікаційна система;

КЕП — кваліфікований електронний підпис;

КО — кінцеве обладнання (абонентський термінал/кінцевий пристрій);

КСЗІ — комплексна система захисту інформації;

КЦ — комунікаційний центр;

НД ТЗІ — нормативний документ з технічного захисту інформації;

НКЕК — Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку;

НСД — несанкціонований доступ;

ОДС — оперативно-диспетчерська служба;

ОПТС — опорна/транзитна (підсилювальна) телефонна станція (вузол транзиту у фіксованій мережі);

СКС-7 — система сигналізації №7 (SS7);

ТЗІ — технічний захист інформації;

ЦКМЗ — центр комутації мобільного зв’язку;

2FA — Two-Factor Authentication, двофакторна автентифікація;

ACD — Automatic Call Distribution, система автоматичного розподілу

викликів (черги);

AD — Active Directory, служба каталогів (керування обліковими записами/політиками);

AML — Advanced Mobile Location, технологія підвищеної точності визначення місцезнаходження абонента;

BCP — Business Continuity Plan, план/заходи забезпечення безперервності роботи;

CAD — Computer-Aided Dispatch, система диспетчеризації/ведення інцидентів;

CIA — Confidentiality–Integrity–Availability, тріада «конфіденційність–цілісність–доступність»;

DMZ — Demilitarized Zone, демілітаризована мережна зона;

DR / DRP — Disaster Recovery (Plan), аварійне відновлення / план аварійного відновлення;

EDR — Endpoint Detection and Response, виявлення та реагування на загрози на кінцевих пристроях;

eCall — emergency Call, автоматизований екстрений виклик (з авто під час ДТП);

ESB — Enterprise Service Bus, інтеграційна шина (шина обміну даними);

ESInet — Emergency Services IP network, IP-мережа екстрених служб (для NG112);

LDAP — Lightweight Directory Access Protocol, протокол доступу до служби каталогів;

MFA — Multi-Factor Authentication, багатофакторна автентифікація;

MDM — Mobile Device Management, керування мобільними пристроями;

mTLS — mutual TLS, взаємна TLS-автентифікація (клієнт↔сервер);

NG112 — Next Generation 112, 112 наступного покоління (IP/мультимедіа);

NIST — National Institute of Standards and Technology (США), орган/підходи до стандартів безпеки (у контексті рекомендацій);

NTP — Network Time Protocol, протокол синхронізації часу;

PAM — Privileged Access Management, керування привілейованим доступом;

PSAP — Public Safety Answering Point, пункт (центр) приймання екстрених викликів;

QA — Quality Assurance, контроль якості;

QoS — Quality of Service, параметри якості мережного сервісу;

RADIUS — Remote Authentication Dial-In User Service, протокол централізованої автентифікації/авторизації;

RBAC — Role-Based Access Control, рольова модель керування доступом;

RPO — Recovery Point Objective, допустима втрата даних (точка відновлення);

RTO — Recovery Time Objective, цільовий час відновлення;

SAML — Security Assertion Markup Language, протокол федеративної автентифікації;

SBC — Session Border Controller, прикордонний контролер сеансів (VoIP/SIP);

SIEM — Security Information and Event Management, система збору/аналізу подій безпеки;

SIP — Session Initiation Protocol, протокол встановлення мультимедійних сеансів (телефонія/VoIP);

SIP-I — варіант SIP для взаємодії з ISUP/SS7 (SIP із інкапсуляцією ISUP);

SOC — Security Operations Center, центр моніторингу та реагування на інциденти ІБ;

SoD — Separation of Duties, розподіл повноважень (несумісність ролей);

SSH — Secure Shell, захищений віддалений доступ/адміністрування;

SS7 — Signaling System No.7, система сигналізації №7;

TCO — Total Cost of Ownership, повна вартість володіння;

TOTP — Time-based One-Time Password, одноразовий код на основі часу;

WORM — Write Once Read Many, незмінне сховище (запис один раз — читання багато разів);

ВСТУП

Одним із завдань МВС є надання екстреної допомоги населенню [1]. Комунікаційний центр служби 112 є "серцем" цієї системи — ключовим елементом критичної інфраструктури держави, що забезпечує приймання та оброблення екстрених викликів, координацію дій суб'єктів реагування та порятунок людських життів. Ефективність функціонування цієї служби безпосередньо залежить від безперебійності та захищеності її інформаційно-комунікаційної системи (ІКС). В умовах повномасштабної агресії та постійних кібератак на критичну інфраструктуру, питання кібербезпеки набуває особливої гостроти. Порушення конфіденційності, цілісності або доступності даних може призвести до катастрофічних наслідків: затримки реагування, втрати інформації та невиправданих людських втрат.

Актуальність теми зумовлена комплексним характером сучасних загроз, включаючи кібератаки на системи управління та екстреного реагування. Дослідження захищеності комунікаційного центру 112 є критичною практичною потребою, що впливає на національну безпеку та захист громадян.

Метою дипломної роботи є дослідження захищеності комунікаційного центру служби 112 шляхом аналізу його функціонування, структури та інформаційно-комунікаційних процесів, визначення потенційних загроз і вразливостей, а також формування практичних рекомендацій щодо посилення кіберзахисту та забезпечення безперервності роботи.

Завданнями дослідження є:

- розглянути поняття служби 112, її призначення та роль у системі екстреної допомоги населенню [1];

- проаналізувати загальні функції служби 112 [2],

- дослідити призначення комунікаційного центру та його основні задачі в системі 112 [3];

- описати узагальнену структуру комунікаційного центру (функціональні підсистеми, інформаційні потоки, взаємодія з екстреними службами) [4];

- визначити можливі кіберзагрози та ризики для інформаційно-комунікаційної системи комунікаційного центру;

- запропонувати базові організаційні й технічні заходи захисту (керування доступом, автентифікація, парольна політика) [5,6];

- сформувати висновки щодо поточного рівня захищеності та перспектив підвищення кіберстійкості [7-9].

Методи дослідження включають аналіз наукових та нормативних джерел, системний і структурно-функціональний аналіз, моделювання типових загроз та сценаріїв атак, порівняння підходів до організації безпеки у критичних системах, узагальнення та формування рекомендацій [3-9].

У цій дипломній роботі будуть висвітлені функції та структура комунікаційного центру служби 112 [3,4], аналіз потенційних кіберзагроз, а також рекомендації щодо посилення захищеності [5,6], що допоможе підвищити надійність системи екстреної допомоги [2].

Структура дипломної роботи включає вступ, три розділи, висновки та список використаних джерел. У першому розділі розглядаються функції служби 112: її призначення, роль, засади функціонування та обробка викликів. Другий розділ присвячений опису комунікаційного центру: його задачі, структура та організаційні аспекти. У третьому розділі проводиться дослідження захищеності: аналіз загроз, вразливостей та заходи кіберзахисту [1-9].

Очікуваним результатом є цілісний опис функцій і структури центру, визначення ризиків та практичні рекомендації. Практична цінність роботи полягає в посиленні кіберстійкості критичної інфраструктури та підвищенні ефективності надання екстреної допомоги населенню [2-6].

1 ПРИЗНАЧЕННЯ ТА ФУНКЦІОНУВАННЯ СЛУЖБИ 112

1.1 Що таке служба 112: походження, історія та загальна концепція

Комунікаційний центр "Служба 112" є ключовим елементом системи екстреної допомоги. Служба 112 (система екстреної допомоги за єдиним номером) — це організаційно-технічна модель, у якій для громадян діє одна універсальна «точка входу» в екстреній ситуації. Людина звертається за номером 112, після чого оператор приймає повідомлення, уточнює місце та обставини події, реєструє звернення і маршрутизує його до потрібної(их) служби реагування — поліції, швидкої медичної допомоги, підрозділів ДСНС, аварійної газової служби тощо. Практичний сенс цієї концепції полягає в тому, щоб не витрачати час на вибір між кількома номерами та не повторювати одну й ту саму інформацію різним диспетчерам: центр 112 бере на себе первинну оцінку події та координацію передачі даних у профільні відомства, забезпечуючи швидший старт реагування й можливість комплексного залучення сил, якщо інцидент цього потребує [1,2].

Передумови появи таких систем формувалися поступово разом із розвитком засобів зв’язку, урбанізацією та потребою держави діяти оперативно в умовах криз. До кінця XIX століття оповіщення про пожежі, аварії чи нещасні випадки мало переважно механічний, «візуально-звуковий» характер: церковні дзвони, сигнальні вогні, постріли з гармат, ручні калатала нічних сторожів. Допомога викликалася повільно й нерідко випадково — залежно від того, хто став свідком події та як швидко інформацію передадуть «з рук у руки». Перші професійні пожежні команди та медичні бригади, які часто діяли при монастирях або військових госпіталях, існували автономно: координація між різними підрозділами була слабкою, а час від події до прибуття допомоги міг обчислюватися годинами [1].

Ситуація радикально змінилася з появою телефону та дротового зв’язку, коли з’явилася можливість подати сигнал про небезпеку «тут і

зараз». У 1880-х роках у США набули поширення вуличні пожежні тривожні скриньки (fire alarm boxes), що стало одним із перших кроків до стандартизованих каналів виклику допомоги. Далі почали з'являтися спеціальні номери та сама логіка «центру прийому звернень», де громадянин телефонує в одну точку, а система вже забезпечує правильну комутацію та взаємодію служб. Важливими історичними віхами стали впровадження у Великій Британії (1937 рік) єдиного номера 999 — як реакція на трагічний випадок, коли через перевантаження телефонної лінії люди не змогли вчасно викликати допомогу, — та затвердження в США (1968 рік) номера 911 як універсального, що закріпило модель: диспетчерський центр приймає виклик і самостійно перенаправляє його до потрібних підрозділів [1].

Європейський етап розвитку став відповіддю на зростання мобільності населення та потребу мандрівників отримувати допомогу в будь-якій країні без знання місцевих номерів. Ідея загальноєвропейського екстреного номера була ініційована у 1991 році, а з 1998 року на рівні ЄС було закріплено вимогу забезпечити доступ до 112 [10]. У такій моделі 112 сприймається не як заміна всіх національних номерів «в одну мить», а як універсальний стандарт, що гарантує безоплатний доступ до екстреної допомоги та роботу «паралельно» з локальними номерами, забезпечуючи зрозумілий та однаковий для всіх механізм звернення [1].

Подальший розвиток системи 112 прямо пов'язаний із мобільним зв'язком і переходом від «простого дзвінка» до технологічно насиченого екстреного сервісу. У GSM-мережах номер 112 став стандартом, який технічно підтримується пристроями і дозволяє здійснювати виклик навіть у ситуаціях, коли користувач обмежений у доступі до звичайних функцій телефону (наприклад, при заблокованому екрані), а в окремих сценаріях — за відсутності SIM-карти (залежно від правил мережі та реалізації) [1]. Окрема лінія еволюції — автоматичне визначення місцеперебування абонента під час екстреного звернення. Європейський підхід E112, закладений у рекомендаціях Європейської Комісії № 2003/558/EG, орієнтується на те, щоб

диспетчер отримував геодані швидко та точно, за аналогією до концепції Enhanced 911 (E911) у США. На цій основі логічно розвивається ідея eCall — європейської служби аварійного сповіщення на автотранспорті, коли у разі серйозної ДТП формується автоматизований виклик 112 із передаванням мінімального набору даних, включно з координатами [10].

В Україні довгий час екстрене реагування було «розкладене» між окремими номерами 101, 102, 103 і 104, що створювало типові проблеми в комплексних подіях: при великих ДТП, пожежах із постраждалими чи техногенних аваріях доводилося окремо викликати різні служби, витрачати час на повторний опис ситуації й отримувати допомогу фрагментарно. Шлях до впровадження єдиного номера розпочався на початку 2000-х, а активніша фаза реалізації пов’язується з періодом підготовки до Євро-2012. Нормативне підґрунтя було закріплено законом про систему екстреної допомоги населенню за єдиним телефонним номером 112 (у тексті зазначено як ключову правову основу), а у 2022 році проєкт отримав новий імпульс до фіналізації та практичного розгортання. Далі акцент змістився від «концепції» до поетапного розширення мережі комунікаційних центрів і створення реальної операційної інфраструктури, зокрема через запуск центрів у різних регіонах [1-4]. Станом на 18 грудня 2025 року повідомлялося про запуск офіційного мобільного застосунку “112 Ukraine” як додаткового каналу швидкого звернення, де оператор 112 визначає, які служби залучати [11].

У прикладному вимірі система 112 в Україні позиціонується як «єдине вікно», яке має бути доступним цілодобово й безкоштовно, незалежно від того, з мобільного чи стаціонарного телефону здійснюється звернення, і навіть за обмежених умов (наприклад, коли питання SIM-карти не повинно ставати бар’єром). Окремо підкреслюється інклюзивність: можливість звернення для людей з вадами слуху або мовлення через SMS, а також через відеозв’язок із підтримкою жестової мови; за потреби — залучення спеціалістів для перекладу та допомоги іноземцям або іншим вразливим

групам [1,11]. Такий підхід розширює розуміння екстреної допомоги: це не лише швидкість, а й здатність системи прийняти виклик від будь-якої людини та перетворити його на керовану, документовану процедуру реагування [2].

Ядром цієї моделі виступає комунікаційний центр 112 — центральний вузол, що забезпечує приймання, обробку та розподіл викликів і працює безперервно. На вхідному етапі центр приймає голосові звернення на 112, SMS-повідомлення та інші екстрені комунікації, після чого застосовує механізми автоматичної локалізації (GPS, дані мобільних мереж та інші технології) для визначення місцезнаходження абонента. Далі оператори здійснюють реєстрацію й класифікацію: фіксують тип інциденту (пожежа, злочин, медична криза, витік газу тощо), уточнюють критичні деталі (кількість залучених осіб, ступінь загрози), а за необхідності підключають додаткову підтримку для забезпечення доступності сервісу. На етапі координації відбувається маршрутизація: інформація передається у відповідні диспетчерські екстрених служб, причому у складних випадках оператор 112 може ініціювати одночасне сповіщення кількох відомств, використовуючи єдину базу даних і обмін у режимі реального часу. Паралельно центр забезпечує контроль та документування — фіксацію етапів обробки, зберігання записів дзвінків і дій для аудиту, юридичних потреб та аналітики, що дозволяє оцінювати якість реагування й удосконалювати процеси [3,4].

Щоб система була стійкою до збоїв і пікових навантажень, у її логіці передбачені резервні та масштабувальні механізми. Як обов’язкове дублювання в резервних центрах і організація маршрутів передавання через операторів зв’язку, аби у разі відмови основного центру відбулося автоматичне перемикання без втрати керованості. Окремо наголошується можливість швидкого масштабування — збільшення ресурсів (оператори, серверні потужності) під час надзвичайних ситуацій або воєнних дій, а також спрощена інтеграція зі сторонніми сервісами завдяки сервісній архітектурі

програмного комплексу. У великих регіонах робота може спиратися на значну кількість операторів, а сам центр поступово перетворюється на «інтелектуальну платформу», у якій допускаються елементи прогнозування навантажень та оптимізації ресурсів [3,4].

У підсумку історичний розвиток екстрених служб демонструє послідовний перехід від механічного оповіщення й автономних команд до інтегрованих систем, де вирішальними стають швидкість передачі даних, точність локації, стандартизоване управління інцидентом і здатність координувати кілька служб одночасно. Водночас цей прогрес має зворотний бік: якщо раніше ключовою проблемою була відсутність зв'язку, то сьогодні головним ризиком стає вразливість цифрових комунікаційних каналів та критичної інфраструктури комунікаційних центрів [6]. Саме тому сучасна Служба 112 у наведеній логіці — це не «короткий номер», а комплексна система управління екстреними зверненнями, де технологічність, безперервність роботи, інклюзивність і захищеність є взаємопов'язаними умовами ефективного порятунку людей [1-3].

1.2 Нормативно-правові засади функціонування системи 112 в Україні

Єдина державна система екстреної допомоги за номером 112 створюється як «єдине вікно» для громадян у надзвичайних ситуаціях: людина робить один виклик, а центр 112 приймає, реєструє та передає інформацію до відповідних сил реагування (поліція, ДСНС, екстрена медична допомога, аварійні служби тощо) [2]. Базова правова ідея системи — забезпечити цілодобове, безоплатне приймання екстрених викликів і координоване реагування різних відомств у межах єдиного інформаційного процесу [2].

Загальне законодавче підґрунтя системи 112 е ключовим актом, що визначає правові та організаційні засади створення і функціонування системи 112, є Закон України від 13.03.2012 № 4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112». Закон закріплює поняття системи 112, її складові (центри 112, оперативно-диспетчерські служби, підрозділи екстреної допомоги), а також принципи функціонування: виклики на 112 здійснюються безоплатно, система забезпечує приймання/оброблення викликів, визначення залучених підрозділів, передачу інформації диспетчерським службам, взаємодію під час реагування, облік і зберігання даних щодо викликів [2].

Подальша модернізація правового режиму системи 112 здійснена Законом України від 07.09.2022 № 2581-IX, яким внесено зміни для вдосконалення системи, зокрема введено окремі норми щодо доступу до даних і метаданих та захисту персональних даних (у структурі змін — статті 6-1 і 6-2), а також уточнено фінансові й організаційні аспекти функціонування [3].

Оскільки 112 — це не лише номер, а й інформаційно-комунікаційна інфраструктура державного рівня, важливе значення мають підзаконні акти, які деталізують технологічну модель роботи.

Наказ МВС України від 09.06.2023 № 473 затвердив Положення про інформаційно-комунікаційну систему 112 (ІКС 112). Документ описує структуру ІКС 112, її завдання та порядок функціонування, що дозволяє уніфікувати: приймання/реєстрацію звернень, формування електронних карток подій, маршрутизацію повідомлень до диспетчерських служб, а також вимоги до взаємодії підсистем, резервування та відмовостійкості [4].

Для практичної інтеграції 112 із медичним напрямом реагування діє спільний Наказ МВС України та МОЗ України від 09.02.2024 № 78/225, який затвердив Порядок електронної інформаційної взаємодії ІКС 112 з інформаційно-комунікаційними системами оперативно-диспетчерських

служб центрів екстреної медичної допомоги та медицини катастроф. Це забезпечує узгоджений обмін даними (формати, канали, регламенти, організаційні ролі) для виклику екстреної медичної допомоги через 112 у режимі реального часу [5].

Окремий пласт правового забезпечення пов’язаний із телеком-середовищем, через яке надходить екстрений виклик. У цьому контексті застосовується Закон України «Про електронні комунікації» (16.12.2020 № 1089-IX) як базовий для правил надання електронних комунікаційних послуг та взаємодії з постачальниками мереж [12].

Комунікаційний центр 112 обробляє чутливу інформацію (дані заявника, місце події, медичні/ризикові відомості, службові протоколи), тому правове регулювання обов’язково включає блок захисту інформації та кіберзахисту.

Закон України «Про інформацію» (02.10.1992 № 2657-XII) задає загальні правила інформаційних відносин: режими доступу, засади конфіденційності, законність обробки й використання інформації, що є фундаментом для роботи з даними в центрах 112 [8].

Спеціальні вимоги до захисту даних у системах, де інформація обробляється технічними засобами, визначає Закон України «Про захист інформації в інформаційно-комунікаційних системах» (05.07.1994 № 80/94-ВР). Для ІКС 112 це означає необхідність організаційних і технічних заходів протидії НСД, а також побудову/впровадження комплексного захисту в межах вимог законодавства [9].

Оскільки значна частина даних у 112 є персональними, застосовується Закон України «Про захист персональних даних» (01.06.2010 № 2297-VI), який встановлює загальні правила правомірної обробки персональних даних, обов’язки володільця/розпорядника та гарантії прав суб’єктів даних [13].

Надійна ідентифікація/автентифікація операторів, адміністраторів та юридична значимість електронних протоколів у системі 112 підтримуються нормами Закону України «Про електронну ідентифікацію та електронні

довірчі послуги» (05.10.2017 № 2155-VIII), що регламентує застосування засобів е-ідентифікації та довірчих сервісів (підпис, печатка, часові мітки тощо) в електронній взаємодії [14].

З позиції технічного захисту інформації (ТЗІ) базові принципи державної політики закріплені Указом Президента України від 27.09.1999 № 1229/99, яким затверджено Положення про технічний захист інформації в Україні. Для ІКС 112 це є підґрунтям вимог щодо комплексності заходів захисту (робочі місця, серверна інфраструктура, канали зв'язку, контроль технічних витоків тощо) [15].

Кіберзахист як обов'язкова складова стійкості державних/критичних систем підтримується Постановою КМУ від 19.06.2019 № 518, якою затверджено Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури (організаційні та технологічні умови кіберзахисту, що підлягають виконанню відповідними суб'єктами). Цей документ є орієнтиром для процедур моніторингу, реагування, керування ризиками й відновлення працездатності для систем, критичних для безпеки населення [6].

Термінологічну єдність під час розроблення політик, регламентів і документації із захисту інформації забезпечує НД ТЗІ 1.1-003-99, який встановлює терміни й визначення у сфері захисту інформації в комп'ютерних системах від НСД (використовується як база для коректного трактування понять «загроза», «вразливість», «контроль доступу», «інцидент» тощо) [7].

Окремо, розвиток систем державного рівня в межах цифрової трансформації та інформатизації підтримується Законом України «Про Національну програму інформатизації» (04.02.1998 № 74/98-ВР), у межах якого ІКС 112 може розглядатися як елемент державної інформаційної інфраструктури, що потребує планового розвитку та підтримки [16].

У контексті євроінтеграції важливим є орієнтир на європейську модель Е112, де акцент робиться на автоматичному отриманні/передаванні інформації про місцезнаходження абонента під час екстреного виклику. Це

відображено у Рекомендації Європейської Комісії 2003/558/ЕС (25.07.2003) щодо обробки даних про місцеположення абонента в електронних мережах для надання «location-enhanced» екстрених послуг.

Практично цей підхід є також технологічною основою для концепцій на кшталт eCall (автоматизоване аварійне сповіщення у разі ДТП), де ключовим є швидке і точне визначення локації та передача мінімально необхідних даних для реагування [10].

У сукупності наведені акти формують для системи 112 цілісну рамку вимог, які можна звести до таких груп:

Організаційно-функціональні: цілодобовий прийом і обробка екстрених викликів, безоплатність звернення, фіксація/облік і зберігання даних про виклики, взаємодія з диспетчерськими службами та підрозділами реагування [2-4].

Технологічні та інтеграційні: стандартизована робота ІКС 112, електронний обмін даними між 112 і відомчими системами (зокрема медичним сегментом), резервування та відмовостійкість.

Інформаційна безпека і персональні дані: правомірність обробки інформації/персональних даних, захист від НСД, впровадження організаційних і технічних заходів безпеки, кіберзахист як умова стійкості системи.

Європейська сумісність: рух до моделі Е112 із підсиленою локалізацією виклику як фактором зменшення часу реагування [4-15].

Функціонально система 112 реалізує комплекс завдань, що безпосередньо випливають із її концепції та нормативного регулювання:

Єдиний номер для всіх екстрених служб — спрощує доступ населення до допомоги та мінімізує помилки під час звернення.

Комплексне реагування — оператор здійснює первинну класифікацію події та передає інформацію до профільної служби або кількох служб одночасно при комбінованих інцидентах.

Оптимізація часу реагування — формування електронної картки події та її передавання через ІКС 112 скорочує затримки між прийманням звернення та запуском реагування [2-5].

Доступність для людей з інвалідністю — підтримка альтернативних каналів комунікації (зокрема текстових/мультимедійних) як складова сучасної моделі екстреної допомоги [2,11].

Автоматичне визначення місця події (E112) — локалізація абонента та передавання координат підвищують ефективність допомоги, особливо коли заявник не може повідомити адресу [10].

Цілодобова безоплатна робота — приймання екстрених звернень 24/7 і безоплатність виклику є базовими принципами системи.

Обробка, зберігання та передавання інформації — ведення обліку викликів, збереження даних і передавання їх службам реагування з одночасним дотриманням вимог інформаційної безпеки та захисту персональних даних.

Нормативно-правові засади системи 112 в Україні формують єдину рамку, що поєднує: спеціальне законодавство про 112, підзаконне регулювання ІКС 112 і взаємодії з диспетчерськими службами, а також комплекс норм щодо інформації, персональних даних, технічного та кіберзахисту. У результаті система 112 функціонує як критично важливий комунікаційний механізм держави, де ефективність реагування напряму залежить від належної організації процесів і гарантованого захисту інформації [2-15].

1.3 Функціонування та інтеграція комунікаційного центру служби 112 з іншими системами екстрених служб.

Комунікаційний центр «Служба 112» є ключовим елементом системи екстреної допомоги населенню в Україні, функціонуючи як єдиний номер для виклику всіх профільних екстрених служб. Ця система запроваджена для забезпечення швидкого та ефективного реагування на надзвичайні ситуації, що загрожують життю, здоров'ю, майну чи громадському порядку. За принципом «єдиного вікна», вона інтегрує традиційні методи реагування з сучасними інформаційно-телекомунікаційними технологіями, дозволяючи оперативно залучати ресурси від поліції, рятувальників, медиків та газових служб [2,3].

Система 112 визначена як підсистема Єдиної інформаційної системи Міністерства внутрішніх справ (ЄІС МВС) і призначена для приймання, обробки, зберігання та передачі інформації про екстрені комунікації до оперативно-диспетчерських служб. Вона забезпечує комплексне надання допомоги, включаючи віддалене спостереження за подіями через відеосистеми та аналітичну підтримку рішень [4]. Міністерство внутрішніх справ (МВС) є головним координатором, забезпечуючи технічну координацію викликів, розподіл навантаження між центрами та моніторинг обробки дзвінків [3].

Суб'єкти системи включають Державну службу надзвичайних ситуацій (ДСНС) для реагування на пожежі, вибухи та природні катастрофи; Національну поліцію для боротьби зі злочинами та порушенням порядку; Екстрену медичну службу (під Міністерством охорони здоров'я) для надання медичної допомоги; Екстрену газову службу для усунення витоків газу; операторів телекомунікацій для забезпечення доступу; та місцеві органи влади для логістики та ресурсів [2,12]. Ця інтеграція дозволяє одночасно сповіщати кілька служб у складних інцидентах, забезпечуючи координацію на всіх етапах реагування [5].

Функціонування центру описується як послідовність процесів, що забезпечують швидке та точне реагування. Перший етап — приймання екстреної комунікації (дзвінок, SMS чи інший канал) та її первинна

реєстрація. Оператор фіксує вхідні дані, включаючи час, канал зв'язку та базову інформацію від заявника [4].

Далі відбувається ідентифікація та визначення місцезнаходження абонента. Система має доступ до даних постачальників електронних комунікацій, зокрема для мобільного зв'язку — номер телефону та геолокацію термінала на момент звернення. Це критично для точного направлення допомоги, особливо в випадках, коли заявник не може вказати адресу [10].

Третій крок — класифікація події та заповнення електронної картки інциденту. Оператор використовує уніфікований класифікатор подій для визначення типу ситуації, пріоритетності та необхідних ресурсів. Контролюється повнота та достовірність даних, з можливістю уточнення через зворотний зв'язок.

Четвертий етап — визначення потрібних екстрених служб (однієї або кількох) і передача інформації до відповідних оперативно-диспетчерських служб (ОДС). Інформація з картки інциденту маршрутизується автоматично, забезпечуючи швидке сповіщення .

П'ятий крок включає отримання зворотної інформації про реагування та підтримку зв'язку з заявником за потреби. Оператор моніторить статус інциденту, оновлюючи дані про хід допомоги [4,5].

Нарешті, фіксується весь процес: аудіозаписи, журнали аудиту, протоколи подій. Формується статистика та аналітика для покращення системи [8,9]. Цей цикл забезпечує ефективність, з цілодобовою роботою та дотриманням алгоритмів реагування [2].

Інтеграція на організаційному рівні базується на регламентах та уніфікованих стандартах. Взаємодія між центром 112 та ОДС здійснюється за Регламентом проходження інформації в Інформаційно-комунікаційній системі (ІКС) 112. Уніфікований класифікатор подій забезпечує, щоб усі служби інтерпретували тип інциденту, пріоритет та ресурси однаково [3,4].

Передбачено основні та резервні канали передачі даних, а також роботу єдиного резервного центру 112 у разі збоїв основного [4]. Це гарантує безперервність роботи. Координація включає одночасне сповіщення кількох служб для комплексних інцидентів, з реальним обміном інформацією під час реагування [5].

Місцеві органи влади забезпечують логістику, приміщення для центрів та доступність на локальному рівні [2]. Телекомунікаційні оператори гарантують безбар'єрний доступ до 112 [12]. Цей рівень фокусується на функціональній міжвідомчій співпраці, з механізмами обміну даними та процедурами диспетчеризації [5].

На технічному рівні інтеграція реалізується через електронну взаємодію суб'єктів системи 112 [5]. ІКС 112 включає механізми контролю обміну даними: синтаксичний та семантичний контроль, перевірку повноти файлів, повідомлення про помилки та журнали аудиту [4].

Інформація з електронної картки інциденту передається до систем диспетчеризації поліції (102), ДСНС (101), екстреної медичної допомоги (103) та газової служби (104) у стандартизованому форматі. Зворотні повідомлення про хід реагування оновлюють статус інциденту в реальному часі [5].

Технічна інфраструктура, керована МВС, включає канали передачі інформації, з'єднання диспетчерських служб з підрозділами реагування [4]. Це забезпечує синхронізацію даних між відомчими системами, з акцентом на інформаційну безпеку та стійкість комунікацій [6,9].

ІКС 112 складається з кількох підсистем, що забезпечують інтеграцію [4]. Підсистема електронних комунікацій відповідає за маршрутизацію, прийом, моніторинг, ідентифікацію, позиціонування та передачу даних до ОДС, з підтримкою зворотної комунікації [12].

Інформаційно-облікова підсистема реєструє комунікації та ситуації, класифікує події, обліковує ресурси реагування та закриває інциденти.

Геоінформаційна підсистема підтримує просторову прив'язку подій, з картами, адресами та шарами об'єктів для вибору найближчих ресурсів [4].

Підсистема взаємодії забезпечує міжвідомчий обмін та синхронізацію даних [5].

Підсистема підтримки прийняття рішень надає підказки операторам щодо маршрутів, ресурсів та пріоритетів [4].

Підсистема інформаційної безпеки включає організаційні, технічні та криптографічні заходи захисту даних [6,9]. Ця структура робить ІКС 112 центральною «шиною» для інтеграції всіх екстрених систем [4].

Окрім голосових дзвінків, система підтримує SMS, обмін повідомленнями, відео та інші електронні канали [12]. Звернення можливі через мобільний застосунок «Дія» для зареєстрованих користувачів [11].

Новий офіційний застосунок «112», розроблений МВС, дозволяє виклики навіть без мобільного зв'язку, за наявності Wi-Fi. Користувач авторизується, телефонує через додаток, оператор оцінює ситуацію та направляє служби. Додаток корисний у підвалах, укриттях чи зонах зі слабким покриттям, з планами додати жестову мову [11]. Персональні дані захищені, використовуються лише для обробки викликів [13].

У перспективі NG112 впроваджуються IP-мережі (ESInet) для мультимедіа та стандартизованих сервісів обміну даними [10,12].

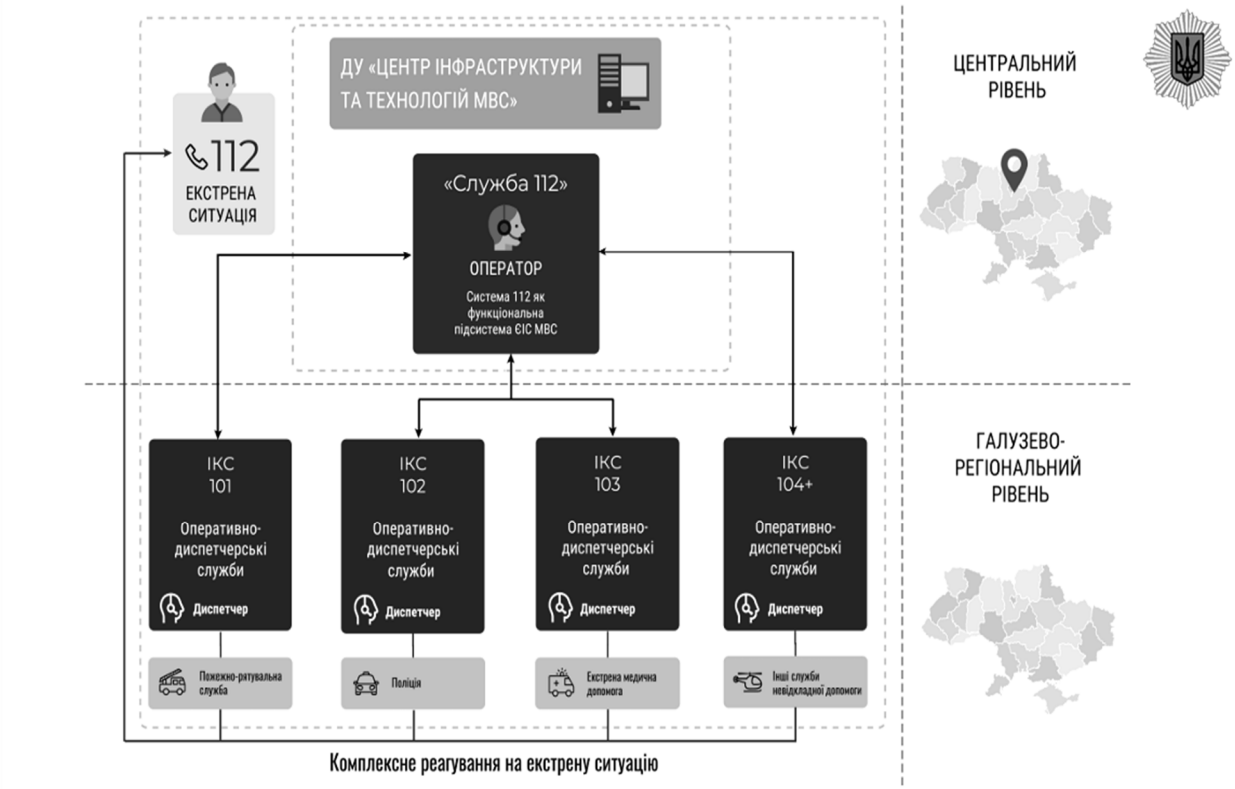

Рисунок 1.1– Структура та принцип роботи системи [4]

Розбудова Служби 112 є частиною євроінтеграційного шляху України, з розширенням географії обробки викликів [10]. Навчання операторів фокусується на ефективному реагуванні [2].

Застосунок 112 вже доступний для завантаження, з можливістю роботи офлайн. Майбутнє — перехід до NG112 з IP-мережами для мультимедіа, покращенням аналітики та інтеграції з іншими системами, як «Дія» [11,12].

Це забезпечить вищу ефективність, доступність та координацію, зменшуючи час реагування та підвищуючи безпеку населення [2].

2 КОМУНІКАЦІЙНИЙ ЦЕНТР СЛУЖБИ 112: ПРИЗНАЧЕННЯ, ЗАДАЧІ ТА СТРУКТУРА

2.1 Загальна характеристика КЦ 112 та кадрове забезпечення.

Призначення та місце комунікаційного центру (КЦ) 112 у системі екстреної допомоги.

Комунікаційний центр Служби 112 (далі — КЦ 112) є центральною диспетчерською ланкою державної системи екстреної допомоги, яка реалізує принцип «єдиного вікна»: громадянин звертається за номером 112, а далі система самостійно організовує залучення потрібних служб [2]. У нормативному полі України функціонування системи 112 визначено урядовим Порядком, затвердженим постановою КМУ № 1031 (із подальшими змінами), де закріплюється загальна логіка роботи системи та суб’єктів взаємодії [17].

На практичному рівні КЦ 112 — це не просто «кол-центр», а структурний підрозділ з цілодобовою роботою (24/7), регламентованими процедурами приймання повідомлень, фіксації даних, пріоритизації та маршрутизації подій. Його ключові функції полягають у тому, щоб швидко прийняти звернення, уточнити критичні дані (що сталося, де сталося, чи є загроза життю/майну), зафіксувати інформацію в електронній картці інциденту та забезпечити взаємодію з екстреними службами до завершення реагування. Ця логіка підтверджується і в офіційних повідомленнях МВС про роботу Служби 112, де наголошено на координації реагування та технологічній основі системи [11].

КЦ 112 слід розглядати як «операційне ядро» системи 112: саме він перетворює звернення громадян у керовану процедуру реагування, забезпечуючи стандартизацію обробки викликів, фіксацію даних і узгоджену роботу кількох служб в єдиному інформаційному контурі [3,4].

Організація роботи КЦ 112 та основні процеси обробки викликів.

Типовий процес роботи КЦ 112 складається з послідовних етапів: прийом повідомлення, уточнення обставин, класифікація інциденту, визначення пріоритету, передача до відповідних служб, контроль прийняття інформації та документування результату [4]. Важливо, що у 2025 році урядовими змінами закріплено підхід до уніфікації класифікації подій: передбачено наявність «уніфікованого класифікатора подій та екстрених ситуацій», який розробляється МВС і використовується під час обробки звернень. Це прямо підсилює методичну єдність роботи операторів у різних регіонах [17].

Окремим напрямом є інклюзивність і доступність. За офіційною інформацією МВС, виклики можуть оброблятися з урахуванням потреб людей з порушеннями слуху чи мовлення: комунікація здійснюється через відеозв'язок із операторами, які володіють жестовою мовою (процедурно — через попереднє SMS і отримання посилання на з'єднання). Крім того, 65 з понад 260 операторів володіють іноземними мовами (англійська, польська, іспанська тощо), що дозволяє обслуговувати іноземних громадян. Система також інтегрує європейські технології, такі як автоматичне оповіщення про дорожні пригоди (e-Call, 43 повідомлення оброблено) та переадресацію з номеру 911 [10,11].

Ще один компонент — розширення каналів звернення та стійкість у кризових умовах. У грудні 2025 року МВС повідомило про запуск офіційного застосунку «112», який може працювати навіть без мобільного зв'язку (наприклад, в укритті за наявності Wi-Fi), а також задекларувало подальше розширення функціоналу, зокрема опцію виклику жестовою мовою в застосунку [11].

Організаційна модель КЦ 112 будується на стандартизованому «ланцюгу реагування» (прийом → класифікація → маршрутизація → контроль → фіксація результату) [4]. Технічне забезпечення КЦ 112 відповідає європейським стандартам: воно включає передові рішення для

швидкої передачі даних, високий рівень кібербезпеки та безперервність роботи (оператори продовжують обробку викликів навіть під час повітряних тривог з укриттів) [10]. Закріплення уніфікованого класифікатора та розвиток додаткових каналів звернення (зокрема мобільного застосунку) підвищують керованість, доступність і стійкість системи, що критично важливо в умовах воєнного стану та пікових навантажень [6,11,17].

Кадрове забезпечення КЦ 112: ролі, чисельність і принципи формування змін.

Ефективність КЦ 112 напряму залежить від кадрової моделі. Типова структура персоналу включає такі ролі:

– Оператор 112 (call-taker): приймає звернення, уточнює обставини, заповнює картку події та визначає категорію інциденту.

– Диспетчер/координатор взаємодії: маршрутизує подію до потрібної служби, контролює підтвердження прийняття та уточнення даних [4,5].

– Старший зміни/супервізор: контролює роботу зміни, якість обробки викликів, вирішує нестандартні випадки та організовує взаємодію при масових інцидентах.

– Фахівці технічної підтримки (IT/зв’язок): забезпечують працездатність систем (телефонія, мережа, робочі місця, запис розмов, інтеграції) [4,12].

– Адміністратор безпеки / фахівець з ТЗІ: контролює доступи, журналювання, політики безпеки та реагування на інциденти інформаційної безпеки [6,9].

– Аналітик/контроль якості: аналізує статистику викликів, готує звітність, проводить аудит помилок та покращує регламенти й навчання.

Такий розподіл дозволяє відокремити «прийом інформації» від «керування реагуванням» і «контролю якості», що знижує помилки під час пікових навантажень [4].

Орієнтовна чисельність персоналу (умовно, залежно від навантаження та населення) у регіональних КЦ зазвичай оцінюється в межах 60–120 осіб із

10–20 працівниками одночасно в зміні, тоді як для міських/міжмуніципальних центрів — 15–40 осіб і 3–8 у зміні. Ключовими чинниками розрахунку є прогнозована кількість звернень, середня тривалість розмови, час на заповнення картки події, необхідність резерву на пікові години, а також вимога безперервної роботи 24/7 із заміщенням у разі відпусток і тимчасової непрацездатності.

Водночас офіційні дані демонструють реальні масштаби кадрового ядра. Наприклад, у повідомленні МВС про роботу центру в Дніпрі зазначено, що там працюють понад 70 операторів, які цілодобово приймають виклики з низки областей центрального та східного макрорегіонів.

Також МВС повідомляло, що станом на липень 2025 року у Службі 112 налічувалося 265 операторів, частина з яких обробляє дзвінки іноземними мовами; окремо фіксується значний обсяг звернень жестовою мовою.

Кадрова модель КЦ 112 повинна поєднувати ролі «оперативного фронту» (оператори та координатори) з управлінським контролем (супервізори) і підтримувальними функціями (ІТ/зв’язок, безпека, аналітика). Практика реальних центрів (зокрема Дніпра) підтверджує, що кадрове ядро вимірюється десятками операторів на центр, а загальна чисельність Служби зростає разом із географією покриття та впровадженням інклюзивних і багатомовних сценаріїв обслуговування [4,11].

Фінансові джерела забезпечення КЦ 112.

Фінансове забезпечення КЦ 112 має змішаний характер і включає як державні ресурси (утримання персоналу, експлуатаційні витрати, зв’язок, кіберзахист, модернізація), так і міжнародну фінансову підтримку, спрямовану на розбудову інфраструктури та цифрових компонентів [2,3].

Ключовим міжнародним джерелом у публічному просторі є співпраця МВС з Європейським інвестиційним банком. У лютому 2025 року МВС прямо повідомляло, що проєкт розбудови центрів передбачає надання 40 млн євро в межах кредитної угоди на розбудову відповідних центрів [18].

Окремо ЄІБ у жовтні 2024 року оголосив про пакет підтримки на 52 млн євро для впровадження системи 112: він включає грантову складову ЄС та заплановану позику ЄІБ на 40 млн євро; у деталізації ЄІБ також зазначає, що пакет містить позику 40 млн євро та два гранти ЄС (інвестиційний грант і технічну допомогу), які в сумі формують грантову частину.

Такі джерела фінансування важливі тим, що дозволяють не лише «побудувати приміщення», а профінансувати комплексні елементи системи: сучасні кол-центри, ІТ-інфраструктуру, інтеграції між службами, підвищення стійкості та відповідність європейським стандартам організації екстреної допомоги [10].

Фінансування КЦ 112 доцільно трактувати як довгострокову інвестицію в критично важливу соціальну інфраструктуру. Поєднання державного утримання з міжнародними кредитно-грантовими інструментами дає змогу одночасно забезпечувати безперервну роботу (зарплати, зміни, зв’язок, кіберзахист) і масштабувати інфраструктуру (нові центри, інтеграції, цифрові сервіси) [2,3,18].

Поточний стан мережі КЦ 112 та плани розширення.

Розбудова Служби 112 в Україні відбувається поетапно через створення регіональних центрів, які покривають макрорегіони. Перший комунікаційний центр було офіційно відкрито у Києві в липні 2023 року; тоді ж МВС публічно декларувало план масштабувати 112 спершу в усіх містах-мільйонниках, а далі — на всю територію держави.

Наступним кроком стало розширення мережі на захід: МВС повідомляло про запуск центру у Львові з 1 грудня 2023 року та поступове підключення західних областей упродовж перших місяців 2024 року.

У 2024 році відбулося посилення центрального та східного напрямів: центр у Дніпрі розпочав роботу у вересні, після чого МВС офіційно зафіксувало його роль у покритті низки областей та окремо зазначило кадровий склад (понад 70 операторів).

Щодо подальшого розширення, МВС неодноразово заявляло про підготовку 4-го центру в Одесі. У жовтні 2024 року прямо зазначалось, що одеський регіональний центр має охопити південні області.

Паралельно з географічним розширенням відбувається функціональне нарощування. Станом на лютий 2025 року МВС повідомляло, що від початку запуску (1 липня 2023 року) до центрів надійшло майже 5 млн викликів, а понад 768 тис. були передані до екстрених служб; також фіксувались звернення через e-Call і переадресація викликів з 911.

Станом на липень 2025 року МВС повідомило про понад 7 млн викликів за два роки роботи та значний обсяг інклюзивних звернень жестовою мовою, що підтверджує перехід від «пілота» до системи з масовим навантаженням.

У грудні 2025 року запроваджено новий інструмент доступу — застосунок «112», який, за офіційною позицією МВС, працює в умовах відсутності мобільного сигналу та матиме подальший розвиток (зокрема, жестова мова в застосунку).

Розширення Служби 112 в Україні має дві взаємопов’язані траєкторії: територіальну (створення центрів макрорегіонального покриття) та технологічну (нові канали звернень, уніфікація класифікації подій, інтеграції на кшталт e-Call, підвищення стійкості й доступності). Сукупність офіційно задекларованих планів (Одеса як південний вузол) і впроваджених рішень (мобільний застосунок) свідчить, що наступний етап розвитку логічно пов’язаний не лише з «кількістю центрів», а з якістю сервісу, швидкістю маршрутизації та здатністю працювати в деградованих умовах зв’язку [10,11].

Загальний висновок до розділу.

КЦ 112 в Україні формується як сучасна диспетчерсько-координаційна структура, що поєднує регламентовані процеси обробки звернень, кадрову модель із чітким розподілом ролей та фінансово-технологічну основу для масштабування [3,4,11,18]. Наявні офіційні дані про етапи розгортання

центрів (Київ → Львів → Дніпро → підготовка Одеси), обсяги викликів і розвиток інклюзивних каналів підтверджують системний характер впровадження [11]. Додатково, міжнародні кредитно-грантові інструменти та нормативні зміни (зокрема щодо класифікатора подій) створюють умови для переходу від «мережі центрів» до повноцінної, уніфікованої національної системи екстрених комунікацій, сумісної з європейськими підходами [10,17,18].

Плани розширення системи КЦ 112 передбачають повне покриття всієї території України до 2027 року, з відкриттям додаткових центрів у Харкові, Запоріжжі та інших регіонах. Згідно з стратегією МВС, у 2026 році заплановано інтеграцію з системами "розумного міста" у великих агломераціях, впровадження AI для автоматичного категоризації викликів та розширення підтримки жестової мови до 100% операторів. Фінансування розширення включатиме гранти від ЄС (до 50 мільйонів євро) та державні інвестиції (близько 200 мільйонів гривень щорічно) [18]. Очікується збільшення штату до 600 осіб на національному рівні, з акцентом на кібербезпеку та мультимовність [11]. Ці плани спрямовані на підвищення ефективності реагування, скорочення часу обробки викликів та інтеграцію з європейською системою E112 [10].

2.2 Як побудований КЦ 112: організаційна і технічна структура.

Система екстреної допомоги населенню за єдиним телефонним номером 112 (далі – Система 112) є комплексною структурою, що забезпечує оперативне реагування на надзвичайні ситуації в Україні [2]. Вона побудована на принципах централізованого управління, інтеграції служб та використання сучасних інформаційно-комунікаційних технологій. Організаційна та технічна структура Системи 112 визначена Законом

України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» від 13 березня 2012 року № 4499-VI, а також іншими нормативними актами, такими як Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 [6] та Наказ МВС України від 09 червня 2023 р. № 473 [4]. Система інтегрує роботу аварійно-рятувальних служб, поліції, медичної допомоги та інших суб'єктів, забезпечуючи єдиний вхідний пункт для викликів [5].

Організаційна структура Системи 112 включає ієрархічну систему центрів обробки викликів (Public Safety Answering Points – PSAP), які координують дії спеціалізованих служб [4]. На національному рівні управління здійснюється Міністерством внутрішніх справ України (МВС), Державною службою України з надзвичайних ситуацій (ДСНС), Міністерством охорони здоров'я (МОЗ) та іншими центральними органами виконавчої влади (ЦОВВ) [2]. Робоча група з впровадження включає представників МВС, ДСНС, МОЗ, Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку (НКЕК), Служби безпеки України (СБУ), Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) та асоціацій операторів зв'язку [12].

На регіональному рівні функціонують центри 112, пілотні проєкти яких запущено в Львівській, Київській, Дніпропетровській областях. Наприклад, у Львівській області центр розташовано в будівлі ГУ ДСНС, де залучено обласну державну адміністрацію (ОДА), обласну раду, ГУ ДСНС, МВС, Департамент охорони здоров'я та ПрАТ «Львівгаз». Оператори центрів – це диспетчери, які приймають виклики, проводять первинну оцінку ситуації, реєструють дані та передають інформацію відповідним службам (поліція – 102, пожежна охорона – 101, швидка допомога – 103, газова служба – 104) [4]. Оператори володіють кількома мовами (українська, англійська, польська), серед них є психологи для роботи з викликами, пов'язаними з кризовими ситуаціями [11]. Закон № 2581-IX від 07 вересня 2022 р.

встановлює 112 як єдиний номер, скасовуючи окремі номери служб, та створює підстави для єдиного центру обробки викликів з технічною координацією, розподілом навантаження та моніторингом [3].

Технічна структура Системи 112 базується на програмно-апаратному комплексі «Оберіг», розробленому Державним підприємством «Українські спеціальні системи» ДСНС та Інститутом проблем математичних машин і систем НАН України [11]. Комплекс включає сервери для обробки викликів, бази даних для фіксації подій у реальному часі, засоби відеоспостереження та електронні пристрої для локалізації абонентів (Е112 – автоматичне визначення місцезнаходження) [10]. Виклики приймаються з будь-яких телефонів (стаціонарних, мобільних), безплатно, з пріоритетом у мережі, та вимагають SIM-карти для запобігання зловживанням [12]. Технічні компоненти забезпечують: цілодобовий диспетчерський вузол “єдиного вікна”, що поєднує людей, регламенти та IT/телеком-інфраструктуру в один керований процес: прийом звернення → оцінка/класифікація → передача та координація реагування → контроль виконання → документування і аналітика [4].

Організаційна структура КЦ 112 .

Організаційно КЦ 112 будується за змінним (черговим) принципом 24/7 із чітким розподілом ролей. Типова модель включає такі рівні та групи:

а) Керівництво та управління (адміністративний рівень)

Керівник КЦ / начальник зміни (черговий менеджер) – відповідає за безперервність роботи, дотримання регламентів, взаємодію з керівництвом екстрених служб, реагування на нестандартні ситуації (масові події, перевантаження, відмова систем).

Координатор/супервайзер залу – оперативно керує роботою операторів: розподіляє навантаження, контролює якість, приймає ескалації, організовує резервування робочих місць.

б) Оперативний рівень (операційний зал):

Оператор прийому викликів (call-taker)

Приймає звернення (голос/повідомлення/інші канали), ідентифікує проблему, уточнює ключові дані, створює *картку інциденту* та визначає первинний пріоритет.

Диспетчер/маршрутизатор (dispatcher)

Передає інцидент у відповідну службу (101/102/103/104) або одночасно в кілька служб, супроводжує інцидент до завершення, фіксує зміни статусів [4,5].

Оператор координації (за потреби, у складних інцидентах)

Підтримує зв’язок із підрозділами на місці події, об’єднує інформацію від різних служб, забезпечує узгодженість дій у мультивідомчих подіях .

в) Підтримка якості та навчання:

Фахівець з контролю якості (QA) – вибірково перевіряє записи, картки інцидентів, дотримання скриптів і регламентів; формує рекомендації щодо покращення.

Інструктор/тренер – первинна підготовка нових операторів, тренування на типових сценаріях, відпрацювання кризових випадків.

г) Технічна та безпекова підтримка (бек-офіс):

Системний адміністратор / інженер зв’язку – працездатність телефонії, мережі, серверів, резервування, оновлення [12].

Адміністратор прикладних систем (CAD/CRM/ГІС) – довідники, шаблони, інтеграції, права доступу.

Фахівець з кіберзахисту/ІБ (або відповідальний за ІБ) – контроль доступів, журнали, інциденти ІБ, сегментація, взаємодія із SOC/службою безпеки [6,9].

Процесна модель роботи (як рухається інформація).

Організаційна структура завжди “підв’язана” до стандартизованого процесу [4] і складається з таких кроків.

Приймання звернення (дзвінок/повідомлення) → автоматична реєстрація факту звернення .

Створення електронної картки інциденту: хто звернувся, що сталося, де сталося, чи є загроза життю .

Класифікація (тип події) та пріоритезація (критичність).

Маршрутизація: передача в одну/кілька служб, підтвердження прийняття.

Супровід: уточнення даних, оновлення статусів, фіксація ключових рішень .

Закриття інциденту: результат реагування, підсумок, позначки для аналітики.

Контроль якості та звітність: вибірковий аудит, метрики, виявлення "вузьких місць".

Технічна структура КЦ 112 (канали, системи, інфраструктура).

Технічна структура КЦ 112 зазвичай будується як три взаємопов'язані контури: комунікаційний, інформаційний (обробка), інтеграційно-інфраструктурний [4,5].

а) Комунікаційний контур (вхідні/вихідні канали)

Телефонія 112: шлюзи до операторів зв'язку, маршрутизація, пріоритезація виклику, черги (ACD), переадресація/перерозподіл на резервний майданчик.

Запис розмов (Call Recording) із прив'язкою до картки інциденту [8].

Додаткові канали (за наявності): SMS/чат, eCall (для авто), інші цифрові канали звернень [12].

б) Контур обробки (робочі місця та прикладні системи)

АРМ оператора (робоче місце): гарнітура/телефонія, екран з чергою викликів, форма внесення даних.

CAD/CRM (система ведення інцидентів): картка події, статуси, історія, шаблони питань, довідники.

ГІС-модуль (картографія): відображення адреси/координат, прив'язка до адміністративних зон, потенційні ризикові об'єкти.

База знань і сценарії (скрипти): підказки оператору, алгоритми опитування, інструкції з першої допомоги (за регламентом) [4].

в) Інтеграційно-інфраструктурний контур (обмін даними, надійність, захист)

Інтеграція з екстреними службами (101/102/103/104):

1) обмін електронними повідомленнями/картками (API, захищені канали, інтеграційна шина/ESB);

2) підтвердження прийняття інциденту та повернення статусів (виїзд/прибуття/завершення) [5].

Серверна інфраструктура: сервери прикладних систем, БД, журналювання, сховище записів.

Безперервність роботи (BCP/DRP):

- резервування ключових компонентів (телефонія, БД, мережа);
- резервний майданчик або “гарячий/теплий” резерв;
- UPS + генератор, дублювання інтернет-каналів [4].

Кібер- та інформаційна безпека: сегментація мережі, міжмережеві екрани, контроль доступу (RBAC), журналювання, резервні копії, захист персональних даних [6,9,13].

Таблиця 2.1 - Узагальнена схема структури (логіка взаємодії) [4]

Громадянин → (112: голос/повідомлення) → Телефонна → платформа/ACD → Оператор (АРМ)
Запис розмов
Система інцидентів (CAD/CRM)
ГІС/геолокація ←→ Картка інциденту ←→ Довідники/скрипти
Інтеграція/API/ESB → 101 (ДСНС) / 102 (Поліція) / 103 (ЕМД) / 104 (Газ)
Статуси реагування → Картка інциденту → Аналітика/звіти

Принципи масштабування та розвитку КЦ 112.

Масштабування комунікаційного центру 112 — це кероване нарощування спроможності (людей, процесів, техніки та інтеграцій) без втрати якості, швидкості реагування й інформаційної безпеки [4]. На практиці КЦ 112 має бути готовим одночасно до двох сценаріїв: поступового зростання навантаження (розширення території, підключення нових служб, цифрові канали) і пікових/кризових стрибків (масові події, аварії, воєнні загрози, сезонні піки) [6].

Нижче наведено ключові принципи, яких дотримуються під час розвитку КЦ 112.

а) Поетапність і керованість змін.

Розвиток КЦ 112 повинен відбуватися поетапно, з контрольними точками та вимірюваними результатами:

1) спочатку оптимізуються регламенти й маршрутизація (щоб зняти "організаційні затори");

2) далі нарощуються робочі місця й канали зв'язку [12];

3) потім — інтеграції, аналітика, резервування та кіберзахист [6].

Критично важливо: кожна зміна (новий канал, нова інтеграція, новий сценарій) має проходити пілотування → тестування → навчання персоналу → введення в промислову експлуатацію.

б) Модульність архітектури.

Технічна структура КЦ 112 повинна бути модульною, щоб додавання потужностей не вимагало "перебудови всього центру".

Модульність означає:

1) можливість додавати АРМ (робочі місця) пакетами;

2) горизонтальне нарощування прикладних сервісів (CAD/CRM, ГІС, запис розмов, інтеграційні шлюзи);

3) "підключення" нових служб через стандартні інтерфейси (API/шина/черги повідомлень), а не через ручні або разові рішення [5].

в) Стандартизація процесів і ролей.

Зі збільшенням масштабу зростає ризик хаосу, тому обов'язкові:

1) єдині скрипти опитування (що/де/скільки постраждалих/яка загроза);

2) єдині критерії пріоритезації (життєва загроза, пожежа, кримінальний ризик тощо);

3)стандартні статуси інциденту та правила їх зміни ;

4)регламент “хто приймає рішення” у нестандартних випадках (ескалація до супервайзера/начальника зміни).

Стандартизація потрібна не для “формальності”, а для того, щоб будь-яка зміна персоналу/зміни/підрозділу не руйнувала якість.

г) Організаційне масштабування персоналу.

Нарощування кількості операторів — лише частина задачі.

Паралельно мають масштабуватися:

1) супервізія (щоб контролювати якість і підтримувати операторів у складних випадках);

2) навчання (постійні тренування сценаріїв, оновлення інструкцій);

3) контроль якості (QA) (перевірка записів і карток інцидентів);

4) психологічна стійкість персоналу (профілактика вигорання, ротації, підтримка в кризових викликах).

Для пікових навантажень ефективним є принцип резервної спроможності:

- резервні оператори (додаткові ставки/підміни);

- крос-навчання (частина працівників здатна підсилити прийом викликів);

- сценарій “кризового режиму” (скорочений скрипт, швидша маршрутизація, пріоритет критичних викликів).

д) Масштабування комунікаційних каналів і черг.

Для зростання викликів головне — не “додати телефонів”, а забезпечити:

1) керування чергами (ACD), правила розподілу (за навичками, мовою, типом події);

2) контроль параметрів: середній час відповіді, довжина черги, відсоток втрачених викликів [4];

3) достатню пропускну здатність шлюзів/каналів та резервні маршрути [12].

Окремий напрям розвитку — омніканальність: поступове додавання текстових звернень, цифрових повідомлень, спеціальних каналів для людей з порушенням слуху/мовлення — але лише якщо центр готовий процесно й технічно (черги, оператори, правила фіксації) [11,12].

е) Надійність і безперервність (BCP/DR).

КЦ 112 не може “зупинитися”, тому масштабування завжди включає принципи відмовостійкості:

1) резервування ключових вузлів (телефонія, бази даних, мережа, запис розмов);

2) наявність резервного майданчика (або можливість швидкого перенесення функцій);

3) визначені показники RTO/RPO (за який час відновлюємо роботу і яка допустима втрата даних);

4) регулярні навчальні “перемикання” на резерв (щоб резерв був не “на папері”) [6].

Також важливе енергозабезпечення: UPS/генератор, дублювання критичних ліній і зв’язку [4].

є) Кібербезпека як умова розвитку (Security by Design).

Будь-яке розширення (нові АРМ, нові інтеграції, нові канали) збільшує площу атаки. Тому розвиток має базуватися на:

1) сегментації мережі та принципі “мінімально необхідного доступу” [9];

2) ролях і правах (RBAC), багатофакторній автентифікації, контролі привілейованих акаунтів [6,14];

3) журналюванні та моніторингу подій (централізовані логи, кореляція інцидентів) [9];

4) резервних копіях і тестах відновлення;

5) керуванні вразливостями (оновлення, сканування, контроль конфігурацій).

Особливо критично — безпека інтеграцій між службами: обмін має бути автентифікований, контрольований, протоколюваний, із чіткою відповідальністю сторін.

ж) Масштабування інтеграцій і взаємодії зі службами.

З розвитком системи зростає кількість підключених структур (пожежно-рятувальна, поліція, ЕМД, газ, місцеві аварійні служби тощо). Щоб це не перетворилося на десятки “ручних мостів”, потрібні принципи:

1) уніфікований формат картки інциденту (обов’язкові поля, довідники, коди причин);

2) стандартизовані статуси та підтвердження прийняття;

3) асинхронний обмін (черги повідомлень), щоб збій однієї сторони не зупинив весь центр;

4) “деградований режим” — як діяти, якщо інтеграція тимчасово недоступна (резервний канал/голос/ручна реєстрація з подальшим внесенням у систему).

з) Дані, аналітика та управління якістю.

Розвиток КЦ 112 без аналітики — це “збільшення штату наосліп”. Тому потрібні:

1) KPI (час відповіді, час реєстрації інциденту, частка ескалацій, повторні звернення, хибні/зловмисні виклики);

2) контроль якості заповнення карток (повнота полів, точність адрес, коректність класифікації);

3) регулярні звіти для управлінських рішень: де вузькі місця, у які години пік, які типи інцидентів ростуть.

Окрема задача — якість довідників (адреси, райони, типи подій, об’єкти ризику), бо від них напряму залежить швидкість маршрутизації [4-6].

и) Фінансова сталість і керування ресурсами.

Масштабування має плануватися з позиції ТСО (повна вартість володіння), а не лише “купили обладнання”. Важливо врахувати:

1) ліцензії, підтримку, оновлення, зберігання записів і даних;

2) сервісні контракти, SLA, заміну компонентів;

3) витрати на навчання й сертифікацію персоналу;

4) резервування (бо надійність завжди коштує додатково).

Практичний принцип: краще нарощувати модульно, щоб витрати йшли “в ногу” з реальним ростом навантаження [18].

Напрями розвитку (як “дорожня карта”) як 3 горизонти:

1) Короткостроково (організаційне посилення):

- уточнення регламентів, скриптів, пріоритезаці;
- KPI + контроль якості;
- підсилення супервізії/навчання.

2) Середньостроково (технічне нарощування):

- додаткові АРМ і потужності телефонії/черг;
- покращення інтеграцій, резервні канали;
- резервування критичних компонентів.

3) Довгостроково (цифрова еволюція):

- омніканальність (текст/цифрові звернення) [12];
- розширена аналітика (дашборди, прогноз навантаження);
- інтелектуальні підказки оператору (обережно, з людським контролем і вимогами до захисту даних) [4-6].

Узагальнюючий висновок.

Принципи масштабування КЦ 112 зводяться до балансу трьох речей: спроможність (люди+техніка), безперервність (резервування) і безпека (контроль доступів/даних/інтеграцій). Якщо розвивати лише один елемент (наприклад, збільшити кількість операторів без резервування та аналітики), центр швидко досягне межі ефективності й почне втрачати якість обробки інцидентів [4,6].

Система підтримує багатомовну обробку викликів, інтеграцію з eCall (автоматичне сповіщення про аварії в транспорті) та веб-сайт для онлайн-звернень (архівований на__http://www.112.gov.ua/) [10,11]. Бюджет на розгортання в ключових містах склав близько 630 млн грн, з акцентом на інформаційно-телекомунікаційні технології для взаємодії суб'єктів [18].

У 2022 році прийнято Закон № 7581, який посилює технічну базу для повного впровадження по всій країні [19].

Система 112 забезпечує швидке реагування , зменшення дублювання зусиль служб та підвищення ефективності допомоги [2]. Організаційно-технічна структура спрямована на інтеграцію традиційних методів реагування з цифровими технологіями, що робить її ключовим елементом національної системи безпеки [4,6].

2.3 Задачі КЦ 112 та логіка обробки інциденту

Комунікаційний центр (КЦ) 112— це “вхідні двері” державної системи екстреної допомоги: він приймає звернення громадян, перетворює їх на структуровану «картку інциденту» і забезпечує швидке залучення потрібних служб (101–104). Ключова ідея: людина робить один виклик, а система сама організовує правильну маршрутизацію, пріоритет і взаємодію [2].

КЦ 112 (Служба 112) – структурний підрозділ МВС, що обробляє екстрені комунікації. Завдання: приймання викликів, визначення типу інцидента, геолокація, передача даних службам (101-104), фіксація процесу, зворотний зв'язок [4].

Оператор приймає виклик, класифікує (пожежа, злочин тощо), передає через API або електронну систему [5]. Взаємодія: з постачальниками комунікацій для даних про абонента, з геопорталом для локації [12].

Основні задачі КЦ 112 :

а) Приймання екстрених звернень і гарантія доступності

КЦ 112 забезпечує приймання звернень через доступні канали (передусім голос, а також — за наявності реалізації — текстові/цифрові канали) [12]. Окрема вимога сучасних систем 112 — доступність для осіб з інвалідністю (альтернативні формати комунікації, рівноцінність сервісу) [2].

б) Швидкий збір мінімально достатньої інформації (“критична трійка”)

Оператор збирає рівно те, що запускає реагування, без зайвих розмов:

Де сталося? (адреса/орієнтири/координати/напрям руху для ДТП)

Що сталося? (тип події + короткий опис)

Що потрібно? (які служби, чи є загроза життю, чи треба багатослужбове реагування)

в) Класифікація та пріоритизація

Кожне звернення приводиться до стандартизованого вигляду: визначається категорія (медичний/пожежний/кримінальний/техногенний тощо), рівень загрози, кількість постраждалих, ризики для оточення. Далі встановлюється пріоритет (умовно: “негайно” → “терміново” → “звичайне” → “консультаційне/неекстрене”).

г) Маршрутизація: передача або диспетчеризація

Є два організаційні підходи, які на практиці можуть комбінуватися:

Дворівнева модель: КЦ 112 приймає, класифікує та передає дзвінок/картку до профільної диспетчерської 101/102/103/104.

Єдиний PSAP: КЦ 112 не лише приймає, а й диспетчеризує ресурси (call-taking + dispatch) у межах одного центру [4].

д) Супровід інциденту до закриття

Після передачі КЦ 112 контролює, що звернення прийняте службою, за потреби уточнює дані (повторний контакт із заявником), підтримує багатосторонню взаємодію при складних подіях і фіксує результат (закриття картки) [5].

е) Фіксація, доказовість, якість, аналітика

КЦ 112 забезпечує запис розмов, журнал дій оператора, контроль часових параметрів і аналітику (частка хибних/нецільових, типові помилки, навчальні кейси). Матеріали інциденту архівуються (у типовій моделі ІКС 112 — зберігання 5 років) [8].

“Доставка” виклику 112 до КЦ: нормативно-технічна логіка (Наказ №89).

Щоб оператор КЦ 112 міг відповісти, виклик має бути технічно доставлений мережею оператора зв’язку до ІКС 112. Це врегульовано Порядком передачі викликів під час здійснення екстрених комунікацій за номером 112 (Наказ Адміністрації Держспецзв’язку №89 від 06.02.2023, реєстрація в Мін’юсті №493/39549) [20].

Головні правила доставки:

а) оператори електронних комунікацій зобов’язані забезпечити передачу голосових викликів 112 до комунікаційних центрів “Служба 112” [20];

б) передача організовується одночасно до основного та резервного КЦ 112;

в) основний і резервний КЦ працюють у режимі розподілу навантаження (тобто це не “пасивний резерв”, а частина робочої схеми);

г) якщо оператор не має прямого включення в КЦ 112, допускається передача через мережі інших операторів;

д) виклики 112 повинні мати пріоритетне обслуговування;

е) мобільний виклик 112 має бути можливим без SIM-карти (у такому випадку номер абонента не передається, але виклик мусить бути доставлений);

є) передавання здійснюється з використанням SIP/SIP-I або СКС-7;

ж) оператор повинен передавати КЦ 112 супровідну інформацію:

1) для фіксованого зв’язку — абонентські дані та адреса встановлення кінцевого обладнання;

2) для мобільного — номер абонента та місцезнаходження терміналу на момент виклику, а за наявності технічної можливості — AML (підвищена точність координат).

Окремо важливо: callback із номера “112” від КЦ до заявника не є екстреною комунікацією і виконується як звичайний виклик — це юридично й технічно відділяє “екстрений канал” від стандартної телефонії [20].

“Доставка” виклику 112 до КЦ: як працюють схеми (Наказ №89)

Щоб оператор Комунікаційного центру (КЦ) 112 зміг прийняти звернення, виклик має бути технічно доставлений із мережі оператора зв’язку до Інформаційно-комунікаційної системи 112 (ІКС 112) [20]. Саме цю частину (маршрут, протоколи, резервування, дані, що супроводжують виклик) описує Порядок передачі викликів під час здійснення екстрених комунікацій за єдиним телефонним номером 112 (Наказ №89 від 06.02.2023)

Суть доставки: мережа оператора “підхоплює” виклик 112, надає йому пріоритет, додає службові дані (ідентифікатор/локацію), і передає в ІКС 112 так, щоб виклик міг бути прийнятий в основному або резервному КЦ, без “точки відмови” [20].

Ключові правила доставки:

а) Два центри одночасно: маршрути будуються так, щоб виклик міг бути доставлений і до основного, і до резервного КЦ 112.

б) Резерв не “мертвий”: основний і резервний КЦ працюють у розподілі навантаження (active/active або наближено до цього), а при аваріях — забезпечують перехоплення викликів.

в) Можливий транзит через інші мережі: якщо прямого стику немає, допускається доставка через мережі інших операторів (головне — зберегти пріоритет і технічні атрибути).

г) Пріоритет 112: у мережі виклик 112 обробляється як екстрений (мінімізація затримок/відмов у маршрутизації).

д) Працює навіть без повної ідентифікації абонента: для мобільного виклику передбачають доставку навіть коли абонент не може надати

“класичні” дані (наприклад, без SIM/без номера), але з передаванням доступних технічних параметрів.

е) Транспорт/сигналізація: передача до ІКС 112 виконується через SIP/SIP-I (IP-модель) або СКС-7 (SS7, “класична” телефонна сигналізація).

ж) Локація: для мобільного виклику оператор передає місцезнаходження терміналу на момент виклику, а за технічної можливості — AML (точніші координати) [20].

Важливо: у цій логіці КЦ 112 отримує не “голий дзвінок”, а дзвінок + технічний пакет даних, який скорочує час на питання “де ви?” і зменшує ризик помилок при передачі службам реагування.

Технічні маршрути виклику 112 показано на рисунках 2.1-2.4.

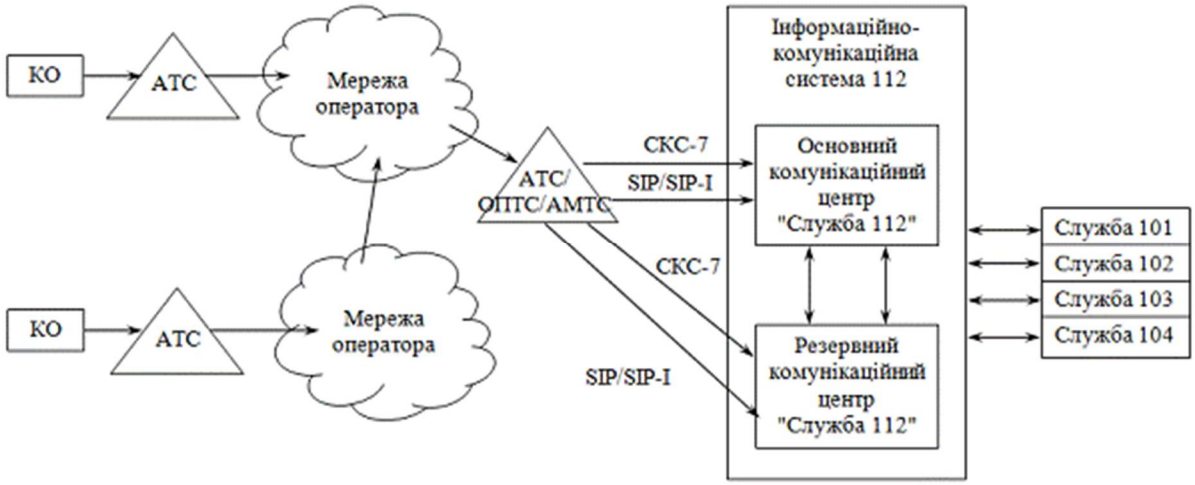

Рисунок 2.1 - Фіксований голосовий зв’язок (без ВСС) [20]

Хід подій за схемою, що відображено на рисунку 2.1.

а) КО набирає 112.

б) Виклик заходить на АТС (абонентську/місцеву), за потреби проходить через ОПТС/АМТС (транзит/міжмісто).

в) Далі оператор передає виклик у ІКС 112 через SIP/SIP-I або СКС-7.

г) ІКС 112 розподіляє виклик між основним і резервним КЦ (з урахуванням балансу/доступності).

д) Після прийняття оператором КЦ дані події передаються у 101–104.

Сенс рисунку 2.1: мінімальний ланцюг без “проміжного спеціального вузла”: класична телефонна маршрутизація → стикування з 112 → прийом у КЦ [20].

Схема передачі виклику 112 у фіксованій мережі з ВСС показано на рисунку 2.2.

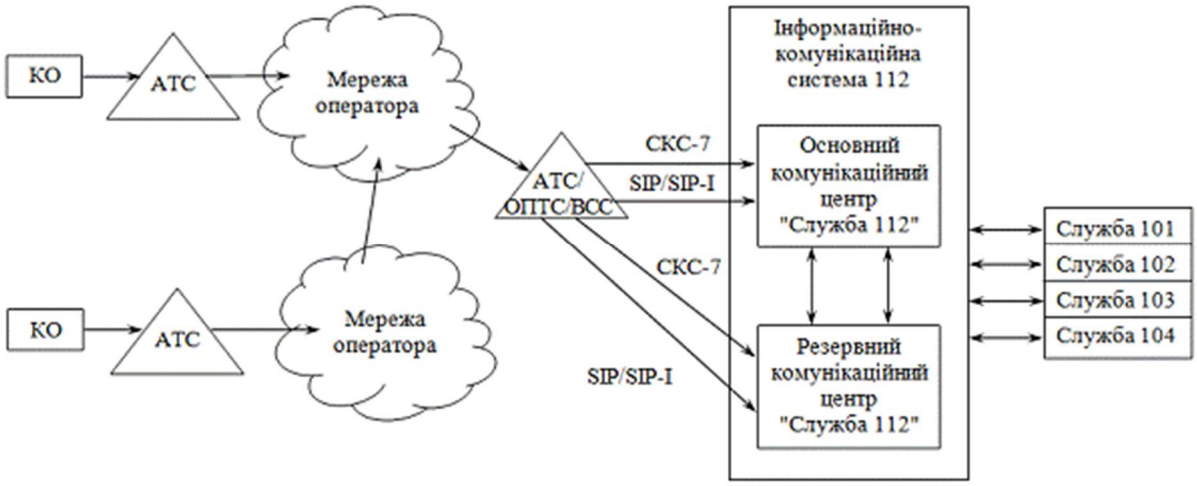

Рисунок 2.2- Схема передачі виклику 112 у фіксованій мережі з ВСС (Додаток 2 до Наказу №89) [20]

Що додає ВСС (вузол спеціальних служб) у “хід подій”?

а) КО → АТС/ОПТС/АМТС — так само, як у Рисунку 2.1.

б) Далі виклик потрапляє на ВСС — спеціальний елемент маршрутизації/концентрації екстрених викликів.

в) І вже з ВСС виклик передається до ІКС 112 (через SIP/SIP-I або СКС-7) з потрібними атрибутами.

г) Далі- стандартно: ІКС 112 → Основний/Резервний КЦ → 101–104 [20].

Навіщо це потрібно?

ВСС “вирівнює” екстрені потоки: зручніше централізовано керувати маршрутизацією 112, спрощувати стики, масштабувати підключення, і швидше перебудовувати маршрути при аваріях [20].

Схема передачі виклику 112 у мобільній мережі показано на рисунку 2.3.

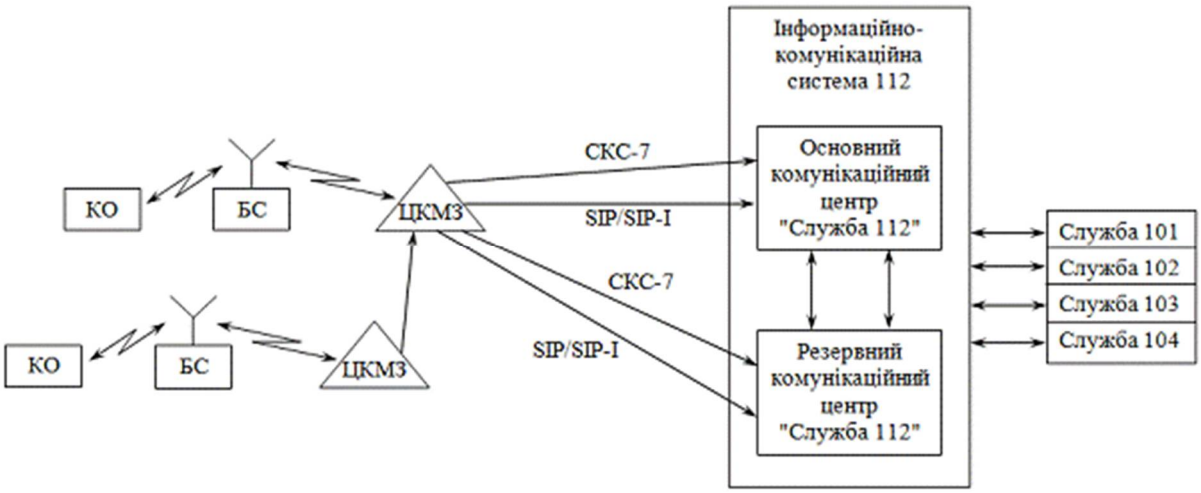

Рисунок 2.3 - Схема передачі виклику 112 у мобільній мережі (Додаток 3 до Наказу №89) [20]

Хід подій за схемою, що відображена на рисунку 2.3.

а) КО (телефон) ініціює виклик 112.

б) Виклик приймає БС (базова станція) — це “вхід” у стільникову мережу.

в) Далі виклик і сигналізація переходять у ЦКМЗ (умовно: мобільний комутаційний центр/ядро мережі).

г) Оператор передає виклик у ІКС 112 через SIP/SIP-I або СКС-7.

д) Паралельно з доставкою голосу/сесії передаються доступні технічні дані: ідентифікатори (коли є) та локація (cell-ID/сектор; за можливості — AML).

е) Далі — ІКС 112 → Основний/Резервний КЦ → 101–104 [20].

Ключова відмінність від фіксованої мережі: першим “свідком” виклику є радіодоступ (БС), тому мережа може одразу додати геоприв’язку, і КЦ отримує стартову локацію ще до уточнень від заявника [20].

Схема передачі виклику 112 у мобільній мережі з ВСС показано на рисунку 2.4.

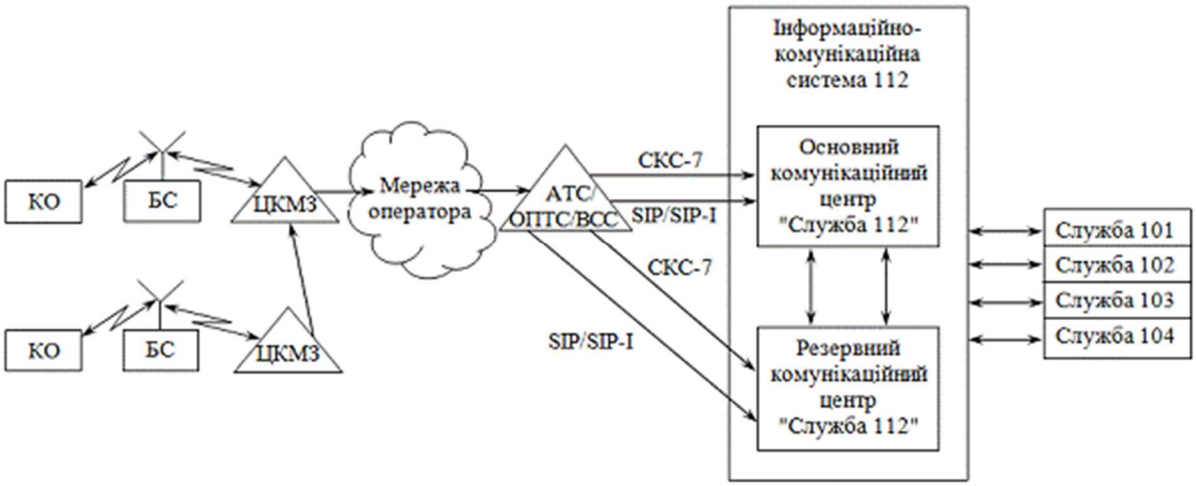

Рисунок 2.4 - Схема передачі виклику 112 у мобільній мережі з ВСС (Додаток 4 до Наказу №89) [20]

Що змінюється в “ході подій”?

а) КО → БС → ЦКМЗ — як у Додатку 3.

б) Далі виклик проходить через ВСС (як “шлюз/концентратор” екстрених).

в) З ВСС виклик віддається до ІКС 112 (SIP/SIP-I або СКС-7).

г) Далі — стандартно: ІКС 112 → Основний/Резервний КЦ → 101–104.

Сенс рисунку 2.4: поєднує переваги мобільної локації (через БС/ядро) та переваги централізації/керованості маршрутів (через ВСС) [20].

Чому на схемах завжди два КЦ і дві стрілки до ІКС 112 ?

Подвійне підключення (основний + резервний КЦ) на схемах — це не “красивий дубль”, а логіка живучості:

а) у нормі ІКС 112 розподіляє потоки (оператори в обох центрах приймають звернення);

б) при деградації одного центру виклики автоматично переносяться на доступний;

в) для КЦ це означає: стабільність прийому 112 навіть при аваріях каналів, вузлів чи майданчика.

Практичний ефект для процесів КЦ 112 (чому “доставка” — це вже частина якості реагування).

Доставка за Наказом №89 робить так, що оператор КЦ часто стартує не “з нуля”, а вже має [20]:

а) канал зв’язку, встановлений з пріоритетом;

б) ідентифікатор (коли доступний);

в) первинну локацію (cell-ID/AML або інші дані, які мережа може надати);

г) можливість швидше заповнити картку події та передати в 101–104 без зайвих уточнень.

Мінус 20–40 секунд на “де ви?” у критичних ситуаціях — це не косметика, а різниця між “встигли/не встигли” [20].

Схеми Додатків 1–4 Наказу №89 відображають єдину логіку**:** виклик 112 іде з мережі оператора до ІКС 112 по стандартизованих протоколах (SIP/SIP-I або СКС-7), з пріоритетом, із супровідними даними та з обов’язковою живучістю через основний і резервний КЦ**.** Відмінності між Додатками — лише у вузлах доступу (фікс/мобайл) та наявності ВСС, але “хід подій” незмінний: забезпечити швидке і гарантоване потрапляння виклику до оператора 112 [20]**.**

Чому це важливо для процесів КЦ 112: технічна доставка і передача локації/ідентифікаторів — це те, що дозволяє оператору почати роботу вже з частково заповненими даними, скоротити час на уточнення “де?”, зменшити помилки і швидше передати звернення службам [20].

У профільних рекомендаціях для операторів 112 підкреслюється важливість стандартизованих процедур опитування та “decision index”, що прямо впливає на стабільність якості та швидкість реагування [10].

3 КОМПЛЕКСНЕ ДОСЛІДЖЕННЯ СТАНУ ЗАХИЩЕНОСТІ КОМУНІКАЦІЙНОГО ЦЕНТРУ СЛУЖБИ 112

3.1 Аналіз потенційних вразливостей та оцінка векторів атак на КЦ 112

Комунікаційний центр служби 112 є об’єктом критичної інформаційної інфраструктури та ключовим елементом державної системи екстреної допомоги населенню України [2]. Він забезпечує приймання, обробку й маршрутизацію екстрених викликів, документування подій, формування аналітичної звітності, обмін службовими повідомленнями в реальному часі, а також координацію між поліцією, швидкою медичною допомогою, пожежно-рятувальними підрозділами та центрами 112 інших регіонів [3,4].

До складу системи входять автоматизовані робочі місця операторів, серверні комплекси баз даних і прикладного програмного забезпечення, системи голосового зв’язку на базі VoIP, геоінформаційні системи, а також захищені канали взаємодії з відомчими системами МВС, ДСНС, МОЗ та іншими регіональними центрами 112 [4,5].

Система постійно обробляє персональні дані заявників, відомості про їхнє місцезнаходження, медичну інформацію, дані про надзвичайні події та службові відомості обмеженого доступу [13]. Через це до неї пред’являються найвищі вимоги за моделлю CIA-тріади (конфіденційність, цілісність, доступність) [6,9]. Будь-яке порушення може призвести до затримки реагування екстрених служб або навіть до втрати людських життів [6].

Діяльність і захист інформації в комунікаційному центрі 112 регулюються комплексом нормативно-правових актів України у сфері інформації, кібербезпеки, технічного й криптографічного захисту [6,7,8,9]. Основними серед них є:

Закон України «Про інформацію» [8];

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [9];

Закон України «Про основні засади забезпечення кібербезпеки України» [21];

Закон України «Про Національну програму інформатизації» [16];

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [14];

Указ Президента України від 29.12.1999 № 1229/99 «Положення про технічний захист інформації в Україні» [15];

Постанова Кабінету Міністрів України від 29.03.2017 № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [6];

Нормативні документи з технічного захисту інформації (НД ТЗІ 2.5-004-99, 2.5-005-99, 1.1-003-99) [7,22,23];

Національний стандарт ДСТУ 2226:2022 щодо криптографічного захисту інформації [24].

Система 112 підлягає обов’язковій атестації комплексної системи захисту інформації (КСЗІ) та включена до державного реєстру об’єктів критичної інфраструктури [6].

Як об'єкт критичної інфраструктури, Система 112 підпадає під Загальні вимоги з кіберзахисту, затверджені Постановою КМУ № 518 [6]. Ці вимоги передбачають обов'язкове впровадження заходів кіберзахисту на основі управління ризиками, розробку плану кіберзахисту, щорічний перегляд та оцінку стану захисту. Однак, попри нормативне регулювання, система вразлива до атак через її залежність від комунікаційних мереж, інтеграцій з іншими державними системами та людського фактору. Нижче наведено аналіз потенційних вразливостей та векторів атак за вказаними напрямками [6,9].

Ризики, пов'язані з доступом- вразливості доступу виникають через фізичний та цифровий доступ до центрів обробки викликів (КЦ 112). Фізичний доступ: центри, можуть бути вразливими до несанкціонованого проникнення, особливо в умовах воєнного стану. Вектор атаки – інсайдерські

загрози або фізичні вторгнення, що призводять до саботажу обладнання [6]. Цифровий доступ: система використовує інформаційно-комунікаційну підсистему МВС, де дані зберігаються 5 років [4]. Вразливості включають слабкі механізми авторизації, наприклад, відсутність двофакторної аутентифікації для операторів [14]. Оцінка: високий ризик, оскільки атака може заблокувати обробку викликів, як у кібератаках на українську інфраструктуру 2015 р. (відключення електроенергії) [25]. Захист: вимагає впровадження контролю доступу відповідно до НД ТЗІ 1.1-003-99 та Закону "Про захист інформації в ІКС" [7,9].

Потенційні вразливості:

Недостатній контроль фізичного доступу до серверних/комутаційних шаф, робочих місць операторів (USB-порти, периферія, “чужий ноутбук у мережі”) [9].

Слабка сегментація зон (операторська зала, адмін-зона, серверна) або відсутність принципу “мінімально необхідного доступу”.

Відсутність/формальність процедур для відвідувачів і підрядників (супровід, журнали, тимчасові перепустки).

Типові вектори атак (в оборонному описі) :

Проникнення в приміщення під легендою “ремонт/перевірка”, підключення пристрою до мережі.

Компрометація робочої станції через фізичний носій або “тимчасове” підключення до АРМ.

Ризик/вплив.

Високий за наслідками: можливе втручання в роботу АРМ, витік персональних даних, зупинка сервісів [6,13].

Рекомендовані контрзаходи.

Зонування (операторська/адмін/серверна), контроль доступу, відеоспостереження, журнали [9].

Блокування/контроль USB, політики пристроїв, MDM/EDR для АРМ [6].

“Гостьова” мережа окремо, заборона підключення неавторизованих пристроїв [6].

Ризики, пов'язані з мережею.

Мережеві вразливості є критичними, оскільки Система 112 залежить від комунікаційних мереж для прийому викликів та передачі даних (включаючи геолокацію). Вектор атаки: DDoS-атаки, як у агресії проти України (понад 2200 атак на критичну інфраструктуру у 2021 р.) [26], можуть перевантажити сервери, заблокувавши доступ до номеру 112. Інші вектори – мережеві вторгнення через вразливості в електронних комунікаціях (SMS, відео), або MITM-атаки на передачу даних [12]. У воєнному контексті агресор застосовував кіберкампанії проти України, включаючи атаки на урядові мережі [27,28]. Оцінка: дуже високий ризик, оскільки атака може паралізувати реагування на надзвичайні ситуації. Захист: передбачено Постановою № 518 – моніторинг ризиків, резервування мереж [6]. Рекомендації: впровадження шифрування трафіку та сегментації мереж відповідно до Закону "Про інформацію" [8].

Мережа (VoIP/SIP, LAN, WAN, резервування).

Потенційні вразливості.

DDoS/DoS по периметру (канали зв’язку, SIP-інфраструктура, DNS, VPN) [6].

Перевантаження/флуд SIP (масові запити, дзвінки-роботи), що “забивають” черги [12].

Помилки маршрутизації між операторами/вузлами, недостатній моніторинг деградації (виклики ніби “йдуть”, але не доходять до черги оператора) [12].

Слабка мережна сегментація: АРМ операторів, сервери, запис, БД, інтеграційний шлюз в одному сегменті [9].

Небезпечні протоколи адміністрування або доступ адміністратора з “будь-якої” мережі.

Типові вектори атак.

Атаки на доступність: перевантаження каналів/серверів, виведення з ладу прикордонного обладнання [6].

Латеральний рух з компрометованого АРМ у серверний сегмент (якщо мережа плоска) [9].

Ризик/вплив для 112.

Доступність — критична, тож навіть “без витоку” ризик дуже високий [6].

Рекомендовані контрзаходи.

Захист периметру: DDoS-механізми, rate-limit, SBC з політиками, фільтрація, резервні канали [6].

Жорстка сегментація (VLAN/ACL/Firewall між зонами), “zero trust” для адмін-доступів [9].

Постійний моніторинг QoS/затримок/втрат пакетів/черг викликів + автоматичні алерти [12].

Ризики, пов'язані з обліковими записами.

Облікові записи операторів та адміністраторів є слабким місцем через можливі слабкі паролі або фішинг [14]. Система обробляє персональні дані (номери абонентів, локації) [13], що робить її привабливою для атак. Вектор атаки: соціальна інженерія для отримання доступу, як у загальних кібератаках на Україну (понад 2,200 інцидентів у 2021 р.) [26]. Інсайдерські загрози: оператори можуть випадково або навмисно розголошувати дані. Оцінка: середній-високий ризик, посилений людським фактором [6]. Захист: обов'язкова конфіденційність даних за Законом № 2581-IX та навчання персоналу [3]. Рекомендації: впровадження КЕП (кваліфікованого електронного підпису) та регулярні аудити [14].

Потенційні вразливості.

Спільні логіни (“оператор1/оператор2”) або передача паролів між змінами [6].

Відсутність багатофакторної автентифікації (MFA) для адміністраторів, спільне використання облікових записів [14].

Надмірні права: оператор може редагувати критичні поля, видаляти записи, змінювати маршрутизацію/довідники.

Слабкі процеси життєвого циклу доступу: несвоєчасне блокування при звільненні/ротації [6].

Незахищені облікові записи сервісів/інтеграцій (паролі в конфігах, ключі без ротації) [9].

Типові вектори атак.

Фішинг/соціальна інженерія → компрометація обліковки → доступ до карток інцидентів/довідників/інтеграцій.

Зловживання інсайдером: “тиха” правка даних, зміна пріоритетів, приховування інцидентів.

Ризик/вплив: високий через ризик порушення цілісності (найнебезпечніше для реагування).

Рекомендовані контрзаходи.

Персональні облікові записи, MFA, рольова модель (RBAC), принцип найменших привілеїв [6,14].

PAM для адмінів, сесійний контроль, заборона “прямих” адмін-доступів з операторських АРМ [9].

Журнали аудиту “хто і що змінив” + незмінність логів (централізація/SIEM) [9].

Інтеграції з іншими системами (ДСНС, МВС, МОЗ, геопорталом) створюють вразливості через передачу даних. Вектор атаки: експлуатація API або інтерфейсів для витоку даних, як у malware-атаках на Україну (DDoS, дефейс сайтів) [29]. У пілотних проєктах та контактними центрами збільшує поверхню атаки [11]. Оцінка: високий ризик, особливо в умовах кібервійни. Захист: електронна взаємодія регулюється Наказом МВС № 78/225, з використанням захищених каналів [5]. Рекомендації: сегментація інтеграцій та моніторинг відповідно до Постанови № 518 [6].

Потенційні вразливості.

Незахищені API/шини обміну: слабка автентифікація, відсутність взаємної перевірки (mTLS), “широкі” мережні правила між системами [5].

Ризики на стику форматів: помилки валідації вхідних даних (ін’єкції/підміни полів), некоректна обробка вкладень/повідомлень [9].

Каскадний ефект: збій/компрометація одного партнера “тягне” КЦ (черги, таймаути, блокування потоків) [6].

Облікові записи сервісів інтеграції без ротації ключів та без обмеження IP/прав [14].

Типові вектори атак.

Компрометація суміжної системи → використання довірчих каналів → вплив на КЦ (латеральний рух через інтеграцію) [6].

Підміна або спотворення даних інциденту на етапі передачі (цілісність), якщо канал/підпис не контрольований належним чином [9].

Ризик/вплив.

Високий: інтеграції — це “коридори довіри”, і саме там часто виникає системний ризик [6].

Рекомендовані контрзаходи.

Контракт безпеки на інтеграції: mTLS, підпис/контроль цілісності, allowlist IP, окремі ключі на кожного партнера, ротація [14].

“Шлюз інтеграцій” у DMZ/окремій зоні, жорстка ізоляція від БД та внутрішніх сервісів [9].

Таймаути/черги/ізоляція збоїв: щоб падіння зовнішнього сервісу не “клацнуло” КЦ [5].

Людський фактор є домінуючим у кібербезпеці (до 90% інцидентів) [6]. Вектор атаки: соціальна інженерія, недостатнє навчання операторів (включаючи психологів та багатомовних спеціалістів) [11]. У воєнний час – психологічний тиск або інфільтрація. Оцінка: високий ризик, оскільки помилки можуть призвести до затримок у реагуванні. Захист: регулярне навчання за Постановою № 518. Рекомендації: симуляції атак та підвищення обізнаності [6].

Загальна оцінка: Система 112 вразлива через геополітичний контекст, з потенціалом атак для дестабілізації суспільства. Необхідно посилити кіберзахист, інвестуючи в технології та навчання [6].

Потенційні вразливості.

Фішинг і соціальна інженерія (особливо під легендою терміновості: “оновлення”, “перевірка”, “інцидент”) [6].

Помилки оператора: неправильна класифікація/пріоритет, внесення некоректних даних, пропуск критичних полів [4].

Втома/стрес/плинність кадрів → зниження уважності, обхід процедур [4].

Неформальні практики: запис паролів, “передай доступ змінщику”, використання месенджерів для службових даних.

Типові вектори атак.

Атака не на техніку, а на людину: змусити натиснути, повідомити код, відкрити файл, “допомогти підряднику”.

Інсайдерська дія: навмисне спотворення записів або витік даних.

Ризик/вплив.

Середній–високий (часто найімовірніший шлях), а для 112 наслідки можуть бути критичні.

Рекомендовані контрзаходи

Регулярні короткі навчання + симуляції фішингу (без “каральної” культури) [6].

Чіткі чек-листи обробки інциденту, контроль обов’язкових полів, підказки в інтерфейсі [4].

Поділ обов’язків: оператор не може одноосібно змінювати довідники/маршрути/критичні правила [6].

Політики роботи з даними (заборона несанкціонованих каналів), контроль винесення інформації [13].

Поверхня атаки КЦ 112 формується на стику комунікаційних-мереж (SIP/VoIP), внутрішньої IT-інфраструктури, інтеграцій з екстреними

службами та роботи персоналу [12]. Умовно її можна показати так: Абонент/оператор зв’язку → прикордонні SIP/VoIP вузли (шлюзи, SBC) → платформа прийому 112 (черги та логіка розподілу) → АРМ операторів/диспетчерів → внутрішні сервіси даних (БД інцидентів, GIS, записи, журнали) → інтеграції зі службами реагування (101/102/103/інші) → канали адміністрування й підтримки (VPN, API, адмін-доступи) [4,5].

Кожен “перехід” між блоками — це точка ризику: протокол, облікові записи, ключі, мережеві правила, людський фактор [6].

Найкритичніші вектори — ті, що впливають на доступність прийому викликів і цілісність картки інциденту [6]. Тому пріоритети захисту мають бути: стійкість до перевантажень, жорсткий контроль доступів, ізольовані інтеграції, аудит дій користувачів і системна робота з людським фактором [6]. Компрометація будь-якої ланки може призвести до порушення доступності прийому викликів, цілісності картки інциденту або конфіденційності персональних даних [13].

3.2 Оцінка ефективності наявних механізмів захисту та відповідності вимогам безпеки

Комунікаційний центр 112 (КЦ 112) — критичний сервіс, для якого доступність (availability) є пріоритетом №1, а цілісність і конфіденційність — обов’язкові умови коректного реагування та захисту персональних даних. Оцінка ефективності механізмів захисту виконується за логікою: що вже зменшує ризики, де залишаються “дірки”, які посилення дадуть найбільший ефект [6].

Організаційні заходи в системі 112 регулюються Законом України "Про систему екстреної допомоги населенню за єдиним телефонним номером 112" (№ 4499-VI від 13.03.2012, з змінами № 2581-IX від 07.09.2022) [2,3] та

Постановою КМУ № 518 від 19.06.2019 "Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури". Вони включають:

Розробку та щорічний перегляд планів кіберзахисту, управління ризиками кібербезпеки (оцінка, запобігання, моніторинг).

Навчання персоналу: регулярне, диференційоване за ролями (оператори, диспетчери), з акцентом на кібергігієну та реагування на інциденти [6].

Координацію між суб’єктами: МВС (керує Службою 112), місцеві органи, оператори зв’язку (надання даних про абонентів, локацію) [12].

Обмін інформацією: з державними органами, міжнародними партнерами (наприклад, інтеграція з європейською системою 112) [10].

Розподіл ролей і функцій (оператори/старші зміни/адміністратори/ІБ/керівник) знижує ризик “універсального доступу”, коли одна людина може зробити все [6].

Регламентовані сценарії обробки інциденту (прийняв → уточнив → зареєстрував → передав → супроводив) стабілізують процес, зменшують помилки і вплив людського фактору.

Формальна дисципліна змінності та чергувань: контроль присутності, передача зміни, фіксація нестандартних ситуацій — важлива база для розбору інцидентів і відповідальності [4].

Ефективність та відповідність: Ці заходи працюють добре, забезпечуючи оперативність (час реагування – до 1 хвилини на виклик) та відповідність базовим вимогам кіберзахисту (Адміністрація Держспецзв’язку). Система відповідає Закону "Про інформацію" (№ 2657-XII від 02.10.1992) щодо захисту персональних даних (згода на обробку, конфіденційність) [8]. Однак потребує посилення: відсутність обов’язкових щорічних аудитів ризиків (лише за потреби), недостатнє фінансування навчання (за даними КМУ, 2025–2026 рр. планується збільшення), вразливість до соціальної інженерії через брак симуляцій атак. Слабка

дисципліна доступів: доступи видаються швидко, а відкликаються повільно (звільнення/переведення/відпустка/підрядники).

Посилення, яке дає максимум ефекту: впровадити короткий, але жорсткий цикл: видача доступу за заявкою → обмеження роллю → регулярний перегляд доступів → негайне відкликання [6].

Технічні заходи базуються на інформаційно-комунікаційній системі 112 (апаратно-програмні комплекси, мережі електронного зв'язку) та вимогах до авторизованих систем захисту (Закон "Про захист інформації в інформаційно-комунікаційних системах" № 80/94-ВР від 05.07.1994).

Шифрування та резервування: Обов'язкове створення зашифрованих резервних копій державних ресурсів (під час воєнного стану – за кордоном), заборона розміщення в окупованих/агресорських територіях [9].

Захист від несанкціонованих дій: Сертифіковані засоби криптографічного захисту, технічні комплекси для обробки конфіденційної інформації [24].

Інтеграція: Доступ до геопросторових даних через національний геопортал, обмін з базами операторів зв'язку (номери, локації) [4].

Застосунок "112 Ukraine": Підтримка викликів через SMS, відео, месенджери з жестовою мовою для осіб з інвалідністю [11].

Ефективність та відповідність: Технічні заходи ефективні для базового захисту (відповідність ДСТУ та нормам Держспецзв'язку), забезпечуючи безперервність (цілодобовий режим) та цілісність даних [24]. Система відповідає вимогам до критичної інфраструктури (ризикоорієнтований підхід, реагування на інциденти за національним планом) [6]. Позитив: розширення NG112 (next-generation) для безпечного середовища [10]. Недоліки: вразливість до кібератак (DDoS, витоки даних), потреба в модернізації (інтеграція з ДСНС для обміну в реальному часі, 2025 р.), відсутність обов'язкового використання AI для виявлення загроз [6,30].

Контроль доступу регулюється Наказами МВС № 473 від 09.06.2023 (Положення про інформаційну безпеку) [4] та № 78/225 від 09.02.2024 (Порядок електронної взаємодії) [5].

Рольовий доступ: Оператори Служби 112, диспетчери служб – авторизований доступ за правилами, перевірка на санкційні/терористичні списки [4].

Автентифікація: Кваліфіковані електронні підписи (КЕП), перевірка документів (паспорти, повноваження) [14].

Обмеження: Доступ до персональних даних – лише з згодою або за законом; заборона на несанкціоновані дії [13].

Ефективність та відповідність: Механізм ефективний для запобігання витокам (відповідність Закону "Про захист персональних даних") [13], з перевіркою ідентичності. Добре працює: інтеграція з базами для локації абонентів [4]. Потребує посилення: MFA для всіх критичних входів; PAM-логіка для адмінів (окремі адмін-акаунти, сесії через jump-host, мінімум прав, короткі “вікна” доступу) [14], ризики інсайдерських загроз (потрібні регулярні перевірки).

Журналювання включає фіксацію викликів, обробки та реагування (Закон № 4499-VI) [2].

Запис та зберігання: Аудіозаписи, дані про виклики (час, локація, абонент) – зберігання 5 років у системі 112.

Звітність: Формування статистики, передача до оперативно-диспетчерських служб [4].

Моніторинг: Хронологічний журнал операцій для контролю [9].

Ефективність та відповідність: Ефективне для аудиту (відповідність нормам про резервування) [6], допомагає в розслідуваннях. Добре: автоматизоване фіксування в реальному часі [4]. Недоліки: брак інтеграції з SIEM-системами для аналізу аномалій, потреба в шифруванні журналів для захисту від маніпуляцій [9]. Для 112 важливо не просто “є бекапи”, а чи реально відновиться робота:

резервні копії без регулярних тестів відновлення = “віра”, а не контроль; небезпечно, коли бекап-доступи в тому ж домені/мережі, що й основна інфраструктура (ризик шифрування бекапів ransomware-атакою).

Посилення: правило 3-2-1, ізоляція копій, регулярні DR-навчання, фіксація RPO/RTO для ключових компонентів (виклики, картки інцидентів, записи розмов, довідники). Централізоване логування, синхронізація часу (NTP), незмінність логів (WORM/обмеження прав), правила виявлення (use-cases), регулярний перегляд подій.

Щоб оцінка була “технічною”, а не описовою, доречно застосувати контрольні питання/індикатори:

Доступність: чи витримує система пікові навантаження, чи є захист від DDoS/перевантажень, чи перевірявся failover? [6].

Цілісність: хто може змінювати записи інцидентів? чи фіксуються зміни (хто/що/коли)? чи є контроль несанкціонованих правок? [9].

Конфіденційність: шифрування каналів/даних, обмеження доступу до персональних даних і записів, мінімізація даних на робочому місці оператора [13].

Керованість: чи є інвентаризація активів, регулярні оновлення, контроль конфігурацій, сканування вразливостей, процес реагування [6].

Підзвітність: чи можна по логах відновити повну картину події за 10–15 хвилин аналізу, а не “2 дні вручну” [9].

Окремий “механізм захисту”, який часто недооцінюють — це якість документації: політики доступу, журнали змін, інструкції реагування, акти тестування відновлення, протоколи навчань. Без цього технічні заходи складно перевірити й підтримувати [4]. Для оформлення звітів/розділів роботи та структурування матеріалів доцільно дотримуватись вимог оформлення технічної документації та правил опису джерел [31].

Наявні механізми захисту в системі 112 загалом ефективні та відповідають вимогам безпеки (базовий профіль кіберзахисту, закони про інформацію та її захист) [6,8,9]. Сильні сторони: оперативність, інтеграція з

ЄС-стандартами [10], безкоштовність [2], захист персональних даних [13]. Система добре захищена від базових загроз (цілодобовий моніторинг, резервування) [4], сприяючи зменшенню часу реагування на 20–30% (за даними МВС, 2025 р.) [11].

Однак потребує посилення:

Організаційно – обов'язкові аудити ризиків, розширення навчання.

Технічно – впровадження AI-виявлення загроз, модернізація для стійкості до кібератак.

Контроль доступу – 2FA та моніторинг інсайдерів [14].

Журналювання – інтеграція з аналітичними системами [9].

Рекомендації: Розробити секторальний профіль кіберзахисту для системи 112 (за Постановою № 518), збільшити фінансування (план КМУ на 2025–2026 рр.) [18], провести незалежні аудити.

Саме ці посилення дають найбільше зниження ризику при відносно помірних затратах і прямо впливають на стійкість КЦ 112 до інцидентів [6].

3.3 Рекомендації щодо підвищення рівня захисту КЦ 112: SSH-ключі, двофакторна автентифікація (2FA) та рольова модель керування доступом (RBAC)

У контексті забезпечення кібербезпеки критичної інфраструктури, такої як Кол-центр екстреної допомоги 112 (КЦ 112), впровадження сучасних механізмів аутентифікації та контролю доступу є вкрай важливим. Система 112, як ключовий елемент національної системи екстреної допомоги, обробляє конфіденційну інформацію, координуючи дії служб порятунку, медичної допомоги та правоохоронних органів [2]. Згідно з Постановою Кабінету Міністрів України № 518 від 19 червня 2019 р. «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури», об'єкти

на кшталт КЦ 112 повинні відповідати вимогам щодо захисту від несанкціонованого доступу, включаючи багатофакторну аутентифікацію та розмежування прав. Нижче наведено рекомендації щодо переходу на SSH-ключі, впровадження двофакторної автентифікації (2FA) та рольової моделі керування доступом (RBAC), з акцентом на мінімальні привілеї, розмежування прав та контроль адміністративного доступу. Ці заходи дозволять знизити ризики фішингу, несанкціонованого доступу та внутрішніх загроз, підвищивши загальний рівень захисту системи [6,32-37].

Перехід на SSH-ключі є першочерговим кроком для посилення безпеки віддаленого доступу до серверів КЦ 112 [6,35]. Мета: прибрати найбільш “ламкий” механізм (пароль) із віддаленого адміністрування та зробити доступ керованим (видимим, облікованим і оборотним) [9,34]. Традиційні паролі вразливі до атак brute-force, фішингу та витоку даних, тоді як SSH-ключі базуються на асиметричній криптографії, де приватний ключ зберігається лише у користувача, а публічний – на сервері [24,34]. Переваги SSH-ключів включають: вищий рівень криптографічного захисту (ключі довжиною 2048-4096 біт стійкіші за паролі), автоматизацію входу без введення паролів, що зменшує помилки користувачів, та можливість єдиного входу (single sign-on) для кількох серверів. Для впровадження рекомендується: 1) Генерація пари ключів за допомогою команди ssh-keygen на клієнтських пристроях операторів КЦ 112, з обов’язковим захистом приватного ключа фразою-паролем (passphrase) для додаткової безпеки. 2) Передача публічного ключа на сервер за допомогою ssh-copy-id та збереження його у файлі ~/.ssh/authorized_keys [24]. 3) Вимкнення парольної аутентифікації в конфігурації SSH-сервера (файл /etc/ssh/sshd_config, параметр PasswordAuthentication no) для запобігання атакам на паролі. 4) Регулярне оновлення та ротація ключів, а також моніторинг доступу через журнали (наприклад, /var/log/auth.log) [9,35]. У КЦ 112 це дозволить контролювати адміністративний доступ, обмеживши його лише авторизованими ключами, та застосовувати принцип мінімальних привілеїв,

де оператори отримують доступ лише до необхідних ресурсів [6]. Впровадження таких заходів знизить ризики зовнішніх атак, як це рекомендовано в практиках NIST для критичної інфраструктури [32,34,35]].

Двофакторна автентифікація (2FA) є ефективним засобом для запобігання несанкціонованому доступу, додаючи другий рівень верифікації після введення пароля. У системі КЦ 112, де оператори працюють з чутливими даними (геолокація викликів, медична інформація), 2FA захищає від компрометації облікових записів через фішинг або витік паролів. 2FA базується на трьох факторах: щось, що користувач знає (пароль), щось, що має (пристрій), та щось, що є (біометрія). Мета: навіть якщо пароль/сесія/ключ частково скомпрометовані — нападник не отримує доступ без другого фактора. Рекомендовані типи для КЦ 112: 1) Програмні токени, генеровані додатками на зразок Google Authenticator або Authy, які створюють одноразові коди (TOTP) кожні 30 секунд – це зручно для мобільних пристроїв операторів і не залежить від SMS. 2) Апаратні токени (наприклад, YubiKey), які підключаються через USB і генерують коди без мережі, ідеальні для висококритичних середовищ. 3) Біометрична верифікація (відбитки пальців або розпізнавання обличчя) для стаціонарних робочих місць. Переваги: навіть при витоку пароля доступ неможливий без другого фактора; адаптивна 2FA (наприклад, вимога лише для доступу ззовні мережі) зменшує навантаження на користувачів. Для впровадження: інтегрувати 2FA в систему аутентифікації КЦ 112 за допомогою протоколів на зразок RADIUS або SAML, з обов’язковим навчанням персоналу [14]. Контроль адміністративного доступу реалізується через вимогу 2FA для адмін-ролей, а принцип мінімальних привілеїв – через обмеження 2FA для чутливих операцій (наприклад, зміна конфігурації системи) [6]. Це відповідає вимогам Закону України «Про захист інформації в інформаційно-комунікаційних системах» та практикам NIST, знижуючи ризики на 90% за даними досліджень [32,33].

Рольова модель керування доступом (RBAC) забезпечує розмежування прав на основі ролей, що є критичним для КЦ 112, де різні користувачі (оператори, адміністратори, аналітики) мають різні рівні доступу. RBAC спрощує управління, призначаючи дозволи ролям, а не окремим користувачам, що зменшує помилки та полегшує аудит. Мета: кожен користувач/служба отримує рівно ті права, які потрібні для його задач, і не більше. Це різко зменшує шкоду від помилок і компрометації акаунтів [6]. NIST у каталозі контролів прямо закладає least privilege, включно з вимогами: розділяти привілейовані/непривілейовані ролі, переглядати призначені привілеї та логувати виконання привілейованих функцій [6,32,36,37]. Основні принципи: 1) Призначення ролей (role assignment) – користувач активує роль лише за потреби. 2) Авторизація ролей (role authorization) – ролі повинні бути авторизованими для користувача. 3) Авторизація дозволів (permission authorization) – дозволи активуються лише в авторизованих ролях. У КЦ 112 рекомендується ієрархічна RBAC: базова роль «Оператор» для прийому викликів, «Адміністратор» для конфігурації з успадкуванням базових прав, та «Аудитор» для перегляду логів без змін. Обмеження (constraints) забезпечують separation of duties (SoD), наприклад, один користувач не може поєднувати ролі створення та авторизації доступу. Для впровадження: 1) Визначити ролі на основі посадових інструкцій (згідно з Наказом МВС України № 473 від 09.06.2023) [4]. 2) Інтегрувати RBAC в систему за допомогою інструментів на зразок Active Directory або LDAP [14]. 3) Застосувати принцип мінімальних привілеїв, де ролі надають лише необхідні дозволи (наприклад, оператор не має доступу до баз даних). 4) Контроль адмін-доступу через сесії з обмеженим часом та логування [9]. Це дозволить розмежувати права, зменшити внутрішні загрози та забезпечити відповідність Загальним вимогам з кіберзахисту [6,36,37].

Впровадження цих рекомендацій – перехід на SSH-ключі, 2FA та RBAC – комплексно підвищить рівень захисту КЦ 112, мінімізуючи ризики несанкціонованого доступу та забезпечуючи відповідність нормативним

актам [9,14]. Очікуваний ефект: зменшення ризику компрометації через паролі/фішинг; локалізація наслідків інциденту завдяки мінімальним привілеям; підвищення керованості доступу (видно “хто/коли/що робив”). Контрольні метрики : 100% адмін-доступів → через VPN+2FA; 100% серверів/мережевих пристроїв → SSH без паролів (де можливо); 0 shared admin accounts (або формально дозволені — лише як break-glass із жорстким аудитом); % ключів із підтвердженим власником + датою ротації; кількість “мертвих” ключів/акаунтів, видалених за результатами аудиту. Рекомендується провести пілотне тестування на окремих вузлах системи, з подальшим навчанням персоналу та аудитом [6,32-37].

ВИСНОВКИ

У ході виконання магістерської роботи проаналізовано, що Комунікаційний центр служби 112 є критично важливою інформаційною системою, яка працює з чутливими даними та повинна забезпечувати безперервність роботи під навантаженням і в умовах кіберзагроз [2,6].

Описано структуру КЦ 112 і логіку обробки інциденту: від прийому виклику, формування картки події та маршрутизації до служб 101/102/103/104 до роботи АРМ операторів, баз даних і інтеграцій [4,5]. Визначено основні вектори ризику (“поверхню атаки”): комунікаційні-інтерфейси (SIP/VoIP), віддалений адмін-доступ, зовнішні інтеграції, а також людський фактор [12]. Це створює реальні сценарії загроз: компрометація облікових записів, несанкціонований доступ до даних, спотворення інформації та порушення доступності сервісу [6].

Оцінка наявних заходів показала, що організаційні регламенти є базою, але найбільшого посилення потребують контроль доступу, автентифікація, розмежування привілеїв та журналювання [6,14,24]. Запропоновано пріоритетні кроки підвищення захищеності: перехід на SSH-ключі для адміністрування, впровадження 2FA для критичних контурів та застосування RBAC із принципом мінімальних привілеїв [6,14,24].

Загалом мету роботи досягнуто: систематизовано процеси КЦ 112, визначено ключові ризики та сформовано практичні рекомендації [6,9], що знижують ймовірність компрометації, обмежують наслідки інцидентів і підвищують керованість та стійкість системи [6].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 112 (служба екстреної допомоги) . Вікіпедія : вільна енциклопедія. – Режим доступу: 112 (служба екстреної допомоги) — Вікіпедія
2. Закон України № 4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» . Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про систему екстреної допомо... | від 13.03.2012 № 4499-VI
3. Закон України № 2581-IX від 07.09.2022 «Про внесення змін до деяких законів України щодо вдосконалення системи екстреної допомоги… 112». Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про внесення змін до деяких ... | від 07.09.2022 № 2581-IX
4. Наказ МВС України № 473 від 09.06.2023 офіційне видання: Офіційний вісник України від 05.07.2023 — 2023 р., № 59, стор. 392, стаття 3353, код акта 118884/2023. Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про затвердження Положення про і... | від 09.06.2023 № 473
5. Наказ МВС України № 78/225 від 09.02.2024 офіційне видання: Офіційний вісник України від 13.03.2024 - 2024 р., № 24, стор. 158, стаття 1586, код акта 123482/2024. Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про затвердження Порядку елек... | від 09.02.2024 № 78/225
6. КАБІНЕТ МІНІСТРІВ УКРАЇНИ ПОСТАНОВА від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури» Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про затвердження Загальних вимог... | від 19.06.2019 № 518

7. Нормативний документ НД ТЗІ 1.1-003-99 від 28 квітня 1999 року. Про «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» Цей документ було затверджено Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України . Державна служба спеціального зв'язку та захисту інформації https://cip.gov.ua › api › attachment › download https://cip.gov.ua/services/cm/api/attachment/download?id=66088
8. Закон України від 02.10.92 N 2657-XII "Про інформацію" Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Закон України від 02.10.92 N 2657-XII "Про інформацію"
9. Закон України «Про захист інформації в інформаційно-комунікаційних системах» Документ 80/94-ВР, чинний, поточна редакція — Редакція від 20.04.2025, підстава - 4336-IX . Офіційний портал Верховної Ради України https://zakon.rada.gov.ua Режим доступу Про захист інформації в інф... | від 05.07.1994 № 80/94-ВР
10. Рекомендація Європейської Комісії 2003/558/ЕС (25.07.2003) щодо обробки даних про місцеположення абонента в електронних мережах для надання «location-enhanced» екстрених послуг. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003H0558
11. МВС України. Офіційний веб-сайт. Новини про роботу Служби 112. – Режим доступу: https://mvs.gov.ua/uk/news
12. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX. Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#Text
13. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
14. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 № 2155-VIII. Офіційний портал Верховної

Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text

15. Указ Президента України від 27.09.1999 № 1229/99 «Положення про технічний захист інформації в Україні». Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text
16. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text
17. Постанова КМУ № 1031 від 11.11.2015 «Про затвердження Порядку функціонування системи екстреної допомоги населенню за єдиним телефонним номером 112» (зі змінами). Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1031-2015-п#Text
18. Європейський інвестиційний банк (ЄІБ). Пакет підтримки для впровадження системи 112 в Україні (52 млн євро). – Режим доступу: https://www.eib.org/en/projects/all/20220122
19. Закон України № 7581 від 2022 р. (щодо посилення технічної бази системи 112). Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/7581-2022#Text
20. Наказ Адміністрації Держспецзв'язку №89 від 06.02.2023 «Про затвердження Порядку передачі викликів під час здійснення екстрених комунікацій за єдиним телефонним номером 112». Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0493-23#Text
21. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

22. НД ТЗІ 2.5-004-99. Нормативний документ з технічного захисту інформації. – Режим доступу: https://cip.gov.ua/services/cm/api/attachment/download?id=66089
23. НД ТЗІ 2.5-005-99. Нормативний документ з технічного захисту інформації. – Режим доступу: https://cip.gov.ua/services/cm/api/attachment/download?id=66090
24. ДСТУ 2226:2022. Національний стандарт щодо криптографічного захисту інформації. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2226:2022#Text
25. CERT-UA. Звіт про кібератаки на українську інфраструктуру (2015 р.). – Режим доступу: https://cert.gov.ua/article/12345
26. CERT-UA. Звіт про кібератаки в Україні (2021 р.). – Режим доступу: https://cert.gov.ua/article/56789
27. СБУ. Звіт про кіберкампанії проти України. – Режим доступу: https://ssu.gov.ua/novyny/kiberzahrozy
28. МВС України. Звіт про кібератаки на урядові мережі. – Режим доступу: https://mvs.gov.ua/uk/news/kiberzahyst
29. CERT-UA. Звіт про malware-атаки в Україні. – Режим доступу: https://cert.gov.ua/article/67890
30. NIST. SP 800-53. Security and Privacy Controls for Information Systems and Organizations. – Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
31. ДСТУ 3008:2015. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ: ДП «УкрНДНЦ», 2016. – 26 с.
32. Козловський В. О., Ковтун В. В. Ааналіз ефективності двофакторної автентифікаці ї та людського фактора у кібербезпеці // Кібербезпека: освіта, наука, техніка. – 2021. – № 1 (13). – С. 5–14. – Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/853?articlesBySameAuthorPage=2

33. D. S. K. ., S. S. ., & S. K. . (2024). Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems. European Journal of Electrical Engineering and Computer Science, 8(2), 1–6. https://doi.org/10.24018/ejece.2024.8.2.19593 – Режим доступу: https://eu-opensci.org/index.php/ejece/article/view/19593
34. Zavacka O. Practical Assessment of the SSH Services' Transition to Post-Quantum Cryptography // Baltic Journal of Modern Computing. – 2025. – Vol. 13, No. 4. – P. 1–15. – Режим доступу: https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/13_4_06_Zavacke.pdf
35. Практична оцінка переходу служб SSH до пост-квантової криптографії. – Режим доступу: https://jpasmd.donnu.edu.ua/article/view/14809/14708
36. Іванченко Є. В. Застосування моделі RBAC для керування доступом в інформаційних системах // Дослідження та оптимізація інформаційно-телекомунікаційних систем. – 2023. – № 1. – С. 20–30. – Режим доступу: https://duikt.edu.ua/uploads/p_2779_46212583.pdf
37. Smith J. Application of RBAC in Modern Security Systems // ResearchGate. – 2024. – Режим доступу: https://www.researchgate.net/publication/396563419

ДОДАТОК А

ПРЕЗЕНТАЦІЯ

Рисунок А.1 - Титульний слайд

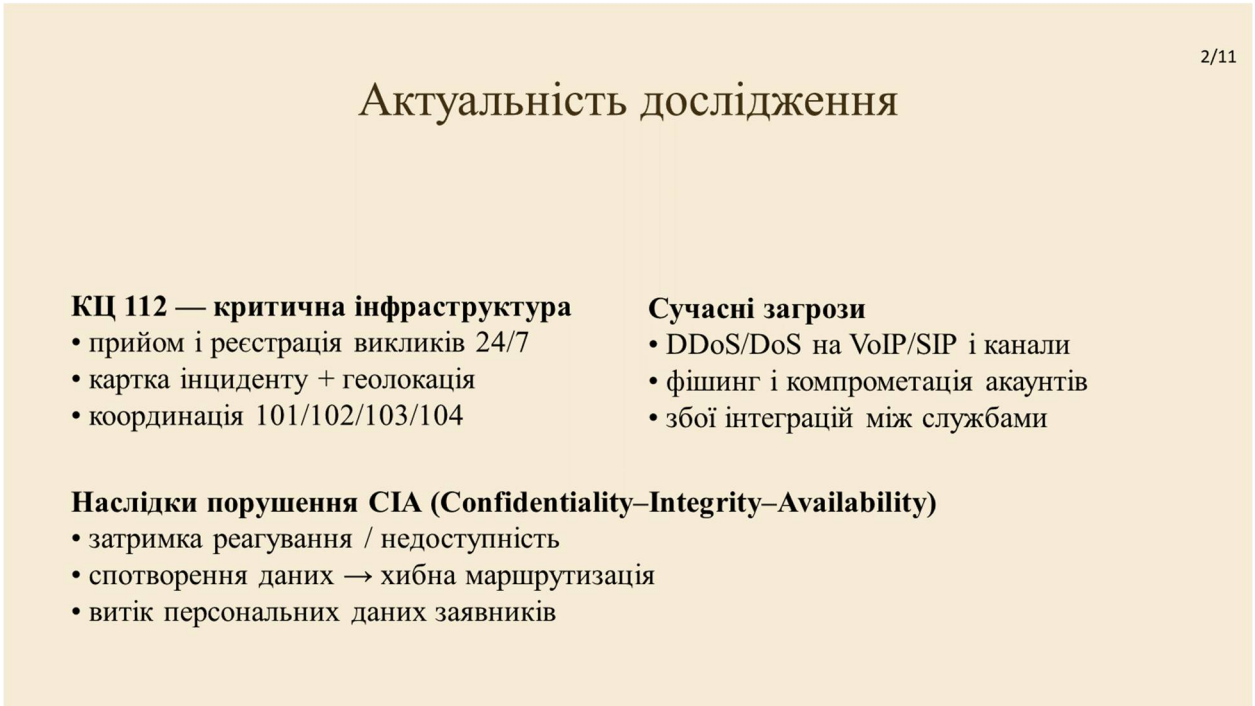

Рисунок А.2 – Актуальність дослідження

Рисунок А.3 – Мета та завдання роботи

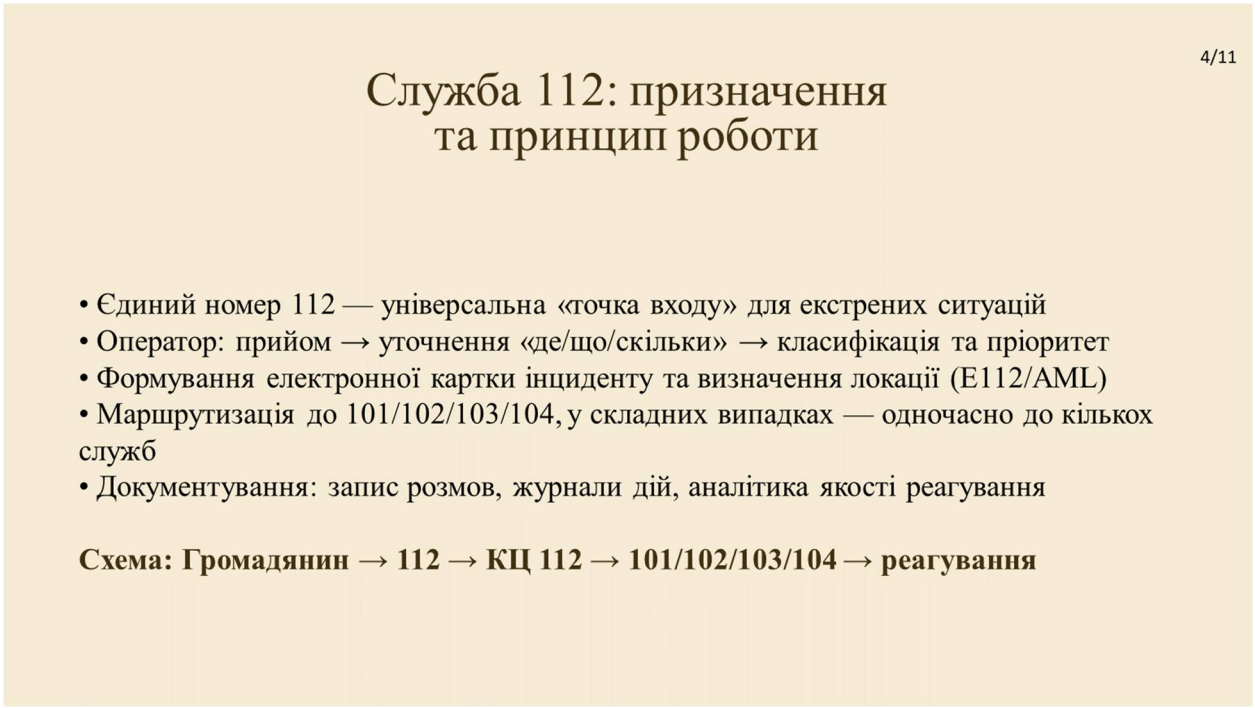

Рисунок А.4 – Служба 112 : призначення та принцип роботи

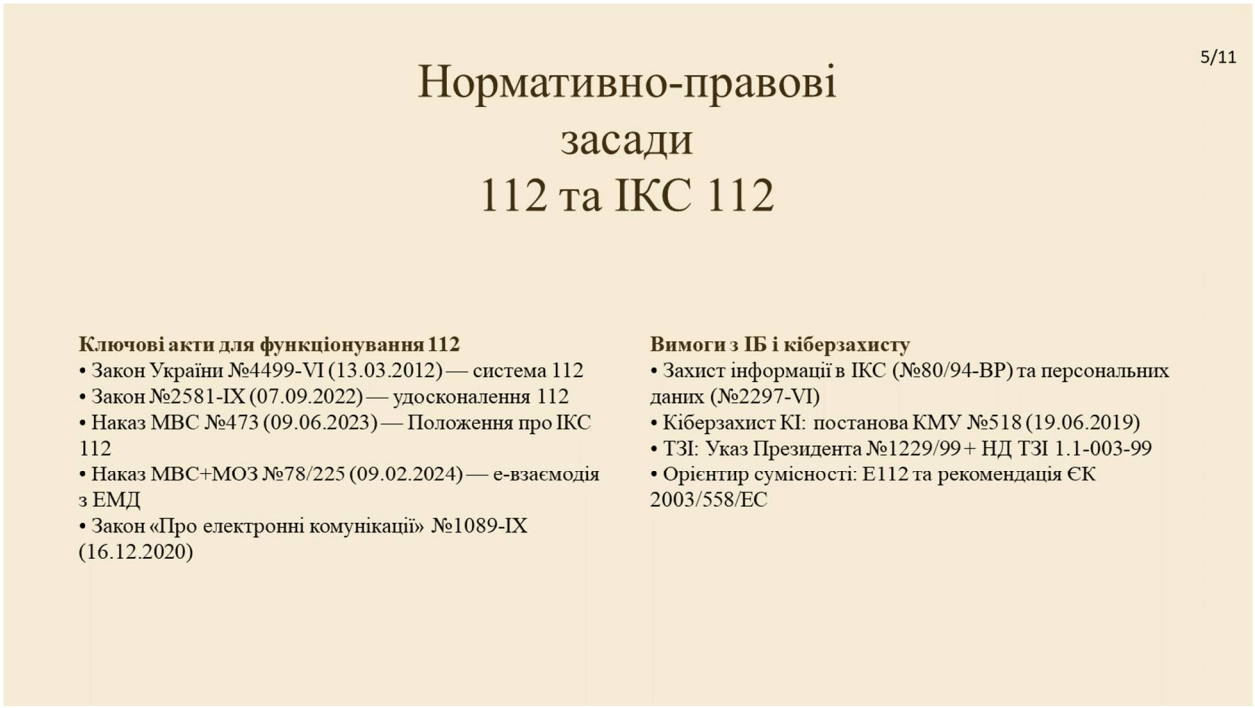

Рисунок А.5 – Нормативно-правові засади 112 та ІКС 112

Рисунок А.6 – КЦ 112: організаційна та технічна структура

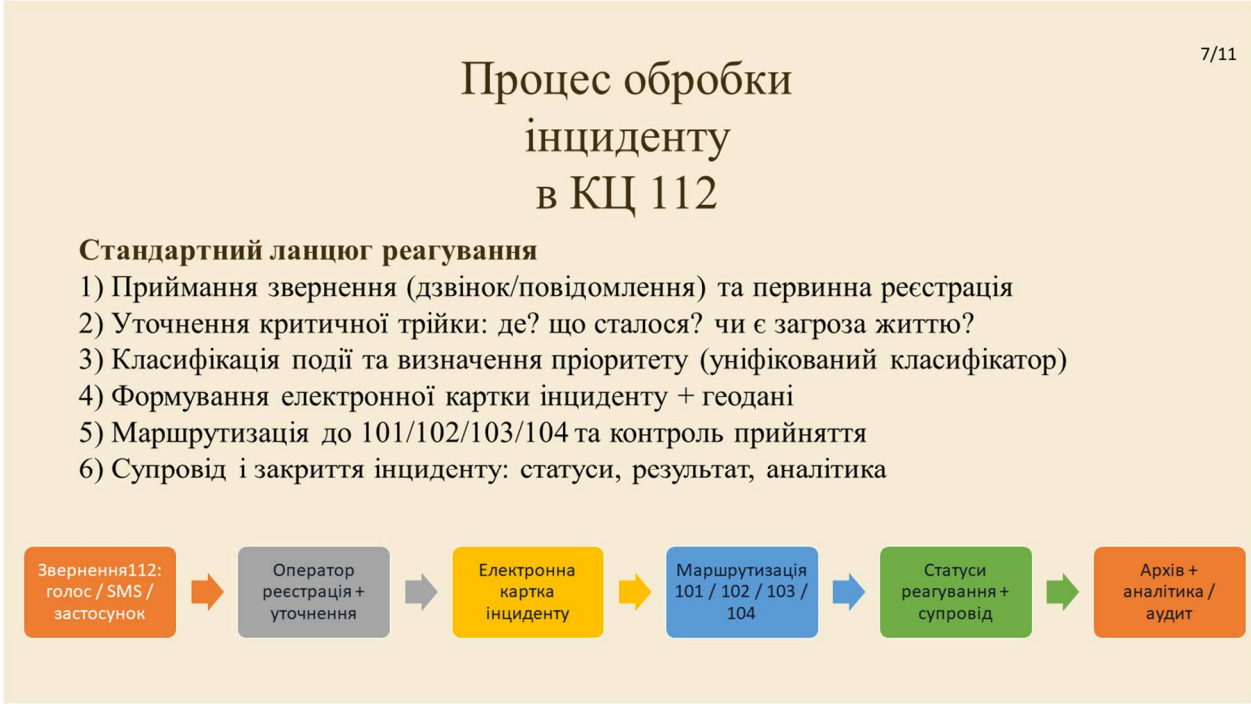

Рисунок А.7 – Процес обробки інциденту в КЦ 112

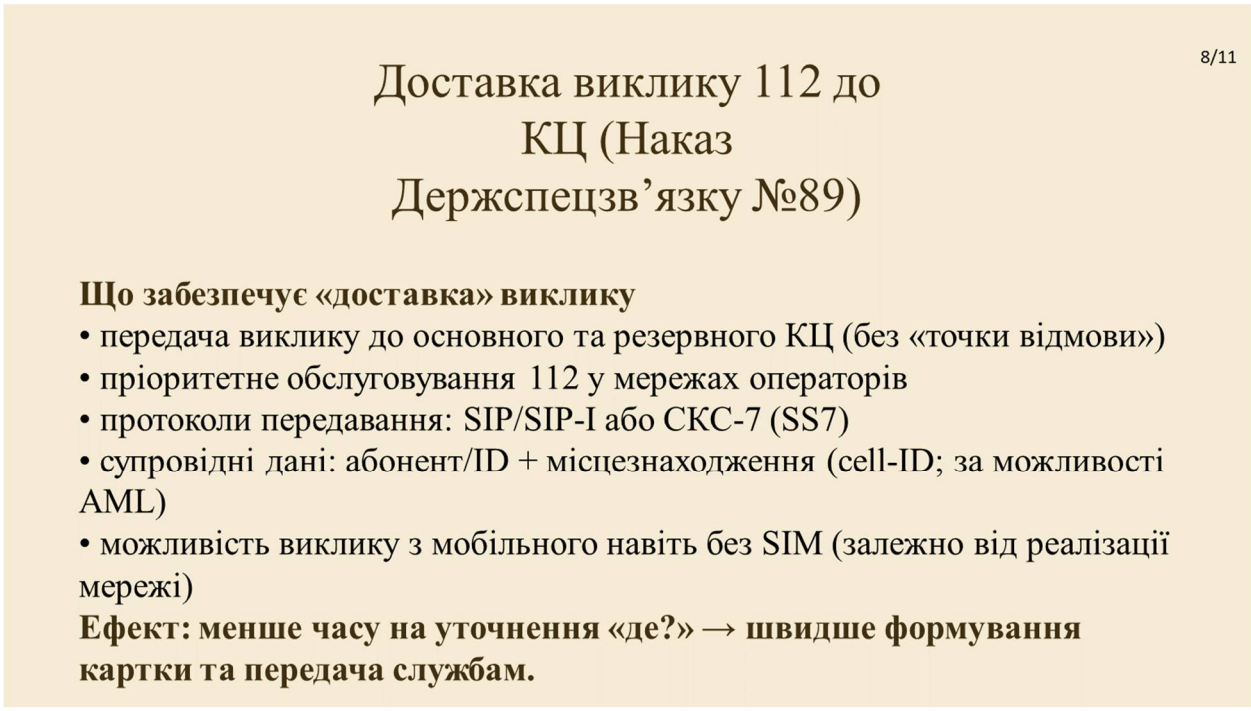

Рисунок А.8 – Доставка виклику 112 до КЦ (Наказ Держспецзв'язку №89)

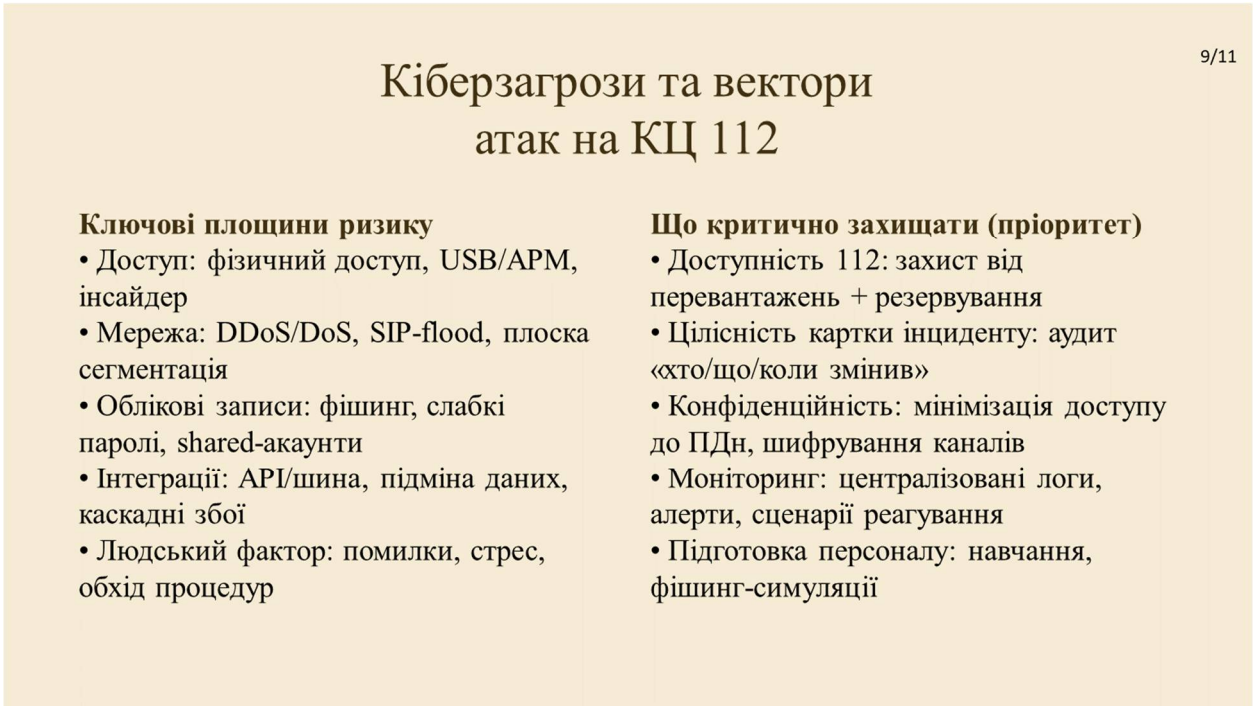

Рисунок А.9 – Кіберзагрози та вектори атак на КЦ 112

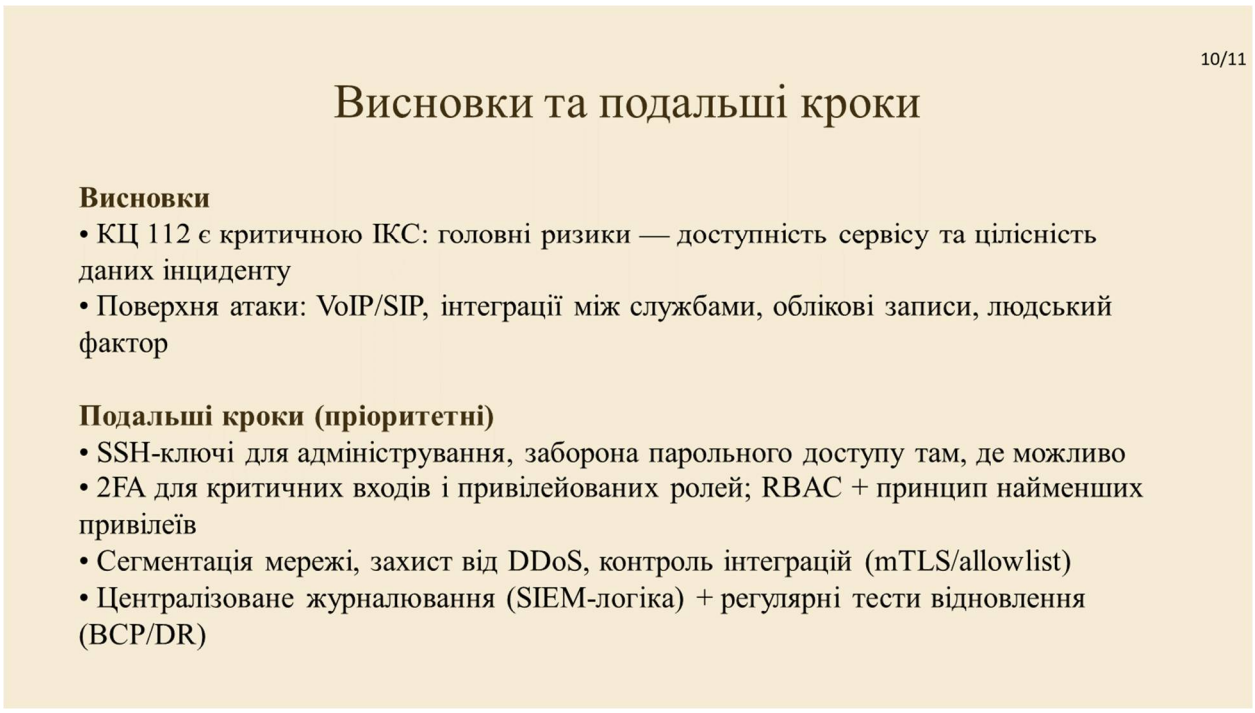

Рисунок А.10 – Висновки та подальші кроки

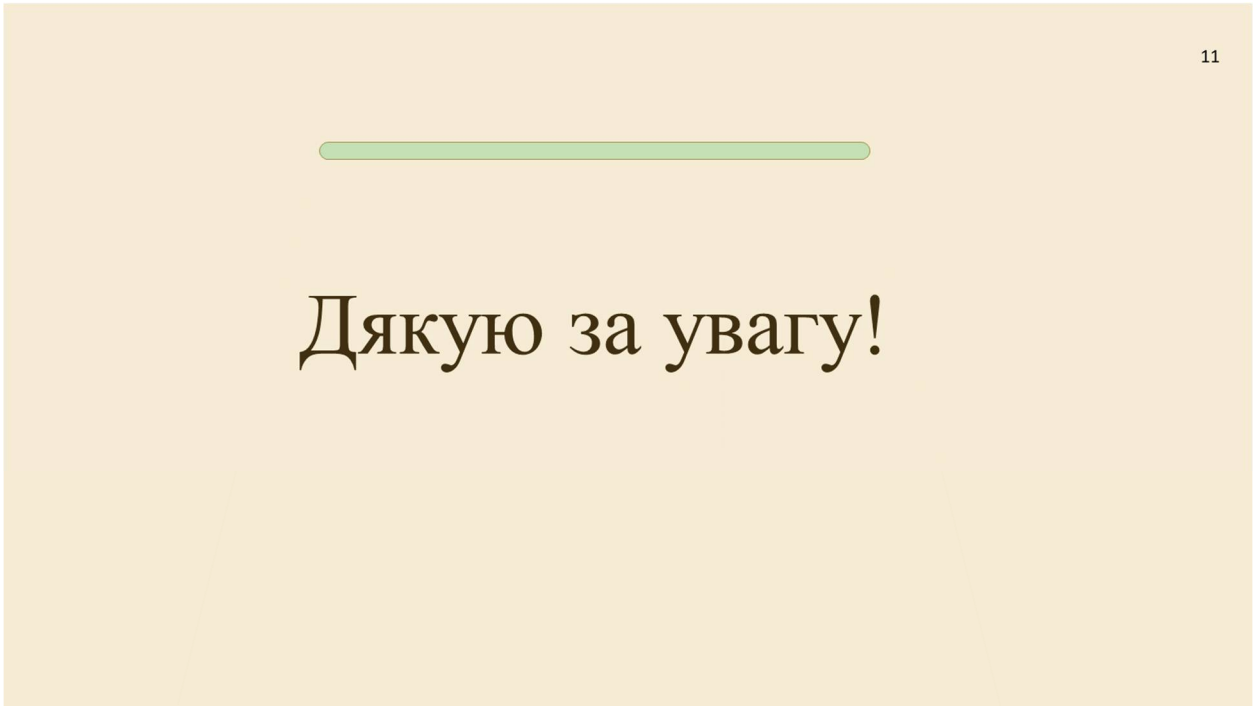

Рисунок А.11 - Фінальний слайд