Карпатський національний університет імені Василя Стефаника
Факультет історії, політології, і міжнародних відносин
Кафедра політичних інститутів та процесів

ДИПЛОМНА РОБОТА

на здобуття першого (бакалаврського) рівня вищої освіти

на тему:

«Гібридні загрози в релігійній сфері:форми, інструменти,механізми протидії.»

Виконав: студент 4 курсу, групи Пнб-42,
спеціальності 052 Політолгія,
освітньої програми “ Політологія.
Національна безпека.”
Жикаляк Іван Миколайович

Керівник: Міщук Мар'яна Богданівна
Рецензент: кандидат політичних наук,
доцент Ломака І.І.

м. Івано-Франківськ – 2026 р.

Зміст

Вступ

Актуальність теми. У сучасних умовах гібридні загрози стали одним із найнебезпечніших інструментів впливу на державу та суспільство. Їхня специфіка полягає в поєднанні різних засобів тиску інформаційних, політичних, організаційних, мережевих і цифрових, які використовуються для дестабілізації суспільних відносин, послаблення державних інституцій та формування вигідних для зовнішнього або внутрішнього деструктивного впливу настроїв.

Особливе місце в цьому контексті посідає релігійна сфера, оскільки вона безпосередньо пов'язана з цінностями, світоглядом, моральними орієнтирами та суспільною довірою. Релігійні організації мають значний вплив на громадську думку, а тому можуть ставати не лише об'єктом гібридного впливу, а й середовищем поширення дезінформації, пропагандистських наративів, конфліктогенних ідей і суспільного напруження. У зв'язку з цим вивчення гібридних загроз у релігійній сфері набуває особливого значення як для політичної науки, так і для практики забезпечення суспільної стабільності в Україні.

Мета дослідження. Метою бакалаврської роботи є дослідження гібридних загроз у релігійній сфері та визначення основних напрямів протидії їм в Україні.

Завдання дослідження. Відповідно до мети дослідження поставлено такі завдання:

- дослідити сутність гібридних загроз та особливості їх прояву в релігійній сфері;

- охарактеризувати основні форми реалізації гібридних загроз у релігійній сфері, зокрема дезінформацію, пропаганду, мережеві операції та кіберзагрози;

- вивчити нормативно-правові та інституційні рамки свободи совісті й безпеки в Україні та відповідно до міжнародних стандартів;

- проаналізувати основні підходи до протидії гібридним загрозам у релігійній сфері в Україні та за кордоном.

Об'єкт дослідження – гібридні загрози як форма сучасного деструктивного впливу на суспільні процеси.

Предмет дослідження – форми прояву та механізми протидії гібридним загрозам у релігійній сфері.

Методи дослідження. Для досягнення поставленої мети та виконання визначених завдань у роботі використано загальнонаукові та спеціальні методи дослідження. Зокрема, застосовано методи аналізу і синтезу, узагальнення, порівняння, системний та структурно-функціональний методи, що дали можливість розглянути гібридні загрози в релігійній сфері як комплексне суспільно-політичне явище.

Практичне значення одержаних результатів полягає в тому, що основні положення та висновки роботи можуть бути використані у подальших дослідженнях проблематики гібридних загроз, а також при підготовці рекомендацій щодо посилення стійкості релігійної сфери до деструктивних інформаційних, організаційних і цифрових впливів.

Структура дослідження. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел (43 найменування).

Розділ 1. Теоретико-методологічні засади дослідження гібридних загроз у релігійній сфері

1.1. Поняття, ознаки та класифікації гібридних загроз

Поняття «гібридні загрози» сформувалося як відповідь на зміну логіки сучасного протиборства, коли досягнення стратегічних цілей забезпечується не одним видом сили, а комбінацією взаємопов'язаних впливів, які важко однозначно кваліфікувати як «мир» або «війну». У цьому сенсі гібридність означає не «новий тип війни», а радше спосіб організації ворожих дій: синхронізацію різнорідних засобів, їхню адаптацію до вразливостей цільової держави та прагнення зберігати простір для заперечення причетності й уникнення відповідальності. Таке розуміння дозволяє коректно перенести аналіз у гуманітарні сфери, зокрема релігійну, де впливи часто маскуються під легітимні форми суспільної активності, свободи слова або свободи віросповідання.

У політико-правовому дискурсі ЄС гібридні загрози описуються як поєднання примусових і підривних методів, інструментів та дій, що здійснюються державними або недержавними акторами і спрямовані на досягнення цілей, залишаючись нижче порогу формальної війни, тобто без очевидного «тригера» для класичних механізмів оборони та міжнародно-правової реакції [15]. Це визначення є важливим тим, що наголошує на двох опорних елементах: змішаності засобів та розрахунку на неоднозначність, яка ускладнює атрибуцію та політичну консолідацію відповіді.

Гібридні загрози поєднують військові та невійськові, приховані та відкриті засоби, включно з дезінформацією, кібератаками, економічним тиском, використанням нерегулярних збройних груп і навіть регулярних сил [25]. Ключова мета такої комбінації полягає у розмиванні меж між миром і війною, формуванні сумніву та підриві стійкості суспільства і державних інституцій (НАТО). Для дослідження гуманітарних доменів це принципово, оскільки впливи тут працюють насамперед через довіру, ідентичність, соціальні норми та інтерпретації подій.

Аналітичні моделі Єврокомісії та Hybrid CoE дають операціоналізоване визначення, придатне для наукового аналізу: гібридна активність кваліфікується як така, що передбачає одночасне застосування множинних інструментів у межах скоординованої кампанії для експлуатації вразливостей або можливостей і, як наслідок, підриву процесу ухвалення рішень противника за збереження певного ступеня правдоподібного заперечення [20, с. 26]. Це визначення зручне тим, що задає перевірювані ознаки: множинність інструментів, координацію в часі та за цілями, фокус на вразливостях, вплив на decision-making та деніабіліті. Наприклад, у релігійній сфері гібридна кампанія може поєднувати поширення повідомлень про нібито утиски віруючих, мережеве підсилення цих меседжів через лояльні медіа та спільноти, а також тиск на цифрові платформи релігійної організації. У такому випадку окремі дії працюють не ізольовано, а як частини одного сценарію, спрямованого на посилення недовіри, поляризації та конфліктності [20, с. 26, 34–35; 26, с. 4].

У теоретичній площині витоки поняття гібридності пов’язані з описом «змішаних» конфліктів, у яких поєднуються конвенційні спроможності, нерегулярні тактики, тероризм і кримінальна складова. Ф. Гоффман підкреслює саме синергію та одночасність таких модальностей, які застосовуються в одному театрі дій для посилення ефекту, а не як набір випадкових елементів [21, с. 8]. Перенесення цього підходу на рівень «загроз» пояснює, чому гібридні кампанії часто мають мережеву структуру, опосередковані інституціями та медіа, і можуть довго залишатися нижче рівня прямого збройного зіткнення.

Відмежування «гібридних загроз» від «гібридної війни» доцільно робити через критерій рівня ескалації та режиму функціонування системи безпеки. У практичних керівництвах зі стратегічних комунікацій наголошено, що гібридні загрози реалізуються через поєднання ворожих заходів у так званій «сірій зоні» між миром, кризою та війною, просуваючи стратегічні цілі противника без переходу до відкритого конфлікту [26, с. 4]. Отже, «загроза» у гібридному сенсі є тривалою конкурентною активністю, яка може ескалювати до «війни», але не тотожна їй за правовими наслідками та інструментарієм відповіді.

З огляду на наведені підходи, базовими ознаками гібридних загроз слід вважати багатодоменність і комбінованість, стратегічну координацію, пріоритет когнітивного ефекту, опосередкованість, а також неоднозначність і складність атрибуції. Практичні огляди підкреслюють, що саме неоднозначність, інтегрованість заходів та орієнтація на психологічні й соціальні ефекти роблять гібридні впливи стійкими до стандартних процедур реагування [26, с. 8].

Для гуманітарного виміру критичною є теза про «системні вразливості» демократичних держав і інституцій. Hybrid CoE визначає гібридні загрози як скоординовані та синхронізовані дії, що навмисно націлені на системні вразливості демократичних держав та експлуатують пороги виявлення й атрибуції [39]. Це безпосередньо пов’язує гібридність з довірою, соціальною згуртованістю, легітимністю інститутів, а в релігійній сфері з авторитетом духовних лідерів, символічним капіталом конфесій і чутливістю ідентичнісних маркерів.

У моделі JRC та Hybrid CoE наголошується на комплексності й доцільності розрізняти домени, в межах яких атакуються функції держави, а також інструменти, якими реалізується вплив; у межах моделі запропоновано 13 доменів, що демонструють необхідність «цілісного» підходу, який поєднує цивільні й військові компоненти [20, с. 26–27]. Для релігійної сфери тут принципово, що поряд із «інформаційним» та «політичним» доменами прямо фігурують «соціальний/суспільний» і «культурний», тобто ті площини, де релігійна ідентичність та конфесійні мережі можуть ставати середовищем або інструментом впливу.

Приклад прикладної класифікації через «інструменти влади» пропонує MCDC: гібридна активність описується як синхронізоване використання множинних інструментів влади, адаптованих до конкретних вразливостей у повному спектрі суспільних функцій для досягнення синергетичних ефектів [24, с. 4]. У межах цієї логіки придатним для подальших розділів бакалаврської роботи стає поділ не лише за «сферами» інформаційна, економічна, кібер тощо, а й за механікою: що саме є вразливістю, які засоби її «вмикають» і який ефект планується делегітимація, демобілізація, радикалізація чи керований конфлікт.

Окремий критерій класифікації, важливий саме для гуманітарних доменів, це спрямованість на соціокультурні розломи. У переліках інструментів гібридної активності модель JRC та Hybrid CoE прямо називає експлуатацію соціокультурних розколів етнічних, релігійних і культурних як інструмент, що впливає на соціальний/суспільний і культурний домени [20, с. 34–35]. Це дає методологічно коректну основу для подальшого аналізу релігійної сфери як середовища, де розкол може не просто відображатися, а технологічно конструюватися через наративи, фінансування, мережеві зв'язки та керовані провокації.

Отже, у межах цієї бакалаврської роботи доцільно фіксувати робоче визначення гібридних загроз як скоординованих багатодоменних кампаній, що синхронно застосовують різні інструменти для експлуатації системних вразливостей, підриву процесів ухвалення рішень і суспільної стійкості за умов неоднозначності та ускладненої атрибуції. Відповідно, класифікація має будуватися щонайменше за трьома взаємодоповнюючими осями: домени впливу, інструменти та режим реалізації. Така схема забезпечує керованість подальшого аналізу і дозволяє уникнути змішування легітимних форм релігійної діяльності з ворожими операціями, що маскуються під них.

1.2. Релігійна сфера як об'єкт гібридного впливу: актори, середовище, вразливості

Релігійна сфера є зручним «входом» для гібридного впливу, тому що поєднує символічний ресурс (цінності, ідентичність, моральний авторитет) із розгалуженою соціальною інфраструктурою (громади, мережі довіри, благодійні та освітні ініціативи). У логіці гібридних загроз ключовим є не пряме знищення інституцій, а підрив соціальної згуртованості та керованості суспільних процесів через експлуатацію наявних поділів і напружень, зокрема ціннісних та світоглядних. Саме тому гуманітарні домени, включно з релігією, розглядаються як середовище,

де атакуючий суб'єкт може досягати політичних цілей «нижче порогу» відкритого конфлікту, комбінуючи інформаційні, організаційні та інші інструменти [15; 39]. Практично це може проявлятися через розпалювання конфліктів навколо переходу релігійних громад, користування храмами, публічних заяв духовних лідерів або поширення повідомлень про нібито «утиски» певної конфесії.

Конфліктності релігійні організації виступають одночасно й ресурсом стійкості, і потенційною «точкою входу» для маніпуляцій: авторитет релігійних лідерів полегшує легітимацію меседжів, а мережевість громад прискорює їхнє поширення. У документах ООН/ООН-структур підкреслюється необхідність створення «безпечних просторів» для діалогу, підтримки локальних ініціатив і використання позитивних/альтернативних наративів для протидії мові ненависті й підбурюванню, де релігійні актори можуть відігравати практичну роль у модерації та зниженні напруги [29, с. 3, 9]. Це означає, що одна й та сама релігійна громада за різних умов може або стримувати конфлікт, або ставати середовищем його прискорення, якщо її комунікаційні механізми, символічний авторитет чи локальні мережі довіри використовуються для поширення маніпулятивних наративів.

Основні актори гібридного впливу у релігійній сфері включають державні структури (або структури під їхнім контролем), а також недержавних посередників: медіа-мережі, «громадські» організації, фонди, експертні середовища, окремих лідерів думок. Спільна ознака прагнення зберегти правдоподібне заперечення причетності, коли вплив реалізується через формально автономні організації з непрозорими управлінськими та фінансовими зв'язками. Практично це означає, що гібридний вплив у релігійній сфері часто маскується під пастирську, культурну, гуманітарну або правозахисну діяльність, але має зовнішню координацію та політичну мету [39; 26, с. 30]. Наприклад, йдеться не обов'язково про прямий політичний тиск, а про підтримку медійних платформ, благодійних ініціатив чи мереж комунікації, які поступово формують потрібні інтерпретації подій та залежності всередині релігійного середовища.

Середовище гібридного впливу значною мірою задається інституційно-правовими правилами функціонування релігійних організацій: реєстрацією,

майновими питаннями, доступом до публічних ресурсів, участю в освіті та медіа, благодійною діяльністю. Уразливість виникає там, де процедури допускають надмірну дискрецію або нерівність підходів до різних громад, створюючи «точки тиску» від блокування діяльності й спорів щодо майна до стимулювання конкурентних конфесійних конфліктів. Водночас міжнародні стандарти фіксують рамку: свобода думки, совісті та релігії охоплює як внутрішнє переконання, так і зовнішнє «виявлення» віри; обмеження допустимі лише на підставі закону і лише настільки, наскільки це необхідно для охорони публічної безпеки, порядку, здоров'я, моралі або прав інших осіб [34, с. 16–20; 41]. У практичному вимірі це особливо важливо у випадках спорів щодо реєстрації громади, зміни її підлеглості або користування культовою спорудою, коли будь-яка правова невизначеність швидко переходить у площину інформаційного й суспільного конфлікту.

Окрема уразливість з'являється на стику безпеки та прав людини: коли державні обмеження щодо релігійної діяльності є непропорційними або юридично слабко обґрунтованими, вони створюють простір для конфліктної інтерпретації та пропагандистського використання. Комітет ООН з прав людини наголошує, що підстави для обмеження свободи релігії тлумачаться вузько, а держава має доводити необхідність і пропорційність втручання у кожному конкретному випадку [40, п. 8]. Це означає, що навіть безпеково мотивовані рішення, якщо вони не мають чіткої правової логіки та належного пояснення, можуть використовуватися як матеріал для наративів про «гоніння», «дискримінацію» або «заборону віри».

Важливим контуром середовища є інформаційний і цифровий вимір. Релігійна ідентичність легко перетворюється на інструмент фреймінгу («свої/чужі», «зрада/вірність», «сакральне/профанне»), що знижує поріг маніпуляції та прискорює поляризацію. У концептуальних моделях гібридних загроз прямо виділяються домени, де атакуючий суб'єкт працює з культурою та ідентичністю, поступово формуючи «підготовлене» інформаційне середовище й зміщуючи інтерпретації подій у потрібний бік; практичні інструменти тут типові загострення суспільних поділів, кампанії з дезінформації, мережеве «підживлення»

конфліктів [20, с. 33–35; 26, с. 9]. На практиці це може виглядати як одночасне поширення у Telegram-каналах, соціальних мережах і коментарях під новинами однакових повідомлень про «захоплення храмів», «образу святинь» або «переслідування віруючих», що створює враження масштабної загрози навіть за відсутності перевірених фактів.

Емпірично вразливість підсилюється там, де вже існують або накопичуються соціальні ворожості, пов’язані з релігією, а також там, де зростають урядові обмеження, що сприймаються як вибіркові чи несправедливі. Порівняльний моніторинг Pew Research Center показує, що високі рівні державних обмежень і соціальних ворожостей щодо релігійних груп у багатьох країнах співіснують, формуючи конфліктогенний фон [35, с. 5]. Для аналізу гібридних загроз це означає, що за наявності напруги її значно дешевше «активувати» інформаційно й організаційно, ніж конструювати з нуля. Саме тому релігійне середовище, де вже є недовіра, внутрішні суперечності або конкуренція за символічний вплив, є особливо чутливим до зовнішнього втручання.

У підсумку релігійну сферу доцільно розглядати як систему перетину трьох елементів: акторів (хто і з якою метою діє), середовища (правила, інституції, мережі комунікації) та вразливостей (де можливе непропорційне посилення конфлікту). Це визначення є важливим тим, що дозволяє далі описувати форми й інструменти реалізації гібридних загроз не як розрізнені явища, а як узгоджені пакети впливу, «підшиті» під конкретні слабкі місця релігійного поля [20, с. 26].

1.3. Нормативно-правові та інституційні рамки свободи совісті й безпеки: Україна та міжнародні стандарти

У сфері протидії гібридним загрозам держава неминуче працює «на стику» безпеки та прав людини. Саме тому нормативно-правові рамки мають подвійну функцію: (а) гарантувати свободу совісті й рівність релігійних організацій; (б) легітимізувати та обмежити інструменти реагування на ворожі впливи

(інфільтрацію, дезінформацію, підрив довіри), щоб протидія не перетворювалася на дискримінацію чи довільне втручання. Європейський підхід до «countering hybrid threats» підкреслює потребу в узгодженій міжвідомчій взаємодії, підвищенні стійкості та ситуаційній обізнаності як базі для правомірних рішень [15].

Міжнародним «ядром» стандартів свободи релігії є ст. 18 Міжнародного пакту про громадянські і політичні права (МПГПП), яка охоплює як внутрішній вимір свободи (переконання), так і зовнішній (проявлення релігії/віри). Для протидії гібридним загрозам критично важливий принцип: обмеження допускаються лише у вузько визначених цілях і за умов законності та необхідності, інакше «безпекове» обґрунтування перетворюється на універсальну підставу для заборон [41].

Комітет ООН з прав людини в Загальному коментарі № 22 деталізує ст. 18 МПГПП і фактично задає «тест допустимості»: обмеження свободи проявляти релігію можливі лише якщо вони (1) встановлені законом; (2) є необхідними для захисту громадської безпеки, порядку, здоров’я, моралі або прав і свобод інших; (3) є пропорційними конкретній потребі. Окремо підкреслено, що підстави обмежень мають тлумачитися суворо, а «національна безпека» як самостійний мотив обмеження проявлення релігії не допускається, якщо вона не «поміщається» у перелік ст. 18(3) [40].

На європейському континенті ключовим орієнтиром є ст. 9 Європейської конвенції з прав людини (ЄКПЛ) та практика ЄСПЛ. Конвенційна модель також відрізняє свободу переконань і свободу їх проявлення та дозволяє втручання лише «згідно із законом» і лише настільки, наскільки це «необхідно в демократичному суспільстві» для легітимних цілей (зокрема громадської безпеки, охорони порядку, здоров’я і моралі, захисту прав інших) [11].

Практичне значення для теми гібридних загроз має те, що ЄСПЛ у своїх підходах вимагає від держави доведення необхідності та пропорційності втручання; тобто не достатньо послатися на «ризики» або «напругу» потрібні фактичні підстави, коректна правова процедура і мінімально достатні заходи. Водночас Суд підкреслює, що свобода релігії є одним із фундаментів

демократичного суспільства і застосовується не лише до віруючих, а й до атеїстів та агностиків, що прямо обмежує спокусу «сакралізувати» державну політику як інструмент мобілізації [16].

Окремий нормативний «міст» між безпекою і свободою совісті формують рекомендаційні стандарти ОБСЄ/БДІПЛ та Венеційської комісії. У «Guidelines for Review of Legislation Pertaining to Religion or Belief» наголошується на принципах недискримінації, нейтральності держави щодо віровчень, прозорих процедур реєстрації/діяльності та використанні загального кримінального й адміністративного права для реагування на правопорушення без створення надмірно репресивних спеціальних режимів для «незручних» груп [34].

В Україні конституційна рамка свободи совісті задана ст. 35 Конституції України: гарантується свобода світогляду і віросповідання, а обмеження можливі лише законом і лише в інтересах охорони громадського порядку, здоров'я і моралі населення або захисту прав і свобод інших людей. Ця конструкція задає межі «сек'юритизації»: навіть за наявності гібридних ризиків держава має діяти в рамках формалізованих підстав та процедур, а не через ситуативні заборони [1].

Профільним законом є Закон України «Про свободу совісті та релігійні організації», який деталізує зміст свободи совісті, принцип рівності громадян незалежно від ставлення до релігії та повторює «обмежувальний тест»: свобода сповідувати релігію/переконання підлягає лише тим обмеженням, які необхідні для охорони громадської безпеки та порядку, життя, здоров'я і моралі, а також прав і свобод інших громадян, і які встановлені законом та відповідають міжнародним зобов'язанням України [9]. Одночасно закон містить окремі механізми щодо обмеження діяльності релігійних організацій, афілійованих із визначеними іноземними центрами, як інструмент реагування на ризики використання релігійних структур у ворожих операціях (за умови дотримання процедурності та доказовості) [9].

Інституційно державну політику у сфері релігії та свободи совісті забезпечує Державна служба України з етнополітики та свободи совісті (ДЕСС) як центральний орган виконавчої влади. Нормативна база її статусу та повноважень

визначена постановою КМУ № 812: ДЕСС забезпечує формування і реалізацію державної політики у сфері релігії та, зокрема, у межах повноважень здійснює контроль за додержанням законодавства про свободу совісті та релігійні організації [3]. Для моделі протидії гібридним загрозам це важливо як «цивільний» контур управління ризиками (правова експертиза, моніторинг, координація), який має працювати паралельно із безпековими інституціями, але не підміняти суд і не створювати позапроцедурні санкції [3].

На рівні стратегічної рамки (наднаціональний контекст) НАТО визначає гібридні загрози як комбінацію військових і невійськових, прихованих і відкритих засобів, включно з дезінформацією та кібератаками, спрямованих на підрив та дестабілізацію суспільств, що прямо виводить релігійну сферу в зону ризику як «провідник» впливу на ідентичність і соціальну довіру [25]. Відповідно, юридично коректна протидія у релігійній сфері має спиратися на стандарти прав людини (щоб не «підсилювати» ворожий наратив про утиски), а інституційно на міжвідомчу координацію та стійкість, а не на ситуативні заборони як першу реакцію [25].

Висновок до розділу 1. Гібридні загрози слід розуміти як скоординовані багатодоменні дії, у межах яких поєднуються різні інструменти впливу інформаційні, організаційні, політичні, економічні, цифрові та інші. Їхня особливість полягає в тому, що вони спрямовані на використання вразливостей держави й суспільства, діють переважно нижче порогу відкритого збройного протистояння та часто супроводжуються можливістю заперечення справжньої причетності. Такий підхід дає змогу розглядати гібридні загрози не як набір окремих проявів, а як цілісну кампанію, у якій важливими є і сфери впливу, і використані інструменти, і спосіб їх поєднання.

Релігійна сфера є особливо чутливою до гібридного впливу, оскільки поєднує символічний ресурс, суспільну довіру, моральний авторитет і розгалужені мережі комунікації. Саме тому вона може використовуватися для маніпуляції ідентичністю, посилення поляризації та провокування конфліктів. Водночас реагування у цій сфері не може виходити за межі законності та стандартів свободи

совісті. Будь-які обмеження чи втручання мають бути правомірними, необхідними, пропорційними й належно обґрунтованими, інакше вони самі здатні посилити напругу та створити нові підстави для дестабілізації.

Розділ 2. Форми, інструменти та технології реалізації гібридних загроз у релігійній сфері

2.1. Дезінформація, пропаганда, мережеві операції

У структурі гібридних загроз дезінформація та пропаганда виступають інструментами впливу на сприйняття реальності, довіру й поведінку цільових груп. Для аналітичної точності доцільно використовувати рамку "інформаційного безладу", де розрізняють: misinformation (поширення хибного без наміру шкоди), disinformation (свідоме поширення хибного для завдання шкоди) та malinformation (поширення правдивої інформації з наміром завдати шкоди, зокрема через "витоки" приватних даних у публічний простір) [3, с. 5].

У релігійній сфері ефект дезінформації посилюється тим, що релігійна ідентичність є "високозначущим" маркером належності та цінностей. Впливові кампанії спираються на наявні лінії соціальної напруги та "підживлюють" поляризацію, підмінюючи суспільну дискусію логікою "свій/чужий". У такій логіці релігійна група або символ легко подається як загроза або як "жертва", що переводить раціональну перевірку фактів у площину захисту "наших" цінностей [22, с. 4].

Ключовою технологією тут є фреймінг конструювання інтерпретаційної рамки, яка задає "правильне" прочитання подій: хто винний, кому загрожують, що є "нормою", а що "відхиленням". У дезінформаційних кампаніях ідентичності навмисно "атакуються" через threat-oriented framing подання однієї ідентичності або комбінації ідентичностей як такої, що перебуває в конфлікті з іншою, а повідомлення підлаштовується під конкретну аудиторію [22, с. 5].

Окремий чинник результативності емоційні наративи, які цілеспрямовано активують страх, гнів, відразу, образу, тобто емоції, що знижують вимоги аудиторії до доказовості та підвищують готовність до колективних дій. На релігійному матеріалі це часто проявляється у "моральній паніці", демонізації опонента, навішуванні ярликів "ворога віри", "секти", "екстремістів", а також у роздмухуванні уявних загроз традиції чи святиням. Мета збільшити недовіру між

групами (“вони” проти “нас”) і ускладнити суспільний діалог [22, с. 5]. Наприклад, у кризові періоди в інформаційному просторі можуть поширюватися повідомлення про нібито “захоплення храму”, “осквернення святині” чи “заборону богослужінь”, коли окремий інцидент або неперевірене повідомлення подається як доказ системного переслідування певної релігійної спільноти. У такому випадку сама емоційна подача часто виявляється сильнішою за перевірку фактичних обставин.

Створення псевдонаративів у релігійній тематиці зазвичай працює як комбінація трьох елементів: “зерно правди” (реальна подія, цитата, фото), хибна інтерпретація або підміна контексту та “пояснювальна легенда”, яка закриває прогалини й дає просту причинно-наслідкову схему. Практично важливо, що псевдонаратив може включати і malinformation, наприклад публікацію приватного листування, списків, адрес, персональних даних для дискредитації релігійної спільноти або провокування конфлікту, при тому що фактичне ядро може бути правдивим [3, с. 5]. Наприклад, фотографія з локального конфлікту біля релігійного об’єкта може супроводжуватися твердженням про “масові гоніння”, навіть якщо сам інцидент мав інший контекст або був побутовою суперечкою. Аналогічно окрема цитата релігійного діяча, вирвана з ширшого виступу, може бути подана як доказ “екстремізму”, “зради” або “підготовки провокацій”.

Нормативний вимір проблеми полягає в тому, що дезінформація і пропаганда здатні шкодити репутації та приватності або підбурювати до насильства, дискримінації чи ворожнечі щодо ідентифікованих груп, але “широкі” заборони на підставі розмитих понять на кшталт “необ’єктивної” чи “фальшивої” інформації несумісні з міжнародними стандартами свободи вираження. Водночас підкреслюється, що державні актори не повинні поширювати завідомо неправдиві повідомлення або діяти з недбалою зневагою до перевірюваних даних [23, с. 1–2].

Технологічно дезінформаційний вплив у релігійній тематиці прискорюється сучасним медіасередовищем: цілодобовий новинний цикл, соціальні мережі, взаємопов’язаність аудиторій та здатність масштабувати повідомлення через організовані мережі акаунтів. У межах стратегічних комунікацій акцент робиться на тому, що результат визначає не лише повідомлення, а й аналіз цільової аудиторії,

платформи та узгодженість інформаційних дій із ширшими цілями впливу; окремо фіксується, що соціальні медіа можуть використовуватися як “зброя” в гібридних сценаріях, а мережі тролів та онлайн-коментаторів здатні системно деформувати інформаційний діалог [10, с. 2–3]. На практиці це може проявлятися в одночасному поширенні однакових повідомлень у кількох Telegram-каналах, групах у соціальних мережах і коментарях під новинами, що створює ілюзію масового обурення або “очевидної суспільної думки”, хоча фактично йдеться про скоординоване інформаційне підсилення потрібного наративу.

Поряд із дезінформацією та пропагандою важливе місце у структурі гібридних загроз займають мережеві операції. У релігійній сфері вони часто реалізуються через схему «спонсор–проксі», коли центр впливу делегує активність формально автономним структурам фондам, медіа-ініціативам, “культурним” і “гуманітарним” проєктам, зберігаючи можливість заперечення причетності та уникаючи прямої відповідальності. Мережа при цьому будується як сукупність взаємопов’язаних вузлів, які діють під легітимним прикриттям, але виконують узгоджену політичну задачу: від зміни порядку денного до створення довгострокових залежностей і контролю над рішеннями в межах релігійних організацій [36, с. 11–15]. Вразливість релігійного середовища посилюється високим рівнем довіри всередині спільнот, авторитетом лідерів та наявністю стійких горизонтальних контактів між громадами, що робить мережеві операції менш помітними у звичайному житті організацій.

Фінансування виступає базовим важелем інфільтрації, оскільки дає можливість управляти поведінкою без формального підпорядкування. Практичні ризики формують непрозорі пожертви, “цільові гранти”, благодійні збори, оплата заходів і поїздок, утримання медіаплатформ та інфраструктури, а також підтримка пов’язаних НГО як транзитних ланок. Міжнародні рекомендації щодо протидії зловживанням у секторі неприбуткових організацій підкреслюють типові слабкі місця: відсутність належних внутрішніх контролів, недостатня прозорість руху коштів, неналежна перевірка контрагентів і кінцевих отримувачів, використання організацій-прикриттів для маскування реальних бенефіціарів та механізмів впливу

[19, с. 26–28; 13–36]. У релігійному сегменті ці патерни проявляються як “благодійність” або “підтримка духовних ініціатив”, що фактично формує залежність і дисциплінує мережу через ресурсні важелі. Наприклад, зовнішній вплив може здійснюватися не через прямі політичні вимоги, а через фінансування паломницьких поїздок, медійних проєктів, гуманітарних програм або утримання окремих інформаційних майданчиків, які поступово формують потрібний порядок денний у середині релігійного середовища.

Кадровий вплив є довгостроковою технологією захоплення порядку денного і може включати просування лояльних осіб у керівні органи, створення “кадрових ліфтів”, контроль освіти та підготовки кадрів, а також призначення на чутливі напрями комунікації, фінанси, молодіжні проєкти, гуманітарні програми. Умовою результативності кадрового впливу є те, що зовні він виглядає як внутрішня автономна кадрова політика, а зовнішня координація прихована через фінансову залежність, неформальних кураторів, “радників” або навчально-організаційні платформи. Саме тому міжнародні стандарти щодо свободи релігії наголошують на важливості правосуб’єктності релігійних спільнот і мінімізації довільного втручання держави у внутрішні процеси: будь-які обмеження та втручання в організаційну автономію мають бути правомірними, необхідними та пропорційними [32, с. 14–18]. Водночас ця сама автономія, якщо поєднана з низькою прозорістю, може створювати “сліпу зону” для мережевого захоплення через кадри. Практично це може означати ситуацію, коли особи, відповідальні за комунікацію чи фінансові рішення, тривалий час формально діють від імені громади, але фактично орієнтуються на зовнішній центр впливу, який забезпечує їм організаційну, інформаційну або ресурсну підтримку.

Організаційні залежності посилюються юридичними та інфраструктурними факторами: статус юридичної особи, доступ до банківських послуг, управління майном, видавнича та освітня діяльність, мережі гуманітарної допомоги формують точки, де легальна діяльність може бути перепрограмована під зовнішній контроль. У цьому контексті принциповим є питання прозорості власності та контролю: європейська AML-рамка, зокрема вимоги щодо ідентифікації кінцевих

бенефіціарних власників у відповідних структурах, спрямована на зменшення ризику прихованого контролю через юридичні оболонки й посередників [12, ст. 30–31]. Для релігійної сфери практичний висновок полягає у тому, що пов’язані фонди, НГО та медіапроєкти потребують прозорої моделі управління, внутрішнього аудиту та процедур прийняття значних пожертв, інакше вони стають “порталом” для зовнішнього впливу.

З позиції протидії ключове підвищувати стійкість мережі до зовнішнього захоплення, не руйнуючи свободу совісті й автономію релігійних організацій. Це означає картографування вузлів впливу грошей, кадрів, інфраструктури, медіа, підсилення внутрішнього врядування і контролів, створення легальних механізмів взаємодії з державними та фінансовими інституціями. Окремо доцільно формувати політику щодо проксі-акторів: критерії ризику, інструменти документування зв’язків, пропорційні реагування, які враховують складність атрибуції та багаторівневість мереж [36, с. 16–20]. Водночас необхідно брати до уваги, що громадянське суспільство, у тому числі релігійні ініціативи, у гібридних сценаріях розглядається як “простір боротьби”, а отже потрібні сталі механізми координації, кризових комунікацій і підвищення організаційної стійкості, аби мережеві операції не досягали ефекту розколу та делегітимації [17, с. 2–4].

Дезінформація, пропаганда та мережеві операції є взаємопов’язаними формами реалізації гібридних загроз у релігійній сфері. Їхня ефективність ґрунтується на використанні суспільної довіри, релігійної ідентичності, організаційних зв’язків і сучасних засобів комунікації. Саме тому небезпека таких впливів полягає не лише у поширенні окремих неправдивих повідомлень, а й у поступовому формуванні залежностей, поляризації та дестабілізації релігійного середовища.

2.2. Кіберзагрози в релігійній сфері

Цифровізація релігійного життя, зокрема використання сайтів громад, сторінок у соціальних мережах, трансляцій богослужінь, груп у месенджерах,

онлайн-пожертв, електронних реєстрів членства та баз контактів, створює технічну «поверхню атаки», яка стає важливою частиною гібридних впливів. У логіці таких операцій кіберкомпонент не зводиться лише до класичного злому, оскільки його цілі є ширшими: підрив довіри до релігійних інституцій, провокування внутрішніх конфліктів, зрив комунікації, викрадення й подальше використання персональних даних, а також створення інформаційних приводів для пропаганди. Європейський огляд загроз прямо пов'язує маніпуляції інформацією з підготовчими активностями для інших атак, зокрема фішингу та соціальної інженерії, що особливо важливо для релігійного середовища як емоційно чутливого та ідентичнісного простору [14, с. 107]. Наприклад, злам офіційної сторінки релігійної громади може використовуватися не лише для технічного блокування роботи, а й для публікації провокативного повідомлення, яке далі поширюється як нібито справжня позиція цієї спільноти.

Кіберзагрози щодо релігійних спільнот доцільно розглядати через три базові виміри безпеки: конфіденційність, цілісність і доступність. У сучасному ландшафті загроз атаки на доступність, зокрема DDoS, а також ransomware належать до ключових ризиків поряд із соціальною інженерією та загрозами даним. Це означає, що навіть без складних APT-сценаріїв типові інструменти можуть завдати суттєвої шкоди організаціям з обмеженим IT-ресурсом, до яких нерідко належать місцеві релігійні громади [14, с. 4]. Практично це може проявлятися у відключенні сайту громади в день великого релігійного свята, блокуванні онлайн-трансляції богослужіння або втраті доступу до бази контактів волонтерів і парафіян у період збору допомоги.

Соціальна інженерія залишається одним із найпоширеніших стартових векторів атак. У звіті ENISA наголошено, що фішинг і pretexting через email продовжують бути провідною причиною інцидентів, а також підкреслюється роль правдоподібних легенд і контекстуальних підробок, які імітують внутрішні розсилки, партнерів, благодійні фонди або термінові прохання про допомогу [14, с. 63–64]. Для релігійного середовища такі сценарії особливо ефективні, оскільки апелюють до морального авторитету, емпатії та звички до пожертв. Наприклад,

члени громади можуть отримати лист або повідомлення нібито від настоятеля чи адміністратора парафії з проханням терміново переказати кошти на “лікування”, “ремонт храму” або “допомогу постраждалим”, хоча насправді такий збір є шахрайським.

Окремий ризик становить компрометація пошти та акаунтів адміністраторів сторінок і акаунтів, коли зловмисник фактично перехоплює офіційний голос спільноти. Наслідки такого втручання є не лише фінансовими, як-от шахрайські збори, а й репутаційними, адже від імені громади можуть поширюватися провокативні заяви, «викривальні» повідомлення або матеріали, що розпалюють міжконфесійне напруження. У цьому контексті важливо враховувати дані про вагу соціальної інженерії для компрометацій у секторі малих і середніх організацій, де людський фактор стає визначальним у ланцюгу інциденту [43, с. 11]. У практичному вимірі це означає, що навіть один скомпрометований акаунт може стати джерелом масштабного конфлікту, якщо від імені релігійної організації буде оприлюднено образливу або політично провокативну заяву.

Додатковим технологічним зсувом останніх років стало використання штучного інтелекту для масштабування соціальної інженерії: персоналізації листів, генерації переконливих текстів під стиль конкретної спільноти, швидкого створення графіки й оголошень, а також атак типу prompt bombing, які перевантажують процеси підтримки та комунікації. У Verizon для SMB-сегмента зафіксовано prompt bombing як окремий патерн інцидентів, що свідчить про адаптацію зловмисників до нових комунікаційних платформ і процедур [43, с. 11]. Для релігійних організацій це означає, що атаки можуть бути спрямовані не лише на гроші, а й на зрив роботи волонтерських координацій, гарячих ліній, записів на допомогу тощо. Наприклад, автоматизовані звернення або масові повідомлення можуть паралізувати сторінку громади чи засіб комунікації з людьми, які реально потребують підтримки.

Цифрові платформи, зокрема соціальні мережі, відеохостинги, месенджери та рекламні кабінети, додають до кіберкомпонента гібридних загроз платформну специфіку. Боти та мережі керованих акаунтів виступають інструментом

прискореного охоплення: вони створюють ілюзію масовості, підсилюють потрібні повідомлення, атакують опонентів скаргами, коментарними набігами та штучними дискусіями. Дослідження про соціальних ботів описує їхню здатність імітувати людську поведінку, взаємодіяти з контентом і впливати на динаміку поширення інформації в онлайні, що робить їх придатними для операцій підміни консенсусу [18, с. 96–99]. Наприклад, після публікації новини про релігійний конфлікт під нею можуть одночасно з'являтися десятки однотипних коментарів, які формують враження, ніби суспільство вже одностайно засудило певну громаду або, навпаки, підтримало агресивні дії проти неї.

Боти на платформах працюють у зв'язці з таргетингом. Контент, у тому числі провокативний, може спрямовуватися до аудиторій за інтересами, географією, мовою та поведінковими сигналами. Водночас на рівні регулювання ЄС існують прямі обмеження щодо таргетованої реклами на основі чутливих категорій даних: Digital Services Act забороняє показ таргетованої реклами на основі профілювання з використанням спеціальних категорій персональних даних [38, ст. 26(3)]. Для релігійної сфери це має принципове значення, оскільки релігійні переконання належать до чутливих категорій у праві ЄС, а отже мають підвищений режим захисту [37, ст. 9(1)]. На практиці це не усуває ризиків повністю, але задає важливі юридичні рамки для протидії та доведення порушень. Наприклад, конфліктний контент може спеціально підсилюватися саме в тих локальних громадах, де вже існує напруження між конфесіями, щоб прискорити ескалацію.

Витоки даних у релігійній сфері мають подвійний ефект: прямий, тобто фінансові й юридичні наслідки, і непрямий, зокрема психологічний тиск, стигматизацію та підвищення конфліктогенності. До вразливих наборів даних належать списки членів громади, контакти служителів і волонтерів, адреси, історія пожертв, записи про участь у заходах, а також дані про допомогу вразливим групам. ENISA описує загрози даним як широкий спектр подій від витоків і неправомірного доступу до втрати чи експозиції конфіденційної інформації, що в гібридних сценаріях легко переходить у площину шантажу та дискредитації [14, с. 69–71]. Для релігійних спільнот витік таких даних може стати інструментом

залякування, доксингу та стимулювання ворожнечі. Наприклад, оприлюднення списків волонтерів, донорів або активних учасників громади може бути використане для тиску, публічного цькування чи погроз.

Правовий вимір витоків у цій темі є критично важливим, оскільки персональні дані, що виявляють релігійні або філософські переконання, у GDPR прямо віднесені до спеціальних категорій і загалом заборонені до обробки, окрім визначених винятків [37, ст. 9(1)]. Це означає, що у випадку інцидентів релігійні організації мають справу не зі звичайними контактами, а з даними підвищеної чутливості, де шкода від розкриття часто є непропорційно більшою, ніж у стандартних комерційних базах. Показово також, що GDPR містить спеціальну норму про правила захисту даних церков і релігійних об'єднань у державах-членах за умови їх узгодження з Регламентом [37, ст. 91], що додатково підтверджує інституційну вагу питання.

Кіберкомпонент у гібридних загрозах часто працює як постачальник матеріалу для подальших інформаційних операцій. Викрадені листування, фото, внутрішні документи, списки донорів або чернетки проповідей можуть публікуватися дозовано й у маніпулятивному контексті, щоб створити відчуття скандалу чи викриття. Важливою є саме технологія цього впливу: доступ до акаунтів, ексфільтрація, підміна метаданих, фрагментація витоку та його синхронізація з бот-активністю на платформах. Логіка зв'язку інформаційних маніпуляцій і подальших атак, таких як фішинг, соціальна інженерія або інфікування, у звіті ENISA подана як системний ланцюг, що пояснює, чому кібер- та інформаційний компоненти в гібридних впливах майже завжди взаємопов'язані [14, с. 107]. Практичним прикладом може бути ситуація, коли після зламу електронної пошти окремі фрагменти листування публікуються у вибірковому вигляді, щоб створити враження змови, внутрішнього розколу або фінансових зловживань у межах громади.

Атаки на доступність, насамперед DDoS, у релігійній сфері мають специфічні пікові точки: великі свята, масові заходи, онлайн-трансляції, періоди благодійних кампаній і кризові події. ENISA визначає DDoS як загрозу доступності, коли

користувачі не можуть отримати доступ до даних, сервісів чи ресурсів, і підкреслює сталу роль цієї загрози в сучасному ландшафті [14, с. 8]. Для релігійних спільнот це означає зрив комунікації з вірянами та благодійниками, а в гібридних сценаріях демонстрацію контрольованості простору та символічний сигнал сили. Наприклад, блокування сайту або трансляції в день великого релігійного свята може мати значно більший психологічний ефект, ніж та сама атака у звичайний день.

ENISA також фіксує, що наприкінці звітного періоду спостерігалося суттєве зростання DDoS-інцидентів як за кількістю, так і за масштабом, і ENISA пов'язує це зі зростанням впливу хактивізму та загостренням геополітичних напружень [14, с. 79]. Це безпосередньо стосується релігійної сфери, оскільки релігійні об'єкти та онлайн-майданчики можуть обиратися як символічні цілі: атака на сайт чи трансляцію стає не просто технічним інцидентом, а медійним повідомленням і приводом для подальшої пропаганди.

Ransomware у релігійній сфері небезпечний не лише шифруванням, а й ефектом сорому та шантажу. Загроза оприлюднення листування з парафіянами, даних про пожертви або внутрішні конфлікти може стати сильнішим важелем, ніж власне зупинка роботи. ENISA відносить ransomware до найвищих загроз у загальному рейтингу та розглядає його як один із домінантних типів інцидентів у періоді спостереження [14, с. 4; 34]. Для організацій зі слабкою резервною інфраструктурою й мінімальними процедурами відновлення це створює ризик тривалої втрати довіри навіть у разі технічного відновлення систем. Наприклад, сама загроза оприлюднення даних про пожертви, приватні звернення до священнослужителів або внутрішні конфлікти може завдати громаді більшої шкоди, ніж тимчасове блокування доступу до файлів.

Цифрові платформи також є середовищем для транзакційних атак: фішингових сторінок пожертв, підробних оголошень про збір коштів, фейкових акаунтів служителів і клонів офіційних сторінок громад. У звіті NCSC про фішинг показано, що зловмисники активно використовують різні канали доставки від email і SMS до пошукової реклами та підробних сайтів і доменів, а також експлуатують довіру до відомих брендів і звичних сценаріїв взаємодії [27, с. 4–7].

У релігійній сфері брендом часто виступає не корпорація, а авторитет конкретної громади чи лідера, тому компрометація або імітація такого бренду безпосередньо б’є по довірі. Наприклад, фейкова сторінка парафії або благодійного проєкту може зовні повністю копіювати справжній ресурс і використовуватися для збору коштів, які фактично потрапляють до зловмисників.

Водночас кіберзагрози в релігійній сфері не обмежуються лише технічним або інформаційним виміром, а можуть ставати чинником ескалації конфліктів, провокацій і радикалізації. Провокації у такому середовищі мають прикладний характер: вони не стільки доводять правоту певної сторони, скільки запускають керовану соціальну реакцію страх, гнів, мобілізацію, яка руйнує довіру між громадами, делегітимізує державні інституції та підвищує конфліктність середовища. Релігійні теми в цьому випадку використовуються як емоційний мультиплікатор: символи, святині, моральні авторитети, ритуали та ідентичність здатні переводити політичні або соціальні суперечності в площину сакрального, де компроміс часто сприймається як зрада [31, с. 55; 42, с. 7]. Наприклад, після появи в мережі фейкового повідомлення про нібито наругу над святинею або образу віруючих навіть невелика локальна подія може швидко перетворитися на масштабний конфлікт між громадами.

Конфліктогенність найчастіше досягається через тригери з високою символічною вагою: наругу над місцем культу, пошкодження релігійної атрибутики, провокативні вкиди про нібито заборони чи переслідування, публічні образи групи за ознакою релігії або переконань. Такі дії можуть бути невеликими за масштабом, але дуже значними за резонансом, оскільки сама подія стає приводом для інформаційної хвилі та подальшої ланцюгової реакції взаємних звинувачень [42, с. 16; 33, с. 20]. Наприклад, відео з частковим або вирваним з контексту епізодом біля храму може бути подане як доказ системного насильства над певною конфесією, хоча реальні обставини інциденту були значно складнішими.

Окремим прискорювачем ескалації виступає мова ненависті й приниження, особливо коли вона нормалізується як право на думку або маскується під захист

традицій. ECRI визначає hate speech широко: як публічне приниження, розпалювання ненависті, стигматизацію, негативне стереотипування, погрози чи виправдання таких практик на ґрунті, зокрема, релігії або переконань [13, с. 2]. У релігійній сфері це особливо небезпечно, оскільки опонент перестає сприйматися як співгромадянин і перетворюється на морально дегуманізований об’єкт, щодо якого допускаються радикальні дії [13, с. 3].

Механізм переходу від провокації до радикалізації зазвичай складається з трьох взаємопов’язаних фаз: ініціації, інтерпретації та мобілізації. Критичним елементом тут є нав’язування такої інтерпретаційної рамки, в якій ситуація подається як екзистенційна загроза, а звичайні правові процедури оголошуються недостатніми або неефективними. Саме в цій точці з’являються заклики до самозахисту громади, блокувань, зривів заходів чи покарання винних, що переводить конфлікт у практичну площину [31, с. 50; 13, с. 3]. Наприклад, після серії емоційних дописів і взаємних обвинувачень у мережі окремі групи можуть почати закликати до фізичного “захисту храму”, чергувань, блокувань або недопущення представників іншої громади до релігійного об’єкта.

Для правозастосування та оцінки ризиків важливо розрізняти образливі висловлювання, дискримінаційне підбурювання та підбурювання до насильства або ворожнечі з реальною ймовірністю шкоди. Рамковою методикою для такого розмежування вважається шестикомпонентний тест Рабатського плану, який задає високий поріг для криміналізації й водночас орієнтує на виявлення випадків, де існує обґрунтована ймовірність того, що мова справді спровокує дію проти цільової групи [30, с. 1]. Для релігійної сфери це принципово, оскільки надмірно широкі заборони можуть бути використані проти меншин і критиків, тоді як ігнорування реального підбурювання створює простір для насильства [30, с. 1; 13, с. 3, 4].

Провокації в релігійному середовищі часто проєктуються як інцидент із повідомленням. OSCE/ODIHR у поясненні феномену злочинів ненависті підкреслює, що їхній ефект виходить за межі конкретної жертви: вони надсилають сигнал цілій спільноті та суспільству про неприйнятність групи, стимулюють потенційних правопорушників і можуть фрагментувати соціальну тканину [33, с.

20]. Така сама логіка працює і для псевдоінцидентів інсценувань або навмисно роздмуханих епізодів, коли навіть у разі подальшого спростування фактів первинний емоційний ефект уже досягнуто [33, с. 20; 42, с. 18]. Наприклад, навіть неправдива новина про напад на представників певної конфесії може встигнути спровокувати хвилю агресивних реакцій раніше, ніж буде офіційно спростована.

Другою віссю ескалації є конкуренція за простір і символи: храми, кладовища, пам'ятні місця, реліквії, публічні ритуали. Саме ці об'єкти є м'якими цілями, оскільки вони відкриті за своєю природою, мають передбачувані години проведення подій, збирають значну кількість людей і несуть символічний зміст. План дій ООН щодо захисту релігійних об'єктів прямо фіксує проблему балансу між посиленням протоколів безпеки та збереженням відкритого характеру релігійних місць [42, с. 16]. Гібридний вплив використовує цю дилему таким чином, що посилення охорони може подаватися як тиск на віру, а її недостатність як нездатність держави захистити громадян, що знову підживлює недовіру [42, с. 16; 31, с. 63]. Наприклад, конфлікт довкола доступу до храму, проведення богослужіння або користування релігійною спорудою легко перетворюється на символічний привід для ширшого суспільного протистояння.

Третьою віссю є організаційна радикалізація, коли конфлікт підштовхується не лише індивідуальними емоціями, а й груповими структурами: появою охоронних дружин, ініціативних комітетів, парамілітарних символів, внутрішніх списків ворогів, а також спробами силового контролю за подіями. За таких умов навіть незначні інциденти можуть призводити до швидкої ескалації, оскільки вже існує готова інфраструктура мобілізації. OSCE/ODIHR у рекомендаціях наголошує на обов'язку релігійних спільнот і лідерів проявляти належну пильність, щоб не допустити дрейфу до нетерпимості, ворожості або насильства, а також оперативно й публічно дистанціюватися від підбурювання ненависті [31, с. 55; 31, с. 50].

В умовах гібридних загроз особливу роль відіграє реакція публічних авторитетів політичних, релігійних і громадських лідерів, оскільки саме вони здатні або гасити ескалацію, або прискорювати її. ECRI прямо підкреслює підвищену відповідальність таких лідерів через їхній вплив на широку аудиторію

та ефективність протидії hate speech через counter-speech, яке демонструє руйнівний і неприйнятний характер підбурювання [13, с. 3]. Практично це означає, що в кризовий момент потрібна швидка публічна рамка: насильство є неприйнятним, інцидент розслідується, колективна відповідальність заборонена, громади перебувають під захистом. Інакше інформаційний вакуум заповнюється радикальними інтерпретаціями [13, с. 3; 30, с. 1].

Окремий ризик становить інформаційне замикання групи, коли зовнішні джерела оголошуються ворожими, а всередині формується єдина версія подій. Такий стан створює сприятливий ґрунт для повторюваних провокацій: кожен наступний інцидент підкріплює попередній, а будь-які спростування інтерпретуються як частина змови. Для руйнування цього циклу потрібні інструменти прозорого кризового управління: швидка верифікація факту, зрозумілий для громад перебіг розслідування, захист свідків і місць культу, а також окремі засоби комунікації з релігійними лідерами та громадами [42, с. 18, 19; 31, с. 51]. Наприклад, якщо після інциденту громада отримує лише чутки й емоційні дописи, а не зрозуміле офіційне пояснення, це значно підвищує ризик подальшого радикального розвитку ситуації.

План дій ООН містить практичні антиескалаційні заходи, які добре узгоджуються з логікою протидії провокаціям: регулярні оцінки ризиків щодо загроз релігійним об’єктам, визначення особливо вразливих місць, створення систем раннього попередження, тренінги для громад щодо виявлення загроз і взаємодії з правоохоронцями, побудова довіри та регулярний обмін інформацією між владою й релігійними лідерами [42, с. 18, 19]. У гібридному контексті це працює як зменшення ефекту раптовості та зниження ймовірності панічної реакції, яку зазвичай і прагне спровокувати противник [42, с. 18; 33, с. 20].

Нарешті, радикалізація часто має легалізаційний компонент: група шукає моральне й правове виправдання насильству через нібито бездіяльність держави. Тут важливою є демонстрація невідворотності правової реакції на злочини ненависті та на насильницькі інциденти в релігійному середовищі. OSCE/ODIHR показує, що саме повідомлювальний ефект таких злочинів вимагає спеціальної

уваги держави, оскільки шкода стосується не лише жертви, а й суспільної згуртованості [33, с. 20, 31]. Практичний висновок полягає в тому, що фіксація мотиву упередженості, коректна кваліфікація, облік і публічна комунікація результатів без стигматизації груп знижують простір для маніпуляцій та формують превентивний ефект [33, с. 46; 31, с. 63].

Управління ризиками в такому середовищі неможливе без розуміння того, що кіберінцидент є не ізольованою технічною подією, а частиною ширшої операційної логіки. Саме тому доцільно використовувати рамкові підходи до кіберризику, де кібербезпека пов'язується з управлінням ризиками організації та її місією. NIST CSF 2.0 вводить функцію GOVERN як ядро, яке формує стратегію, очікування, політики та контроль виконання, і прямо пов'язує її з іншими функціями для життєвого циклу інцидентів [28, с. 7–9]. Для релігійних організацій це означає, що навіть мінімальний рівень формалізації, зокрема визначення відповідальних за сторінки, процедури відновлення доступу, наявність резервних копій та перевірка термінових запитів на кошти, уже є елементом протидії гібридним загрозам.

Отже, кіберзагрози в релігійній сфері охоплюють не лише технічні атаки на цифрову інфраструктуру, а й використання платформ, даних, ботів, провокацій і конфліктних сценаріїв для підриву довіри, ескалації напруження та дестабілізації середовища. Їхня особливість полягає в поєднанні технічних інструментів із психологічними, інформаційними та символічними механізмами впливу. Саме тому кіберкомпонент у релігійній сфері слід розглядати як одну з ключових форм реалізації сучасних гібридних загроз.

Висновок до розділу 2. У релігійній сфері гібридні загрози реалізуються не через один окремий інструмент, а через поєднання кількох взаємопов'язаних впливів, які підсилюють один одного. Найпомітнішими серед них є дезінформація, пропаганда, мережеві операції та кіберзагрози. Особливу роль відіграє дезінформаційний вплив, коли події навмисно подаються у викривленому вигляді, релігійна ідентичність використовується для поділу на «своїх» і «чужих», а окремі конфлікти перетворюються на символічно загострені теми. Не менш важливими є

кадрові, фінансові та організаційні залежності, через які зовнішній вплив може тривалий час залишатися малопомітним, але поступово змінювати внутрішнє середовище релігійних організацій.

Кіберкомпонент і провокації додатково посилюють загальну небезпеку таких загроз. Технічні атаки, витоки даних, злам акаунтів і маніпуляції на цифрових платформах можуть використовуватися не лише для порушення роботи, а й для тиску, дискредитації та підвищення напруги між громадами. Водночас складність становить те, що в релігійній сфері не завжди легко відрізнити легітимну діяльність від керованого зовнішнього впливу, а високий рівень конфліктогенності знижує поріг ескалації. Саме тому протидія потребує постійного моніторингу, уважного аналізу зв’язків між подіями, інформаційними хвилями й акторами, а також заздалегідь підготовлених механізмів реагування у правовій, комунікаційній та цифровій площинах.

Розділ 3. Механізми протидії гібридним загрозам у релігійній сфері

3.1. Державна політика та міжвідомча координація: превенція, реагування, стратегічні комунікації

Державна протидія гібридним загрозам у релігійній сфері має будуватися як політика національної стійкості, де релігійні відносини розглядаються не лише як гуманітарний простір, а й як потенційний вектор дестабілізації через маніпуляцію ідентичністю, мережевий вплив, інформаційні та кібероперації. У такій логіці ключовим стає поєднання двох режимів: режиму гарантування свободи совісті та режиму захисту національної безпеки. Саме тому державна політика не може зводитися до реактивних заборон або точкових дій окремих органів. Вона має бути системою цілей, повноважень, процедур та інструментів, що працюють узгоджено в секторі безпеки і оборони та в гуманітарному блоці державного управління, із демократичним цивільним контролем і чіткими правовими межами [5]. Український досвід останніх років показав, що релігійна тематика може використовуватися не лише як гуманітарне чи світоглядне питання, а і як інструмент політичної мобілізації, зовнішнього впливу та інформаційної дестабілізації, тому підхід до неї поступово набуває виразного безпекового виміру [4].

У сучасному розумінні гібридні загрози поєднують різні засоби впливу і діють нижче порога формальної війни, використовуючи інформаційні кампанії, політичні та економічні важелі, кібератаки, агентурні мережі та інструменти соціальної поляризації. НАТО прямо фіксує, що гібридні виклики є багатовимірними і спрямованими на уразливості держав і суспільств, а відповідь має спиратися на стійкість і взаємодію цивільних та військових інструментів, включно з підтримкою союзників у разі потреби [25]. Це означає, що для релігійної сфери як чутливої до символів, наративів і довіри потрібні не «одноразові кампанії», а сталі міжвідомчі механізми раннього виявлення, реагування і відновлення.

Правова рамка є основою легітимності протидії. Будь-які обмежувальні або втручальні заходи у релігійній сфері мають бути прив’язані до закону, визначених процедур, належного доказування та можливості судового контролю. Показовим є те, що українське законодавство останніх років вводить спеціальні інструменти реагування на ризики афілійованості релігійних організацій з іноземними структурами, діяльність яких в Україні забороняється, і передбачає процедурні кроки, включно з рішеннями уповноваженого органу та подальшими правовими наслідками [4]. Така модель демонструє підхід «безпека через право»: держава визначає критерії ризику, фіксує компетенцію органів виконавчої влади і закріплює механізми, які можуть бути перевірені в правовому полі. Конкретним прикладом цього є ухвалення Закону України «Про захист конституційного ладу у сфері діяльності релігійних організацій» від 20.08.2024 № 3894-IX, який прямо запровадив спеціальні правові механізми щодо організацій, пов’язаних із центрами впливу держави-агресора [4].

Стратегічний рівень політики задають документи, які формалізують пріоритети протидії дезінформації та ворожим впливам і визначають роль стратегічних та кризових комунікацій. У Стратегії інформаційної безпеки України стратегічні комунікації трактуються як скоординоване і належне використання комунікативних можливостей держави, а кризові комунікації як комплекс заходів у відповідь на кризу із залученням уповноважених суб’єктів [7]. Для релігійної сфери це має практичний наслідок: держава повинна мати не «позицію за фактом скандалу», а підготовлені механізми, меседжі, алгоритми публічного реагування та пояснення рішень, які мінімізують можливість інформаційної ескалації. Практичним прикладом інституціоналізації такого підходу стало введення в дію Стратегії інформаційної безпеки Указом Президента України від 28.12.2021 № 685/2021 [7].

Інституційно важливим елементом міжвідомчої координації в інформаційній площині є Центр протидії дезінформації при РНБО України. Його функції включають аналіз і протидію дезінформації та деструктивним інформаційним впливам, розроблення пропозицій щодо підвищення ефективності заходів протидії,

а також координаційну взаємодію з органами державної влади та іншими суб'єктами [2]. Для релігійної сфери це означає можливість створення постійного «контруруху» до ворожих псевдонаративів: виявлення кампаній з маніпуляцією конфесійною ідентичністю, синхронізація позицій державних органів, підтримка фактчекінгу, підготовка інформаційних спростувань і попереджень про провокації. Конкретним кроком у цьому напрямі стало створення Центру протидії дезінформації Указом Президента України від 19.03.2021 № 187/2021 [2], що дало державі окремий інституційний механізм для реагування на інформаційні операції, у тому числі на ті, що можуть зачіпати релігійну тематику.

Однак інформаційна координація сама по собі не вирішує проблеми, якщо немає секторального провайдера політики у сфері релігії, здатного переводити аналітику у правові та управлінські дії. Таким провайдером є Державна служба України з етнополітики та свободи совісті (ДЕСС), яка визначена як центральний орган виконавчої влади, що забезпечує формування та реалізує державну політику у сфері релігії, а також здійснює контроль за додержанням законодавства про свободу совісті та релігійні організації в межах повноважень [3]. У контексті гібридних загроз ДЕСС має бути інтегрована у міжвідомчі контури як «власник процесу» у сфері релігії: від формування регуляторних рішень і консультацій з релігійними середовищами до участі у кризових протоколах та взаємодії з безпековими структурами.

Окремо варто підкреслити, що регуляторні повноваження ДЕСС розширюються інструментами, які безпосередньо адресують ризики гібридного впливу через інституційну залежність. Положення про ДЕСС передбачає, зокрема, проведення досліджень щодо наявності ознак афілійованості релігійної організації з іноземною релігійною організацією, діяльність якої в Україні заборонена, а також розгляд питання підтвердження фактів використання релігійної організації для пропаганди ідеології «русского міра» [3]. На практиці це задає державі механізм «управління ризиком» у релігійній сфері, який має працювати не ситуативно, а процедурно, з доказовою базою, визначеними строками, порядком повідомлення і подальшими юридичними наслідками. Саме в цьому і полягає конкретизація

державної політики: від загального декларування загроз до створення спеціального адміністративного механізму їх оцінки та фіксації [3].

Щоб міжвідомча координація була реальною, а не декларативною, вона має опиратися на єдиний контур ситуаційної обізнаності та обміну даними. Європейський підхід у сфері протидії гібридним загрозам робить акцент саме на підвищенні «situational awareness» та інтеграції інформації між інституціями, включно з аналітичними осередками і координаційними механізмами [15]. Для України це означає потребу у спільному інформаційному середовищі принаймні для ключових суб'єктів: РНБО (включно з ЦПД), ДЕСС, СБУ та кібербезпекової вертикалі, а також профільних міністерств. У релігійній сфері дані для такого контуру включатимуть індикатори ескалації (конфліктні події, сплески дезінформації), індикатори мережевого впливу (координація меседжів, джерела фінансування, організаційні зв'язки) та індикатори кіберризиків (фішинг, витоки, атаки на ресурси спільнот). У практичному вимірі це означає, що різкі інформаційні хвилі навколо релігійної тематики, однотипні публікації на різних платформах або паралельні локальні конфлікти мають розглядатися не ізольовано, а як можливі елементи єдиного сценарію впливу [15].

Кіберскладова у релігійній сфері має подвійний характер: це захист цифрових ресурсів держави та суспільства від втручань, самих релігійних організацій як соціальної інфраструктури (сайти, засоби комунікації, бази даних, пожертви, системи доступу). Організаційним ядром координації у сфері кібербезпеки виступає Національний координаційний центр кібербезпеки, утворений при РНБО України [8]. Його поява та статус підкреслюють, що кіберзагрози не можуть розглядатися як «технічна проблема IT-відділу»; це питання координації на рівні державної політики. Для релігійної сфери це створює можливість підключення до державних протоколів кіберреагування, розроблення рекомендацій для релігійних організацій та включення їх у підхід «стійкість через мінімальні стандарти захисту». Конкретним прикладом інституційного оформлення такого підходу стало введення в дію рішення РНБО України від 27 січня 2016 року, яким було створено НКЦК [8].

На стратегічному рівні Стратегія кібербезпеки України фіксує необхідність розвитку національної системи кіберзахисту, підвищення стійкості і координації, а також планування і здійснення заходів реагування на кіберінциденти у взаємодії суб'єктів [6]. У практичній площині це має трансформуватися у міжвідомчі «мости» між гуманітарним блоком (релігійна політика) і кіберблоком: ДЕСС має мати контактну рамку з координаційними структурами кібербезпеки для інцидентів, що зачіпають релігійні спільноти, а ЦПД має отримувати кіберіндикатори як частину загальної картини гібридної операції. Інакше держава реагує фрагментарно: окремо «спростовує наратив», окремо «гасить інцидент», але не бачить цілісної операції. Для релігійної сфери це особливо важливо, оскільки сучасні громади активно використовують сторінки у соціальних мережах, месенджери, онлайн-збори пожертв і цифрові бази контактів, а отже можуть ставати об'єктом не лише інформаційних, а й кіберінцидентів [6].

Управлінська конструкція протидії в релігійній сфері повинна мати чітко визначені рівні: стратегічний (цілі, принципи, рамки), оперативний (постійний моніторинг і координація), тактичний (реагування на інциденти). На стратегічному рівні ядро формує система національної безпеки з її базовими принципами і розподілом повноважень [5]. На оперативному рівні доцільною є постійна міжвідомча група (або координаційний режим) за напрямом «гібридні загрози в релігійній сфері» з опорою на ЦПД як аналітично-координаційний вузол і ДЕСС як секторальний регулятор. На тактичному рівні потрібні стандартизовані «кризові протоколи»: хто піднімає тривогу, хто підтверджує факт, хто комунікує, хто забезпечує безпеку об'єктів, хто взаємодіє з громадами. Відсутність протоколів породжує головний ризик гібридних операцій керовану невизначеність і хаос, у якому противник нав'язує інтерпретацію події.

Превенція в межах державної політики має починатися з картування вразливостей та визначення індикаторів раннього попередження. Це не «академічна вправа», а управлінська основа: без неї координація перетворюється на обмін загальними фразами. Стратегія інформаційної безпеки, фіксуючи значення стратегічних і кризових комунікацій, фактично задає вимогу до

державних інституцій діяти на випередження у питаннях дезінформації та деструктивних впливів [7]. У релігійній сфері превенція включає: регулярний моніторинг інформаційного поля щодо конфесійних тем; оцінку ризиків конфліктогенності в регіонах; аналіз зовнішніх механізмів впливу; мінімальні стандарти кібергігієни для релігійних організацій, що мають значну аудиторію; навчання спікерів і посадових осіб принципам кризового реагування. Превенція також передбачає «зв'язки довіри» швидкий зв’язок держави з представниками релігійних середовищ для деескалації та верифікації інформації. Саме відсутність таких механізмів створює умови, за яких чутки, емоційні публікації або провокаційні вкиди починають виконувати роль основного джерела інформації для громади.

Реагування, на відміну від превенції, завжди відбувається в умовах дефіциту часу, тому воно має спиратися на заздалегідь визначені механізми. НАТО у своїх підходах наголошує на ролі стійкості та готовності держав, підкреслюючи, що первинна відповідальність за реагування лежить на державі, а взаємодія та підтримка можуть посилювати можливості у протидії гібридним діям [25]. У релігійній сфері реагування може включати дуже різні сценарії: від провокацій навколо культових споруд і «вкидів» про нібито насильство чи «гоніння» до витоків даних громад і таргетованих кампаній із розпалювання ненависті. Саме тому міжвідомча взаємодія має бути сценарною: під кожен тип інциденту визначається ведучий орган, набір дій, комунікаційна лінія і критерії завершення кризи. Наприклад, у випадку інформаційного вкиду про нібито «захоплення храму» або «силове переслідування віруючих» важливо не лише перевірити факт, а й одразу визначити, хто комунікує позицію держави, хто забезпечує порядок на місці та хто працює з місцевою громадою для недопущення ескалації.

Стратегічні комунікації у протидії гібридним загрозам не є «доповненням», а інструментом управління наслідками і ризиками. Практика НАТО StratCom CoE підкреслює, що у гібридному середовищі вплив здійснюється через поєднання інструментів і цілеспрямоване використання інформаційного простору, а стратегічні комунікації покликані забезпечувати узгодженість і ефективність

відповіді [26, с. 4, 8]. Для релігійної сфери це означає, що державі потрібні не лише спростування, а керована рамка пояснення: що саме сталося, які факти підтверджені, які дії робить держава, які права гарантуються, де проходять межі законності, які запобіжники діють проти зловживань. Комунікація має бути єдиною за змістом (міжвідомча узгодженість) і диференційованою за аудиторіями (віряни, місцеві громади, медіа, міжнародні партнери). Саме у цьому полягає практичне значення стратегічних комунікацій: не просто відповісти на вкид, а не дати противнику закріпити потрібну йому інтерпретацію події [26, с. 4, 8].

Окремий блок державної політики інституційне «закріплення результату» після кризи. Гібридні операції часто повторюються, тестуючи систему на стійкість і помилки. Тому після кожного інциденту необхідний міжвідомчий розбір: які індикатори спрацювали, де був провал у координації, які рішення були надмірними або недостатніми, чи була належна комунікація, які прогалини в правовому регулюванні проявилися. Цей цикл навчання відповідає логіці державної політики як безперервного процесу, а не як «кампанії». Законодавчі рамки національної безпеки задають загальні принципи організації сектору та підходи до цивільного контролю, що дозволяє перетворювати уроки криз у вдосконалення процедур і підзвітності [5].

У релігійній сфері особливе значення має запобігання вторинним ефектам державних рішень, які противник може використати для ескалації. Наприклад, правові механізми щодо афілійованості та пропаганди «русского міра» можуть ставати мішенню для зовнішніх кампаній, які намагаються подати законні процедури як «репресії». Тому державна політика має поєднувати юридичну роботу з інформаційною: пояснювати критерії і процедури, підкреслювати можливість оскарження, демонструвати доказову базу у межах допустимого. Законодавча конструкція, що визначає критерії афілійованості і передбачає рішення уповноваженого органу та повідомлення зацікавлених сторін, створює основу для такого пояснення, якщо вона правильно «перекладена» на мову публічної комунікації [4].

Отже, державна політика і міжвідомча координація у протидії гібридним загрозам у релігійній сфері мають спиратися на чотири взаємопов'язані опори. Перша правова визначеність і процедурність, що забезпечує легітимність і судовий контроль [4]. Друга секторальний провайдер політики у сфері релігії (ДЕСС), інтегрований у безпекову координацію [3]. Третя інституційна координація інформаційної протидії (ЦПД при РНБО) і стратегічні комунікації як управлінський інструмент [2]. Четверта кіберкоординація і стійкість цифрового середовища, що забезпечується на рівні державної архітектури кібербезпеки [8]. Усі чотири опори мають працювати синхронно, інакше держава буде програвати в «швидкості циклу» гібридним операціям, які завжди комбінують впливи та експлуатують розриви між відомствами.

3.2. Роль релігійних організацій і громадянського суспільства: саморегуляція, медіаграмотність, діалог

Релігійні організації та інститути громадянського суспільства є базовим рівнем суспільної стійкості до гібридних впливів, оскільки саме через них проходять щоденні комунікації, локальні мережі довіри, символічні маркери ідентичності та практики взаємодопомоги. У гібридному середовищі противник прагне не лише поширити окремі фейки, а створити довготривалі розломи: «свій/чужий», «правильна/неправильна віра», «патріоти/зрадники», підштовхуючи громади до саморуйнівної конфліктності. Тому ефективна протидія не може бути суто державною функцією: потрібна взаємодія "whole-of-society" участь громад, НУО, медіа та релігійних інституцій у підвищенні стійкості, що узгоджується з підходом ЄС до протидії гібридним загрозам і фокусується на поєднанні державних та суспільних інструментів [15].

У національній рамці безпеки така роль недержавних акторів логічно випливає з концепції національної безпеки як системи, що охоплює не лише силовий компонент, а й суспільну стійкість, захист інтересів людини і держави та організовану взаємодію суб'єктів безпеки. У практичному вимірі це означає, що

релігійні організації та громадянське суспільство виступають “партнерами стійкості”: вони швидше бачать локальні напруження, краще розуміють внутрішні механізми довіри та здатні швидко нейтралізувати провокації через авторитетні внутрішні мережі [5].

Саморегуляція релігійних організацій у контексті гібридних загроз має розглядатися як запобіжний механізм проти інфільтрації, неформального контролю та токсичних залежностей. Йдеться про внутрішні правила прозорості пожертв і зовнішнього фінансування, процедурні запобіжники конфлікту інтересів, стандарти публічної комунікації, дисциплінарні реакції на мову ненависті, а також мінімальні вимоги до управління ризиками (комплаєнс). В українських умовах додатковий стимул до такої “процедурності” створює спеціальне правове регулювання щодо захисту конституційного ладу у сфері діяльності релігійних організацій: навіть за нейтральності держави до конфесій, питання організаційних зв’язків, підлеглості чи зовнішнього визначального впливу набувають безпекового значення і потребують документованої прозорості всередині самої організації [4].

Принципово важливо, щоб саморегуляція не перетворювалася на “самоцензуру” або інструмент внутрішніх розправ. Її ціль зменшити уразливості, якими користується противник: непрозорі фінансові потоки, залежність від зовнішніх центрів, керована кадрова політика, вразливі комунікаційні механізми. Саме тому саморегуляція має бути формалізована (положення, протоколи, політики), підкріплена аудитом і орієнтована на захист прав та безпеки членів громади, а не на конфесійне протиставлення. Така логіка узгоджується з більш широким підходом держави до балансу свободи і безпеки, де правова визначеність і процедурність є способом мінімізувати зловживання та інформаційні маніпуляції навколо “переслідувань” [5; 4].

Громадянське суспільство в цьому блоці виконує функцію «підсилювача стандартів»: воно може надавати інструменти прозорості (шаблони політик, методики оцінки ризиків, тренінги комплаєнсу), допомагати в медіації конфліктів та забезпечувати незалежний моніторинг інформаційних провокацій. У гібридному середовищі особливе значення мають горизонтальні мережі довіри між громадами,

НУО і місцевими лідерами, адже вони зменшують час реакції на провокацію та знижують ймовірність “самозаймання” конфлікту через чутки. Уся ця діяльність є елементом суспільної стійкості, яку підкреслюють і підходи НАТО щодо протидії гібридним загрозам через готовність, резильєнтність і взаємодію різних секторів [25].

Медіаграмотність для релігійних організацій і громадянського суспільства є не додатковою опцією, а інструментом зниження системних ризиків. Стратегія інформаційної безпеки України прямо закріплює значення стратегічних і кризових комунікацій, протидії деструктивним інформаційним впливам та розвитку спроможностей, які зменшують ефект дезінформаційних кампаній [7]. У релігійній сфері медіаграмотність має бути адаптована до типових сценаріїв маніпуляції: “вкиди” про нібито заборони чи «гоніння», штучне загострення навколо культових споруд, емоційні підміни понять, провокативні фейкові «свідчення» та псевдодокументи. Практичний мінімум внутрішні правила поширення чутливої інформації (перевірка першоджерела, підтвердження з двох незалежних джерел, відмова від репостів «у паніці», фіксація фактів до оцінок).

Важливо розділяти просвітницький та кризовий контури. Просвітницький контур це регулярні заняття для духовенства та активу громад, формування навички “думати повільніше, ніж поширювати”, підготовка локальних довідок про типові маніпуляції та правила реагування. Кризовий контур це готові алгоритми на випадок інциденту: хто уповноважений коментувати, як швидко зібрати факти, як повідомити людей без ескалації і як протидіяти хвилі фейків. Така логіка безпосередньо підтримує вимогу стратегічних і кризових комунікацій як державного інструменту, але реалізується на рівні громад через дисципліну повідомлень і взаємодію з партнерами [7].

Співпраця релігійних організацій та громадянського суспільства з державними інституціями у сфері протидії дезінформації є доцільною тоді, коли вона процедурно врегульована і зберігає конфесійну нейтральність. Центр протидії дезінформації при РНБО створює інституційну основу для координаційних та аналітичних функцій, що можуть бути корисні громадам у вигляді попереджень

про інформаційні операції, виявлення наративів і допомоги у верифікації [2]. У релігійній сфері практична модель співпраці може включати: (1) механізм повідомлення від громад і НУО про підозрілі інформаційні кампанії; (2) обмін узагальненими індикаторами (без розкриття чутливих персональних даних); (3) підтримку фактчекінгу; (4) підготовку коротких роз'яснень, які громади можуть поширювати внутрішніми засобами без "перегріву" теми.

Окремим ресурсом підвищення ефективності є інструментарій стратегічних комунікацій як управління довірою та інтерпретаціями. У гібридному середовищі часто вирішальним стає не сам інцидент, а рамка його пояснення і швидкість формування "першої версії", яка закріплюється в масовій свідомості. Саме тому стратегічні комунікації мають сенс на рівні громад: це дисципліна повідомлень, узгодженість ролей, робота з аудиторіями та використання "надійних голосів" для деескалації. Відповідні практичні орієнтири стратегічних комунікацій у контексті гібридних загроз систематизує інструментарій НАТО StratCom CoE, який підкреслює необхідність узгодженості, розуміння середовища та цілеспрямованого використання комунікаційних можливостей [26 с. 4, 8].

Діалог у релігійній сфері виконує подвійну функцію: він зменшує конфліктогенність і поляризацію, він створює механізми швидкої деескалації та верифікації під час провокацій. Для гібридного противника найцінніший результат розриви всередині суспільства; тому міжконфесійні платформи, місцеві ради церков, медіаційні ініціативи НУО та практики "контактних груп" у громадах мають стратегічне значення. На рівні державної політики важливо, щоб діалог не був "разовою подією", а підтримувався інституційно: через сталі комунікаційні механізми та робочі процедури взаємодії з уповноваженим органом у сфері свободи совісті. Саме для цього існує профільний державний інститут, який формує та реалізує політику в релігійній сфері і може виступати координатором взаємодії в межах компетенції [3].

Цифровий вимір роботи релігійних організацій істотно посилює ризики, але одночасно відкриває швидкі інструменти підвищення стійкості. Державна архітектура кібербезпеки, зокрема через інституційне закріплення НКЦК та

стратегічні документи, задає рамку координації й необхідність підвищення кіберстійкості суб'єктів [8; 6]. На рівні громад це має бути реалізовано через мінімальні стандарти кібергігієни: двофакторна автентифікація для адміністраторів сторінок, розмежування доступів, резервні копії, протоколи на випадок зламу, правила роботи з базами контактів і пожертвами, безпечні засоби внутрішньої комунікації. Роль НУО тут практична: вони можуть забезпечити тренінги, типові політики, аудит базових налаштувань, а також комунікаційну підтримку під час кіберінциденту, щоб громада не стала жертвою паніки або вторинних маніпуляцій.

У підсумку, ефективна протидія гібридним загрозам у релігійній сфері потребує партнерської моделі, де держава забезпечує правові рамки і координацію, а релігійні організації та громадянське суспільство закривають "польовий" рівень стійкості. Саморегуляція мінімізує організаційні вразливості й токсичні залежності [4]. Медіаграмотність зменшує ефект дезінформації і робить громади менш реактивними до провокацій [7]. Діалог і стратегічні комунікації перетворюють розрізнені реакції на керований процес деескалації та збереження довіри [26]. В умовах гібридного протиборства саме така взаємодія дозволяє зменшити потенціал поляризації й забезпечити баланс свободи совісті та безпеки, що відповідає загальним підходам ЄС і НАТО до протидії гібридним загрозам [15; 25].

3.3. Вітчизняний та зарубіжний досвід протидії гібридним загрозам в релігійній сфері

Інформаційна та кібербезпека в релігійній сфері є взаємопов'язаними, оскільки гібридні загрози реалізуються через комбінації інструментів: інформаційний вплив формує мотивацію і поведінку аудиторій, а кіберкомпонент забезпечує доступ, масштабування, а інколи й компрометацію довіри через злам засобів комунікації. Концептуальні моделі гібридних загроз підкреслюють багатодоменність і «зв'язування» різних засобів впливу в єдиний сценарій, у якому результат досягається не одним інструментом, а їхнім поєднанням у потрібний момент [20 с. 26, 34, 35]. У релігійній сфері це проявляється як одночасні «вкиди»

про нібито утиски чи «зраду», синхронізовані з атаками на сторінки громад, витоками персональних даних вірян або компрометацією внутрішніх чатів, що підсилює паніку і провокує конфліктогенність.

Показовим прикладом для України є ситуації, коли навколо переходів релігійних громад або змін юрисдикції в інформаційному просторі навмисно поширювалися емоційно загострені повідомлення про «захоплення храмів», «переслідування віруючих» чи «силовий тиск», хоча реальна ситуація часто була значно складнішою або юридично врегульованою. У таких випадках саме поєднання інформаційного тиску, маніпулятивних інтерпретацій та цифрового поширення контенту створювало ефект гібридної ескалації.

Моніторинг у такій ситуації має будуватися як раннє виявлення індикаторів гібридної активності: аномальні інформаційні хвилі, повторювані наративи, координовані «скарги» і масові звернення, синхронізація повідомлень між різними платформами, появи псевдоавторитетних «джерел» або підроблених документів. Європейський підхід до протидії гібридним загрозам акцентує ситуаційну обізнаність, обмін інформацією та координацію як передумову ефективної відповіді, що прямо перекладається на потребу системного збору сигналів із відкритих джерел, локальних спільнот і профільних інституцій [15]. Для релігійних організацій це означає, що моніторинг не може бути епізодичним реагуванням на окремий скандал, а має бути постійною функцією хоча б у мінімальному форматі, коли є відповідальний, регулярний огляд інформаційного поля, фіксація інцидентів і механізмів поширення.

Практика останніх років показала, що інформаційні хвилі навколо релігійної тематики часто активізуються не спонтанно, а синхронно з політичними або безпековими подіями. Саме тому вітчизняний досвід свідчить: навіть базовий моніторинг локальних спільнот, Telegram-каналів і сторінок у соціальних мережах дає змогу виявляти загрозу ще до переходу інформаційної атаки у фазу відкритого суспільного конфлікту.

Практична якість моніторингу суттєво зростає, коли організація застосовує стандартизовану мову опису інцидентів і противникових технік. Корисним

інструментом для цього є бази знань про тактики і техніки зловмисників, які дають уніфіковані категорії для опису спроб доступу, соціальної інженерії, викрадення облікових даних, впливових операцій та інших сценаріїв. У контексті захисту цифрових ресурсів релігійних спільнот така стандартизація полегшує фіксацію, аналіз і навчання персоналу: замість загальної формули «нас атакують» з'являються конкретні визначення фішинг, підміна акаунта, злам пошти, компрометація адміністратора, координація бот-мережі, що пришвидшує правильні рішення [50]. Це особливо важливо, коли громади співпрацюють із громадськими організаціями або державними структурами: однакова термінологія зменшує помилки й втрати часу під час ескалації інцидентів.

Фактчек у релігійній сфері має враховувати, що більшість гібридних повідомлень не є «чистою брехнею», а поєднують правдиві фрагменти з маніпулятивним контекстом, емоційною рамкою та підміною причинно-наслідкових зв'язків. Для побудови практики перевірки корисною є рамка «інформаційного безладу» (misinformation, disinformation, malinformation), яка дозволяє розрізняти ненавмисні помилки, умисні вкиди та шкідливе використання справжньої інформації, наприклад витоки приватних даних або вирвані з контексту цитати [3]. У релігійній площині malinformation часто стає ключовим інструментом: навіть правдивий факт, поданий як «доказ змови», може запускати ескалацію і насильницькі інтерпретації, якщо громада не має навички відділяти факт від інтерпретації.

Наприклад, у резонансних конфліктах навколо церковного майна, статусу окремих громад або висловлювань релігійних діячів у публічному просторі часто використовувалися реальні фото, документи чи уривки заяв, але подані у вирваному з контексту вигляді. Саме така часткова правдивість робить гібридні інформаційні впливи особливо переконливими для аудиторії.

Окремий різновид фактчек-завдань пов'язаний із маніпуляціями ідентичністю: противник «вшиває» політичні та ворожі меседжі у релігійні маркери, змушуючи людей реагувати не на аргументи, а на сигнал «свій/чужий». Дослідження щодо експлуатації соціальної ідентичності в дезінформації

показують, що саме ідентичнісні лінії розлому є найефективнішим важелем поляризації й довготривалого підриву довіри, бо вони працюють на рівні належності й моральної оцінки, а не перевірки фактів [22]. Відповідно, фактчек у релігійних спільнотах має включати не лише перевірку джерела, а й аналіз рамки: хто визначає «справжніх» і «несправжніх», які емоції нав'язуються, які групи демонізуються і яку поведінку це має спровокувати.

Правильна протидія дезінформації не повинна перетворюватися на обмеження свободи вираження або селективну цензуру, інакше це підриває легітимність самої відповіді й стає ресурсом для нових наративів про «гоніння». У цьому сенсі важливою є міжнародна позиція, що боротьба з фейками та пропагандою має узгоджуватися з правами людини, принципами пропорційності та прозорості, а не підмінюватися довільними заборонами [23]. Для релігійних організацій практичний висновок такий: під час спростувань слід уникати мови ворожнечі, не «приклеювати» ярлики до цілих груп і не публікувати персональні дані опонентів; натомість фокусуватися на перевірюваних фактах, джерелах і корекції інтерпретацій.

Стратегічні комунікації є операційним продовженням фактчеку: перевірити інформацію недостатньо, потрібно ще правильно і вчасно донести перевірений зміст, не підсилюючи провокацію. Практичні рекомендації з протидії гібридним впливам у комунікаціях наголошують на узгодженості повідомлень, розумінні аудиторій, швидкому реагуванні та плануванні кризової комунікації як окремої функції [26 с. 4, 8]. Для релігійної сфери це означає визначити «єдиний голос» на випадок інциденту, мати шаблони коротких повідомлень для громади, розділяти внутрішню комунікацію, щоб зняти паніку, і зовнішню, щоб не розкручувати конфлікт, а також не відповідати на кожен вкид однаково інколи ефективніша тактика пояснити своїм і не піарити провокатора.

Подібний підхід активно використовується і в зарубіжній практиці, зокрема в країнах Балтії, де протидія гібридним впливам будується не лише на спростуванні дезінформації, а й на швидкому інформуванні власної аудиторії через довірені

засоби комунікації. Це дозволяє знижувати ефект паніки та не давати провокаційним наративам закріпитися в інформаційному полі.

Організаційна архітектура інформаційної безпеки в Україні задає рамку координації та пріоритетів, у межах яких релігійні організації й громадянське суспільство можуть вибудовувати власні процеси. Стратегія інформаційної безпеки формалізує потребу підвищення стійкості до деструктивних інформаційних впливів, розвитку стратегічних і кризових комунікацій та інституційної спроможності протидії [7]. На рівні релігійних спільнот це має перетворюватися на конкретні процедури: регулярне навчання адміністраторів сторінок і модераторів чатів, правила перевірки «термінових» повідомлень, перелік надійних джерел, політика щодо провокативного контенту та механіка швидкого спростування.

Інституційним інструментом координації в цій сфері виступає Центр протидії дезінформації, який створює можливість систематизувати сигнали про інформаційні операції, формувати аналітичні продукти й підтримувати публічну комунікацію щодо інформаційних загроз [2]. Для релігійних організацій та НУО корисною є модель «двостороннього контуру»: громади передають узагальнені сигнали тип вкиду, платформа, тематика, часові піки, натомість отримують попередження про активні наративи й рекомендації щодо комунікації. Принципово важливо, щоб такий обмін не зводився до політичної лояльності, а будувався на процедурі, доказовості й мінімізації персональних даних.

Для України це особливо актуально в умовах війни, коли релігійна тематика може використовуватися як інструмент розколу суспільства або делегітимації державної політики. У таких умовах навіть окремі локальні інформаційні інциденти можуть штучно роздуватися до рівня загальнонаціональної конфліктної теми.

Кіберзагрози, які найбільш типово вражають організації з обмеженими ресурсами, а такими часто є місцеві релігійні громади, мають повторювану структуру: фішинг і компрометація пошти, крадіжка паролів адміністраторів сторінок, захоплення акаунтів у месенджерах, шкідливі вкладення, вимагання

(ransomware), витоки даних донорів та контактних баз. Загальноєвропейські огляди загроз систематизують ці ризики як пріоритетні для організацій, що активно використовують цифрові платформи, особливо в умовах криз і високої інформаційної напруги [14]. Для релігійних спільнот додатковою проблемою є «довіра за замовчуванням»: шахрайські повідомлення часто маскуються під волонтерські збори, церковні оголошення або «термінові прохання настоятеля», що робить соціальну інженерію особливо ефективною.

На практиці це може проявлятися у вигляді фейкових зборів «від імені парафії», підроблених повідомлень від священнослужителів або несанкціонованих публікацій у зламаних церковних акаунтах. Навіть одиничний такий інцидент здатний підірвати довіру всередині громади та створити підґрунтя для ширшої інформаційної атаки.

Емпіричні звіти з аналізу інцидентів підкреслюють, що ключовим вектором доступу в багатьох атаках залишаються людський фактор і зламані облікові дані, а не складні технічні «нульові дні». Для організацій рівня громад це означає прагматичний пріоритет: керування доступами, унікальні паролі, менеджери паролів, мінімізація прав, багатофакторна автентифікація, контроль поштових скриньок, сегментація доступу до фінансових інструментів, таких як онлайн-банкінг і платіжні сервіси, та резервні копії [43]. Такі заходи дають найкраще співвідношення ефекту і вартості та напряму зменшують ризик катастрофічного сценарію, коли зламано одразу всі критичні ресурси.

Проти фішингу як основного масового інструменту доцільно застосовувати поєднання організаційних і технічних кроків: маркування зовнішніх листів, заборона входу в критичні сервіси з невідомих пристроїв, короткі інструкції щодо перевірки посилань, внутрішній механізм для швидкого уточнення підозрілих повідомлень, а також регулярні вправи з симуляцією фішингу. Аналітичні огляди протифішингових інцидентів показують, що успіх атак часто забезпечується повторюваними шаблонами, такими як підробка доставки, «термінове підтвердження», фальшивий рахунок, фейковий скидання пароля, тому навчання й стандарти реакції суттєво зменшують результативність зловмисника [27]. У

релігійних громадах варто додатково вводити правило подвійного підтвердження для фінансових прохань: жодних платежів лише на підставі повідомлення в месенджері.

Для системного захисту інфраструктури корисно застосовувати рамкові моделі, які переводять безпеку з набору хаотичних дій у керований процес. NIST Cybersecurity Framework 2.0 пропонує логіку функцій ідентифікація, захист, виявлення, реагування, відновлення, яку можна адаптувати навіть у невеликих організаціях: описати активи, тобто акаунти, сайти, пожертви, бази контактів, визначити мінімальні контролі, налаштувати виявлення інцидентів, зокрема сповіщення про входи й журнали, а також мати план реагування та резервування [28]. Для релігійних організацій важливо, що ця логіка сумісна з партнерством: НУО або місцеві ІТ-волонтери можуть допомогти з інвентаризацією активів, базовими налаштуваннями і «пакетом мінімальної кібергігієни» без потреби великих бюджетів.

Окремо слід враховувати, що частина ризиків лежить на стороні платформ і регуляторних вимог до них. Digital Services Act створює більш жорсткі рамки відповідальності платформ за ризики поширення незаконного контенту та системні ризики, що має значення для кейсів координованих атак, бот-мереж і кампаній ненависті, спрямованих на релігійні групи [38]. Паралельно GDPR встановлює вимоги до захисту персональних даних, і в контексті релігійних організацій це критично: витоки списків вірян, донорів або учасників чутливих подій перетворюються на інструмент шантажу, стигматизації й провокацій, тобто мають не лише юридичні, а й безпекові наслідки [37]. Практичний висновок полягає в тому, що потрібно мінімізувати збирання даних «про запас», обмежувати доступ, визначати строки зберігання та мати сценарій дій у разі витоку.

Бот-активність і координована неавтентична поведінка є характерним механізмом масштабування гібридного впливу: вона створює ілюзію масової підтримки або обурення, «заливає» коментарі, стимулює емоційні реакції й підштовхує модераторів до помилок. Наукові огляди соціальних ботів показують, що автоматизовані акаунти можуть швидко посилювати видимість наративів і

втручатися в дискусії, змінюючи сприйняття «нормальності» позиції [18]. Для релігійних спільнот це означає потребу в модераційних правилах, фіксації хвиль підозрілої активності та використанні базових індикаторів, таких як однотипні акаунти, синхронні коментарі, повторювані тексти й аномальні часові піки, як підстави для посилення модерації й переходу на «повільніші» режими комунікації під час атаки.

Кризові протоколи мають охоплювати як інформаційні, так і кіберінциденти, бо на практиці вони часто відбуваються одночасно: злам сторінки громади використовується для публікації провокацій, а витік листування для «компрометуючих» добірок, які запускають конфлікт. Класична логіка реагування на кіберінциденти включає підготовку, виявлення й аналіз, стримування, ліквідацію наслідків і відновлення, а також післяінцидентну роботу з уроками й корекцією контролів [49]. Для релігійних організацій у практичному вигляді це має бути оформлено як короткий документ: ролі, хто вирішує, хто комунікує, хто відновлює доступи, «гарячі» контакти, список активів, правила доказовості, порядок зміни паролів і відсікання доступів, а також план резервного засобу повідомлень громаді на випадок захоплення основних сторінок.

Кризові протоколи інформаційної безпеки повинні додатково містити правила деескалації та межі допустимої риторики, особливо коли провокації спрямовані на розпалювання ворожнечі. Європейські стандарти протидії hate speech та підхід «порогового тесту» до підбурювання до ненависті задають орієнтир: критично оцінювати контекст, намір, позицію спікера, охоплення і ймовірність шкоди, щоб не допустити переходу від гострої дискусії до небезпечної ескалації [13; 30]. На практиці в громадах це означає, що під час атаки модерація має бути більш суворою, але процедурною; неприйнятними є заклики до насильства, дегуманізація і «колективна вина», а в публічних заявах слід фокусуватися на фактах, правових рамках і заспокоєнні аудиторій.

Нарешті, захист інфраструктури та протоколи реагування повинні враховувати й фізичний вимір безпеки, оскільки інформаційні кампанії можуть готувати ґрунт для нападів на культові споруди або провокацій біля релігійних

об’єктів. Міжнародні рекомендації щодо захисту релігійних місць підкреслюють важливість превенції, партнерства з місцевими спільнотами, оцінки ризиків та комунікації для забезпечення безпечного і мирного богослужіння [42]. В українських умовах це особливо актуально: комбіновані атаки можуть починатися з онлайн-розпалювання, продовжуватися офлайн-провокаціями, а завершуватися новою хвилею медійних маніпуляцій; тому інформаційна, кібер- і фізична компоненти протидії мають плануватися як єдина система.

Зарубіжний досвід протидії гібридним загрозам у гуманітарній площині показує, що вирішальним є не «сила відповіді», а якість стійкості системи. Найуспішніші підходи будуються як керований цикл: раннє виявлення, швидка координація, пропорційне реагування, відновлення і корекція правил за підсумками інциденту. У релігійній сфері це має особливе значення через високу чутливість ідентичності та ризик перетворення інформаційної хвилі на локальну конфліктну подію. У країнах, де протидія гібридним впливам стала системною практикою, релігійні організації розглядаються не лише як потенційна мішень, а як учасник суспільної резильєнтності, здатний підтримувати соціальну згуртованість і знижувати напруженість у кризові періоди.

Наприклад, у Фінляндії та Естонії стійкість до гібридних впливів посилюється через поєднання державної координації, інформаційної грамотності населення, міжсекторальної взаємодії та розвитку культури раннього реагування. Хоча ці практики не спрямовані виключно на релігійну сферу, вони є цінними саме тому, що дозволяють запобігати використанню будь-яких чутливих соціальних тем, у тому числі релігійних, як інструменту розколу.

Ключовою рисою міжнародних підходів є правова й процедурна визначеність. Там, де державна політика спирається на прозорі критерії ризику, чіткі процедури та передбачуваність рішень, у противника менше можливостей експлуатувати наративи про «переслідування» або «вибіркові утиски». Баланс свободи совісті й безпеки досягається не шляхом розширення дискреції, а через стандарти доказовості, пропорційності та відповідальності за рішення. Для України це означає потребу у стабільній практиці пояснення державних кроків мовою прав

і безпеки одночасно: не декларативно, а через зрозумілі причини, межі втручання і механізми контролю. Така передбачуваність знижує конфліктогенність і робить суспільство менш вразливим до маніпуляцій.

Узагальнюючи зарубіжні практики, можна стверджувати, що протидія гібридним загрозам у релігійній сфері ефективна тоді, коли будується на партнерській моделі взаємодії. Держава задає рамку, інструменти координації та підтримку спроможностей, громадянське суспільство забезпечує незалежний моніторинг і просвітницьку роботу, релігійні організації виступають інструментом стабілізації середовища, оскільки мають доступ до спільнот і здатні швидко знімати емоційні напруження. Однак партнерство працює лише за умови, що воно інституціоналізоване, тобто має регулярні механізми зв'язку, узгоджені протоколи, зрозумілу відповідальність і правила поводження з чутливою інформацією. Інакше воно перетворюється на формальність або на інструмент політичної конкуренції, що лише посилює вразливості.

Практичний сенс для України полягає в тому, щоб перевести реагування з режиму «кризового шуму» у режим керованих процедур. Релігійна сфера потребує простих, але дисциплінованих механізмів: визначених контактних осіб, швидкого внутрішнього підтвердження інформації, попередньо підготовлених шаблонів повідомлень для громади, а також правила, що саме вважається підтвердженим фактом і хто має право робити публічні заяви. Досвід інших країн підказує, що найчастіша помилка реагування на емоції аудиторії, коли організація починає публічно сперечатися з провокатором, відтворюючи його рамку. Значно ефективніше працює нейтральна фактична комунікація, спрямована на власну громаду, з мінімізацією конфронтаційної риторики і з акцентом на деескалацію.

Окремий напрям, який у міжнародних практиках розглядається як обов’язковий, з’єднання інформаційної безпеки з кібербезпекою. На операційному рівні гібридні дії часто реалізуються через комбінацію: інформаційний вкид створює паніку, а кіберінцидент забезпечує «доказ» або доступ до засобів комунікації. Тому релігійним організаціям потрібна не абстрактна цифрова обізнаність, а конкретний мінімум кіберстійкості: контроль доступів,

багатофакторний захист, резервні засоби зв'язку, базовий план дій при зламі акаунтів і витоку даних. У країнах, де такі стандарти працюють, їх роблять максимально доступними і адаптованими до малих організацій: короткі політики, зрозумілі інструкції, навчання на реальних сценаріях. Для України цінним є саме цей принцип зробити безпеку «побутовою дисципліною», а не окремим дорогим проєктом.

Додатково варто враховувати, що релігійні спільноти часто мають волонтерські й благодійні процеси, які містять фінансові та персональні дані, а отже стають привабливими для зловмисників. Міжнародні підходи в таких випадках орієнтуються на мінімізацію даних, обмеження доступу і чітке розділення ролей, щоб один компрометований акаунт не давав доступ до всіх систем одразу. Це важливо не лише з погляду кіберризиків, а й з погляду репутаційної безпеки: довіра до релігійних організацій є одним з головних ресурсів суспільної стійкості, і саме довіру найчастіше намагаються зруйнувати через інциденти, що демонструють «некомпетентність» або «нечесність».

Ще один висновок із зарубіжного досвіду полягає у тому, що деескалація є не менш важливою, ніж викриття. У релігійній сфері противник може прагнути не переконати, а розпалити. Тому ефективна протидія включає практики локальної медіації, підтримку майданчиків міжконфесійного спілкування, спільні соціальні ініціативи, які підсилюють горизонтальні зв’язки. У суспільствах, де такі зв’язки міцні, провокаціям важче «приклеїтися» до масової свідомості, бо у людей є довірені джерела перевірки реальності, а конфлікти не переходять у стадію взаємної демонізації.

У підсумку для України найбільш раціональним є підхід, що поєднує правову визначеність, інституційну координацію, практичні стандарти організаційної стійкості для релігійних спільнот і розвиток культури деескалації. Це не потребує одномоментних масштабних витрат, але потребує дисципліни і повторюваності. У гібридному середовищі виграє не той, хто реагує найжорсткіше, а той, хто має стабільні правила, здатність швидко підтвердити факти, зберегти довіру і не

допустити перетворення інформаційного інциденту на реальний конфлікт у суспільстві.

Висновок до розділу 3. Протидія гібридним загрозам у релігійній сфері має бути багаторівневою і поєднувати зусилля держави, релігійних організацій, громадянського суспільства та цифрових платформ. Найважливішими умовами її ефективності є превенція, раннє виявлення ризиків і підготовлене реагування. У цьому контексті особливе значення мають міжвідомча координація, стратегічні комунікації, правове реагування на основі доказів і дотримання принципів законності, необхідності та пропорційності. Не менш важливою є внутрішня стійкість самих релігійних організацій, яка залежить від прозорості управління, контролю фінансових і кадрових ризиків, наявності внутрішніх правил публічної комунікації та кризових протоколів.

Водночас практична протидія неможлива без інформаційної та кібербезпеки. Для релігійних громад і пов’язаних із ними структур важливими є постійний моніторинг інформаційного середовища, швидке спростування неправдивих повідомлень, передбачувані моделі кризових комунікацій, а також базові стандарти кібергігієни захист доступів, двофакторна автентифікація, резервні копії, навчання відповідальних осіб і готовність до відновлення після інциденту. Основними проблемами залишаються фрагментарність реагування, відсутність уніфікованих процедур і нестача довіри між учасниками взаємодії. Саме тому для України особливо важливими є формалізація індикаторів ризику, створення типових моделей взаємодії та розвиток програм підвищення стійкості у релігійній сфері.

Висновки

Гібридні загрози в релігійній сфері є складним і багаторівневим явищем, у якому поєднуються інформаційні, організаційні, фінансові, мережеві та цифрові інструменти впливу. Їхня небезпека полягає не лише в поширенні окремих неправдивих повідомлень чи провокацій, а в здатності поступово підривати довіру, загострювати внутрішні суперечності та перетворювати релігійне середовище на простір конфлікту. У цьому сенсі релігійна сфера є не другорядною, а однією з чутливих ділянок суспільного життя, через яку можна впливати на настрої, ідентичність і рівень суспільної згуртованості.

Релігійна сфера є вразливою до гібридного впливу тому, що поєднує символічний ресурс, моральний авторитет, мережі довіри та сталі форми комунікації всередині громад. Саме ці особливості можуть використовуватися як для підтримки стабільності, так і для маніпуляції. Якщо в середовищі вже існують суперечності, конкуренція, недовіра або правова невизначеність, зовнішній чи внутрішній деструктивний вплив отримує значно більше можливостей для посилення напруги. Тому релігійні організації можуть бути не лише об’єктом загроз, а й середовищем, через яке такі загрози поширюються або, навпаки, стримуються.

Найпоширенішими формами реалізації гібридних загроз у релігійній сфері є дезінформація, пропаганда, мережеві операції та кіберзагрози. Дезінформаційний вплив особливо ефективний тоді, коли він спирається на релігійну ідентичність, емоційні наративи, образ «своїх» і «чужих», а також на викривлене подання окремих подій як доказу ширшого переслідування, ворожості чи несправедливості. Мережеві операції, пов’язані з фінансуванням, кадровим впливом і створенням організаційних залежностей, є менш помітними, але часто довготривалішими за наслідками. Кіберзагрози доповнюють ці механізми, оскільки дають можливість зламувати канали комунікації, викрадати дані, створювати фейкові повідомлення від імені громад або підсилювати вже наявний конфлікт через цифрові платформи.

Окрему небезпеку становить те, що в релігійній сфері навіть невеликий інцидент може мати непропорційно великий суспільний ефект. Публічний конфлікт навколо храму, вирвана з контексту заява духовного лідера, злам сторінки громади чи поширення неправдивого повідомлення про «гоніння» можуть швидко перерости в ширшу хвилю недовіри, радикалізації та взаємних звинувачень. Саме тому головною проблемою залишається не лише наявність окремих загроз, а їхня здатність взаємно підсилювати одна одну. У таких умовах складно провести чітку межу між легітимною релігійною діяльністю, внутрішнім конфліктом і зовнішньо керованим впливом, що ускладнює і правову оцінку, і практичне реагування.

Протидія гібридним загрозам у релігійній сфері має бути комплексною. Вона не може зводитися лише до державних заборон, окремих спростувань або технічного захисту цифрових ресурсів. Ефективною може бути лише така модель, у якій поєднуються державна координація, правові механізми, стратегічні комунікації, внутрішня стійкість релігійних організацій і партнерство з громадянським суспільством. Для держави це означає потребу в чітких процедурах, доказовості, міжвідомчій взаємодії та зрозумілому публічному поясненні своїх рішень. Для релігійних організацій необхідність прозорішого управління, уважнішого контролю фінансових і кадрових ризиків, внутрішніх правил публічної комунікації та готовності до кризових ситуацій. Для громадянського суспільства посилення ролі медіаграмотності, фактчекінгу, посередництва й діалогу у зниженні конфліктогенності.

Важливе місце у цій системі займає інформаційна та кібербезпека. Для релігійних громад практичне значення мають не лише загальні декларації про цифрову стійкість, а дуже конкретні речі: контроль доступів, двофакторна автентифікація, резервні копії, перевірка фінансових запитів, правила реагування на злам акаунтів, захист персональних даних і підготовлені моделі кризової комунікації. У багатьох випадках саме такі базові дії можуть запобігти значно більшим наслідкам, ніж спроби реагувати вже після масштабної ескалації. Не менш важливо, щоб інформаційна відповідь не підсилювала конфлікт, а навпаки знімала

напругу, повертала ситуацію в площину фактів і не давала закріпитися маніпулятивним наративам.

Для України найбільш доцільним є підхід, що поєднує правову визначеність, інституційну координацію, розвиток організаційної стійкості релігійних громад і культуру деескалації. Найслабшими місцями поки що залишаються фрагментарність реагування, відсутність уніфікованих кризових процедур у багатьох громадах, недостатня інтеграція гуманітарної сфери в загальні підходи до безпеки та нестача довіри між різними учасниками взаємодії. Саме тому практичними кроками мають стати формалізація індикаторів ризику, створення типових протоколів реагування, підготовка відповідальних осіб у громадах, розроблення простих моделей інформаційної й кіберготовності та посилення механізмів взаємодії між державою, релігійними організаціями і громадянським суспільством.

Подальше вивчення цієї теми доцільно зосередити на більш прикладному рівні: на аналізі конкретних кейсів, порівнянні різних конфесійних і регіональних середовищ, розробленні вимірюваних індикаторів гібридного впливу та оцінці ефективності окремих механізмів протидії. Це дало б змогу перейти від загальної моделі до точніших практичних рішень для українських умов. Загалом тема гібридних загроз у релігійній сфері має не лише теоретичне, а й виразне прикладне значення, оскільки безпосередньо пов’язана із захистом суспільної стійкості, прав людини та внутрішньої безпеки держави.

Список використаних джерел

1. Аулін О., Ауліна О. Стратегічні комунікації у протидії деструктивним російським наративам. Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2023. Вип. 67. URL: https://nbuviap.gov.ua/images/e_biblioteka/naukovi_resursi/Socialni%20komunikacii/Aulin%20O.%20Aulina%20O.%20Strategicni%20komunikacii%20.pdf (дата звернення 28.03.2026).

2. Єленський В. Релігійна свобода і безпека у воюючій країні: випадок України. Наукові записки ІПіЕНД ім. І. Ф. Кураса НАН України. 2020. Вип. 3–4 (99–100). С. 394–409. URL: https://ipiend.gov.ua/wp-content/uploads/2020/06/elenskyi_religiina.pdf (дата звернення 28.03.2026).

3. Здіорук С. Етноконфесійна палітра в умовах гібридної війни Росії проти України. Наукові записки ІПіЕНД ім. І. Ф. Кураса НАН України. 2020. Вип. 3–4 (99–100). С. 410–430. URL: https://ipiend.gov.ua/wp-content/uploads/2020/06/zdioruk_etnokonfesiina.pdf (дата звернення 28.03.2026).

4. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення 13.02.2026).

5. Мухін В. Є., Завгородній В. В., Завгородня Г. А. Інформаційна безпека та гібридні загрози : навч. посіб. Київ : ТРОПЕА, 2024. 104 с. URL: https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/scientific-publications/monographs/information_security_and_hybrid_threats.pdf (дата звернення 28.03.2026).

6. Пирожков С. І. та ін. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз : національна доповідь. Київ : НАН України, 2022. 552 с. URL: https://ipiend.gov.ua/wp-content/uploads/2022/05/nats_dopovyd.pdf (дата звернення 28.03.2026).

7. Питання Центру протидії дезінформації : Указ Президента України від 19.03.2021 № 187/2021. URL: https://zakon.rada.gov.ua/go/187/2021 (дата звернення 15.02.2026).

8. Про затвердження Положення про Державну службу України з етнополітики та свободи совісті та внесення змін до Положення про Міністерство культури України : постанова Кабінету Міністрів України від 21.08.2019 № 812. URL: https://zakon.rada.gov.ua/go/812-2019-%D0%BF (дата звернення 15.02.2026).

9. Про захист конституційного ладу у сфері діяльності релігійних організацій : Закон України від 20.08.2024 № 3894-IX. URL: https://zakon.rada.gov.ua/go/3894-20 (дата звернення 15.02.2026).

10. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 15.02.2026).

11. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/go/685/2021 (дата звернення 15.02.2026).

12. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (в частині утворення НКЦК) : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/go/242/2016 (дата звернення 15.02.2026).

13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення 15.02.2026).

14. Про свободу совісті та релігійні організації : Закон України від 23.04.1991 № 987-XII. URL: https://zakon.rada.gov.ua/laws/show/987-12 (дата звернення 13.02.2026).

15. Сальнікова О., Сівоха І., Іващенко А. Стратегічні комунікації в сучасних війнах гібридного типу. Social Development & Security. 2019. Т. 9, № 5. С.

133–142. URL: https://paperssds.eu/index.php/JSPSDS/article/download/146/148/ (дата звернення 28.03.2026).

16. Станіна О. Д. Вплив дезінформації на економічну безпеку країни в умовах розповсюдження цифрових технологій. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2021. № 2. С. 312–316. URL: https://er.dduvs.edu.ua/handle/123456789/6795 (дата звернення 28.03.2026).

17. Степико М. Сучасні виклики українській національній ідентичності. Наукові записки ІПіЕНД ім. І. Ф. Кураса НАН України. 2020. Вип. 3–4 (99–100). С. 253–265. URL: https://ipiend.gov.ua/wp-content/uploads/2020/06/stepyko_suchasni.pdf (дата звернення 28.03.2026).

18. Татарин С. Боти як інструмент політичної маніпуляції. Прикладні дослідження та технології. 2022. С. 89–91. URL: https://elartu.tntu.edu.ua/bitstream/lib/39710/2/PDT_2022_Tatarun_S-Bots_as_a_tool_of_political_89-91.pdf (дата звернення 28.03.2026).

19. Центр Разумкова. Війна і Церква. Церковно-релігійна ситуація в Україні 2022 р. (інформаційні матеріали). Київ, 2023. URL: https://razumkov.org.ua/images/2023/02/13/2022_Religiya_SITE.pdf (дата звернення 28.03.2026).

20. Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). URL: https://www.echr.coe.int/documents/d/echr/convention_ENG (дата звернення 13.02.2026).

21. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union. 05.06.2015. L 141. P. 73–112. URL: https://eur-lex.europa.eu/eli/dir/2015/849/oj/eng (дата звернення 13.02.2026).

22. European Commission against Racism and Intolerance (ECRI). ECRI General Policy Recommendation No. 15 on combating hate speech : adopted on 8

December 2015. Strasbourg : Council of Europe, 2016. 66 p. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech/16808b5b01 (дата звернення 15.02.2026).

23. European Commission; High Representative of the Union for Foreign Affairs and Security Policy. Joint Framework on countering hybrid threats: a European Union response (JOIN(2016) 18 final), 06.04.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата звернення 15.02.2026).

24. European Court of Human Rights. Guide on Article 9 of the European Convention on Human Rights: Freedom of thought, conscience and religion. URL: https://inhak.saglik.gov.tr/Eklenti/21157/0/avrupainsanhaklarisozlesmesiklavuzu-madde9-ingpdf.pdf (дата звернення 13.02.2026).

25. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. September 2024. 131 p. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (дата звернення 15.02.2026).

26. Financial Action Task Force (FATF). Best Practices Paper: Combating the Terrorist Financing Abuse of Non-Profit Organisations (Recommendation 8). Paris : FATF/OECD, 2023. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-Combating-TF-Abuse-NPO-R8.pdf.coredownload.inline.pdf (дата звернення 13.02.2026).

27. Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda. Vienna, 3 March 2017. 5 p. URL: https://www.osce.org/files/f/documents/6/8/302796.pdf (дата звернення 13.02.2026).

28. MCDC (Multinational Capability Development Campaign). Countering Hybrid Warfare. 2017. URL: https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf (дата звернення 13.02.2026).

29. National Cyber Security Centre (NCSC), Switzerland. Anti-Phishing Report 2023. 2024. URL: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/infos-unternehmen/phishing/20240409%20Anti-

Phishing%20Report%202023.pdf.download.pdf/20240409%20Anti-Phishing%20Report%202023.pdf (дата звернення 15.02.2026).

30. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST.CSWP.29. 2024. 32 p. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення 15.02.2026).

31. NATO. Countering hybrid threats (Topic), updated 29.01.2026. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (дата звернення 15.02.2026).

32. NATO StratCom Centre of Excellence. Strategic Communications Hybrid Threats Toolkit. 2021. URL: https://stratcomcoe.org/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf (дата звернення 15.02.2026).

33. Office of the United Nations High Commissioner for Human Rights (OHCHR). One-pager on “incitement to hatred”: The Rabat threshold test. 2020. 1 p. URL: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_threshold_test.pdf (дата звернення 15.02.2026).

34. OSCE Office for Democratic Institutions and Human Rights (ODIHR). Freedom of Religion or Belief and Security : Policy Guidance. Warsaw : OSCE/ODIHR, 2019. 73 p. URL: https://www.osce.org/files/f/documents/e/2/429389.pdf (дата звернення 15.02.2026).

35. OSCE Office for Democratic Institutions and Human Rights (ODIHR). Guidelines on the Legal Personality of Religious or Belief Communities. Warsaw : OSCE/ODIHR, 2014. URL: https://www.osce.org/files/f/documents/9/9/139046.pdf (дата звернення 13.02.2026).

36. OSCE Office for Democratic Institutions and Human Rights (ODIHR). Hate Crime Laws : A Practical Guide. Revised edition. Warsaw : OSCE/ODIHR, 2022. 77 p. URL: https://www.osce.org/sites/default/files/f/documents/1/4/523940.pdf (дата звернення 15.02.2026).

37. OSCE/ODIHR; Venice Commission. Guidelines for Review of Legislation Pertaining to Religion or Belief. 2004. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)028-e (дата звернення 13.02.2026).

38. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A02016R0679-20160504 (дата звернення 15.02.2026).

39. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065 (дата звернення 15.02.2026).

40. UN Human Rights Committee. General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion), 30.07.1993. URL: https://hrlibrary.umn.edu/gencomm/hrcom22.htm (дата звернення 13.02.2026).

41. United Nations. International Covenant on Civil and Political Rights (ICCPR). URL: https://www.ohchr.org/sites/default/files/ccpr.pdf (дата звернення 13.02.2026).

42. United Nations. Plan of Action to Safeguard Religious Sites : In Unity and Solidarity for Safe and Peaceful Worship. 2019. 29 p. URL: https://www.unaoc.org/wp-content/uploads/Plan-of-Action-to-Safeguard-Religious-Sites-11092019.pdf (дата звернення 15.02.2026).

43. Verizon. 2025 Data Breach Investigations Report: Small and Medium Business Snapshot. 2025. URL: https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення 15.02.2026).