МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н. КАРАЗІНА

Кафедра міжнародних відносин, міжнародної інформації та безпеки

КОМПЛЕКС НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ

з дисципліни
«Концепції та стратегії міжнародної інформаційної безпеки»

рівень вищої освіти: другий (магістерський)

галузь знань: 29 «Міжнародні відносини»

спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

освітня програма «Міжнародні відносини, суспільні комунікації та регіональні студії»

спеціалізація _____
(шифр і назва)

вид дисципліни: за вибором
(обов'язкова / за вибором)

факультет Міжнародних економічних відносин та туристичного бізнесу

Укладач: д.держ.упр., проф. Солових В.П.

1. Навчальний контент.

Тема 1. Поняття, предмет та завдання курсу.

Розширене тлумачення безпеки в індустріальному і постіндустріальному суспільстві. Інформаційне суспільство. Теоретичні концепції інформаційного суспільства. Глобалізація інформації як актуальна проблема міжнародних відносин. Критерії глобалізації. Інформація як стратегічний ресурс людства і як стратегічний ресурс держави. Інформація як глобальна проблеми сучасності. Політичні ризики і загрози інформаційному суспільству, проекція на військову сферу. Інформатизація і глобалізація, революція у військовій справі.

Тема 2. Теоретичні концепції інформаційної безпеки в міжнародних відносинах.

Теорія інформаційної зброї. Концепції інформаційної безпеки як стратегії національної безпеки та оборони інформаційно-розвинутих країн світу. Сучасні інформаційні загрози (кібер, медіа та психотероризм, інформаційна злочинність). Типологія інформаційних озброєнь. Прогнозування глобальних інформаційних конфліктів у театрі воєнних дій. Інформаційні війни.

Тема 3. Інституційні основи міжнародної інформаційної безпеки.

Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки. Міжнародні угоди з питань міжнародної безпеки. Вплив ІКТ на проблему інформаційної безпеки. Еволюція нормотворчої діяльності ООН у сфері міжнародної інформаційної безпеки. Проблема ухвалення Міжнародної конвенції з інформаційної безпеки. Інформаційна безпека у програмах і практиці діяльності європейських регіональних організацій. Концепція інформаційної безпеки в рамках ЄС. Доктрина інформаційної безпеки в рамках НАТО. Інформаційна безпека у програмах ОБСЄ.

Тема 4. Протистояння інформаційним війнам як складова інформаційної безпеки.

Інформаційна війна та інформаційна боротьба: основні поняття. Форми та способи ведення інформаційної боротьби. Психологічна і кібернетична війна як складові інформаційної війни. Інформаційна зброя і технології її використання. Спеціальні інформаційні операції: методика та методологія здійснення. Аналіз впливу спеціальних інформаційних операцій на міжнародні відносини.

Тема 5. Інформаційна безпека України у контексті міжнародних відносин.

Доктрина інформаційної безпеки України. Українські ініціативи в області МІБ, історія її висунення і просування. Українсько-американські стосунки в цьому процесі. Альтернативні ініціативи США. Перспективи встановлення міжнародного контролю над інформаційними видами зброї.

Лекція 1.

Тема 3. Іституційні основи міжнародної інформаційної безпки.

3.1. Інформаційна безпека у програмах і практиці діяльності європейських регіональних організацій.

3.2. Концепція інформаційної безпеки в рамках ЄС.

3.3. Доктрина інформаційної безпеки в рамках НАТО.

3.4. Інформаційна безпека у програмах ОБСЄ.

Мета лекції: *Ознайомлення слухачів зі світовим досвідом забезпечення*

3.1. Інформаційна безпека у програмах і практиці діяльності європейських регіональних організацій.

Європейські держави, які умовно можна об'єднати під назвою «країни позаблокового статусу», належать до найрозвиненіших на континенті, в тому числі з точки зору темпів розвитку інформаційного суспільства, а також усвідомлення необхідності протидії кіберзагрозам, захист інформації та критичної інформаційної інфраструктури й інформаційнопсихологічної безпеки громадян та забезпечення інформаційної безпеки в цілому як складової національної безпеки. Тож, обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку провідних європейських країн в інформаційній сфері, критично оцінюючи та адаптуючи до власних реалій їх позитивний досвід у сфері забезпечення інформаційної безпеки. У цьому контексті корисним та цікавим убачається досвід таких країн, як Австрія, Швейцарія, Фінляндія та Ірландія, адже вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства, створення розвиненої інфраструктури інформаційних технологій та забезпечення високого рівня доступу населення до них.

Із закінченням холодної війни біполярний світ став набагато складнішим, відтак втратила самостійну цінність концепція неприєднання, неучасті у військово-політичних союзах і т.п. Зокрема, позбулося свого безпосереднього змісту поняття нейтралітету, пов'язане з неучастю у війнах, тому такий статус ряду країн Європи залишається значною мірою даниною історичним традиціям. На сьогодні такі держави позначають як постнейтральні або позаблокові (буквально - неприєднані, non-aligned). Кожна із цих держав має власну історію нейтралітету, однак протягом останніх 20 років усі вони зіштовхнулися з проблемою доцільності збереження нейтрального статусу та з необхідністю запровадження тих або інших обмежень щодо нього. Аналогічна тенденція продовжує діяти й нині, оскільки міжнародні процеси й змістовне наповнення нових загроз, серед яких це і регіональні конфлікти, і міжнародний тероризм, і поширення зброї масового знищення, а також кіберзлочинність – вимагають від міжнародної спільноти узгоджених дій та масштабного співробітництва.

Особливе місце з-поміж країн позаблокового статусу посідає Швейцарія, котра не є ані членом НАТО, ані ЄС.

З 1992 року у Швейцарії діє Федеральний акт про захист даних, який втілює загальноєвропейські принципи захисту інформації, в тому числі так званих «чутливих» відомостей та, зокрема, персональних даних. У 2010 році Верховний суд Швейцарії надав додаткові гарантії конфіденційності персональних даних, підтримавши місцевого

уповноваженого із захисту таких даних та ухваливши порядок, відповідно до якого збір інформації про IP-адреси користувачів файлообмінних мереж без їхньої згоди (в тому числі в контексті боротьби з порушеннями авторських прав) є незаконним.

У цілому забезпечення інформаційної безпеки електронних даних та інформаційних мереж здійснюється у Швейцарії відповідно до затвердженої у 2012 році Національної стратегії захисту від кіберризиків, метою якої визначено:

- раннє виявлення кіберзагроз і небезпек;
- підвищення стійкості критичної інфраструктури;
- ефективне зниження кіберризиків, зокрема кіберзлочинності, кібершпигунства й кіберсаботажу.

Передумовами для зниження кіберризиків при цьому вважається індивідуальна відповідальність та національне співробітництво між приватним сектором і органами влади, а також співпраця з іншими країнами. Держава має втручатися у процеси забезпечення кібербезпеки тільки тоді, коли суспільні інтереси перебувають під загрозою або якщо це відповідає принципу субсидіарності. Обробка кіберризиків має розглядатися як елемент процесів бізнесу, виробництва або управління, до яких мають бути інтегровані

всі суб'єкти – від адміністративних і технічних рівнів до найвищого керівництва. Ефективний підхід до управління кіберризиками, заснований на принципі розподілу обов'язків між владою, приватним сектором і населенням, передбачає, що кожна організаційна одиниця (політична, економічна або соціальна) відповідає за те, щоб знати про кібер-аспекти та усувати інформаційні ризики, пов'язані з конкретними процесами, або по можливості зменшувати їх.

На початку 2018 року Швейцарія розпочала розробку закону про інформаційну безпеку, позаяк визнано, що незаконне використання інформації та втручання в роботу інформаційних систем може серйозно вплинути на істотні інтереси держави та права її громадян. Ґрунтуючись на загальновизнаних міжнародних стандартах, закон про інформаційну безпеку має забезпечити єдину формально-правову основу для контролю й упровадження інформаційної безпеки у сфері компетенції Федерального уряду Швейцарії. Закон стосується насамперед федеральних органів державної влади – парламенту, федеральних судів, федеральної прокуратури, національного банку та ін. Приватні особи й бізнес підпадають під дію закону тільки у разі провадження інформаційно «чутливої» діяльності за дорученням федеральних органів. Федеральна рада прагне також поглибити співробітництво з кантонами, які мають бути представлені у відповідному координаційному органі та брати участь у стандартизації відповідних заходів. Серед іншого закон регулює питання управління ризиками, класифікує інформацію й установлює принципи безпеки у сфері використання інформаційно-технічних ресурсів. Передбачається, що закон про безпеку інформації матиме пріоритет над законодавством про свободу інформації.

Убачається доцільним розглянути далі досвід забезпечення інформаційної безпеки європейських країн, які не є членами НАТО, однак є членами ЄС, на прикладі Австрії, Фінляндії та Ірландії. Передусім зазначимо, що членство в ЄС накладає на ці країни обов'язки щодо дотримання стандартів цієї організації стосовно розвитку інформаційного суспільства та забезпечення інформаційної безпеки. Так, ще 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки:

- захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій».

2001 року Європейська Комісія оприлюднила документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому окреслено сучасне бачення ЄС проблематики інформаційної безпеки та, зокрема, визначено такі засади європейської політики інформаційної безпеки:

підвищення обізнаності користувачів щодо можливих загроз під час

користування комунікаційними мережами; створення європейської системи попередження та інформування про

нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки.

В Австрії, Фінляндії та Ірландії, як і в інших країнах ЄС, значна увага приділяється проблемам кібербезпеки, окресленим у Документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», де остання визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, а саме:

- традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах);
- публікації незаконного контенту в електронних медіа;
- специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Основними викликами безпеці інформаційних інфраструктур зазначених країн, як і ЄС в цілому, є:

- некоординовані внутрішньодержавні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;
- відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Вагомим елементом інформаційної безпеки усіх без винятку країн ЄС є захист персональних даних, засади якого визначені директивою 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» [354]. Обов'язкові для країн-членів ЄС нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року, для Австрії, Фінляндії та Ірландії набувають чинності у 2018 році. У документі переглянуто цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження на переміщення даних між різними країнами. Важливим нововведенням убачається також запровадження більш суворого покарання за несвоєчасне повідомлення інформації про виток даних.

Одним із лідерів ЄС за показниками розвитку інформаційного суспільства справедливо вважають Фінляндію, адже в рейтингу країн Євросоюзу вона утримує першість за рівнем цифрової грамотності (понад 50 % населення) й посідає друге місце за показником поширення мережі широкосмугового зв'язку (34 % населення).

Головними державними інституціями, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій Фінляндії, Омбудсмен з питань захисту даних (Data Protection Ombudsman). До повноважень Міністерства транспорту та комунікацій належить розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розробка й реалізація національної політики у сфері інформаційної безпеки.

Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), до компетенції якого входить контроль та державне регулювання у сфері інформаційно-комунікаційних технологій. До повноважень FICORA належить:

- контроль за функціонуванням електронних комунікаційних мереж;
- інформування про можливі загрози інформаційній безпеці;
- підвищення обізнаності громадян з питань інформаційної безпеки;
- планування й управління використанням радіочастот, мережевими адресами, а також контроль за змістом програм і реклами на телебаченні та радіо.

У структурі FICORA функціонує CERT-FI (Computer Emergency Response Team of

Finland) – фінська комп'ютерна група швидкого реагування, основним завданням якої є попередження, виявлення та реагування на кіберінциденти, а також поширення інформації про загрози інформаційній безпеці. У забезпеченні інформаційної безпеки активну участь бере також громадянське суспільство. Серед неурядових організацій, що опікуються проблематикою інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association - FiSA). FiCom здійснює планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, моніторинг ситуації в ІКТ-секторі, бере участь у регулюванні ринку інформаційно-комунікаційних технологій тощо. Натомість метою FiSA є розвиток професіоналізму й обізнаності у сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки. У 2015 році компанія CGI відкрила у Фінляндії центр інформаційної безпеки, завданням якого є відстеження кібератак.

Стратегія національної безпеки Фінляндії, зазначаючи, що критична інфраструктура країни все більше залежить від інформаційних систем та мереж, передбачає мінімізацію відповідних ризиків важливим завданням забезпечення всеосяжної безпеки. Концепція всеосяжної безпеки, окрім традиційного сценарію протидії військовим загрозам, охоплює також інші проблеми на кшталт зміни клімату, дефіциту енергетичних та водних ресурсів, міграції, тероризму, торгівлі наркотиками, кібератак тощо.

Стратегія кібербезпеки Фінляндії, затверджена у 2013 році, наголошує на тому, що загрози, які виходять з кіберпростору, стають усе більш серйозними, адже кібератаки можуть використовуватися як інструмент політичного й економічного тиску, в тому числі в комплексі із традиційними військовими засобами. При цьому кіберпростір – це джерело величезного потенціалу та ресурсів, позаяк збільшує можливості розвитку бізнесу, працевлаштування та залучення іноземних інвесторів. Стратегія також визначає, що Фінляндія як невелика й відкрита до співробітництва країна має «відмінні шанси піднятися до авангарду кібербезпеки». Бачення кібербезпеки полягало в такому:

- країна спроможна забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях;
- громадяни, органи влади та юридичні особи можуть ефективно використовувати безпечний кіберпростір, що виникає завдяки заходам кібербезпеки, здійснюваних на національному й міжнародному рівнях;
- до 2016 року Фінляндія має стати провісником повної готовності до протидії кіберзагрозам та управління порушеннями, що викликані цими загрозами.

Якщо розслідування кіберінцидентів здійснює поліція, то організація всеосяжного кіберзахисту покладається на Сили оборони Фінляндії під проводом Міністерства оборони. Потенції військового кіберзахисту включають розвідку, кібератаки та ведення кібервійн, однак головним вектор військової потуги в кіберпросторі спрямований на інтелектуальне попередження загроз. Зауважимо, що 2015 року Міністерство внутрішніх справ Фінляндії ініціювало оновлення закону про розвідувальну діяльність з метою надання поліції та військовим права на розвідку в інформаційних мережах [362].

Фінська модель інформаційного суспільства має яскраво виражену соціальну спрямованість з поєднанням динамічної взаємодії бізнесу й суспільством за активної посередницької ролі держави. При цьому держава залишає за собою дві функції: управління розвитком та дерегулювання [363]. До переліку її основних завдань входить створення національної інформаційної інфраструктури з метою сприяння підвищенню рівня поінформованості населення країни. Саме тому ще з 2003 року уряд Фінляндії в рамках Стратегії кібербезпеки здійснює заходи з інформування громадян країни про методи і способи захисту від негативного інформаційного впливу.

Варто також відзначити, що в 2013 році уряд Фінляндії затвердив національну Стратегію інформаційної безпеки, яка окреслила такі пріоритети:

− створення національного центру інформаційної безпеки для комплексного збору та аналізу даних, загальної ситуаційної обізнаності, а також національного та міжнародного співробітництва;

− удосконалення управління загрозами та ефективністю обслуговування стратегічно важливих інформаційних систем;

− підвищення базових знань населення та бізнесу у сфері інформаційної безпеки шляхом надання конфіденційних і безпечних мережевих сервісів та послуг;

− розробка і здійснення професійної підготовки на всіх рівнях з метою зміцнення інформаційної безпеки;

− інвестування в міжнародне співробітництво та участь у міжнародній науково-дослідній діяльності, орієнтованій на інформаційну безпеку.

Як бачимо зі змісту основних пріоритетів Стратегії інформаційної безпеки Фінляндії, усі вони розроблені відповідно до принципів, за якими побудована модель національного інформаційного суспільства.

Що стосується Австрійської Республіки, то програми становлення інформаційного суспільства в цій країні втілюють політичну стратегію об'єднання Європи на базі новітніх технологій, інформаційнокомунікаційної інфраструктури та інтелектуального потенціалу регіону. На інформаційну політику Австрії значний вплив чинять міжнародні організації, що мають резиденції у Відні, складовою програм діяльності яких є розвиток інформаційного суспільства. У Плані дій Уряду Австрії передбачено такі напрями інформаційної інтеграції країни, як:

- координація трансформації інформаційного сектору;
- створення відповідних державних інституцій з регулювання ринку інформаційних технологій;
- стимулювання виробництва інформаційних продуктів та послуг;
- підтримка лідерства Австрії в галузі електронних технологій, зокрема виробництва мікрочипів та інтегрованих електронних схем;
- лібералізація торгівлі інформаційними продуктами й послугами; розвиток електронної комерції;
- сприяння торгівлі інноваційними технологіями з третіми країнами;
- створення об'єднаних мереж австрійських та європейських центрів прикладних досліджень інформаційного суспільства;
- використання потенціалу міжнародних організацій;
- наукова кооперація (на паритетних засадах);
- розробка проектів для соціальної сфери, освіти, охорони здоров'я, екології;
- міжнародне співробітництво за гуманітарними напрямами.

Стратегія кібербезпеки Австрії зазначає, що звичайні військові напади на країну в найближчій перспективі малоймовірні, натомість для Австрійської Республіки та ЄС в цілому все більшої актуальності набувають нові проблеми, ризики й загрози. Це, насамперед:

- міжнародний тероризм;
- поширення зброї масового знищення;
- внутрішні й регіональні конфлікти або заворушення, які стосуються Європи або мають глобальні наслідки;
- «відмова держави»; природні або техногенні катастрофи;
- кібератаки;
- загрози для стратегічної інфраструктури;
- транснаціональна організована злочинність;
- торгівля наркотиками, корупція, незаконна міграція;
- безуспішна інтеграція;

- брак ресурсів (енергія, продовольство, вода тощо), зміна клімату, екологічна шкода й пандемії;
- піратство й загрози транспортним маршрутам, а також наслідки міжнародної фінансово-економічної кризи у сфері безпеки [363].

Напади з кіберпростору становлять безпосередню загрозу безпеці й належному функціонуванню державного апарату, економіки, науки й суспільства. Недержавні суб'єкти (приміром, злочинці, учасники організованих злочинних угруповань або терористи), а також державні суб'єкти (скажімо, секретні служби й військові) можуть зловживати можливостями кіберпростору у своїх власних цілях і перешкоджати його належному функціонуванню. Як загрози в кіберпросторі, так і його продуктивне використання практично не лімітовані. Тому головним пріоритетом Австрії є забезпечення безпеки й кібербезпеки на національному й міжнародному рівнях. Всеосяжна політика кібербезпеки означає, що зовнішня й внутрішня безпека, а також усі аспекти цивільної й військової безпеки тісно пов'язані та взаємозалежні. Забезпечення кібербезпеки виходить за межі компетенції традиційних органів безпеки й потребує залучення інструментів багатьох інших сфер безпекової політики. Інтегрована політика кібербезпеки має наголошувати на поділі завдань між державою, економікою, науковими колами й громадянським суспільством, включаючи заходи у таких напрямах:

- політико-стратегічне управління;
- оцінювання ризиків;
- запобігання загрозам та забезпечення готовності;
- визнання й реагування, обмеження наслідків і відновлення;
- розвиток урядових і неурядових можливостей.

Політика кібербезпеки має бути проактивною, що означає роботу із запобігання загрозам кіберпростору й людні в кіберпросторі або пом'якшення їх впливу («налаштування безпеки»). Політика кібербезпеки також має бути заснована на принципі солідарності, позаяк через глобальний характер кіберпростору кібербезпека Австрії, ЄС і всього світового співтовариства дуже взаємозалежна. Тому для забезпечення кібербезпеки потрібне інтенсивне співробітництво на спільній основі на європейському й міжнародному рівні [364].

Стратегієя кібербезпеки Австрії національним координатором і центральним органом у сфері кібербезпеки визначила Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю [366, с. 79]. Федеральне міністерство внутрішніх справ Австрії, до складу якого входить вказаний Центр, є органом з контррозвідувальними функціями, що виконує завдання із забезпечення державної безпеки. Це, зокрема, – боротьба з тероризмом, політичним екстремізмом, незаконною міграцією, протидія злочинам проти конституційного ладу та основ державної безпеки .

Ірландію, де розташовані великі європейські офіси таких компаній, як Google і Facebook, часто називають європейською Силіконовою долиною, оскільки ця країна докладає багато зусиль для підготовки та працевлаштування IT-фахівців. У 2013 році компанія Microsoft проінвестувала 170 мільйонів євро у створення та розвиток європейського дата-центру в Ірландії. Ця ініціатива була підтримана місцевою владою, адже Ірландія прагне стати європейським лідером у сфері обробки big data, а її кліматичні умови підходять для підтримки необхідної температури роботи серверів. Кім того у Дубліні створюється тренінговий центр, котрий, як планується, у щільній співпраці з урядом та навчальними закладами країни проводитиме навчання в таких перспективних галузях, як захист критичної інфраструктури й кібербезпека транспорту.

Національна стратегія кібербезпеки Ірландії на 2015-2017 роки передбачала, що уряд

всіляко сприятиме стійкій та безпечній експлуатації комп'ютерних мереж і відповідної інфраструктури ірландськими громадянами й підприємствами. Розвиток і поширення інформаційнокомунікаційних технологій посприяв вагомому поліпшенню якості життя, появі інноваційних послуг та радикальним змінам в організації бізнесу. Відтак, держава, критична інфраструктура, юридичні особи й громадяни залежать від надійного функціонування інформаційно-комунікаційних технологій та Інтернету. Порушення роботи цих систем, яким би джерелом воно не було спричинене, створює безпосередню загрозу функціонуванню державного механізму й економіки, може відчутно вплинути на повсякденне життя мільйонів громадян. Тому на будь-яку загрозу безпеці кіберпростору потрібне своєчасне, надійне й послідовне реагування як на національному, так і на міжнародному рівні. З цією метою уряд Ірландії намітив виконання відповідними суб'єктами країни таких завдань:

підвищити стійкість і надійність критично важливої інформаційної інфраструктури в найважливіших секторах економіки, особливо в державному; продовжувати взаємодію з міжнародними партнерами, аби кіберпростір залишався відкритим, безпечним, цілісним і безкоштовним, а також здатним сприяти економічному та соціальному розвитку; підвищувати обізнаність про відповідальність бізнесу та приватних осіб з питань забезпечення безпеки своїх інформаційних мереж, інфраструктури та даних, а також підтримувати таку обізнаність за допомогою інформації, навчання та узагальнення практики; забезпечувати для державних органів всеосяжні та гнучкі нормативно-правові рамки для боротьби з кіберзлочинністю, які були би доречними й домірними із потребами захисту «чутливих» чи особистих даних; створювати потенціал для органів влади і приватного сектору для функціонування та аварійного управління в умовах кіберінцидентів.

3.2. Концепція інформаційної безпеки в рамках ЄС.

Вивчення практики європейських країн у побудові влсних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також аналіз ряду міжнародних правових документів дає змогу нам резюмувати про відсутність єдиної моделі національної системи правового забезпечення інформаційної безпеки

Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері. При цьому, з огляду на геополітичне положення України, її провідним орієнтиром мають стати передусім країни Центральної Європи, адже саме вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства шляхом створення розвиненої інфраструктури інформаційних технологій з унікально високим рівнем доступу населення до них, випереджаючи за цим показником інші країни світу.

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки, як зазначають В.Шатун та О.Гладун, події останніх років у нашій державі показали неспроможність влади адекватно протистояти інформаційним війнам, позаяк проблеми інформаційної політики досі не вирішені на належному рівні.

Питання щодо умовних кордонів Центральної Європи наразі лишається дискусійним. Традиційно до країн Центральної Європи відносять Німеччину, Ліхтенштейн, Австрію, Швейцарію та деякі інші. Утім, де-факто до них належать й учасники Вишеградської групи – Угорщина, Польща, Чехія та Словаччина, а також частина країн Балканського півострова. Зважаючи на те, що питання інформаційної безпеки у країнах позаблокового статусу доцільно розглянути окремо, наразі зосередимося на забезпеченні інформаційної безпеки у Німеччині, Польщі, Угорщині та Хорватії.

Передусім зауважимо, що Федеративна Республіка Німеччини, Угорська Республіка, Республіка Польща та Республіка Хорватія є членами Організації Північноатлантичного договору та Європейського Союзу. Відповідно, на них

поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в Організації Північноатлантичного договору (НАТО)», офіційна політика НАТО у сфері кіберзахисту, стратегічна концепція кібербезпеки, сформульована на Лісабонському саміті й уточнена за результатами Варшавського саміту, та ін.

Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, але й ЄС, який сьогодні об'єднує розвинуті країни, котрі відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах. 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки, а саме:

- захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій», де застосовано модель тріади CIA (CIA Triad), яка передбачає такі основні характеристики інформаційної безпеки:

1) конфіденційність;
2) цілісність;
3) доступність [103, с. 43].

У документі Європейської Комісії «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), визначено базові засади Співтовариства до проблеми забезпечення інформаційної безпеки. Термінологічне сполучення «мережева та інформаційна безпека» трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, котрі становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі й системи. Згаданий документ визначає такі пріоритетні напрями європейської політики забезпечення інформаційної безпеки:

- підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
- створення європейської системи попередження та інформування про нові загрози;
- забезпечення технологічної підтримки;
- підтримка ринково орієнтованої стандартизації та сертифікації;
- правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
- зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнамичленами електронних підписів під час надання державних онлайн послуг тощо;
- розвиток міжнародного співробітництва з питань інформаційної безпеки.

У всіх без винятку країнах ЄС питаням правового забезпечення інформаційної безпеки надається особлива увага. При цьому першочергового значення набувають питання протидії кіберзагрозам, які є складовими процесу забезпечення інформаційної безпеки. З 1999 року реалізуються програми «Безпечніший Інтернет» (Safer Internet), у рамках яких здійснюються заходи, спрямовані на боротьбу не лише зі шкідливим контентом, але й з небезпечною поведінкою в мережі.

Процес формування європеського глобальної системи правового забезпечення

інформаційної безпеки має тривалий характер. Ще в 2007 році Європейська Комісія прийняла документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю». У даному документі, хоча й на рівні декларації, визначено кіберзлочини як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, котрі включають: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Дещо пізніше, у 2009 році у Повідомленні Європейської Комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» були визначені головні виклики тапроблеми, які потребують першочергового реагування зі сторони країн ЄС, а також окреслило основні заходи щодо посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам . Відповідно до даного документу засадничними викликами безпеці інформаційної безпеки країн ЄС є:

- некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього запобігання та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнахчленах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;
- відсутність міжнародного консенсусу стосовно пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Окрім зазначеного, важливим аспектом правового забезпечення інформаційної безпеки у рамках ЄС є питання інформаційної відкритості органів державної влади країн учасниць. Системоутворюючою тезою даного аспекту є: «…загальновизнано, що демократична система може функціонувати найбільш ефективно лише у разі, коли громадськість повністю поінформована». У даному ракурсі слід також послатися і на рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка перебуває в розпорядженні державних органів». У даному документі відмічено, що для гарантування адекватної участі всіх у суспільному житті необхідно забезпечити, з урахуванням неминучих винятків та обмежень, доступ громадськості до інформації, що перебуває в розпорядженні державних органів усіх рівнів. Першочергово значення тут набувають питання захисту персональних даних.

З цього приводу, у резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року визначено глобальну й відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають в офф-лайн-режимі, мають також бути захищені онлайн, у тому числі право на приватність». Засади захисту персональних даних у правовій практиці країн ЄС можна звести до такого:

пріоритетність права особи розпоряджатися своїми персональними даними; використання персональних даних без дозволу володільця тягне відповідальність згідно з законодавством; для будь-кого, хто здійснює користування персональними даними фізичних осіб з їхнього дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл).

Попри згадані документи ЄС про захист персональних даних, основним серед них слід вважати директиву 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних». У ньому декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та одночасно надаються

гарантії захисту основних прав громадян, до яких належить і право на недоторканність особистих даних та їх захист від третіх осіб. Директива ЄС зобов'язує кожну державу-члена прийняти свої національні закони про захист приватних відомостей, які відповідали б рекомендаціями OECD 1980 року. З-поміж цих рекомендацій варто відзначити «Принцип гарантованої безпеки N11», який вимагає, аби «персональні дані були захищені розумними засобами безпеки від таких загроз, як утрата чи неавторизований доступ, руйнування, використання, модифікація або розголошення».

Обов'язкові для країн-членів ЄС нові правила захисту персональних даних (GDPR), які ухвалено 14 квітня 2016 року, набувають чинності у 2018 році. Ці правила поширюватимуться не лише на європейські компанії, але й на суб'єктів інших країн, які пропонують товари й послуги в ЄС. У документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження переміщення даних між країнами.

Слід констатувати, що країни ЄС сформували «в певному сенсі злагоджену систему захисту інформації», але водночас кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки.

Така, для Німеччини характерна детальна нормативно-правова розробка системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві. Приміром, відповідно до закону «Про перевірку безпеки» [386] секретною інформацією вважаються факти, вироби та відомості, незалежно від форми їх представлення, які в державних інтересах мають зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає необхідному рівню захисту:

- «цілком таємно»;
- «таємно»;
- «конфіденційно»
- «для службового користування».

До системи секретної інформації належить державна таємниця (відомості з грифом «цілком таємно» і «таємно») та відомча таємниця (відомості з грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що стосуються конфіденційної сфери приватних осіб, зумовлена інтересами зовнішньої безпеки держави. Зокрема, особливо важливою та такою, що підлягає особливому захисту, вважається конфіденційна інформація про етнічне походження, політичні погляди, релігійні та філософські переконання, членство в об'єднаннях, здоров'я і статеве життя фізичних осіб.

У жовтні 1997 року в Німеччині ухвалено Акт захисту інформації в телекомунікаціях (TDPA). Відповідно до його загальних принципів збирання, обробка та використання інформації допускається лише у випадках, коли це дозволено законом або здійснюється за згодою користувача. Інформація може бути зібрана, оброблена або використана лише окремо для різних послуг, яких потребує один і той самий користувач, причому згода останнього не є умовою для надання послуг.

Крім того, з 2005 року в Німеччині діє так званий «Акт про свободу інформації», який регламентує питання доступу до неї. Нагляд за виконанням положень цього нормативного акта покладено на комісара із захисту інформації та персональних даних. У країні від 1990 року діє також закон про доступ приватних осіб і дослідників до архівів «Штазі» – служби безпеки колишньої НДР.

Федеральна служба інформаційної безпеки (BSI) є головним органом на який покладено обов'язки по забезпеченню інформаційної безпеки країни. BSI входить до Федерального міністерства внутрішніх справ, яке, серед інших функцій:

- забезпечує внутрішню безпеку і захист конституційного ладу Німеччини;
- здійснює боротьбу з тероризмом, екстремізмом, шпигунством і саботажем.

Відповідно до закону «Про Федеральне відомство безпеки інформаційних систем» BSI збирає та оцінює інформацію стосовно загроз кібербезпеці держави, виявляє нові типи кібератак, аналізує відповідні контрзаходи. На BSI покладається також виконання таких функцій у взаємодії з НАТО та ЄС:

- оцінка ризику впровадження інформаційних технологій;
- розробка критеріїв, методів та випробних засобів для оцінки ступеня захищеності національних комунікаційних систем;
- перевірка ступеня захищеності інформаційних систем і видача відповідних сертифікатів;
- видача дозволів на впровадження інформаційних систем у важливі державні об'єкти;
- здійснення спеціальних заходів безпеки інформаційного обміну в державних органах, поліції тощо;
- консультування представників промисловості з питань інформаційної безпеки.

Крім того, відомство провадить заходи з пропаганди необхідності забезпечення інформаційної безпеки.

З метою оптимізації оперативного співробітництва між усіма державними установами та поліпшення координації заходів із протидії кібератакам у ФРН на базі Федерального відомства безпеки інформаційних систем створено національний центр кіберзахисту (NCAZ), який безпосередньо взаємодіє з іншими суб'єктами кібербезпеки країни, у тому числі з приватним сектором, країнами-партнерами з ЄС, НАТО, а також міжнародними організаціями.

Питаннями забезпечення інформаційної безпеки Німеччини в межах своєї компетенції опікуються також Федеральне бюро захисту конституції (BFV) та Управління інформаційних операцій, створене 2009 року у структурі бундесверу через масовані атаки на обчислювальні мережі державних структур ФРН у лютому 2009 року. Наприкінці 2010 року в рамках реалізації концепції кіберзахисту у структурі командування бундесверу остаточно завершене також формування підрозділу інформаційних і комп'ютерних мережевих операцій, який від 5 квітня 2017 року функціонує як «Сили кібернетичного та інформаційного простору Німеччини». До завдань зазначеного підрозділу входить, зокрема:

- розробка нових методів кібератак;
- проникнення в комп'ютерні мережі іноземних держав і організацій з метою отримання розвідувальних даних;
- проведення операцій деструктивного впливу на мережі й автоматизовані системи або блокування їх роботи.

Аналіз відкритих джерел щодо політки інформаційнох безпеки Німеччини здає змогу зробити нам висновок, що серед пріоритетів протидії кіберзагрозам, Німеччина обрала тактику так званої «активної оборони». Виділення наступальної складової інформаційного протиборства і створення відповідної окремої структури є, за оцінками німецьких експертів, адекватною відповіддю на сучасні загрози інформаційній безпеці Німеччини.

Подібна тактика забезпечення інформаційної безпеки успішно діє і у Франції, де 17 липня 2014 року на рівні законодавчого акту визначено глобальну політику безпеки інформаційних систем. Даним правовиим актом вустановлено правила захисту державних інформаційних систем, та пріортетні механізм протидії кіберзагрозам на рівні держави. Дещо пізніше, а саме 27 березня 2015 року, вийшов Декрет № 2015-351, де уряд Франції сформулював нові положення безпеки інформаційних систем операторів галузей, роль яких має критичне значення для життєдіяльності нації.

Наведені вище законодавчі кроки яскраво підтверджують, що у країнах Центральної Європи питанням інформаційної безпеки приділяється особлива увага.

Що стосується подібної практики наших ближчих сусідів, зокрема Польщі, зазначимо, національна інформаційна політика Республіки Польща концептуально

зорієнтована на розвиток вільного відкритого суспільства, забезпечення основоположних прав людини та громадянина, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних мас-медіа. Правовим втілення польської концепції інформаційної безпеки є прийняті у 1990-х роках «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», де визначено напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій (33%-49% зарубіжного капіталу), ліцензування інформаційної діяльності. Окремо виписано права церкви на інформаційну діяльність, з огляду на значний вплив клерикальної інформації на політичні пріоритети та моральність польського суспільства.

Основні функціональні повноваження у забезпеченні кібернетичної безпеки Польщі покладено на Агентство внутрішньої безпеки (ABW). У 2013 році за участю даного органу розроблено Стратегію кібербезпеки Польщі та створено при Міністерстві національної оборони Центру криптології, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій [398]. ABW також сформувало урядову команду реагування на комп'ютерні інциденти (CERT) [399], головним завданням якої є забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз. Зокрема, це стосується захисту від атак на інфраструктуру, що складається з ІТ-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв у функціонуванні органів державної влади [400]. Під керівництвом ABW у 2015 році розроблена й Доктрину кібербезпеки Польщі, яка оперує ключовими поняттями теорії безпеки на кшталт «загроз», «викликів», «ризиків» тощо.

У 2015 році у Польщі розпочато роботу над Доктриною інформаційної безпеки. З-поміж загроз інформаційній безпеці у Доктрині названі, наступні: ескалація напруження у міжнародних стосунках; дискредитація польської міжнародної політики і формування негативного іміджу країни на міжнародній арені, в тому числі й серед союзників по НАТО та ЄС; формування образу Польщі як країни ксенофобів та антисемітів; провокування польсько-литовського конфлікту на тлі польської меншини в Литві; підбурювання польсько-українського конфлікту на складному історичному тлі з можливим застосуванням терористичних замахів, які буцімто могли би здійснити українці проти поляків чи навпаки.

Доктрина інформаційної безпеки Польщі розглядається як виконавчий документ до Стратегії національної безпеки.

Важливим аспектом, який доречно й розвивати в українських реаліях, є залучення у Польщі до боротьби з інформаційними загрозами громадянське суспільство. Зокрема успішним прикладом такої діяльності є створена у 2018 році неурядова організація - Центр аналізу пропаганди і дезінформації. Даний Центр займається виявленням і протидією російській пропаганді. Вказана фундація є першою такого роду інституцією у Польщі, діяльність якої спрямовуватиметься на аналіз і пошук системного підходу до ідентифікації та протидії російській дезінформації в польському інформаційному просторі. Окрім науково-дослідної й аналітичної роботи, Центр співпрацюватиме з іншими суб'єктами, аби закласти фундамент розуміння у польському суспільстві загроз, позаяк інформаційна і психологічна війна проникає у різні сфери життєдіяльності суспільства й держави.

Іншою особливістю правовго забезпечення інформаційної безпеки у Польщі та й ряді інших країн Східної Європи, є безпосередній вплив на політику держави в інформаційній сфері вступ до НАТО. Це спонукало країни до приведення у відповідність до стандартів НАТО національне інформаційне закнодавство. Прикладом цього можна назвати прийнятий у січні 1999 року закон «Про захист конфіденційної інформації», ухвалення якого було однією з умов вступу Польщі до НАТО . Іншим прикладом такого процесу є прийнятий у 1995 році закон Угорщини про державні та офіційні секрети у.

У цілому ж угорська політика у сфері забезпечення інформаційної безпеки налаштована переважно на обмеження. Так, закон про засоби масової інформації (2010) викликав критику з боку світових медіа та ЄС - Угорщину звинуватили в запровадженні тотального контролю за ЗМІ, включно з Інтернетом, у ліквідації свободи слова, ба навіть у прагненні встановити тоталітарний режим. Європейський парламент ухвалив резолюцію (вперше стосовно країни – члена ЄС) із засудженням того, як угорський уряд ставиться до демократії, свободи слова, прав людини. Згодом парламент Угорщини вніс косметичні поправки до цього закону, які втім не торкнулися ключових питань (структури управління угорськими ЗМІ), але були сприйняті ЄС позитивно.

Угорщина стала першою із постсоціалістичних країн, котра прийняла «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес» (1992), яким, зокрема, запроваджено інститут Парламентського комісара із захисту інформації та свободи інформації. Відповідно до цього закону особу, чиї персональні дані обробляються, належить повністю поінформувати про мету цих дій. Допускається збір виключно тих даних, які необхідні для досягнення вказаної мети, а зберігатися вони можуть лише протягом терміну, допоки мета не буде досягнута. Кожному надається право діставати доступ до своєї персональної інформації та в разі потреби вимагати її виправлення або знищення. Особливий захист передбачено для так званих «чутливих» (sensitive) даних, які стосуються «расового походження, національності й етнічного статусу, політичних думок чи партійної приналежності, релігійних чи інших переконань» або «відомостей про хвороби, сексуальне життя чи судимості». Крім того, правове підґрунтя забезпечення інформаційної безпеки в частині захисту персональних даних в Угорщині становлять закони «Про право на інформаційне самовизначення та свободу інформації» (2011) та «Про обробку і захист медичної інформації та пов'язаних з нею персональних даних» (1997). З будь-яких питань, пов'язаних із захистом персональних даних, особа може звернутися до Національного бюро із захисту даних та свободи інформації.

Правове забезпечення інформаційної безпеки Угорщини, в т.ч. кібербезпеки, втілено у законі «Про електронну інформаційну безпеку державних та муніципальних органів» (2013) та п. 31 Стратегії національної безпеки Угорщини, затвердженої у 2012 році. Стратегія національної безпеки, зокрема, передбачає, що держава має бути готова управляти ризиками й загрозами, пов'язаними з національною безпекою, обороною, боротьбою проти злочинності, а також запобігати нештатним ситуаціям у кіберпросторі, гарантувати адекватний рівень кібербезпеки й виконувати інші завдання, пов'язані із забезпеченням кібербезпеки. При цьому основним завданням визнається систематичне визначення пріоритетів у сфері потенційних загроз і ризиків у кіберпросторі, а також підвищення поінформованості суспільства щодо них. Відповідні положення дістали подальшого розвитку в Національній стратегії кібербезпеки Угорщини, затвердженій 2013 року.

Досить цікави є досвід правового забезпечення інформаційної безпеки держави у Хорватії. У цій країні ще з 2007 року діє Акт про інформаційну безпеку. Цим законодавчим актом визначені поняття інформаційної безпеки, її елементи, заходи забезпечення і стандарти, а також функціональні компетентності органів для прийняття й реалізації рішень у сфері протидії загрозам та забезпеченні інформаційної безпеки держави, а також нагляду за дотриманням відповідних стандартів.

У 2015 році в Хорватії прийнято національну стратегію кібербезпеки, яка базується на таких основних принципах:

- усебічність підходу до кібербезпеки, що охоплює кіберпростір, інфраструктуру й користувачів відповідно до хорватської юрисдикції (громадянство, реєстрація, домен, адреса);
- інтеграція заходів у різних сферах забезпечення кібербезпеки;
- проактивність завдяки постійному коригуванню заходів та періодичному уточненню їх стратегічних кордонів;

- зміцнення стійкості, надійності й керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності й доступності певних груп інформації та соціальних цінностей;
- захист прав і свобод людини у кіберпросторі, передусім – конфіденційності та власності;
- постійне вдосконалення правової бази;
- субсидіарність при розподілі повноважень; відповідність витрат на забезпечення кібербезпеки ступеню ризику тощо.

Стратегія кіберзахисту є частиною стратегії оборони, що є сферою відповідальності Міністерства оборони Хорватії. Кібертероризм, кіберзлочинність та деякі інші кібернетичні аспекти національної безпеки розглядаються також компетентними органами у системі безпеки й розвідки, як такі, що потребують спеціального підходу.

Слід зазначити, що забезпечення інформаційної безпеки, в тому числі шляхом активних інформаційних операцій, наприкінці минулого століття стало важливим компонентом боротьби Хорватії за свої тимчасово окуповані території, де понад чотири роки існувала сепаратистська «Республіка Сербська країна». При цьому, за оцінками експертів, якщо в мілітарному значенні боротьба за повернення вказаних територій закінчилася у серпні 1995 року під час операції «Буря», в дипломатичному – на початку 1998-го, водночас із мирною реінтеграцією хорватського Подунав'я, то в інформаційному сенсі війна закінчилася лише через 15 років після закінчення бойових дій.

Важливою складовою забезпечення інформаційної безпеки держави є міжнародна діяльність України у контексті широкого висвітлення подій, які гостро торкаються питань основних її складових. Аналіз міжнародного інформаційного простору дає підстави стверджувати, що Україна стала об'єктом інформаційних атак (інформаційно-психологічних акцій), спрямованих га встановлення контролю над усіма сферами існування незалежної держави. Нерозуміння важливості проведення з боку України акцій інформаційного впливу задля підтримки наших національних інтересів і державної політики за кордоном, як засвідчують останні події, завдає державі величезних економічних, політичних, іміджевих та інших збитків.

Російська Федерація, наприклад, не обмежується проведенням інформаційних атак на українське населення. Через мережу російського мовлення за кордоном – потужну систему інформаційного впливу – вона проводить інформаційні операції для формування негативного іміджу нашої держави.

Прикладом успішності інформаційної експансії Росії можуть слугувати результати опитування «Як бачать в ЄС війну на сході України», яке американська компанія TNS проводила 3–8 вересня 2015 р. у восьми країнах – членах ЄС: Великобританії, Іспанії, Італії, Нідерландах, Німеччині, Польщі, Франції і Швеції. Зокрема, 53% опитаних європейців вважають, що в Україні відбувається громадянська війна. Серед тих, хто сприймає події в Україні як громадянську війну, найбільша частка німців (61%), італійців (59%) та голландців (58%). Менше підтримують це визначення британці та французи (42%). На жаль, навіть у Польщі більшість респондентів підтримала тезу про громадянську війну в Україні, хоч поляків найбільше і серед тих, хто не погоджується із цим твердженням (36%). З офіційною версією України, що в державі триває антитерористична операція, погоджується лише третина респондентів (з них лише 8% цілком згодні з цією думкою). 20–24% респондентів взагалі не знають, що відбувається на сході України.

Такі цифри засвідчують непідготовленість України до інформаційного протистояння зовнішньополітичним впливам. Однією з причин цього може бути те, що в нашій державі на інституційному рівні забезпеченням окремих напрямів інформаційної безпеки опікується низка органів державної влади, зокрема Міністерство інформаційної політики, Національна рада України та Державний комітет з питань телебачення й радіомовлення, Національна комісія державного регулювання у сфері зв'язку та інформатизації, МЗС України, МВС України, СБ України, Державна служба спеціального зв'язку та захисту інформації, МО України, СЗР України тощо. Проте, всі вони виявилися неготовими з

об'єктивних і суб'єктивних причин до протидії сучасним викликам і загрозам. Проблема в тому, що жоден із державних органів, які беруть участь у забезпеченні інформаційної безпеки України, не відповідає за незадовільний стан протидії інформаційній агресії через відсутність суб'єкта юридичної координації зусиль забезпечення національної безпеки в інформаційній сфері. Кожен виконує виключно свою функцію, не знаючи, що роблять інші відомства в цій сфері.

Британський тижневик The Economist розглядає тему збройного протистояння на сході України у статті під заголовком «Україна і Росія разом у пастці війни на Донбасі». Автор пояснює, що замість відкритої повномасштабної агресії проти України Кремль «створив образ громадянської війни, абсурдно зображуючи київський уряд «фашистським» режимом, а сепаратистів «борцями за свободу».

Американський аналітичний центр The Atlantic Council у публікації під заголовком «Це суперечить здоровому глузду, але озброєння України насправді заощадить гроші платників податків США» пише про те, що існує п'ять основних причин, чому американці мають насправді бути зацікавлені у наданні Вашингтоном озброєння Україні.

По-перше, читаємо у статті, «ми захищаємо наші інтереси та союзників, допомагаючи Україні захистити себе». «Кожен український солдат, який бореться за свою країну, означає на одного американця менше, необхідного для захисту Європи», – пише автор допису.

По-друге, продовжує він, ця війна безпосередньо стосується США та Європи, адже «Москва, по суті, оголосила війну Європі та міжнародному порядку». «Наразі Росія веде інформаційну війну проти кожного європейського уряду від країн Балтії до Іспанії. Москва відкрито субсидує політичні партії по всій Європі в спробі підірвати демократичні уряди», – зауважено у статті.

В ній пояснюється, що без надання України допомоги, щоб вона могла захистити себе, вплив Росії поширюватиметься, і «тоді Східна Європа буде жити в тіні війни, етнополітичної напруженості й всюдисущої реальності територіальних ампутацій». Цитуючи слова співробітника Фонду Карнеґі Шермана Ґарнетта, автор вказує, що «Україна є наріжним каменем у дузі європейської безпеки», а отже, якщо залишити Україну напризволяще, то «її поразка чи розпад потягне за собою розпад європейської безпеки».

По-третє, нагадав автор, у 1994 році США гарантували безпеку України в обмін на її відмову від ядерної зброї.

По-четверте, стверджується, що попередні нереалізовані спроби допомоги Україні заохотили Росію до ще більшої ескалації агресії з боку Росії, у той час як підтримка Києва з боку Заходу може врешті змусити Росію шукати політичного врегулювання чи повернутися до виконання своїх зобов'язань за Мінськими угодами.

По-п'яте, оскільки США є найсильнішою державою у світі, то Вашингтон не може просто заплющити очі на агресію, особливо ж агресію з участю ядерної держави. Залишення Києва віч-на-віч із агресором може призвести до вигідних фінансових оборудок із Росією чи риторичної підтримки боротьби з тероризмом, але це відчиняє двері до нового терору постійної війни, читаємо в публікації на сайті американської аналітичної установи.

За результатами проведених наукових досліджень, нині першочергової уваги потребують такі *ключові загрози національній та міжнародній безпеці в інформаційній сфері*:

–глобальні зміни і трансформації в інформаційній сфері формують новітні виклики і загрози, які становлять реальну загрозу безпеці людства та міжнародному правопорядку;

–в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції;

–більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури;

–наслідки використання сучасної інформаційної зброї можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

Окрім проведеного аналізу, важливим убачається й досвід інших країн Європейського простору, які проходять аналогічний шлях євроінтеграції. Тож дослідження, оцінка та імплементація позитивних набутків цих країн мають неабияке значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки події останніх років у нашій державі показали, що ми поки що не готові належним чином вести інформаційні війни, а політика у сфері забезпечення інформаційної безпеки та інформаційна політика загалом потребують удосконалення.

Для нас, як країни яка заявила про свої наміри Євроінтеграції та членства в НАТО, цікави є досвід Румунії й Болгарії як членів НАТО та Європейського Союзу. Першочергово тому, що в цих країнах вже апробовані і діють стандарти ЄС та НАТО щодо інформаційної політики та правового забезпечення інформаційної безпеки. Зокрема, це стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)», офіційна політика НАТО у сфері кіберзахисту, стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського й уточнена за результатами Варшавського самітів [338], та ін. Як члени ЄС ці країни втілюють також у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені «Європейськими критеріями безпеки інформаційних технологій» (1991), «Єдиними критеріями безпеки інформаційних технологій» (1996) , документами «Мережева та інформаційна безпека: європейський політичний підхід» (2001) і «На шляху до загальної політики у сфері боротьби з кіберзлочинністю» (2007) та ін. Аналіз згаданих міжнародних документів дає змогу виокремити пріоритетні напрямами забезпечення інформаційної безпеки у цих країнах:

- підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
- створення європейської системи попередження та інформування про нові загрози;
- забезпечення технологічної підтримки;
- підтримка ринково орієнтованої стандартизації та сертифікації;
- правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
- зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнамичленами електронних підписів під час надання державних онлайн послуг тощо;
- розвиток міжнародного співробітництва з питань інформаційної безпеки.

Основними викликами інформаційній безпеці Румунії та Болгарії як членів ЄС є:

- некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;
- відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури .

Попри зазначені пріоритети важливо значення на рівні законодавства надається захисту персональних даних. У Директиві 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких належить право на недоторканність особистих даних та їх

захист від третіх осіб.

Важливим нововведенням є також запровадження більш суворого покарання за несвоєчасне повідомлення інформації про витік даних. Компаніям, що порушили положення нової директиви й не доповіли про факт витоку або злому протягом 72 годин з моменту виявлення інциденту, загрожує штраф до 4% річного доходу або до 20 млн. євро [419]. Крім того, відповідна Директива передбачає необхідність отримання згоди користувачів на обробку їхніх персональних даних, причому на обробку даних з різними цілями потрібні окремі згоди. Згода має бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Згода не буде вважатися вільною, якщо користувач змушений її дати, щоб одержати доступ до сайту, програми або додатка. Винятком є випадки, коли персональні дані користувача потрібні для виконання угоди. У тому разі, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних. Компанії, що працюють із персональними даними, мусять також вести облік операцій з персональними даними (тип даних і мета їх обробки), мінімізувати використання персональних даних відповідно до принципу data protection by design, а також проводити внутрішній аудит.

У Румунії теж досить суворий підхід до даного питання. Так, у Румунії в теперішній час триває активний процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційнотелекомунікаційні системи об’єктів критичної інфраструктури держави. Законопроект «Про кібербезпеку», який у грудні 2014 року був схвалений сенатом Румунії, передбачає також створення Національної системи кібернетичної безпеки Румунії, технічну координацію якої покладено на Румунську службу інформації як головного суб’єкта забезпечення кібербезпеки держави.

Особливу увагу Національна стратегія забезпечення кібербезпеки Румунії (2013) приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки.

Пункт 4.7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, зокрема підтримувати створення джерел контр-інформаційних впливів.

Систему протидії кіберзлочинності Молдови, попри критику науковцями країни політики держави із забезпечення інформаційної безпеки у, можна вважати відносно надійною. Так, ще 2009 року парламент цієї країни ратифікував Конвенцію Ради Європи про кіберзлочинність. Крім того, у березні 2012 року Молдова підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах. Ухвалено також закон «Про попередження та боротьбу зі злочинністю у сфері комп’ютерної інформації» (січень 2010 року). Згідно із цим законом генеральна прокуратура Молдови наділена повноваженнями координувати та здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. Метою закону є вдосконалення регламентації правовідносин за такими напрямами: запобігання та боротьба з кіберзлочинністю, сприяння провайдерам і користувачам інформаційних систем, співробітництво державних служб із неурядовими організаціями та іншими представниками громадянського суспільства, а також міжнародне співробітництво з організаціями та країнами, що мають досвід у відповідних питаннях. Генеральна прокуратура з метою сприяння розслідуванням відкрила Центр розслідування

кіберзлочинів, один з відділів якого уповноважений реагувати на випадки загроз безпеці в урядових структурах, бізнесі та громадському секторі.

Окрім зазначеного у Молдові здійснено ряд важливих заходів на шляху зміцнення національної інформаційної безпеки. Зокрема, у результаті ратифікації Факультативного протоколу до Конвенції ООН про права дитини, що стосується торгівлі дітьми, дитячої проституції та порнографії, Конвенції Ради Європи про кіберзлочинність і Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства Молдова стала активним учасником процесу застосування загальної кримінальної політики у сфері боротьби з інформаційною злочинністю, у тому числі злочинами, пов'язаними із онлайн-експлуатацією дітей.

Іншим важливим заходом на національному рівні стало прийняття закону «Про електронний підпис та електронний документ» (29 травня 2014 року), розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів. Загалом слід зауважити, що у Молдові розпочато процес приведення чинного законодавства у відповідність до положень Директиви 2006/24/ЄС від 15 березня 2006 року про зберігання інформації, створеної або обробленої при наданні послуг зв'язку загального користування або мереж зв'язку загального користування, й унесення змін до директив ЄС про захист персональних даних 2002/58/ЄС [433] і 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію й призначення європейських критичних інфраструктур та оцінку необхідності поліпшення їх захисту та ін.

У Молдові в 2013 році прийнято Національну стратегію розвитку інформаційного суспільства «Moldova digitală 2020» («Цифрова Молдова 2020») і План дій з її впровадження, розроблений Міністерством інформаційних технологій та зв'язку. У Стратегії вперше розглядається проблема створення умов для підвищення ступеня безпеки й довіри до кіберпростору, а ключові дії щодо створення цих умов становлять окрему главу вищезгаданого Плану дій. Стратегія визначає, що використання нових технологій породжує багато можливостей для розвитку, але й численні ризики й уразливості, що потребують підвищеної уваги держави й зацікавлених учасників. Ці ризики характеризуються асиметрією, вираженою динамікою та глобальним характером, що ускладнює їхнє виявлення і протидію за допомогою заходів, пропорційних ефектові їхньої матеріалізації. Таким чином, попередження кібератак і боротьба з ними, у тому числі зі злочинністю в цій сфері, є одним із пріоритетів міжнародних організацій, а бурхливий ріст числа кібератак на світовому рівні (на 600% з 2005 року) вказує на нагальну необхідність вжиття заходів щодо страхування інформаційної інфраструктури Республіки Молдова від можливих ризиків, пов'язаних із незаконною діяльністю у цій сфері. Важливість цієї проблеми була підкреслена в Концепції національної безпеки та Стратегії національної безпеки Республіки Молдова, де визначено цілі системи забезпечення національної безпеки та загрози у інформаційній сфері.

На думку експертів, останні ініціативи щодо регламентації інформаційного простору містять цілу низку серйозних прогалин, які можуть призвести до зловживань. Зокрема, Концепцію інформаційної безпеки доцільно узгодити із новою Стратегією національної безпеки, однак останній проект Стратегії національної безпеки в червні 2017 року був відкликаний з парламенту президентом, а новий проект досі не розроблений. Крім того, проект Концепції передбачає надто суворий контроль Інтернету з боку деяких державних установ, зокрема Служби інформації та безпеки Республіки Молдова, які зможуть втручатися в діяльність провайдерів, а також контролювати інформаційний простір, включаючи соціальні мережі.

Цікавим є досвід Білорусії, де нагляд за інформаційним простором та система обмежень є наразі ключовими елементами державної інформаційної політики. З 2010 до 2015 року у країні діяла постанова Оперативно-аналітичного центру при президентові і Міністерства зв'язку та інформатизації Республіки Білорусь від 29.06.2010 №4/11 «Про

затвердження Положення про порядок обмеження доступу користувачів інтернет-послуг до інформації, забороненої до поширення відповідно законодавчих актів». Постанова приписувала провайдерам фільтрувати інтернет-контент відповідно до двох чорних списків url-адрес, один із яких перебував у публічному доступі, а інший був доступний тільки провайдерам (закритий список містив приблизно 80 url-адрес, доступ до яких державних, культурних і урядових закладів обмежувався, і містив популярні опозиційні сайти на кшталт Charter97.org і Belaruspartisan.org). У теперішній час відповідні обмеження реалізуються відповідно до указу президента Білорусі від 1 лютого 2010 року № 60 «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», декрету президента від 28 грудня 2014 року «Про невідкладні заходи з протидії незаконному обігу наркотиків» та закону Республіки Білорусь від 17 липня 2008 року «Про засоби масової інформації».

У березні 2010 року від білоруських провайдерів зажадали більш щільного співробітництва з державними системами спостереження (СОРМ), які здійснюють повний онлайн-нагляд по всій країні, що регламентується значною кількістю нормативно-правових актів. Як і в Росії та сусідніх країнах, СОРМ Білорусі з метою боротьби зі злочинністю дає виконавчим органам і органам національної безпеки можливість перехоплювати повідомлення з будь-яких комунікаційних каналів. Провайдери інтернет-послуг і оператори зв'язку зобов'язані встановлювати відповідне устаткування й надавати державним органам цілодобовий доступ до нього. Відповідно до указу «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет» № 60 [439] провайдери мусять вести облік Ір-адрес, а держава може витребувати інформацію щодо інтернет-діяльності будь-якого громадянина. З 2007 року до інтернет-кафе висувається вимога зберігати історію інтернет-активності користувачів протягом року й інформувати виконавчі органі про підозрілі дії. СОРМ працює здебільшого відповідно до законів «Про оперативно-розшукову діяльність», «Про органи державної безпеки Республіки Білорусь» та указу № 129 «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, що здійснюють оперативно-розшукову діяльність».

У Білорусі немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет. Білорусь також подавала заявку на приєднання до Конвенції про кіберзлочинність, прийнятої в Будапешті в 2012 році, що й визначило необхідність дотримуватися відповідних міжнародних стандартів. Такий крок Білорусі став вельми несподіваним, особливо в контексті їхніх тісних зв'язків з Росією, адже Китай і РФ виступили проти конвенції й висловилися на захист альтернативної концепції боротьби з кіберзлочинністю, за якою держава отримує значно більше повноважень, ніж це передбачається Будапештською конвенцією.

Розслідуванням комп'ютерних злочинів у Білорусі опікується спеціальне управління Міністерства внутрішніх справ, яке координує роботу з іншими виконавчими органами усередині країни й аналогічними міжнародними організаціями у США, Євросоюзі, країнах СНД та в інших державах. У суспільстві висловлюються непоодинокі підозри, що це управління займається переважно переслідуванням кримінальних правопорушників, а ніяк не розробкою законодавства з питань кібербезпеки, а також бере участь у переслідуванні та онлайн-відстеженні політичних активістів.

Що стосується участі Республіки Білорусь у забезпеченні кібербезпеки на регіональному рівні, то слід зауважити, що Рада голів держав Співдружності Незалежних Держав у 2013 році прийняла Концепцію співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій. Відповідно до цього документа країни-члени СНД обмінюються робочою, статистичною й методологічною інформацією та ведуть єдину базу даних щодо кіберзлочинців. На підставі цієї Концепції з 2015 року здійснюється розробка програми співробітництва між країнами СНД у боротьбі з кіберзлочинністю, яка підлягає затвердженню Радою міністрів країн СНД.

Також у 2017 році розпочато підписання нової Угоди про співробітництво держав-членів СНД у боротьбі зі злочинами у сфері інформаційних технологій.

3.3. Доктрина інформаційної безпеки в рамках НАТО.

8 червня 2017 року було прийнято Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України», яким внесено зміни до законів України «Про національну безпеку України» та «Про засади внутрішньої і зовнішньої політики» у частині євроатлантичної інтеграції. Одним із пріоритетів національних інтересів України цим законом визначено інтеграцію у євроатлантичний безпековий простір з метою набуття членства в Організації Північноатлантичного договору. Остаточно обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку країн Європи в інформаційній сфері. Найбільш успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства є країни Європи, що входять до НАТО.

Зазначені зміни в законодавстві свідчать про поглиблення співпраці України з НАТО задля набуття членства в цій організації. За таких умов набуває все більшого значення координація діяльності органів виконавчої влади, ЗМІ тощо з питань співробітництва з НАТО в інформаційній сфері. Цей вектор розвитку зовнішньої політики України впливає й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору, що, у свою чергу, потребує глибокого розуміння сутності політики інформаційної безпеки НАТО та інформаційної політики Альянсу в цілому.

Досліджуючи питання політики інформаційної безпеки НАТО в сучасних умовах, слід передусім з'ясувати сутність інформаційної політики цієї організації в цілому, а також питання забезпечення безпеки інформації та кібербезпеки у системі Альянсу.

Наразі регулювання інформаційної сфери у країнах НАТО здійснюється за такими напрямами:

1) заохочення конкуренції, боротьба з монополізмом та концентрацією ЗМІ;
2) забезпечення права і технічних можливостей для доступу до інформації та інформаційних ресурсів усього населення;
3) дотримання свободи слова;
4) захист інтересів національних меншин, національної культурної спадщини, мови, протистояння культурній експансії інших країн; захист молоді в інформаційній сфері;
5) охорона інтелектуальної власності, боротьба з піратством;
6) протидія кіберзлочинності; впровадження електронного урядування;
7) правове регулювання мережі Інтернет;
8) забезпечення інформаційної безпеки тощо.

Система інформаційної політики НАТО є похідною від реалізації демократичного принципу цивільного контролю над військово-політичною сферою в умовах участі громадськості в міжнародному військовополітичному процесі. З підвищенням суспільного інтересу до діяльності Альянсу на початку 1990-х років основна роль у провадженні інформаційної діяльності відводиться власним інститутам НАТО. Основним органом проведення інформаційної політики організації є Атлантична рада, яка оприлюднює свої рішення й заяви для преси та широкого загалу. Крім Атлантичної ради, інформуванням громадськості опікуються установи країн-членів НАТО.

Одну із провідних ролей у реалізації інформаційної політики Альянсу відіграє Бюро інформації та преси. Воно входить до числа структур відділу Генерального секретаря (після празького саміту 2002 року його функції виконує Департамент публічної дипломатії, який забезпечує інформаційну діяльність). У ході реалізації різних програм і заходів Бюро інформації та преси сприяє урядам країн-членів і держав-партнерів у розширенні розуміння громадськістю ролі й напрямків політики НАТО. Бюро підтримує тісні зв'язки з національними інформаційними органами й неурядовими організаціями та здійснює

заходи, спрямовані на роз'яснення громадськості цілей, завдань і досягнень НАТО.[23]

Якщо вести мову про забезпечення безпеки інформації, то слід зазначити, що при створенні НАТО в 1949 році системи безпеки країнучасниць істотно різнилися. Перша натівська система засекречування містила вісім рівнів таємності, була розроблена для документів у вигляді «твердих копій», а також передбачала створення в кожній країні двох центральних режимних органів і певну кількість підпорядкованих їм структур. На початку 1990-х років НАТО розпочала політичну та військову трансформацію структур безпеки, відчувши не тільки позитивні (скорочення часу обміну, збільшення місткості носіїв, швидкість пошуку, класифікацію, створення баз даних), а й негативні (втрата конфіденційності, цілісності змісту інформації або цілісності системи, втрата доступу) наслідки інформатизації. Виникнення нових загроз у сфері інформаційної безпеки зумовило необхідність осучаснення підходів до забезпечення безпеки інформації.

Засади політики НАТО щодо забезпечення безпеки так званої класифікованої інформації викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)». Класифікована інформація - термін, який використовується у законодавстві країнчленів НАТО стосовно частини «уразливої» (sensitive) інформації, тобто інформації, чутливої до загроз, що виникають у зв'язку з несанкціонованим доступом до неї, а тому потребує захисту або принаймні обмеження доступу до неї. НАТО має п'ять рівнів захисту інформації з обмеженим доступом: Cosmic TOP Secret (CTS), NATO Secret (NS), NATO Confidential (NC), NATO Restricted (NR), Unclassified but Sensitive. При цьому, у внутрішньодержавному законодавстві застосовують не більше трьох рівнів класифікації для інформації з обмеженим доступом, враховуючи інформацію з грифом, що відповідає рівню RESTRICTED і належить до офіційної, службової та громадської публічної таємниці. Певні термінологічні та сутнісні розбіжності у визначенні та класифікації інформації з обмеженим доступом в національному законодавстві країн НАТО компенсуються уніфікацією підходів до такої інформації у базових сферах діяльності держав-членів – військовій, економічній, правоохоронній та ін.

Документ СМ (2002)49 встановлює основні вимоги до системи забезпечення фізичної, організаційної, процедурної та технічної безпеки, зокрема й безпеки інформації. Дотримуючись спільних зобов'язань, кожна країна-член НАТО надає інформації з обмеженим доступом власну оцінку, і, залежно від того, як інші члени виконують прийняті на себе зобов'язання, визначає, яку саме інформацію зробити доступною Альянсу. Відтак, будь-яке відхилення одного чи декількох членів Альянсу від виконання їхніх зобов'язань може призвести до скорочення обсягу та якості переданої їм інформації. Зазначений документ проголошує п'ять основних принципів політики безпеки НАТО:

1) широти;
2) глибини;
3) централізації;
4) управління доступом;
5) персонального контролю.

Засадничим принципом безпеки інформації в системі НАТО є при цьому те, що інформація має зберігати свій ступінь захисту протягом усього циклу її обігу, починаючи від джерела. При цьому контроль за розподілом і поширенням інформації має унеможливити її витік.

Завдання, які пов'язані із забезпеченням захисту інформації входять до компетенції Комітету внутрішньої безпеки НАТО (NSC). Даний Комітет є дорадчим органом при Північноатлантичній Раді з питань, що стосуються безпеки НАТО. Усередині НАТО національний уповноважений орган з безпеки інформації виконує функції керівництва створенням органу правління та режимних відділів, забезпечення безпеки таємної інформації НАТО в усіх установах, що перебувають під її юрисдикцією, як усередині країни, так і за її межами, забезпечення розробки планів захисту інформації в разі виникнення надзвичайних обставин з метою запобігання втрати конфіденційності

інформації НАТО. Представники національного уповноваженого органа із забезпечення безпеки інформації беруть участь у нарадах Комітету безпеки НАТО, де виробляються політика й інструкції у безпековій сфері. На обсяг функцій відповідального уповноваженого впливають розмір і кількість населення країни, географія місць обробки таємної інформації й не в останню чергу розподіл повноважень між органами у сфері національної безпеки. В окремих країнах НАТО уповноважений орган з безпеки інформації входить до структури міністерств закордонних справ, оборони та юстиції, в інших країнах - його керівником є прем'єр-міністр або міністр внутрішніх справ.

Співробітництво між НАТО та країнами-партнерами, в тому числі з Україною, в рамках Ради євроатлантичного партнерства (РЄАП) та Програми «Партнерство заради миру» (ПЗМ) також передбачає певні зобов'язання сторін щодо обміну інформацією та забезпечення її безпеки. Зокрема, перед обміном будь-якою таємною інформацією між країноюучасницею ПЗМ і НАТО, органи, на які покладається забезпечення безпеки інформації, мають бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити її захист відповідно до вимог сторони, котра її передає.

Приєднання країни до програми ПЗМ передбачає ратифікацію Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або ПЗМ. Згідно з положеннями цієї Угоди сторони погоджуються консультуватися з політичних і безпекових питань, розширювати й інтенсифікувати політичне та військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах передбачає обмін учасників секретною інформацією або іншою інформацією з обмеженим доступом. Відповідальним органом при захисті інформації, якою обмінюються сторони при співробітництві в рамках РЄАП/ПЗМ, є NOS. Крім того, між НАТО та країною-партнером укладається окрема адміністративна угода щодо стандартів взаємного забезпечення безпеки інформації, якою обмінюються сторони, а також призначається офіцер зв'язку між NOS і національним органом з безпеки інформації. Всі дані, якими обмінюються сторони в рамках РЄАП/ПЗМ, є інформацією з обмеженим доступом і призначена тільки для урядового використання. На відміну від стандартів щодо захисту інформації, прийнятих в системі НАТО, в мінімальних стандартах з обробки і захисту таємної інформації, якою обмінюються сторони в рамках програм РЄАП/ПЗМ, немає рівня «цілком таємно», адже кількість такої інформації в системі НАТО вкрай обмежена, а додаткові вимоги із забезпечення безпеки інформації такого рівня таємності невиправдано ускладнили би процедуру взаємного обміну.

Україна також активне співробітничає в галузі безпеки інформації в рамках програми НАТО «Наука заради миру і безпеки» [321]. Щорічно затверджується й Річна національна програма під егідою Комісії Україна – НАТО. В умовах тимчасової окупації Росією Автономної

Республіки Крим та м. Севастополя, проведення в окремих районах Донецької та Луганської областей антитерористичної операції та загальної ситуації, що склалася внаслідок збройної агресії Росії проти України, Річна національна програма під егідою Комісії Україна – НАТО на 2017 рік мала особливе значення для забезпечення захисту національних інтересів і безпеки України, передусім у контексті використання потенціалу та практичної допомоги НАТО та держав – членів Альянсу у підвищенні обороноздатності України для протидії агресії Росії та реформування за стандартами НАТО сектору безпеки й оборони та оборонно-промислового комплексу.

Важливим завданням НАТО є недопущення актів агресії у кіберпросторі, адже кібератаки частішають та стають усе більш організованими та збитковими для державних установ, підприємств, об'єктів критичної інфраструктури, а також можуть сягнути критичного рівня, який загрожує національному та євроатлантичному процвітанню, безпеці та стабільності всього світового співтовариства. Джерелом таких атак можуть бути іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи. Так, П.Корніш з лондонського Королівського інституту іноземних справ пропонує таку класифікацію інформаційних загроз: діяльність хакеріводинаків;

організована злочинність у глобальних мережах; ідеологічний і політичний екстремізм; інформаційна агресія держав. При цьому, в системі НАТО під кібербезпекою розуміється підтримка стану готовності до протидії потенційним загрозам високої інтенсивності та вжиття наступальних контрзаходів.

Незважаючи на те, що НАТО з часів створення постійно захищає свої інформаційні системи, на Празькому саміті 2002 року це питання було винесене до кола політичних. Беручи до уваги технічний прогрес, досягнутий після Празького саміту, лідери країн Альянсу на Ризькому саміті у 2006 році ще раз визнали необхідність забезпечення кібернетичної безпеки. Водночас, перед кібернападами на Естонію в 2007 році діяльність НАТО в галузі кіберзахисту зосереджувалася переважно на захисті комунікаційних систем, які належали Альянсу та використовувалися його членами. Кібернапади 2007 року змусили НАТО серйозніше замислитися над проблемами забезпечення безпеки кіберпростору, зокрема, сприймати загрози, що походять з Інтернет-простору, як стратегічно важливі. Надалі НАТО провела ретельну оцінку свого підходу до кіберзахисту, за результатами якої в жовтні 2007 року була підготовлена доповідь міністрам оборони країн-членів з рекомендаціями щодо конкретних завдань НАТО, а також нових заходів з удосконалення захисту від кібернападів. Офіційна політика НАТО у сфері кіберзахисту (NATO Cyber Defence Policy) була схвалена міністрами оборони держав-членів і представлена учасникам організації у квітні 2008 р. на саміті в Бухаресті. Її мета – «забезпечити можливості для надання підтримки країні-союзниці, на її вимогу, у протидії кібератаці».

Кількість та складність кібернападів швидко збільшувалася після нападів на Естонію в 2007 році, а вже влітку 2008 року війна РФ проти Грузії продемонструвала, що кібернапади стали основною складовою воєнних дій із застосуванням традиційної зброї. Тож у 2010 році на Лісабонському саміті НАТО було вирішено розробити нову політику організації з питань кіберзахисту, а також конкретний план дій, який набув чинності з червня 2011 року. В рамках їх реалізації НАТО використовує процеси оборонного планування з метою сприяння розвитку захисту союзників від кіберзлочинності, а також для оптимізації взаємодії, співробітництва та обміну інформацією. З питань протидії небезпекам, що виникають у кіберпросторі, НАТО тісно співпрацює за країнами ЄС та з ООН.

У цьому контексті слушно зауважує В. Пилипчук про те, що Латвія, Литва та Естонія змогли протистояти спробам втручання РФ у внутрішні справи завдяки набуттю членства у ЄС і НАТО.

У Стратегічний концепції та Декларації Лісабонського саміту зазначається, що швидкий розвиток та постійне ускладнення кібернападів роблять захист інформаційно-комунікаційних систем країн-членів НАТО таким, від якого залежить майбутня безпека організації, а інформаційні атаки фігурують серед найнебезпечніших викликів і загроз безпеці та процвітанню держав-членів Альянсу. В ієрархії викликів, перелічених у вказаній концепції, загрози, які походять з інформаційного простору, розташовані одразу ж після поширення зброї масового знищення й тероризму. Така увага зумовлена, зокрема, феноменом секьюритизації, завдяки якому кібербезпека «еволюціонувала з технічної дисципліни у стратегічний концепт». Сьогодні НАТО забезпечує розвиток засобів запобігання, виявлення, реагування й відновлення після атак за допомогою створених Органу з управління кібернетичною безпекою, Спільного Центру передового досвіду з кіберзахисту і Сил реагування на комп'ютерні інциденти.

Орган з управління кібернетичною безпекою (ОУКБ) відповідає виключно за узгодження діяльності в галузі кіберзахисту в межах організації. ОУКБ НАТО керує Комісія з управління діяльністю в галузі кіберзахисту, до складу якої входять керівники політичних, військових, оперативних і технічних органів НАТО, які відповідають за питання кіберзахисту. Вона є основним консультативним органом

Північноатлантичної ради з питань кіберзахисту та надає поради країнамчленам організації з усіх аспектів кіберзахисту. ОУКБ НАТО входить до складу Управління нових

викликів безпеці Штаб-квартири НАТО. Центр передового досвіду в галузі кіберзахисту (м. Таллінн), який одержав у жовтні 2008 року акредитацію при НАТО, не наділений оперативними функціями і виступає в ролі дослідницького й навчального центру, де розробляються доктринальні й концептуальні засади кібербезпеки. Він позиціонується як «головне джерело експертизи у сфері спільної кібероборони», яке «акумулює, створює й поширює знання з ключових питань кібербезпеки усередині НАТО, між державами Альянсу і його партнерами». Центр здійснює наукові дослідження та підготовку з питань ведення інформаційних операцій у віртуальному просторі. За підтримки з боку Комітету з планування використання цивільних систем зв'язку, Центру передового досвіду в галузі боротьби з тероризмом (м. Анкара), а також програми НАТО «Наука заради миру і безпеки» Центр передового досвіду в галузі кіберзахисту проводить експертні перемови, навчальні семінари та обміни інформацією із зацікавленими партнерами й міжнародними організаціями (приміром, з ЄС та ОБСЄ). У 2015 році Центр опублікував книгу про кібервійну Росії проти України під назвою «Cyber War in Perspective: Russian Aggression against Ukraine», де проведено аналіз поточної діяльності у сфері захисту інформації та стратегічних і тактичних наслідків кібервійни. На сторінках цього видання експерти, зокрема, зазначають, що поняття «кібератака» включає наразі цифрову пропаганду, DDoS-кампанії, дефейси web-сайтів, витоки інформації внаслідок атак, використання шкідливого програмного забезпечення з метою шпигунства. Британський експерт Р.Хьюз розглядає ОУКБ та талліннський Центр як елементи єдиної організаційної системи, де перший наділений «широкими можливостями щодо здійснення електронного моніторингу в «реальному часі» та діє на оперативнотактичному рівні, тоді як Центр, розробляючи довгострокову доктрину НАТО, становить «інтелектуальну платформу» і є елементом стратегічного рівня. У теперішній час експерти Центру розглядають мілітаризацію Інтернету як однин з найнебезпечніших трендів світового кіберпростору.

У заяві, оприлюдненій за результатами Варшавського саміту глав держав та урядів, які брали участь у засіданні Північноатлантичної ради у липні 2016 року, зазначається, що кібернапади становлять очевидний виклик безпеці Альянсу й можуть бути не менш згубними для сучасних суспільств, ніж напади із застосуванням звичайних видів зброї. Відтак, кіберзахист є частиною головного завдання НАТО – колективної оборони, а кіберпростір визнається сферою операцій, де НАТО має захищати себе так само ефективно, як робить це у повітрі, на землі та на морі. Це підвищить спроможність НАТО щодо захисту та проведення операцій у цих сферах, збереже свободу дій та рішень у будь-яких умовах та сприятиме забезпеченню НАТО ширшими можливостями стримування та оборони.

НАТО розвиває співробітництво з кіберзахисту відповідно до Вказівок щодо співпраці з кіберзахисту з партнерами та міжнародними організаціями 2008 року та Рамкового документу щодо співпраці з кіберзахисту між НАТО та країнами-партнерами 2009 року, визнаючи необхідність визначення спільних підходів до використання сучасних систем захисту інформації з урахуванням вимог інформаційної безпеки. Забезпечення безпеки інформації в разі створення спільних інформаційних та телекомунікаційних систем, де циркулює інформація з обмеженим доступом, відбувається шляхом розроблення пропозицій щодо захисту конфіденційного зв'язку з використанням обладнання НАТО, необхідного для створення відокремлених інформаційно-комунікаційних систем в органах влади, а також підвищення кваліфікації їх фахівців з питань захисту інформації у рамках ПЗМ.

НАТО також усвідомлює необхідність посилення моніторингу критично важливих мереж у межах Альянсу та усунення виявлених недоліків. З цією метою талліннський Центр організує навчання та надає допомогу країнам-членам у поліпшенні програм кіберзахисту, а союзники мають розширювати свої засоби раннього попередження у формі загальної мережі моніторингових вузлів і сенсорів. НАТО застосовує процес оборонного планування задля сприяння розвитку можливостей кіберзахисту союзників, надання допомоги окремим країнам-членам та оптимізації обміну інформацією, співпраці та взаємосумісності. У

зв'язку з підвищенням небезпеки кібератак НАТО визначає вимоги для всіх країн, зацікавлених у збереженні цілісності, непорушності та конфіденційності їхнього інформаційного простору. Зокрема, інформаційна структура країн-членів Альянсу має постійно вдосконалюватися, темпи розвитку новітніх інформаційних технологій та їх поширення мають прискорюватися. Потрібен також розвиток систем електронної сертифікації та криптографії, належна підготовка персоналу. Формування й реалізація єдиної державної політики в контексті забезпечення безпеки національних інтересів від загроз в інформаційній сфері має стати одним із пріоритетних напрямків розвитку кожної держави. Розвиток індустрії інформаційних та телекомунікаційних засобів, поширення їх на внутрішньому медіа-ринку, модернізація систем теле- і радіомовлення, оновлення технічної бази для забезпечення захисту інформації також є важливими заходами на шляху до забезпечення інформаційної безпеки.

Унаслідок нападів, спрямованих проти державних органів та здійснених за допомогою мережі Інтернет, увага НАТО поширилася на питання кіберзахисту окремих країн-членів. Альянс не виключає необхідності швидкого реагування на кібернетичні атаки шляхом надсилання групи експертів до будь-якої країни-члена, котра постраждала від кібернападу, або до країни, яка відчуває загрозу вторгнення у її інформаційний простір. Проте основну роль у захисті та безпеці власних комунікаційних систем продовжують відігравати самі союзники. Від них НАТО вимагає надійної та безпечної допоміжної інфраструктури, тому продовжуватиме працювати з національною владою над розробкою принципів і критеріїв забезпечення мінімального рівня кіберзахисту там, де національні мережі й мережі НАТО взаємопов'язані. З часом НАТО планує повністю забезпечити себе відповідним набором засобів кіберзахисту, включно з пасивними та активними елементами. З метою подолання ризиків безпеці, що виникають у кіберпросторі, НАТО також тісно співпрацює з іншими організаціями.

Проблема забезпечення інформаційної безпеки НАТО, крім питань технічного забезпечення й стратегічного планування, має також і політичний вимір. Передусім це стосується можливості застосування статті 5 Вашингтонського договору до інформаційних атак. Основними протагоністами розширення дії принципу колективної відповідальності у сфері забезпечення інформаційної безпеки в системі НАТО виступають Естонія й, до певної міри, США. Зокрема, професор Дж. Голдгейєр відзначає, що за своїм визначенням кібератаки не є «збройним нападом», тобто не підпадають під дію ст. 5, однак робить висновок, що Альянс «має об'єднатися у протидії атакам, що загрожують безпеці будь-кого із членів НАТО» [340]. Варто зазначити, що питання протидії загрозам інформаційній безпеці, зокрема й кібербезпеці, відносять до сфери «м'якої безпеки» (soft security), тоді як головним завданням НАТО традиційно вважається протидія конвенційним викликам безпеки – забезпечення «жорсткої безпеки» (hard security). Тому ще одним проблемним чинником, котрий проявляється на трансатлантичному рівні, є «поділ праці» між членами НАТО, внаслідок якого одні країни спеціалізуватися на темах «м'якої безпеки», а інші проводять «тверді» військові місії. Наслідком цього є розбіжність у підходах протидії: США, Франція, Велика Британія й Німеччина зіставляють інформаційну безпеку з військовою стратегією, натомість Естонія, котра не володіє потужним військовим потенціалом, наголошує на провідній ролі громадянського суспільства та приватного сектору.

Лекція 2

Тема 4. Протистояння інформаційним війнам як складова інформаційної безпеки.

8.1.Інформаційна війна та інформаційна боротьба: основні поняття.

8.2. Форми та способи ведення інформаційної боротьби.

8.3. Психологічна і кібернетична війна як складові інформаційної війни. Інформаційна зброя і технології її використання.

4.1.Інформаційна війна та інформаційна боротьба: основні поняття.

Ключовим елементом у теоретичній моделі є поняття **інформаційна онлайн мережева війна** (IOMB)**,** що визначається, як комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних перваг у економічних, військових, політичних, культурних та громадських протистояннях.

В своїй основі IOMB має три ключові технологічні аспекти: хай-тек, хайх'юм та хай-сенсоро. Кожен з цих аспектів має власні технології, які формують профільні напрямки дослідження та практичної роботи (див. мал. 1.34.).

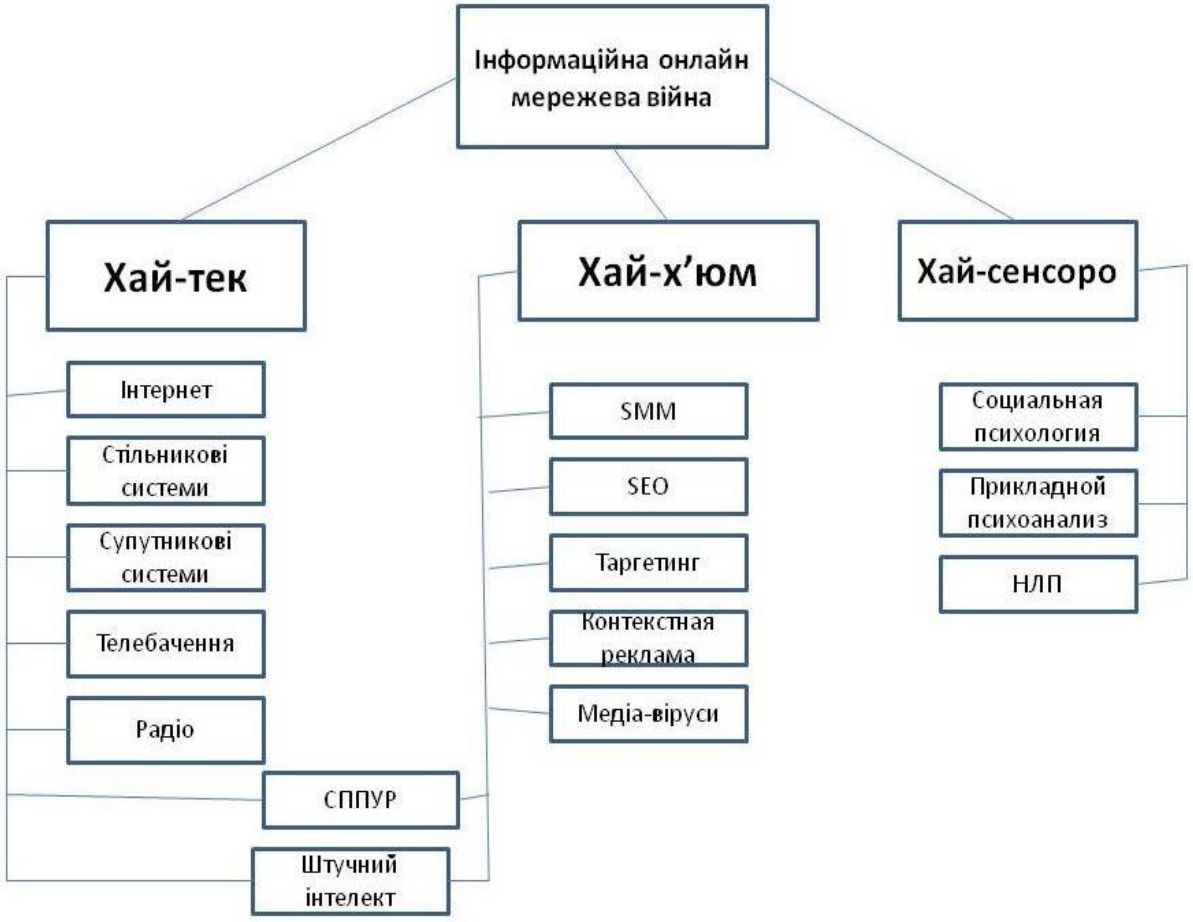
Хай-тек в IOMB – сучасні високі техногії цифрових комунікацій, що в основі мають системи телебачення, радіо, Інтернет, месенджерів, стільникової, супутникової та інших видів сучасного зв'язку та базуються на таких гаджетах, як стаціонарні комп'ютерні пристрої, планшети, смартфони, пристрої індивідуального та групового зв'язку.

До цього аспекту відноситься класичне *телебачення,* в ефірному та цифровому форматах. Останне визначають, як технологію трансляції телевізійного зображення та звуку за допомогою кодування відеосингалу та сигналу звуку із використанням цифрових каналів за стандартом MPEG.

Радіо, як класичне електронне ЗМІ, розглядається у традиційному аналоговому (AM, FM) та цифровому форматах. Останній визначається, як технологія трансляції сигналів радіостанцій в цифровій формі за допомогою електромагнітних хвиль радіодіапазона.

Інтернет, в контексті досліджуваної теми розглядається, як всесвітня система об'єднаних комп'ютерних мереж для зберігання та транслювання інформації. На основі цієї мережі, як комунікаційної платформи формуються типові поштові сервіси, сервери зберігання даних, а також нові формати мережевого телебачення та радіо.

Мал.1. Модель інформаційної онлайн мережевої війни



При цьому *інтернет-телебачення* визначається, як телебачення міжмережевого протоколу (on-line TV) — система, що базується на двустороньому цифровому переданні телевізійного сигналу через інтернетз'єднання за допомогою широкополосного підключення.

Інтернет-радіо або веб-радіо, визначають як групу технологій трансляції потокових аудіоданих через мережу Інтернет для здійснення широкої трансляції програм. Також, в якості терміна інтернет-радіо визначається радіостанція, що використовує для трансляції технологію потокового віщання у глобальній мережі Інтернет.

Месенджери – мережі миттєвого з'єднання. Типовими прикладами таких технологій є WhatsApp, Facebook Chat, Hangouts (Google), Skype, LINE, WeChat, Viber, Kik, Snapchat, ICQ, Telegram.

Стільниковий звязок – один з різновидів мобільного зв'язку, в основі якого закладено стільникову мережу. Ключова особливість полягає в тому, що спільна зона покриття поділяється на ланки (соти), що визначаються зонами покриття окремих базових станцій. Соти частково перекриваються створюючи мережу.

Супутниковий зв'язок (радіо та телебачення) - один з різновидів космічного радіозв'зку, що базується на використанні штучних супутників в якості ретрансляторів. Цей зв'язок здійснюється між наземними станціями, що є стаціонарними або мобільними. Супутниковий зв'язок є продовженням розвитку традиційного радіорелейного зв'язку шляхом винесення ретранслятора на велику висоту.

Хай-х'юм в ІОМВ – сучасні високі соціально-гуманітарні технології створення, зберігання, розповсюдження та пошуку інформації. До них відноситься SMM, SEO, таргетинг, контекстна реклама, медіа-віруси та ін.

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації,

орієнтований на підвищення позиції веб-сайту у пошукових системах.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунта або окремого контенту в соціальних мережах.

Таргетинг – рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення.

Контекстна реклама – метод розміщення інформації, що орієнтована на зміст інтернет-ресурсу, представлена у вигляді банеру чи текстового повідомлення.

Медіа-віруси – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть в прихованому вигляді завуальовані ідеї та меседжі.

Хай-сенсоро в ІОМВ - сучасні високі психотехнології, що дають можливість регулювати та керувати соціальними комунікаційними процесами на рівні соціальних груп та окремих індивідуумів. Типовими в цьому аспекті є соціальна психологія, прикладний психоаналіз та НЛП.

Соціальна психологія – галузь в психології, що орієнтована на вивчення принципів та закономірностей діяльності людини в умовах взаємодії в соціальних групах. Основні проблеми соціальної психології: закономірності спілкування та взаємодії людей, діяльність великих (нації, класи) і малих соціальних груп, соціалізація особистості та розвиток соціальних установок.

Прикладний психоаналіз – напрямок знань в психології, що досліджує практику використання ідей та концепцій орієнтованих на досягнення глибокого розуміння різноманітних аспектів людської природи, культури та суспільства. Найбільша кількість досліджень, в цьому плані припадає на галузі історії, біографії, літератури, мистецтва, релігії, міфології та антропології.

Нейро-лінгвістичне програмування – технологія моделювання вербальної та невербальної поведінки людей за допомогою поєднання форм мовлення, руху очей, тіла та пам'яті.

В структурі зазначеної моделі існують елементи, що мають ознаки двох аспектів. Це Системи підтримки прийняття управлінський рішень (СППУР) та Системи штучного інтелекту. Вони мають характерні ознаки хай-тек та хайх'юм.

Кожен з зазначених аспектних напрямків має свої методологічні складові та прикладні інструменти, що в комплексі формують сучасну систему управління інформаційно-комунікаційними процесами, в форматі економічних, політичних, військових, культурних та громадських конфліктів.

міємо докорінну зміну методів створення, накопичення, зберігання, п Основою будь-якого інформаційного протистояння є інформаційний процес, що визначається як діяльність із створення, накопичення, зберігання, пошуку та розповсюдження відомостей або даних певного тематичного характеру.

Базовими поняттями для вивчення сучасних мережевих інформаційних протистоянь є інформація та комунікація, які формують основу всього того, що в подальшому розглядається як інформаційна війна.

Інформацію розуміють як відомості або дані про навколишнє середовище, що оточує людину. А комунікація - це процес передання або обміну інформацією .

У різні епохи інформаційні процеси носили в собі відбитки тих технологій, які було винайдено на певному етапі. Це позначалося на особливостях проведення відповідних інформаційних протистоять.

Кожен з таких винаходів за історичною значущістю та технічними характеристиками можна визначити або як інформаційний вибух, або як інформаційну революцію.

Під поняттям інформаційна революція ми розу ошуку та поширення інформації . До таких явищ можна віднести появу мовлення, писемності, комп'ютерної техніки. Всі ці винаходи були початком принципово нового напрямку розвитку інформаційно-

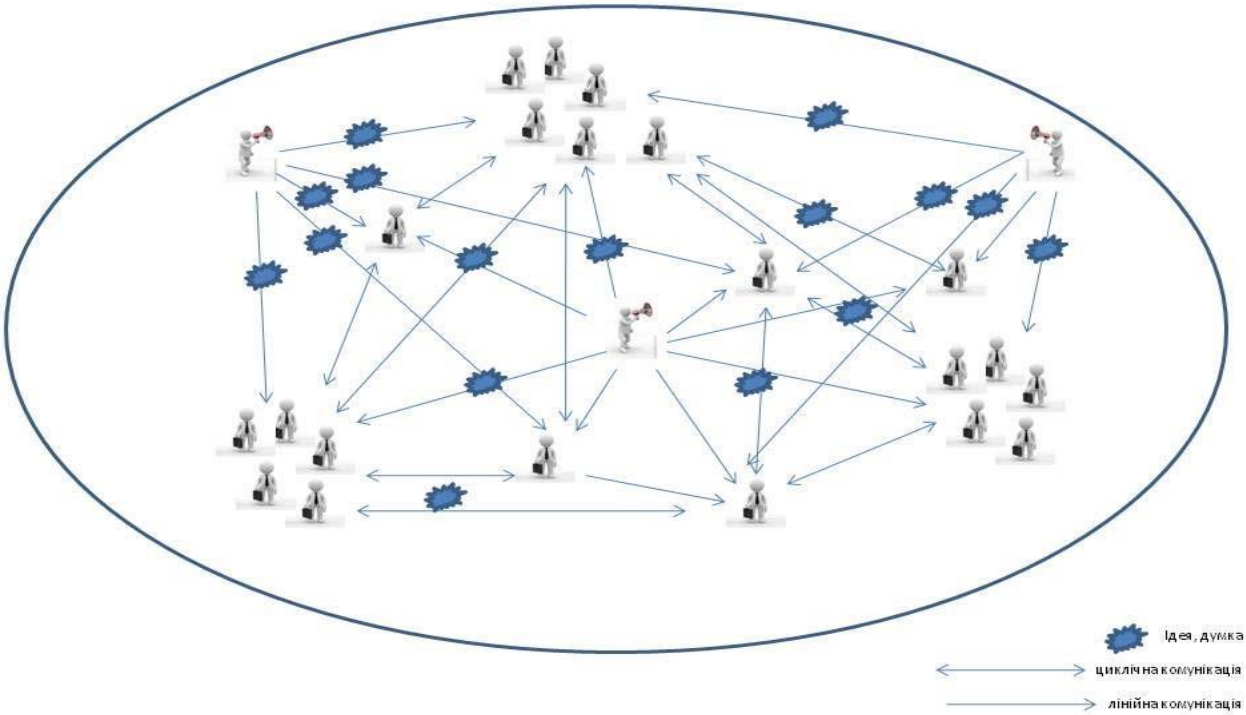
комунікаційних технологій.

За визначенням, інформаційний вибух – це суттєве прискорення процесів створення, накопичення, пошуку та поширення інформації. Типовим прикладом останнього є винайдення абеткової писемності (як модернізація системи писемності), друкарства (оптимізація писемних процесів), Інтернету (еволюція комп'ютерних технологій).

Будь-які інформаційні процеси відбуваються в певних площинах або теренах, які можна узагальнити в рамках поняття інформаційне поле. Останнє визначається, як соціальний або географічний простір, у межах якого відбуваються типові комунікаційні процеси, які охоплюють їх учасників

(суб'єкти) на основі обміну інформацією (об'єкт) (мал. 1.35).

Мал. 1.35. Інформаційне поле



До цього аспекту відноситься класичне телебачення, в ефірному та цифровому форматах. Останне визначають, як технологію трансляції телевізійного зображення та звуку за допомогою кодування відеосингалу та сигналу звуку із використанням цифрових каналів за стандартом MPEG.

Радіо, як класичне електронне ЗМІ, розглядається у традиційному аналоговому (AM, FM) та цифровому форматах. Останній визначається, як технологія трансляції сигналів радіостанцій в цифровій формі за допомогою електромагнітних хвиль радіодіапазона.

Інтернет, в контексті досліджуваної теми розглядається, як всесвітня система об'єднаних комп'ютерних мереж для зберігання та транслювання інформації. На основі цієї мережі, як комунікаційної платформи формуються типові поштові сервіси, сервери зберігання даних, а також нові формати мережевого телебачення та радіо.

Лінійна модель комунікації передбачає однобічний, цілеспрямований процес передання інформації від автора повідомлення до отримувача. На першому етапі у

свідомості автора з'являється певна ідея (думка) яку він, на другому етапі, перетворює на інформацію шляхом кодування – матеріалізації ідеї у вигляді слова, тексту, малюнка, звука. Сформована таким чином інформація (контент) на третьому етапі транслюється через посередника (технічні засоби комунікації або інша особа) або особисто автором (артикуляція або демонстрація). На четвертому етапі повідомлення досягає отримувача, який його декодує (читає, переглядає, прослуховує) для того, щоб зрозуміти базову ідею (думку), яка була закладена автором повідомлення. Надіслану ідею отримувач обробляє та формує власне судження з цього приводу у вигляді певної ідеї. На цьому процес лінійної комунікації закінчується.

У разі, якщо отримувач інформації має намір відреагувати на повідомлення, він спрямовую свою думку, на основі отриманої ідеї автору, застосовуючи той же самий механізм. Він кодує свою думку, транслює її, потім відбувається її декодування та сприйняття. Це циклічна модель комунікації, яка передбачає взаємний обмін інформацією, в процесі якого учасники комунікації поступово змінюють ролі автора та отримувача повідомлення

(мал. 1.36).

Мал. 1.36. Базовий комунікаційний процес

Базовими сферами застосування сучасної інформаційної війни є: політична, дипломатична, військова, фінансово-економічна. Інформаційні протистояння в цих сферах, за структурою, виглядають як ***циклічний або лінійний обмін інформацію, яка може/має спричинити певну шкоду отримувачу, а автору надати певну перевагу***. Саме в цьому і полягає сутність **сучасної інформаційної війни**.

Базовою методологічної основою сучасних інформаційних протистоянь є **маніпуляція** - ***засіб психологічного впливу, що застосовується задля прихованого проникнення в психіку жертв із метою занесення цілей, бажань, намірів, відносин або установок маніпулятора*** [152, с.59]. Фактично це приховане управління людьми та їх поведінкою.

Головним форматом здійснення інформаційних протистоять є поняття **інформаційна зброя** або **інформаційна атака**. Останні розуміють як ***здійснення тимчасового або остаточного виведення з ладу систем та підрозділів противника, що відповідають за процеси управління та інформування*** [152, с.35].

Головною метою інформаційної атаки є ***отримання суттєвих переваг в реальному військовому, економічному або політичному протистояннях***

[152, с.36].

Традиційним базовим інструментом інформаційного протистояння є **медіа**, які здійснюють посередницьку функцію із трансляції ідей та думок у вигляді конкретних меседжів, між автором повідомлення та отримувачем. Медіа ***розуміють як канали та***

засоби зберігання, передачі і подання інформації або даних [217, с.168]. Фактично до медіа можна віднести будьякий інформаційний носій, що виконує означені функції. Разом з тим існує ще таке поняття як **мас-медіа**, яке іноді ототожнюють із поняттям медіа. Втім масмедіа мають дещо конкретніші обриси і визначається як: ***технології та засоби трансляції інформації від конкретного джерела на широку аудиторію, яка обмежується рамками певного інформаційного поля в якому ці мас-медіа діють*** [48, с. 126].

Типові мас-медіа поділяються на три групи, за специфікою функціонування [217, с.168].

- друкована преса (газети, журнали, бюлетені та ін.);
- аудіовізуальні (радіо, телебачення, Інтернет);
- інформаційні служби (агенції, прес-служби, прес-бюро, центри громадських зв'язків тощо);
- рекламно-інформаційні носії (зовнішня реклама, візуальна реклама та ін.);
- засоби маскультури (кіно, театри, концерти та ін.)

За регіональним розповсюдженням мас-медіа поділяються на [217, с.168]:

- транснаціональні (на міждержавному рівні);
- національні (в кордонах певного державного утворення);
- регіональні (окрема територіально-адміністративна зона);
- місцеві (прив'язані до конкретної місцевості – місто, район, село або окрема організація).

Здобутком XX ст. стало народження нового формату інформаційнокомунікаційних протистоянь, який отримав назву **кібервійна**. Останню розуміють як ***боротьбу сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних засобів противника з метою отримання суттєвих переваг у економічних, політичних та військових протистояннях*** [152, с. 38]**.**

Головними діючими особами в такій війні є спеціальні фахівці: **хакери** (ті, що видобувають інформацію) та **кракери** (ті, що псують програмноапаратні засоби).

У форматі кібервійни визначаються наступні види [152, с. 38]:

- вандалізм – псування інтернет-сторінок, зміна змісту негативними або пропагандистськими матеріалами;
- пропаганда – поширення звернень, що закликають до певних дій, або розміщення відповідної інформації на чужих інтернетмайданчиках;
- збирання інформації – зламування сторінок приватних осіб або окремих організацій для отримання закритої інформації
- від втручання в роботу програмно-апаратного забезпечення – dDoss атаки на комп'ютери, що виконують адміністративно-контрольні функції в державних, громадських, військових та комерційних організаціях;
- атаки на мережеву інфраструктуру – напад на комп'ютери, що контролюють життєдіяльність міст, зокрема телефонних ліній, водопостачання, електропостачання, пожежної безпеки, транспортного сполучення та ін.

З народженням інтернет-технологій web 2.0 формується новий напрямок інформаційних конфліктів – **мережева війна**. Це поняття містить таке визначення, як: ***інформаційно-комунікаційне протистояння у форматі офлайн та он-лайн мережевих структур.***

Типовими **оф-лайн мережевими структурами** вважаються ***організації або тимчасові/ситуативні об'єднання індивідуумів на основі спільної діяльності або загальних інтересів***.

До **он-лайн мережевих структур** відносяться ***інтернет-ресурси формату WEB***

2.0-3.0 – віртуальні соціальні мережі (VKontakte, Facebook та ін.).

Провідне значення в теорії, методології та методиці ведення сучасних інформаційних війн посідає поняття **гібридна війна**. Таку війну розуміють, як: ***засіб протистояння, який поєднує в собі комплекс різноманітних інструментів політичного, економічного, військового та ідеологічного характеру***. Іноді для визначення цього явища застосовують такий термін, як: **асиметрична війна**. Це визначення підкреслює та визначає нетрадиційний специфічний креативний характер протистояння, що відбувається за допомогою нестандартних комбінованих стратегії та тактики ведення конфлікту. Під час такої війни ресурси та характер дій противників відрізняються один від одного. Головна мета – шляхом певної концентрації компенсувати недостатність ресурсів і можливостей однієї із сторін або отримання суттєвої переваги по конкретному напрямку в рамках конфлікту.

Полем застосування інструментів гібридної/асиметричної війни є: населення конфліктної зони, тилове населення, міжнародна спільнота.

Формат ведення такого виду війни:

- громадські заворушення – акції громадської непокори, демонстрації, блокування, вуличні зіткнення;
- повстання – відкритий військовий виступ проти офіційної влади;
- партизанський рух – прихований збройний опір офіційній владі;
- тероризм – організація та здійснення гучних вбивств, підривання транспортних засобів, споруд, місць масових соціальних контактів (он-лайн та оф-лайн);
- громадянська війна – військові дії між прихильниками різних ідеологічних, територіальних або національних груп у межах однієї держави.

2. Плани практичних (семінарських) занять, завдання для самостійної роботи та поточного контролю знань, умінь та навичок студентів

Тема 1. Поняття, предмет та завдання курсу

Мета теми: створити стійке уявлення слухачів про зміст та завдання дисципліни, залучити до наукового дослідження окремих питань теми та творчої діяльності.

Питання для самостійного вивчення:

1. Розширене тлумачення безпеки в індустріальному і постіндустріальному суспільстві.
2. Інформаційне суспільство.
3. Політичні ризики і загрози інформаційному суспільству, проекція на військову сферу.
4. Інформатизація і глобалізація, революція у військовій справі.
5. Трансформація сучасного суспільства.
6. Роль інформації сучасному суспільстві.
7. Інформатизація як засіб організації сучасного суспільства..

Завдання. Студенти готують короткі есе на наведені питання у плані теми. Потім по черзі обґрунтовують свою точку зору. Після обговорення кожного питання викладач підводить підсумки.

Теми рефератів.

1. Інформаційне суспільство: загальна характеристика та специфіка сучасного існування.
2. Вплив інформатизації на процеси глобалізації сучасного світу.
3. Політичні та економічні ризики інформатизації.

Література:

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с
2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.
3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.
4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/
5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.
6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

Тема 2. Теоретичні концепції інформаційної безпеки в міжнародних відносинах

Мета практичного заняття: сформулювати у студентів знання щодо теоретичних підходів вивчення інформаційної безпеки в міжнародних відносинах.

Практичне заняття: 2 год.

План практичного заняття:

1 Теорія інформаційної зброї.

2. Концепції інформаційної безпеки як стратегії національної безпеки та оборони інформаційно-розвинутих країн світу.

3. Прогнозування глобальних інформаційних конфліктів.

Завдання. Студенти готують відповіді на наведені питання у плані практичного заняття. Потім по черзі обґрунтовують свою точку зору. Після обговорення кожного питання викладач підводить підсумки.

Теми рефератів.

1. Можливі інформаційні конфлікти в Європі
2. Можливі інформаційні конфлікти в Америці
3. Можливі інформаційні конфлікти в Азії.

Питання для самостійного вивчення:

1. Голобальні конфлікти та інформаційні війни
2. Інформаційна безпека в умовах глобалістики.

Література:

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с
2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.
3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.
4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkik

h_infovoyn/

5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.

6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

Тема 3. Інституційні основи міжнародної інформаційної безпеки

Мета практичного заняття: сформулювати у студентів знання щодо інституційних основ міжнародної інформаційної безпеки..

Практичне заняття: 4 год.

План практичного заняття:

1. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.
2. Міжнародні угоди з питань міжнародної безпеки.
3. Вплив ІКТ на проблему інформаційної безпеки.
4. Еволюція нормотворчої діяльності ООН у сфері міжнародної інформаційної безпеки.
5. Проблема ухвалення «Міжнародної конвенції з інформаційної безпеки».

Завдання. Студенти готують відповіді на наведені питання у плані практичного заняття. Потім по черзі обґрунтовують свою точку зору. Після обговорення кожного питання викладач підводить підсумки.

Питання для самостійного вивчення:

1. Вплив ІКТ на проблему інформаційної безпеки.
2. Еволюція нормотворчої діяльності ООН у сфері міжнародної інформаційної безпеки.
3. Проблема ухвалення Міжнародної конвенції з інформаційної безпеки.
4. Інформаційна безпека у програмах і практиці діяльності європейських регіональних організацій.
5. Концепція інформаційної безпеки в рамках ЄС.
6. Доктрина інформаційної безпеки в рамках НАТО.
7. Інформаційна безпека у програмах ОБСЄ.

Завдання. Студенти обирають одне із питань і готують письмову роботу з одного з питань.

Література:

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с

2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.

3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.

4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkik h_infovoyn/

5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.

6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних

відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

Тема 4. Протистояння інформаційним війнам як складова інформаційної безпеки

Мета практичного заняття: сформулювати у студентів знання та навички щодо протистояння інформаційним війнам як складової інформаційної безпкеи.

Практичне заняття: 2 год.

План практичного заняття:

1. Інформаційна війна та інформаційна боротьба: основні поняття.
2. Форми та способи ведення інформаційної боротьби.

Завдання. Студенти готують відповіді на наведені питання у плані практичного заняття. Потім по черзі обґрунтовують свою точку зору. Після обговорення кожного питання викладач підводить підсумки.

Питання для самостійного вивчення:

1. Психологічна і кібернетична війна як складові інформаційної війни.
2. Інформаційна зброя і технології її використання.

Література:

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с

2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.

3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.

4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/

5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.

6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

Тема 5. Інформаційна безпека України у контексті міжнародних відносин

Мета практичного заняття: сформулювати у студентів знання та навички щодо формування державної політики інформаційної безпеки України.

Практичне заняття: 2 год.

План практичного заняття:

1 Доктрина інформаційної безпеки України.

Завдання. Студенти готують відповіді на наведені питання у плані практичного заняття. Потім по черзі обґрунтовують свою точку зору. Після обговорення кожного питання викладач підводить підсумки.

Питання для самостійного вивчення:

1. Українські ініціативи в області МІБ, історія їх висунення і просування.

Література:

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с

2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.

3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.

4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/

5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.

6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

3. Завдання для підсумкового контролю знань, умінь та навичок студентів, семестрових екзаменів (залікових робіт)

1. Розширене тлумачення безпеки в індустріальному і постіндустріальному суспільстві.
2. Інформаційне суспільство.
3. Теоретичні концепції інформаційного суспільства.
4. Політичні ризики і загрози інформаційному суспільству, проекція на військову сферу.
5. Інформатизація і глобалізація, революція у військовій справі.
6. Вплив інформаційної революції на систему міжнародної безпеки.
7. Міжнародні програми миру і стабільності у контексті потенційних глобальних інформаційних конфліктів.
8. Позиція ООН щодо проблеми міжнародної інформаційної безпеки.
9. Глобалізація інформації як актуальна проблема міжнародних відносин.
10. Критерії глобалізації.
11. Інформація як стратегічний ресурс людства і як стратегічний ресурс держави.
12. Інформація як глобальна проблеми сучасності.
13. Політичні ризики і загрози інформаційному суспільству, проекція на військову сферу.
14. Інформатизація і глобалізація, революція у військовій справі.
15. Теорія інформаційної зброї.
16. Концепції інформаційної безпеки як стратегії національної безпеки та оборони інформаційно-розвинутих країн світу.
17. Прогнозування глобальних інформаційних конфліктів у театрі воєнних дій.
18. Інформаційні війни
19. Сучасні інформаційні загрози (кібер, медіа та психотероризм, інформаційна злочинність).
20. Типологія інформаційних озброєнь.
21. Спеціальні інформаційні операції: методика та методологія здійснення.
22. Аналіз впливу спеціальних інформаційних операцій на міжнародні відносини.
23. Правове регулювання міжнародного співробітництва в сфері міжнародної інформаційної безпеки.
24. Міжнародні угоди з питань міжнародної безпеки.
25. Вплив ІКТ на проблему інформаційної безпеки.
26. Еволюція нормотворчої діяльності ООН у сфері міжнародної інформаційної безпеки.
27. Проблема ухвалення Міжнародної конвенції з інформаційної безпеки.

28. Інформаційна безпека у програмах і практиці діяльності європейських регіональних організацій.
29. Концепція інформаційної безпеки в рамках ЄС.
30. Доктрина інформаційної безпеки в рамках НАТО.
31. Інформаційна безпека у програмах ОБСЄ.
32. Інформаційна війна та інформаційна боротьба: основні поняття.
33. Форми та способи ведення інформаційної боротьби.
34. Психологічна і кібернетична війна як складові інформаційної війни.
35. Інформаційна зброя і технології її використання.
36. Доктрина інформаційної безпеки України.
37. Українські ініціативи в області МІБ, історія їх висунення і просування. Українсько-американські стосунки в цьому процесі. Альтернативні ініціативи США.
38. Перспективи встановлення міжнародного контролю над інформаційними видами зброї.

4. Рекомендована література

Основна література

1. Державна інформаційна політика: Навч. посібник / За заг. ред.. д-ра держ. упр., проф. В.Б. Дзюндзюка. − Х.: Вид-во ХарРІ НАДУ «Магістр», 2012. − 279 с
2. Міжнародні відносини та зовнішня політика (1945 – 70-ті роки) : Підручник / В.А. Манжола, М.М. Білоусов, Л.Ф. Гайдуков та ін. – К.: Либідь, 2014. – 958 с.
3. Міжнародна інформація: терміни і коментарі. Навчальний посібник// Макаренко Є.А., Рижков М.М., Кучмій О.П., Фролова О.М. – К: Центр вільної преси, 2014. – 480 с.
4. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/
5. Капітоненко М. Міжнародні конфлікти. – К.: Либідь, 2017. – 352 с.
6. Капітоненко М.Г. Традиційні міждержавні та внутрішні конфлікти в постбіполярній системі міжнародних відносин // Актуальні проблеми міжнародних відносин. – Вип. 36, част. 2. – К.: ІМВ, 2014. – С. 37-43.

Допоміжна література

1. Бжезинский З. Великая шахматная доска. Господство Америки и его геостратегические императивы.-М., 1999.
2. Дипломатический словарь. В 3-х томах. М., 1986.
3. Камінський А. Вступ до міжнародних відносин: Курс лекцій. – Львів, 2015.
4. Киссинджер Г. Дипломатия. Пер. с англ. В.В.Львова / Послесл. Г.А.Арбатова. – М., 1997.
5. Коппель О.А.. Пархомчук О.С. Міжнародні системи. Світова політика.- Київ: ФАДА, ЛТД. – 2014. – 224 с.
6. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України. Дисертація на здобуття наукового ступеня д.ю.н. – ДВНЗ «Ужгородський національний університет». – Ужгород, 2019.
7. Золотар О. О. Правові основи інформаційної безпеки людини. Дисертація на здобуття наукового ступеня д.ю.н.. – К., 2018.
8. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту. Кандидатська дисертація на здобуття наукового ступеня к.політ.н. – К., 2018.
9. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства. Дисертація на здобуття наукового ступеня к.держ.упр. – К., 2017.
10. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в

Україні. Автореферат дисертації на здобуття наукового ступеня к.ю.н. – К., 2017.