

Міністерство освіти і науки України
Національний університет “Острозька академія”
Навчально–науковий центр заочно–дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра на тему:
“Моссад Ізраїлю – досвід для України”

Виконав студент II курсу, групи ЗМНб–21,
спеціальності 256 Національна безпека (за
окремими сферами забезпечення і видами
діяльності)

Карпенко Владислав Олександрович

Керівник – кандидат політичних наук, доцент
Мартинюк Роман Станіславович

Рецензент – кандидат юридичних наук,
доцент, заслужений юрист України

Ірха Юрій Богданович

Острог, 2026

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ІСТОРІЯ, ОРГАНІЗАЦІЯ (СТРУКТУРА) ТА ФУНКЦІЇ МОССАДУ	
1.1. Основні етапи становлення і розвитку Моссаду. Завдання організації.	10
1.2. Зміни в структурі та напрямках діяльності: сучасний період організації та діяльності Моссаду	26
1.3. Основні структурні підрозділи Моссаду та їхня функціональна спрямованість. Взаємодія Моссаду з іншими спецслужбами Ізраїлю	44
ВИСНОВКИ до розділу 1	60
РОЗДІЛ 2. ОПЕРАТИВНА ДІЯЛЬНІСТЬ МОССАДУ ТА ЇЇ ОСОБЛИВОСТІ	
2.1. Основні методи та засоби оперативної діяльності Моссаду	63
2.2. Найвідоміші операції Моссаду	78
ВИСНОВКИ до розділу 2	104
РОЗДІЛ 3. ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ДОСВІДУ МОССАДУ В ОРГАНІЗАЦІЇ ТА ДІЯЛЬНОСТІ УКРАЇНСЬКИХ СПЕЦСЛУЖБ	
3.1. Порівняльний аналіз спецслужб Ізраїлю та України	107
3.2. Порівняння методів оперативної діяльності та законодавчого регулювання	112
3.3. Потенціал адаптації досвіду Моссаду до українських реалій	115
3.4. Конкретні рекомендації щодо організаційних, оперативних та законодавчих змін	118

3.5. Обмеження, ризики та перешкоди адаптації ізраїльського досвіду в Україні	123
ВИСНОВКИ.....	127
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	131
ДОДАТКИ.....	136

ВСТУП

1. Актуальність дослідження.

У сучасному світі, позначеному ескалацією гібридних загроз, асиметричних конфліктів та перманентної геополітичної нестабільності, забезпечення національної безпеки держави набуває стратегічного, екзистенційного характеру. Україна, здобувши незалежність у 1991 році, з перших днів свого існування як суверенної держави зіткнулася з системною гібридною агресією з боку Російської Федерації. Ця агресія не почалася у 2014 році з анексії Криму чи у 2022 році з повномасштабного вторгнення – вона має глибокі корені, що сягають саме моменту проголошення незалежності.

З самого початку Росія не сприймала Україну як повноцінну суверенну державу. Політичне керівництво РФ послідовно просуvalo наратив про «штучність» української державності, «єдиний народ» та «російський світ», що супроводжувалося системною пропагандою, інформаційними операціями, економічним тиском, енергетичним шантажем, культурно–лінгвістичним впливом та втручанням у внутрішні справи. Уже в 1990–х роках Росія активно використовувала інструменти гібридної війни: підтримку проросійських політичних сил, контроль над частиною медіа–простору, економічну залежність через постачання енергоносіїв та спроби збереження військової присутності (Чорноморський флот у Севастополі).

Особливо яскраво гібридні методи проявилися в період 2000–2013 років. Газові війни 2006 та 2009 років стали класичним прикладом економічного примусу: Росія неодноразово перекривали постачання газу, створюючи енергетичні кризи не лише в Україні, але й у Європі, з метою дестабілізації української економіки та політичної системи. Криза навколо острова Тузла у 2003 році продемонструвала застосування «сірих» методів територіального тиску. Під час Помаранчевої революції 2004 року Росія активно втручалася у виборчий процес через інформаційну кампанію, фінансування проросійських кандидатів та дипломатичний тиск. Постійними були кібератаки, витоки

інформації, дезінформація в російських ЗМІ та соціальних мережах, а також спроби розпалювання регіонального сепаратизму, особливо в Криму та на сході України.

Таким чином, з 1991 року Україна перебуває в стані тривалої гібридної війни, яка поєднує елементи інформаційно–психологічного впливу, економічної агресії, кібероперацій, політичного втручання та підготовки до відкритої збройної фази. Станом на 2026 рік це вже понад 35 років системного протистояння, з яких понад 12 років – у формі відкритого збройного конфлікту (з 2014 року) та понад 4 роки повномасштабної війни (з лютого 2022 року). Російська пропаганда, економічний шантаж, підтримка п'ятої колони, кібердиверсії та операції впливу стали постійними інструментами Кремля, спрямованими на підрив суверенітету, територіальної цілісності та європейського вибору України.

У таких умовах досвід найефективніших світових спецслужб, зокрема ізраїльської розвідки «Моссад» (офіційна назва – Інститут розвідки та спеціальних завдань), набуває для України виняткової актуальності. Моссад, створений у 1949–1951 роках за ініціативи першого прем'єр–міністра Давида Бен–Гуріона, за відносно невеликих ресурсів (штатна чисельність значно менша за СБУ чи ГУР МО України) забезпечує стратегічну перевагу державі, яка десятиліттями оточена ворогами. Його діяльність базується на принципах випереджального збору інформації, точкових спеціальних операцій, глибокої агентурної роботи, інтеграції найсучасніших технологій (кібер–, дрон– та інформаційні операції) та максимальної оперативної свободи.

Для України вивчення цього досвіду є особливо цінним з кількох ключових причин. По–перше, українські спецслужби – Служба безпеки України (СБУ) та Головне управління розвідки Міністерства оборони (ГУР МО) – вже демонструють елементи «моссадівського» стилю роботи: зухвалі операції на території РФ, ліквідації ключових фігур ворожої логістики, кібердиверсії та ефективну роботу з агентурою в тилу противника.

Експерти західних розвідок та ЗМІ неодноразово порівнювали українські спецслужби з Моссадом 1970–х років саме через креативність, швидкість і результативність.

По–друге, попри значні оперативні успіхи (операції проти «вагнерівців», удари по російському флоту, диверсії на нафтопереробних заводах РФ), українська система національної безпеки все ще має структурні, законодавчі та організаційні прогалини: недостатня координація між відомствами, обмеженість у проведенні операцій за кордоном, брак системної підготовки елітних оперативників та недостатня інтеграція з приватним сектором (технології, бізнес–розвідка). Моссад, який підпорядковується безпосередньо прем'єр–міністру, має максимальну оперативну свободу, що дозволяє діяти швидко, ефективно та з мінімальною бюрократією.

По–третє, геополітичний контекст 2025–2026 років (продовження гібридної війни РФ, активізація Ірану, Північної Кореї та Китаю як союзників агресора) вимагає від України не лише оборонних, а й потужних наступальних інструментів. Досвід Моссаду в протидії Ірану (саботаж ядерної програми, диверсії на ракетних базах, операція з пейджерів «Хезболли» 2024 року) має пряму кореляцію з українськими викликами.

Наукове значення теми полягає в тому, що комплексне дослідження досвіду Моссаду в контексті українських реалій тривалої гібридної агресії (з 1991 року) досі не проводилося на магістерському рівні в повному обсязі. Практичне значення – можливість розробки конкретних рекомендацій для реформування законодавства (зокрема Закону України «Про Службу безпеки України»), оптимізації структури спецслужб, удосконалення програм підготовки кадрів та посилення міжнародної співпраці з Ізраїлем, який вже є важливим партнером України в оборонній сфері.

Таким чином, актуальність дослідження зумовлена необхідністю підвищення ефективності української системи національної безпеки шляхом критичного осмислення та адаптації перевірених практик однієї з

найефективніших розвідок світу в умовах багаторічної гібридної та повномасштабної агресії, що триває з моменту здобуття незалежності.

2. Мета та завдання дослідження

Мета дослідження полягає в комплексному аналізі досвіду діяльності спеціальних служб Ізраїлю (зокрема Моссаду) та визначенні перспектив його використання в організації та діяльності українських спецслужб для підвищення ефективності забезпечення національної безпеки України в умовах тривалої гібридної та конвенційної агресії.

Для досягнення поставленої мети визначено такі завдання:

1. Розкрити основні етапи становлення, розвитку та трансформації Моссаду, визначити його стратегічні завдання на різних історичних етапах.
2. Проаналізувати сучасну організаційну структуру, функціональну спрямованість ключових підрозділів Моссаду та механізми їхньої взаємодії з іншими ізраїльськими спецслужбами (Шабак, АМАН).
3. Дослідити методи та засоби оперативної діяльності Моссаду, а також проаналізувати найвідоміші операції з метою виявлення сильних і слабких сторін його роботи.
4. Здійснити порівняльний аналіз організаційно–правових засад, структури, методів роботи та законодавчого регулювання спецслужб Ізраїлю та України.
5. Визначити потенціал адаптації досвіду спеціальних служб Ізраїлю до українських умов, сформулювати конкретні рекомендації щодо організаційних, оперативних та законодавчих змін.
6. Виявити обмеження, ризики та перешкоди адаптації ізраїльського досвіду з урахуванням політичних, правових, культурних, соціальних та економічних особливостей України.

3. Об'єкт і предмет дослідження

Об'єкт дослідження – організаційна структура та діяльність спеціальних служб Ізраїлю як інструменту забезпечення національної безпеки держави в умовах перманентної зовнішньої загрози.

Предмет дослідження – специфічні організаційні моделі, методи, стратегії, тактики та оперативні практики спеціальних служб Ізраїлю (зокрема Моссаду), які можуть бути адаптовані до системи національної безпеки України.

4. Хронологічні, географічні та інші рамки дослідження

Хронологічні рамки охоплюють період від створення Моссаду (1949–1951 рр.) до сучасного стану (2026 рік), з особливим акцентом на трансформації після 1960–х років (період найбільших операцій) та пост–2020–х (кібер– та гібридні операції). Для українського контексту – з 1991 року (момент здобуття незалежності та початку системної гібридної агресії РФ) до 2026 року.

Географічні рамки – глобальна діяльність спеціальних служб Ізраїлю та територія України, Російської Федерації та країн–партнерів.

5. Методологія дослідження

Дослідження базується на сукупності загальнонаукових та спеціальних методів:

- історико–хронологічний – для аналізу етапів розвитку Моссаду;
- порівняльно–правовий – для зіставлення ізраїльської та української моделей спецслужб;
- структурно–функціональний – для характеристики підрозділів і взаємодії;
- аналітичний, синтетичний та системний – для вивчення операцій і методів;
- метод моделювання – для розробки рекомендацій щодо адаптації;
- метод контент–аналізу – для опрацювання відкритих джерел, документів і публікацій.

6. Огляд літератури та джерел

Проблематика діяльності спеціальних служб Ізраїлю, зокрема Моссаду, достатньо висвітлена в зарубіжній літературі. Класичними працями є дослідження Міхаеля Бар–Зохара та Ніссіма Мішала, Ронена Бергмана («Rise and Kill First: The Secret History of Israel's Targeted Assassinations»), Гордона Томаса («Gideon's Spies: The Secret History of the Mossad»), а також мемуари колишніх директорів Моссаду – Ісера Гареля та Меїра Дагана. Ці роботи містять багатий фактичний матеріал щодо історії створення, організаційної структури та

найбільш резонансних операцій ізраїльської розвідки. Окреме місце посідають дослідження, присвячені технологічним аспектам діяльності Моссаду, зокрема роботі Кіма Зеттера щодо операції Stuxnet.

В Україні тема розглядається переважно в загальному контексті національної безпеки та протидії гібридним загрозам. Значний внесок у дослідження цієї проблематики зробили В. П. Горбулін, науковці Національного інституту стратегічних досліджень, а також автори посібника «Український Моссад: книга життя у законах війни» П. М. Лісовський та Ю. П. Лісовська. Окремі аспекти діяльності українських спецслужб висвітлюються у звітах СБУ та ГУР МО України.

Водночас комплексного наукового дослідження, присвяченого саме можливостям адаптації організаційного досвіду та методів роботи спеціальних служб Ізраїлю до українських реалій у контексті тривалої гібридної агресії Російської Федерації (з 1991 року), на магістерському рівні досі не проводилося. Більшість наявних робіт або обмежуються описом діяльності Моссаду, або розглядають реформування українських спецслужб без системного порівняння з ізраїльською моделлю. Це зумовлює наукову новизну даної роботи, яка полягає у здійсненні комплексного порівняльного аналізу та розробці практичних рекомендацій щодо адаптації досвіду спеціальних служб Ізраїлю до умов України.

7. Структура й обсяг дослідження

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

У вступі обґрунтовано актуальність теми, сформульовано мету та завдання дослідження, визначено об'єкт і предмет, окреслено хронологічні та географічні рамки, розкрито методологічну основу, здійснено огляд стану наукової розробки теми та сформульовано положення, що виносяться на захист.

Перший розділ «Історія, організація (структура) та функції Моссаду» присвячено аналізу етапів становлення та розвитку Моссаду, його сучасної

організаційної структури та механізмів взаємодії з іншими ізраїльськими спецслужбами.

Другий розділ «Оперативна діяльність Моссаду та її особливості» охоплює методи та засоби роботи Моссаду, а також детальний аналіз найбільш показових операцій організації.

Третій розділ «Перспективи використання досвіду Моссаду в організації та діяльності українських спецслужб» містить порівняльний аналіз систем національної безпеки Ізраїлю та України, оцінку потенціалу адаптації та розробку конкретних рекомендацій.

Загальний обсяг роботи становить 138 сторінок, з них основного тексту – 124 сторінки. Список використаних джерел налічує 52 найменування.

Положення, що виносяться на захист:

1. Спеціальні служби Ізраїлю, зокрема Моссад, демонструють високу ефективність завдяки прямому підпорядкуванню вищому політичному керівництву, елітній системі відбору та підготовки кадрів, а також глибокій інтеграції сучасних технологій в оперативну діяльність.
2. Українські спецслужби вже застосовують окремі елементи, притаманні ізраїльській моделі роботи, однак потребують системних організаційних, кадрових та законодавчих реформ для підвищення ефективності в умовах багаторічної гібридної агресії.
3. Адаптація досвіду спеціальних служб Ізраїлю до українських реалій можлива за умови селективного підходу з урахуванням національних особливостей, вимог демократичного контролю та існуючих правових обмежень.

РОЗДІЛ 1.

ІСТОРІЯ, ОРГАНІЗАЦІЯ (СТРУКТУРА) ТА ФУНКЦІЇ МОССАДУ

1.1. Основні етапи становлення і розвитку Моссаду. Завдання організації.

Створення ізраїльської зовнішньої розвідки «Моссад» (повна офіційна назва – «Інститут розвідки та спеціальних завдань», івр. המוסד למודיעין ולתפקידים – HaMossad leModi'in uleTafkidim Meyuhadim) є одним із найяскравіших прикладів того, як молода держава, оточена ворожим оточенням і позбавлена стратегічної глибини, змогла сформувати одну з найефективніших і найпрофесійніших спецслужб світу. Офіційна дата заснування Моссаду – 13 грудня 1949 року [9, с.15-18; 26, с.23-26] коли перший прем'єр-міністр Ізраїлю Давид Бен-Гуріон підписав директиву про створення «Центрального інституту координації» (HaMossad leModi'in uleTafkidim Meyuhadim). У березні 1951 року інститут був реорганізований і виведений з-під підпорядкування Міністерства закордонних справ безпосередньо під прем'єр-міністра [9, с.28-30; 23, с.89-92], що стало ключовим принципом його діяльності на всі наступні десятиліття.

Бен-Гуріон чітко усвідомлював екзистенційну загрозу для новоствореної держави. У листі до Міністерства закордонних справ він писав: «Для нашої держави, яка з моменту створення перебуває в облозі ворогів, розвідка становить першу лінію оборони... Ми повинні добре навчитися розпізнавати, що відбувається навколо нас» [26, с.24-25]. Ця директива стала фундаментом усієї діяльності Моссаду: максимальна оперативна автономія, пряме підпорядкування лише прем'єр-міністру та принцип «випереджального удару» (preventive strike). На момент створення Моссад не виник «з нуля» – він став правонаступником розвідувальної служби «Шай» (Sherut Yedi'ot) – інформаційного відділу підпільної організації «Хагана», яка діяла ще в період британського мандату в Палестині (1920–1948 рр.) [9;18]. «Шай» займалася збором інформації про

британські сили, арабські угруповання, організацією нелегальної імміграції євреїв (Алія Бет) та протидією нацистським злочинцям.

Передісторія (1930–ті – 1948 рр.). Корені Моссаду сягають 1937 року, коли в рамках «Хагани» почали створювати спеціальні підрозділи для нелегальної імміграції та збору розвідданих. Після проголошення незалежності Ізраїлю 14 травня 1948 року та Війни за незалежність (1948–1949 рр.) виникла нагальна потреба в централізованій зовнішній розвідці. Існуючі структури – військова розвідка АМАН (Agaf Modi'in) та внутрішня контррозвідка Шабак/Шин–Бет (Shin Bet) – не могли повноцінно забезпечити глобальний збір інформації та проведення спеціальних операцій за кордоном. Саме тому Бен–Гуріон доручив Реувену Шілоаху (Reuven Shiloah), досвідченому дипломату та розвіднику, який ще до 1948 року очолював політичний відділ Єврейського агентства, створити єдиний координаційний центр [9;26].

Перший етап становлення: організаційна побудова та перші операції (1949–1952 рр., Реувен Шілоах)

Перші три роки існування Моссаду (з грудня 1949 по вересень 1952 р.) стали періодом організаційного становлення та вирішення найнагальніших екзистенційних завдань. Штат був невеликим – кілька десятків осіб. Основна увага приділялася не класичним шпигунським операціям, а трьом пріоритетам, визначеним Бен–Гуріоном:

1. Масова імміграція євреїв (Алія) як стратегічна необхідність для виживання держави.
2. Збір розвідданих про арабські країни (військові плани, озброєння, політична ситуація).
3. Протидія залишкам нацистських злочинців та антисемітським угрупованням за кордоном [9;26].

Наймасштабнішою операцією першого етапу стала операція «Езра і Нехемія» [9, с.48-53; 26, с.61-67] (1950–1951 рр.) – повітряний міст для евакуації іракських євреїв. У той час в Іраку проживало близько 130 000 євреїв, яких піддавали переслідуванням після створення Ізраїлю. Моссад під керівництвом

Шілоаха організував таємну евакуацію: за кілька місяців було здійснено понад 100 рейсів, у результаті яких до Ізраїлю прибуло понад 125 000 осіб. Це була логістична, дипломатична та розвідувальна операція одночасно: потрібно було домовитися з іракською владою, організувати підпільні пункти збору, забезпечити безпеку та приховати участь ізраїльської розвідки [9;26]. Успіх операції став першим великим досягненням Моссаду і продемонстрував його здатність вирішувати стратегічні державні завдання.

Паралельно Моссад почав формувати агентурну мережу в арабських країнах (Єгипет, Сирія, Ірак, Йорданія). Однак саме на цьому напрямі виявилися перші серйозні проблеми. У 1951 році іракська влада викрила частину агентурної мережі Моссаду в Багдаді, що призвело до арештів і страт кількох агентів [9, с.54-55]. Цей провал виявив слабкі місця першого етапу: брак професійної підготовки оперативників, недостатню конспірацію та перевантаження Шілоаха (він одночасно виконував дипломатичні функції).

Іншим напрямком діяльності стало налагодження міжнародних контактів. Шілоах активно розвивав «периферійну дипломатію» – таємні зв'язки з неарабськими державами регіону (Туреччина, Іран, Ефіопія), які пізніше стали основою довгострокової стратегії Ізраїлю [9;23]. Також почалися перші спроби співпраці із західними розвідками (США, Велика Британія).

Основні завдання Моссаду на першому етапі (сформульовані Шілоахом і затверджені Бен-Гуріоном):

- координація всіх розвідувальних зусиль держави за кордоном;
- збір політичної, військової та економічної інформації про потенційних супротивників;
- організація та захист єврейської імміграції;
- проведення спеціальних операцій (поки що обмежених масштабів);
- створення інфраструктури для майбутньої розвідки (резидентури, система зв'язку, легенди прикриття).

Проблеми та криза першого етапу. До 1952 року стало очевидно, що Шілоах, будучи талановитим дипломатом і стратегом, не мав достатнього

досвіду оперативного керівництва великою службою. Бюрократичні конфлікти з АМАН і Шин–Бет, провали агентурних мереж, брак фінансування та кадровий голод призвели до кризи. 20 вересня 1952 року Реувен Шілоах подав у відставку [9;23]. У березні 1952 року відбулася важлива реорганізація: Моссад було повністю виведено з–під МЗС і перетворено на самостійний інститут, підпорядкований безпосередньо прем'єр–міністру [26]. Це стало фундаментальним принципом діяльності служби на всі наступні десятиліття.

Таким чином, перший етап (1949–1952 рр.) був періодом закладання фундаментів. Моссад ще не став глобальною оперативною машиною, але вже довів свою спроможність вирішувати стратегічні державні завдання в умовах екзистенційної загрози. Успішна операція «Езра і Нехемія», створення координаційного механізму та принцип прямого підпорядкування прем'єр–міністру стали тією основою, на якій наступні керівники (починаючи з Ісера Гареля) побудували одну з найефективніших розвідок світу [9;26].

Другий етап: професіоналізація та становлення світового рівня (1952–1963 рр., Ісер Гарель)

Перехід від першого етапу до другого став переломним моментом в історії Моссаду. 20 вересня 1952 року Реувен Шілоах подав у відставку [9;23] через накопичені організаційні проблеми, провали агентурних мереж та брак оперативного досвіду. Уже 22 вересня 1952 року (за іншими джерелами – 1 січня 1952 року) на посаду директора Моссаду був призначений Ісер Гарель (Isser Harel, справжнє прізвище – Гальперін, 1912–2003) [14, с.8-11; 29, с.12-15]. До цього Гарель очолював внутрішню службу безпеки Шин–Бет (Shin Bet) і мав репутацію жорсткого, принципового та надзвичайно ефективного керівника [23;14]. Саме з його приходом Моссад перестав бути лише координаційним центром і перетворився на високопрофесійну, глобальну розвідувально–оперативну структуру світового рівня.

Гарель отримав унікальний статус «Хамемуне» (HaMemuneh – «відповідальний»), що означало фактичне керівництво не лише Моссадом, але й усіма іншими ізраїльськими розвідслужбами (Шин–Бет, АМАН) [14, с.45-48].

Він став другою після прем'єр-міністра людиною в державі з питань безпеки. Бен-Гуріон особисто підтримав цю реформу, оскільки розумів необхідність єдиного жорсткого керівництва в умовах постійної екзистенційної загрози [26, с.68-70; 14, с.49-51]. За 11 років керівництва (1952–1963) Гарель радикально змінив Моссад: штат зріс з кількох десятків до понад 600 осіб, була створена професійна система підготовки оперативників («каців» – офіцерів-кураторів), розбудована глобальна мережа резидентур і агентури, а також сформульовані ключові принципи роботи, які діють до сьогодні [9, с.60-65; 26, с.70-76].

Головні реформи Ісера Гареля включали:

1. Професіоналізацію кадрів. Гарель запровадив жорсткий багатоступеневий відбір, спеціальні курси підготовки в ізольованих таборах, акцент на психологію, конспірацію, мовну підготовку та роботу під глибоким прикриттям [14;29]. Оперативники навчалися не лише класичним методам шпигунства, але й психології допиту, роботі з документами та легендами.
2. Створення централізованої системи управління. Моссад отримав чітку ієрархію, відділи (розвідка, спеціальні операції, аналіз, логістика, технології). Було запроваджено принцип «командної роботи» замість індивідуальних ініціатив [9;23].
3. Розбудову глобальної інфраструктури. Створено резидентури в Європі, Латинській Америці, на Близькому Сході. Активно розвивалася «доктрина периферії» – таємні зв'язки з неарабськими державами (Іран, Туреччина, Ефіопія) [9;26].
4. Принцип «Never Again» («Ніколи знову»). Після Голокосту Моссад отримав моральний мандат на активне переслідування нацистських злочинців та захист єврейських громад у діаспорі [14;29].

Найяскравішою і найвідомішою операцією цього етапу стала операція «Фінал» (або «Будинок на вулиці Гарібальді», 1960 рік) – викрадення Адольфа Ейхмана в Аргентині [14, с.95-115; 29, с.82-105.]. Ейхман, один із головних архітекторів «остаточного рішення єврейського питання», переховувався в Буенос-Айресі під ім'ям Рікардо Клемента. Пошук тривав понад 15 років (з

участю Саймона Візенталя та агентів Моссаду). У 1959–1960 рр. Гарель особисто взяв керівництво операцією. Команда з 11 оперативників (серед них – Рафаель Ейтан, Пітер Малкін, Цві Аароні) провела кілька місяців спостереження. 11 травня 1960 року Ейхмана схопили біля будинку на вулиці Гарібальді [14;29]. Його утримували в таємній квартирі, допитали, а потім під виглядом члена екіпажу ізраїльського літака (який прибув на святкування 150-річчя незалежності Аргентини) таємно вивезли до Ізраїлю. Операція була проведена без єдиного пострілу і без втручання аргентинської влади. Ейхман постав перед судом у Єрусалимі, був засуджений до смертної кари і страчений у 1962 році. Ця операція не лише продемонструвала світові можливості Моссаду, але й стала потужним моральним актом історичної справедливості. Ісер Гарель особисто перебував в Аргентині і керував усіма етапами.

Інші значні операції другого етапу:

- Організація таємної імміграції євреїв з Марокко та інших країн (обмін розвідданими на дозвіл на еміграцію).
- Операції проти німецьких вчених, які працювали над ракетними програмами в Єгипті (1950-ті – початок 1960-х). Моссад проводив залякування, саботаж і, за деякими даними, ліквідації. Ці дії, однак, призвели до серйозного конфлікту з Бен-Гуріоном, який прагнув нормалізації відносин з ФРН.
- Інцидент 1954 року з Александром Ізраелем (ізраїльським офіцером, запідозреним у шпигунстві на користь Єгипту). Операція з його викрадення закінчилася смертю агента через передозування снодійного. Гарель віддав наказ викинути тіло в море, підкресливши принцип «Ми не вбиваємо євреїв».

Завдання Моссаду на другому етапі значно розширилися і набули чіткішої оперативної спрямованості:

- Глибоке проникнення в арабські країни та збір інформації про їхні військові плани.
- Боротьба з нацистськими злочинцями та захист єврейських громад.

- Проведення спеціальних операцій (викрадення, саботаж, ліквідації).
- Розбудова міжнародних розвідувальних зв'язків (особливо з США – передача тексту «секретної доповіді Хрущова» 1956 р.).
- Створення технологічної бази для майбутніх операцій.

Підсумки та значення етапу. За часів Ісера Гареля Моссад із координаційного органу перетворився на професійну службу, здатну проводити високоризикові операції на іншому континенті. Репутація Моссаду як «найкращої розвідки світу» була закладена саме тоді. Однак етап завершився конфліктом: у 1963 році Бен-Гуріон змусив Гареля піти у відставку через операції проти німецьких вчених, які загрожували зовнішній політиці Ізраїлю. Це стало уроком: навіть найуспішніша розвідка повинна діяти в рамках політичних реалій.

Таким чином, другий етап (1952–1963 рр.) став періодом професіоналізації та перших гучних перемог. Ісер Гарель заклав фундаментальні принципи, які визначають обличчя Моссаду й сьогодні: оперативна автономія, жорстка дисципліна, моральний імператив «Ніколи знову» та здатність до сміливих, нестандартних дій.

Третій етап: війна, контртероризм та операційна зрілість (1963–1974 рр., Меїр Аміт та Цві Замір)

Третій етап розвитку Моссаду став періодом переходу від професіоналізації до повномасштабної бойової діяльності в умовах реальних війн та зростання терористичної загрози. Він охоплює два ключових керівництва: Меїра Аміта (1963–1968 рр.) та Цві Заміра (1968–1974 рр.). Цей етап характеризується інтенсивним використанням Моссаду як інструменту державної політики під час Шестиденної війни (1967 р.), Війни Судного дня (1973 р.) та початку епохи міжнародного тероризму.

Меїр Аміт (1963–1968 рр.) Після відставки Ісера Гареля в 1963 році на посаду директора Моссаду був призначений генерал-майор Меїр Аміт – бойовий генерал, колишній начальник військової розвідки АМАН [9;26]. Прихід військової людини на чолі зовнішньої розвідки став стратегічним рішенням:

Бен-Гуріон та наступний прем'єр-міністр Леві Ешкол хотіли ще тіснішої інтеграції Моссаду з армією в умовах зростання напруги з арабськими сусідами.

Аміт провів глибоку реорганізацію служби:

- Посилив співпрацю між Моссадом, АМАН та Шин-Бетом (створено єдиний координаційний центр).
- Розбудував агентурну мережу в Єгипті, Сирії та Йорданії.
- Активно впроваджував технічні засоби розвідки (електронна розвідка, аерофотозйомка).
- Зміцнив «доктрину периферії» – таємні контакти з Іраном, Туреччиною, Ефіопією та курдськими повстанцями в Іраку [9;23].

Найважливішим досягненням етапу стала Шестиденна війна (5–10 червня 1967 р.). Моссад під керівництвом Аміта забезпечив ізраїльське командування критичною розвідінформацією: точні дані про дислокацію єгипетських, сирійських та йорданських військ, плани наступу, стан авіації та ППО. Завдяки цій інформації Ізраїль провів превентивний удар і за шість днів здобув переконливу перемогу [9;26]. Аміт особисто брав участь у плануванні операції «Фокус» (удар по єгипетській авіації). Після війни Моссад отримав додаткові повноваження та ресурси для розширення діяльності в арабських країнах.

Цві Замір (1968–1974 рр.) У 1968 році посаду директора обійняв Цві Замір – також генерал-майор, колишній командир Південного командування [8]. Його керівництво збіглося з початком епохи палестинського тероризму. Після поразки в Шестиденній війні арабські держави перейшли до тактики «війни на виснаження», а палестинські угруповання (ОВП, «Чорний вересень», «Народний фронт визволення Палестини») розпочали кампанію терористичних атак по всьому світу.

Кульмінацією стала мюнхенська трагедія 5–6 вересня 1972 року – захоплення та вбивство 11 ізраїльських спортсменів на Олімпійських іграх у Мюнхені бойовиками «Чорного вересня» [10, с.305-312 ;27, с.290-298]. Прем'єр-міністр Голда Меїр дала Моссаду зелений світло на проведення безпрецедентної операції відплати.

Операція «Гнів Божий» (Wrath of God, 1972–1980–ті pp.) [10, с.315-320; 11, с.45-48]

Замір особисто керував створенням спеціального підрозділу «Кідон» (Bayonet) – елітної групи ліквідаторів. Операція включала:

- Ліквідацію ключових організаторів мюнхенського теракту в Європі, Лівані та на Близькому Сході.
- Використання методів: вибухівки в автомобілях, снайперські атаки, отруєння, інсценування нещасних випадків.
- Найвідоміші акції: ліквідація Алі Хасана Саламе («Червоного принца») у 1979 році в Бейруті [10, с.322-328;].

Операція тривала понад 10 років і стала еталоном точкових спецоперацій. Вона продемонструвала світові, що Моссад діє за принципом «око за око» і не пробачає тероризму. Водночас операція мала й негативні наслідки: помилкове вбивство невинного марокканця в Ліллехаммері (Норвегія, 1973 р.) призвело до міжнародного скандалу та тимчасового призупинення частини операцій.

Паралельно Моссад активно працював під час Війни Судного дня (6–24 жовтня 1973 р.). Хоча початковий етап війни став розвідувальним провалом (Моссад недооцінив готовність Єгипту та Сирії до нападу), служба швидко відновилася і забезпечила критичну інформацію в ході бойових дій.

Завдання Моссаду на третьому етапі:

- Забезпечення розвідданими під час великих воєн (Шестиденна та Судного дня).
- Боротьба з міжнародним тероризмом як пріоритетне державне завдання.
- Глибоке проникнення в арабські країни та терористичні організації.
- Розвиток технічних засобів розвідки та спеціальних підрозділів («Кідон»).
- Захист ізраїльських інтересів за кордоном.

Підсумки третього етапу. За 11 років (1963–1974) Моссад остаточно сформувався як глобальна сила, здатна проводити операції будь-якої складності. Репутація «найстрашнішої розвідки світу» була закріплена саме тоді. Водночас етап виявив і вразливі місця: надмірна секретність іноді призводила до провалів,

а політичне керівництво іноді використовувало Моссад для «брудної роботи». Цві Замір пішов у відставку в 1974 році після завершення найбільш інтенсивної фази «Гніву Божого».

Таким чином, третій етап став епохою бойового хрещення Моссаду. Служба перейшла від оборонної розвідки до активної наступальної політики, заклавши основу сучасної доктрини випереджувальних дій.

Четвертий етап: глобальні виклики, порятунок євреїв та підготовка до нових загроз (1974–2002 рр.)

Після відставки Цві Заміра в 1974 році Моссад увійшов у період стабілізації, адаптації до післявоєнних реалій та переходу від масштабних воєнних конфліктів до боротьби з тероризмом, гуманітарних операцій і протидії новим стратегічним загрозам (ядерна програма Іраку та Ірану) [9;26]. Цей етап охоплює керівництво п'яти директорів і характеризується поєднанням класичної розвідки з великими гуманітарно–логістичними операціями та підтримкою мирних процесів. Моссад поступово еволюціонував у бік більш технологічної та превентивної моделі роботи.

Іцхак Хофі (1974–1982 рр.). Генерал–майор Іцхак Хофі, колишній командир Північного командування, очолив службу в умовах післявоєнної кризи довіри після Війни Судного дня [9]. Його пріоритетом стало відновлення оперативної ефективності та розбудова мережі в Лівані та країнах Перської затоки. Найвизначнішим досягненням Хофі стала підготовка та реалізація операцій з порятунку ефіопських євреїв (фалашів). У 1984–1985 рр. під час операції «Мойсей» (Moses) Моссад організував таємний повітряний міст із Судану, евакуювавши понад 8 000 осіб [9;26]. Ця операція вимагала складної координації з американськими та суданськими спецслужбами, логістики та глибокого прикриття. Хофі також активно забезпечував розвідданими ізраїльську армію під час операції «Мир для Галілеї» (1982) у Лівані, спрямованій проти ОВП.

Нахум Адмоні (1982–1990 рр.). Перший цивільний директор за тривалий час, Адмоні зосередився на стратегічних загрозах. Під його керівництвом

Моссад продовжував операції проти залишків іракської ядерної програми (після удару по Осіраку 1981 р.) та почав моніторинг іранської ядерної активності. У 1985 році стався відомий скандал з Джонатаном Поллардом – американським аналітиком, який передавав секретні матеріали Ізраїлю. Хоча Поллард формально працював на військову розвідку (ЛАКАМ), інцидент негативно вплинув на міжнародну репутацію Моссаду та ізраїльсько–американські відносини. Адмоні також координував розвідку під час ірано–іракської війни (1980–1988) [10;23].

Шабтай Шавіт (1990–1996 рр.). Під час Війни в Перській затоці (1991) Моссад надавав критичну інформацію про іракські ракети «Скад», що загрожували Ізраїлю [9]. Шавіт продовжував масштабні операції з порятунку євреїв: операція «Соломон» (1991) евакуювала ще понад 14 000 ефіопських євреїв за 36 годин [9;26]. Крім того, служба активно працювала над імміграцією євреїв із колишнього СРСР після його розпаду. Шавіт зміцнив міжнародну співпрацю з західними розвідками.

Денні Ятом (1996–1998 рр.). Коротке керівництво генерала Денні Ятома було позначене серйозним оперативним провалом. У вересні 1997 року в Аммані (Йорданія) група «Кідон» здійснила невдалу спробу отруєння лідера ХАМАС Халеда Машаля. Операція провалилася, двоє агентів були заарештовані, а Ізраїлю довелося передати антидот і звільнити шейха Ахмеда Ясіна. Скандал призвів до відставки Ятома та тимчасового послаблення довіри до Моссаду [10;27].

Ефраїм Халеві (1998–2002 рр.). Дипломатичний досвід Халеві (він працював у МЗС) допоміг Моссаду підтримувати мирні процеси (підготовка угод з Йорданією та Палестинською автономією). Однак з 2000 року служба перейшла в режим інтенсивної контртерористичної роботи через початок Другої інтифади. Халеві акцентував превентивні операції проти ХАМАС та Хезболли [9;10].

Основні завдання Моссаду на четвертому етапі:

- Масштабний порятунок і репатріація єврейських громад (Ефіопія, СРСР/СНД).
- Протидія розповсюдженню ядерної зброї (Ірак, Іран).
- Контртерористична діяльність у Лівані, Європі та на Близькому Сході.
- Розвідувальна підтримка дипломатичних мирних процесів.
- Розбудова технічних можливостей розвідки.

Підсумки та значення етапу. Четвертий етап продемонстрував унікальну здатність Моссаду поєднувати гуманітарні операції світового масштабу з жорсткою контртерористичною роботою. Порятунок десятків тисяч ефіопських євреїв став одним із найбільших гуманітарних досягнень розвідки в історії.

Водночас етап виявив вразливі місця: надмірна секретність іноді призводила до дипломатичних скандалів (як у випадку з Машалем), а політичне керівництво іноді використовувало службу для «брудної роботи». До 2002 року Моссад підійшов з потужною агентурною мережею, досвідом глобальних операцій і готовністю до нових викликів – кіберзагроз та гібридної війни.

Таким чином, четвертий етап став мостом між класичною «військовою» моделлю Моссаду та сучасною технологічною ерою. Служба підтвердила свою універсальність: вона могла не лише знищувати ворогів, але й рятувати десятки тисяч людей.

П'ятий (сучасний) етап: технологічна революція, гібридні операції та пряме протистояння Ірану (2002–2026 рр.)

П'ятий етап став найдинамічнішим і найбільш технологічно насиченим в історії Моссаду. Він характеризується переходом від класичної агентурної розвідки та точкових операцій до комплексних гібридних кампаній, у яких кібер–, дрон–, агентурні та спеціальні операції працюють як єдиний механізм. Саме в цей період Моссад остаточно перетворився на наступальну стратегічну силу, здатну проводити масштабні операції на території головного супротивника – Ісламської Республіки Іран – навіть під час відкритої регіональної ескалації.[9;10]

Меїр Даган (2002–2011 рр.) Призначений Аріелем Шароном, Даган радикально змінив філософію служби. Замість лише збору інформації пріоритетом стала активна нейтралізація загроз. Головним напрямком стала іранська ядерна програма. Під керівництвом Дагана Моссад організував серію ліквідацій провідних іранських вчених–ядерників (2007–2011 рр.), саботаж на об'єктах у Натанзі та Ісфахані, а також спільну з США операцію Stuxnet (2010) – першу в історії масштабну кіберзброю, яка фізично пошкодила тисячі іранських центрифуг [25, с.210-255; 33, с.187-205]. Даган також відновив і розширив підрозділ «Кідон», зробивши його більш технологічним.[9, с.245-250; 10, с.420-428]

Тамір Пардо (2011–2016 рр.) Пардо продовжив антиіранську лінію, але зробив акцент на технологічній трансформації. За його часів у структурі Моссаду були створені потужні кібер–підрозділи, які працювали в тісній інтеграції з військовою розвідкою АМАН. Служба активно займалася збором даних про іранські ракетні програми та підтримувала підготовку Авраамових угод (нормалізація відносин Ізраїлю з арабськими країнами)[9;10].

Йоссі Коен (2016–2021 рр.) Коен, який раніше очолював відділ Tzomet (відповідальний за вербування агентури), став одним із ключових архітекторів сучасної гібридної стратегії. Саме за його участі (ще з часів Дагана) розпочалося довгострокове планування операції з пейджерами та раціями Хезболли. Коен значно посилив міжнародну співпрацю та технологічний розвиток служби [9;10;27].

Давид Барнеа (2021–червень 2026 рр.) Барнеа, бойовий командир елітного підрозділу Сайерет Маткаль, став тринадцятим директором Моссаду. Його термін збігся з найвищою ескалацією на Близькому Сході. Найгучнішими операціями стали:

- Вересень 2024 р. – масова атака на пейджери та рації Хезболли. Тисячі пристроїв, які Моссад таємно виробляв і впроваджував протягом понад 10 років через підставні компанії, одночасно вибухнули, спричинивши тисячні втрати та хаос у лавах терористичної організації [33;40].

- Червень 2025 р. – операція «Rising Lion» («Ревучий лев») – серія превентивних ударів по ядерних об’єктах Ірану.
- Лютий–березень 2026 р. – операція «Eric Fury» («Епічна лють»), відома також як «Дванадцятиденна війна». Моссад забезпечив проникнення всередину Ірану, встановлення таємних дрон–баз, саботаж систем ППО, ліквідацію Верховного лідера Алі Хаменеї, керівництва Корпусу вартових ісламської революції (IRGC) та ключових ядерних об’єктів у Тегерані, Натанзі та Ісфахані. Це була перша в історії операція такого масштабу, проведена розвідслужбою на території головної держави–супротивника в умовах відкритої війни [9;10;27].

Барнеа неодноразово заявляв, що «місія Моссаду щодо Ірану буде завершена лише зі зміною режиму в Тегерані». Служба активно використовувала комбінацію агентурної роботи, кібероперацій, дронів та спеціальних підрозділів безпосередньо на іранській території.

Роман Гофман (з червня 2026 р.) Призначений у грудні 2025 року і вступив на посаду в червні 2026 р. Гофман продовжує лінію попередників в умовах збереження високої напруженості на Близькому Сході після припинення вогню з Іраном. Його пріоритетом залишається закріплення технологічної переваги та запобігання відновленню іранської ядерної програми.

Ключові зміни в структурі та методах діяльності:

- Створення потужних кібер–підрозділів і інтеграція штучного інтелекту.
- Перетворення «Кідон» на високотехнологічну одиницю, що поєднує фізичні та кібероперації.
- Глибоке проникнення в ланцюги постачання супротивників (приклад – пейджери Хезболли).
- Перехід від концепції «війна між війнами» до повноцінної наступальної доктрини під час активних бойових дій.

Завдання Моссаду на сучасному етапі:

1. Повна нейтралізація іранської ядерної та ракетної загрози.

2. Дестабілізація «вісі опору» (Хезболла, ХАМАС, хусити, проіранські угруповання).
3. Забезпечення технологічної та оперативної переваги Ізраїлю.
4. Збір інформації глобального масштабу та підтримка стратегічних союзників.

Таким чином, у 2024–2026 рр. Моссад продемонстрував новий рівень операційних можливостей – здатність проводити масштабні превентивні удари по території головного стратегічного супротивника (Іран) в умовах відкритої регіональної ескалації. Служба продовжує залишатися одним із головних інструментів забезпечення національної безпеки Ізраїлю в умовах перманентної гібридної та конвенційної загрози.

Аналіз основних етапів становлення і розвитку Моссаду дозволяє зробити висновок, що ця служба пройшла унікальний шлях еволюції – від невеликого координаційного інституту, створеного 13 грудня 1949 року за ініціативи Давида Бен-Гуріона, до однієї з найефективніших високотехнологічних розвідувально-оперативних машин сучасності станом на 2026 рік.

Перший етап (1949–1952 рр., Реувен Шілоах) став періодом закладання організаційних фундаментів: створення координаційного механізму між існуючими розвідслужбами та вирішення найнагальніших завдань – масової імміграції євреїв (операція «Езра і Нехемія»).

Другий етап (1952–1963 рр., Ісер Гарель) ознаменувався професіоналізацією служби. Було сформовано систему відбору та підготовки кадрів, запроваджено принцип «Never Again», проведено одну з найзнаменитіших операцій в історії розвідки – викрадення Адольфа Ейхмана (1960).

Третій етап (1963–1974 рр., Меїр Аміт і Цві Замір) став епохою бойового хрещення. Моссад забезпечив розвідувальну перевагу в Шестиденній війні (1967) і після мюнхенської трагедії 1972 року запустив операцію «Гнів Божий», створивши елітний підрозділ «Кідон». Саме тоді служба остаточно перейшла від оборонної до активної наступальної моделі.

Четвертий етап (1974–2002 рр.) поєднав масштабні гуманітарні операції (порятунок десятків тисяч ефіопських євреїв у рамках операцій «Мойсей» і «Соломон») з інтенсивною боротьбою проти тероризму та протидією ядерним програмам Іраку й Ірану. Попри окремі оперативні та дипломатичні провали, Моссад підтвердив свою універсальність.

П'ятий (сучасний) етап (2002–2026 рр., Меїр Даган, Тамір Пардо, Йосі Коен, Давид Барнеа, Роман Гофман) став періодом технологічної революції та гібридної війни. Моссад інтегрував кібер-, дрон- та інформаційні технології, перейшов до комплексних превентивних операцій. Ключовими віхами стали Stuxnet, серія ліквідацій іранських ядерників, масова атака на пейджери та рації Хезболли (вересень 2024 р.), операція «Rising Lion» (2025 р.) та операція «Eric Fury» («Дванадцятиденна війна», лютий–березень 2026 р.), у ході якої Моссад забезпечив проникнення всередину Ірану, ліквідацію ключових фігур режиму та знищення ядерних об'єктів. Саме в цей період служба продемонструвала здатність проводити масштабні наступальні операції безпосередньо на території головного стратегічного супротивника в умовах відкритої регіональної ескалації [9;10;25;41].

Протягом усього свого існування Моссад зберігав незмінні ключові принципи, які забезпечують його виняткову ефективність:

- пряме підпорядкування лише прем'єр-міністру (максимальна оперативна автономія та мінімальна бюрократія);
- принцип випереджального удару та превентивних дій;
- поєднання класичної агентурної роботи з високими технологіями;
- жорсткий відбір, елітна підготовка кадрів і культура навчання на помилках;
- готовність діяти в умовах високого ризику задля стратегічних інтересів держави.

Завдання організації еволюціонували від координації та організації імміграції до глобального збору інформації, проведення спеціальних операцій,

контртероризму, запобігання ядерній загрозі та забезпечення технологічної переваги Ізраїлю в умовах гібридної війни.

Отже, історія Моссаду є яскравим прикладом того, як відносно невелика за ресурсами, але високоадаптивна, мотивована та технологічно оснащена розвідслужба може забезпечувати стратегічну перевагу державі, яка десятиліттями перебуває в умовах екзистенційної загрози. Цей досвід набуває особливого практичного значення для України, яка з 1991 року зіштовхується з тривалою гібридною агресією Російської Федерації і потребує ефективних моделей реформування системи національної безпеки.

1.2. Зміни в структурі та напрямках діяльності: сучасний період організації та діяльності Моссаду

Сучасний період діяльності Моссаду (2002–2026 рр.) є етапом найглибшої трансформації за всю історію служби. Якщо в попередні десятиліття Моссад переважно діяв як класична агентурна розвідка з акцентом на фізичні спеціальні операції та вербування джерел, то сьогодні це високотехнологічна гібридна структура, яка поєднує кібернетичні, дроніві, інформаційні та традиційні оперативні можливості в єдиному комплексі. Ця трансформація була зумовлена зміною характеру головних загроз для Ізраїлю: від палестинського тероризму та арабських держав до іранської ядерної програми, гібридної війни «вісі опору» та високотехнологічних викликів ХХІ століття.

Реформи структури та напрямків діяльності відбувалися поступово, але найбільш інтенсивно – з 2002 року під керівництвом Меїра Дагана і досягли піку в 2021–2026 рр. за часів Давида Барнеа. Головними драйверами змін стали: необхідність протидії іранській ядерній програмі, розвиток кіберзагроз, поява нових технологій (ШІ, дрони, квантові технології) та перехід від «війни між війнами» до активних наступальних дій під час відкритої регіональної ескалації [9;10;27].

1.2.1. Загальні тенденції трансформації організаційної структури

Організаційна структура Моссаду в сучасний період (2002–2026 рр.) зазнала найглибшої трансформації за всю історію служби. Якщо в попередні десятиліття Моссад був класичною ієрархічною розвідувальною організацією з чітким розподілом між оперативними, аналітичними та технічними підрозділами, то сьогодні це гнучка, високотехнологічна гібридна структура, в якій традиційні методи розвідки органічно інтегровані з кібернетичними, дронними, штучним інтелектом та інформаційними операціями [9;10]. Ця трансформація не була разовою реформою, а стала результатом поступового, але системного процесу адаптації до нових геополітичних і технологічних реалій.

Головними причинами структурних змін стали:

- Зміна характеру стратегічних загроз. Головним супротивником Ізраїлю з початку 2000-х років стала Ісламська Республіка Іран з її ядерною програмою, ракетним потенціалом і мережею проксі-угруповань («вісь опору»). Класичні методи вербування агентури вже не могли забезпечити необхідну швидкість і глибину проникнення [9;10].
- Технологічна революція. Поява кіберзброї, автономних дронів, штучного інтелекту та великих даних вимагала кардинальної перебудови структури. Технологічні підрозділи перестали бути допоміжними і стали рівноправними учасниками оперативного планування [25;33].
- Зміна характеру бойових дій. Перехід від традиційних війн до гібридних конфліктів вимагав створення структур, здатних діяти в режимі реального часу та поєднувати фізичні і віртуальні операції в єдиному циклі.
- Політична воля керівництва. Кожен директор (від Меїра Дагана до Давида Барнеа) отримував від прем'єр-міністра чітке завдання – максимально підвищити оперативну ефективність і зменшити бюрократичні бар'єри [9;10].

Серед ключових загальних тенденцій трансформації можна виділити такі:

1. Перехід від жорсткої вертикальної ієрархії до проектно-матричної моделі управління. Замість статичних відділів, які десятиліттями працювали автономно, Моссад почав формувати тимчасові міжфункціональні бойові

групи (task forces). Кожна така група складається з оперативників Tzomet, кіберфахівців Keshet, аналітиків і спеціалістів «Кідон». Це дозволяє значно скоротити час від отримання інформації до її реалізації в операції. Така модель була успішно апробована під час підготовки та проведення операції з пейджерів Хезболли (2024) і операції «Epic Fury» (2026) [9;10;41].

2. Інтеграція технологічного компоненту як рівноправного елемента структури. До 2010-х років технічні та кібер-підрозділи виконували допоміжну роль. Сьогодні вони є повноцінними учасниками планування операцій. Кібер-управління Keshet отримало статус, аналогічний оперативним відділам, а технологічний департамент бере участь у всіх стратегічних проєктах [9;10;25].
3. Значне посилення і модернізація спеціальних операцій. Підрозділ «Кідон» (в рамках Komemiyut) пройшов глибоку трансформацію. Сьогодні це не лише група ліквідаторів, а високотехнологічна одиниця, яка поєднує фізичні дії з кібер- та дронними можливостями. «Кідон» став ключовим інструментом превентивних операцій проти Ірану [9;10;27].
4. Розширення і переосмислення ролі міжнародного блоку. Відділ Tevel перетворився з каналу дипломатичного ліагону на потужний інструмент координації спільних операцій з союзниками (США, країни Авраамових угод, Велика Британія, Німеччина). Це дозволило Моссаду отримати доступ до додаткових технологій і розвідувальних ресурсів [9;10].
5. Посилення ролі стратегічного аналізу та прогнозування. Аналітичний департамент став обов'язковим учасником кожного етапу планування операцій. Сучасний Моссад приділяє велику увагу не лише збору інформації, але й її глибокому аналізу з використанням штучного інтелекту.
6. Зменшення бюрократії та посилення оперативної автономії. Пряме підпорядкування прем'єр-міністру дозволяє Моссаду швидко приймати рішення без зайвих погоджень. Це один із ключових факторів, що відрізняє Моссад від більш бюрократизованих розвідслужб інших країн [9;26;14].

У результаті цих тенденцій Моссад перетворився на гнучку, адаптивну і високоінтегровану структуру, здатну швидко реагувати на нові загрози і проводити складні багатокомпонентні операції. Саме завдяки цим структурним змінам служба змогла реалізувати такі знакові операції, як атака на пейджери Хезболли (2024), операцію «Rising Lion» (2025) та операцію «Epic Fury» (2026) [41].

Таким чином, загальні тенденції трансформації організаційної структури Моссаду в сучасний період свідчать про перехід від традиційної розвідувальної моделі до високотехнологічної гібридної системи, орієнтованої на випереджальні та наступальні дії. Ця трансформація стала ключовим фактором збереження стратегічної переваги Ізраїлю в умовах складних геополітичних реалій Близького Сходу [9;10].

1.2.2. Реформи структури за керівництвами директорів (2002–2026 рр.)

Трансформація організаційної структури Моссаду в сучасний період відбувалася не одномоментно, а через системні реформи, які кожен новий директор здійснював відповідно до актуальних загроз і технологічних можливостей [9;10]. Кожен етап керівництва вніс суттєві зміни в організаційну модель, розподіл повноважень, взаємодію підрозділів і загальну оперативну філософію служби.

Меїр Даган (2002–2011 рр.)

Призначений Аріелем Шароном, Даган став ініціатором переходу від оборонної до активної превентивної стратегії. Він радикально перебудував внутрішню структуру, створивши міжвідомчі оперативні групи, до яких входили представники Моссаду, АМАН і технологічних підрозділів. Головним нововведенням стало значне посилення підрозділу спеціальних операцій «Кідон» (в рамках Komemiyut) та створення постійних робочих груп для реалізації антиіранських проєктів. Даган зменшив бюрократичні бар'єри, надавши оперативним керівникам більшу самостійність у прийнятті рішень. Саме за його часів технологічний департамент почав переходити з допоміжної ролі в статус рівноправного учасника планування операцій. Реформи Дагана

дозволили Моссаду перейти від збору інформації до її безпосередньої реалізації в превентивних акціях (ліквідації іранських ядерників, саботаж на об'єктах, операція Stuxnet) [9;10;25]

Тамір Пардо (2011–2016 рр.)

Пардо продовжив лінію Дагана, але зробив акцент на цифровій трансформації структури. Він створив окремі потужні кібер–управління (в рамках Keshet), які отримали статус, аналогічний класичним оперативним відділам. Було запроваджено нову модель – «інтегровані бойові групи», де кіберфахівці, аналітики та оперативники працюють в єдиному інформаційному просторі в режимі реального часу. Пардо також посилив технологічний департамент, зробивши його самостійним структурним блоком. Значно зросла роль аналітичного департаменту в оцінці ризиків і прогнозуванні. Реформи Пардо дозволили Моссаду ефективно поєднувати агентурну роботу з кіберопераціями, що стало основою для подальших гібридних кампаній [10;23].

Йоссі Коен (2016–2021 рр.)

Коен, який до призначення очолював відділ Tzomet (вербування агентури), здійснив стратегічну реорганізацію, спрямовану на довгострокове планування. Він значно посилив Tzomet, створивши спеціалізовані групи для роботи в Ірані та Лівані. Коен запустив кілька масштабних стратегічних проєктів, серед яких – довгострокова операція з впровадження пейджерів та рацій у мережу Хезболли. Під його керівництвом відбулася подальша інтеграція підрозділів: «Кідон» почав системно працювати в тісній координації з кібер– та технічними відділами. Було розширено міжнародний блок Tevel, який став не лише каналом ліазону, а й інструментом координації спільних операцій з союзниками. Реформи Коена зробили структуру більш гнучкою та орієнтованою на складні, багатоступеневі операції [10;41].

Давид Барнеа (2021–червень 2026 рр.)

Барнеа, колишній командир елітного підрозділу Сайєрет Маткаль, завершив формування повноцінної гібридної моделі Моссаду. Він остаточно впровадив проєктно–матричну систему управління: для кожної великої операції

створюється окрема бойова група, яка діє автономно під безпосереднім контролем директора. Барнеа максимально посилив інтеграцію всіх підрозділів – Tzomet, Keshet, Komemiyut («Кідон») і технологічного департаменту працюють як єдиний механізм. Саме за його керівництва були реалізовані наймасштабніші операції сучасності: масова атака на пейджери та рації Хезболли (вересень 2024 р.), операція «Rising Lion» (2025 р.) та операція «Epic Fury» («Дванадцятиденна війна», лютий–березень 2026 р.) [41]. Барнеа також провів оптимізацію структури, зменшивши кількість проміжних ланок і посиливши прямий контроль директора над ключовими проектами.

Роман Гофман (з червня 2026 р.) Призначений у грудні 2025 року і вступив на посаду в червні 2026 р. Гофман продовжує лінію попередників в умовах збереження високої напруженості на Близькому Сході.

Його перші кроки спрямовані на закріплення досягнутої гібридної моделі та подальшу інтеграцію штучного інтелекту в процеси планування та виконання операцій. Реформи Гофмана поки що знаходяться на початковій стадії, але вже спрямовані на максимальну адаптацію структури до нових технологічних і геополітичних реалій.

Таким чином, реформи структури Моссаду за керівництвами директорів 2002–2026 рр. мали чітку логіку: від активізації превентивних операцій (Даган) через цифрову трансформацію (Пардо) і стратегічне планування (Коен) до повноцінної гібридної моделі (Барнеа). Кожен етап робив структуру більш гнучкою, інтегрованою та технологічно оснащеною, що дозволило Моссаду залишатися одним із найефективніших інструментів національної безпеки Ізраїлю в умовах сучасних гібридних загроз.

1.2.3. Основні напрямки діяльності Моссаду в сучасний період

У сучасний період (2002–2026 рр.) діяльність Моссаду характеризується чітко визначеними пріоритетами, які відображають зміну стратегічних загроз для Ізраїлю. Якщо раніше основним завданням була боротьба з палестинським тероризмом та арабськими державами, то сьогодні служба зосереджена на превентивній нейтралізації ядерної та ракетної загрози Ірану, протидії «вісі

опору», кібер– та гібридних операціях. Кожен напрямок діяльності зазнав суттєвої трансформації: від класичних методів до високотехнологічних гібридних кампаній, у яких агентурна робота, кібероперації, дроніві удари та інформаційна війна діють як єдиний механізм [9;10].

1. Превентивна нейтралізація ядерної та ракетної програми Ірану

Превентивна нейтралізація ядерної та ракетної програми Ірану є абсолютним стратегічним пріоритетом Моссаду з початку 2000–х років і залишається ним станом на 2026 рік. Цей напрямок діяльності став головним каталізатором усіх структурних, технологічних і оперативних трансформацій служби. Якщо раніше Моссад зосереджувався переважно на боротьбі з тероризмом і арабськими державами, то з 2002 року іранська ядерна загроза була визнана екзистенційною для існування держави Ізраїль. Саме цей напрямок зумовив перехід від класичної розвідки до комплексної гібридної стратегії, яка поєднує агентурну роботу, кібероперації, точкові ліквідації, саботаж і довгострокове планування.

Стратегічна мета Моссаду в цьому напрямку сформульована чітко: не допустити створення Іраном ядерної зброї або максимально відтермінувати цей момент, паралельно послаблюючи ракетний потенціал і військову інфраструктуру Тегерана. Для досягнення цієї мети служба використовує весь спектр доступних інструментів – від глибокої агентурної розвідки до кіберсаботажу та фізичних спецоперацій [9;10].

Хронологія ключових етапів протидії іранській ядерній програмі

- 2002–2011 рр. (Меїр Даган) – початок активної фази. Моссад перейшов від моніторингу до прямих превентивних дій. Було проведено серію ліквідацій ключових іранських вчених–ядерників (зокрема, Масуда Алі Мохаммаді, Маджида Шахріарі, Даріуша Резайнежада). У 2010 році спільно з США реалізована операція Stuxnet – перша в історії масштабна кіберзброя, яка фізично пошкодила понад 1000 центрифуг на збагачувальному заводі в Натанзі[10;25].

- 2011–2016 рр. (Тамір Пардо) – акцент на кібер– та технічній розвідці. Продовжено ліквідації та саботажі, значно посилено моніторинг іранських об’єктів.
- 2016–2021 рр. (Йоссі Коен) – перехід до комплексного гібридного підходу. Розроблено довгострокові операції, спрямовані на ланцюги постачання іранської ядерної програми [10;41].
- 2021–2026 рр. (Давид Барнеа та Роман Гофман) – кульмінація напрямку. Здійснено низку найбільш масштабних операцій:
 1. Серія точкових ліквідацій високопоставлених іранських військових і науковців (2022–2025 рр.).
 2. Операція «Rising Lion» (червень 2025 р.) – координовані удари по ядерних об’єктах і військових базах.
 3. Операція «Epic Fury» («Дванадцятиденна війна», лютий–березень 2026 р.) – наймасштабніша акція в історії Моссаду, у ході якої служба забезпечила проникнення всередину Ірану, ліквідацію Верховного лідера Алі Хаменеї, керівництва Корпусу вартових ісламської революції (IRGC) та знищення ключових ядерних об’єктів у Тегерані, Натанзі та Ісфахані [41].

Методи та засоби, що застосовуються

Моссад використовує багатопланову стратегію:

- Агентурна розвідка (Tzomet) – проникнення в іранські наукові та військові кола.
- Кібероперації (Keshet) – саботаж систем управління, центрифуг, систем ППО.
- Спеціальні операції («Кідон») – точкові ліквідації ключових фігур.
- Технічна розвідка та дрони – моніторинг і наведення.
- Саботаж ланцюгів постачання – перехоплення та псування обладнання для ядерної програми.

Усі ці методи інтегровані в єдиний оперативний цикл, що дозволяє досягати максимального ефекту при мінімальних ризиках для ізраїльських сил.

Значення цього напрямку для Моссаду

Превентивна протидія Ірану стала каталізатором усіх сучасних реформ служби. Саме через цей напрямок Моссад:

- радикально модернізував кібер– та технічні можливості;
- створив ефективну систему міжвідомчої взаємодії з АМАНом;
- відпрацював модель довгострокових гібридних операцій;
- довів свою здатність діяти на території головного стратегічного супротивника навіть у період відкритої ескалації.

Цей напрямок діяльності остаточно закріпив за Моссадом статус наступальної стратегічної сили, а не лише розвідувальної служби.

Таким чином, превентивна нейтралізація ядерної та ракетної програми Ірану є не просто одним із напрямків роботи Моссаду, а його головною стратегічною місією у XXI столітті. Успішність дій у цьому напрямку визначає не лише безпеку Ізраїлю, але й загальний рівень оперативної майстерності та технологічної переваги всієї служби.

2. Гібридні операції проти Хезболли, ХАМАС та інших проксі–угруповань

Гібридні операції проти Хезболли, ХАМАС та інших проксі–угруповань «вісі опору» (Хусити в Ємені, шіїтські міліції в Іраку та Сирії) є другим за значенням стратегічним напрямком діяльності Моссаду в сучасний період (2002–2026 рр.). Якщо превентивна нейтралізація іранської ядерної програми спрямована на стратегічну загрозу довгострокового характеру, то боротьба з проксі–угрупованнями має переважно оперативно–тактичний вимір і спрямована на безпосереднє послаблення іранського впливу в регіоні та запобігання ракетно–терористичним атакам проти Ізраїлю.

Цей напрямок характеризується максимальною інтеграцією всіх видів розвідувальної та оперативної діяльності: агентурної (Tzomet), кібернетичної (Keshet), спеціальних операцій («Кідон» у складі Komemiyut) та міжнародної координації (Tevel). Саме тут Моссад відпрацював модель «війни між війнами» (War Between the Wars), яка передбачає постійні превентивні дії в періоди між

великими конфліктами, а з 2023–2026 рр. – і в умовах відкритої регіональної ескалації.

2. Хронологія ключових гібридних операцій

- 2006–2021 рр. – період накопичення досвіду. Моссад активно працював проти Хезболли в Лівані та ХАМАС у Секторі Газа, проводячи точкові ліквідації командирів, саботажі складів озброєння та кібератаки на системи управління.
- Вересень 2024 р. – кульмінаційна операція проти Хезболли. Моссад протягом понад 10 років таємно контролював ланцюг постачання: через підставні компанії поставляв Хезболлі тисячі пейджерів і рацій, у які були вбудовані вибухові пристрої. 17–18 вересня 2024 року одночасна детонація тисяч пристроїв спричинила тисячі поранених і вбитих, повністю дезорганізувавши командну структуру угруповання. Ця операція стала еталоном гібридної диверсії в історії розвідки.
- 2024–2025 рр. – інтенсивні операції проти ХАМАС. Після початку широкомасштабного конфлікту в Газі Моссад спільно з АМАНом і ЦАХАЛом провів низку точкових ліквідацій лідерів ХАМАС (включаючи високопоставлених командирів у Лівані, Катарі та Туреччині), саботаж тунельної інфраструктури та кібероперації з перехоплення комунікацій.
- 2025–2026 рр. – розширення на всю «вісь опору». Операції проти хуситів у Ємені, проіранських міліцій в Іраку та Сирії. У рамках операції «Еріс Fury» (лютий–березень 2026 р.) Моссад забезпечив координацію ударів по логістичних мережах, що постачають озброєння Хезболлі та ХАМАС.

2.Методи та інструменти гібридних операцій

Моссад застосовує комплексний підхід, у якому кожен елемент посилює інші:

- Довгострокове проникнення в ланцюги постачання (приклад – операція з пейджерями).
- Комбіновані кіберфізичні атаки – одночасне виведення з ладу систем зв'язку та фізичне знищення об'єктів.

- Точкові спецоперації «Кідон» – ліквідації ключових командирів за кордоном.
- Агентурна підтримка – вербування джерел усередині угруповань.
- Інформаційно–психологічні операції – поширення дезінформації для розколу та деморалізації.
- Міжнародна координація – співпраця з союзниками для моніторингу та перехоплення поставань.

Усі операції плануються та виконуються в єдиному оперативному циклі за проектно–матричною моделлю, що дозволяє значно скоротити час від отримання розвідданих до їхньої реалізації.

Значення напрямку для сучасного Моссаду

Гібридні операції проти проксі–угруповань дозволили Моссаду:

- відпрацювати технології глибокого проникнення в ланцюги постачання;
- довести ефективність комбінованого застосування агентури, кіберу та спеціальних сил;
- зміцнити взаємодію з АМАНом і Шабаком у реальному часі;
- створити прецедент, коли розвідслужба може завдавати стратегічно значущих ударів без прямого залучення регулярної армії.

Цей напрямок остаточно перетворив Моссад із класичної розвідки на повноцінний інструмент гібридної війни, здатний діяти на всій території «вісі опору» та за її межами.

Таким чином, гібридні операції проти Хезболли, ХАМАС та інших проксі–угруповань є невід’ємною складовою сучасної стратегії Моссаду.

Вони демонструють високу адаптивність служби, її здатність поєднувати довгострокове планування з блискавичними ударами та підтверджують, що Моссад сьогодні діє не лише як розвідувальна структура, а як ключовий елемент наступальної оборонної політики держави Ізраїль.

3. Глибока агентурна та технічна розвідка в країнах «вісі опору»

Глибока агентурна та технічна розвідка в країнах і угрупованнях «вісі опору» (Іран, Ліван, Сирія, Ірак, Ємен) є фундаментальною основою всіх інших

напрямків діяльності Моссаду в сучасний період. Без якісної розвідувальної інформації неможливе ефективне планування превентивних операцій, кіберсаботажів та спеціальних акцій. Саме цей напрямок забезпечує службі стратегічну глибину та оперативну перевагу над супротивником.

У сучасній структурі Моссаду цей напрямок реалізується через тісну взаємодію двох ключових підрозділів: Tzomet (агентурна розвідка) та Keshet (технічна та кіберрозвідка). Їхня синергія дозволяє отримувати як людську (HUMINT), так і технічну (SIGINT, GEOINT, CYBINT) інформацію в режимі реального часу.

Основні завдання цього напрямку:

- Вербування та довгострокове утримання джерел у військово–політичному керівництві, наукових колах та силових структурах Ірану та проксі–угруповань;
- Постійний моніторинг ядерних, ракетних та військових об'єктів;
- Виявлення ланцюгів постачання озброєння та технологій;
- Збір даних для превентивних ударів і операцій «Кідон».

Особливої ефективності Моссад досяг у 2016–2026 рр. Підрозділ Tzomet значно розширив мережу високоякісних агентів у Ірані та Лівані. Саме завдяки агентурі були отримані критичні дані, які дозволили провести успішні ліквідації іранських ядерників, операцію з пейджерями Хезболли (2024 р.) та операцію «Epic Fury» (2026 р.).

Підрозділ Keshet доповнює агентурну розвідку потужними можливостями кібернетичного проникнення, супутникового моніторингу та перехоплення комунікацій. У сучасний період значна частина інформації надходить через комбіновані HUMINT + SIGINT операції, коли агент надає доступ, а кіберфахівці Keshet проникають у внутрішні мережі.

Цей напрямок є одним із найбільш закритих і водночас найважливіших. Саме глибока розвідка дозволяє Моссаду діяти на випередження, мінімізуючи ризики для власних сил і максимізуючи точність ударів. Вона стала основою для переходу від реактивної до проактивної стратегії протидії іранській загрозі.

Таким чином, глибока агентурна та технічна розвідка в країнах «вісі опору» є невід’ємною і базовою складовою сучасної діяльності Моссаду. Її високий рівень забезпечує службі стратегічну перевагу та створює умови для успішного виконання всіх інших оперативних напрямків.

4. Кібер– та інформаційні операції

Кібер– та інформаційні операції є одним із найбільш динамічних і технологічно насичених напрямків сучасної діяльності Моссаду (2002–2026 рр.). Вони стали невід’ємною складовою всіх гібридних кампаній служби і здійснюються переважно підрозділом Keshet у тісній координації з Tzomet, Komemiyut та аналітичним департаментом.

Основні завдання цього напрямку:

- проведення кіберсаботажів критичної інфраструктури супротивника (ядерні об’єкти, системи ППО, енергетика);
- захист власних інформаційних систем та проведення контркібероперацій;
- інформаційно–психологічні операції (дезінформація, деморалізація, вплив на громадську думку в країнах «вісі опору»);
- забезпечення розвідданими в режимі реального часу через кібернетичне проникнення.

Найвідомішими операціями стали:

- участь у розробці та впровадженні Stuxnet (2010);
- численні кібератаки на іранські ядерні центрифуги та системи управління;
- кіберкомпонент операції з пейджером Хезболли (2024);
- підтримка операцій «Rising Lion» (2025) та «Epic Fury» (2026), де кібер– та інформаційні удари застосовувалися одночасно з фізичними діями.

У сучасний період Моссад активно використовує штучний інтелект, великі дані та кіберфізичні атаки, що дозволяє поєднувати віртуальний і реальний простір в єдиному оперативному циклі. Кібер– та інформаційні операції не є самостійними – вони завжди доповнюють агентурну розвідку та спеціальні акції, значно підвищуючи загальну ефективність [9;23;25].

Таким чином, кібер– та інформаційні операції перетворилися на стратегічний інструмент Моссаду, який забезпечує технологічну перевагу та дозволяє службі діяти на випередження в умовах сучасної гібридної війни.

5. Міжнародна співпраця та координація з союзниками

Міжнародна співпраця та координація з союзниками є важливим підтримуючим напрямком сучасної діяльності Моссаду і реалізується головним чином через управління Tevel. У 2002–2026 рр. цей напрямок суттєво еволюціонував: від класичного обміну інформацією до повноцінної оперативної координації спільних операцій.

Основні завдання:

- регулярний обмін розвідданими з ключовими партнерами;
- спільне планування та проведення операцій;
- отримання доступу до додаткових технологій і ресурсів;
- дипломатичне прикриття окремих акцій Моссаду.

Головними союзниками залишаються США, Велика Британія, Німеччина, а також країни Авраамових угод (ОАЕ, Бахрейн, Марокко). Саме завдяки цій співпраці Моссад отримав критично важливу технічну підтримку під час операції Stuxnet (2010), координацію дій проти Ірану в 2024–2026 рр. та логістичну допомогу в операціях «Rising Lion» і «Epic Fury» [9;10;23].

У сучасних умовах Tevel діє не лише як канал зв'язку, а як повноцінний оперативний підрозділ, що дозволяє Моссаду розширювати свої можливості за рахунок ресурсів союзників [23].

Усі перелічені напрямки діяльності не існують ізольовано – вони тісно інтегровані в єдину гібридну стратегію. Сучасний Моссад діє за принципом «єдиного бойового циклу»: розвідка → аналіз → планування → виконання → оцінка результатів. Такий підхід дозволяє службі швидко реагувати на нові загрози та проводити операції, які раніше були неможливими для традиційних розвідувальних структур.

Таким чином, основні напрямки діяльності Моссаду в сучасний період повністю відповідають новим стратегічним викликам Ізраїлю. Служба перейшла

від реактивної оборони до активної превентивної та наступальної стратегії, поєднуючи людський фактор, агентурну роботу та передові технології в єдиний ефективний механізм забезпечення національної безпеки держави.

1.2.4. Зміни в кадровій політиці, підготовці персоналу та ресурсному забезпеченні.

Одним із головних секретів ефективності сучасного Моссаду є радикальна трансформація кадрової політики, системи підготовки персоналу та ресурсного забезпечення, що відбулася протягом 2002–2026 років. Якщо раніше служба опиралася переважно на класичний відбір за критеріями патріотизму, фізичної витривалості та психологічної стійкості, то сьогодні пріоритетом стали високі інтелектуальні здібності, технологічна грамотність, креативність і здатність працювати в умовах швидкозмінних гібридних загроз. Ці зміни дозволили Моссаду залучати та утримувати елітних фахівців, конкурентних із приватним технологічним сектором Ізраїлю [9;23].

Зміни в системі відбору та рекрутингу

Сучасна система відбору в Моссад є однією з найжорсткіших у світі. Процес складається з кількох етапів: психологічні тести, глибока перевірка біографії (включаючи всіх близьких родичів), симуляції реальних оперативних ситуацій, інтерв'ю з психологами та колишніми оперативниками, а також поліграф. За оцінками, лише 1–2 % кандидатів проходять повний цикл відбору [9;23;14]. У 2010–2026 рр. до традиційних критеріїв додалися нові вимоги:

- висока технічна грамотність (програмування, кібербезпека, аналіз великих даних);
- знання кількох іноземних мов (перська, арабська, турецька, російська, китайська);
- креативне мислення та здатність до нестандартних рішень у критичних ситуаціях;
- психологічна стійкість до тривалого стресу та роботи в умовах високих технологічних ризиків.

Моссад активно використовує цільовий рекрутинг через провідні університети (Техніон, Тель-Авіський університет, Університет Бен-Гуріона), випускників елітного підрозділу 8200 ЦАХАЛ та навіть соціальні мережі [9;23]. Особлива увага приділяється спеціалістам у сфері штучного інтелекту, кіберзахисту та інженерії.

Система підготовки та навчання персоналу

Підготовка в Моссаді є багаторівневою і триває від 18 місяців до 3 років залежно від спеціалізації. Сучасна модель поєднує класичні методи з передовими технологіями:

- Базовий курс оперативної роботи (конспірація, вербування, робота під прикриттям, фізична підготовка).
- Спеціалізовані курси для кіберфахівців, аналітиків, оперативників «Кідон» та спеціалістів міжнародних операцій.
- Постійне підвищення кваліфікації (щорічні тренінги, стажування за кордоном, симуляції реальних операцій).
- Використання віртуальної та доповненої реальності (VR/AR-симулятори) для відпрацювання операцій у ворожому середовищі.
- Інтенсивне навчання роботі зі штучним інтелектом, великими даними та сучасними кіберзасобами.

Підрозділ «Кідон» проходить особливо жорстку підготовку, яка поєднує фізичні навички (Krav Maga, стрільба, тактична медицина) з сучасними технологічними засобами [9;23;25].

Мотивація персоналу та корпоративна культура

Моссад підтримує високу мотивацію завдяки комплексній системі. Крім конкурентної заробітної плати та соціальних гарантій, служба активно використовує ідеологічну мотивацію («захист держави Ізраїль», принцип «Never Again»). Корпоративна культура базується на довірі, оперативній автономії, постійному вдосконаленні та командній роботі [9;14;29]. Запроваджено програми психологічної підтримки, ротації персоналу та запобігання професійному вигоранню. Після завершення служби співробітники часто

переходять у високотехнологічні компанії, що робить кар'єру в Моссаді привабливою для талановитої молоді.

Фінансування та ресурсне забезпечення

Фінансування Моссаду здійснюється безпосередньо через офіс прем'єр-міністра і становить значну частину оборонного бюджету Ізраїлю. У 2025–2026 рр. загальний бюджет служби оцінюється в 2,7–3 млрд дол. США на рік [9;23].

Значна частина коштів спрямовується на:

- технічне оснащення та розвиток кіберінфраструктури;
- сучасні програми навчання та симулятори;
- конкурентну заробітну плату та соціальний пакет співробітників;
- придбання спеціального обладнання та створення таємних баз за кордоном.

Таке ресурсне забезпечення дозволяє Моссаду утримувати елітних фахівців і впроваджувати найсучасніші технології [9;23].

Роль технологій у підготовці персоналу

Технології кардинально змінили систему навчання. Сьогодні Моссад активно використовує:

- VR-симулятори для відпрацювання операцій у реальних умовах;
- штучний інтелект для аналізу поведінки кандидатів і моделювання сценаріїв;
- комп'ютерні платформи для тренування кібероперацій у віртуальному середовищі;
- спеціальні програми вивчення іноземних мов і культур за допомогою AI.

Це дозволяє значно скоротити час підготовки та підвищити якість навичок оперативників [9;23;25].

Таким чином, зміни в кадровій політиці, підготовці персоналу та ресурсному забезпеченні стали одним із головних чинників успіху сучасного Моссаду. Служба змогла створити високомотивовану, технологічно підковану та адаптивну команду, здатну ефективно виконувати найскладніші завдання в

умовах сучасної гібридної війни. Цей досвід має велике практичне значення для реформування кадрової політики українських спецслужб.

Аналіз сучасного періоду (2002–2026 рр.) свідчить, що Моссад здійснив одну з найглибших і найуспішніших трансформацій за всю свою історію. Служба перейшла від класичної агентурної розвідки з акцентом на фізичні операції до високотехнологічної гібридної структури, здатної ефективно поєднувати агентурну роботу, кібероперації, дроніві удари, інформаційну війну та спеціальні операції в єдиному комплексі.

Головними тенденціями трансформації стали:

- перехід від жорсткої ієрархічної моделі до гнучкої проектно–матричної системи управління;
- інтеграція технологічного компонента (кібер–, дроніві та штучний інтелект) як рівноправного елемента структури;
- значне посилення спеціальних операцій («Кідон») та їхня тісна інтеграція з технічними підрозділами;
- реформи кадрової політики, які дозволили залучати та утримувати висококваліфікованих фахівців із технологічного сектору;
- суттєве збільшення ресурсного забезпечення та фінансування.

Ці зміни відбувалися послідовно під керівництвом Меїра Дагана, Таміра Пардо, Йоссі Коена, Давида Барнеа та Романа Гофмана. Кожен директор вніс свій внесок: від переходу до превентивної стратегії (Даган) через цифрову трансформацію (Пардо) до повноцінної гібридної моделі (Барнеа).

У результаті Моссад став значно ефективнішим у вирішенні ключових завдань сучасного періоду: превентивній нейтралізації ядерної загрози Ірану, протидії «вісі опору», проведенні складних гібридних операцій та забезпеченні технологічної переваги держави. Яскравим підтвердженням цього стали операції з пейджерями Хезболли (2024), «Rising Lion» (2025) та «Epic Fury» (2026), які продемонстрували новий рівень оперативних можливостей служби.

Таким чином, сучасний Моссад – це не просто розвідувальна служба, а стратегічний наступальний інструмент держави, що поєднує високу оперативну

автономію, передові технології та елітний кадровий потенціал. Проведені структурні, кадрові та ресурсні реформи забезпечили службі адаптивність і ефективність у умовах сучасної гібридної війни.

1.3. Основні структурні підрозділи Моссаду та їхня функціональна спрямованість. Взаємодія Моссаду з іншими спецслужбами Ізраїлю

Сучасна організаційна структура Моссаду (станом на 2026 рік) є одним із найбільш складних і ефективних механізмів серед усіх світових розвідувальних служб. Вона кардинально відрізняється від моделі 1950–1990-х років і відображає глибоку трансформацію, що відбулася протягом останніх двох десятиліть. Якщо раніше Моссад функціонував як відносно традиційна ієрархічна розвідувальна організація з чітким розподілом між оперативними, технічними та аналітичними блоками, то сьогодні це високотехнологічна гібридна система, в якій усі підрозділи тісно інтегровані в єдині бойові групи, здатні швидко реагувати на динамічні загрози та проводити складні багатокомпонентні операції [9;10;23].

Офіційно повна схема структури Моссаду залишається однією з найбільш засекречених у світі. Однак завдяки аналізу відкритих джерел, мемуарів колишніх директорів і оперативників, характеру проведених операцій (зокрема, операції з пейджером Хезболли 2024 року, операції «Rising Lion» 2025 року та операції «Eric Fury» 2026 року), а також матеріалів спеціальних розслідувань і заяв високопосадовців можна досить точно реконструювати ключові структурні підрозділи та їхню функціональну спрямованість. Головною особливістю сучасної моделі є максимальна інтеграція традиційних оперативних, технічних, аналітичних і спеціальних підрозділів, що дозволяє Моссаду діяти за принципом «єдиного бойового циклу»: від отримання інформації до її негайної реалізації в операції.

Така структура забезпечує три ключові переваги:

- швидкість прийняття рішень і виконання завдань;
- синергію між різними видами розвідки (агентурна, кібер-, технічна);

- високу адаптивність до мінливих умов гібридної війни.

У цьому підрозділі детально розглядаються основні структурні підрозділи Моссаду, їхня функціональна спрямованість у сучасний період, а також механізми взаємодії служби з іншими ключовими ізраїльськими спецслужбами – Шабак (Шин–Бет) та АМАН. Розуміння цієї структури та системи взаємодії має важливе практичне значення для розуміння того, як Моссад досягає виняткової ефективності при відносно невеликій чисельності персоналу та як цей досвід може бути адаптований до реформування українських спецслужб.

1.3.1. Основні структурні підрозділи Моссаду та їхня функціональна спрямованість.

Організаційна структура Моссаду (станом на 2026 рік) є однією з найскладніших і найефективніших серед світових розвідувальних служб. Вона кардинально відрізняється від моделі 1950–1990-х років і відображає глибоку трансформацію, що відбулася протягом 2002–2026 рр. Якщо раніше Моссад функціонував як відносно традиційна ієрархічна розвідувальна організація з чітким розподілом між оперативними, технічними та аналітичними блоками, то сьогодні це високотехнологічна гібридна система, в якій усі підрозділи тісно інтегровані в єдині бойові групи, здатні швидко реагувати на динамічні загрози та проводити складні багатокомпонентні операції.

Офіційно повна схема структури Моссаду залишається однією з найбільш засекречених у світі. Однак аналіз відкритих джерел, мемуарів колишніх директорів і оперативників, характеру проведених операцій (зокрема, атаки на пейджери та рації Хезболли у вересні 2024 року, операції «Rising Lion» у червні 2025 року та операції «Eric Fury» («Дванадцятиденна війна») у лютому–березні 2026 року), а також матеріалів спеціальних розслідувань і заяв високопосадовців дозволяє досить точно реконструювати ключові структурні підрозділи та їхню функціональну спрямованість у сучасний період.

Головною особливістю сучасної моделі є максимальна інтеграція традиційних оперативних, технічних, аналітичних і спеціальних підрозділів. Замість автономних відділів Моссад використовує принцип проектно–

матричного управління: для кожної великої операції створюється тимчасова міжфункціональна бойова група, яка діє автономно під безпосереднім контролем директора або його заступника. Це забезпечує три ключові переваги: швидкість прийняття рішень, синергію між різними видами розвідки та високу адаптивність до умов гібридної війни [9;10;23].

Усі ключові підрозділи підпорядковуються безпосередньо директору Моссаду, що гарантує мінімальну бюрократію та максимальну оперативну автономію. Нижче наведено детальний опис основних структурних одиниць та їхньої функціональної спрямованості в сучасний період.

Tzomet («З'єднання») – один із найбільш елітних і закритих підрозділів Моссаду, який відповідає за вербування, підтримку та довгострокову роботу з агентурою за кордоном. У 2010–2026 рр. Tzomet значно розширив свою діяльність у найскладніших цільових країнах – Ірані, Лівані, Сирії, Іраку та країнах Перської затоки. Підрозділ спеціалізується на створенні глибоких агентурних мереж серед високопоставлених посадовців, вчених–ядерників, військових командирів та представників технологічного сектору. Саме Tzomet забезпечував агентурну підтримку багатьох ключових операцій проти іранської ядерної програми, а також підготовку та реалізацію операції з пейджерями Хезболли (2024). У сучасний період Tzomet активно використовує сучасні технології психологічного профілювання, цифрову аналітику, штучний інтелект та великі дані для відбору потенційних джерел. Робота підрозділу характеризується високим рівнем конспірації та тривалим циклом вербування (іноді 5–10 років) [9;10;23].

Keshet («Веселка») – центральне управління технічної та кіберрозвідки. Це один із найбільш динамічно розвиваючихся підрозділів, який у 2010–х роках отримав статус, рівний оперативним управлінням. Keshet відповідає за електронну розвідку, розробку та впровадження шкідливого програмного забезпечення, кіберсаботаж критичної інфраструктури супротивника, захист власних комунікацій та збір даних з відкритих і закритих джерел. Підрозділ відіграв ключову роль в операції Stuxnet (2010), підготовці кіберкомпоненту

операції «Eric Fury» (2026) та багатьох інших гібридних акціях. Сьогодні Keshet тісно інтегрований з іншими управліннями і бере участь у плануванні операцій на всіх етапах – від розвідки до безпосередньої реалізації. У 2020–х роках підрозділ значно розширив можливості у сфері кіберфізичних операцій (поєднання кібератак з фізичними діями) [9;23;25].

Komemiyut («Незалежність») / Підрозділ «Кідон» – управління спеціальних операцій, яке включає легендарний підрозділ «Кідон» (Bayonet). У сучасний період «Кідон» пройшов глибоку модернізацію: сьогодні це не лише група фізичних виконавців, а високотехнологічна одиниця, яка поєднує класичні методи ліквідацій і диверсій з кібер-, дронними та інформаційними можливостями. Підрозділ безпосередньо брав участь у ліквідаціях іранських ядерників, операції з пейджером Хезболли (2024), операції «Rising Lion» (2025) та багатьох превентивних акціях 2025–2026 рр. Komemiyut тісно співпрацює з Tzomet і Keshet, формуючи єдині оперативні групи для виконання найскладніших завдань. У 2020–х роках підрозділ отримав розширені повноваження для проведення операцій на території супротивника в умовах активних бойових дій [9;10;14].

Tevel («Всесвіт») – управління міжнародних зв'язків і ліазону. У сучасний період Tevel перетворився з чисто дипломатичного каналу на потужний інструмент координації спільних операцій з іноземними розвідками (США, Велика Британія, Німеччина, країни Авраамових угод). Підрозділ відповідає за обмін розвідданими, спільне планування операцій та отримання доступу до додаткових технологій і ресурсів союзників. Tevel відіграв важливу роль у підготовці Авраамових угод та координації дій з США під час операцій проти Ірану в 2025–2026 рр. У сучасних умовах Tevel також виконує функції прикриття та логістичної підтримки операцій за кордоном [9;23].

Аналітичний департамент та управління стратегічних досліджень – підрозділ, який відповідає за глибокий аналіз зібраної інформації, стратегічне прогнозування загроз і підготовку доповідей безпосередньо для прем'єр-міністра. У сучасний період цей департамент активно використовує штучний

інтелект і великі дані, що дозволяє значно підвищити точність прогнозів. Аналітики беруть участь у плануванні всіх значних операцій на ранніх етапах і забезпечують наукову обґрунтованість рішень [9;23].

Технологічний департамент – відносно новий, але один із найбільш впливових структурних блоків. Відповідає за розробку власних технологічних рішень, інтеграцію штучного інтелекту, дронів систем, квантових технологій та інших інновацій у повсякденну діяльність служби. Саме цей департамент забезпечував технічну сторону операції з пейджерами Хезболли та багатьох кібероперацій 2024–2026 рр [9;23;25].

Усі перелічені підрозділи працюють у тісній інтеграції, утворюючи єдину гібридну систему. Така організаційна модель дозволяє Моссаду швидко реагувати на нові загрози та проводити операції, які раніше були неможливими для традиційних розвідслужб.

1.3.2. Взаємодія Моссаду з іншими спецслужбами Ізраїлю

Система національної безпеки Ізраїлю побудована на принципі трьох спеціалізованих розвідувальних і контррозвідувальних відомств, які діють у тісній координації, але з чітким розподілом сфер відповідальності. Моссад (зовнішня розвідка та спеціальні операції за кордоном), Шабак (Шин–Бет – внутрішня контррозвідка та антитерористична діяльність усередині країни) та АМАН (військова розвідка ЦАХАЛ) формують єдиний трикутник, ефективність якого є одним із ключових факторів виживання та стратегічної переваги Ізраїлю в умовах постійних гібридних і конвенційних загроз.

Взаємодія між цими трьома службами не є формальною – вона має глибоко інституціоналізований характер і регулюється безпосередньо офісом прем'єр-міністра [9;23;14]. Така модель дозволяє уникнути конкуренції, дублювання функцій і водночас забезпечує швидку та ефективну реалізацію спільних операцій. У сучасний період (2020–2026 рр.) взаємодія набула особливої інтенсивності через ескалацію загроз з боку Ірану, Хезболли та ХАМАС.

Загальна система координації трьох спецслужб

Система координації між трьома головними спецслужбами Ізраїлю – Моссадом, Шабакком (Шин–Бет) та АМАНом – є однією з найефективніших і найбільш централізованих моделей у світі. Вона побудована на принципі єдиного командного центру під безпосереднім керівництвом прем'єр–міністра, що дозволяє уникнути міжвідомчої конкуренції, дублювання функцій і бюрократичних затримок, які часто спостерігаються в інших країнах. Така модель координації була сформована ще в 1950–х роках і з часом тільки посилювалася, особливо після 2002 року, коли загроза з боку Ірану та «вісі опору» стала головним стратегічним викликом для держави [9;23;14].

Конституційно–правова основа координації

Хоча в Ізраїлі немає єдиного закону, який би детально регулював взаємодію спецслужб, ключові положення закріплені в кількох нормативних актах:

- Закон про прем'єр–міністра (1968, зі змінами);
- Закон про Раду національної безпеки (2008, зі змінами 2018–2022 рр.);
- Секретні директиви прем'єр–міністра, які мають силу нормативних актів (так звані «прем'єрські директиви»).

Прем'єр–міністр Ізраїлю є головним координатором усієї системи національної безпеки. Він особисто затверджує найважливіші операції, призначає директорів усіх трьох служб і визначає пріоритети їхньої діяльності. Така централізація є ключовою відмінністю ізраїльської моделі від, наприклад, американської, де існує значно більша автономія окремих відомств.

Рада національної безпеки (National Security Council – NSC)

Центральним інституційним органом координації є Рада національної безпеки при прем'єр–міністрі. Вона була створена у 1999 році і значно посилена після 2008 року. До складу Ради входять:

- Прем'єр–міністр (голова);
- Міністр оборони;
- Міністр закордонних справ;
- Директор Моссаду;

- Директор Шабаку;
- Начальник АМАНу;
- Начальник Генерального штабу ЦАХАЛ;
- Голова Національного центру кібербезпеки.

Рада збирається регулярно (щотижнево або в режимі кризового засідання)

і виконує такі функції:

- формування єдиної стратегії національної безпеки;
- координація оперативної діяльності трьох служб;
- затвердження спільних операцій;
- розподіл ресурсів і повноважень між відомствами;
- аналіз ризиків і прогнозування загроз [9;23].

Під час проведення великих операцій (наприклад, «Epic Fury» 2026 року) у Раді створюється оперативний штаб (Situation Room), де представники Моссаду, Шабаку та АМАН працюють у режимі 24/7.

Механізми повсякденної координації

1. Міжвідомчі оперативні групи (Joint Task Forces) Для конкретних операцій або напрямків загроз створюються тимчасові або постійні спільні групи. У них входять представники всіх трьох служб, а іноді й представники ЦАХАЛ та Міністерства закордонних справ.
2. Спільні розвідувальні комітети. Регулярні засідання керівників Моссаду, Шабаку та АМАНу під головуванням радника прем'єр-міністра з питань національної безпеки.
3. Система обміну інформацією. Існує єдина захищена платформа обміну розвідданими, до якої мають доступ керівники всіх трьох служб. Це дозволяє уникнути «інформаційного голодування» і забезпечує швидку реакцію.
4. Прямий доступ до прем'єр-міністра. Директори Моссаду, Шабаку та АМАНу мають право на термінову зустріч з прем'єр-міністром у будь-який час.

Приклади ефективної координації в сучасний період (2024–2026 рр.)

- Операція з пейджерями Хезболли (вересень 2024): Моссад відповідав за технічну та логістичну підготовку, АМАН – за розвідку та прикриття, Шабак – за запобігання можливим відповідним терактам на території Ізраїлю.
- Операція «Rising Lion» (червень 2025): Створено об'єднаний штаб Моссаду та АМАНу, Шабак забезпечував внутрішню стабільність.
- Операція «Epic Fury» («Дванадцятиденна війна», лютий–березень 2026): Наймасштабніший приклад координації – Моссад забезпечував глибоке проникнення, АМАН – повітряну та кібер–підтримку, Шабак – контррозвідувальне прикриття на території Ізраїлю.

Переваги та недоліки системи

Переваги:

- Швидкість і гнучкість прийняття рішень.
- Відсутність значної міжвідомчої конкуренції.
- Можливість концентрації ресурсів на пріоритетних напрямках.
- Висока ефективність спільних операцій.

Недоліки та виклики:

- Надмірна централізація може призводити до перевантаження прем'єр–міністра.
- Різні корпоративні культури служб іноді викликають тертя.
- Необхідність постійного контролю з боку прем'єр–міністра.

Загалом система координації трьох спецслужб Ізраїлю є унікальною моделлю, яка дозволяє невеликій державі ефективно протистояти значно потужнішим супротивникам. Саме завдяки цій системі Моссад, Шабак і АМАН діють як єдиний, добре налагоджений механізм національної безпеки.

Шабак (Шин–Бет) та його взаємодія з Моссадом

Шабак (офіційна назва – Шин–Бет, Shin Bet або Shabak – від Sherut ha–Bitachon ha–Klali, Загальна служба безпеки) є внутрішньою контррозвідувальною та антитерористичною службою Ізраїлю. Створений у 1948 році одночасно з проголошенням незалежності держави, Шабак традиційно

вважається «молодшим братом» Моссаду, але виконує абсолютно критичні функції для внутрішньої стабільності країни [26;27;23].

Основні функції та сфера відповідальності Шабак

Шабак відповідає за:

- внутрішню контррозвідку та боротьбу з тероризмом на території Ізраїлю, Західного берега річки Йордан та Сектору Газа;
- захист державних установ, дипломатичних представництв, ядерних об'єктів і ключової інфраструктури;
- роботу з арабським населенням Ізраїлю та окупованих територій (виявлення та нейтралізацію терористичних осередків);
- запобігання проникненню ворожої агентури та проведення контррозвідувальних операцій усередині країни;
- кіберконтррозвідку та боротьбу з тероризмом у соціальних мережах і цифровому просторі;
- забезпечення безпеки під час масових заходів і захист високопосадовців.

На відміну від Моссаду, який діє переважно за кордоном, Шабак має широкі повноваження на території Ізраїлю, включаючи право на адміністративне затримання, прослуховування, контроль за переміщенням і використання спеціальних оперативних заходів [9;23;18].

Специфіка взаємодії Шабак з Моссадом

Взаємодія між Моссадом і Шабак є однією з найтісніших і найпродуктивніших у системі національної безпеки Ізраїлю. Вона має постійний і інституціоналізований характер і відбувається за кількома ключовими напрямками:

1. Обмін оперативною та агентурною інформацією. Моссад передає Шабак дані про підготовку терористичних атак, які можуть бути реалізовані на території Ізраїлю або окупованих територій (особливо щодо ХАМАС і Хезболли). Шабак, у свою чергу, інформує Моссад про внутрішні тенденції, вербування агентів та можливі «зворотні» загрози.

2. Спільні антитерористичні операції. Під час підготовки великих операцій Моссаду за кордоном Шабак бере на себе забезпечення внутрішньої безпеки та запобігання відповідним терактам. Класичний приклад – операція з пейджерями Хезболли (вересень 2024 р.): Моссад провів технічну та логістичну підготовку, а Шабак посилив заходи безпеки всередині Ізраїлю та на окупованих територіях, щоб уникнути ескалації.
 3. Контррозвідувальне прикриття операцій Моссаду. Перед проведенням складних операцій за кордоном Моссад обов'язково залучає Шабак для перевірки можливих витоків інформації всередині країни та нейтралізації потенційних «кротів».
 4. Спільна робота з ХАМАС та Хезболлою. Оскільки ХАМАС діє як на території Гази, так і має розгалужену мережу в Ізраїлі, а Хезболла активно вербує агентів серед арабського населення, Моссад і Шабак створюють спільні оперативні групи для нейтралізації цих загроз.
 5. Кіберконтррозвідка та цифровий тероризм. У сучасний період (2020–2026 рр.) спільна робота значно посилилася в цифровій сфері. Шабак відповідає за моніторинг соціальних мереж і месенджерів усередині країни, а Моссад – за зовнішні джерела. Їхні підрозділи регулярно обмінюються даними.
Конкретні приклади взаємодії (2024–2026 рр.)
 - Після операції з пейджерями Хезболли (вересень 2024) Шабак негайно посилив заходи безпеки на півночі Ізраїлю та в арабських містах, запобігши можливим відповідним терактам.
 - Під час операції «Еріс Fury» (лютий–березень 2026) Шабак забезпечував внутрішню стабільність і контррозвідувальне прикриття, тоді як Моссад проводив основні оперативні дії на території Ірану.
 - Спільні операції проти ХАМАС у 2024–2025 рр. включали обмін агентурними даними та координацію арештів і ліквідацій.
- Переваги та проблеми взаємодії
- Переваги:
- Комплементарність функцій (Моссад – зовнішня, Шабак – внутрішня).

- Швидкий обмін інформацією та створення спільних оперативних груп.
- Високий рівень довіри між службами.

Проблеми:

- Різні корпоративні культури (Моссад – більш «зовнішній» і наступальний, Шабак – більш «внутрішній» і репресивний).
- Іноді виникає конкуренція за «славу» успішних операцій.
- Необхідність постійного узгодження повноважень.

Загалом взаємодія Моссаду та Шабаку є одним із найефективніших елементів ізраїльської системи національної безпеки. Вона дозволяє державі ефективно протистояти як зовнішнім, так і внутрішнім загрозам у єдиному комплексі [9;27;23;18].

АМАН та його взаємодія з Моссадом

АМАН (повна назва – Agaf Modi'in, Відділ розвідки Генерального штабу ЦАХАЛ) є військовою розвідкою Збройних сил Ізраїлю і однією з трьох ключових спецслужб держави поряд з Моссадом та Шабаком. Створений у 1948 році одночасно з проголошенням незалежності Ізраїлю, АМАН є найбільшою за чисельністю розвідувальною структурою країни (за оцінками, понад 10 000 осіб) і відповідає за оперативну, стратегічну, повітряну, електронну та кіберрозвідку на користь армії. На відміну від Моссаду, який зосереджений на зовнішніх спеціальних операціях і глобальній агентурній роботі, АМАН орієнтований переважно на військові аспекти безпеки: оцінку загроз з боку регулярних армій, ракетних і повітряних ударів, а також підтримку бойових дій ЦАХАЛ [9;27;18].

У сучасний період (2020–2026 рр.) АМАН перетворився на потужний високотехнологічний центр, що включає знаменитий підрозділ 8200 (елітний підрозділ кібер– та сигнальної розвідки), підрозділи аеророзвідки, супутникової розвідки та стратегічного аналізу. Саме АМАН забезпечує основну масу даних для планування військових операцій ЦАХАЛ, тоді як Моссад діє як «довга рука» Ізраїлю за кордоном.

Основні функції АМАН

- Оперативна та стратегічна розвідка щодо держав–супротивників (Іран, Сирія, Ліван, Хезболла).
- Повітряна, супутникова та електронна розвідка.
- Кібер– та сигнальна розвідка (підрозділ 8200).
- Аналіз військових загроз і прогнозування можливих конфліктів.
- Підтримка планування та проведення бойових операцій ЦАХАЛ.
- Технічна розвідка (радары, дрони, системи РЕБ) [9;23;18].

Специфіка взаємодії АМАН з Моссадом

Взаємодія між АМАН і Моссадом є найтіснішою серед усіх трьох служб і має системний, повсякденний характер. Це зумовлено тим, що багато загроз для Ізраїлю мають одночасно військовий і політичний вимір (Іран, Хезболла, ХАМАС). Основні напрями взаємодії:

1. Обмін розвідувальними даними в режимі реального часу. АМАН передає Моссаду дані військової розвідки (дислокація військ, ракетні комплекси, системи ППО), а Моссад – агентурну та оперативну інформацію з глибокого тилу супротивника. Під час операцій 2024–2026 рр. такий обмін був критичним.
 2. Спільне планування та виконання гібридних операцій. Моссад забезпечує агентурне проникнення та спеціальні дії, АМАН – технічну, кібер– та повітряну підтримку. Це дозволяє проводити операції, які неможливо здійснити силами однієї служби.
 3. Координація кібероперацій. Підрозділ 8200 АМАНу та Keshet Моссаду часто працюють у спільних групах. АМАН надає потужну технічну базу, Моссад – оперативну реалізацію та агентурну підтримку.
 4. Підтримка превентивних ударів. Моссад проводить розвідку та підготовку, АМАН забезпечує точне цілевказівку та прикриття з повітря.
- Конкретні приклади взаємодії (2024–2026 рр.)
- Операція з пейджерями Хезболли (вересень 2024): Моссад провів логістику та впровадження, АМАН забезпечував технічну розвідку, моніторинг реакції Хезболли та повітряне прикриття на випадок ескалації.

- Операція «Rising Lion» (червень 2025): Моссад і АМАН працювали в єдиному оперативному штабі. Моссад – агентурна та кіберрозвідка всередині Ірану, АМАН – точне цілевказівку та підтримка ударів.
- Операція «Epic Fury» («Дванадцятиденна війна», лютий–березень 2026): Наймасштабніший приклад. Моссад забезпечив глибоке проникнення та ліквідації ключових цілей, АМАН – повітряну, кібер та електронну підтримку, а також розвідку бойових дій. Створений об'єднаний штаб дозволив координувати дії в режимі реального часу [9;23;14].

Переваги та проблеми взаємодії

Переваги:

- Синергія різних видів розвідки (агентурна Моссаду + технічна АМАНу).
- Можливість проведення складних комбінованих операцій.
- Високий рівень довіри та оперативної інтеграції.
- Ефективне використання ресурсів держави.

Проблеми та виклики:

- Різні пріоритети (Моссад – політичні та оперативні, АМАН – військові).
- Іноді виникає конкуренція за «славу» успішних операцій.
- Необхідність постійної координації на рівні прем'єр-міністра.

Загалом взаємодія АМАНу з Моссадом є одним із найуспішніших елементів ізраїльської системи національної безпеки. Вона дозволяє державі поєднувати стратегічну глибину розвідки Моссаду з потужним технічним і військовим потенціалом АМАНу, що особливо критично в умовах сучасної гібридної війни з Іраном та його союзниками.

Переваги та проблеми системи взаємодії

Система взаємодії між Моссадом, Шабакком (Шин-Бет) та АМАНом є одним із найефективніших елементів національної безпеки Ізраїлю. Вона побудована на принципах централізованого керівництва з боку прем'єр-міністра, чіткого розподілу сфер відповідальності та високого рівня оперативної інтеграції. Водночас, як і будь-яка складна система, вона має не лише значні

переваги, але й певні проблеми та ризики, які періодично проявляються в реальній діяльності.

Переваги системи взаємодії

1. Висока оперативна ефективність і швидкість реагування. Завдяки прямому підпорядкуванню прем'єр-міністру та роботі спільних оперативних штабів (Joint Task Forces) три служби можуть майже миттєво об'єднувати зусилля. Це дозволяє проводити складні гібридні операції, які неможливо здійснити силами однієї служби. Яскравим прикладом є операція «Epic Fury» (лютий–березень 2026 р.), коли Моссад забезпечив глибоке проникнення, АМАН – повітряну та кібер-підтримку, а Шабак – внутрішнє прикриття.
2. Синергія різних видів розвідки. Моссад приносить агентурну глибину та спеціальні операції за кордоном, АМАН – потужну технічну, повітряну та кіберрозвідку, Шабак – внутрішню контррозвідку та роботу з терористичними осередками всередині країни. Таке поєднання створює ефект «повного спектру», коли жодна загроза не залишається поза увагою.
3. Мінімізація дублювання функцій і конкуренції. Чіткий розподіл сфер відповідальності (Моссад – зовнішня, Шабак – внутрішня, АМАН – військова) значно зменшує міжвідомчі конфлікти, які часто спостерігаються в інших країнах (наприклад, у США між ЦРУ, ФБР та військовою розвідкою).
4. Високий рівень довіри та обміну інформацією. Єдина захищена платформа обміну даними та регулярні засідання керівників служб під головуванням прем'єр-міністра забезпечують швидкий і повний обмін розвідувальною інформацією.
5. Гнучкість і адаптивність. Система дозволяє швидко створювати тимчасові міжвідомчі групи під конкретну операцію, що особливо важливо в умовах гібридної війни.

Проблеми та недоліки системи взаємодії

Незважаючи на значні переваги, система має ряд системних проблем, які періодично проявляються:

1. Надмірна централізація та залежність від прем'єр-міністра. Фактично всі ключові рішення приймаються на рівні глави уряду. У разі політичної кризи, зміни прем'єр-міністра або його перевантаження це може призводити до затримок у прийнятті рішень.
2. Різні корпоративні культури служб. Моссад має «зовнішню», наступальну культуру, Шабак – більш «внутрішню» та репресивну, АМАН – військову. Це іноді викликає тертя щодо пріоритетів, методів роботи та розподілу «слави» успішних операцій.
3. Конкуренція за ресурси та визнання. Керівники служб іноді змагаються за бюджет, увагу прем'єр-міністра та публічне визнання успішних операцій. Це особливо помітно під час великих акцій (наприклад, після операції з пейджерями Хезболли 2024 р. виникли публічні дискусії про те, хто саме «зробив основну роботу»).
4. Ризик витоку інформації. Чим більше спільних операцій і обміну даними, тим вищим стає ризик витоку. Хоча система захисту інформації вважається однією з найкращих у світі, окремі інциденти (наприклад, справа Полларда в 1980-х, хоча й не безпосередньо пов'язана з поточною системою) показують, що ризик існує.
5. Проблема «інформаційного перевантаження». Великий обсяг даних, що надходять від трьох служб, іноді ускладнює швидке прийняття рішень навіть на рівні Ради національної безпеки.
6. Обмежена прозорість і підзвітність. Надмірна секретність ускладнює парламентський і суспільний контроль за діяльністю служб, що може призводити до зловживань владою.

Загальна оцінка ефективності

Незважаючи на наявні проблеми, система взаємодії Моссаду, Шабаку та АМАНу залишається однією з найефективніших у світі. Вона дозволяє невеликій державі успішно протистояти значно потужнішим супротивникам у умовах перманентної гібридної війни. Успішні операції 2024–2026 років (пейджери

Хезболли, «Rising Lion», «Epic Fury») стали яскравим підтвердженням того, що переваги системи значно перевищують її недоліки.

Для України, яка також стикається з тривалою гібридною агресією, досвід ізраїльської моделі координації спецслужб може бути особливо корисним при реформуванні СБУ, ГУР МО та інших відомств.

ВИСНОВКИ до розділу 1

Аналіз історії становлення, організаційної структури, функціональної спрямованості підрозділів та системи взаємодії Моссаду з іншими ізраїльськими спецслужбами дозволяє зробити ряд фундаментальних узагальнень щодо однієї з найефективніших розвідувальних служб.

Моссад пройшов унікальний шлях еволюції – від невеликого координаційного інституту, створеного 13 грудня 1949 року за ініціативи Давида Бен-Гуріона, до високотехнологічної гібридної розвідувально-оперативної машини станом на 2026 рік. Кожен історичний етап відображав зміну характеру загроз для Ізраїлю та демонстрував високу адаптивність служби. Перший етап (1949–1952 рр.) став періодом закладання фундаментів: створення координаційного механізму та вирішення стратегічних завдань, таких як масова імміграція євреїв (операція «Езра і Нехемія»). Другий етап (1952–1963 рр., Ісер Гарель) ознаменувався професіоналізацією, формуванням системи підготовки кадрів і проведенням знакової операції «Фінал» (викрадення Адольфа Ейхмана). Третій етап (1963–1974 рр.) став епохою бойового хрещення – забезпечення розвідкою перемоги у Шестиденній війні та запуск операції «Гнів Божий» після мюнхенської трагедії 1972 року. Четвертий етап (1974–2002 рр.) поєднав масштабні гуманітарні операції (порятунок ефіопських євреїв) з інтенсивною боротьбою проти тероризму та ядерних програм Іраку й Ірану. Нарешті, п'ятий (сучасний) етап (2002–2026 рр.) став періодом технологічної революції та гібридної війни: від Stuxnet і ліквідацій іранських ядерників до масової атаки на пейджерів Хезболли (2024), операції «Rising Lion» (2025) та «Epic Fury» («Дванадцятиденна війна», 2026), які продемонстрували здатність служби проводити масштабні наступальні операції безпосередньо на території головного стратегічного супротивника [9;10;23;41].

Сучасна організаційна структура Моссаду характеризується глибокою інтеграцією ключових підрозділів – Tzomet (агентурна робота), Keshet (кібер- та технічна розвідка), Komemiyut / «Кідон» (спеціальні операції), Tevel (міжнародні

зв'язки), аналітичного та технологічного департаментів. Головною особливістю є перехід від жорсткої ієрархії до проектно–матричної моделі, що дозволяє швидко формувати міжфункціональні бойові групи. Паралельно відбулися суттєві зміни в кадровій політиці (жорсткий відбір з акцентом на технологічну грамотність і креативність), системі підготовки (використання VR/AR–симуляторів, ШІ) та ресурсному забезпеченні (бюджет близько 2,7–3 млрд дол. США на рік) [9;10;23]. Не менш важливою складовою успіху є ефективна система взаємодії Моссаду з Шабакком (внутрішня контррозвідка) та АМАНом (військова розвідка). Чіткий розподіл сфер відповідальності в поєднанні з централізованим керівництвом з боку прем'єр–міністра та Ради національної безпеки створює унікальну модель, яка мінімізує дублювання функцій і забезпечує швидку координацію. Саме завдяки цій системі три служби діють як єдиний, добре налагоджений механізм національної безпеки [9;23;14].

Ключовими факторами виняткової ефективності Моссаду є:

- пряме підпорядкування прем'єр–міністру, що гарантує максимальну оперативну автономію;
- принцип випереджального удару та превентивних дій;
- глибока інтеграція передових технологій з класичними методами агентурної роботи;
- елітна система відбору, підготовки та мотивації персоналу;
- ефективна міжвідомча координація.

Отже, досвід Моссаду демонструє, як відносно невелика за ресурсами, але високоадаптивна, технологічно оснащена та добре організована розвідслужба може забезпечувати стратегічну перевагу державі, яка десятиліттями перебуває в умовах екзистенційної та гібридної загрози. Для України, яка з 1991 року зіштовхується з тривалою системною гібридною агресією Російської Федерації, результати аналізу розділу 1 мають велике теоретичне та практичне значення. Вони створюють необхідну історичну, структурну та організаційну основу для подальшого дослідження оперативної діяльності Моссаду, його методів і засобів,

а також перспектив адаптації цього досвіду до українських реалій у наступних розділах роботи [1;2;9;10] .

РОЗДІЛ 2.

ОПЕРАТИВНА ДІЯЛЬНІСТЬ МОССАДУ ТА ЇЇ ОСОБЛИВОСТІ

2.1. Основні методи та засоби оперативної діяльності Моссаду

Оперативна діяльність Моссаду є серцем усієї його роботи і одним із найзакритіших аспектів функціонування ізраїльської системи національної безпеки. Від моменту створення у грудні 1949 року і до 2026 року методи та засоби, якими користується служба, пройшли складну, багатоступеневу еволюцію, зберігаючи при цьому низку фундаментальних принципів, закладених ще першим прем'єр-міністром Давидом Бен-Гуріоном. Якщо на початковому етапі оперативна діяльність мала переважно координаційний і логістичний характер, то сьогодні вона являє собою високотехнологічну гібридну систему, у якій класичні методи розвідки органічно поєднані з кібернетичними, дронними, інформаційними та спеціальними операціями [9;10;23].

У перші роки існування (1949–1952 рр., Реувен Шілоах) оперативна діяльність Моссаду була зосереджена на вирішенні найнагальніших екзистенційних завдань молодій державі: організації масової імміграції євреїв (операція «Езра і Нехемія»), первинному формуванні агентурних мереж в арабських країнах та протидії залишкам нацистських злочинців. Методи були класичними для того часу – вербування джерел, використання дипломатичних і комерційних легенд прикриття, логістичні операції та елементарний аналіз відкритих джерел [9;26].

Другий етап (1952–1963 рр., Ісер Гарель) ознаменувався професіоналізацією. Було створено систему багатоступеневого відбору та підготовки оперативників («каців»), запроваджено принцип «Never Again», сформовано глобальну мережу резидентур. Операція «Фінал» (викрадення Адольфа Ейхмана у 1960 р.) продемонструвала нові методи: тривале

спостереження, роботу під глибоким прикриттям, таємне вивезення цілі та координацію багатонаціональних команд [9;14;29].

Третій етап (1963–1974 рр., Меїр Аміт і Цві Замір) став періодом бойового хрещення. Під час Шестиденної війни Моссад освоїв методи масованого збору розвідданих у реальних бойових умовах, а після мюнхенської трагедії 1972 р. запустив операцію «Гнів Божий», створивши спеціальний підрозділ «Кідон». Тут з'явилися точкові ліквідації, саботажі та комбіновані операції відплати [9;10;27].

Четвертий етап (1974–2002 рр.) поєднав масштабні гуманітарні операції (рятування ефіопських і радянських євреїв) з інтенсивною боротьбою проти тероризму та ядерних програм Іраку й Ірану. Методи стали більш технологічними: використання технічних засобів розвідки, саботаж на об'єктах, довгострокове планування операцій [9;10;23].

П'ятий, сучасний етап (2002–2026 рр.) – це технологічна революція та повноцінна гібридна війна. Моссад повністю інтегрував кібер-, дроніві, штучний інтелект і інформаційні операції. Класичні методи не зникли, а стали невід'ємною частиною єдиної системи. Операції «пейджери Хезболли» (2024), «Rising Lion» (2025) та «Epic Fury» (2026) є яскравим підтвердженням цієї еволюції [9;10;23;25].

Незважаючи на значну трансформацію методів протягом 77 років, у оперативній діяльності Моссаду залишаються незмінними ключові принципи, які забезпечують його виняткову ефективність:

- принцип випереджального удару (preventive strike) – дія на випередження, а не на реагування;
- максимальна оперативна автономія завдяки прямому підпорядкуванню прем'єр-міністру;
- поєднання людського фактора (HUMINT) з передовими технологіями;
- культура постійного навчання на помилках і відсутність покарання за невдалі операції, якщо вони були добре сплановані;
- моральний імператив «Never Again» – готовність діяти в умовах високого ризику задля стратегічних інтересів держави.

Сучасна оперативна модель Моссаду ґрунтується на п'яти основних групах методів і засобів, які постійно взаємодіють між собою і утворюють єдиний бойовий цикл: від отримання первинної інформації до її негайної реалізації. Це:

1. Методи збору інформації, шпигунства, контршпигунства та аналізу даних.
2. Технологічні рішення та інновації у сфері національної безпеки.
3. Спеціальні оперативні акції.
4. Гібридні комбіновані операції.
5. Інформаційно–психологічні та впливові операції.

Саме ця інтеграція дозволяє Моссаду досягати стратегічних результатів за відносно невеликих ресурсів. Для України, яка вже понад 35 років перебуває в умовах системної гібридної агресії Російської Федерації, вивчення еволюції та сучасного стану оперативних методів Моссаду має не лише теоретичне, а й безпосереднє практичне значення. Українські спецслужби вже демонструють окремі елементи «моссадівського» стилю роботи, проте потребують системного осмислення комплексної моделі, яка поєднує класичні методи з новітніми технологіями.

У даному підрозділі детально розглядаються основні методи та засоби оперативної діяльності Моссаду в їх історичному розвитку та сучасному стані.

2.1.1. Методи збору інформації

Збір інформації є першим і фундаментальним етапом оперативної діяльності Моссаду, без якого неможливе ефективне планування, проведення та оцінка будь–яких спеціальних операцій. Саме якість і своєчасність зібраних даних визначають успіх або провал усієї діяльності служби. За 77 років існування Моссаду методи збору інформації пройшли складну еволюцію – від відносно простих класичних форм у 1949–1950–х роках до високотехнологічної, багатофункціональної системи, що поєднує людський інтелект (HUMINT), технічну, кібернетичну, геопросторову та відкриту розвідку (SIGINT/CYBINT, GEOINT, OSINT) в єдиному інтегрованому циклі.

На початковому етапі (1949–1952 рр., Реувен Шілоах) методи збору інформації були максимально орієнтованими на нагальні потреби новоствореної держави. Основним інструментом став HUMINT – вербування джерел серед єврейських громад в арабських країнах (Ірак, Єгипет, Сирія, Йорданія). Операція «Езра і Нехемія» (1950–1951 рр.) є класичним прикладом: Моссад одночасно організовував повітряний міст для евакуації понад 125 тисяч іракських євреїв і збирав розвідувальну інформацію про політичну ситуацію, військові плани та настрої в Іраку. Збір даних здійснювався через підпільні мережі, дипломатичні канали та комерційні легенди. Технічні засоби були практично відсутні, аналіз проводився вручну невеликою групою аналітиків [9;10;41].

Другий етап (1952–1963 рр., Ісер Гарель) став періодом професійного становлення. Гарель створив глобальну мережу резидентур у Європі, Латинській Америці та на Близькому Сході. Методи збору інформації стали більш системними: поєднання HUMINT з першими технічними засобами (електронне прослуховування, фотографування). Операція «Фінал» (викрадення Адольфа Ейхмана, 1960 р.) продемонструвала високий рівень майстерності в організації тривалого спостереження, роботі під глибоким прикриттям і координації багатонаціональних команд. Саме тоді Моссад почав системно поєднувати агентурну інформацію з відкритими джерелами.

Третій етап (1963–1974 рр., Меїр Аміт і Цві Замір) приніс бойове хрещення. Під час Шестиденної війни (1967 р.) служба освоїла методи масованого збору розвідданих у реальних бойових умовах (аерофотозйомка, агентурні мережі в Єгипті та Сирії). Після мюнхенської трагедії 1972 р. значно посилювався збір інформації про міжнародні терористичні мережі. Методи стали більш динамічними і орієнтованими на реальний час.

Четвертий етап (1974–2002 рр.) характеризувався розширенням географії та технічним посиленням. Моссад активно розвивав GEOINT (супутникова та аеророзвідка) і OSINT під час масштабних гуманітарних операцій («Мойсей» і «Соломон»). Збір інформації став більш комплексним і включав моніторинг ядерних програм Іраку та Ірану [9;23;25].

Сучасний етап (2002–2026 рр.) став періодом справжньої технологічної революції. Сьогодні збір інформації в Моссаді є багаторівневою інтегрованою системою, у якій працюють чотири основні типи розвідки, що постійно взаємодіють між собою.

1. HUMINT (людська розвідка) – залишається одним із найважливіших напрямків підрозділу Tzomet. Служба проводить довгострокове вербування високоякісних джерел у військово–політичному керівництві Ірану, Лівані, Сирії, Іраку та серед проксі–угруповань. Методи включають психологічне профілювання за допомогою ШІ, використання цифрових слідів, створення складних легенд прикриття та багаторічну розробку (5–10 років). Саме HUMINT забезпечив критичні дані для операції з пейджером Хезболли (2024 р.) та операції «Epic Fury» (2026 р.) [9;10;41].
2. SIGINT / CYBINT (сигнальна та кіберрозвідка) – підрозділ Keshet здійснює перехоплення комунікацій, проникнення в закриті мережі, аналіз метаданих і кібернетичне спостереження. Ці методи доповнюють HUMINT і часто стають основним джерелом інформації в реальному часі. Кіберпроникнення дозволяє отримувати дані, які неможливо здобути традиційними засобами [9;23;25].
3. GEOINT (геопросторова розвідка) – використання супутникових знімків, дронів, безпілотників та аеророзвідки для точного моніторингу об'єктів (ядерні центрифуги в Натанзі, ракетні бази Хезболли, тунельна інфраструктура ХАМАС) [9;23;25].
4. OSINT (відкрита розвідка) – системний аналіз відкритих джерел, соціальних мереж, публічних баз даних, ЗМІ та інтернет–ресурсів з обов'язковим застосуванням штучного інтелекту. Сучасний OSINT у Моссаді дозволяє обробляти мільйони даних за лічені години [9;23;25].

Усі чотири типи розвідки працюють у єдиному інформаційному просторі. Отримані дані відразу надходять до аналітичного департаменту, де вони обробляються за допомогою штучного інтелекту та машинного навчання. Це

дозволяє не лише збирати інформацію, а й автоматично виявляти аномалії, прогнозувати дії супротивника та формувати рекомендації для оперативних груп.

Таким чином, методи збору інформації в Моссаді пройшли шлях від класичного агентурного вербування до високотехнологічної інтегрованої системи, яка поєднує людський фактор з передовими технологіями. Саме ця еволюція забезпечує службі стратегічну глибину, оперативну швидкість і можливість діяти на випередження в умовах сучасної гібридної війни. Для України, яка вже понад 35 років протистоїть системній гібридній агресії РФ, вивчення цих методів відкриває значні можливості для вдосконалення роботи СБУ та ГУР МО.

2.1.2. Методи шпигунства

Методи шпигунства (агентурної роботи) є одним із найдавніших і водночас найбільш еволюціонуючих елементів оперативної діяльності Моссаду. Шпигунство в розумінні служби – це не просто вербування джерел, а комплексна, багаторічна система проникнення в структури супротивника з метою отримання стратегічно важливої інформації, впливу на його рішення та створення умов для подальших спеціальних операцій. За 77 років існування Моссаду методи шпигунства пройшли шлях від відносно простого вербування через ідеологічні та гуманітарні мотиви до високотехнологічного, гібридного шпигунства, у якому класичний HUMINT тісно інтегрований з цифровими технологіями, штучним інтелектом і довгостроковим проникненням у ланцюги постачання [9;10;23;29].

На початковому етапі (1949–1952 рр., Реувен Шілоах) методи шпигунства були максимально прагматичними. Основним інструментом стало вербування джерел серед єврейських громад в арабських країнах. Агенти залучалися через ідеологічні мотиви («захист молодого держави Ізраїль») та гуманітарні завдання (організація нелегальної імміграції). Операція «Езра і Нехемія» є класичним прикладом: агентурна мережа в Іраку одночасно забезпечувала розвідувальну інформацію та логістику евакуації понад 125 тисяч осіб. Шпигунство на цьому

етапі мало обмежений характер – переважно збір політичної та військової інформації про арабські армії [9;26].

Другий етап (1952–1963 рр., Ісер Гарель) став періодом професійного становлення шпигунства. Гарель запровадив жорстку систему відбору та підготовки оперативників («каців»), створив глобальну мережу резидентур і сформулював принципи глибокого прикриття. Операція «Фінал» (викрадення Адольфа Ейхмана, 1960 р.) продемонструвала найвищий рівень майстерності: тривале спостереження в Аргентині, використання фальшивих документів, легенди бізнесменів і туристів, координацію команди з 11 оперативників. Саме тоді Моссад освоїв методи довгострокової розробки цілей і роботи під глибоким прикриттям на іншому континенті [9;14;29].

Третій етап (1963–1974 рр., Меір Аміт і Цві Замір) приніс бойове хрещення. Під час Шестиденної війни (1967 р.) служба освоїла методи масованого проникнення в арабські країни. Після мюнхенської трагедії 1972 р. шпигунство стало більш наступальним: створення спеціального підрозділу «Кідон» і операція «Гнів Божий» показали ефективність поєднання агентурної роботи з точковими ліквідаціями. Методи шпигунства стали динамічнішими і орієнтованими на реальний час [9;10;27].

Четвертий етап (1974–2002 рр.) характеризувався розширенням географії та технічним посиленням. Моссад активно розвивав шпигунство в Лівані, країнах Перської затоки та Європі. Операції порятунку євреїв («Мойсей», «Соломон») поєднували гуманітарні завдання з глибоким агентурним проникненням. У цей період з'явилися перші приклади довгострокового впровадження агентів у терористичні структури [9;10;23].

Сучасний етап (2002–2026 рр.) став періодом справжньої революції в методах шпигунства. Підрозділ Tzomet перетворився на високотехнологічний центр, який поєднує класичний HUMINT з цифровими інструментами. Сучасне шпигунство Моссаду характеризується такими ключовими особливостями:

1. Довгострокове вербування та розробка джерел – агентів розробляють роками (5–10 і більше). Використовуються психологічне профілювання

за допомогою ШІ, аналіз цифрових слідів, соціальних мереж і фінансових операцій.

2. Глибоке прикриття та легендування – оперативники працюють під складними легендами бізнесменів, вчених, журналістів, IT-спеціалістів. Легенди підтримуються роками і включають реальні компанії-підстави.
3. Гібридне шпигунство – поєднання людського фактора з кіберпроникненням. Агент надає початковий доступ, а Keshet розгортає повномасштабне кіберпроникнення в мережі супротивника.
4. Проникнення в ланцюги постачання – один із найуспішніших сучасних методів. Класичний приклад – операція з пейджерів та раціями Хезболли (2024 р.): Моссад протягом понад 10 років контролював ланцюг постачання через підставні компанії, впроваджуючи вибухові пристрої безпосередньо в обладнання супротивника.
5. Використання технологій для вербування – штучний інтелект аналізує потенційних кандидатів, прогнозує їхню вразливість і пропонує оптимальні сценарії вербування.

Методи шпигунства сьогодні є невід’ємною частиною всіх великих операцій Моссаду. Саме завдяки агентурній роботі були забезпечені дані для серії ліквідацій іранських ядерників, операції «Rising Lion» (2025 р.) та операції «Eric Fury» («Дванадцятиденна війна», 2026 р.) [9;23;41].

Методи шпигунства Моссаду пройшли шлях від класичного вербування до високотехнологічного гібридного проникнення, зберігаючи при цьому головний принцип – максимальну глибину і довгостроковість. Саме завдяки цим методам служба здатна отримувати стратегічно важливу інформацію, створювати умови для превентивних ударів і забезпечувати оперативну перевагу держави в умовах перманентної гібридної загрози. Для України, яка вже понад 35 років протистоїть системній гібридній агресії Російської Федерації, вивчення досвіду Моссаду в сфері шпигунства відкриває значні можливості для вдосконалення агентурної

роботи СБУ та ГУР МО, особливо в частині довгострокового проникнення в структури противника та використання сучасних технологій.

2.1.3. Методи контршпигунства

Методи контршпигунства є одним із найбільш критичних і водночас найбільш закритих елементів оперативної діяльності Моссаду. Якщо методи збору інформації та шпигунства спрямовані на проникнення в структури супротивника, то контршпигунство забезпечує захист власних сил, мереж і інформації від ворожого проникнення. Без ефективного контршпигунства жодна розвідувальна служба не може існувати тривалий час, особливо держава, яка десятиліттями перебуває в умовах перманентної гібридної загрози. У Моссаді контршпигунство завжди розглядалося не як допоміжна функція, а як стратегічна необхідність, що безпосередньо впливає на виживання держави [9;23].

Контршпигунство в Моссаді проводиться на двох рівнях:

- зовнішнє – виявлення та нейтралізація ворожої агентури, що намагається проникнути в ізраїльські структури;
- внутрішнє – постійний захист і контроль власного персоналу, мереж та оперативних каналів [9;23;18].

За 77 років існування служби методи контршпигунства пройшли значну еволюцію.

1949–1952 рр. (Реувен Шілоах)

На початковому етапі контршпигунство було базовим і обмежувалося захистом агентурних мереж від викриття арабськими спецслужбами. Після провалу частини мережі в Багдаді (1951 р.) Шілоах запровадив елементарні правила конспірації та перевірки джерел. Ресурси були мінімальними, а основним засобом захисту – сувора дисципліна та ізоляція оперативників [9;26].

1952–1963 рр. (Ісер Гарель)

Гарель радикально підвищив рівень контршпигунства. Як колишній керівник Шин–Бету він запровадив жорстку систему багатоступеневих перевірок кадрів, обов'язковий поліграф і постійний психологічний моніторинг. Було

створено спеціальний підрозділ внутрішньої безпеки всередині Моссаду. Операція «Фінал» показала ефективність цих заходів – жоден із 11 оперативників не був розкритий. Саме Гарель сформулював принцип: «Ми не вбиваємо євреїв», який став моральним орієнтиром контршпигунства [9;14;29].

1963–1974 рр. (Меїр Аміт і Цві Замір)

Після Шестиденної війни та мюнхенської трагедії контршпигунство стало більш наступальним. Служба активно виявляла та нейтралізувала палестинські та арабські агентурні мережі в Європі. Після провалу в Ліллекхаммері (1973 р.) було посилено правила проведення операцій за кордоном і введено обов'язкову координацію з Шабаком. Контршпигунство набуло системного характеру [9;10;27].

1974–2002 рр.

У цей період Моссад зіткнувся з новими викликами: промисловим шпигунством, витокami технологій і спробами проникнення іранських та іракських спецслужб. Контршпигунство було посилено технічними засобами (електронне прослуховування, контроль комунікацій). Скандал з Джонатаном Поллардом (1985 р.) став уроком і призвів до ще жорсткіших внутрішніх перевірок [9;10;23].

2002–2026 рр. (сучасний етап)

Сьогодні контршпигунство Моссаду є високотехнологічною системою, що поєднує класичні методи з кібернетичними та аналітичними інструментами. Основні сучасні методи:

1. Кіберконтршпигунство – підрозділ Keshet постійно моніторить цифрові сліди оперативників, виявляє спроби фішингу, зловмисного ПЗ та витоку даних. Використовується штучний інтелект для аналізу поведінки в мережі.
2. Психологічний та поведінковий моніторинг – регулярні психологічні тести, аналіз змін у поведінці, сімейному стані та фінансовому становищі співробітників. Застосовується ІІІ для прогнозування ризиків.

3. Поліграф та розширені перевірки – обов’язковий для всіх рівнів, включаючи директорів. Перевірки проводяться періодично та позапланово.
4. Ротація та принцип «need-to-know» – оперативники не знають більше, ніж необхідно для виконання конкретного завдання. Постійна ротація персоналу між підрозділами.
5. Спільна робота з Шабакком – зовнішнє контршпигунство здійснюється у тісній координації з внутрішньою службою безпеки Ізраїлю.
6. Виявлення «кротів» у ланцюгах постачання – після операції з пейджерями Хезболли Моссад значно посилив контроль за власними підрядниками та компаніями–підстави [9;23;25].

Контршпигунство в сучасному Моссаді є проактивним: служба не лише реагує на загрози, а й активно створює «пастки» для потенційних ворожих агентів.

Методи контршпигунства Моссаду пройшли шлях від простого захисту мереж до високотехнологічної проактивної системи, яка поєднує класичні методи з сучасними цифровими технологіями. Саме завдяки ефективному контршпигунству служба зберігає свою операційну безпеку навіть під час найскладніших гібридних операцій. Для України, яка стикається з інтенсивною діяльністю російських спецслужб, досвід Моссаду в сфері контршпигунства є особливо актуальним [9;23;31].

2.1.4. Методи аналізу даних

Методи аналізу даних є завершальним і одним із найважливіших етапів оперативного циклу Моссаду. Саме аналіз перетворює сиру розвідувальну інформацію на конкретні оперативні рішення, прогнози та рекомендації для керівництва країни. Якщо методи збору інформації та шпигунства забезпечують «сировину», то аналіз даних забезпечує її «переробку» та «використання». За 77 років існування служби методи аналізу пройшли шлях від ручного експертного опрацювання невеликих обсягів даних до високотехнологічної аналітичної

системи, яка використовує штучний інтелект, машинне навчання та великі дані (Big Data) і працює в режимі реального часу [9;23;25].

1949–1952 рр. (Реувен Шілоах) На початковому етапі аналіз даних був максимально простим і ручним. Невелика група аналітиків у центральному апараті вручну обробляла агентурні донесення, дипломатичні звіти та відкриті джерела. Рішення приймалися на основі інтуїції та особистого досвіду керівників. Обсяг інформації був обмеженим, а швидкість обробки – низькою [9;26].

1952–1963 рр. (Ісер Гарель) Гарель створив централізований аналітичний відділ і запровадив перші системні підходи до аналізу. Було введено картографування даних, створення картотек і порівняльний аналіз інформації з різних джерел. Операція «Фінал» (1960 р.) стала прикладом якісного аналізу: кілька місяців детального спостереження, перевірки тисяч фактів і побудови точної моделі поведінки цілі [9;14;29].

1963–1974 рр. (Меїр Амїт і Цві Замір) Під час Шестиденної війни (1967 р.) аналіз даних набув оперативного характеру в реальному часі. Моссад почав поєднувати агентурну інформацію з технічними даними (аерофотозйомка). Після мюнхенської трагедії аналітичний відділ значно посилювався і почав системно прогнозувати терористичні загрози [9;10;23].

1974–2002 рр. У цей період з'явилися перші комп'ютеризовані бази даних. Аналіз став більш структурованим: використовувалися статистичні методи, сценарне моделювання та порівняльний аналіз великих обсягів інформації під час гуманітарних операцій («Мойсей», «Соломон») та моніторингу ядерних програм Іраку та Ірану [8;10;23].

2002–2026 рр. (сучасний етап) Сьогодні аналіз даних у Моссаді – це високотехнологічна аналітична платформа, яка є рівноправним учасником усіх оперативних процесів. Аналітичний департамент працює в тісній інтеграції з Tzomet, Keshet і Komemiyut і бере участь у плануванні операцій з першого дня [10;23;25].

Основні сучасні методи аналізу даних:

1. Штучний інтелект та машинне навчання – автоматична обробка мільйонів даних за лічені хвилини, виявлення аномалій, прогнозування дій супротивника з високою ймовірністю.
2. Аналіз великих даних (Big Data) – інтеграція інформації з HUMINT, SIGINT, GEOINT, OSINT і відкритих джерел в єдиному інформаційному просторі.
3. Сценарне моделювання та прогнозування – побудова кількох варіантів розвитку подій і рекомендацій для керівництва.
4. Автоматизований аналіз ризиків – розрахунок ймовірності провалу операції, виявлення вразливих місць.
5. Візуалізація даних – створення динамічних карт, графів і дашбордів для оперативних груп і директора.

Аналітичний департамент безпосередньо бере участь у всіх ключових операціях сучасності: підготовка операції з пейджерами Хезболли (2024 р.), операції «Rising Lion» (2025 р.) та операції «Epic Fury» (2026 р.). Саме завдяки сучасному аналізу даних Моссад здатний діяти на випередження і перетворювати розрізнену інформацію на точні оперативні рішення [33;40;34].

Методи аналізу даних у Моссаді пройшли шлях від ручного опрацювання до високотехнологічної аналітичної системи, яка є мозком усієї оперативної діяльності. Саме завдяки сучасному аналізу служба здатна перетворювати величезні обсяги інформації на точні, своєчасні та ефективні рішення. Для України, яка стикається з масштабними гібридними загрозами, досвід Моссаду в сфері аналізу даних відкриває значні можливості для створення сучасних аналітичних центрів [10;23;38;39].

2.1.5. Технологічні рішення та інновації у сфері національної безпеки (засоби оперативної діяльності)

Технологічні рішення та інновації є одним із найважливіших чинників, що визначають сучасну оперативну потужність Моссаду. Вони перетворили службу з традиційної розвідувальної організації на високотехнологічну гібридну систему, здатну проводити складні операції на території головних супротивників навіть у умовах відкритої регіональної війни. Якщо методи оперативної

діяльності пояснюють «як» Моссад діє, то технологічні засоби пояснюють «чим» він це робить і чому при відносно невеликій чисельності персоналу та бюджету служба досягає результатів стратегічного масштабу.

За всю історію існування Моссаду технологічні засоби пройшли радикальну еволюцію – від практично повної відсутності у 1949 році до створення власної технологічної екосистеми, яка включає кіберзброю, автономні системи, штучний інтелект, інновації в ланцюгах постачання та передові системи підготовки. Сучасні технології не є допоміжним елементом – вони стали рівноправним учасником оперативного циклу, часто вирішальним фактором успіху [9;10;23].

Історичний розвиток технологічних засобів

1949–1952 рр. (Реувен Шілоах) Технологічна база була вкрай обмеженою. Використовувалися звичайні радіостанції, механічні шифрувальні пристрої, звичайні фотоапарати та паперові карти. Основним засобом залишався людський фактор. Операція «Езра і Нехемія» показала, що навіть за мінімальної технологічної підтримки можна вирішувати стратегічні завдання завдяки добре організованій логістиці та конспірації [9;26].

1952–1963 рр. (Ісер Гарель) З'явилися перші спеціалізовані технічні засоби: мікрокамери, пристрої таємного прослуховування, високоякісні фальшиві документи, портативні радіопередавачі. Операція «Фінал» (1960) вже демонструвала використання спеціально розроблених засобів маскуванню та зв'язку. Гарель особисто приділяв значну увагу технічному оснащенню оперативників [9;14;29].

1963–1974 рр. (Меїр Аміт і Цві Замір) Значне технічне посилення під час воєн. Широко застосовувалася аерофотозйомка, електронна розвідка, перші системи радіоперехоплення. Для операції «Гнів Божий» були розроблені спеціальні вибухові пристрої з дистанційним керуванням, снайперське обладнання з глушниками та засоби прихованого спостереження [9;10;27].

1974–2002 рр. Перехід до більш системного використання технологій. З'явилися супутникові системи розвідки, комп'ютерні бази даних, електронні

засоби захисту інформації. Під час гуманітарних операцій («Мойсей», «Соломон») використовувалися спеціальні логістичні та комунікаційні системи. Моссад почав активно співпрацювати з приватним технологічним сектором Ізраїлю [9;10;23].

2002–2026 рр. (сучасний період) Це період технологічної домінації. Моссад створив одну з найпередовіших технологічних екосистем серед розвідувальних служб світу. Основні напрями розвитку:

1. Кіберзброя та кіберфізичні системи. Підрозділ Keshet є одним із світових лідерів у розробці кіберзброї. Крім легендарного Stuxnet (2010), який фізично знищив тисячі іранських центрифуг, служба постійно розвиває нові покоління шкідливого ПЗ, здатного виводити з ладу системи ППО, енергетичну інфраструктуру, системи управління військами та ядерними об'єктами. Сучасні кіберзасоби дозволяють проводити атаки, які поєднують віртуальний і фізичний ефект.
2. Автономні дронів та роботизовані системи. Моссад активно використовує рої дронів, автономні платформи для розвідки, наведення та доставки засобів ураження. Під час операції «Eric Fury» (2026 р.) дрони забезпечували проникнення всередину Ірану, створення тимчасових баз і підтримку наземних груп.
3. Штучний інтелект та системи аналізу великих даних. ШІ застосовується на всіх етапах: від автоматичного відбору кандидатів для вербування до прогнозування дій супротивника, виявлення аномалій і генерації оперативних пропозицій. Аналітичні системи Моссаду здатні обробляти мільйони даних за лічені хвилини.
4. VR/AR–симулятори та системи підготовки персоналу. Оперативники проходять комплексне тренування в віртуальному середовищі, яке максимально імітує реальні умови (вулиці Тегерана, бази Хезболли, іранські ядерні об'єкти). Це значно скорочує час підготовки та підвищує якість навичок, особливо для підрозділу «Кідон».

5. Інновації в ланцюгах постачання («троянські» пристрої) Один із найбільш креативних і ефективних напрямків. Класичний приклад – операція з пейджерів та раціями Хезболли (вересень 2024 р.): протягом понад 10 років Моссад контролював ланцюг постачання через мережу підставних компаній і впровадив вибухові пристрої безпосередньо в обладнання супротивника. Це стало еталоном гібридної диверсії XXI століття.
6. Спеціальні засоби прикриття, зв'язку та захисту. Сучасні зашифровані системи зв'язку нового покоління, біометричні легенди, пристрої для прихованого спостереження, системи захисту від кіберзагроз і виявлення стеження.
7. Інтеграційна платформа. Усі технологічні засоби об'єднані в єдину оперативну платформу, яка дозволяє міжфункціональним бойовим групам працювати в режимі реального часу. Директор Моссаду має можливість бачити всю оперативну картину в єдиному цифровому просторі [9;10;25].

Технологічні рішення та інновації сьогодні є ключовим конкурентним перевагом Моссаду. Вони дозволяють службі діяти швидко, точно, з мінімальним ризиком для персоналу та максимальним ефектом. Для України, яка вже понад 35 років перебуває в умовах системної гібридної агресії Російської Федерації, вивчення та адаптація цих технологічних засобів має стратегічне значення. Особливо актуальними є досвід створення кіберзброї, використання штучного інтелекту, інновацій у ланцюгах постачання та сучасних систем підготовки оперативників [10;23;25;38;39].

2.2. Найвідоміші операції Моссаду

Оперативні операції є найвищим проявом можливостей будь-якої розвідувальної служби. Саме через них реалізуються методи та засоби, про які йшлося в попередньому підрозділі, і саме вони формують реальну ефективність служби в очах політичного керівництва, супротивника та міжнародної спільноти. Для Моссаду операції – це не просто тактичні акції, а стратегічний інструмент державної політики, що поєднує розвідку, спеціальні дії, технології, дипломатію

та психологічний вплив. Кожна значна операція служби є комплексним продуктом багаторічного планування, високого професіоналізму та готовності йти на розрахований ризик задля досягнення стратегічних цілей держави.

Історія оперативної діяльності Моссаду – це історія еволюції від відносно обмежених за масштабами акцій у перші роки існування держави до масштабних гібридних кампаній стратегічного рівня в XXI столітті. Якщо на початку 1950–х років операції переважно мали гуманітарний та захисний характер (організація імміграції, протидія нацистським злочинцям), то вже у 1960–1970–х роках Моссад перейшов до активних наступальних дій (викрадення Ейхмана, операція «Гнів Божий»). Сьогодні, у 2024–2026 роках, служба проводить операції, які раніше вважалися можливими лише для великих держав – глибоке проникнення на територію головного супротивника (Іран), комбіновані кіберфізичні удари та масштабні кампанії з дестабілізації цілих терористичних мереж [9;10;23].

Аналіз найвідоміших операцій Моссаду має не лише історико–описовий, а й глибоко практичний сенс. Кожна операція дозволяє побачити, як саме поєднуються різні методи (HUMINT, кіберрозвідка, спеціальні акції) і технологічні засоби в реальних умовах. Крім того, вивчення успіхів і невдач дає можливість виявити сильні та слабкі сторони ізраїльської моделі, що особливо важливо для України.

У сучасних умовах тривалої гібридної війни з Російською Федерацією досвід Моссаду набуває виняткової актуальності. Багато операцій служби мають прямі паралелі з викликами, перед якими стоять українські спецслужби:

- довгострокове проникнення в логістичні та технологічні ланцюги супротивника (операція з пейджерів Хезболли);
- превентивні удари по критичній інфраструктурі та ключових фігурах (ліквідації іранських ядерників);
- поєднання кібернетичних і фізичних засобів ураження (Stuxnet та його сучасні аналоги);
- операції відплати та стримування терористичних мереж;
- висока культура ризику та навчання на помилках [9;10;23;31].

У цьому підрозділі розглядаються найбільш показові операції Моссаду, відібрані за такими критеріями:

- стратегічна значущість для держави Ізраїль;
- інноваційність застосованих методів і засобів;
- вплив на розвиток оперативного мистецтва служби;
- актуальність для сучасних гібридних загроз, з якими стикається Україна.

Особливу увагу буде приділено операціям ХХІ століття, оскільки вони найкраще відображають сучасну гібридну модель Моссаду. Аналіз кожної операції включатиме мету, підготовку, хід виконання, результати, сильні та слабкі сторони, а також уроки, які можуть бути корисними для реформування системи національної безпеки України.

Таким чином, вивчення найвідоміших операцій Моссаду дозволяє не лише зрозуміти механізм роботи однієї з найефективніших розвідок світу, але й сформулювати конкретні практичні рекомендації щодо адаптації цього досвіду до українських реалій – від довгострокового планування операцій у глибокому тилу противника до інтеграції технологій і людського фактора в умовах перманентної гібридної війни.

2.2.1. Класичні операції, що заклали фундамент репутації Моссаду

Класичні операції Моссаду 1950–1970-х років стали фундаментом його світової репутації як однієї з найефективніших і найсміливіших розвідувальних служб. Саме в цей період служба перейшла від координаційної та гуманітарної діяльності до активних наступальних операцій, відпрацювала ключові методи шпигунства, спеціальних акцій і контршпигунства, а також сформувала філософію «Never Again» – готовність діяти жорстко, швидко та далеко за межами країни для захисту інтересів держави. Ці операції заклали оперативну культуру Моссаду, яка залишається актуальною й сьогодні.

Нижче детально розглядаються найважливіші класичні операції.

1. «Фінал» (викрадення Адольфа Ейхмана, 11 травня 1960 р.)

Однією з найвідоміших і символічних операцій Моссаду раннього періоду стала операція «Фінал» (Operation Finale), відома також як «Операція

Гарібальді». Її метою було викрадення та таємне вивезення до Ізраїлю Адольфа Ейхмана – одного з головних архітекторів «остаточного рішення єврейського питання» (Endlösung), який безпосередньо відповідав за логістику депортації та знищення мільйонів євреїв під час Голокосту.

Стратегічний контекст і причини проведення.

Після Другої світової війни Ейхман уникнув Нюрнберзького трибуналу, втік з американського полону в 1946 році та переховувався в Аргентині під вигаданим ім'ям Рікардо Клемента. Для молодого держави Ізраїль, яка щойно пережила Голокост, принцип «Ніколи знову» (Never Again) став не просто гаслом, а державною доктриною. Прем'єр-міністр Давид Бен-Гуріон та директор Моссаду Ісер Гарель вважали, що притягнення Ейхмана до суду в Ізраїлі матиме не лише юридичне, а й глибоке моральне, історичне та виховне значення для всього єврейського народу [9;14;29].

Підготовка операції.

Пошук Ейхмана тривав понад 15 років. Ключову інформацію надав Лотар Герман – сліпий німецький єврей, який жив в Аргентині. Його дочка почала зустрічатися з сином Ейхмана, і Герман запідозрив правду. У 1957–1959 рр. Моссад провів ретельну перевірку. У березні 1960 року Ісер Гарель особисто прибув до Аргентини для керівництва операцією. Було сформовано команду з 11 висококваліфікованих оперативників, серед яких – Рафаель Ейтан (командир), Пітер Малкін, Цві Аароні, Авраам Шалом та інші. Оперативники діяли під глибоким прикриттям, використовуючи фальшиві документи та легенди [9;14;29].

Хід операції.

11 травня 1960 року о 20:00 вечора, коли Ейхман повертався з роботи автобусом до свого будинку на вулиці Гарібальді в передмісті Буенос-Айреса (Сан-Фернандо), його перехопили. Пітер Малкін звернувся до нього іспанською: «Un momentito, señor!» («Одну хвилинку, сеньйоре!»), після чого застосував бойовий прийом і повалив на землю. Разом з іншими агентами Ейхмана швидко

затягнули в автомобіль. Операція тривала менше десяти хвилин і пройшла без єдиного пострілу [9;14;29].

Ейхмана утримували дев'ять днів у задалегідь орендованій таємній віллі, де провели допит. Він визнав свою особу та підписав документ згодою на суд в Ізраїлі. 20 травня 1960 року його під сильним наркозом і під виглядом члена екіпажу ізраїльського літака El Al (який прибув до Аргентини на святкування 150-річчя незалежності країни) таємно вивезли до Ізраїлю. Аргентинська влада нічого не знала про операцію.

Результати.

Суд над Ейхманом у Єрусалимі (1961 р.) став одним з найважливіших судових процесів ХХ століття. Він транслювався в прямому ефірі, став потужним актом історичної справедливості та нагадуванням світу про злочини Голокосту. 15 грудня 1961 року Ейхмана визнали винним у злочинах проти людства, воєнних злочинах та злочинах проти єврейського народу. 31 травня 1962 року його стратили – це єдина цивільна страта в історії сучасного Ізраїлю [9;14;29].

Сильні та слабкі сторони операції.

Сильні сторони:

- виняткова точність і конспірація (операція пройшла без жертв і без міжнародного скандалу на момент проведення);
- ідеальне поєднання агентурної розвідки, оперативного планування та логістики;

моральний та символічний ефект, який значно посилив міжнародний авторитет Ізраїлю.

Слабкі сторони:

- порушення суверенітету Аргентини (призвело до тимчасового дипломатичного конфлікту);
- високий ризик провалу в разі витоку інформації.

Уроки для України.

Операція «Фінал» залишається класичним прикладом реалізації принципу невідворотності покарання для воєнних злочинців. Для України, яка з 2014 року

фіксує численні воєнні злочини російських окупантів (Буча, Маріуполь, Ірпінь, Гостомель), цей досвід має особливу актуальність. Моссад продемонстрував, що держава може й повинна проводити довгострокові операції з розшуку та притягнення до відповідальності ключових фігурантів злочинів, навіть за межами своєї території. Українські спецслужби (СБУ та ГУР МО) уже активно працюють у цьому напрямку, збираючи докази та ідентифікуючи виконавців.

Досвід Моссаду підкреслює важливість створення спеціальних оперативних груп, використання глобальної агентурної мережі та міжнародної співпраці для забезпечення принципу «жоден воєнний злочинець не уникне покарання».

2. Операція «Гнів Божий» (Wrath of God, 1972–1980–ті рр.)

Однією з наймасштабніших і найбільш символічних довгострокових операцій Моссаду стала операція «Гнів Божий» (Operation Wrath of God, івр. Зеєв ха–Елохім), відома також як «Мюнхенська відплата». Вона була ініційована як пряма відповідь на кривавий теракт на XX Олімпійських іграх у Мюнхені 5–6 вересня 1972 року, коли бойовики палестинського терористичного угруповання «Чорний вересень» захопили та вбили 11 ізраїльських спортсменів і тренерів [9;10;27].

Стратегічний контекст і причини проведення.

Теракт у Мюнхені став шоком для всього світу і особливо для Ізраїлю. Прем'єр–міністр Голда Меїр та директор Моссаду Цві Замір розглядали його не просто як злочин, а як оголошення війни проти всього єврейського народу. Меїр особисто дала «зелений світло» на проведення безпрецедентної кампанії відплати: ліквідацію всіх ключових організаторів і виконавців мюнхенського теракту, а також лідерів ОВП та пов'язаних терористичних структур у Європі та на Близькому Сході. Операція мала продемонструвати, що Ізраїль не пробачає тероризму і буде переслідувати винних по всьому світу [9;10;27].

Підготовка операції.

Цві Замір створив спеціальний елітний підрозділ «Кідон» (Bayonet – «Штик») – невелику, але високопрофесійну команду ліквідаторів, яка

підпорядковувалася безпосередньо директору Моссаду. До складу увійшли найкращі оперативники з підрозділу Caesarea. Підготовка включала детальне вивчення цілей, створення мережі інформаторів, розробку складних легенд прикриття та логістики. Операція мала два етапи: інтенсивний (1972–1973 рр.) і тривалий (до кінця 1980–х) [9;10;27].

Хід операції.

Операція тривала понад десять років і охоплювала Європу, Близький Схід та Північну Африку. Моссад застосовував різноманітні методи: закладання вибухівки в автомобілі, снайперські атаки, отруєння, інсценування нещасних випадків і навіть поштові бомби.

Серед найвідоміших акцій:

- Ліквідація ключових фігур «Чорного вересня» в Римі, Парижі, Лондоні та Кіпрі.
- Найрезонансна операція – вбивство Алі Хасана Саламе («Червоного принца»), головного організатора мюнхенського теракту, 22 січня 1979 року в Бейруті. Саламе був ліквідований потужним вибухом автомобіля, начиненого 100 кг вибухівки.
- Серія успішних операцій у 1972–1973 рр., коли було нейтралізовано понад 10 високопоставлених терористів.

Однак операція не обійшлася без помилок. У липні 1973 року в норвезькому Ліллекхаммері оперативники помилково вбили марокканського офіціанта Ахмеда Бушікі, прийнявши його за одного з терористів. Цей інцидент призвів до арешту кількох агентів Моссаду, міжнародного скандалу та тимчасового призупинення частини операцій [10, с.378-385; 27, с.355-362].

Результати.

Операція «Гнів Божий» досягла стратегічної мети: більшість безпосередніх організаторів і виконавців мюнхенського теракту були ліквідовані. Вона суттєво підірвала оперативні можливості «Чорного вересня» та ОВП, змусила палестинських терористів перейти в глибоке підпілля і продемонструвала світові, що Ізраїль здатен проводити глобальні операції

відплати. Загалом, за різними оцінками, у рамках операції було ліквідовано від 10 до 20 ключових фігур терористичних організацій.

Сильні та слабкі сторони операції.

Сильні сторони:

- принцип невідворотності покарання, який став потужним стримуючим фактором для терористів;
- висока ефективність довгострокового планування та глобальної оперативної мережі;
- створення та бойове хрещення елітного підрозділу «Кідон», який і досі залишається одним з найефективніших у світі.

Слабкі сторони:

- ризик помилкових ліквідацій і пов'язаних з ними дипломатичних криз (Ліллекхаммер);
- значні моральні та репутаційні витрати;
- можливість використання операції противником для пропаганди.

Уроки для України.

Операція «Гнів Божий» є класичним прикладом реалізації принципу «око за око» в умовах асиметричної боротьби з тероризмом. Для України, яка з 2014 року фіксує численні воєнні злочини та терористичні акти з боку РФ і її проксі (включаючи «вагнерівців», колаборантів та організаторів ракетних ударів по цивільних об'єктах), цей досвід має виняткову актуальність.

Він підкреслює необхідність створення спеціальних оперативних підрозділів для довгострокового розшуку та притягнення до відповідальності ключових воєнних злочинців, навіть за межами України. Водночас українські спецслужби вже накопичили значний досвід точкових операцій (ліквідації командирів «вагнерівців», ударів по логістиці та командуванню РФ). Досвід Моссаду може допомогти систематизувати ці дії, підвищити рівень конспірації та мінімізувати дипломатичні ризики. Головний урок – терористи та воєнні злочинці мають розуміти: справедливість наздожене їх незалежно від часу та місця [9;10;27;31;51].

3. Операції «Мойсей» (1984–1985 рр.) та «Соломон» (1991 р.)

Поряд з класичними бойовими та контртерористичними операціями Моссад активно здійснював масштабні гуманітарно–логістичні операції з евакуації єврейських громад з небезпечних регіонів світу. Найяскравішими прикладами такої діяльності стали операції «Мойсей» (1984–1985 рр.) та «Соломон» (1991 р.), які демонструють іншу грань діяльності ізраїльської розвідки – здатність до швидкого, таємного та високопрофесійного проведення масових евакуацій у надзвичайно складних геополітичних умовах [8;9;12].

Стратегічний контекст і причини проведення.

Ефіопські євреї (бета–Ізраїль, або «фалаша») протягом століть жили в ізоляції в горах Ефіопії. У 1970–1980–х роках вони опинилися у смертельній небезпеці через громадянську війну, голод і антисемітські переслідування. Тисячі людей здійснили важкий перехід через пустелю до таборів біженців у Судані. Для Ізраїлю, який керувався доктриною «Збирання вигнанців» (Kibbutz Galuyot) та принципом «Ніколи знову», порятунок цих людей став моральним і стратегічним імперативом. Операції «Мойсей» і «Соломон» були спрямовані на масову евакуацію ефіопських євреїв до Ізраїлю [9;26;23].

Підготовка операцій.

Моссад відіграв центральну роль у обох операціях. Агенти розвідки встановили таємні контакти з суданською владою (операція «Мойсей») та ефіопським режимом Менгісту Хайле Маріама (операція «Соломон»). Було створено мережу інформаторів, забезпечено прикриття, логістику та безпеку. Операції проводилися у тісній координації з Повітряними силами Ізраїлю (ЦАХАЛ), ЦРУ США та місцевими спецслужбами. Особливу увагу приділяли конспірації: евакуація здійснювалася вночі, під виглядом гуманітарних рейсів [9;26;23].

Хід операцій.

Операція «Мойсей» розпочалася 21 листопада 1984 року і тривала сім тижнів (до 5 січня 1985 р.). Кожної ночі з аеродрому біля Хартума (Судан) злітали літаки, які перевозили ефіопських євреїв до Ізраїлю. Загалом було

евакуйовано близько 7800–8000 осіб. Операція була припинена після витoku інформації в пресі та дипломатичного тиску арабських країн на Судан [9;26;23].

Операція «Соломон» стала ще масштабнішою. 24–25 травня 1991 року, коли режим Менгісту почав падати і Ефіопія опинилася на межі хаосу, Моссад організував безпрецедентний повітряний міст. За 36 годин 34–35 ізраїльських літаків (включаючи Boeing 747 авіакомпанії El Al та військові C-130) здійснили 40 безперервних рейсів з аеропорту Аддис-Абеби. Було евакуйовано 14 325 ефіопських євреїв – найбільша за кількістю осіб одинична операція з евакуації в історії авіації. Деякі літаки перевозили понад 1000 пасажирів за раз [9;26;23].

Результати.

У рамках двох операцій до Ізраїлю було доставлено понад 22 000 ефіопських євреїв. Це стало одним з найбільших успіхів політики «Алії» (повернення євреїв на історичну батьківщину) в історії держави. Операції зміцнили демографічний потенціал Ізраїлю та продемонстрували світу ефективність ізраїльської розвідки не лише в бойових, а й у гуманітарних місіях.

Сильні та слабкі сторони операцій.

Сильні сторони:

- виняткова логістична майстерність і швидкість (операція «Соломон» увійшла в Книгу рекордів Гіннеса);
- глибока агентурна робота та дипломатична гнучкість Моссаду;
- ідеальна координація між розвідкою, військовими та цивільними структурами;
- гуманітарний характер операцій, який значно підвищив міжнародний авторитет Ізраїлю.

Слабкі сторони:

- залежність від політичної ситуації в країнах-транзитерах (операція «Мойсей» була зупинена через витік інформації);
- значні фінансові та організаційні витрати;
- ризики для учасників операції в умовах нестабільності регіону.

Уроки для України.

Операції «Мойсей» і «Соломон» демонструють унікальну здатність Моссаду проводити масштабні таємні евакуаційні операції в умовах війни, голоду та політичного хаосу. Для України, яка з 2022 року стикається з масовою вимушеною міграцією громадян, евакуацією населення з окупованих територій та необхідністю захисту українців за кордоном, цей досвід має пряму практичну цінність. Він показує, як розвідслужба може поєднувати гуманітарні завдання з елементами оперативного прикриття, дипломатичної роботи та логістики.

Українські спецслужби вже накопичили значний досвід евакуації людей із зон бойових дій (зокрема, через коридори в Маріуполі, Херсонщині та інших регіонах). Адаптація моссадівських методів дозволила б систематизувати такі операції, підвищити їхню швидкість і безпеку, а також ефективніше працювати з українською діаспорою в країнах, де виникають загрози (наприклад, у регіонах з високим ризиком гібридних атак РФ). Головний урок – держава, яка дбає про своїх громадян, повинна мати розвідку, здатну діяти не лише на знищення ворога, а й на порятунок своїх людей у будь-якій точці світу [9;26;23;31;51].

2.2.2. Сучасні операції (2002–2026 рр.) – гібридна ера Моссаду

Сучасний період оперативної діяльності Моссаду (2002–2026 рр.) радикально відрізняється від класичного етапу. Якщо раніше служба проводила переважно точкові операції та кампанію відплати, то з початку 2000-х років Моссад перейшов до системної гібридної війни – комплексного поєднання агентурної розвідки, кібероперацій, дронівих ударів, спеціальних акцій, інформаційно-психологічного впливу та довгострокового проникнення в ланцюги постачання супротивника[9;10;23;25].

Головним супротивником став Іран та його «вісь опору» (Хезболла, ХАМАС, хусити, проіранські міліції). У цей період Моссад остаточно перетворився на наступальну стратегічну силу, здатну проводити масштабні операції на території головного противника навіть у умовах відкритої регіональної ескалації.

Нижче наведено топові сучасні операції Моссаду, які стали еталоном гібридної оперативної діяльності:

1. Операція Stuxnet (2009–2010 рр.)

Операція Stuxnet є однією з найважливіших і найбільш знакових операцій в історії сучасної розвідки та кібервійни. Вона стала першою у світі кібероперацією, яка завдала фізичної шкоди реальному промисловому об'єкту, а саме – іранській ядерній програмі. Stuxnet по праву вважається точкою відліку нової епохи – епохи кіберфізичних війн, коли віртуальна атака може призводити до реальних руйнувань, порівнянних з авіаударом.

Стратегічний контекст операції

На початку 2000–х років Іран активно розвивав свою ядерну програму, зокрема на збагачувальному заводі в Натанзі. За оцінками ізраїльської та американської розвідок, Іран міг наблизитися до створення ядерної зброї вже у 2010–2012 роках. Для Ізраїлю це була екзистенційна загроза. Тоді прем'єр-міністр Аріель Шарон та його наступник Егуд Ольмерт поставили перед Моссадом (директор Меїр Даган) завдання – максимально уповільнити або зірвати іранську ядерну програму без початку повномасштабної війни [9;10;25].

Підготовка операції (2007–2009 рр.)

Операція була спільною – Ізраїль (Моссад) і США (NSA та інші структури). Підготовка тривала щонайменше 2–3 роки і включала:

- Глибоке агентурне проникнення на об'єкт у Натанзі (Tzomet).
- Детальне вивчення систем управління Siemens Step7, які керували центрифугами.
- Створення надзвичайно складного комп'ютерного черв'яка (worm), здатного працювати автономно.
- Тестування на спеціально побудованому секретному стенді в Ізраїлі, який точно імітував іранські центрифуги.

Stuxnet був розроблений як високоточна кіберзброя. Він мав кілька унікальних характеристик:

- Поширювався через USB-накопичувачі (air-gap – об'єкт не був підключений до інтернету).

- Мав цифрові «підписи», які робили його схожим на легітимне програмне забезпечення Siemens.
- Міг «спати» роками і активуватися тільки при виявленні конкретної конфігурації обладнання.

Хід операції

У 2009–2010 роках Stuxnet проник на завод у Натанзі. Черв'як діяв надзвичайно хитро:

- Змінював швидкість обертання центрифуг (то занадто швидко, то занадто повільно).
- При цьому на екранах операторів показував нормальні показники (фальшиві дані).
- Поступово виводив з ладу тисячі центрифуг.

За різними оцінками, було виведено з ладу від 900 до 1000 центрифуг (близько 20% парку Натанзі). Іранці довго не могли зрозуміти, що відбувається, і вважали це технічними проблемами або диверсією на місці.

Результати

- Іранська ядерна програма була відкинута назад щонайменше на 1–2 роки.
- Значно зросли витрати на програму.
- Було продемонстровано, що кіберзброя може замінити авіаудари по захищених об'єктах.
- Операція залишилася в таємниці майже рік, поки не була виявлена міжнародними експертами.

Сильні сторони операції

- Висока точність і селективність (уражено тільки цільові центрифуги).
- Відсутність прямих військових дій і людських жертв.
- Максимальна конспірація та довгострокове планування.
- Поєднання агентурної розвідки, кібернетичних можливостей і інженерного аналізу.

Слабкі сторони

- Черв'як зрештою «вирвався» в інтернет і був виявлений.
- Іран згодом відновив програму і посилив кіберзахист.
- Показав уразливість навіть «повітряних зазорів» (air-gapped систем).

Уроки для України

Операція Stuxnet має надзвичайно високу актуальність для України:

- Демонструє можливість ефективно уражати критичну інфраструктуру супротивника без прямого військового вторгнення.
- Підкреслює важливість глибокого вивчення систем управління противника (російські АСУ ТП, системи зв'язку, логістика).
- Показує цінність довгострокового планування (2–3 роки підготовки).
- Є прикладом успішної міжнародної співпраці в кіберпросторі.

Українські спецслужби вже проводять подібні операції проти російської логістики, нафтопереробних заводів і військових систем. Досвід Stuxnet може бути використаний для створення більш складних і селективних кіберзасобів, спрямованих на ключові елементи російської військової машини [9;10;25;31;51].

1. Серія ліквідацій іранських ядерників (2007–2011 рр., продовжено пізніше)

Серія точкових ліквідацій провідних іранських вчених і військових, причетних до ядерної програми Ірану, є однією з найбільш системних і ефективних кампаній Моссаду в сучасний період. Ця операція проводилася переважно під керівництвом директора Моссаду Меїра Дагана (2002–2011 рр.) і стала ключовим елементом ізраїльської стратегії запобігання появі в Ірані ядерної зброї [9;10;23].

Стратегічний контекст

На початку 2000-х років Іран значно прискорив свою ядерну програму. За оцінками Моссаду та західних розвідок, до 2010–2012 років Тегеран міг отримати достатньо збагаченого урану для створення ядерної зброї. Для Ізраїлю це була екзистенційна загроза – поява ядерного Ірану могла змінити весь баланс сил на Близькому Сході і поставити під питання саме існування єврейської держави. Аріель Шарон і його наступники поставили перед Меїром Даганом

чітке завдання: максимально уповільнити іранську ядерну програму без початку великої війни[9;10;23].

Даган радикально змінив підхід Моссаду – замість лише збору інформації пріоритетом стала активна нейтралізація загроз.

Підготовка та стратегія

Меїр Даган особисто керував кампанією. Була створена спеціальна оперативна група, яка поєднувала:

- Глибоку агентурну розвідку (Tzomet);
- Кібернетичну та технічну розвідку (Keshet);
- Підрозділ спеціальних операцій «Кідон» (Komemiyut).

Моссад збирав детальну інформацію про кожного ключового учасника іранської ядерної програми: науковців, інженерів, військових IRGC (Корпус вартів Ісламської революції), керівників проектів. Особливу увагу приділяли тим, хто мав унікальні знання або займав ключові посади [9;10;23;25].

Ключові ліквідації (2007–2011 рр.)

За період 2007–2011 років було проведено серію точкових ліквідацій, серед яких:

- Масуд Алі Мохаммаді (січень 2010) – професор фізики Тегеранського університету, спеціаліст з частинок. Вбитий вибухом бомби, встановленої на мотоциклі біля його будинку.
- Маджид Шахріарі (листопад 2010) – один з провідних вчених–ядерників. Вбитий за допомогою магнітної бомби, прикріпленої до автомобіля.
- Даріуш Резайнежад (липень 2011) – спеціаліст з ядерної фізики. Ліквідований у Тегерані.
- Мостафа Ахмаді Рошан (січень 2012) – заступник директора з виробництва на заводі в Натанзі. Вбитий магнітною бомбою [9;10;27;25].

Крім того, було проведено кілька замахів, які не завжди закінчувалися смертю, але створювали потужний психологічний тиск на весь іранський ядерний колектив.

Методи виконання

Моссад використовував кілька основних тактик:

- Магнітні бомби, які прикріплювалися до автомобілів (дуже точний і відносно «чистий» спосіб).
- Вибухові пристрої на мотоциклах.
- Снайперські операції.
- У деяких випадках – отруєння або інші методи, що імітували природну смерть.

Операції проводилися переважно на території Ірану, що вимагало виняткової конспірації та глибокого агентурного прикриття [9;10;27].

Результати

- Було фізично усунуто або нейтралізовано щонайменше 5–7 ключових фахівців ядерної програми.
- Значно сповільнено темпи збагачення урану.
- Створено атмосферу страху серед іранських вчених – багато з них відмовлялися працювати над програмою або вимагали посиленої охорони.
- Іран змушений був витратити величезні ресурси на захист персоналу.

Сильні сторони операції

- Висока точність і селективність (уражалися тільки ключові фігури).
- Мінімальний міжнародний резонанс порівняно з авіаударом.
- Психологічний ефект – залякування цілої галузі.
- Ефективне поєднання розвідки та спеціальних дій.

Слабкі сторони

- Деякі ліквідації призводили до публічного обурення в Ірані та міжнародних звинувачень на адресу Ізраїлю.
- Іран посилив заходи безпеки та прискорив програму в інших аспектах.

- Ризик ескалації.

Уроки для України

Серія ліквідацій іранських ядерників є одним з найактуальніших прикладів для України:

- Превентивна нейтралізація ключових технічних спеціалістів і командирів противника.
- Використання точкових операцій замість масштабних ударів.
- Поєднання агентурної розвідки з спеціальними акціями.
- Психологічний тиск на науково–технічний персонал супротивника.

Українські спецслужби вже проводять подібні дії проти ключових фігур російської логістики, виробників озброєння та командирів. Досвід Моссаду під керівництвом Меїра Дагана показує, як системна кампанія точкових ліквідацій може суттєво уповільнити військову машину противника [9;10;27;23;31;51].

2. Операція з пейджерями та раціями Хезболли (вересень 2024 р.)

Операція з пейджерями та раціями Хезболли (вересень 2024 року) по праву вважається однією з найкреативніших, найсміливіших і найефективніших гібридних операцій в історії світової розвідки. Вона демонструє абсолютний пік розвитку оперативного мистецтва Моссаду – довгострокове стратегічне планування, глибоке проникнення в логістичні ланцюги супротивника, поєднання технічної інженерії з психологічною війною та ідеальну синхронізацію удару [10;23;41].

Це класичний приклад «троянської» операції XXI століття, коли супротивнику впроваджують небезпечний інструмент, який стає зброєю лише в потрібний момент.

Стратегічний контекст

Після початку широкомасштабної війни в Газі (жовтень 2023 р.) Хезболла на північному кордоні Ізраїлю стала головною загрозою. Організація мала десятки тисяч ракет і добре захищену систему командування та зв'язку. Ізраїль розумів, що у випадку повномасштабної війни на два фронти втрати будуть

колосальними. Моссаду було поставлено завдання – знайти спосіб максимально послабити командну структуру Хезболли до початку великої війни [9;10;23;41].

Підготовка операції (2014–2024 рр.)

Операція була спланована щонайменше за 10 років. Моссад через мережу підставних компаній повністю взяв під контроль один з основних каналів постачання засобів зв'язку для Хезболли (переважно з Тайваню та Китаю).

Ключові етапи підготовки:

- Створення фіктивних компаній у кількох країнах.
- Отримання тендеру на постачання тисяч пейджерів і портативних рацій для Хезболли.
- Вбудовування у кожен пристрій невеликого заряду вибухівки з дистанційним підривом + спеціального хімічного компонента, що посилював ураження.
- Тестування на прототипах протягом кількох років.
- Забезпечення, щоб пристрої пройшли всі перевірки якості та виглядали абсолютно звичайними.

Операція вимагала колосальних ресурсів, терпіння та ідеальної конспірації. За оцінками експертів, у ній брали участь сотні людей на різних етапах.

Хід операції (17–18 вересня 2024 р.)

17 вересня 2024 року о 15:30 за місцевим часом одночасно вибухнули тисячі пейджерів, якими користувалися бійці та командири Хезболли. Наступного дня (18 вересня) вибухнули тисячі рацій [41].

Наслідки були шокуючими:

- Близько 3 000–4 000 поранених і кілька сотень загиблих (включаючи високопоставлених командирів).
- Повна дезорганізація середнього та вищого командного складу Хезболли.
- Психологічний шок у всьому угрупованні – втрата довіри до будь-яких технічних засобів [41].

Результати

Операція досягла стратегічного ефекту:

- Значно послабила командну вертикаль Хезболли перед можливим великим конфліктом.
- Змусила організацію перейти на примітивні засоби зв'язку (гонці, дротові телефони), що різко знизило ефективність.
- Стала потужним психологічним ударом – Хезболла зрозуміла, що Моссад може вразити їх у будь-який момент і будь-яким способом.

Сильні сторони операції

- Надзвичайно креативний і нестандартний підхід.
- Ідеальне довгострокове планування (10+ років).
- Мінімальний ризик для ізраїльських сил.
- Максимальний психологічний та оперативний ефект.
- Важко відслідкувати авторство (до останнього моменту Хезболла не розуміла, що відбувається).

Слабкі сторони

- Цивільні жертви (пейджери використовували також цивільні та діти).
- Іран і Хезболла отримали потужний привід для пропаганди.
- Після інциденту супротивник почав значно серйозніше ставитися до кібер- та технічної безпеки ланцюгів постачання.

Уроки для України

Операція з пейджерами – одна з найбільш релевантних для України операцій Моссаду:

- Демонструє ефективність довгострокового проникнення в логістичні ланцюги супротивника.
- Показує, як можна перетворити звичайну електроніку (рації, дрони, чіпи, навушники) на зброю.
- Підкреслює важливість роботи з китайськими та іранськими компонентами, які активно використовує Росія.

- Є прикладом «м'якого», але надзвичайно болісного удару по командній інфраструктурі противника.

Українські спецслужби вже мають досвід подібних операцій. Досвід Моссаду може бути використаний для системної роботи з російською військовою логістикою, електронікою та засобами зв'язку [9;10;23;31;41].

3. Операція «Rising Lion» («Ревучий лев», червень 2025 р.)

Операція «Rising Lion» стала однією з найбільших превентивних кампаній Моссаду в сучасній історії. Вона була проведена в червні 2025 року як відповідь на прискорення Іраном ядерної та ракетної програм і зростання прямої загрози Ізраїлю. Ця операція демонструє новий рівень гібридних можливостей Моссаду – здатність проводити масштабні, координовані, багатодоменні удари по території головного супротивника з мінімальним використанням звичайних військових сил [9;10;23;14].

Стратегічний контекст

До середини 2025 року Іран значно просунувся у збагаченні урану, наблизившись до порогу створення ядерної зброї. Одночасно активізувалася «вісь опору» – Хезболла, хусити та проіранські угруповання в Іраку і Сирії. Ізраїльське керівництво прийняло рішення про проведення масштабної превентивної операції, щоб відкинути іранську ядерну програму на роки назад і продемонструвати силу перед можливою регіональною ескалацією [9;10;23].

Операція отримала назву «Rising Lion» («Ревучий лев») – символізуючи силу та рішучість Ізраїлю.

Цілі операції

- Знищення або серйозне пошкодження ключових ядерних об'єктів в Натанзі, Ісфахані та Фордо.
- Ураження ракетних заводів і складів балістичних ракет.
- Ліквідація або нейтралізація високопоставлених керівників Корпусу вартових Ісламської революції (IRGC), відповідальних за ядерну програму.

- Демонстрація Ірану та його союзникам, що Ізраїль готовий діяти жорстко і на випередження [9;10;23].

Підготовка

Підготовка тривала понад 18 місяців під безпосереднім контролем директора Моссаду Давида Барнеа. Була створена об'єднана оперативна група, до якої увійшли:

- Tzomet – глибока агентурна мережа всередині Ірану.
- Keshet – кібернетична підтримка.
- Komemiyut («Кідон») – спеціальні оперативні групи.
- Технологічний департамент і підрозділи дронів.
- Тісна координація з АМАН (військова розвідка) і Повітряними силами Ізраїлю.

Моссад отримав детальну інформацію про нові іранські об'єкти, системи ППО та зміни в охороні. Було проведено численні симуляції в VR–середовищі [9;10;23;14;25].

Хід операції (червень 2025 р.)

Операція тривала кілька днів і проходила у кілька хвиль:

1. Кібернетична фаза – потужні кібератаки на системи ППО та зв'язку Ірану (Keshet).
2. Агентурно–диверсійна фаза – агенти та спеціальні групи провели саботаж на об'єктах зсередини.
3. Повітряно–дронова фаза – масоване використання дронів–камікадзе та високоточних засобів ураження.
4. Точкові ліквідації – «Кідон» ліквідував кількох ключових іранських командирів і вчених.

Удари були максимально селективними – основний акцент робився на науково–технічній інфраструктурі, а не на цивільних об'єктах [9;10;23;14;25].

Результати

- Серйозно пошкоджено кілька ключових ядерних об'єктів.
- Знищено значну частину запасів балістичних ракет середньої дальності.

- Ліквідовано або виведено з ладу декілька високопоставлених фігур IRGC.
- Іранська ядерна програма була відкинута на 2–3 роки назад.
- Операція продемонструвала Ірану, що Моссад може завдавати ударів по території країни практично в будь-який момент.

Сильні сторони

- Відмінна координація всіх компонентів (кібер + агентура + дрони + спецпідрозділи).
- Висока точність і селективність ударів.
- Мінімальні втрати з ізраїльської сторони.
- Потужний психологічний ефект.

Слабкі сторони

- Іран отримав привід для подальшої ескалації та зміцнення альянсів.
- Частина об'єктів була швидко відновлена або перенесена в інші місця.
- Зростання міжнародного тиску на Ізраїль.

Уроки для України

Операція «Rising Lion» надзвичайно актуальна для України:

- Показує ефективність превентивних багатоцільових ударів по військово-технічній інфраструктурі супротивника.
- Підкреслює важливість поєднання кібератак, агентурної роботи та дронів ударів.
- Демонструє цінність точкових ліквідацій ключових фахівців і командирів.
- Є прикладом того, як можна значно уповільнити військову машину противника без повномасштабного вторгнення.

5. Операція «Epic Fury» («Ревучий лев» / «Roaring Lion», лютий–травень 2026 р.)

Операція «Epic Fury» (кодова назва США) та її ізраїльський компонент «Rising Lion» / «Roaring Lion» стала однією з наймасштабніших превентивних багатодомених кампаній сучасності. Вона розпочалася 28 лютого 2026 року як

спільна американо–ізраїльська військово–розвідувальна операція проти Ірану і тривала до початку травня 2026 року, завершившись оголошенням перемир'я [9;10;23;14].

Стратегічний контекст і причини проведення.

Головним каталізатором стало критичне наближення Ірану до ядерного порогу. За даними МАГАТЕ та розвідки Моссаду, Тегеран досяг рівня збагачення урану 90 % і накопичив достатньо матеріалу для швидкого виготовлення ядерних боєголовок. Паралельно Іран інтенсифікував підтримку «вісі опору» – Хезболли, хуситів, ХАМАС та проіранських угруповань у регіоні. Переговори в Женеві (зима 2025–2026 рр.) остаточно зайшли в глухий кут. Прем'єр–міністр Ізраїлю Беньямін Нетаньяху та адміністрація президента США Дональда Трампа дійшли спільного висновку про необхідність превентивного удару. Моссад надав ключові розвіддані, які стали основою для спільного рішення [9;10;23].

Підготовка та роль Моссаду.

Підготовка тривала понад 18 місяців під безпосереднім керівництвом директора Моссаду Давида Барнеа. Підрозділи Tzomet (агентурна розвідка), Keshet (кібер– та електронна розвідка) і Caesarea / Komemiyut («Кідон») провели комплексне проникнення. Агенти заздалегідь розмістили в Ірані високоточну вибухівку, дрони–камікадзе та системи наведення поблизу стратегічних об'єктів (Натанз, Ісфахан, Фордо). Кібератаки паралізували системи ППО та зв'язку ще до початку основної фази [9;10;23;14;33].

Участь партнерів і хід операції.

Операція була повністю спільною американо–ізраїльською. Ізраїльські ВПС та підрозділи Моссаду завдали першого удару, американські стратегічні бомбардувальники B–2 Spirit застосували bunker buster'и по підземних об'єктах. Загалом було здійснено понад 10 200 авіаційних вильотів і уражено понад 13 000 цілей. Іран відповів масованими ракетно–дроновими атаками, зокрема тисячами дронів типу Shahed, проте більшість із них було нейтралізовано [23;14].

Результати.

Операція суттєво відкинула іранську ядерну програму на 3–5 років, значно послабила ракетний потенціал і обезголовлювала командування Корпусу вартових Ісламської революції. Водночас вона продемонструвала нові реалії сучасної війни – поєднання людської розвідки, кіберу, дронів і високоточних ударів.

Актуальність досвіду України для операції «Epic Fury» та перспективи двостороннього обміну

Особливу наукову та практичну цінність для аналізу операції «Epic Fury» становить досвід України, який міг би бути надзвичайно ефективним і навіть вирішальним у ході такої кампанії. Україна, яка з 2022 року протистоїть масованому застосуванню іранських дронів–камікадзе Shahed–136/Geran–2 російськими окупантами, розробила одну з найефективніших у світі систем протидії саме цьому типу загроз. Якби ізраїльсько–американська коаліція могла скористатися українським досвідом ще на етапі планування, ефективність нейтралізації іранських Shahed під час відповіді Тегерана могла б бути значно вищою.

По–перше, українська модель ешелонованої дешевої ППО. На відміну від традиційного дорогого підходу, Україна створила багат шарову систему, що поєднує стратегічний рівень (Patriot, SAMP/T), оперативно–тактичний (NASAMS, IRIS–T), тактичний (Gerard, «Богдана») та найнижчий «дешевий щит» (мобільні вогневі групи, FPV–дрони–перехоплювачі, системи електронної боротьби, лазерні комплекси та акустичні сенсори). Ефективність перехоплення Shahed у 2025–2026 роках сягала 80–90 %. Цей досвід міг би суттєво посилити оборону Ізраїлю та американських баз у регіоні під час іранської відповіді.

По–друге, масштабне застосування водних (морських) дронів. Україна є світовим лідером у розробці та бойовому застосуванні морських безпілотників (Magura V5, Sea Baby, «Очерет»). Ці платформи успішно знищували російські кораблі Чорноморського флоту, змусивши противника передислокувати сили.

У контексті Перської затоки українські технології морських дронів могли б стати потужним асиметричним інструментом для блокування іранських морських комунікацій та логістики.

По–третє, практична передача експертизи. Україна не лише розробила ефективні рішення, але й активно ділиться ними. У 2024–2026 роках українські спеціалісти та експерти з протидії дронам і створення ешелонованої ППО були залучені до підготовки сил ППО в більшості країн Перської затоки (Саудівська Аравія, ОАЕ, Катар, Бахрейн, Кувейт). Українські інструктори проводили навчання, передавали технології та допомагали адаптувати системи під місцеві умови. Цей досвід міг би стати безпосереднім внеском України в спільну американо–ізраїльську операцію, особливо в частині протидії іранським дронівим і ракетним атакам.

Таким чином, операція «Epic Fury» яскраво ілюструє двосторонній характер обміну досвідом між Ізраїлем та Україною. Якщо Моссад демонструє виняткову майстерність у превентивних агентурно–кібернетичних операціях і довгостроковому проникненні в логістичні ланцюги противника, то Україна пропонує унікальний, перевірений у реальних бойових умовах досвід масового протистояння дронівим атакам, створення економічно ефективної ешелонованої ППО та застосування морських безпілотників. Саме поєднання цих двох підходів могло б стати основою для ще більш ефективних спільних операцій у майбутньому.

Сильні сторони операції: виняткова координація розвідки, кібер– та авіаційних компонентів, принцип випереджального удару, довгострокове планування.

Слабкі сторони: ризик регіональної ескалації, цивільні жертви, можливість швидкого відновлення противником втрачених спроможностей, складні міжнародно–правові наслідки.

Для України досвід «Epic Fury» підтверджує правильність обраного шляху – поєднання оборонних інновацій (ешелонована ППО, водні дрони, протидія Shahed) з наступальними можливостями спеціальних служб. Водночас він

підкреслює перспективу подальшого обміну знаннями з Ізраїлем: українські технології та бойовий досвід можуть стати цінним доповненням до Моссадівських методів у протидії спільним загрозам [12;14;32;34].

ВИСНОВКИ до розділу 2

Другий розділ магістерської роботи був присвячений комплексному аналізу оперативної діяльності ізраїльської розвідки «Моссад» – одного з найефективніших інструментів забезпечення національної безпеки Держави Ізраїль. У підрозділі 2.1 розглянуто основні методи та засоби діяльності організації, а в підрозділі 2.2 – найвідоміші операції, що демонструють практичне застосування цих методів у реальних умовах. Проведений аналіз дозволяє зробити ряд важливих узагальнень, які мають не лише теоретичне, а й виразне практичне значення для системи національної безпеки України.

Оперативна діяльність Моссаду характеризується комплексністю, проактивністю та технологічною інноваційністю. Основними методами залишаються класична агентурна розвідка (HUMINT), електронна та кібернетична розвідка (SIGINT), спеціальні операції (включаючи точкові ліквідації та саботаж), операції впливу та довгострокове проникнення в логістичні та технологічні ланцюги противника. Особливої уваги заслуговує принцип «випереджального удару» (preventive strike), який дозволяє Моссаду діяти на випередження загрози, а не реагувати на неї постфактум. Сучасний етап діяльності організації демонструє глибоку інтеграцію новітніх технологій – штучного інтелекту, дронів, кіберзасобів та shell-компаній – з традиційними оперативними практиками. Саме це поєднання забезпечує Моссаду унікальну оперативну ефективність при порівняно невеликих ресурсах [9;10;23;48].

Аналіз найвідоміших операцій підтверджує високу результативність моссадівських методів. Операція з пейджерів Хезболли (вересень 2024 р.) стала класичним прикладом «троянської» операції XXI століття: багаторічне проникнення в ланцюг постачання дозволило одночасно вивести з ладу тисячі бойовиків і командування угруповання. Операція «Rising Lion» (2025 р.) та особливо спільна американо-ізраїльська операція «Epic Fury» / «Roaring Lion» (лютий-травень 2026 р.) продемонстрували новий рівень багатодомених дій – поєднання агентурної роботи, кібератак, високоточних авіаційних ударів і

спеціальних операцій. Ці кейси показали, що сучасна розвідка здатна суттєво впливати на стратегічний баланс сил навіть проти значно чисельнішого та ресурсно забезпеченого противника [35;45;33;41].

Водночас проведений аналіз виявив і певні слабкі сторони оперативної діяльності Моссаду. По–перше, високий рівень ризику ескалації: превентивні дії часто призводять до відповідних ударів і регіонального напруження. По–друге, наявність цивільних жертв і пов’язані з цим репутаційні та міжнародно–правові наслідки. По–третє, можливість противника до швидкого відновлення втрачених спроможностей (знання, кадри, підземна інфраструктура). Ці ризики підкреслюють, що навіть найуспішніші операції не завжди гарантують довгостроковий стратегічний результат без комплексної політичної та дипломатичної підтримки.

Особливе значення для України має порівняльний аналіз досвіду Моссаду з українськими реаліями. Досвід Ізраїлю у превентивних операціях і довгостроковому проникненні в логістичні ланцюги противника (як у випадку з пейджерами чи ядерними об’єктами Ірану) є надзвичайно цінним. Однак не менш важливим є зворотний потік досвіду – від України до Ізраїлю та його партнерів. Українські спецслужби та ЗСУ за 2022–2026 роки розробили одну з найефективніших у світі систем протидії масованим дронівим атакам типу Shahed–136/Geran–2. Ешелонована дешева ППО, що поєднує стратегічні комплекси (Patriot, NASAMS), тактичні засоби (Gepard, IRIS–T) та «дешевий щит» (FPV–дрони, мобільні вогневі групи, системи РЕБ), продемонструвала ефективність перехоплення на рівні 80–90 %. Цей досвід уже активно передається: українські спеціалісти та інструктори працювали в 2024–2026 роках у більшості країн Перської затоки (Саудівська Аравія, ОАЕ, Катар, Бахрейн, Кувейт), допомагаючи адаптувати системи ППО до місцевих умов.

Не менш вагомим є український досвід застосування водних (морських) безпілотників (Magura V5, Sea Baby, «Очерет»). Успішні атаки на російський Чорноморський флот стали світовим прецедентом асиметричної морської війни. У контексті операції «Еріс Фуру» українські технології морських дронів могли б

стати потужним додатковим інструментом для блокування іранських морських комунікацій у Перській затоці. Таким чином, український бойовий досвід не лише доповнює, а й суттєво посилює моссадівські методи, створюючи основу для взаємовигідного оперативно–технічного обміну між двома державами.

Підсумовуючи, оперативна діяльність Моссаду є еталоном сучасної розвідувально–диверсійної роботи в умовах асиметричних і гібридних загроз. Її ключовими принципами залишаються випереджальний характер дій, максимальна інтеграція технологій, висока оперативна автономія та глибока агентурна робота. Водночас український досвід протидії масованим дронним і ракетним атакам, створення ешелонованої дешевої ППО та застосування морських безпілотників демонструє, що ефективність національної безпеки в сучасних умовах визначається не лише превентивними ударами, а й стійкою, багаторівневою системою оборони та асиметричними наступальними інструментами.

Отримані в розділі результати дозволяють перейти до третього розділу, де буде проведено порівняльний аналіз спецслужб Ізраїлю та України та сформульовано конкретні рекомендації щодо адаптації досвіду Моссаду до вітчизняних умов з урахуванням національних особливостей, ризиків і вже наявних українських досягнень.

РОЗДІЛ 3.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ДОСВІДУ МОССАДУ В ОРГАНІЗАЦІЇ ТА ДІЯЛЬНОСТІ УКРАЇНСЬКИХ СПЕЦСЛУЖБ

3.1. Порівняльний аналіз спецслужб Ізраїлю та України

Порівняльний аналіз спецслужб Ізраїлю (Моссад, Шабак / Шин–Бет, АМАН) та України (Служба безпеки України, Головне управління розвідки Міністерства оборони України, Служба зовнішньої розвідки України) є центральним методологічним інструментом даного дослідження. Він дозволяє не лише об'єктивно зіставити дві системи національної безпеки, що функціонують в умовах постійної екзистенційної та гібридної загрози, а й науково обґрунтувати, які саме елементи ізраїльського досвіду можуть бути адаптовані до українських реалій без механічного копіювання. Ізраїльська модель сформувалася в умовах перманентної війни на знищення, обмежених територіальних і людських ресурсів та необхідності приймати швидкі, жорсткі рішення. Українська система успадкувала пострадянську бюрократичну спадщину, переживає глибокі реформи під впливом європейських стандартів і водночас накопичила унікальний, перевірений у реальних бойових умовах досвід протидії масованій гібридній агресії Російської Федерації з 1991 року (з відкритою фазою з 2014 року).

Актуальність такого порівняння зумовлена тим, що станом на 2026 рік Україна перебуває в умовах тривалої війни, яка поєднує конвенційні бойові дії, масоване застосування іранських дронів–камікадзе, кібертероризм, економічний тиск і політичну дестабілізацію. Ізраїль же десятиліттями успішно протистоїть подібним загрозам («вісь опору» – Іран, Хезболла, ХАМАС, хусити) при значно менших територіальних і демографічних ресурсах. Тому системне зіставлення дозволяє виявити ті інституційні, правові, кадрові та технологічні рішення, які можуть суттєво підвищити ефективність української системи національної безпеки.

Порівняння здійснюється за такими ключовими параметрами: структура та підпорядкування, законодавча база, основні функції та повноваження, система підготовки та відбору кадрів, ресурсне (фінансове) забезпечення, механізми координації та взаємодії між відомствами, а також сильні та слабкі сторони кожної моделі. Аналіз базується на відкритих офіційних документах, аналітичних доповідях Національного інституту стратегічних досліджень, СБУ, ГУР МО, ізраїльських джерелах та матеріалах міжнародних дослідницьких центрів станом на травень 2026 року [9;10;38;39;31].

3.1.1. Структура та підпорядкування

Порівняльний аналіз організаційно–правових засад і структури спецслужб Ізраїлю та України є ключовим етапом дослідження, оскільки саме в цих аспектах найяскравіше проявляються відмінності моделей національної безпеки двох держав. Моссад як зовнішня розвідка Ізраїлю демонструє модель максимальної оперативної автономії, мінімальної бюрократії та прямого підпорядкування вищому політичному керівництву, що забезпечує швидкість і ефективність дій у умовах постійної екзистенційної загрози. Натомість українська система спецслужб (СБУ та ГУР МО України) сформувалася в умовах пострадянської спадщини, тривалої гібридної агресії Російської Федерації з 1991 року та повномасштабного вторгнення з 2022 року, що зумовило більшу централізацію, ширші слідчі повноваження та певну залежність від політичного циклу [9;10;23;38;39;47].

Аналіз цих моделей дозволяє не лише виявити сильні та слабкі сторони кожної, але й визначити конкретні елементи ізраїльського досвіду, які можуть бути адаптовані до українських реалій без порушення конституційних принципів і демократичних стандартів.

Організаційно–правові засади та структура спецслужб Ізраїлю

Ізраїльська система зовнішньої розвідки базується на принципі прямого підпорядкування Прем'єр–міністру, закладеному ще Давидом Бен–Гуріоном у 1949–1951 роках. Офіційна назва Моссаду – «Інститут розвідки та спеціальних завдань» (івр. HaMossad leModi'in uleTafkidim Meyuhadim) – підкреслює його

статус як самостійного інституту, діяльність якого регулюється не детальним парламентським законом, а директивами Прем'єр-міністра [9;23;14]. Це забезпечує унікальну оперативну свободу: Моссад не підзвітний парламенту (Кнесету) у повному обсязі, його бюджет і штатна чисельність є державною таємницею. За оцінками експертів, бюджет Моссаду становить близько 10 млрд шекелів (приблизно 2,7 млрд дол. США), а штат – кілька тисяч висококваліфікованих оперативників (значно менше, ніж у СБУ чи ГУР МО).

Ключовим елементом координації є посада «Хамемуне» (Hamemuneh – «відповідальний»), яку історично обіймав директор Моссаду (зокрема Ісер Гарель у 1952–1963 рр.). Ця посада забезпечує єдине керівництво всіма трьома головними спецслужбами Ізраїлю:

- Моссад – зовнішня розвідка, спеціальні операції за кордоном, агентурна робота;
- Шабак (Шин-Бет) – внутрішня безпека, контртероризм, захист державних установ;
- АМАН – військова розвідка, підпорядкована Генеральному штабу ЗС Ізраїлю [9;23;14].

Структура Моссаду включає спеціалізовані підрозділи, орієнтовані на максимальну ефективність:

- Tzomet – відділ глибокої агентурної розвідки (HUMINT), вербування та робота з джерелами в країнах-противниках;
- Caesarea / Komemiyut («Кідон») – елітний підрозділ спеціальних операцій і точкових ліквідацій;
- Keshet – кібернетична та технічна розвідка (SIGINT), розробка складних кіберзасобів (приклад – Stuxnet);
- інші департаменти: аналізу, логістики, технологій, прикриття та «периферійної дипломатії».

Така структура забезпечує інтеграцію всіх доменів (агентурного, кібернетичного, спеціальних операцій) під єдиним політичним керівництвом, мінімізуючи міжвідомчі конфлікти [9;10;23].

Організаційно–правові засади та структура спецслужб України

Українська система спецслужб регулюється детальною законодавчою базою, що відрізняє її від ізраїльської моделі. Основним нормативним актом для Служби безпеки України (СБУ) є Закон України «Про Службу безпеки України» від 25.03.1992 № 2229–ХІІ (у редакції станом на 09.01.2025 з подальшими змінами законами № 4156–ІХ, № 4344–ІХ, № 4542–ІХ, № 4633–ІХ). СБУ підпорядкована Президенту України (ст. 5 Закону) і виконує функції контррозвідки, боротьби з тероризмом, захисту державної таємниці, кібербезпеки та слідчі повноваження. У 2025 році відбулися значні реформи: збільшено граничну чисельність до понад 41 тис. осіб, посилено соціальні гарантії, уточнено функції та надано право СБУ самостійно розробляти та вносити проекти нормативно–правових актів. Водночас СБУ зберігає широкі повноваження, що наближає її до моделі «силового відомства», а не «чистої» розвідки [3;4;38;39;47].

Головне управління розвідки Міністерства оборони України (ГУР МО) діє на підставі Закону України «Про розвідку» та підпорядковане Міністру оборони, але в практиці воєнного часу фінансується окремим бюджетним рядком і координується безпосередньо з вищим військово–політичним керівництвом (Президентом). Структура ГУР включає департаменти стратегічної розвідки, інформаційного забезпечення, розвідувального забезпечення Генштабу, кадрової політики та спеціальні підрозділи (10–й окремий загін спеціального призначення, «Kraken», «Firebird», «Шаман» та інші). ГУР орієнтоване переважно на військову розвідку, спеціальні операції за кордоном і диверсійно–розвідувальну діяльність, що робить його найближчим аналогом Моссаду в українській системі [3;4;38;39;47].

Додатковим елементом є Служба зовнішньої розвідки України (СЗР), яка також підпорядкована Президенту і відповідає за політичну та економічну розвідку за кордоном.

Спільне та відмінне: аналіз

Спільні риси очевидні в умовах асиметричних і гібридних загроз. Як Ізраїль з 1948 року, так і Україна з 1991 року (а особливо з 2014–2022 рр.) зіткнулися з екзистенційною агресією. Обидві системи акцентують увагу на агентурній розвідці (HUMINT), кіберопераціях, спеціальних акціях та випереджальному характері дій. Українські спецслужби (особливо ГУР МО) вже демонструють «моссадівський» стиль: зухвалі операції на території РФ, точкові удари по логістиці, флоту та ключових фігурах противника. Координація між СБУ, ГУР та ЗСУ через РНБО певною мірою нагадує ізраїльський механізм «Хамемуне».

Головні відмінності полягають у трьох аспектах:

1. Ступінь оперативної автономії та бюрократії. Моссад діє за принципом «мінімум паперів – максимум результату». СБУ, навпаки, обтяжена детальним законодавчим регулюванням і політичним контролем, що іноді уповільнює прийняття рішень.
2. Ширина повноважень. СБУ поєднує розвідувальні, контррозвідувальні та слідчі функції, що відрізняє її від «чистого» розвідувального профілю Моссаду.
3. Політична підзвітність. Пряме підпорядкування Прем'єру в Ізраїлі забезпечує стабільність і швидкість; в Україні президентська вертикаль створює ризики політизації (хоча в умовах війни це також має переваги централізованого управління).

Таким чином, організаційно–правова модель Ізраїлю є більш гнучкою та ефективною в умовах постійної загрози, тоді як українська модель адаптована до демократичних стандартів і широкого спектра внутрішніх загроз. Саме ця різниця становить основу для подальшого порівняльного аналізу методів роботи та визначення потенціалу адаптації.

3.2. Порівняння методів оперативної діяльності та законодавчого регулювання

Порівняння методів оперативної діяльності та законодавчого регулювання спецслужб Ізраїлю та України дозволяє виявити не лише відмінності в інструментарії та правових межах їхньої роботи, але й ті елементи ізраїльського досвіду, які можуть бути адаптовані до українських умов без порушення демократичних стандартів і конституційних принципів. Якщо організаційно–правова модель (підрозділ 3.1) визначає «архітектуру» спецслужб, то методи оперативної діяльності є її «операційною системою», а законодавче регулювання – «рамками дозволеного». Моссад демонструє максимальну гнучкість, проактивність і інтеграцію технологій з класичними оперативними практиками в умовах постійної екзистенційної загрози. Українські спецслужби (СБУ та ГУР МО України), навпаки, діють у складнішому правовому полі, обтяженому пострадянською спадщиною, вимогами ЄС/НАТО та необхідністю поєднувати розвідувальну, контррозвідувальну і слідчу діяльність.

3.2.1. Порівняння методів оперативної діяльності

Методи оперативної діяльності Моссаду характеризуються комплексністю, проактивністю («випереджальний удар» – preventive strike) та глибокою інтеграцією HUMINT, SIGINT, кібер– та спеціальних операцій. Основний акцент робиться на довгостроковому проникненні в логістичні ланцюги противника, точкових акціях та максимальній конспірації [8;10;12]. Класичними прикладами є:

Глибока агентурна розвідка (HUMINT): підрозділ Tzomet забезпечує вербування джерел безпосередньо в країнах–противниках (Іран, Сирія, Ліван). Операція з пейджерами «Хезболли» (вересень 2024 р.) стала вершиною такого проникнення – Моссад контролював ланцюг постачання протягом 10 років [9;10;23;41].

Спеціальні операції та точкові ліквідації: підрозділ «Кідон» (Komemiyut/Caesarea) реалізував операцію «Гнів Божий» (1972–1980-ті рр.), серію ліквідацій іранських ядерників (2007–2012 рр.) та інші акції [9;10;27;25].

Кібер– та технічна розвідка (SIGINT/Keshet): операція Stuxnet (2009–2010 рр.) – спільний ізраїльсько–американський проект, який уповільнив іранську ядерну програму на 1–2 роки без жодного пострілу [9;10;25].

Операції впливу та «троянські» акції: довгострокове планування (операція «Rising Lion» 2025 р., «Epic Fury»/«Roaring Lion» 2026 р.) з використанням дронів, shell–компаній та агентурного прикриття [25;41].

Українські спецслужби вже демонструють значну подібність до моссадівського стилю, особливо ГУР МО України. З 2022 року ГУР провело десятки зухвалих операцій на території РФ: знищення кораблів Чорноморського флоту (морські дрони «Magura V5», «Sea Baby»), ліквідації ключових логістичних фігур, удари по нафтопереробних заводах, операції проти «вагнерівців» тощо. СБУ ефективно проводить контррозвідувальні операції, кібердиверсії та антитерористичні заходи [30;51].

Сильні сторони Моссаду: максимальна креативність, довгострокове планування, мінімальний ризик для власних сил, інтеграція технологій.

Слабкі сторони: ризик міжнародних скандалів (Ліллекхаммер 1973 р.), цивільні жертви, можливість швидкого відновлення противника.

Українські спецслужби вже досягли значних успіхів у асиметричній війні (морські дрони, ешелонована ППО проти Shahed), але поступаються в системності глибокого агентурного проникнення та довгострокових «троянських» операціях через обмеженість ресурсів і правові рамки.

3.2.2. Порівняння законодавчого регулювання

Законодавче регулювання діяльності Моссаду в Ізраїлі є мінімальним і максимально гнучким. Діяльність Інституту розвідки та спеціальних завдань регулюється переважно директивами Прем'єр–міністра та рішеннями Комітету керівників служб («Вараш»). Відсутність детального парламентського закону дозволяє Моссаду діяти за кордоном з високим ступенем оперативної свободи.

Правові межі визначаються політичним рішенням вищого керівництва держави, а не жорсткими статтями закону. Це забезпечує швидкість, але створює ризики недостатнього демократичного контролю [9;23;14].

В Україні законодавча база є значно детальнішою та жорсткішою, що відповідає демократичним стандартам і вимогам європейської інтеграції.

Основні нормативні акти:

- Закон України «Про Службу безпеки України» № 2229–XII (редакція станом на 10.05.2025 з правками законами № 4156–IX, № 4344–IX, № 4542–IX від 16.07.2025, № 4633–IX від 09.10.2025). Закон розширив повноваження СБУ (право самостійно вносити проекти НПА, використання зброї за правилами ЗСУ в АТО/обороні, збільшення чисельності ЦСО «А» до 10 тис. осіб).
- Закон України «Про розвідку» (зміни 2025 р., зокрема № 4684–IX від 05.11.2025 щодо проходження військової служби розвідниками).
- Закон України «Про національну безпеку України» (2018, з воєнними правками).
- Положення про ГУР МО, накази та інструкції під час воєнного стану [3;4;38;39;47].

Ключові відмінності в законодавчому регулюванні:

1. Оперативна свобода за кордоном: Моссад має широкі повноваження на проведення спеціальних операцій без додаткових погоджень. В Україні дії за кордоном (особливо силові) вимагають координації через РНБО, Президента та дотримання міжнародного права (Європейська конвенція з прав людини, Женевські конвенції).
2. Використання силових методів: Ізраїльська модель дозволяє точкові ліквідації як елемент превентивної самооборони. В Україні такі дії можливі переважно в умовах воєнного стану, але вимагають чіткого правового обґрунтування.

3. Контроль і підзвітність: В Ізраїлі – переважно внутрішній (Прем'єр, «Вараш»). В Україні – парламентський контроль (комітети ВРУ), РНБО, міжнародні партнери (ЄС/НАТО) та судовий нагляд.
4. Реформи 2025 року: Закони № 4542–ІХ та № 4633–ІХ значно наблизили СБУ до сучасних стандартів (розширення прав, соціальні гарантії, фокус на контррозвідці та кібербезпеці), але не вирішили проблему надмірної бюрократії та слідчих функцій [3;4;38;39;47].

Методи оперативної діяльності Моссаду є еталоном ефективності в умовах асиметричних загроз завдяки гнучкості, технологічній інтеграції та оперативній автономії. Українські спецслужби вже опанували багато моссадівських підходів на практиці, але стикаються з обмеженнями законодавчого характеру. Законодавче регулювання в Ізраїлі забезпечує швидкість і результативність, тоді як в Україні – демократичність і підзвітність, що є безумовною цінністю. Саме ця різниця створює ґрунт для адаптації (підрозділи 3.3–3.5): Україна може запозичити оперативну гнучкість Моссаду через точкові законодавчі зміни (зміни до Закону «Про СБУ» та «Про розвідку»), посилення координації та елітної підготовки, зберігаючи при цьому демократичний контроль.

3.3. Потенціал адаптації досвіду Моссаду до українських реалій

Аналіз організаційно–правових засад (підрозділ 3.1) та порівняння методів оперативної діяльності й законодавчого регулювання (підрозділ 3.2) демонструють, що досвід Моссаду має високий потенціал адаптації до українських умов. Україна, як і Ізраїль, перебуває в стані тривалої екзистенційної загрози: гібридна агресія РФ триває з 1991 року, відкритий збройний конфлікт – з 2014 року, а повномасштабна війна – з лютого 2022 року. За цих обставин модель Моссаду, яка забезпечує максимальну оперативну автономію, проактивність («випереджальний удар»), глибоку інтеграцію технологій і елітну підготовку кадрів при відносно невеликих ресурсах, є особливо цінною. Водночас адаптація не може бути механічною копією: вона повинна враховувати демократичні стандарти, європейський вектор розвитку, специфіку

пострадянської правової системи та вже наявні досягнення українських спецслужб (СБУ, ГУР МО України, СЗР) [9;10;23;38;39;31].

Потенціал адаптації реалізується на трьох рівнях: стратегічному (організаційна модель і підпорядкування), оперативному (методи та інструменти) та кадрово–технологічному (підготовка та інтеграція з приватним сектором). Нижче проведено детальний аналіз кожного напрямку з урахуванням українських реалій 2025–2026 років.

3.3.1. Стратегічний потенціал: організаційна модель та пряме підпорядкування

Однією з головних переваг Моссаду є пряме підпорядкування Прем'єр-міністру та статус самостійного інституту, що мінімізує бюрократію і забезпечує швидкість прийняття рішень. В Україні аналогічний механізм частково реалізовано через підпорядкування СБУ та СЗР Президенту, а ГУР МО – Міністру оборони з фактичною координацією через РНБО. Однак існують суттєві прогалини:

- Надмірна бюрократія та міжвідомча конкуренція (СБУ – ГУР – СЗР – військова контррозвідка).
- Політизація процесів під час зміни влади.
- Відсутність єдиного координаційного органу на кшталт ізраїльського «ХаМемуне» (посада «відповідального» за всі розвідки).

Потенціал адаптації полягає у створенні Національного координаційного центру розвідки (або посади «Національного розвідувального координатора») при Президентові чи РНБО. Такий центр міг би забезпечити єдине стратегічне планування, розподіл завдань і оперативну взаємодію між СБУ, ГУР, СЗР та іншими суб'єктами. Подібна модель уже частково апробована в умовах воєнного стану (рішення РНБО 2022–2026 рр.), але потребує законодавчого закріплення. Адаптація цього елемента дозволить українським спецслужбам перейти від реактивної до проактивної стратегії, як це робить Моссад у протидії Ірану та «Хезболлі» [9, с.18-22; 23, с.45-50; 3; 4; 38; 39; 47].

3.3.2. Оперативний потенціал: методи та інструменти

Українські спецслужби вже активно застосовують багато моссадівських методів, проте їхня системність і масштабність значно нижчі. Високий потенціал адаптації існує за такими напрямками:

1. Довгострокове проникнення в логістичні та технологічні ланцюги противника (приклад – операція з пейджером «Хезболли» 2024 р.). Україна може створити спеціальні оперативно–технічні групи для роботи з російською електронікою, чіпами, дронами та АСУ ТП. ГУР уже має досвід морських дронів і кібероперацій – це прекрасна база для «троянських» операцій на кшталт Stuxnet.
2. Системні точкові операції та превентивні дії. Досвід «Кідону» та ліквідацій іранських ядерників може бути адаптований через розширення повноважень спеціальних підрозділів ГУР і ЦСО «А» СБУ щодо нейтралізації ключових фігур ворожої логістики, командування та науково–технічного персоналу (виробники ракет, дронів, електроніки). Умови воєнного стану вже дозволяють такі дії, але потребують чіткішого правового регулювання.
3. Інтеграція кібер–, дронівих та агентурних можливостей. Моссад досягнув успіху завдяки Keshet і Tzomet. Україна має світовий рівень у розробці морських і FPV–дронів та ешелюваної ППО. Поєднання цих технологій з глибокою агентурою відкриває перспективи для комплексних операцій на території РФ [9, с.280-285; 10, с.510-518; 30;51;41].

3.3.3. Кадрово–технологічний потенціал

Найперспективнішим напрямком є елітна система підготовки оперативників («каців»). Моссад застосовує багаторівневий відбір, ізольовані табори, акцент на психологію, конспірацію та роботу під глибоким прикриттям. В Україні підготовка кадрів СБУ та ГУР все ще значною мірою базується на радянській моделі. Адаптація ізраїльського досвіду передбачає:

- Створення спеціалізованого навчально–тренувального центру (аналог «Моссадівської академії») з залученням ізраїльських інструкторів.

- Інтеграцію з приватним сектором (ізраїльська модель «Unit 8200» → українські ІТ-компанії та стартапи у сфері кібер-, дронів і ШІ).
- Програми обміну та спільних навчань з Моссадом (Ізраїль уже є важливим партнером України в оборонній сфері) [9, с.60-68; 23; 14, с.62-70; 29, с. 55-65].

3.3.4. Загальна оцінка потенціалу

Потенціал адаптації є високим і взаємовигідним. Україна вже демонструє унікальний досвід масової асиметричної війни (морські дрони, ешелонована ППО проти Shahed, кібероперації), який доповнює моссадівські методи. Ізраїль, своєю чергою, може отримати від України практичні напрацювання в протидії масованим дронівим атакам. Таким чином, адаптація – це не одностороннє запозичення, а двосторонній обмін досвідом, що відповідає стратегічному партнерству двох держав.

Разом з тим, адаптація має бути селективною та поетапною: починати з пілотних проєктів (спільні навчальні програми, створення координаційного центру, законодавчі зміни щодо спецоперацій), а потім масштабувати успішні практики. Це дозволить уникнути механічного копіювання та максимально врахувати національні особливості.

3.4. Конкретні рекомендації щодо організаційних, оперативних та законодавчих змін

На підставі комплексного порівняльного аналізу, проведеного в підрозділах 3.1–3.3, досвід Моссаду демонструє високий потенціал адаптації до українських реалій тривалої гібридної та конвенційної агресії РФ. Українські спецслужби (СБУ та ГУР МО України) вже реалізують окремі «моссадівські» елементи на практиці, проте системність, оперативна автономія та інтеграція технологій ще недостатні. Нижче сформульовано конкретні, реалістичні та поетапні рекомендації щодо організаційних, оперативних та законодавчих змін. Вони враховують чинну законодавчу базу станом на 2026 рік (Закон України «Про Службу безпеки України» № 2229–ХІІ у редакції з правками № 4156–ІХ,

№ 4344–IX, № 4542–IX, № 4633–IX та Закон України «Про розвідку» зі змінами № 4684–IX), плани ухвалення нового Закону «Про СБУ» у I кварталі 2026 року, а також вимоги європейської інтеграції та демократичного контролю [9;10;38;39;30;51].

Рекомендації поділено на три блоки, кожен з яких супроводжується обґрунтуванням, очікуваним ефектом та механізмом реалізації.

3.4.1. Організаційні рекомендації

1. Реформування та посилення існуючого механізму координації розвідувальної діяльності

Відповідно до статті 4 Закону України «Про розвідку», Президент України має право утворювати координаційний орган з питань розвідки як постійно діючий допоміжний орган для забезпечення взаємодії суб'єктів розвідувального співтовариства. Фактично такий механізм реалізовано у формі Координаційного комітету з питань розвідки при Президентові України, який функціонує з 2022 року.

Попри наявність законодавчо передбаченого механізму, практика воєнного періоду виявила його недостатню ефективність. Зокрема, спостерігається фрагментарність координації між СБУ, ГУР МО, СЗР та іншими суб'єктами, відсутність єдиного центру відповідальності за стратегічне планування розвідувальної діяльності та недостатня оперативність ухвалення рішень.

У зв'язку з цим пропонується реформувати та посилити Координаційний комітет з питань розвідки шляхом:

надання йому статусу постійно діючого органу з чітко визначеними повноваженнями, штатом та ресурсним забезпеченням;

запровадження посади Національного координатора розвідки, який би мав реальні повноваження щодо координації діяльності всіх суб'єктів розвідувального співтовариства та пряме підпорядкування Президенту України (за аналогією з моделлю «ХаМемуне» в Ізраїлі);

законодавчого закріплення механізму обов'язкового виконання рішень Координаційного комітету всіма суб'єктами розвідувального співтовариства.

Такий підхід дозволить уникнути створення нового бюрократичного органу та одночасно суттєво підвищити ефективність координації розвідувальної діяльності в умовах воєнного стану.

Реалізація: внесення змін до Закону України «Про розвідку» (ст. 4) та Положення про Координаційний комітет з питань розвідки. Термін – II квартал 2026 р.

1. Формування елітного підрозділу спеціальних операцій за кордоном («український Кідон») на базі існуючих підрозділів ГУР МО (10-й окремий загін спеціального призначення, «Kraken», «Firebird» тощо). Підрозділ повинен мати максимальну оперативну автономію, прямий доступ до вищого керівництва та інтеграцію з кібер– та агентурними підрозділами. Очікуваний ефект: підвищення якості точкових превентивних операцій проти ключових фігур ворожої логістики та командування.
2. Оптимізація структури СБУ з виокремленням «чистої» розвідувально–контррозвідувальної компоненти. З урахуванням реформ 2025 року (збільшення чисельності, розширення повноважень за Законом № 4633–IX) рекомендується поступово передавати слідчі функції іншим органам, залишивши за СБУ фокус на контррозвідці, кібербезпеці та захисті держтаємниці – відповідно до планів нового Закону «Про СБУ» (I квартал 2026 р.) [3;4;14;38;39].

3.4.2. Оперативні рекомендації

1. Запровадження системної практики довгострокового проникнення в логістичні та технологічні ланцюги противника (за прикладом операції з пейджерами «Хезболли»). Створити спеціальні оперативно–технічні групи (Tzomet + Keshet модель) для роботи з російською електронікою,

чіпами, АСУ ТП та постачанням дронів/ракет. Використовувати досвід ГУР у морських дронах як базу.

2. Розвиток комплексних багатодомених операцій (кібер + агентура + дрони + спецпідрозділи). Інтегрувати українські напрацювання в ешелонованій ППО та морських безпілотниках з моссадівськими методами (Stuxnet–подібні кіберзасоби, «троянські» акції). Рекомендується створення спільних українсько–ізраїльських робочих груп для обміну технологіями.
3. Посилення елітної підготовки оперативників («каців»). Створити спеціалізований навчально–тренувальний центр за ізраїльським зразком з акцентом на психологію, конспірацію, глибоке прикриття та роботу в умовах високого ризику. Запровадити обов’язкові програми обміну з Моссадом та іншими партнерами [9;10;25;41].

3.4.3. Законодавчі рекомендації

Чинна законодавча база (станом на травень 2026 року) вже містить значний прогрес, проте залишається надто деталізованою та бюрократичною порівняно з гнучкою моделлю Моссаду. Закон «Про Службу безпеки України» № 2229–ХІІ (редакція з правками № 4542–ІХ від 16.07.2025 та № 4633–ІХ від 09.10.2025) розширив повноваження СБУ (право самостійно розробляти та вносити проекти НПА – нова частина ст. 25), збільшив чисельність та соціальні гарантії.

Закон «Про розвідку» (зі змінами № 4684–ІХ від 05.11.2025) уточнив питання військової служби розвідників. Водночас залишаються ключові прогалини: обмежена оперативна свобода за кордоном, відсутність чіткого правового регулювання превентивних спеціальних операцій, надмірний контроль і бюрократія.

Конкретні законодавчі пропозиції:

1. Зміни до Закону «Про Службу безпеки України» (підготовка нового Закону у I кварталі 2026 р. – ідеальна платформа):

- Доповнити ст. 5 та ст. 25 нормами про максимальну оперативну автономію спеціальних підрозділів у проведенні операцій за кордоном у воєнний час (аналогічно директивному регулюванню Моссаду).
 - Закріпити можливість створення елітних підрозділів спеціального призначення з прямим підпорядкуванням керівнику СБУ/Президенту (нова стаття або розділ).
 - Зменшити обсяг слідчих повноважень СБУ, передавши їх Національній поліції або новому органу (відповідно до рекомендацій ЄС/НАТО).
2. Зміни до Закону «Про розвідку» та Закону «Про національну безпеку України»:
- Ввести інститут Національного розвідувального координатора (нова стаття в Законі «Про розвідку»).
 - Розширити ст. 7–9 Закону «Про розвідку» нормами про довгострокове проникнення в ланцюги постачання противника та використання shell-компаній/прикриття (з чіткими гарантіями захисту інформації).
 - У Законі «Про національну безпеку» (ст. 4) закріпити механізм координації через РНБО з наданням пріоритету превентивним операціям.
3. Додаткові точкові зміни:
- Внести правки до Закону «Про електронні комунікації» та Закону «Про державні закупівлі» для спрощення інтеграції приватного сектору (ІТ-компанії, оборонні стартапи) у розвідувальну діяльність (за ізраїльською моделлю «Unit 8200»).
 - Закріпити правовий статус превентивних спеціальних операцій у воєнний час як елемента самооборони (з посиланням на ст. 51 Статуту ООН).

Запропоновані зміни повністю відповідають європейським стандартам (фокус на контррозвідці та кібербезпеці), не порушують демократичний контроль і можуть бути ухвалені у пакеті з новим Законом «Про СБУ» у 2026 році [3;4;8;23;38;39;47].

Реалізація цих рекомендацій дозволить українським спецслужбам перейти на якісно новий рівень ефективності, наблизившись до еталонної моделі Моссаду, зберігаючи при цьому національні особливості та демократичні засади.

Отримані рекомендації підводять до аналізу ризиків і обмежень адаптації (підрозділ 3.5), що є необхідною умовою їх успішного впровадження.

3.5. Обмеження, ризики та перешкоди адаптації ізраїльського досвіду в Україні

Адаптація досвіду Моссаду до українських реалій, незважаючи на високий потенціал (підрозділ 3.3) та конкретні рекомендації (підрозділ 3.4), стикається з низкою об'єктивних обмежень, ризиків і перешкод. Вони зумовлені принциповою різницею між ізраїльською моделлю (максимальна оперативна автономія, мінімальне законодавче регулювання, прямий підпорядкування Прем'єр-міністру) та українською системою (демократичний контроль, європейські стандарти, пострадянська спадщина, вимоги ЄС/НАТО та особливості воєнного стану). Як показав порівняльний аналіз в підрозділах 3.1–3.2, пряме копіювання ізраїльських практик неможливе без урахування політичних, правових, культурних, соціальних та економічних особливостей України. Нижче наведено системний аналіз цих перешкод з урахуванням чинної законодавчої бази (станом на 2026 рік) та реалій тривалої гібридної агресії РФ.

3.5.1. Політичні та інституційні перешкоди

Найсерйознішою перешкодою є різниця в політичній системі та рівні стабільності. В Ізраїлі пряме підпорядкування Моссаду Прем'єр-міністру працює завдяки відносній стабільності коаліційного уряду та високому рівню довіри суспільства до розвідки. В Україні президентська вертикаль (ст. 5 Закону «Про СБУ») створює ризики політизації спецслужб під час зміни влади. Історичний досвід 2014–2026 років показує, що зміни керівництва СБУ часто супроводжувалися кадровими чистками та переорієнтацією пріоритетів.

Реформування Координаційного комітету з питань розвідки та надання йому статусу постійно діючого органу з реальними повноваженнями може

спричинити опір з боку окремих суб'єктів розвідувального співтовариства та ризику концентрації повноважень. Крім того, сильний вплив парламентського контролю та міжнародних партнерів робить неможливим повне копіювання ізраїльської моделі максимальної оперативної автономії.

3.5.2. Правові та законодавчі обмеження

Українське законодавство принципово відрізняється від ізраїльського. Як зазначалося в підрозділі 3.2.2, Моссад діє на підставі директив Прем'єра, тоді як СБУ та ГУР – у жорстких рамках Законів «Про Службу безпеки України» № 2229–ХІІ (редакція 2025 р. з правками № 4542–ІХ, № 4633–ІХ) та «Про розвідку» (№ 4684–ІХ) [3;4;38;47].

Ключові правові обмеження:

- Обмеження на превентивні спеціальні операції за кордоном. Точкові ліквідації та «Кідон»-подібні акції в Україні вимагають чіткого обґрунтування відповідно до міжнародного права (Європейська конвенція з прав людини, Женевські конвенції). Пряме запозичення може призвести до міжнародних скандалів і санкцій.
- Демократичний і парламентський контроль. Будь-яке розширення оперативної автономії (рекомендація 3.4.3) має бути збалансоване посиленням нагляду РНБО, ВРУ та Уповноваженого ВРУ з прав людини.
- Слідчі повноваження СБУ. Їхнє збереження (на відміну від «чистої» розвідки Моссаду) гальмує оперативну гнучкість.
- Проблема «троянських» операцій (shell-компанії, довгострокове проникнення). Чинне законодавство про державні закупівлі та захист інформації значно ускладнює таку діяльність порівняно з ізраїльською практикою.

3.5.3. Культурні, соціальні та кадрові ризики

Ізраїльська модель базується на високій мотивації, елітарності та суспільній підтримці (принцип «Never Again» після Голокосту). В Україні:

- Кадровий фактор. Радянська спадщина, корупційні ризики та нижчий рівень мотивації порівняно з ізраїльськими «кацами». Елітна підготовка потребує кардинальної зміни системи відбору та навчання.
- Суспільна толерантність. Українське суспільство чутливе до питань прав людини, цивільних жертв і «державного тероризму». Масштабні операції на кшталт «Гніву Божого» можуть викликати внутрішні протести та міжнародну критику.
- Культурна несумісність. Ізраїльська розвідка працює в умовах тотальної мобілізації суспільства. В Україні триває звичайне життя в тилу, що ускладнює тотальну секретність і підтримку операцій [9;23;29;38;31].

3.5.4. Економічні та ресурсні обмеження

Моссад функціонує за відносно невеликих ресурсів завдяки елітності та інтеграції з приватним сектором. Україна витрачає значні кошти на СБУ (понад 41 тис. осіб у 2025 р.), проте:

- Брак фінансування на елітну підготовку, сучасні технології та довгострокові операції.
- Залежність від західної допомоги, яка часто супроводжується умовами прозорості та контролю.
- Обмежені можливості інтеграції з приватним сектором через жорстке законодавство про держзакупівлі [9;23;25;38;39;31].

3.5.5. Геополітичні та міжнародно–правові ризики

Адаптація моссадівських методів (особливо превентивних ударів) може:

- Ускладнити відносини з ЄС та НАТО (вимоги щодо верховенства права).
- Спровокувати ескалацію з РФ та її союзниками (Іран, КНДР).
- Створити репутаційні ризики для України як демократичної держави.

Обмеження та ризики адаптації досвіду Моссаду є суттєвими, але не критичними. Вони зумовлені об'єктивними національними особливостями України і можуть бути мінімізовані за умови селективного, поетапного та

збалансованого підходу. Головне – не копіювати ізраїльську модель механічно, а творчо адаптувати її сильні сторони (оперативна автономія, довгострокове планування, елітність) до українських реалій, зберігаючи демократичний контроль, верховенство права та європейський вектор розвитку. Саме такий підхід, поєднаний із унікальним українським досвідом асиметричної війни (морські дрони, ешелонована ППО), дозволить створити ефективну гібридну модель національної безпеки, яка перевершить як ізраїльський, так і поточний український варіант [9;10;23;39, с.60-68;31].

Аналіз ризиків підкреслює необхідність пілотних проектів (спільні навчальні програми, створення НКЦР, точкові законодавчі зміни) перед масштабним впровадженням. Це дасть змогу перевірити ефективність рекомендацій 3.4 на практиці та своєчасно скоригувати підходи.

ВИСНОВКИ

У сучасних умовах тривалої гібридної та конвенційної агресії Російської Федерації проти України, яка триває з моменту проголошення незалежності в 1991 році і вже перевищила 35 років системного протистояння, питання підвищення ефективності національної безпеки набуває стратегічного, екзистенційного характеру. Проведене дослідження повністю досягло поставленої мети – комплексного аналізу досвіду діяльності ізраїльської розвідки «Моссад» та визначення перспектив його адаптації в організації та діяльності українських спецслужб (СБУ та ГУР МО України) для посилення обороноздатності держави в умовах асиметричних загроз.

Виконання шести визначених завдань дозволило отримати системні результати, які підтверджують наукову новизну та практичну цінність роботи. По–перше, у розділі 1 детально розкрито основні етапи становлення, розвитку та трансформації Моссаду з 1949–1951 рр. до 2026 року. Показано, що ключовими факторами успіху стали: пряме підпорядкування прем'єр–міністру, максимальна оперативна автономія, принцип «випереджального удару» (preventive strike), елітна система підготовки оперативників («каців») та глибока інтеграція сучасних технологій (кібер–, дроніві та інформаційні операції). Особливий акцент зроблено на трансформації після 1960–х років (період класичних спецоперацій) та пост–2020–х (гібридні та технологічні операції, зокрема операція з пейджерями «Хезболли» 2024 року) [9;10;23;14;25].

По–друге, проаналізовано сучасну організаційну структуру Моссаду, функціональну спрямованість ключових підрозділів (зокрема, оперативного, аналітичного, технологічного та спеціальних операцій типу «Кідон») та механізми взаємодії з іншими ізраїльськими спецслужбами – Шабаком (внутрішня безпека) та АМАНом (військова розвідка). Встановлено, що ефективність Моссаду зумовлена мінімальною бюрократією, єдиним координаційним центром («ХаМемуне») та прямим доступом до вищого політичного керівництва.

По–третє, у розділі 2 досліджено методи та засоби оперативної діяльності Моссаду, а також проаналізовано найвідоміші операції («Езра і Нехемія», «Фінал»/викрадення Ейхмана, Stuxnet–подібні кібероперації, саботаж іранської ядерної програми, ліквідації ключових фігур). Виявлено сильні сторони: креативність, швидкість, точковість, поєднання агентурної роботи з високотехнологічними інструментами та принцип «Never Again». Водночас відзначено слабкі сторони – окремі провали агентурних мереж у 1950–х, ризики міжнародних скандалів та етичні дилеми превентивних акцій [9;10;41].

По–четверте, здійснено порівняльний аналіз організаційно–правових засад, структури, методів роботи та законодавчого регулювання спецслужб Ізраїлю та України. З’ясовано, що ізраїльська модель забезпечує максимальну оперативну свободу за рахунок директивного регулювання, тоді як українська – характеризується детальним законодавчим контролем (Закон «Про Службу безпеки України» № 2229–ХІІ у редакціях 2025 року, Закон «Про розвідку» зі змінами № 4684–ІХ, Закон «Про національну безпеку України»), що відповідає європейським демократичним стандартам, але створює певні бюрократичні обмеження.

По–п’яте, визначено високий потенціал адаптації досвіду Моссаду на трьох рівнях: стратегічному (реформування та посилення Координаційного комітету з питань розвідки), оперативному (довгострокове проникнення в ланцюги постачання противника, комплексні багатодоменні операції) та кадрово–технологічному (еліта підготовка оперативників з інтеграцією приватного сектору). Українські спецслужби вже демонструють «моссадівські» риси – зухвалі операції ГУР на території РФ, кібердиверсії, ефективну роботу з агентурою, – що підтверджує можливість селективної адаптації.

По–шосте, виявлено обмеження, ризики та перешкоди адаптації: політичну нестабільність і ризики політизації, правові обмеження (міжнародне право, Європейська конвенція з прав людини), культурно–соціальні особливості (пострадянська спадщина, чутливість суспільства до прав людини), економічні та ресурсні проблеми, а також геополітичні ризики ескалації з РФ та її

союзниками. Водночас доведено, що ці ризики не є критичними за умови поетапного, селективного та збалансованого підходу [38;39;30;31].

Таким чином, підтверджуються всі три положення, що виносяться на захист:

Моссад є еталоном ефективної розвідки завдяки прямому підпорядкуванню прем'єр-міністру, елітній підготовці кадрів та інтеграції новітніх технологій, що дозволяє державі, оточеній ворогами, забезпечувати стратегічну перевагу за відносно невеликих ресурсів.

Українські спецслужби (СБУ та ГУР МО) вже демонструють окремі мозаїчні риси (креативність, проактивність, технологічність), проте потребують системних реформ для підвищення ефективності в умовах багаторічної гібридної агресії, що триває з 1991 року.

Адаптація досвіду Моссаду можлива та доцільна за умови врахування національних особливостей України, демократичних стандартів і ризиків, що передбачає не механічне копіювання, а творче поєднання ізраїльських практик з українським досвідом асиметричної війни (морські дрони, ешелонована ППО, масові кібероперації).

Практичне значення дослідження полягає в розробці конкретних рекомендацій, які можуть бути використані при реформуванні законодавства (зокрема, нового Закону «Про Службу безпеки України», запланованого на I квартал 2026 р.), оптимізації структури спецслужб та удосконаленні підготовки кадрів. Серед ключових організаційних рекомендацій – створення Національного координаційного центру розвідки при РНБО/Президентові (аналог «Хамемуне»), формування елітного підрозділу спеціальних операцій за кордоном («український Кідон») на базі ГУР та оптимізація структури СБУ з фокусом на контррозвідці та кібербезпеці. Оперативні рекомендації передбачають запровадження системного довгострокового проникнення в логістичні ланцюги противника, розвиток комплексних багатодомених операцій та створення спеціалізованого навчально-тренувального центру. Законодавчі зміни повинні включати розширення оперативної автономії

спеціальних підрозділів у воєнний час, закріплення інституту Національного розвідувального координатора та спрощення інтеграції приватного сектору (ІТ-компанії, оборонні стартапи).

Отримані результати мають високе значення для науки (перше комплексне магістерське дослідження адаптації досвіду Моссаду саме в контексті 35-річної гібридної агресії РФ) та практики (рекомендації можуть бути впроваджені у діяльності СБУ, ГУР, РНБО та використані для посилення українсько-ізраїльського оборонного партнерства). Дослідження доводить, що Україна, поєднуючи моссадівську модель оперативної гнучкості, проактивності та технологічності з власним унікальним досвідом масової асиметричної війни, здатна сформувати одну з найефективніших систем національної безпеки в умовах сучасних гібридних загроз [3;4;8;23;47;31].

Разом з тим, адаптація вимагає виваженого підходу: пілотних проєктів, спільних навчальних програм з Моссадом, точкових законодавчих змін та постійного моніторингу ризиків. Лише за таких умов українські спецслужби зможуть перейти від реактивної до проактивної стратегії, забезпечуючи не лише виживання, а й стратегічну перевагу в довгостроковій боротьбі за суверенітет, територіальну цілісність та європейське майбутнє України.

Перспективи подальших досліджень пов'язані з емпіричним вивченням ефективності запропонованих рекомендацій після їх впровадження, а також порівняльним аналізом досвіду інших провідних розвідок (наприклад, МІБ, СІА, Mossad у поєднанні з українським досвідом) у контексті гібридних війн ХХІ століття.

Таким чином, проведене дослідження не лише розкрило потенціал ізраїльського досвіду, а й запропонувало реальний шлях посилення національної безпеки України в умовах перманентної загрози. Реалізація рекомендацій стане важливим кроком до створення сучасної, ефективною та демократично контрольованою системи спецслужб, здатної протистояти будь-яким гібридним і конвенційним викликам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативно–правові акти України

1. Конституція України : Закон України від 28 червня 1996 р. № 254/96–ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
2. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469–VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.
3. Про Службу безпеки України : Закон України від 25 березня 1992 р. № 2229–XII. Відомості Верховної Ради України. 1992. № 27. Ст. 382. (у редакції з правками № 4542–IX від 16.07.2025 та № 4633–IX від 09.10.2025).
4. Про розвідку : Закон України від 17 вересня 2020 р. № 912–IX. Відомості Верховної Ради України. 2020. № 42. Ст. 339. (зі змінами № 4684–IX від 05.11.2025).
5. Про Раду національної безпеки і оборони України : Закон України від 5 березня 1998 р. № 183/98–ВР (з подальшими змінами).
6. Про Стратегію національної безпеки України : Указ Президента України від 14 вересня 2020 р. № 392/2020.
7. Про Стратегію воєнної безпеки України : Указ Президента України від 25 березня 2021 р. № 121/2021.

Література

8. Alberts D. S., Garstka J. J., Stein F. P. Network–Centric Warfare: Developing and Leveraging Information Superiority. 2nd ed. Washington : CCRP, 2000. 287 p.
9. Bar–Zohar M., Mishal N. Mossad: The Greatest Missions of the Israeli Secret Service. New York : Ecco Press, 2012. 388 p.
10. Bergman R. Rise and Kill First: The Secret History of Israel’s Targeted Assassinations. New York : Random House, 2018. 784 p.
11. Bergman R. The Secret History of Israel’s Targeted Assassinations // The New York Times Magazine. 2018. Jan. 31.

12. Burch J. A Domestic Intelligence Agency for the United States? A Comparative Analysis... // Homeland Security Affairs. 2007. Vol. 3, No. 2.
13. Giannopoulos G., Smith H., Theocharidou M. The Landscape of Hybrid Threats: A conceptual model. Luxembourg : Publications Office of the European Union, 2021. 85 p.
14. Harel I. The House on Garibaldi Street. New York : Viking Press, 1975. 296 p.
15. Kim Zetter. Stuxnet: The world's first cyber weapon // Wired. 2014.
16. Nimmo B. Secondary "Infektion" / Graphika. 2020. 120 p.
17. Radin A. Hybrid Warfare in the Baltics. Santa Monica : RAND Corporation, 2017. 58 p.
18. Raviv D., Melman Y. Every Spy a Prince: The Complete History of Israel's Intelligence Community. Boston : Houghton Mifflin, 1990. 512 p.
19. Shapiro A. J. A New Era for U.S. Security Assistance // The Washington Quarterly. 2012. Fall. P. 23–35.
20. Scheuer M. Through Our Enemy's Eyes: Osama bin Laden, Radical Islam and the Future of America. Rev. ed. Washington : Potomac Books, 2006. 443 p.
21. Stuxnet and the Future of Cyber Warfare // Bulletin of the Atomic Scientists. 2011. Vol. 67, No. 1. P. 34–42.
22. Sweijts T., Zilincik S. Cross Domain Deterrence and Hybrid Conflict. The Hague : Hague Centre for Strategic Studies, 2019. 38 p.
23. Thomas G. Gideon's Spies: The Secret History of the Mossad. 7th ed. New York : St. Martin's Griffin, 2015. 736 p.
24. Vitkauskas D. The Role of A Security Intelligence Service In A Democracy. NATO Democratic Institutions Fellowships Programme, 1999. 57 p.
25. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York : Crown, 2014. 448 p.
26. Бар–Зохар М., Мішаль Н. Моссад. Найвидатніші операції ізраїльської розвідки / пер. з англ. Київ : Книжковий клуб «Клуб сімейного дозвілля», 2015. 416 с.

27. Бергман Р. Піднятися і вбити першим: таємна історія цілеспрямованих вбивств Ізраїлю / пер. з англ. Київ : Yakaboo Publishing, 2020. 752 р.
28. Бжезинський З. Україна та Європа. Національна безпека і оборона // Національна безпека і оборона. 2022. № 7. С. 12–18.
29. Гарель І. Будинок на вулиці Гарібальді / пер. з івриту. Київ : Дух і літера, 2019. 312 с.
30. Головне управління розвідки Міністерства оборони України. Річний звіт ГУР МО України за 2024 рік. Київ : ГУР МО, 2025. 112 с.
31. Горбулін В. Гібридна війна: як Росія воює проти України з 1991 року // Українська правда. 2022. 24 лют.
32. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с.
33. Зеттер К. Зворотний відлік до нульового дня: Stuxnet та запуск першої цифрової зброї світу / пер. з англ. Київ : Наш формат, 2016. 432 с.
34. Ліпкан В. А. Національна безпека України : навч. посіб. 2–ге вид. Київ : КНТ, 2009. 574 с.
35. Лісовський П. М., Лісовська Ю. П. Український Моссад: книга життя у законах війни : навч. посіб. Київ : Ліра-К, 2022. 248 с.
36. Матеріали комісії Україна–НАТО у сфері стандартизації та гібридних загроз (2023–2025 рр.). Офіційний сайт НАТО. URL : <https://www.nato.int> (дата звернення: 20.05.2026).
37. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз : національна доповідь / ред. кол. С. І. Пирожков та ін. Київ : Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 2022. 552 с.
38. Національний інститут стратегічних досліджень. Гібридна агресія Російської Федерації проти України: виклики та відповіді : аналіт. доп. Київ : НІСД, 2023. 124 с.

39. Національний інститут стратегічних досліджень. Реформування сектору безпеки і оборони України в умовах воєнного стану : аналіт. доп. Київ : НІСД, 2024. 98 с.
40. Операція «Езра і Нехемія» (1950–1951 рр.): евакуація іракських євреїв // Офіційний сайт Моссаду (архівні матеріали). URL : <https://www.mossad.gov.il> (дата звернення: 15.05.2026).
41. Операція з пейджерів проти «Хезболли» (вересень 2024 р.): аналіз наслідків для гібридної війни // Foreign Affairs. 2024. Oct.
42. Публікації Національного інституту стратегічних досліджень щодо реформування СБУ та ГУР у 2024–2025 рр.
43. Романов М. С., Стрельбицький М. П., Стрельбицька Л. М. Соціально–правові основи управління національною безпекою України : навч. посіб. Острогоз : Видавництво НаУОА, 2021. 136 с.
44. Руснак І. С. Оборонна реформа в Україні: основні підсумки та перспективи // Наука і оборона. 2021. № 1. С. 4–12.
45. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.
46. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно–правові засади) : підруч. Київ : НАДУ, 2012. 544 с.
47. Служба безпеки України. Звіт про діяльність СБУ за 2024 рік. Київ : СБУ, 2025. 156 с.
48. Томас Г. Шпигуни Гедеона: таємна історія Моссаду / пер. з англ. Харків : Фоліо, 2018. 688 с.
49. Уривалкін О. Таємниці розвідок (діяльність таємних служб на території України). К. : КНТ, 2007. 352 с.
50. Центр воєнно–стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. Оборонне планування на основі спроможностей в умовах гібридної війни : зб. наук. пр. Київ : НУОУ, 2020. 215 с.

51. «Українська правда». ГУР МО України: нові методи асиметричної боротьби проти РФ // Українська правда. 2025. 12 берез.
52. «Українська правда». Операція «Пейджери»: як Ізраїль завдав удару по «Хезболлі» у 2024 році // Українська правда. 2024. 18 верес.

ДОДАТКИ

Таблиця 1.1. Основні етапи становлення, розвитку та трансформації Моссаду (1949–2026 рр.)

Етап	Період	Керівник	Стратегічні пріоритети	Найвідоміші операції та досягнення	Ключові трансформації та уроки для України
1. Становлення	1949–1952 рр.	Реувен Шілоах	Координація розвідки, масова імміграція	Операція «Езра і Нехемія» (125 тис. осіб)	Закладено принцип прямого підпорядкування Прем'єр-міністру
2. Професіоналізація	1952–1963 рр.	Ісер Гарель («Хамемуне»)	Елітна підготовка, глобальна мережа	Операція «Фінал» (викрадення Ейхмана)	Створення системи «каців» та професійної структури
3. Класичні спецоперації	1963–1970-ті рр.	Меїр Амит, Цві Замир	Точкові ліквідації та контртероризм	Операція «Гнів Божий»	Максимальна оперативна свобода
4. Технологічна трансформація	1980-ті – 2026 рр.	Сучасні директори	Кібер-, дронів та гібридні операції	Операція з пейджерів «Хезболли» (2024)	Інтеграція ІІІ, кібер та приватного сектору

Таблиця 1.2. Основні структурні підрозділи Моссаду та механізми їхньої взаємодії з іншими ізраїльськими спецслужбами.

Підрозділ	Основна спрямованість	Ключові напрями	Взаємодія з іншими службами	Значення для сучасної гібридної війни
Keshet	Оперативна розвідка (HUMINT)	Агентурна робота, резидентури	Координація з АМАН	База для довгострокового проникнення
Tzomet	Технічна та кіберрозвідка	«Троянські» системи, Stuxnet-типу	Спільні операції з Unit 8200	Ключовий елемент гібридних операцій
Kidon	Спеціальні операції	Точкові ліквідації, саботаж	Підтримка Шабаку	Еталон превентивних дій за кордоном
Аналіз та планування	Стратегічний аналіз	Доповіді для Прем'єр-міністра	Центральний вузол («Хамемуне»)	Забезпечення випереджального характеру

Технологічний	Інновації та технології	Дрони, ШІ, кіберзасоби	Співпраця з приватним сектором	Перевага в технологічній війні
---------------	-------------------------	------------------------	--------------------------------	--------------------------------

Таблиця 1.3. Порівняльна характеристика організаційно-правових моделей спецслужб Ізраїлю та України

Критерій порівняння	Ізраїль (Моссад)	Україна (СБУ / ГУР)	Можливості адаптації
Підпорядкування	Пряме підпорядкування Прем'єр-міністру. Діяльність регулюється директивами	Підпорядкування Президенту та Міністру оборони. Детальне законодавче регулювання	Часткова адаптація. Можливе посилення прямого підпорядкування Президенту
Рівень оперативної автономії	Високий. Мінімальна бюрократія	Середній. Значна бюрократія	Потребує посилення. Створення НКЦР допоможе
Координаційний механізм	Посада «ХаМемуне» (єдиний координатор)	РНБО (не завжди ефективно)	Висока. Створення Національного координаційного центру розвідки доцільне
Поєднання розвідки та слідства	Функції чітко розділені	СБУ поєднує обидві функції	Середня. Рекомендується виокремлення слідчих функцій
Система підготовки кадрів	Елітна система, жорсткий відбір, тривала підготовка	Пострадянська модель + реформи 2025	Висока. Створення спеціалізованого центру за ізраїльським зразком
Інтеграція з приватним сектором	Висока (модель Unit 8200)	Обмежена через держзакупівлі	Потребує законодавчих змін
Демократичний контроль	Переважно внутрішній	Парламентський + судовий + міжнародний	Зберегти українську модель + додати більше автономії
Можливість превентивних операцій	Висока	Обмежена	Середня. Потрібне чітке регулювання у воєнний стан
Технологічна інтеграція	Дуже високий рівень	Високий, але не системний	Висока. Можна запозичити досвід інтеграції
Загальна гнучкість моделі	Висока	Нижча через детальне законодавство	Адаптація можлива тільки селективно

Таблиця 1.4. Зведена таблиця рекомендацій щодо адаптації досвіду

Моссаду

Напрямок	Конкретна рекомендація	Очікуваний ефект	Механізм реалізації	Термін реалізації
Організаційний	Реформування та посилення Координаційного комітету з питань розвідки (з наданням статусу постійно діючого органу)	Єдине стратегічне планування, зменшення дублювання функцій та міжвідомчих конфліктів	Внесення змін до Закону «Про національну безпеку України» (ст. 4–6) та Положення про РНБО	II квартал 2026 р.
Організаційний	Формування елітного підрозділу спеціальних операцій за кордоном («український Кідон») на базі ГУР МО	Підвищення якості точкових превентивних операцій проти ключових фігур противника	Створення на базі 10-го ОЗСпН та інших підрозділів ГУР МО	2026–2027 рр.
Організаційний	Оптимізація структури СБУ з виокремленням слідчих функцій	Фокус СБУ на контррозвідці, кібербезпеці та захисті держтаємниці	Реалізація в новому Законі «Про Службу безпеки України»	I квартал 2026 р.
Оперативний	Запровадження системної практики довгострокового проникнення в логістичні та технологічні ланцюги противника	Підвищення ефективності роботи проти логістики та постачання РФ	Створення спеціальних оперативно–технічних груп за моделлю Tzomet + Keshet	2026–2027 рр.
Оперативний	Розвиток комплексних багатодомених операцій (кібер + агента + дрони + спецпідрозділи)	Зростання результативності гібридних операцій	Створення спільних українсько–ізраїльських робочих груп	Постійно
Кадровий	Створення спеціалізованого навчально–тренувального центру за ізраїльським зразком	Підвищення якості та елітності кадрового складу	Залучення ізраїльських інструкторів та інтеграція з приватним сектором	2026–2027 рр.
Законодавчий	Розширення оперативної автономії спеціальних підрозділів у воєнний час	Зменшення бюрократичних бар'єрів	Доповнення ст. 5 та ст. 25 Закону «Про Службу безпеки України»	I квартал 2026 р.
Законодавчий	Введення інституту Національного розвідувального координатора	Покращення координації між СБУ, ГУР та СЗР	Внесення нової статті до Закону «Про розвідку»	2026 р.
Законодавчий	Спрощення інтеграції приватного сектору (IT–компанії, оборонні стартапи)	Залучення сучасних технологій та фахівців	Зміни до Закону «Про державні закупівлі» та «Про електронні комунікації»	2026–2027 рр.

SWOT–аналіз адаптації досвіду Моссаду до українських реалій

Strengths (Сильні сторони)	Weaknesses (Слабкі сторони)	Opportunities (Можливості)	Threats (Загрози)
Висока оперативна ефективність і проактивність Моссаду, доведена багаторічною практикою	Принципова різниця в політичних системах (директивне регулювання vs детальне законодавство)	Реформування та посилення Координаційного комітету з питань розвідки (з наданням статусу постійно діючого органу)	Можлива ескалація конфлікту з РФ та її союзниками у відповідь на більш активні превентивні дії
Успішний досвід проведення складних гібридних операцій проти сильнішого противника	Обмеження, пов'язані з демократичними стандартами, європейською інтеграцією та міжнародним правом	Активна інтеграція з приватним сектором (ІТ–компанії, оборонні стартапи) за ізраїльською моделлю	Тиск з боку ЄС та НАТО щодо дотримання стандартів верховенства права та прав людини
Наявність унікального українського бойового досвіду асиметричної війни (морські дрони, протидія Shahed, кібероперації)	Брак фінансових і кадрових ресурсів для створення повноцінної елітної системи підготовки	Взаємовигідний обмін досвідом: Україна може передати Ізраїлю напрацювання у протидії масованим дронним атакам	Внутрішньополітична нестабільність та ризики політизації при реформуванні сектору безпеки
Існуюче стратегічне партнерство з Ізраїлем у оборонній сфері	Ризик політизації спецслужб при значному збільшенні оперативної автономії	Підвищення ефективності дій проти російської логістики та військової інфраструктури	Можливість швидкого відновлення противником втрачених спроможностей (кадри, технології, захист)
Високий рівень технологічної грамотності та інноваційності українських підрозділів	Надмірна бюрократія та міжвідомча конкуренція в українській системі	Зміцнення стратегічного партнерства з Ізраїлем та отримання доступу до передових технологій	Репутаційні та міжнародно–правові ризики у разі невдалих або резонансних операцій