**Карпатський національний університет
імені Василя Стефаника**

Факультет історії, політології і міжнародних відносин
Кафедра політичних наук

Іван МОНОЛАТІЙ

ШПИГУНСТВО ЯК ІНСТРУМЕНТ ДЕРЖАВНОЇ БЕЗПЕКИ

Навчально-методичний посібник для здобувачів освіти
першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Політологія. Національна безпека»,
спеціальність С2 Політологія, галузь знань С «Соціальні науки, журналістика, інформація та міжнародні відносини»

Івано-Франківськ
2025

УДК 327.88:351.86(075.8)

Навчально-методичний посібник «Шпигунство як інструмент державної безпеки» передбачає засвоєння теоретичного матеріалу та формування практичних навичок здобувачами освіти першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Політологія. Національна безпека», спеціальність С2 Політологія, галузь знань С «Соціальні науки, журналістика, інформація та міжнародні відносини» про шпигунство – передачу або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства. Дисципліна спрямована на формування у здобувачів освіти теоретичних знань щодо розуміння природи шпигунства як злочину проти держави, її національної безпеки. Дисципліна орієнтує на розкриття особливостей державної безпеки сучасності в інформаційній, а також політичній, економічній, воєнній і науково-технологічній сферах – через феномен шпигунства в сучасному світі у його історичних і політичних детермінантах.

Рецензенти:

Гулай В. В. – д-р політ. н., проф., завідувач кафедри міжнародної інформації Національного університету «Львівська Політехніка»;

Кобець Ю. В. – канд. політ. н., доцент кафедри політичних наук Карпатського національного університету ім. В. Стефаника;

Мосора М. А. – доктор філософії, асистент кафедри політичних наук Карпатського національного університету ім. В. Стефаника.

Рекомендувала до друку вчена рада
Факультету історії, політології і міжнародних відносин
Карпатського національного університету імені Василя Стефаника

Монолатій І. *Шпигунство як інструмент державної безпеки:* Навчально-методичний посібник для здобувачів освіти першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Політологія. Національна безпека», спеціальність С2 Політологія, галузь знань С «Соціальні науки, журналістика, інформація та міжнародні відносини». Івано-Франківськ: Карпатський національний університет імені Василя Стефаника, 2025. 62 с.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Навчально-методичний посібник розроблено відповідно до силабуса навчальної дисципліни «Шпигунство як інструмент державної безпеки» розроблено відповідно до освітньо-професійної програми підготовки фахівців на першому (бакалаврському) рівні вищої освіти ОПП «Політологія. Національна безпека», спеціальність С2 Політологія.

Курс складається з двох змістовних модулів. Предметом вивчення курсу є шпигунство – передача або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства. Дисципліна спрямована на формування у здобувачів освіти теоретичних знань щодо розуміння природи шпигунства як злочину проти держави, її національної безпеки. Дисципліна орієнтує на розкриття особливостей державної безпеки сучасності в інформаційній, а також політичній, економічній, воєнній і науково-технологічній сферах – через феномен шпигунства в сучасному світі у його історичних і політичних детермінантах.

Метою навчальної дисципліни «Шпигунство як інструмент державної безпеки» є виявлення суті феномену шпигунства, проблем його сутнісної характеристики й співвідношення світового досвіду боротьби з шпигунством в сучасній Україні.

Основними цілями вивчення дисципліни є: 1) опанування здобувачами освіти поняття шпигунства (виконавці, адресати шпигунства); 2) дослідження специфіки політико-правових оцінок шпигунства як інструменту державної безпеки, категоріального апарату, об’єкту, предмету, методів і вимірів шпигунства та його видів; 3) аналіз сучасних підходів щодо вивчення фактів і обставин: а) передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; б) збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; в) ініціативи збирання чи передачі відповідних відомостей як виконавців, так і адресатів шпигунства; 4) аналіз нормативно-правової бази України та зарубіжних країн щодо шпигунства, передачі і збиранні певних відомостей Передача іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; 5) вивчення засад функціонування спеціальних служб України та світу щодо протидії шпигунству.

Курс «Шпигунство як інструмент державної безпеки» є важливою складовою сучасної підготовки фахівців у галузі політичної науки та національної безпеки. Його зміст відповідає потребам нової політологічної парадигми, орієнтованої на аналіз влади, безпеки та інформаційного простору у взаємозв'язку. Сучасна політологія дедалі більше інтегрує поняття «безпека» у свої аналітичні моделі, розглядаючи шпигунство не лише як кримінальний злочин проти держави, а як форму політичної діяльності, спрямовану на зміну балансу сил у міжнародному середовищі. Саме тому розуміння шпигунства стає необхідним інструментом для пояснення механізмів глобального суперництва, інформаційних воєн і стратегічних комунікацій.

Вивчення курсу сприяє формуванню у студентів системного бачення проблем національної безпеки, заснованого на міждисциплінарному підході. Політологічна перспектива дозволяє розглядати шпигунство як соціально-політичне явище, що поєднує правові, етичні, технологічні та культурні виміри. Студенти навчаються аналізувати процеси розвідки та контррозвідки в контексті сучасної теорії держави, міжнародних відносин і політичного реалізму. Особливу увагу приділено аналізу інформаційних загроз, кібершпигунства, політичних маніпуляцій і стратегій дезінформації, які формують нові форми впливу в епоху постправди.

Курс забезпечує розвиток компетентностей, необхідних для аналітичного осмислення сучасних безпекових процесів: уміння виявляти, оцінювати та прогнозувати загрози, аналізувати політику іноземних держав у сфері розвідки, а також визначати потенційні наслідки для безпеки України. Формування таких навичок дозволяє студентам не лише опановувати інструментарій державного управління у сфері безпеки, а й критично мислити, застосовувати методи стратегічного аналізу та політичного прогнозування в реальних умовах геополітичної конкуренції.

Відтак курс інтегрує теоретичну та прикладну підготовку, необхідну для сучасного політолога-націоналіста, здатного діяти в умовах складного, багато-рівневого міжнародного середовища. Він розвиває розуміння шпигунства як чинника впливу на міжнародну політику та національну безпеку, формує вміння мислити категоріями ризику, стратегічних інтересів і політичного реалізму. Засвоєння курсу сприятиме формуванню нового покоління аналітиків, здатних поєднувати науковий підхід із практичними навичками розробки та реалізації державної політики безпеки, що відповідає викликам XXI століття.

ОСНОВНИЙ ЗМІСТ ЛЕКЦІЙНИХ ЗАНЯТЬ

Тема 1. Ґенеза та сутнісні характеристики шпигунства як інституту та процесу в сучасних політичних відносинах.

Лекція присвячена аналізу шпигунства як соціально-політичного інституту та складного процесу, що функціонує на перетині військової, політичної, економічної та психологічної сфер сучасних міжнародних відносин. Вона розкриває історичні витоки шпигунської діяльності, її еволюцію від класичних форм збору розвідувальної інформації до сучасних практик кібер- та економічного шпигунства. Особлива увага приділяється сутнісним характеристикам шпигунства, включно з його функціями (збір інформації, контррозвідка, маніпуляція й прогнозування політичних дій), структурою агентурної мережі, механізмами мотивації агентів та інтеграцією технологічних і психологічних методів у процес діяльності.

Лекція окреслює ключові поняття шпигунства в сучасному політичному контексті, серед яких розвідка, контррозвідка, мотиви та типи агентів, методи збору та обробки інформації, а також аксіологічні та етичні аспекти діяльності. Студенти ознайомляться з логікою профілювання шпигунів, від розпізнавання операційних патернів і психологічних характеристик до оцінки ризиків для безпеки держави та організації. Особливий акцент зроблено на аналізі взаємодії шпигунських практик із сучасними політичними процесами, інститутами влади та міжнародними відносинами, що дозволяє зрозуміти, як діяльність агентів впливає на прийняття рішень на національному та глобальному рівні.

Розглянуті в лекції концептуальні рамки та ключові поняття формують основу для подальшого вивчення конкретних типів шпигунства (воєнного, промислового, економічного, кібер-шпигунства), методів їх профілювання та контрзаходів, а також для розвитку аналітичних компетенцій студентів у сфері безпеки, політики та соціальної психології. Лекція поєднує історико-теоретичний аналіз із сучасними кейсами, демонструючи, як шпигунство виступає структурним елементом політичних відносин та інструментом впливу у міжнародній системі.

Ключові поняття: розвідка, контррозвідка, мотивація агентів, методи збору інформації, профілювання шпигунів, аксіологічні аспекти.

Тема 2. Явище шпигунства та проблема його сучасної характеристики в політичній науці

Лекція присвячена аналізу явища шпигунства як соціально-політичного феномену та проблеми його сучасного визначення у контексті політичної науки. Розглядається, як різні наукові підходи та концептуальні рамки визначають шпигунство, відображаючи його функції, структури та вплив на політичні процеси всередині держави та у міжнародній системі. Особлива увага приділяється труднощам у визначенні шпигунства: його багатоплановості, змішуванню формальної та неформальної діяльності, поєднанню легальних і нелегальних методів збору інформації, а також інтеграції технологічних, психологічних і соціальних компонентів.

Лекція розкриває ключові аспекти сучасного наукового підходу до шпигунства: його політичне та стратегічне значення, роль у міжнародних відносинах, типи і мотивації агентів, методи збору та поширення інформації, а також етичні та правові проблеми, що виникають у зв'язку з діяльністю розвідувальних органів. Висвітлюється, як політична наука аналізує шпигунство не лише як інструмент державної політики, а й як соціокультурне явище, що відображає конфлікти інтересів, довіру та рівень безпеки у суспільстві.

Студенти ознайомляться з концептуальними рамками, які дозволяють системно описувати шпигунство, оцінювати його роль у сучасних політичних процесах та аналізувати вплив на державну безпеку і міжнародні відносини. Особливий акцент робиться на проблемах класифікації шпигунства, сучасних методах його дослідження та способах інтеграції психологічних, технологічних і політичних даних у профілювання агентів. Лекція демонструє, як сучасні виклики, включно з кібернетичними загрозами та економічним шпигунством, змінюють традиційне розуміння шпигунства і потребують комплексного міждисциплінарного підходу в політичній науці.

Ключові поняття: шпигунство, політична наука, функції і роль агентів, методи збору інформації, етичні та правові аспекти, сучасні виклики кібер- та економічного шпигунства.

Тема 3. Історичний розвиток шпигунства. Шпигунство у XX – на початку XXI ст.

Лекція присвячена історичному аналізу шпигунства, його еволюції та трансформації від ранніх форм до сучасних моделей розвідувальної діяльності у XX – на початку XXI століття. Особлива увага приділяється історичному

контексту: ще до XX століття шпигунство виступало інструментом державної політики та безпеки, формувалося у військових конфліктах, дипломатичних інтригах та економічних суперництвах між державами. Приклади ранніх агентурних систем, використання кур'єрів, кодів та таємних документів у середньовіччі та епоху Нового часу ілюструють, як штучно організовані канали збору інформації закладали основи сучасної розвідки.

У першій половині XX століття шпигунство набуває більш формалізованого та професійного характеру. Під час Першої та Другої світових війн розвиваються класичні агентурні системи, посилюється роль контррозвідки та військової розвідки, виникають перші міжнародні мережі агентів, а також механізми координації на рівні державних структур. У період Холодної війни шпигунство стає глобальним феноменом, підсилюється значення ідеологічних мотивів, активно використовуються високотехнологічні методи збору інформації, розвиваються подвійні агенти, а розвідувальні структури інтегруються у політичні процеси. На рубежі XX – XXI століть відбувається трансформація шпигунства у відповідь на глобалізацію та розвиток цифрових технологій. Особлива увага приділяється економічному, бізнес- та кібер-шпигунству, поширенню інсайдерських загроз і використанню сучасних технологій для збору, обробки та передачі інформації. Лекція показує, як історичний досвід формував сучасні концепції шпигунства, включаючи військові, промислові та економічні витоки, а також роль державних і недержавних акторів.

Студенти ознайомляться з історико-аналітичними методами вивчення шпигунства, простежать закономірності розвитку агентурних систем у різні періоди та зрозуміють, як минулі практики вплинули на сучасні методи профілювання шпигунів і побудову контррозвідувальних стратегій.

Ключові поняття: історія шпигунства, агентурна мережа, методи розвідки, воєнне та промислове шпигунство, кібернетичні та економічні загрози, історичні етапи розвитку шпигунства, еволюція профілювання агентів, ранній досвід шпигунства.

Тема 4. Типи та функції шпигунства в сучасних державах за типами політичних режимів

Лекція присвячена детальному аналізу шпигунства як складного соціально-політичного явища та інституту, функції якого тісно пов'язані з політичним режимом держави, її історичним досвідом, технологічним розвитком та інтеграцією у глобальні системи безпеки. Вивчення типів шпигунства

проводиться крізь призму демократичних, авторитарних та тоталітарних режимів, а також із урахуванням сучасних гібридних і перехідних форм управління, які поєднують елементи обох підходів. Лекція показує, що специфіка політичного устрою визначає організацію агентурних мереж, методи збору інформації, завдання, пріоритети та рівень контролю над діяльністю шпигунів.

Історичний контекст дозволяє простежити еволюцію шпигунства від ранніх форм до сучасних моделей. Ще до XX століття шпигунство відігравало ключову роль у дипломатичних інтригах, економічних суперництвах та військових конфліктах. Використання кур'єрів, секретних кодів, агентурних мереж і таємних документів у середньовіччі, Новий час і період становлення національних держав формувало базові принципи сучасної розвідки. У першій половині XX століття шпигунство набуває більш професійного та організованого характеру: під час Першої та Другої світових воєн активно розвиваються військові та контррозвідувальні структури, формуються міжнародні агентурні мережі, зростає значення стратегічного аналізу та координації на державному рівні.

У період Холодної війни шпигунство стає глобальним феноменом. Особливу роль відіграють ідеологічні мотиви, високотехнологічні методи збору інформації, використання подвійних агентів і інтеграція розвідувальних структур у внутрішні та зовнішні політичні процеси. Демократичні держави прагнуть збалансувати ефективність шпигунства із законодавчим та етичним контролем, тоді як авторитарні й тоталітарні режими активно використовують шпигунство для контролю громадян, придушення опозиції, моніторингу політичної активності та забезпечення стабільності режиму. Гібридні та перехідні системи поєднують елементи обох підходів, створюючи складну мережу зовнішніх і внутрішніх завдань для агентурних структур.

Лекція також розглядає сучасні виклики, що виникають у зв'язку з глобалізацією та цифровізацією політичних процесів. Зокрема, поширення кібер- та економічного шпигунства, активне використання цифрових каналів комунікації, міжнародних фінансових та технологічних інтеграцій створюють нові можливості для збору інформації, одночасно підвищуючи рівень ризиків та складність контррозвідувальних заходів. Особливу увагу приділено методам профілювання агентів, структурним особливостям розвідувальних органів, їхнім адаптивним механізмам реагування на зміни політичного середовища, технологічні інновації у сфері збору та обробки даних, а також правовим і етичним обмеженням діяльності.

Студенти отримають системний огляд функцій шпигунства у різних режимах, включно із зовнішньою та внутрішньою розвідкою, контррозвідкою, аналізом і прогнозуванням політичних подій, економічним і промисловим шпигунством, кібернетичними операціями та інформаційним впливом. Висвітлюється взаємозв'язок між типом політичного режиму, технологічними можливостями та глобалізаційними викликами, що дозволяє зрозуміти, як різні держави формують агентурні системи, визначають пріоритети і балансують між безпековими, політичними та економічними цілями. Історико-аналітичний підхід у поєднанні з сучасними кейсами дозволяє студентам усвідомити закономірності розвитку шпигунства, оцінити його функції в умовах глобалізації та цифровізації, а також підготуватися до розробки власних аналітичних оцінок і профілів агентурної діяльності у сучасному світі.

Ключові поняття: типи політичних режимів (демократичний, авторитарний, тоталітарний), гібридні режими, функції шпигунства, агентурна мережа, контррозвідка, профілювання агентів, зовнішнє та внутрішнє шпигунство, глобалізаційні та цифрові виклики, історичний та сучасний досвід.

Тема 5. Державне та приватне шпигунство: світовий та український виміри

Лекція присвячена комплексному аналізу шпигунства у його двох ключових формах – державному та приватному, зокрема в умовах сучасної глобалізації та цифровізації політичних, економічних та соціальних процесів. Державне шпигунство традиційно розглядається як інструмент забезпечення національної безпеки, зовнішньої та внутрішньої розвідки, контррозвідки, а також впливу на міжнародну політику. Приватне шпигунство, включно з корпоративним, промисловим та кібернетичним, спрямоване на захист комерційних інтересів, економічної інформації та інтелектуальної власності.

Історично державне шпигунство формувалося у складі військових і дипломатичних структур ще до XX століття, розвивалося під час світових воєн, Холодної війни та формування глобальних міжнародних систем безпеки. Приватне шпигунство набуває масового характеру у XX столітті, паралельно з індустріалізацією, розвитком науки і технологій, глобальними ринками та міжнародними корпораціями. У XXI столітті обидва типи шпигунства активно інтегруються із цифровими технологіями: збір даних через кібернетичні мережі, соціальні медіа, корпоративні та державні бази даних, інтелектуальні аналітичні системи.

Особливу увагу приділено українському контексту: лекція розкриває, як історичні й сучасні державні розвідувальні органи України адаптуються до викликів гібридної війни, економічного шпигунства та кібернетичних загроз. Аналізуються випадки приватного та корпоративного шпигунства в українських компаніях і державних структурах, підкреслюється значення регуляторних, правових та етичних рамок у забезпеченні безпеки інформації та захисту національних інтересів.

Лекція розглядає взаємозв'язок державного та приватного шпигунства, акцентує на спільних і відмінних методах, завданнях та пріоритетах. Студенти ознайомляться з історичними прикладами, сучасними тенденціями та практичними кейсами, що дозволяє оцінити ефективність і ризики різних форм шпигунської діяльності у глобалізованому та цифровізованому середовищі.

Ключові поняття: державне шпигунство, приватне шпигунство, корпоративна та промислова розвідка, кібернетичне шпигунство, контррозвідка, історичний досвід, український контекст, глобалізаційні та цифрові виклики, етичні та правові аспекти.

Тема 6. Шпигунство як загроза національній безпеці України та країн ЄС і НАТО

Лекція присвячена комплексному аналізу шпигунства як однієї з ключових загроз національній безпеці держав, зокрема України та країн Європейського Союзу і НАТО, у сучасних умовах глобалізації, цифровізації та посилення міждержавної конкуренції. Шпигунство розглядається не лише як інструмент збору інформації, а як багатопланове явище, що охоплює політичні, економічні, технологічні та воєнні сфери. Основна увага приділяється оцінці ризиків, які виникають через діяльність іноземних розвідувальних служб, агентурних мереж, кібернетичних структур та приватних суб'єктів, а також через використання сучасних технологій для несанкціонованого збору та передачі даних.

Досвід України та європейських держав демонструє, що шпигунство відігравало ключову роль у формуванні безпекових стратегій, від захисту кордонів та промислових секретів у XX столітті до протидії гібридним загрозам і кібернетичним операціям у сучасності. Акцент робиться на специфіці загроз для демократичних держав ЄС та країн НАТО, де шпигунство, крім зовнішньої розвідки, активно впливає на внутрішні політичні процеси, економіку, енергетичну та технологічну інфраструктуру.

Особливу увагу приділено українському контексту. Аналізуються ризики, пов’язані з військовим шпигунством, економічним і промисловим збором даних, кібернетичними атаками, використанням подвійних агентів і інсайдерських загроз у державних та приватних структурах. Лекція демонструє, як національні розвідувальні та контррозвідувальні органи України формують комплексні стратегії протидії, взаємодіють із партнерами з ЄС і НАТО, а також інтегрують сучасні технології для виявлення та нейтралізації шпигунських загроз.

Лекція розглядає функції шпигунства як загрози: від збору стратегічної інформації та промислового шпигунства до кібератак на критичну інфраструктуру, маніпулювання суспільною думкою та впливу на політичні рішення. Аналізуються методи оцінки ризиків, профілювання агентів, цифровий моніторинг, алгоритми аналітичної обробки даних, координація державних і міжнародних органів безпеки, а також правові й етичні обмеження діяльності.

Особливий акцент робиться на викликах глобалізації та цифровізації: об’єднання розвідувальних даних у міжнародних базах, використання відкритих джерел та соціальних мереж для збору інформації, розвиток штучного інтелекту і аналітичних платформ для прогнозування загроз. Студенти ознайомляться з сучасними кейсами шпигунства в Україні та країнах ЄС і НАТО, визначатимуть рівень ризику для національної безпеки, а також зрозуміють, як інтеграція держав у глобальні безпекові системи впливає на характер і методи протидії шпигунству. Завдяки комплексному підходу лекція дозволяє сформувати системне розуміння шпигунства як загрози, виявити закономірності його розвитку, оцінити ефективність контррозвідувальних заходів та підготувати студентів до аналітичної роботи з питання національної і колективної безпеки у сучасних політичних умовах.

Ключові поняття: шпигунство, загроза національній безпеці, контррозвідка, агентурна мережа, кібернетичне шпигунство, економічне та промислове шпигунство, подвійні агенти, глобалізація, цифровізація, міжнародна координація, Україна, країни ЄС і НАТО.

Тема 7. Механізми протидії шпигунству в сучасних зрілих демократіях (США, Сполучене Королівство)

Лекція присвячена детальному аналізу механізмів протидії шпигунству у сучасних зрілих демократіях на прикладі Сполучених Штатів Америки та Сполученого Королівства, які традиційно вважаються зразком високоефективних систем національної безпеки. Шпигунство розглядається як багатопланова

загроза, що охоплює політичні, військові, економічні, технологічні та соціальні аспекти життя держави. Основна увага приділяється методам контррозвідки, законодавчому та правовому регулюванню, технологічним інструментам і стратегічній координації між державними структурами та приватним сектором, а також міждержавній співпраці на міжнародному рівні.

Історичний контекст дозволяє простежити еволюцію контррозвідувальних систем. Від формування агентурних мереж та стратегічного аналізу під час Другої світової війни до складних операцій Холодної війни, зокрема США та Велика Британія поступово відпрацьовували методи профілювання агентів, ідентифікації подвійних агентів та нейтралізації шпигунських загроз. Цей досвід формує основу сучасних систем захисту інформації, контролю доступу та превентивних заходів у сфері національної безпеки.

Сучасні виклики глобалізації та цифровізації роблять контррозвідувальні механізми ще більш складними та багаторівневими. Лекція розглядає кібернетичні загрози, економічне і промислове шпигунство, операції із впливу на громадську думку, використання відкритих джерел та соціальних мереж для збору розвідувальної інформації. Значна увага приділяється цифровим технологіям: аналітиці великих даних, штучному інтелекту та алгоритмам прогнозування ризиків, які дозволяють своєчасно виявляти підозрілі патерни поведінки агентів та потенційні загрози.

Лекція також висвітлює організаційні та правові аспекти протидії шпигунству. Демократичні держави розробляють комплексні системи контролю, де контррозвідувальні органи взаємодіють із правоохоронними структурами, судовою системою та приватним сектором. Розглядаються практики перевірки персоналу, навчання і підготовки кадрів, заходи безпеки для захисту стратегічної інформації, а також координація дій на міжнародному рівні через партнерські структури та інтеграцію в альянси безпеки.

Особливу увагу приділено кейсам подвійних агентів, операціям з виявлення внутрішніх і зовнішніх загроз, а також прикладам ефективної протидії шпигунству у критичних сферах: від оборонної промисловості до державних інформаційних систем. Лекція підкреслює баланс між ефективністю контррозвідувальної діяльності та дотриманням прав і свобод громадян, що є характерною рисою зрілих демократій.

Завдяки комплексному історико-аналітичному та технологічному підходу лекція дозволяє студентам сформувати системне розуміння принципів контррозвідувальної діяльності, оцінити ефективність механізмів захисту,

зрозуміти специфіку роботи у цифровому і глобалізованому середовищі та підготуватися до аналітичної роботи з проблем національної безпеки в умовах сучасних викликів.

Ключові поняття: контррозвідка, протидія шпигунству, механізми захисту, США, Сполучене Королівство, агентурна мережа, кібернетичне шпигунство, економічне та промислове шпигунство, цифровізація, глобалізація, подвійні агенти, міжнародна координація, законодавче та правове регулювання, приватний сектор, профілювання агентів, превентивні заходи.

Тема 8. Суб'єкти шпигунства в Україні: політична традиція та сучасність

Лекція присвячена комплексному аналізу суб'єктів шпигунства в Україні, з урахуванням історичної традиції, політичних трансформацій та сучасних викликів національної безпеки. Шпигунство розглядається як багаторівневе явище, що включає державні, приватні та міжнародні агенти, а також діє в межах політичних, економічних, технологічних і соціальних процесів. Основна увага приділяється ідентифікації суб'єктів шпигунства, їхнім завданням, методам діяльності та ролі у формуванні національної безпеки України.

Історичний аспект лекції охоплює досвід різних періодів: від козацької доби та діяльності дипломатичних агентів у період національного відродження XIX – початку XX століття до формування радянських розвідувальних структур і еволюції шпигунства у незалежній Україні. Розглядається, як політичні режими та зовнішньополітичні виклики впливали на організацію агентурних мереж, методи збору інформації та контррозвідувальні стратегії. Лекція демонструє, що історичний досвід формує сучасні підходи до управління ризиками та профілювання агентів.

Сучасний контекст включає аналіз суб'єктів шпигунства в умовах незалежної України, зокрема державних структур (розвідувальні та контррозвідувальні органи), приватних компаній, які займаються кібербезпекою, а також іноземних агентурних мереж. Окрему увагу приділено співпраці України з міжнародними партнерами, зокрема країнами ЄС та НАТО, у сфері обміну розвідувальною інформацією, протидії кіберзагрозам та забезпечення національної безпеки.

Лекція розглядає функції та пріоритети різних суб'єктів шпигунства: від державної розвідки та контррозвідки до приватних і міжнародних акторів, що займаються економічним, промисловим та кібернетичним шпигунством.

Оцінюються методи збору інформації, технологічні інструменти, профілювання агентів, ризики подвійної лояльності та внутрішні загрози. Особливий акцент робиться на оцінці ефективності механізмів захисту національної безпеки та адаптивності українських органів розвідки до сучасних викликів глобалізації та цифровізації.

Лекція формує у студентів системне розуміння того, хто є суб'єктом шпигунства в Україні, як історичні традиції та політична культура вплинули на його розвиток, та як сучасні технології і міжнародна інтеграція змінюють характер загроз і методи протидії. Завдяки комплексному підходу лекція дозволяє студентам оцінити закономірності діяльності різних суб'єктів, побудувати власні аналітичні оцінки ризиків та розробити пропозиції щодо підвищення ефективності захисних стратегій держави.

Ключові поняття: суб'єкти шпигунства, державна розвідка, контррозвідка, приватне шпигунство, економічне і промислове шпигунство, кібернетичне шпигунство, подвійні агенти, політична традиція України, сучасна безпека, міжнародна співпраця, профілювання агентів, глобалізація, цифровізація, ризики національної безпеки.

Отже, аналіз змісту лекцій свідчить, що шпигунство розглядається як багатоплановий соціально-політичний інститут, що поєднує історичні традиції, сучасні технологічні можливості та інтеграцію у глобальні системи безпеки. Вивчення його генези та сутнісних характеристик дозволяє простежити еволюцію від класичних форм агентурної діяльності до сучасного кібер- і економічного шпигунства, а також зрозуміти, як функції збору інформації, контррозвідки, маніпуляції та прогнозування політичних рішень реалізуються через структуровані агентурні мережі і мотивованих агентів. Особлива увага приділяється профілюванню шпигунів, методам аналізу поведінкових патернів та оцінки ризиків для національної безпеки, що формує аналітичні компетенції студентів у сфері безпеки та політики.

Лекції підкреслюють різноманітність підходів до визначення шпигунства у політичній науці, його роль як інструменту державної політики та соціокультурного явища, що відображає конфлікти інтересів і рівень довіри у суспільстві. Історичний аналіз показує, що шпигунство завжди було тісно пов'язане з типом політичного режиму: демократичні держави прагнуть балансувати ефективність і законність, авторитарні та тоталітарні — контролювати громадян та придушувати опозицію, тоді як гібридні режими

поєднують елементи обох стратегій. Сучасні виклики глобалізації та цифровізації розширюють поле діяльності шпигунства, включаючи кібер- та економічні загрози, що підкреслює необхідність інтегрованих, технологічно і аналітично підготовлених підходів до контррозвідувальної діяльності.

Особливий акцент зроблено на українському контексті та міжнародній співпраці, що дозволяє студентам отримати глибоке уявлення про специфіку діяльності суб'єктів шпигунства в умовах пострадянського простору та сучасних викликів глобальної безпеки. У межах курсу розглядаються державні розвідувальні та контррозвідувальні органи України, їхня структура, завдання та оперативні методи, включно з моніторингом інформаційних потоків, оцінкою ризиків внутрішніх і зовнішніх загроз, протидією інсайдерським і кібернетичним атакам. Крім того, студенти знайомляться з приватними суб'єктами шпигунської діяльності, включно з корпоративною розвідкою та кібербезпековими компаніями, а також із діяльністю міжнародних агентурних мереж і їхньою взаємодією з українськими державними структурами. Особлива увага приділяється координації дій із партнерами з ЄС і НАТО, обміну розвідувальною інформацією, інтеграції технологій штучного інтелекту та аналітичних платформ для прогнозування загроз.

Аналіз досвіду США та Великої Британії демонструє ефективність високорозвинених демократичних систем контррозвідки, де застосовується комплексний підхід до профілювання агентів, виявлення подвійних лояльностей і нейтралізації загроз без порушення прав і свобод громадян. Особлива увага приділяється організаційним і технологічним механізмам, включно з аналітикою великих даних, кіберзахистом критичної інфраструктури та превентивними заходами протидії економічному та промисловому шпигунству.

Комплексне вивчення шпигунства дозволить студентам сформувати системне та багаторівневе розуміння його ролі в сучасних політичних процесах, оцінити ризики для національної безпеки держав, міжнародних альянсів та корпоративного середовища, а також розробляти практично обґрунтовані пропозиції щодо підвищення ефективності захисних стратегій у глобалізованому, цифровізованому та високотехнологічному середовищі. Воно забезпечуватиме аналітичну підготовку до оцінки загроз, побудови профілів агентів, планування контррозвідувальних операцій та інтеграції українського досвіду у міжнародні системи безпеки.

***

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК ДЛЯ ЗАСВОЄННЯ ОСНОВНИХ ПОНЯТЬ ЛЕКЦІЙНИХ ЗАНЯТЬ

1. **Шпигунство (Espionage)** – діяльність із прихованого збору інформації для стратегічних, політичних або економічних цілей.
2. **Розвідка (Intelligence)** – систематичний збір і аналіз даних для ухвалення державних рішень.
3. **Контррозвідка (Counterintelligence)** – виявлення та нейтралізація загроз від шпигунів і агентів.
4. **Мотивація агентів (Agent Motivation)** – фактори, що спонукають осіб до шпигунської діяльності.
5. **Методи збору інформації (Information Gathering Methods)** – техніки й засоби отримання секретних даних.
6. **Профілювання шпигунів (Spy Profiling)** – аналіз поведінки та характеристик агентів для прогнозування їхніх дій.
7. **Аксіологічні аспекти (Axiological Aspects)** – ціннісні та етичні питання, що стосуються шпигунства.
8. **Політична наука (Political Science)** – дисципліна, що вивчає політичні процеси, включно із шпигунством.
9. **Функції агентів (Agent Functions)** – роль і завдання агентів у зборі інформації та забезпеченні безпеки.
10. **Етичні аспекти (Ethical Aspects)** – моральні обмеження і стандарти в шпигунській діяльності.
11. **Правові аспекти (Legal Aspects)** – нормативно-правове регулювання розвідки і контррозвідки.
12. **Сучасні виклики (Modern Challenges)** – новітні загрози у шпигунстві, включно з кібер- та економічним.
13. **Історія шпигунства (History of Espionage)** – етапи розвитку шпигунства від давнини до сучасності.
14. **Агентурна мережа (Agent Network)** – система агентів і контактів для збору інформації.
15. **Методи розвідки (Intelligence Methods)** – конкретні операційні прийоми збору даних.
16. **Воєнне шпигунство (Military Espionage)** – збір даних про озброєння, сили та плани потенційного противника.

17. **Промислове шпигунство (Industrial Espionage)** – незаконне отримання комерційно чи технологічно цінної інформації.
18. **Кібернетичне шпигунство (Cyber Espionage)** – збір інформації через цифрові мережі та IT-системи.
19. **Економічні загрози (Economic Threats)** – ризики, пов'язані з економічним шпигунством і втратами ресурсів.
20. **Типи політичних режимів (Political Regime Types)** – демократія, авторитаризм, тоталітаризм та гібридні форми.
21. **Гібридні режими (Hybrid Regimes)** – політичні системи зі змішаними ознаками демократії та авторитаризму.
22. **Зовнішнє шпигунство (Foreign Espionage)** – діяльність, спрямована на отримання інформації від інших держав.
23. **Внутрішнє шпигунство (Domestic Espionage)** – діяльність всередині країни для контролю або виявлення загроз.
24. **Державне шпигунство (State Espionage)** – збір інформації державними органами для національної безпеки.
25. **Приватне шпигунство (Private Espionage)** – шпигунська діяльність приватних осіб або компаній.
26. **Подвійні агенти (Double Agents)** – особи, які працюють одночасно на дві сторони.
27. **Глобалізація (Globalization)** – процес інтеграції держав, економік і суспільств, що впливає на шпигунство.
28. **Цифровізація (Digitalization)** – використання цифрових технологій у шпигунській діяльності.
29. **Міжнародна координація (International Coordination)** – співпраця держав та організацій для протидії шпигунству.
30. **Суб'єкти шпигунства (Espionage Actors)** – усі учасники процесу шпигунства: державні органи, приватні компанії, агенти та мережі.

ОСНОВНИЙ ЗМІСТ СЕМІНАРСЬКИХ ЗАНЯТЬ

Семінарські заняття пропонується розглядати як реалізацію практичних ситуацій теорії ігор – певної аналітичної рамки стратегічної гри з неповною інформацією. Теорія ігор, започаткована *Джоном фон Нойманом* і *Оскаром Моргенштерном*, виходить із припущення, що всі політичні чи воєнні актори діють раціонально, намагаючись максимізувати власну вигоду за умов стратегічної взаємодії з іншими гравцями. Шпигунство – це саме гра з неповною інформацією, де кожен учасник (держава, розвідслужба, політичний актор) має власні цілі, ресурси та обмеження, але не повністю знає про наміри й можливості іншої сторони.

У контексті теорії ігор шпигунство можна моделювати як послідовну гру з елементами прихованих дій (hidden actions) і асиметрії знань (information asymmetry). Гравці: держава А (агент шпигунства), держава В (об'єкт шпигунства). Стратегії: шпигувати/не шпигувати; виявляти/не виявляти; карати/ігнорувати. Виплати: отримання цінної інформації, збереження секретів, покарання противника, дипломатичні або репутаційні втрати. Тип гри: «гра довіри» або «гра у приховування» (signaling game), де один гравець посилає сигнали, а інший намагається їх інтерпретувати. Прикладом є «гра шпигун – контршпигун», у якій виграш одного гравця (отримання секретної інформації) прямо залежить від втрати іншого (викриття або витік даних).

Шпигунство також можна інтерпретувати як варіант дилеми безпеки – класичної моделі теорії ігор, коли дії, спрямовані на підвищення власної безпеки (розвідувальна активність), створюють загрозу для іншої сторони, що у відповідь вживає дзеркальних заходів. Це веде до *рівноваги Неша* – стану, коли жоден актор не може покращити свою позицію, не погіршивши становища іншого. Така рівновага пояснює, чому шпигунська діяльність триває навіть між державами, які формально перебувають у мирі: вигідніше підтримувати "контрольований ризик", ніж відмовитися від нього.

Шпигунство тісно пов'язане з ігровими моделями обману (deception games) і сигнальними іграми (signaling games). Наприклад: а) агент посилає фальшиві сигнали, щоб приховати справжні наміри (дезінформація); б) контррозвідка відповідає дзеркально, створюючи "пастки інформації" (information traps). Такі взаємодії формують ігрову динаміку багаторівневого обману, де раціональність гравців стає відносною – вони діють не на основі істини, а на основі переконань про переконання інших.

Застосування теорії ігор до аналізу шпигунства дозволяє: 1) пояснити поведінкову логіку держав у сфері розвідки та контррозвідки; 2) моделювати оптимальні стратегії реагування на загрози; 3) прогнозувати наслідки інформаційних війн і витоків даних; 4) визначати точку рівноваги між відкритістю та безпекою у міжнародних відносинах. З наукового погляду це відкриває шлях до інтеграції політичної науки, безпекових студій і когнітивного моделювання, що відповідає сучасним тенденціям розвитку аналітичної політології.

Відтак для роботи здобувачів освіти під час семінарських занять пропонується 9 оригінальних сюжетів (ігрових сценаріїв), які дозволяють аналізувати феномен шпигунства через призму теорії ігор із урахуванням політичної логіки, міжнародної безпеки, інформаційних війн і когнітивних стратегій. Кожен сценарій подається як модельна гра з потенційними гравцями, стратегіями, виграшами й теоретичною інтерпретацією.

1. «Гра подвійного агента» (The Double Agent Game)

- Тип гри: послідовна гра з неповною інформацією.
- Гравці: Держава А, Держава Б, агент із «подвійною лояльністю» (подвійний агент).
- Сюжет: шпигун працює одночасно на дві сторони, намагаючись максимізувати власну вигоду, не викривши себе.
- Теоретична рамка: проблема асиметрії інформації та рівноваги Бейєса-Неша.
- Ідея: показує, як довіра в міжнародних відносинах є стратегічним ресурсом, а не моральною категорією.

Тип гри: послідовна гра з неповною інформацією. *Гравці:* держава А, держава Б, агент із «подвійною лояльністю» (подвійний агент). *Теоретична рамка:* рівновага Бейєса-Неша, асиметрія інформації, стратегія сигналів і довіри.

Сюжет і логіка гри. У цій грі агент (шпигун) перебуває в полі перехресних інтересів двох держав – А і Б, які одночасно прагнуть отримати від нього секретну інформацію. Обидві сторони не мають повної інформації щодо справжньої лояльності агента: він може діяти як агент А, впроваджений у Б, або як агент Б, впроваджений у А, або навіть як автономний гравець, що використовує обидві держави у власних інтересах. Ключова особливість цієї гри – асиметрія інформації. Кожен із державних акторів має лише гіпотези щодо типу агента (вірний, подвійний чи фальшивий), тому приймає рішення, виходячи з

апостеріорних ймовірностей, які постійно оновлюються залежно від сигналів, які подає агент. Це створює динаміку стратегічної недовіри: кожна сторона оцінює не лише отриману інформацію, але й мотиви того, хто її надає.

Аналітична ідея. У класичній логіці теорії ігор така модель демонструє, що довіра у шпигунських і міжнародних відносинах не є моральною категорією, а раціональним ресурсом, який можна інвестувати, експлуатувати або втрачати. Довіра тут – це стратегічна змінна, що підлягає оптимізації. Рівновага Бейєса-Неша настає тоді, коли обидві держави обирають оптимальні стратегії співпраці чи контролю, враховуючи ймовірні типи агента, а сам агент знаходить точку, де його корисність (власна вигода, безпека, автономія) максимізується при мінімальному ризику викриття.

Політологічне значення. Цей сюжет може бути інтерпретований як метафора міжнародної довіри в епоху гібридних загроз. У глобальній системі безпеки держави дедалі частіше діють у режимі «обмеженої довіри», сприймаючи партнерів одночасно як союзників і потенційних супротивників. Феномен подвійного агента, перенесений у політичну теорію, показує, що лояльність у міжнародній політиці є функцією вигоди та ризику, а не стабільної ідентичності.

Концептуальний підсумок. «Гра подвійного агента» є моделлю стратегічної взаємодії в умовах радикальної невизначеності, коли головним ресурсом стає не сила, а інформаційна асиметрія. У ній агент – не просто передавач відомостей, а посередник між двома раціональностями, який перетворює довіру на інструмент самозбереження і вигоди. Ця гра показує, що у шпигунстві немає абсолютної лояльності – існують лише змінні поля інтересів, які актори постійно перелічують залежно від контексту. Відносини між державами, як і між агентом і його кураторами, формуються не на основі моралі чи ідентичності, а на підставі динамічної оцінки ризику та вигоди. З точки зору теорії ігор, «подвійний агент» уособлює ігрову рівновагу між обманом і довірою – ситуацію, у якій жоден із гравців не може повністю довіряти іншому, але водночас змушений підтримувати мінімальний рівень взаємодії, щоб не втратити доступ до критичної інформації. У політичному вимірі ця модель розкриває структурну двозначність міжнародної довіри: навіть союзники можуть виступати суперниками у сфері розвідки, а зрадництво може бути формою раціональної поведінки. Таким чином, довіра стає функцією вигоди, а шпигун – її стратегічним виміром. У сучасній безпековій парадигмі «гра подвійного агента» демонструє, що міжнародна стабільність не усуває шпигунство, а інституціоналізує його. Головне питання не в тому, хто

зрадить, а коли, за яких умов і якою ціною – саме ці параметри й визначають архітектоніку глобальної безпеки.

2. «Пастка довіри» (The Trust Trap)

- Тип гри: повторювана дилема ув'язненого.
- Гравці: союзники у військово-політичному блоці.
- Сюжет: держави-членкині підозрюють одна одну у шпигунстві, попри формальний союз.
- Ідея: демонструє парадокс – навіть у системі колективної безпеки (НАТО, ЄС) виникає стратегічна недовіра.
- Мета гри: знайти точку стабільної рівноваги між відкритістю і безпекою.

Тип гри: повторювана гра з неповною інформацією (iterated game). *Гравці:* держава А (ініціатор співпраці), держава Б (реципієнт інформації або партнер), прихований шпигун у структурі довіри. *Теоретична рамка:* дилема довіри в умовах стратегічної взаємозалежності; повторювана «гра довіри» (Trust Game) з елементами обману й морального ризику.

Сюжет і динаміка гри. Дві держави (А і Б) вступають у довготривалу співпрацю в рамках обміну розвідувальною або технологічною інформацією. Обидві сторони розраховують на взаємну вигоду: посилення колективної безпеки, обмін даними, спільні аналітичні програми. Проте одна зі сторін (або прихований агент усередині неї) використовує механізм довіри для стратегічного проникнення – отримання критичних даних, контроль над інформаційними потоками, маніпулювання аналітичними висновками. Початково сторони діють за моделлю гра з позитивною сумою, де довіра підвищує ефективність і вигоди. Але поступово довіра стає вразливістю – стратегічною пасткою, у яку потрапляє той, хто інвестує в неї занадто беззастережно. Саме тому «пастка довіри» – це ситуація, коли здатність довіряти перетворюється на слабкість, а зловживання довірою – на найефективніший інструмент шпигунства.

Аналітична ідея. Ця гра моделює перетворення стратегічного капіталу довіри в інструмент контролю. В умовах неповної інформації кожен гравець змушений оцінювати не лише поточну вигоду, а й майбутні ризики порушення домовленостей. У повторюваній грі, де минулі дії впливають на очікування майбутніх, виникає ефект репутації. Якщо одна сторона зраджує довіру, то інша оновлює свої переконання щодо її надійності — і на наступному етапі змінює стратегію: замість співпраці переходить до ізоляції або асиметричної відповіді. У

термінах теорії ігор, рівновага Бейєса-Неша тут досягається лише за умови мінімального ризику обману – тобто коли очікувана вигода від зради менша, ніж довгострокові втрати від втрати довіри. Але у шпигунських системах ця рівновага нестійка: агент або держава, що прагне короткострокового виграшу, має стимул зламати рівновагу через стратегічний обман. Саме це і формує «пастку довіри» – стабільність системи руйнується зсередини самим механізмом, що її утримував.

Політологічне значення. «Пастка довіри» демонструє, що у міжнародних відносинах і шпигунстві довіра одночасно виступає ресурсом і джерелом ризику. Вона дозволяє державам підвищувати ефективність співпраці, обмінюватися критичною інформацією та створювати синергетичні ефекти, але водночас відкриває вразливості для стратегічного проникнення та маніпуляцій. Ключовим є парадокс довіри: надмірна відкритість створює можливість для зради, а надмірна недовіра руйнує потенційні вигоди від співпраці. У термінах теорії ігор це ілюструє класичну дилему взаємної вигоди, де короткострокова спокуса обману протистоїть довгостроковим втратам через руйнування репутації та партнерських зв'язків. З точки зору політичної науки, довіра виступає стратегічною змінною, що потребує постійного управління: держави і агенти оцінюють, яку її частину інвестувати, а коли обмежити, щоб мінімізувати ризики. Надмірна довіра підвищує вразливість системи безпеки, а повна недовіра унеможливлює співпрацю.

Концептуальний підсумок. «Пастка довіри» підкреслює, що стабільність союзів і партнерство залежить від балансу між співпрацею та контролем, а механізми шпигунства стають невід'ємним елементом управління національною та міжнародною безпекою. Гра моделює, як держави та агенти використовують довіру як стратегічний ресурс, оптимізуючи її інвестиції і обмеження для мінімізації ризиків. Надмірна довіра перетворюється на слабкість, а повна недовіра – на блокування потенційної співпраці. Відтак ефективне управління довірою стає ключовим елементом сучасної безпекової політики та стратегічного аналізу міжнародних відносин.

3. «Кібер-шпигун і цифрова пастка» (The Cyber Spy Dilemma)

- Тип гри: ігри з нульовою сумою та асиметрією інформації.
- Гравці: держава-шпигунка і технологічна корпорація.
- Сюжет: урядова розвідка впроваджує шпигунські алгоритми в комерційні системи ШІ.

- Ідея: цифрове шпигунство як новий вимір «гібридної гри», де інструментом стає саме середовище (data-space).
- Політологічна інтерпретація: межа між безпекою і приватністю стирається, а формується «алгоритмічна влада».

Тип гри: повторювана гра з неповною інформацією та елементами багато-крокового прогнозування. *Гравці:* держава А (ціль цифрової атаки), держава Б (ініціатор кібершпигунства), Кібер-агент (агент або хакер, що здійснює проникнення). *Теоретична рамка:* дилема взаємного ризику в цифровій сфері; застосування моделей асиметричної інформації та стратегій «атака – захист».

Сюжет і динаміка гри. Держава Б прагне отримати критичні дані про державу А через кібершпигунство (наприклад, військові секрети, науково-технічні розробки, фінансові дані). Вона може: 1) атакувати (Attack) – здійснити кібершпецоперацію для отримання інформації; 2) утриматися (Refrain) – не здійснювати атаку, економлячи ресурси і не підвищуючи ризик виявлення. Держава А може: 1) посилити кіберзахист (Defend) – запобігти витоку, але витратити ресурси і потенційно втратити частину ефективності; 2) не посилювати захист (Neglect) – економія ресурсів, але підвищений ризик компрометації. Кіберагент (Cyber Spy) оцінює ймовірність успіху атаки та стратегічну цінність даних. Гра повторюється, оскільки держави постійно оновлюють свої цифрові системи, а агенти вдосконалюють методи проникнення.

Аналітична ідея. 1. Асиметрія інформації: держава Б знає, які вразливості існують, але держава А може їх частково прогнозувати. 2. Дилема ресурсів: Інвестування в кіберзахист витрачає бюджети, але недооцінка загроз може коштувати стратегічної переваги. 3. Повторюваність гри: Кожен етап модифікує стратегії, формуючи динамічну рівновагу ризиків, де короткострокові вигоди кібер-шпигуна можуть бути компенсовані довгостроковими втратами від виявлення. У термінах теорії ігор, оптимальна стратегія для обох сторін – це баланс між атакою/захистом і ризиком компрометації, що часто моделюється через рівновагу Бейєса-Неша або стратегії змішаного типу.

Політологічне значення. «Кібершпигун і цифрова пастка» ілюструє новий вимір державної безпеки в умовах цифровізації та інформаційної глобалізації. У сучасному світі інформація перетворюється на стратегічний ресурс, а кібершпигунство стає інструментом реалізації національних інтересів без прямого військового втручання. Гра демонструє, що безпека держави більше не обмежується фізичним контролем території або військовою потугою; критичною

стає здатність захищати інформаційні активи, контролювати цифрові канали і передбачати дії потенційних противників. Додатково, гра ілюструє складність управління асиметричними ризиками: держави повинні балансувати між інвестиціями у кіберзахист і економією ресурсів, враховуючи постійно змінні технологічні можливості та тактичні дії кіберагентів. Стратегічна поведінка агентів у цифровому просторі часто визначає розстановку сил у міжнародних відносинах, де навіть дрібні інформаційні витоки можуть мати масштабні політичні та економічні наслідки. «Кібершпигун і цифрова пастка» підкреслює, що сучасна безпека – це система постійного моніторингу, аналізу і адаптації, де цифрові технології стають як ресурсом, так і потенційним джерелом уразливості.

Концептуальний підсумок. «Кібершпигун і цифрова пастка» демонструє, що у цифровій сфері стратегічна перевага формується через контроль інформації, прогнозування поведінки противника і оптимізацію ресурсів, а не лише через відкриту військову силу. Інвестиції у кіберзахист, активне протидіяння кібератакам та проведення спецоперацій стають невід'ємною частиною національної безпеки та міжнародної стратегії держави. Гра підкреслює, що ефективна політика у сфері кібербезпеки потребує балансу між ризиком і ресурсами, а також постійного аналізу потенційних загроз, оцінки поведінки кіберагентів і держав у умовах неповної інформації. Водночас, вона показує, що цифровий простір перетворюється на арену стратегічних ігор, де перемога визначається не лише технічними можливостями, а й здатністю швидко адаптувати стратегії до змін у поведінці опонентів та умовах глобальної інформаційної взаємодії.

4. «Гра дзеркала» (The Mirror Game)

- Тип гри: симетрична гра спостереження.
- Гравці: дві розвідки, що копіюють одна одну.
- Сюжет: контррозвідка створює фальшивого шпигуна, який має видати справжнього.
- Ідея: моделює поведінку за принципом «дзеркального відображення» – стратегічна адаптація через повторення.
- Теоретичний зміст: самоорганізована рівновага системи шпигун–контршпигун.

Тип гри: послідовна гра з неповною інформацією та елементами стратегічного наслідування. *Гравці:* держава А (ціль шпигунства), держава Б

(ініціатор шпигунства або контршпигунства), шпигун/агент, який збирає або передає інформацію. *Теоретична рамка:* моделювання стратегій повторюваної взаємодії, дзеркального наслідування, рівновага Неша у повторюваних іграх.

Сюжет і динаміка гри. У «Грі дзеркала» кожна держава спостерігає за поведінкою іншої і реагує, наслідуючи або адаптуючи дії супротивника. Наприклад: а) держава Б вирішує, чи проводити активне шпигунство, чи обмежитися пасивним збором інформації; б) держава А у відповідь може підвищити контршпецзахист або залишити слабкі місця для перевірки реакції опонента; в) агент виконує операції, відображаючи стратегію одного гравця до дій іншого, що створює ефект «дзеркала». Гра повторюється багаторазово, а стратегії адаптуються, формуючи динамічну рівновагу, де жодна сторона не може різко змінити поведінку, не ризикувавши стратегічними втратами.

Аналітична ідея. 1. Повторювана взаємодія: Кожне рішення впливає на майбутні стратегії супротивника, що змушує держави балансувати між атакою, захистом і перевіркою опонента. 2. Дзеркальне наслідування: Реакції держав часто симетричні, що моделює реальні ситуації кібершпигунства та контршпецоперацій, коли дії однієї сторони віддзеркалюються протидією іншої. 3. Ризик і довіра: Держави оцінюють, наскільки можна довіряти опоненту, і визначають оптимальну «відстань» між відкритістю та захистом. У термінах теорії ігор, оптимальна стратегія формується через повторювані ігри з частковою інформацією, де баланс між взаємною вигодою і ризиком порушення довіри визначає стратегію Неша.

Політологічне значення. «Гра дзеркала» демонструє, що у сучасній міжнародній безпеці поведінка держав і агентів часто відображає дії супротивників, створюючи динаміку взаємних реакцій, які формують баланс сил. У цій грі стратегічне наслідування стає механізмом прогнозування і контролю ризиків: держави оцінюють поведінку опонента і адаптують свої дії, що дозволяє мінімізувати загрози та оптимізувати розподіл ресурсів у сферах розвідки, контршпигунства та кібербезпеки. Гра також підкреслює роль інформаційних потоків як стратегічного ресурсу: навіть невеликі зміни у поведінці одного гравця можуть викликати ланцюгові ефекти у стратегічних рішеннях іншого. Це відображає сучасну політологічну парадигму, де симетричні та адаптивні реакції держав визначають стабільність або ескалацію конфліктів, а ефективне управління довірою, ризиком та інформаційною асиметрією стає ключовим елементом національної та міжнародної безпеки. Крім того, гра демонструє, що повторювані взаємодії створюють системи стратегічної залежності, де дії однієї

сторони формують очікування та поведінку іншої. Така модель дозволяє аналізувати складні політичні процеси, наприклад, ескалацію шпигунських конфліктів, протидію кібератакам або адаптацію оборонних стратегій у реальному часі.

Концептуальний підсумок. «Гра дзеркала» підкреслює, що дзеркальне наслідування у шпигунстві та контрспецопераціях – це не лише стратегія відповіді, а ключовий інструмент управління ризиком і довірою. Держави та агенти формують адаптивні стратегії, які коригуються на основі реакцій опонента, створюючи механізм постійного стратегічного моніторингу. Це дозволяє передбачати потенційні загрози, мінімізувати ризики та знаходити оптимальний баланс між відкритістю і контролем. Гра демонструє, що у сучасній політичній і безпековій парадигмі стабільність міжнародних відносин значною мірою залежить від здатності держав прогнозувати та відповідати на дії суперників у режимі постійного стратегічного дзеркала, де інформаційні потоки, адаптивна поведінка агентів та швидка реакція на зміни стають критичною умовою виживання та стратегічної переваги. Отож «Гра дзеркала» ілюструє, що у сучасній системі міжнародної безпеки навіть без прямого військового втручання контроль і маніпуляція інформаційними каналами можуть визначати баланс сил і ефективність державних стратегій.

5. «Гра розкриття» (The Leak Game)

- Тип гри: гра сигналів і фальсифікацій (signaling game).
- Гравці: держава, журналісти, громадськість.
- Сюжет: витік секретних даних (як у випадках Сноудена чи WikiLeaks) стає інструментом політичного тиску.
- Ідея: шпигунство трансформується у публічну політику – боротьбу за довіру громадської думки.
- Рівновага: між свободою інформації та легітимністю державної таємниці.

Тип гри: одночасна гра з неповною інформацією та елементами стратегічного блефу. *Гравці:* держава А (володіє критичною інформацією), держава Б (потенційний отримувач інформації), шпигун або агент-витік (Leak Agent), який контролює передачу або приховування даних. *Теоретична рамка*: теорія ігор з неповною інформацією, модель блефу та стратегічного ризику, рівновага Бейєса-Неша.

Сюжет і динаміка гри. У «Грі розкриття» Держава А володіє критичною інформацією (наприклад, військовими планами, науково-технічними розробками або економічними даними). Вона може: а) заховати інформацію (Conceal) – зберегти контроль над ресурсом, але витратити час і ресурси на захист; б) випустити частину інформації (Partial Leak) – створити ілюзію відкритості, перевірити реакцію опонента; в) Повністю розкрити інформацію (Full Leak) – передати дані, сподіваючись на стратегічну вигоду, але підвищивши ризик шкоди. Держава Б у відповідь може: а) прийняти інформацію та діяти (Act) – використовувати отримані дані для стратегічної переваги; б) ігнорувати витік (Ignore) – не реагувати, щоб уникнути помилкових висновків; в) провести перевірку та контршпецоперацію (Verify / Counteract) — оцінити достовірність і можливі ризики, підвищивши витрати і час. Leak Agent оцінює ймовірність успіху передачі даних і стратегічну цінність витоку, враховуючи ризик виявлення або зворотної шкоди. Гра повторюється, оскільки держави постійно оновлюють інформаційні системи та контроль за витоками.

Політологічне значення. «Гра розкриття» показує, що контроль за інформацією та управління витоками є критичною складовою сучасної національної безпеки. Гра ілюструє, як держави приймають рішення під умовами неповної інформації, оцінюють потенційні вигоди та ризики, а також використовують інформаційні витоки як інструмент стратегічного маневру. Політологічно, гра підкреслює: а) блеф і часткове розкриття як елементи політичної тактики та дипломатії; б) асиметричні вигоди та ризики у відносинах між державами; в) роль агентів і внутрішніх каналів витоку як ключових чинників, що впливають на стратегічну поведінку держав; г) важливість адаптивної політики контролю інформації у системах колективної та національної безпеки.

Концептуальний підсумок. «Гра розкриття» демонструє, що у сучасній міжнародній системі інформація сама по собі стає зброєю, а управління витоками – критичною компетенцією держави. Стратегії держав формуються на основі оцінки короткострокових вигод від розкриття і довгострокових ризиків для національної безпеки. Блеф, часткове розкриття та перевірка інформації стають ключовими механізмами управління довірою, ризиком і стратегічною асиметрією. У термінах теорії ігор ця гра ілюструє комбінацію одночасних рішень з неповною інформацією, де кожна сторона постійно прогнозує дії опонента та коригує власну поведінку. «Гра розкриття» показує, що стратегічна робота з інформаційними потоками та витоками визначає не тільки національну безпеку, а й баланс сил у міжнародних відносинах, роблячи інформацію ресурсом і ризиком одночасно.

6. «Гра фальшивого сигналу» (The False Flag Operation)

- Тип гри: стратегічна гра з дезінформацією.
- Гравці: держава-агресорка, держава-жертва, третя сторона (світова спільнота).
- Сюжет: фальшиве шпигунське звинувачення створюється для виправдання агресії або санкцій.
- Ідея: демонструє, як шпигунство стає політичним наративом, що формує міжнародну легітимність.
- Приклад: операції впливу у добу постправди.

Тип гри: послідовна гра з неповною інформацією та елементами стратегічного блефу. *Гравці:* держава А (ініціатор операції), держава Б (ціль потенційного обману), агенти / шпигуни, які здійснюють або виявляють операції. *Теоретична рамка*: теорія ігор з неповною інформацією, моделювання блефу та стратегічного обману, рівновага Бейєса-Неша.

Сюжет і динаміка гри. У «Грі фальшивого сигналу» держава А намагається створити хибну інформацію або інсценувати дії, щоб збити з пантелику опонента: а) відправити фальшивий сигнал (False Flag) – симулювати погрози або події, що підвищують ймовірність помилкових рішень у держави Б; б) не робити нічого (Neglect) – утриматися від обману, зберігши ресурс, але пропустити потенційні стратегічні переваги. Держава Б у відповідь може: а) вірити сигналу та реагувати (React) – прийняти хибну інформацію за істинну, що може призвести до стратегічних помилок; б) ігнорувати сигнал (Ignore) – не реагувати, але ризикувати пропустити реальні загрози; в) перевірити та контрспецоперацію (Verify / Counter) — оцінити достовірність сигналу, підвищивши ресурси та витрати часу. Агенти виконують операції, оцінюючи ймовірність успіху обману і стратегічну цінність введення противника в оману. Гра повторюється, оскільки держави постійно оцінюють нові сигнали та адаптують стратегічні стратегії.

Політологічне значення. «Гра фальшивого сигналу» демонструє, що сучасна державна безпека вже не обмежується прямим застосуванням військової сили, а активно включає маніпуляції інформаційними потоками, дезінформацію та стратегічний обман як інструменти досягнення національних цілей. У цій грі стратегічний обман стає механізмом реалізації асиметричних переваг, коли відносно слабша сторона може впливати на поведінку сильнішого гравця через введення його в оману, а сильніша – через контроль та адаптацію стратегій – мінімізувати загрози. Політологічно гра підкреслює, що сучасні міжнародні

відносини функціонують як динамічна система сигналів і контрсигналів, де кожна держава постійно оцінює достовірність інформації, адаптує свої дії і прогнозує реакцію опонента. Такі операції впливають не лише на безпеку окремих держав, а й на стабільність регіональних і глобальних альянсів, бо навіть короткострокові дезінформаційні кампанії можуть спровокувати ескалацію, дипломатичні конфлікти або стратегічні помилки. Гра також показує парадокс довіри та недовіри: надмірна довіра до сигналів може призвести до серйозних стратегічних втрат, тоді як надмірна підозрілість підриває ефективність співпраці та інтеграційних процесів. У цьому сенсі стратегічний блеф виступає не лише як засіб обману супротивника, а як інструмент управління ризиком, який змушує держави постійно балансувати між відкритістю, контролем і захистом інформаційних ресурсів. Гра ілюструє сучасну політологічну парадигму, де інформаційний простір стає полем змагання за стратегічну перевагу, а агенти та держави, які володіють здатністю передбачати, інтерпретувати і моделювати сигнали опонента, отримують вирішальну перевагу у реалізації національної політики та безпеки.

Концептуальний підсумок. «Гра фальшивого сигналу» підкреслює, що стратегічний обман є невід'ємним елементом управління сучасною національною та міжнародною безпекою. 1. Асиметричність інформації: Держави приймають рішення за умов неповної та потенційно хибної інформації, що вимагає розвитку аналітичних, контршпигунських та превентивних стратегій. 2. Роль блефу як ресурсу: Фальшиві сигнали виступають інструментом впливу, який дозволяє формувати поведінку опонента, мінімізувати прямі витрати на захист і підвищити стратегічну ефективність власних дій. 3. Баланс між ризиком і вигодою: надмірне використання блефу або повна відсутність контролю над сигналами може призвести до серйозних втрат, тому держави постійно оцінюють рівень ризику і потенційні вигоди від кожної операції. 4. Довгострокові наслідки для міжнародної системи: Фальшиві сигнали та обманні операції формують очікування, довіру або недовіру між державами, впливають на альянси, партнерства і навіть на глобальні механізми колективної безпеки. 5. У термінах теорії ігор «Гра фальшивого сигналу» ілюструє повторювану стратегію з неповною інформацією, де кожна сторона коригує поведінку відповідно до прогнозованих дій супротивника, а ефективність державної політики визначається здатністю маніпулювати інформаційними потоками та передбачати реакції опонентів. Ця гра показує, що контроль, оцінка та моделювання інформаційних сигналів є критичним чинником стратегічної переваги. У сучасній безпековій парадигмі навіть без застосування

військової сили держави, які вміють ефективно управляти фальшивими сигналами, отримують значну перевагу у підтриманні балансу сил, стабільності альянсів та захисті національних інтересів.

7. «Гра технологічної гонки» (The Quantum Race)

- Тип гри: гра з позитивною сумою і невизначеністю майбутнього.
- Гравці: високотехнологічні держави, що конкурують у сфері штучного інтелекту та квантових комунікацій.
- Сюжет: шпигунство використовується для скорочення наукового відставання.
- Ідея: «інтелектуальне шпигунство» як форма асиметричного балансу у глобальній конкуренції знань.

Тип гри: динамічна повторювана гра з неповною інформацією та елементами кооперації й шпигунства. Кожен гравець має обмежені ресурси, але неповне знання про стан технологічного прогресу суперника. Шпигунство функціонує як механізм зменшення інформаційної асиметрії, а водночас – як інструмент стратегічного обману.

Сюжет і динаміка гри. Дві провідні держави (А і Б) змагаються у створенні проривної технології (наприклад, квантового комп'ютера або системи штучного інтелекту, здатної до стратегічного передбачення). Обидві держави прагнуть: а) досягти технологічного прориву першими; б) забезпечити контроль над глобальними інформаційними потоками; в) запобігти витоку власних інновацій. Для цього вони діють у двох режимах: 1) Відкрита інноваційна фаза (Innovation Phase): держави інвестують у дослідження, формують партнерства з корпораціями, університетами, технологічними хабами. Відкрита взаємодія підвищує легітимність, але водночас створює ризики витоку через спільні проєкти. 2) Тіньова шпигунська фаза (Espionage Phase): обидві сторони здійснюють приховані операції: а) вербують науковців або аналітиків супротивника; б) впроваджують «вбудовані вразливості» (backdoors) у цифрові системи; в) симулюють витоки, щоб дезінформувати суперника; г) використовують штучний інтелект для аналізу поведінкових патернів у наукових базах. Динаміка гри полягає у взаємному відстеженні і віддзеркаленні стратегій: кожен крок однієї сторони (новий прорив, захист, або шпигунська атака) змінює рівень невизначеності іншої. Гра повторюється нескінченно, оскільки технологічна перевага завжди тимчасова. Завдяки неповній інформації

жоден гравець не знає точно, чи успіх опонента є результатом інновації, чи викрадення даних що створює стан постійної стратегічної параної.

Політологічне значення. У «Quantum Race» шпигунство постає не як порушення правил, а як інституціоналізований механізм балансу сил у цифрову епоху. Технологічне шпигунство замінює традиційні форми військової розвідки, стаючи частиною інформаційного реалізму – парадигми, де контроль над даними дорівнює контролю над владою. З політологічної точки зору, ця гра ілюструє: а) перехід від силового до когнітивного детеренту[1], коли загроза розкриття даних стає потужнішою за ядерну зброю; б) трансформацію шпигуна у технологічного актора, який діє не через фізичну присутність, а через мережу, код, або штучний інтелект; б) гібридизацію безпеки, де шпигунство, хакерство і наукові дослідження зливаються в єдиний простір політичної боротьби. У цьому сенсі «Quantum Race» є моделлю глобальної конкуренції знань, у якій шпигунство – не лише засіб досягнення мети, а форма політичної комунікації між державами, що сигналізує про рівень технологічної зрілості, стратегічну спроможність і готовність до ризику.

Концептуальний підсумок. У концептуальному вимірі «Гра технологічної гонки» демонструє, що шпигунство стало новою мовою міжнародної політики. Якщо у XX столітті шпигунство символізувало приховані конфлікти між ворогуючими блоками, то у XXI столітті – це символ гібридного контролю над знанням. Концептуально гра виявляє антиномію сучасності: прагнення до інновацій неминуче породжує прагнення до приховання. Саме тому квантова епоха – це не стільки доба прогресу, скільки доба нової невидимої війни, де шпигун – центральна фігура політичного театру майбутнього. Технологічне шпигунство в «Quantum Race» – не маргінальний інструмент, а система саморегуляції глобального порядку, що утримує рівновагу між прозорістю й секретністю, знанням і владою.

8. «Гра третього гравця» (The Third Actor Game)

- Тип гри: багатостороння гра (3+ учасники) з коаліційною динамікою.
- Гравці: дві великі держави + посередницька держава, що маніпулює обома.

[1] **Когнітивний детерент** – здатність стримувати опонента не через фізичну загрозу (катастрофічну силу зброї), а через маніпулювання його інформаційним/пізнавальним простором: знаннями, переконаннями, мотиваціями, сприйняттям ризику та поведінкою його еліт і мас. Тобто замість «якщо ви зробите X – ми зруйнуємо вас», формула стає «якщо ми розкриємо / поширимо Y – ваші ключові політичні, економічні або соціальні підвалини зруйнуються».

- Сюжет: посередник одночасно передає і фільтрує інформацію, граючи роль “контролера знань”.
- Ідея: шпигунство як механізм збереження рівноваги між силами – «інформаційна нейтральність».

Тип гри: Трикутна стратегічна гра з неповною інформацією і подвійною лояльністю. Кожен учасник має власні інтереси, але один із них (третій актор) – гібридний, тобто діє одночасно в інтересах і проти обох сторін. Гра містить елементи морального ризику, інформаційної асиметрії та непрямої дії.

Сюжет і динаміка гри. Дві держави (А і Б) перебувають у стані напруженої конкуренції (політичної, військової чи технологічної). У гру вступає третій актор (В) – формально нейтральний гравець, який пропонує посередництво, інформаційні послуги або технологічну підтримку. Однак цей актор водночас: а) збирає дані від обох сторін; б) продає або передає інформацію іншій стороні; в) створює ілюзію нейтралітету, щоб збільшити власний вплив. Розгортається гра симуляції довіри: 1) держава А прагне використати третього актора як канал для шпигунського проникнення в структури Б; б) держава Б бачить у ньому потенційного союзника або джерело даних про А; в) сам актор В грає подвійну гру, акумулюючи вигоду (економічну, політичну, технологічну) за рахунок маніпулювання рівнем прозорості та доступу. Ця гра має динамічний і нелінійний характер: дії В змінюють рівень довіри між А і Б, а відтак баланс усієї системи. Водночас третій актор не завжди є державою: це може бути приватна корпорація, розвідувальна мережа, медіахолдинг або наднаціональна структура, що контролює інформаційні потоки. Завдяки цьому «гра третього гравця» моделює ситуацію, коли шпигунство стає багаторівневим процесом – не лише між державами, а й через посередників, які створюють ілюзію об’єктивності.

Політологічне значення. «Гра третього гравця» ілюструє сучасну трансформацію шпигунства у добу глобалізації та цифрової дипломатії, коли інформаційна перевага досягається не через безпосереднє протистояння, а через контроль каналів посередництва.У цій моделі нейтралітет стає ресурсом влади: здатністю маніпулювати інформаційними потоками між ворогуючими сторонами. Вона відображає феномен нової міжнародної архітектури, де приватні актори, корпорації чи наддержавні структури фактично набувають функцій розвідки й контррозвідки. У геополітичному сенсі ця гра демонструє, що реальна сила дедалі частіше належить не учасникам конфлікту, а тим, хто «контролює поле» (технології, комунікаційні платформи, або канали інформації). Політологічно,

«гра третього гравця» змінює класичну модель шпигунства: від вертикальної (держава – держава) до мережевої (держава – корпорація – суспільство). Це відкриває новий вимір – інституціалізацію шпигунства у формах міжнародних партнерств, дослідницьких обмінів і дипломатичних платформ, де сама структура довіри стає засобом впливу.

Концептуальний підсумок. «Гра третього гравця» показує, що в сучасній системі міжнародної безпеки непрямий контроль над інформаційними каналами може бути потужнішим, ніж пряме шпигунство. Третій актор функціонує як архітектор інформаційного середовища, який створює умови для того, щоб інші гравці приймали вигідні для нього рішення. У термінах теорії ігор це ситуація змішаної рівноваги Бейєса-Неша, де жоден учасник не володіє повною інформацією, а стратегія кожного залежить від припущень щодо прихованих намірів інших. У політологічному сенсі ця модель ілюструє нову фазу еволюції шпигунства: не як індивідуального злочину чи операції, а як системного механізму балансування влади, у якому посередники стають ключовими гравцями глобальної політики. «Гра третього гравця» показує, що у XXI столітті шпигунство дедалі більше нагадує не дуель, а оркестровану симфонію взаємних маніпуляцій, де виграє не той, хто має найсильнішу армію, а той, хто найкраще розуміє структуру довіри.

9. «Гра на випередження» (The Anticipation Game)

- Тип гри: послідовна гра з прогнозуванням дій супротивника (forward induction).
- Гравці: держава і розвідувальна служба супротивника.
- Сюжет: розвідка створює ілюзію власної слабкості, щоб спровокувати передчасну дію іншої сторони.
- Ідея: шпигунство тут – не лише збір інформації, а створення сценаріїв поведінки ворога.
- Політологічна інтерпретація: гра на когнітивному полі – маніпуляція передбаченням.

Тип гри: послідовна гра з неповною інформацією та елементами прогнозування стратегій супротивника. Це гра передбачення і контрдії, у якій виграє той, хто здатен точніше змоделювати наступний крок опонента на основі неповних даних. Шпигунство виступає тут як інструмент зниження стратегічної невизначеності через добування або фальсифікацію інформації.

Сюжет і динаміка гри:

Дві держави (А і Б) – ведуть приховане суперництво у сфері безпеки (військовій, технологічній або політичній). Кожна з них прагне передбачити дії іншої сторони: мобілізацію військ, розгортання шпигунської мережі, зміну політичного курсу або технологічного прориву. У цій грі: а) держава А намагається завчасно виявити шпигунські дії Б, інвестуючи у розвідку, аналітику великих даних, штучний інтелект, психологічний профайлінг і поведінкове прогнозування; б) держава Б намагається створити ілюзію передбачуваності, водночас приховуючи справжні цілі – використовуючи «інформаційні відлуння» (false echoes), фейкові витоки або симуляцію активності. Кожен хід у грі – це боротьба за темп і ініціативу. Якщо А передбачає крок Б, вона може його нейтралізувати або використати як пастку. Якщо ж Б передбачає передбачення А – гра переходить у метарівень (гра передбачення передбачення), де головним ресурсом стає часова перевага. Шпигунство тут діє як когнітивна зброя: воно дозволяє моделювати мислення супротивника, формувати у нього неправильні очікування та створювати ситуації стратегічного випередження. Динаміка гри набуває рефлексивного характеру: гравці не лише діють, а й моделюють, як їхні дії будуть інтерпретовані іншими.

Політологічне значення. «Гра на випередження» демонструє когнітивний вимір шпигунства – перехід від збору інформації до управління сприйняттям. У сучасній політиці перемогу визначає не лише сила даних, а й здатність інтерпретувати сигнали і діяти швидше, ніж інший здогадається про твої наміри. Ця модель пояснює феномен «превентивної розвідки» у міжнародних відносинах, коли головна мета не оборона чи напад, а створення стратегічного випередження у знанні. Політологічно гра показує, що шпигунство перестає бути лише кримінальним актом чи політичною операцією. Воно стає інструментом когнітивного управління, який формує рамки прийняття рішень опонента ще до того, як ті рішення прийнято. У цьому сенсі «гра на випередження» це не лише боротьба за інформацію, а боротьба за структуру часу у політиці, за можливість діяти першим, коли інший ще мислить. У ширшому контексті ця модель відображає еволюцію сучасної безпеки від силової до когнітивної парадигми, де перемагає не той, хто має більше ресурсів, а той, хто швидше мислить, точніше прогнозує та вміє симулювати свої наміри.

Концептуальний підсумок. «Гра на випередження» розкриває шпигунство як метаінтелектуальну гру, де стратегічна перевага формується через керування інформаційним циклом: передбачення → дезорієнтація → адаптація →

нейтралізація. У термінах теорії ігор, це гра з послідовними ходами та неповною інформацією, де рівновага досягається не у стабільності, а в динамічному балансі адаптивних стратегій. Політологічно ця гра показує, що національна безпека у XXI столітті – це безпека передбачення, тобто здатність не лише реагувати, а й випереджати. Держави, які володіють технологіями аналітики даних, нейромережевого прогнозування, когнітивного моделювання й симуляції, фактично створюють нову форму стратегічної зброї – «зброю знання». «Гра на випередження» завершує цикл шпигунських моделей як перехід від фізичного шпигунства до когнітивного домінування, де головним полем битви стає людський розум, а головним ресурсом – час.

Студенти мають знати, що застосування теорії ігор дозволяє моделювати шпигунство не як суто морально-етичний або кримінальний феномен, а як стратегічну взаємодію у сфері національної та міжнародної безпеки. Ігрові сценарії, включно з «Грою подвійного агента», «Пасткою довіри», «Кібер-шпигуном і цифровою пасткою», «Грою дзеркала», «Грою розкриття» та «Грою фальшивого сигналу», демонструють ключові закономірності:

1. **Асиметрія інформації та стратегічна недовіра**. Усі моделі підкреслюють, що держави і агенти діють за умов неповної інформації, де довіра стає стратегічним ресурсом, а не моральною категорією. Подвійний агент або шпигун у «Грі подвійного агента» ілюструє, що взаємодія будується на оцінці ймовірності лояльності і ризику викриття, що оптимізується через рівновагу Бейєса-Неша.
2. **Дилема довіри і ризику**. «Пастка довіри» показує, що навіть у союзницьких системах колективної безпеки надмірна довіра створює вразливості, а надмірна недовіра руйнує потенційні вигоди від співпраці. Теорія ігор дозволяє формалізувати баланс між короткостроковою спокусою зради і довгостроковими втратами через руйнування репутації.
3. **Цифрові та інформаційні виміри**. Сценарії «Кібер-шпигун і цифрова пастка» та «Гра розкриття» демонструють, що сучасне шпигунство виходить за межі фізичних дій і територіального контролю. Контроль інформаційних потоків, управління витоками та цифровий захист стають ключовими ресурсами для досягнення стратегічної переваги.
4. **Адаптивність та повторюваність стратегій**. «Гра дзеркала» ілюструє механізм повторюваної взаємодії, де держави й агенти постійно наслідують та адаптують стратегії один одного, створюючи самоорганізовану систему контролю ризиків і прогнозування дій опонента.

5. **Стратегічний обман та дезінформація**. «Гра фальшивого сигналу» демонструє, що шпигунство здатне формувати політичні наративи, впливати на міжнародну легітимність і баланс сил. Стратегічний блеф стає інструментом управління ризиком, де інформаційний контроль і маніпуляції визначають ефективність державних стратегій без прямого застосування сили.

Відтак теорія ігор надає потужний аналітичний каркас для розуміння шпигунства як системного та багаторівневого інструменту державної безпеки, який функціонує у складних політичних, соціальних та технологічних умовах. Центральними параметрами в такому аналізі виступають інформаційна асиметрія між державними акторами та агентами, довіра як стратегічний ресурс, повторювана взаємодія між суб'єктами, а також баланс ризиків і потенційних вигод для кожного учасника. Теоретичне моделювання шпигунства дозволяє формалізувати стратегічні рішення та передбачати поведінку як держав, так і окремих агентів у різних сценаріях, включно з конфліктними, кооперативними та змішаними умовами.

Крім того, застосування ігрових моделей сприяє оцінці ефективності різноманітних стратегій захисту та контролю інформаційних потоків, дозволяє інтегрувати традиційні методи контррозвідки з новітніми цифровими технологіями, включаючи кіберрозвідку, аналіз великих даних та алгоритми штучного інтелекту. Такий підхід дає змогу розглядати шпигунство не лише як окрему діяльність агентів, але і як комплексну взаємодію елементів національної безпеки, де кожне рішення визначається як короткостроковими тактичними вигодами, так і довгостроковими стратегічними наслідками.

Моделі, побудовані на основі теорії ігор, також дозволяють враховувати динамічні зміни у зовнішньому середовищі, включно зі змінами у міжнародній політиці, технологічних можливостях та соціально-психологічних параметрах агентів. Це робить можливим формування адаптивних стратегій шпигунства та контршпигунства, здатних ефективно реагувати на непередбачувані події, кризові ситуації та технологічні інновації. Завдяки цьому теорія ігор стає не лише інструментом опису і прогнозування, а й механізмом оптимізації комплексної системи державної безпеки, де інформація, довіра, ризики та стратегічні вигоди взаємопов'язані у складній динамічній мережі.

***

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК ДЛЯ РОБОТИ ПІД ЧАС СЕМІНАРСЬКИХ ЗАНЯТЬ

1. **Теорія ігор (Game Theory)** – аналітична рамка для моделювання стратегічної взаємодії між раціональними акторами з неповною інформацією.
2. **Гравець (Player)** – актор (держава, агент, корпорація), який приймає стратегічні рішення в ігровій моделі.
3. **Стратегія (Strategy)** – план дій гравця, спрямований на максимізацію вигоди у конкретній ігровій ситуації.
4. **Виплата (Payoff)** – результат або вигода гравця залежно від обраних ним стратегій та стратегій інших гравців.
5. **Неповна інформація (Incomplete Information)** – ситуація, коли гравець не має повних знань про наміри, ресурси чи дії інших учасників.
6. **Асиметрія інформації (Information Asymmetry)** – нерівномірний розподіл інформації між гравцями, що впливає на їхні рішення.
7. **Hidden Actions (Приховані дії)** – дії гравця, невидимі або неочевидні для інших учасників гри.
8. **Гра довіри (Trust Game)** – модель, де взаємна довіра гравців визначає ефективність співпраці та ризики зради.
9. **Сигнальна гра (Signaling Game)** – гра, у якій один гравець передає сигнали, а інший інтерпретує їх для прийняття рішень.
10. **Дилема безпеки (Security Dilemma)** – ситуація, коли дії одного актора для власної безпеки створюють загрозу для іншого.
11. **Рівновага Неша (Nash Equilibrium)** – стан гри, у якому жоден гравець не може покращити свій результат без погіршення результату іншого.
12. **Дезінформація (Deception)** – цілеспрямоване передання неправдивих сигналів або відомостей для введення супротивника в оману.
13. **Контррозвідка (Counterintelligence)** – заходи з виявлення та нейтралізації шпигунської діяльності противника.
14. **Пастка довіри (Trust Trap)** – ситуація, коли стратегічна довіра перетворюється на слабкість і стає інструментом маніпуляції.
15. **Подвійний агент (Double Agent)** – шпигун, який працює одночасно на дві сторони і використовує інформацію для власної вигоди.
16. **Рівновага Бейєса-Неша (Bayesian Nash Equilibrium)** – розширення рівноваги Неша для ігор з неповною інформацією, де гравці оновлюють очікування на основі ймовірностей.

17. **Інформаційний витік (Information Leak / Leak Game)** – несанкціоноване розкриття секретної інформації, що може впливати на політичні та стратегічні процеси.
18. **Блеф (Bluff)** – стратегічна дія, спрямована на створення хибного враження щодо намірів або ресурсів.
19. **Кібершпигунство (Cyber Espionage)** – шпигунська діяльність у цифровому просторі з метою отримання стратегічних даних.
20. **Цифрова пастка (Cyber Dilemma)** – стратегічна ситуація в інформаційних системах, де захист і атака взаємопов'язані та несуть ризики.
21. **Дзеркальна гра (Mirror Game)** – симетрична стратегія, коли дії одного гравця повторюються або адаптуються іншою стороною.
22. **Стратегічне наслідування (Strategic Imitation)** – механізм адаптації дій гравця на основі спостережень за опонентом.
23. **Повторювана гра (Iterated Game)** – гра, яка повторюється багаторазово, що дозволяє формувати довгострокові стратегії та ефект репутації.
24. **Асиметричні ризики (Asymmetric Risks)** – нерівномірний розподіл потенційних загроз та втрат між гравцями.
25. **Гра з нульовою сумою (Zero-Sum Game)** – ситуація, де виграш одного гравця дорівнює втраті іншого.
26. **Гра сигналів і фальсифікацій (Signaling and Deception Game)** – стратегія, що поєднує передачу сигналів і дезінформацію для досягнення переваги.
27. **Фальшивий сигнал / False Flag** – створення неправдивого сигналу або події для введення опонента в оману та політичного маніпулювання.
28. **Стратегічна недовіра (Strategic Distrust)** – усвідомлене обмеження довіри до іншого гравця через ризики обману.
29. **Інформаційний ресурс (Information as Resource)** – дані, які можуть бути використані для отримання стратегичної або політичної вигоди.
30. **Гібридна гра (Hybrid Game)** – складна стратегічна взаємодія, яка поєднує традиційні та цифрові, відкриті й приховані дії гравців.

***

ПІДСУМКОВЕ ТЕСТУВАННЯ

1. Що є основним завданням шпигунства?
а) Проведення соціологічних опитувань
б) Збір секретної інформації
в) Організація виборів
г) Надання гуманітарної допомоги

2. Який процес характеризує шпигунство як інститут?
а) Політичні консультації
б) Збір та аналіз таємної інформації
в) Законодавча діяльність
г) Громадське обговорення

3. Коли почало формуватися сучасне шпигунство?
а) XVII–XVIII ст.
б) XIX ст.
в) XX – початок XXI ст.
г) XXI ст.

4. Який вид шпигунства характерний для авторитарних режимів?
а) Політичне
б) Економічне
в) Наукове
г) Волонтерське

5. Що відрізняє державне шпигунство від приватного?
а) Відсутність мети
б) Дія у правовому полі і національних інтересах
в) Виключно міжнародний масштаб
г) Немає відмінностей

6. Який з цих суб’єктів шпигунства існує в Україні?
а) Тільки приватні агенції
б) Державні розвідувальні органи

в) Міжнародні громадські організації
г) Політичні партії

7. Яка загроза шпигунства найбільше стосується України та НАТО?
а) Поширення культурних впливів
б) Витік стратегічної таємної інформації
в) Надання гуманітарної допомоги
г) Туристична діяльність

8. Який сучасний інструмент протидії шпигунству використовується США та Великобританією?
а) Кіберзахист
б) Туристичні патрулі
в) Міжнародні конференції з культури
г) Лобіювання бізнес-інтересів

9. Яка функція шпигунства не є основною?
а) Збір політичної інформації
б) Контррозвідка
в) Вплив на економічні процеси
г) Надання освітніх послуг

10. Який історичний фактор вплинув на розвиток сучасного шпигунства?
а) Розвиток кібертехнологій
б) Зменшення урядового контролю
в) Поширення малих релігій
г) Культурні фестивалі

11. Що з перерахованого є прикладом приватного шпигунства?
а) СБУ
б) Комерційна розвідка
в) Міністерство оборони
г) Місцеві органи влади

12. Хто є ключовим суб’єктом шпигунства у демократичних країнах?
а) Громадські організації

б) Державні розвідувальні служби
в) Приватні волонтерські групи
г) Політичні опозиційні партії

13. Який тип шпигунства характерний для тоталітарних режимів?
а) Соціальне
б) Політичне
в) Волонтерське
г) Гуманітарне

14. Як цифровізація вплинула на шпигунство?
а) Зменшила його значення
б) Поширила нові форми кібершпигунства
в) Виключила державне шпигунство
г) Перетворила його на культурне явище

15. Яка основна мета контррозвідки?
а) Просування культурних проєктів
б) Виявлення та нейтралізація шпигунських загроз
в) Залучення інвестицій
г) Організація міжнародних конференцій

16. Що є характерним для історичного розвитку шпигунства?
а) Це явище виникло виключно у XXI ст.
б) Еволюція від класичної розвідки до сучасного цифрового шпигунства
в) Завжди було легальним
г) Не мало впливу на політику

17. Що не відноситься до функцій шпигунства?
а) Вплив на прийняття політичних рішень
б) Контррозвідка
в) Збір економічної інформації
г) Розробка шкільних програм

18. Який метод протидії шпигунству застосовується у США?
а) Введення воєнного стану

б) Кібербезпека та моніторинг
в) Заборона приватних компаній
г) Туристичні перевірки

19. Який аспект шпигунства є ключовим у міжнародній політиці?
а) Туризм
б) Збір стратегічної інформації
в) Культурні обміни
г) Екологічні програми

20. Який етап розвитку шпигунства відповідає XX ст.?
а) Початкова класична розвідка
б) Масштабне застосування в двох світових війнах
в) Локальні комерційні операції
г) Виключно кібершпигунство

21. Який тип шпигунства найбільш характерний для демократій?
а) Контррозвідка і економічне
б) Політичне та тоталітарне
в) Релігійне
г) Волонтерське

22. Який фактор найбільше впливає на сучасну загрозу шпигунства в Україні?
а) Економічна нестабільність
б) Кіберзагрози та зовнішні розвідувальні служби
в) Туристичні потоки
г) Мовне різноманіття

23. Що характеризує сучасне приватне шпигунство?
а) Дія виключно у межах держави
б) Комерційні цілі та економічна розвідка
в) Вплив на закони
г) Контроль за армією

24. Який інструмент протидії шпигунству застосовує Велика Британія?
а) Локальні культурні фестивалі

б) Превентивна контррозвідка
в) Масові виборчі кампанії
г) Волонтерські мережі

25. Що є особливістю суб’єктів шпигунства в Україні?
а) Відсутність державних структур
б) Поєднання державних органів та приватних агентств
в) Всі дії незаконні
г) Тільки міжнародні організації

***

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

1. Дайте визначення шпигунства як явища, охарактеризуйте його сутність та особливості.
2. Визначте основних учасників шпигунської діяльності: виконавців і адресатів, з конкретними прикладами.
3. Опишіть категоріальний апарат шпигунства: об’єкт, предмет, методи та види діяльності.
4. Проаналізуйте сучасні підходи до визначення шпигунства у зарубіжній літературі.
5. Дослідіть історичні приклади шпигунства в Україні та світі, визначте уроки для сучасності.
6. Проаналізуйте процес збору та передачі відомостей, що становлять державну таємницю, із точки зору виконавця та адресата.
7. Створіть схему процесу шпигунської діяльності з усіма етапами: від збору інформації до її передачі.
8. Вивчіть українське законодавство щодо шпигунства, визначте основні норми та санкції.
9. Порівняйте законодавство України з законодавством двох інших держав щодо протидії шпигунству.
10. Визначте правові механізми контролю за доступом до державної таємниці.
11. Дослідіть методи запобігання шпигунству, які застосовують спеціальні служби України.
12. Вивчіть досвід зарубіжних спецслужб у сфері протидії шпигунству та адаптуйте до українських умов.
13. Проаналізуйте політико-правові оцінки шпигунства та вплив міжнародних стандартів на національну практику.
14. Дослідіть роль міжнародної співпраці у протидії шпигунству та обміні інформацією між державами.
15. Проведіть аналіз сучасних технологій збору інформації (кібершпигунство, соціальні мережі, цифрові комунікації).
16. Оцініть вплив сучасних технологій на методи та ефективність шпигунської діяльності.
17. Розробіть карту потенційних загроз національній безпеці з огляду на шпигунські ризики.
18. Створіть декілька сценаріїв розвитку шпигунських ситуацій, оцініть ймовірність їх реалізації.

19. Змоделюйте можливі дії держав та агентів у ситуаціях шпигунства, використовуючи елементи теорії ігор.
20. Визначте ключові фактори ризику при передачі інформації іноземним державам чи організаціям.
21. Проаналізуйте ефективність існуючих заходів безпеки у запобіганні шпигунству.
22. Розробіть рекомендації щодо вдосконалення системи захисту державної таємниці в Україні.
23. Підготуйте аналітичний звіт про потенційний негативний вплив дій іноземних розвідок на національну безпеку.
24. Вивчіть діяльність міжнародних організацій, спрямовану на контроль і протидію шпигунству.
25. Підготуйте презентацію або доповідь на тему «Шпигунство як сучасний інструмент державної безпеки», із прикладами з України та світу.

***

ПРАКТИЧНІ ЗАВДАННЯ У ФОРМАТІ КЕЙСІВ І СЦЕНАРІЇВ

1. **Виявлення агента**: Проаналізуйте поведінку співробітника державного підприємства, який має доступ до секретних даних і часто спілкується з іноземними партнерами. Складіть карту ризиків.
2. **Кіберзбір даних**: Розгляньте кейс витоку документів через корпоративну мережу. Визначте слабкі місця та запропонуйте заходи захисту.
3. **Міжнародна співпраця**: Дослідіть приклад обміну інформацією між спецслужбами двох держав НАТО. Оцініть ризики та вигоди для України у разі участі у подібних операціях.
4. **Сценарій подвійного агента**: Складіть профіль співробітника, який працює на дві сторони, і змоделюйте потенційні наслідки для державної безпеки.
5. **Фейкові документи**: Проаналізуйте випадок передачі підробленої інформації іноземній розвідці. Визначте методи перевірки достовірності даних.
6. **Аналіз витоку даних у дипломатичних колах**: Виявлено витік через дипломатичні канали. Розробіть план розслідування та протидії.
7. **Оцінка загроз національній безпеці**: На основі нових міжнародних подій складіть карту загроз для України, пов’язаних із шпигунством.
8. **Моделювання поведінки іноземної розвідки**: Змоделюйте дії іноземної розвідки при спробі отримати інформацію про військові навчання України.
9. **Виявлення аномалій**: На підприємстві з державною таємницею зафіксовано незвичну активність у системі доступу. Проаналізуйте ситуацію та запропонуйте заходи.
10. **Соціальна інженерія**: Розгляньте кейс спроби отримати секретну інформацію через психологічний вплив на працівників. Розробіть протидію.
11. **Іноземна організація**: Визначте, як потенційно легальні міжнародні організації можуть збирати дані, і складіть алгоритм оцінки ризику.
12. **Цифрове шпигунство**: Вивчіть випадок крадіжки секретної інформації через мобільні пристрої. Складіть рекомендації щодо цифрової гігієни.
13. **Виявлення витоку у фінансових звітах**: Змоделюйте ситуацію, коли інформація про оборонні закупівлі потрапила до іноземного агентства через бухгалтерію.

14. **Використання теорії ігор**: Складіть стратегічну матрицю дій для українських спецслужб та іноземних агентів у кейсі збору секретних даних.
15. **Протидія шпигунству у відкритих джерелах**: Проаналізуйте інформацію, доступну в медіа та соцмережах, яка може бути використана для шпигунства.
16. **Сценарій кібератаки**: Змоделюйте спробу злому серверів Міністерства оборони. Визначте слабкі місця та запропонуйте протидію.
17. **Захист від внутрішнього витоку**: Складіть план заходів для підприємства з державною таємницею, щоб мінімізувати ризики від внутрішніх співробітників.
18. **Міжнародний кейс**: Проаналізуйте іноземний прецедент шпигунства, адаптуйте уроки до українських умов.
19. **Фінансові стимули та ризики**: Вивчіть випадок, коли агент був завербований через фінансові мотиви. Складіть модель запобігання.
20. **Витік у науковій сфері**: Розгляньте кейс передачі технологій за кордон. Оцініть шкоду та запропонуйте заходи контролю.
21. **Розслідування через аналітику**: Використайте відкриті джерела та аналітичні методи для виявлення потенційного шпигуна.
22. **Розробка навчального сценарію**: Створіть інтерактивний сценарій для тренування співробітників спецслужб у протидії шпигунству.
23. **Оцінка ризику нових технологій**: Дослідіть вплив штучного інтелекту та Big Data на методи шпигунства.
24. **План реагування на шпигунську операцію**: Розробіть покроковий план дій у разі виявлення шпигунської активності в державних органах.
25. **Підготовка аналітичної доповіді**: На основі змодельованого кейсу підготуйте звіт для керівництва, що включає оцінку загроз, ймовірні сценарії та заходи протидії.

***

ПРОБЛЕМАТИКА ПРОФІЛЮВАННЯ ШПИГУНСТВА

Профілювання шпигунства є складним міждисциплінарним інструментом сучасної безпеки, що поєднує військову, політичну, психологічну та соціологічну аналітику для системного розуміння різновидів шпигунської діяльності та розробки ефективних контрзаходів. Мета профілювання полягає не лише у встановленні особистісних характеристик конкретного агента, а й у діагностиці ймовірних операційних патернів, прогнозуванні можливих дій і виявленні структурних вразливостей організації чи системи, в якій агент діяв або може діяти. У процесі профілювання аналітик поєднує кількісні й якісні дані: показники доступу та активності, часові й просторові кореляції подій, свідчення колег і контекстні політичні фактори; цей синтез дозволяє відрізнити поодинокі інциденти від системних витоків та формувати сценарії реагування, які мінімізують ризики для національної безпеки та одночасно зберігають етичні стандарти.

Різновиди шпигунства відрізняються за предметом зацікавлення, каналами доступу й мотивами, отже й профілі, які їх описують, повинні враховувати ці відмінності. У випадках, коли йдеться про отримання військових відомостей, ключовими є індикатори оперативного доступу: служба в збройних силах або у структурах логістики, систематичні запити до карт тактичного розгортання, регулярні відвідини об’єктів підвищеної секретності та використання технічних засобів для збору сигналів. Для осіб, які працюють на промисловий або науково-технічний шпигунський збір, характерною є надмірна зацікавленість до документації, неформальні контакти з підрядниками і постачальниками, а також поведінка, що видає спроби ексфільтрації даних поза межами офіційних каналів. Комерційне та економічне шпигунство частіше має інші маркери: доступ до фінансових звітів, зв’язки з зовнішніми консультантами і нетипові операції з юридичними або контрактними документами. Кібер-шпигунство, яке дедалі частіше поєднується з інсайдерськими акціями, проявляється через аномалії в мережевому трафіку, незвичні патерни логінів і використання бекдорів або підозрілих шифрованих каналів; його профілювання орієнтоване на розпізнавання тактик, технік і процедур (TTP) конкретних кібер-акторів, а також на відстеження слідів exfiltration через зовнішні сервіси чи пристрої.

Мотивації агентів варіюються від ідеологічних переконань і патріотичних прагнень до матеріальних стимулів, шантажу чи особистих мотивів помсти, що накладає відбиток на їхню стійкість та схеми поведінки. Ідеологічно мотивований

агент часто демонструє високу готовність до ризику та стійкість перед викриттям, але може бути передбачуваним у своїх операційних цілях; матеріально мотивований суб'єкт зазвичай більш чутливий до фінансових стимулів і може бути вразливим до корекцій кадрової політики або до правових наслідків. Подвійні агенти та «спеціалізовані» фігури, зокрема науковці і технічні фахівці, які володіють унікальними знаннями, утворюють особливий виклик для профілювання через їхню здатність замаскувати інформаційні потоки та використовувати професійні мережі як прикриття. Саме тому профілювання має включати оцінку психологічних рис: рівня стресостійкості, здатності до маніпуляцій, схильності до подвійного життя і когнітивних стратегій ухвалення рішень, що разом дозволяє прогнозувати ймовірні реакції агента на контрзаходи.

Методи, якими шпигуни здобувають інформацію, поєднують людський фактор із технічними й організаційними інструментами. Соціальна інженерія і підкуп залишаються універсальними підходами для отримання доступу до секретів у будь-якій сфері; паралельно з цим розвиваються техніки кібер-експлуатації, supply-chain атак і використання персональних пристроїв працівників. У промисловому контексті часто спрацьовує поєднання інсайдерського доступу і зовнішніх посередників, у військовому – поєднання доступу через службі та логістичних ланцюгів, у бізнес-сфері – зловживання процесами юридичного супроводу чи фінансових угод, а в кіберсередовищі ключове значення мають своєчасність патчів, сегментація мережі та політики багатофакторної автентифікації. Профілювання має фіксувати не лише виявлені індикатори, але й їхню взаємодію: наприклад, поєднання нетипових мережевих з'єднань з підозрілою поведінкою співробітника уночі сильніше за одиничний індикатор вказує на потенційну загрозу.

Вразливості, які виявляє профілювання, стосуються як людського фактора, так і технічних і процедурних недоліків. Неправильно налаштовані права доступу, відсутність політики «найменшого привілею», слабкі практики BYOD[2],

[2] **Практика BYOD** (Bring Your Own Device, «принось власний пристрій») полягає в тому, що співробітники компанії або організації використовують для робочих цілей особисті електронні пристрої: смартфони, планшети, ноутбуки, іноді навіть носимі гаджети замість або паралельно з корпоративною технікою. Основна ідея BYOD полягає у підвищенні зручності та гнучкості роботи: працівник користується пристроєм, з яким він добре знайомий, що може підвищити продуктивність і швидкість виконання завдань. Переваги BYOD: а) скорочення витрат організації на придбання і обслуговування техніки; б) підвищення гнучкості та мобільності працівників; в) зручність і комфорт роботи для співробітника. Ризики BYOD для безпеки: а) підвищений ризик витоку конфіденційної інформації, оскільки особисті пристрої менш контрольовані; б) можливість проникнення шкідливого програмного забезпечення через особисті пристрої; в) втрата даних при крадіжці або втраті пристрою; г) складність забезпечення

недостатній аудит третьо-сторонніх підрядників і пропуски у навчанні персоналу з кібергігієни створюють «вікна» для проникнень. Також важливими є соціально-психологічні вразливості: низька лояльність персоналу, високий рівень стресу, нерозкриті фінансові проблеми або особисті конфлікти, які можуть стати точками вербування. Контрзаходи мають бути комплексними: технічні інструменти захисту й моніторингу доповнюються політиками оновлень і сегментації мережі, а також кадровими практиками, що включають скринінг, психологічну підтримку, програми лояльності й чіткі протоколи інформування про підозрілі інциденти.

Етичні та правові аспекти профілювання не менш важливі, ніж технічні й аналітичні. Баланс між забезпеченням національної безпеки та дотриманням прав людини, приватності й довіри в організації є ключовим питанням професійної етики у сфері розвідки й контррозвідки. Використання маніпулятивних або превентивних методів, наприклад шантажу, прихованого спостереження без належних правових підстав чи незаконного втручання в приватні комунікації, може чинити довгострокову шкоду не лише окремим особам, а й довірі всередині системи і міжнародному іміджу держави. Тому профілювання має інтегрувати нормативні рамки та принципи пропорційності: рекомендації аналітика повинні супроводжуватися оцінкою правових підстав і ризиків для цивільних і служби.

У підсумку, профілювання шпигунства слугує містком між теоретичною аналітикою і практичними контрзаходами, забезпечуючи системний підхід до виявлення та нейтралізації загроз різного походження: від військових і промислових витоків до економічного та кібер-шпигунства. Воно вимагає синтезу дисциплін, уважної роботи з даними й чіткого етичного компаса, щоб рекомендації аналітиків були не лише ефективними, а й сумісними з правовими й моральними стандартами суспільства.

Таким чином, підсумуймо:

шифрування, управління паролями та оновлення безпеки. Практичні заходи для зменшення ризиків BYOD: а) встановлення правил використання особистих пристроїв (що дозволено, а що заборонено); б) використання систем мобільного управління (MDM, Mobile Device Management) для віддаленого контролю, шифрування та видалення даних; в) Регулярне навчання працівників щодо кібергігієни та захисту даних; г) вимога встановлення антивірусного ПЗ та оновлень безпеки на всіх особистих пристроях. У контексті профілювання шпигунства BYOD стає особливо важливим, оскільки особистий пристрій співробітника може стати каналом витоку інформації або способом обходу традиційних заходів контролю, що вимагає від контррозвідки та IT-безпеки окремих процедур моніторингу і оцінки ризиків.

1. Поняття профілювання шпигунства

Профілювання шпигунства визначається як системний міждисциплінарний аналіз особистісних, психологічних, соціальних та операційних характеристик агентів розвідки та контррозвідки з метою виявлення закономірностей їхньої поведінки, мотивації, тактики і потенційних вразливостей. Воно включає оцінку особистісних рис, когнітивних стратегій, соціальної інтеграції у мережі та впливу політичних та міжнародних чинників на ефективність шпигунської діяльності. Профілювання шпигунства розглядається як складова сучасної безпекової науки, що поєднує елементи військової, політичної, психологічної та соціологічної аналітики.

2. Функції профілювання шпигунства

Функції профілювання можна поділити на кілька ключових аспектів:

1. Діагностична – визначення осіб, здатних до шпигунської діяльності або вже залучених до неї, з урахуванням їхніх психофізіологічних, соціальних та когнітивних характеристик.
2. Прогностична – оцінка ймовірної поведінки агента, передбачення можливих операційних дій, методів витоку інформації та реакцій на зовнішні стимули.
3. Аналітична – виявлення слабких місць у системі безпеки, створення моделей ризиків, оптимізація контролю над агентами та підвищення ефективності контррозвідувальних заходів.
4. Методологічна та навчальна – розробка інструментів для тренування контррозвідників, навчання аналітичному мисленню та ухваленню рішень у кризових умовах.
5. Етична та нормативна – визначення меж допустимого втручання у приватне життя та діяльність агентів, оцінка наслідків превентивних і маніпулятивних методів.

3. Типологія шпигунів у профілюванні

Типологічний підхід дозволяє класифікувати шпигунів за ключовими критеріями:

- Ідеологічно мотивовані агенти – діють за переконаннями, наприклад, політичні емігранти або активісти; мотивація визначає стійкість і ризикованість поведінки.
- Матеріально мотивовані агенти – зацікавлені у грошових або кар’єрних перевагах; їх поведінка більш передбачувана, але водночас вразлива до фінансових або правових стимулів.

- Подвійні агенти – функціонують на користь кількох розвідок одночасно; вимагають складного аналітичного контролю та моделювання ризиків.
- Спеціалізовані агенти – технічні, наукові або кіберагенти; профілювання орієнтоване на оцінку компетентності та інтеграції у специфічні системи.

Кожна категорія характеризується специфічними психологічними та соціальними патернами, що дозволяє прогнозувати дії агентів, визначати потенційні точки втручання та оптимізувати контрзаходи.

4. Аксіологічні аспекти профілювання шпигунства

Профілювання шпигунства має не лише технічний, але й морально-етичний вимір:

- Баланс між національною безпекою та правами людини, особистою свободою і довірою всередині організацій.
- Превентивні дії та маніпулятивні методи контррозвідки повинні оцінюватися з точки зору етики та міжнародного права.
- Вибір методів розвідки та профілювання часто передбачає моральні дилеми: ризик життів агентів або цивільних, вторгнення у приватне життя, використання психологічного тиску.

Аксіологічний підхід дозволяє формувати стандарти професійної етики в діяльності розвідок і контррозвідок, а також розвивати критичне мислення аналітиків і служб безпеки.

5. Міждисциплінарний контекст і наукові підходи

Профілювання шпигунства інтегрує кілька наукових дисциплін:

- Військова наука – аналіз тактики та стратегії агентурної роботи, оцінка ризиків в умовах конфліктів і криз.
- Політична наука – вплив державної політики, міжнародних відносин і ідеологічних чинників на мотивацію і методи агентів.
- Психологія – дослідження особистісних характеристик, когнітивних стратегій, стресостійкості, здатності до маніпуляцій та подвійного життя.
- Соціологія війни – вивчення структур агентурних мереж, взаємодії з локальними і міжнародними спільнотами, аналіз соціальної інтеграції агентів і впливу війни на їх поведінку.

Поєднання цих дисциплін дозволяє створювати системні моделі шпигунської діяльності, прогнозувати ризики та розробляти ефективні контрзаходи.

6. Практичне значення

Профілювання шпигунства формує основу для:

- підвищення ефективності розвідувальних і контррозвідувальних структур;
- навчання аналітиків і контррозвідників;
- розробки превентивних заходів та стратегій нейтралізації агентів;
- оптимізації взаємодії між національною безпекою, політичними інтересами та етичними стандартами.

Профілювання шпигунства є ключовим елементом національної безпеки, що поєднує аналітичні, психологічні, соціальні та етичні аспекти для системного розуміння поведінки агентів і забезпечення ефективної контррозвідувальної діяльності.

ПРАКТИЧНІ ЗАВДАННЯ У ФОРМАТІ АНАЛІТИЧНОГО ПОРТРЕТУВАННННЯ ШПИГУНІВ/ШПИГУНОК

На підставі попереднього розділу («Проблематика профілювання шпигунства»), основної і допоміжної літератури, відеоматеріалів і самостійного пошуку інформаційних ресурсів підготуйте портретування найвідоміших шпигунів/шпигунок у ХХ ст. за схемою:

1. Біографічний контекст

1.1. Походження, освіта, соціальне середовище.

1.2. Політичні й культурні умови формування особистості.

1.3. Ранні впливи (родина, ідеї, події, війна тощо).

2. Мотивація і світогляд

2.1. Ідейні переконання (політичні, національні, моральні).

2.2. Особисті мотиви вступу до розвідки (ідеологія, кар'єра, помста, романтика, страх, інтимні відносини).

2.3. Образ ворога й образ «своєї» держави у свідомості шпигуна.

3. Оперативна діяльність

3.1. Основні операції, у яких брав/брала участь.

3.2. Методи роботи (легенда, контакти, технології).

3.3. Ключові успіхи та провали, наслідки діяльності.

4. Мережа зв'язків і середовище

4.1. Контакти в політичних, наукових, культурних колах.

4.2.Канали комунікації та прикриття.

4.3. Роль партнерів, кураторів, подвійних агентів.

5. Психологічний і когнітивний портрет

5.1. Тип мислення (аналітичний, інтуїтивний, маніпулятивний).

5.2. Риси характеру: ризикованість, холоднокровність, емпатія чи цинізм.

5.3. Механізми прийняття рішень, реакція на ризик і викриття.

6. Історична, політична оцінка і спадщина

6.1. Як оцінюють його діяльність політики, спецслужби, суспільство.

6.2. Образ у літературі, кіно, публіцистиці.

6. 3. Морально-етична дилема: герой, зрадник/зрадниця чи «гвинтик історії»?

Перелік шпигунів і шпигунок XX ст. для портретування:

1. Глущенко Микола
2. Гордієвський Олег
3. Даґан Меїр
4. Джек Девайн
5. Еймс Олдріч
6. Зорге Ріхард
7. Ізабель Педро
8. Коен Елі
9. Мадлен Ферраль (Рут Бен-Давид)
10. Макогін Яків
11. Мата Харі (спр. Маргарета Геертрейда Зелле)
12. Надін Фрей
13. Петров Віктор
14. Ріко Ярий
15. Сильвія Рафаель
16. Скорцені Отто
17. Толкачов Альфред
18. Філбі Кім
19. Фукс Клаус
20. Юзефський Генрик

Підсумовуючи підготовку цього завдання радимо пам’ятати дві максими:

- рядки з трактату Сунь-дзи «Мистецтво війни»: ***«Існує п’ять шляхів використання шпигунів. Бувають місцеві інформатори, внутрішні вивідачі, обернені або ж перевербовані підосланці, шпиги, які мають померти, і ті, які мусять жити»***[3];
- рядки з трагедії Й.-В. Ґете «Фауст»: ***«Як бачиться, ти ладний шпигувать. […] Хоч не всевіда я, а дещо можуть знать»***[4].

***

[3] Сунь-дзи. *Мистецтво війни*. Пер. С. Лесняк. Львів: ВСЛ, 2016. С. 54.
[4] Йоганн Вольфґанґ фон Ґете. *Фауст. Трагедія*. Пер. з нім. М. Лукаш. Київ: Видавництво Жупанського, 2013. С. 63.

НАВЧАЛЬНО-ЛОГІЧНІ ЗАДАЧ СЕРЕДНЬОГО РІВНЯ СКЛАДНОСТІ

(застосування аналітичного мислення, інтерпретації фактів, морально-етична оцінка)

Британська розвідка (MI6)

1. «Викриття Філбі»

MI6 дізнається, що в радянській пресі з'явилися подробиці кількох секретних операцій, до яких мав доступ обмежене коло осіб. Серед них – керівник аналітичного відділу К. Філбі.

Завдання:

– Які кроки мала б зробити британська контррозвідка, щоб перевірити підозру, не викривши внутрішні джерела?

– Які помилки в реальній історії К. Філбі призвели до втрати довіри до MI6?

(Очікувана відповідь: перевірка комунікаційних каналів, подвійна верифікація джерел, спостереження за колом контактів; недооцінка соціальних зв'язків у Кембриджі — стратегічна помилка.)

2. «Зниклі архіви»

У Лондоні зникає архів колишніх радянських агентів. Частина інформації опиняється в медіа.

Питання:

– Як MI5/MI6 можуть визначити, чи це зовнішній злам, чи «внутрішній витік»?

– Яку роль у таких розслідуваннях відіграє аналітична робота (не силові методи)?

(Очікувана логіка: аналіз шаблонів витоку, відстеження тайм-штампів, звірка внутрішнього доступу – превалювання аналітичних методів над каральними.)

Американська розвідка (CIA)

1. «Справа Олдріча Еймса»

У 1980-х роках радянські служби почали систематично виявляти агентів ЦРУ. Підозри падають на співробітників середнього рівня, але прямих доказів немає.

Завдання:

– Як CIA повинна діяти, щоб не створити атмосферу параної, але й не допустити нових втрат?

– Які методи внутрішньої перевірки можуть бути ефективними без порушення прав персоналу?

(Мета: сформувати розуміння балансу між безпекою та довірою у розвідувальній структурі.)

2. «Подвійний канал»

Агент CIA у Східній Європі отримує інформацію, яка виглядає надто точною: можливо, це дезінформація противника.

Питання:

– Як аналітики CIA мають перевірити достовірність джерела?

– Які наслідки може мати необережне використання сумнівних даних у прийнятті політичних рішень?

(Відповідь: перехресна перевірка через незалежні канали; демонстрація принципу «довіряй, але перевіряй» у антишпигунській практиці.)

Ізраїльська розвідка (Mossad)

1. «Операція з подвійним агентом»

Mossad отримує сигнал, що один із їхніх інформаторів у Сирії може працювати також на іншу розвідку.

Завдання:

– Як ізраїльські аналітики мають встановити справжню лояльність агента?

– Які етичні межі допустимі під час перевірки (шантаж, маніпуляції, дезінформація)?

(Завдання на розуміння моральної дилеми в антишпигунській роботі).

2. «Авіаційна пастка»

Mossad перехоплює повідомлення про підготовку замаху, але не може перевірити джерело без ризику розкрити агентурну мережу.

Питання:

– Як приймається рішення у ситуації неповної інформації?

– Яку модель ухвалення рішення можна застосувати (раціональна, імовірнісна, інтуїтивна)?

(Мета: навчити студентів бачити антишпигунську діяльність як баланс ризику й користі, а не лише як пошук «зрадників».)

***

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ТА ЛІТЕРАТУРА

Нормативно-правові акти

1. Закон України «Про національну безпеку України» https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Закон України «Про розвідку» https://zakon.rada.gov.ua/laws/show/912-20#Text
3. Закон України «Про контррозвідувальну діяльність» https://zakon.rada.gov.ua/laws/show/374-15#Text

Основна література:

1. Бар-Зохар М., Мішаль Н. Амазонки Моссаду. Жінки в ізраїльські розвідці. Пер. з англ. К. Диса. Київ: Наш формат, 2024. 352 с.
2. Берґман Р. Встань і вбий першим. Таємна історія ліквідацій ворогів Ізраїлю. Пер. з англ. М. Марченко. Київ: Наш формат, 2025. 704 с.
3. Гофман Д. Е. Шпигун на мільйон доларів. Справжня історія про шпіонаж, Холодну війну та зраду. Пер. з англ. І. Плясов. Харків: Фабула, 2022. 352 с.
4. Далрімпл В. Анархія. Безжальне піднесення Ост-Індської компанії. Пер. з англ. А. Дейнека. Львів: Видавництво Аннети Антоненко; Київ: Ніка-Центр, 2024. 464 с.
5. Девайн Дж. Призма головного шпигуна. Боротьба з російською агресією. Пер. з англ. Є. і В. Тарнавських. Харків: Фоліо, 2024. 252 с.
6. Дмитренко В. Розвідка та інші таємні служби Стародавнього Риму і його супротивників. Львів: Кальварія, 2020. 704 с. https://chtyvo.org.ua/authors/-Dmytrenko_Volodymyr/Rozvidka_ta_inshi_taiemni_sluzhby_Starodavnoho_Rymu_i_ioho_suprotyvnykiv/
7. Кіссінджер Г. Світовий порядок. Роздуми про характер націй в історичному контексті. Пер. з англ. Н. Коваль. Київ: Наш формат, 2017. 320 с.
8. Колодзінський М. Воєнна доктрина українських націоналістів. Київ: ТОВ «Основа», 2019. 287 с. https://chtyvo.org.ua-/authors/Kolodzinskyi-/Voienna_doktryna_ukrainskykh_natsionalistiv/
9. Макінтайр Б. Шпигун і зрадник. Визначна шпигунська історія часів Холодної війни. Пер. з англ. О. Петришин. Київ: Книголав, 2023. 480 с.
10. Меєр Б. Індустрія розслідування. Як приватні шпигуни впливають на політику. Пер. з англ. О. Тельна. Харків: Фабула, 2023. 264 с.

11. Монолатій І. Друг чи ворог УГКЦ? “Приватний шпигун” Яків Макогін та “церковні справи” 1930–1940-х років. *Історія релігії в Україні.* 2024. Т. 34. С. 239–250. https://religio.org.ua/index.php/religio/article/view/1536
12. Монолатій І. Інформаційні «вкиди» Якова Макогона: Геополітичні міркування приватного шпигуна про повоєнне облаштування світу. *Медіафорум : аналітика, прогнози, інформаційний менеджмент.* 2024. Т. 14. С. 327–344. https://journals.chnu.edu.ua/mediaforum/article/view/597
13. Монолатій І. Макогін псевдо Розумовський. Уявлена українська людина. Івано-Франківськ: Лілея-НВ, 2023. 448 с. https://www.istpravda.com.ua-/reviews/64b6ff5c858ad/view_news/
14. Монолатій І. Специфіка трактування військової розвідки у воєнно-політичній думці української еміграції (середина XX ст.). *Вісник Прикарпатського університету. Політологія.* 2024. Вип. 18. С. 263–272. https://journals.pnu.if.ua/index.php/politology/article/view/162
15. Монолатій І. Дорожня карта української військової розвідки (досвід перших визвольних змагань 1917–1921 рр.). *Вісник Прикарпатського університету. Політологія.* 2025. Вип. 20. С. 107–117. https://journals.pnu.if.ua/index.php/politology/article/view/229
16. Плохій С. Убивство у Мюнхені. По червоному сліду. Пер. з англ. М. Климчук. Харків: Клуб сімейного дозвілля, 2017. 512 с. https://shron1.chtyvo.org.ua/Plokhii_Serhii/Ubyvstvo_u_Miunkheni_Po_chervonomu_slidu.pdf?PHPSESSID=ff71u4rrm0ti6mc06opidsudt1
17. Потєхін О., Клименко Ю. Геополітика проти безпеки. Союзницьке стримування агресії в Європі XX – початку XX ст. Київ: Дух і Літера, 2023. 552 с. https://surl.li/yxlzzf
18. Снайдер Т. Нариси таємної війни. Польський художник на службі визволення України. Пер. з англ. П. Грицака. Київ: ТАО, 2023. 398 с. https://www.istpravda.com.ua/reviews/2023/12/14/163455/
19. Сунь-дзи. Мистецтво війни. Пер. С. Лесняк. Львів: ВСЛ, 2016. 100 с. https://chtyvo.org.ua/authors/Tzu_Sun/Mystetstvo_viiny_vyd_2015/
20. Фіглузі Ф. Система ФБР. Кодекс досконалості наймогутнішого відомства США. Пер. з англ. О. Качала. Київ: Наш формат, 2023. 200 с.

Допоміжна література:

1. Ададуров В. (Не) таємна історія Віктора Петрова. 17 миттєвостей із життя агента радянської держбезпеки. Документальний нарис. Львів: УКУ, 2025. 166 с.
2. Андреєв В. Віктор Петров. Нариси інтелектуальної біографії вченого. Дніпропетровськ: Герда, 2012. 472 с. https://surl.li/cshynp
3. Бар-Зохар М., Мішаль Н. МОССАД. Найвидатніші операції ізраїльської розвідки. Пер. з англ. О. Михельсон. 3-тє вид. Київ: Наш формат, 2023. 384 с.
4. Бовгиря А. «Слово і діло». Політичні злочини та політичний розшук в Гетьманщині XVIII ст. 2-ге вид. Київ: Кліо, 2022. 254 с. https://chtyvo.org.ua/authors/Bovhyria_Andrii/Slovo_i_dilo_Politychni_zlochyny_ta_politychnyi_rozshuk_v_Hetmanschyni_XVIII_st/
5. Брюховецький В. Віктор Петров у двобої з Левіафаном. Біографічні розвідки й літературні констатації. Київ: Дух і Літера, 2025. 592 с.
6. Б'юкенен Б. Хакери і держави. Кібервійни як нові реалії сучасної геополітики. Пер. з англ. Ю. Каздобіна. Київ: Наш формат, 2024. 352 с.
7. Ґалеф Дж. Мислення розвідника. Як припинити обманювати себе й побачити найкраще рішення. Пер. з англ. Н. Яцюк. Київ: Наш формат, 2023. 272 с.
8. Ґюркан Е. С. Шпигуни султана. Агентурні, саботажницькі та корупційні мережі XVI століття. Пер. з тур. О. Кульчицький. Львів: Видавництво Анетти Антоненко; Київ: Ніка-Центр, 2023. 320 с. https://anetta-publishers.com/books/199
9. Девайн Дж., Лоеб В. Вдале полювання. Історія головного шпигуна Америки. Пер. з англ. Є. Тарнавського. Харків: Фоліо, 2018. 316 с.
10. Лебедєва К. Микола Глущенко – художник і шпигун. Київ – Харків: Видавець Олександр Савчук, 2022. 157 с. https://amnesia.in.ua/glushchenko
11. *Локальна історія*. 2023. № 9: Розвідка. 96 с.
12. Монолатій І. Виконавець слова. Яків Оренштайн. Український видавець на перехрестях культур, ідеологій та політики. Київ: Дух і Літера, 2025. 272 с.
13. Монолатій І. Ким був і/або не був Яків Макогін? "Gente Ruthenus, natione Americanus" https://zbruc.eu/node/115605
14. Перлрос Н. Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь. Пер. з англ. В. Махонін. Харків: Фоліо, 2022. 574 с. https://surl.lt/xizcin

15. Сирота Р. Війна, шпигуноманія і випробування для української справи у Великій Британії в 1914-1916 роках. *Записки НТШ.* Том CCLVI. Праці Історично-філософської секції. Львів, 2008. С. 363-393.
16. Шаповал Ю. Непрощенний. Олександр Довженко і комуністичні спецслужби. Варшава – Київ – Харків, 2022. 353 с. https://ipiend.gov.ua/wp-content/uploads/2022/08/Dovzhenko-Varshava-2022-.pdf
17. Gut J., Liber J. Wybrane operacje sił i służb specjalnych Stanów Zjednoczonych i Wielkiej Brytanii. Warszawa: Difin, 2024. 267 s.
18. Zięba A. Lobbing dla Ukrainy w Europie międzywojennej. Ukraińskie Biuro Prasowe w Londynie oraz jego konkurenci polityczni (do roku 1932). Kraków: Księgarnia akademicka, 2010. 790 s. https://surl.li/kpcrrf

Авторські відеоматеріали:

1. Монолатій І. «Яків Макогін: патріот, шпигун, самозванець». *Історичний вебінарHistorical Webinar* https://www.youtube.com/watch?v=27XJz7rymLs
2. Монолатій І. «Вигадати собі шпигуна. Як (не)адміральська донька С'юзен Фаллон створила американського героя та українського авантюриста Якова Макогона». *Центр СУА з жіночих студій в УКУ* https://www.youtube.com/watch?v=tDwtQEmTE1E
3. Монолатій І. «Приватні шпигуни та їх роль в українському політичному процесі». *Школа експертів Факультету суспільно-гуманітарних наук КУБГ.* https://www.youtube.com/watch?v=_oyTE60m6Yc
4. Монолатій І. «Шпигунські ігри Якова Макогона: від спецслужб до українського престолу». *Пороблено* https://www.youtube.com/watch?v=1KrMSOqTx0s
5. Монолатій І. «Макогін псевдо Розумовський. Уявлена українська людина». *ТРК РАІ* https://www.youtube.com/watch?v=07kGXwgvtO8

***

ЗМІСТ НАВЧАЛЬНО-МЕТОДИЧНОГО ПОСІБНИКА «ШПИГУНСТВО ЯК ІНСТРУМЕНТ ДЕРЖАВНОЇ БЕЗПЕКИ»

ПОЯСНЮВАЛЬНА ЗАПИСКА …… **3**

ОСНОВНИЙ ЗМІСТ ЛЕКЦІЙНИХ ЗАНЯТЬ …… **5**

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК ДЛЯ ЗАСВОЄННЯ ОСНОВНИХ ПОНЯТЬ ЛЕКЦІЙНИХ ЗАНЯТЬ ……**16**

ОСНОВНИЙ ЗМІСТ СЕМІНАРСЬКИХ ЗАНЯТЬ ……**18**

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК ДЛЯ РОБОТИ ПІД ЧАС СЕМІНАРСЬКИХ ЗАНЯТЬ……..**37**

ПІДСУМКОВЕ ТЕСТУВАННЯ ……...**39**

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ …… **44**

ПРАКТИЧНІ ЗАВДАННЯ У ФОРМАТІ КЕЙСІВ І СЦЕНАРІЇВ ……**46**

ПРОБЛЕМАТИКА ПРОФІЛЮВАННЯ ШПИГУНСТВА …… **48**

ПРАКТИЧНІ ЗАВДАННЯ У ФОРМАТІ АНАЛІТИЧНОГО ПОРТРЕТУВАНННЯ ШПИГУНІВ/ШПИГУНОК …… **54**

НАВЧАЛЬНО-ЛОГІЧНІ ЗАДАЧ СЕРЕДНЬОГО РІВНЯ СКЛАДНОСТІ …….. **56**

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ТА ЛІТЕРАТУРА ……... **58**

Монолатій І. *Шпигунство як інструмент державної безпеки:* Навчально-методичний посібник для здобувачів освіти першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Політологія. Національна безпека», спеціальність С2 Політологія, галузь знань С «Соціальні науки, журналістика, інформація та міжнародні відносини». Івано-Франківськ: Карпатський національний університет імені Василя Стефаника, 2025. 62 с.