**ГАЛИЦЬКИЙ КОЛЕДЖ**

**імені В’ячеслава Чорновола**

**Кафедра видавничої справи**

**та медіакомункацій**

**Медіабезпека: програма лекційних занять**

*для студентів освітньо-кваліфікаційного рівня – бакалавр*

**Тернопіль – 2021**

**УДК 338**

Навчально-методичне видання розглянуть та схвалено для використання

у роботі на засіданні кафедри видавничої справи та медіакомункацій.

Протокол № 1 від 30.08.2021р.

Рецензент: Вишневська Г. Б., кандидат філологічних дисциплін

**Медабезпека: програма лекційних занять** / укл.Фінклер Ю. Е., Тернопіль: Навчально-виробнича майстерня редакційно-видавничих технологій Галицького коледжуімені В’ячеслава Чорновола, 2020. 20 с.

**Коротка анотація:** навчально-методичне видання містить опорний конспект лекцій та рекомендовані джерела для вивчення дисципліни

Оформлення, друк: Мудра Н.

Навчально-виробнича майстерня редакційно-видавничих технологій Галицького коледжуімені В’ячеслава Чорновола

Галицький коледжімені В’ячеслава Чорновола

**ЗМІСТ**

|  |
| --- |
| Вступ………………………………………………………………………………………….4**Змістовий модуль 1. Теоретико-методологічні засади дослідження інформаційної війни. Теорія і практика інформаційно-психологічного протиборства.....................8**Тема 1.1. Інформація в житті людини. Інформаційний вплив та інформаційні війни..8Тема 1.2. Типи інформаційної війни……………………………………………………...8Тема 1.3. Специфіка ведення інформаційної війни. Електронна війна — війна третього тисячоліття…………………………………………………………………………………...8Тема 1.4. Національна безпека в умовах інформаційної війни………………………....9**Змістовий модуль 2. Теоретико-методологічні засади дослідження інформаційної безпеки………………………………………………………………..…………………….10**Тема 2.1. Інформаційна безпека: підходи до концептуалізації та індикатори визначення……………………………………………………………………………...…...10Тема 2.2. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах………………………………………………...…10Тема 2.3. Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст..………………………………………………………………………...…10Тема 2.4. Інститути й інструменти забезпечення інформаційної безпеки України…....11Тема 2.5. Загрози інформаційній безпеці України…………………………………..…11**ЛІТЕРАТУРНІ ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА КУРСУ…………………..……..12** |

**ВСТУП**

«Медіабезпека» – обов’язкова навчальна дисципліна, що вивчається бакалаврами третього року навчання спеціальності «Журналістика». Курс розрахований на 90 годин. Дисципліна є складовою частиною вивчення комунікативістики. В структурі годин курсу виокремлено такі частини: лекційні заняття – 28 год.; практичні заняття – 20 год.

Курс є елементом такого напряму сучасної комунікативістики як національна інформаційна безпека. Курс було розроблено з прицілом на усталені й новітні якісні та кількісні механізми, методики, інструменти аналізу інформаційної безпеки України та країн Європейського Союзу і НАТО. Методологічною основою курсу є комунікаційні постбіхевіоралізм та неоінституціоналізм. У науковому та навчальному плані курс використаний як механізм диверсифікації та поглиблення (звуження) сфери наукового і практичного контент- аналізу.

Курс розділено на два змістові модулі:

1. Теоретико-методологічні засади дослідження інформаційної війни. Теорія і практика інформаційно-психологічного протиборства.

2. Інформаційна безпека України. Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки.

**Метою** викладання навчальної дисципліни «Медіабезпека» є формування у майбутніх медіапрацівників розуміння сутності явища інформаційна війна, інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави.

**Завдання курсу.**

1. З’ясувати роль інформаційно-психологічних операцій в інформаційному просторі України в контексті гарантування інформаційної безпеки як складової національної безпеки держави. Ознайомити студентів з методами агресії проти розуму/інтелекту, що стало можливим завдяки «розвитку засобів масової комунікації і вдосконалення технологій психологічного впливу на індивідуальну і масову свідомість. За допомогою спеціальних психотехнологій здійснюються цілеспрямовані зміни масової свідомості з метою закладання певної інформації (від комерційної до світоглядної). За мету можуть ставитися також зміни культурної і навіть етнічної самоідентифікації великих груп людей для включення їх у психокультуру агресора або для досягнення інших цілей.

2. Розкрити ознаки феномена «медіабезпека», прищепити у студентів навики самостійного аналізу загроз інформаційній безпеці держави.

3. Сформувати навики виокремлення тенденцій, які властиві сучасним загрозам інформаційній безпеці у соціальних медіях.

4. Визначити напрями і можливості вдосконалення системи забезпечення інформаційної безпеки України.

**Обʼєктом** навчальної дисципліни «Медіабезпека» є визначення методами агресії, що стало можливим завдяки розвитку засобів масової комунікації і вдосконалення технологій психологічного впливу на індивідуальну і масову свідомість.

**Предметом** навчальної дисципліни «Медіабезпека» є спеціальні психотехнології, які здійснюються для цілеспрямованої зміни масової свідомості з метою закладання певної інформації (від комерційної до світоглядної)..

У результаті вивчення навчальної дисципліни студент повинен

знати

* специфіку відмінностей між пропагандою та інформаційною війною, ментальною агресією та психологічною війною у контексті функціонування соціально-політичної системи;
* роль і значення інформаційно-психологічних операцій в інформаційному просторі України в контексті гарантування інформаційної безпеки як складової національної безпеки держави;
* класичні вияви психологічної війни - тотальне пересмикування фактів, маніпулювання свідомостю телеглядачів, слухачів і читачів тощо;
* методи, які впливають на зміну етнокультурної само ідентифікації;
* основні ознаки інформаційної безпеки;
* загрози інформаційній безпеці та їх різновиди;
* методики оцінювання загроз інформаційній безпеці у соціальних Інтернет- сервісах;
* особливості інформаційно-психологічного протиборства у XX – на початку XXІ ст.;
* інститути й інструменти забезпечення інформаційної безпеки України;
* причини та методи ведення інформаційної війни Російської Федерації проти України;
* cтандарти Європейського Союзу та НАТО у сфері інформаційної безпеки;

вміти:

* формувати громадську думку;
* застосовувати прийоми, процедури і технології маніпулятивного впливу з метою захисту інформаційного простору держави;
* розрізняти інформаційні війни в політиці;
* належним чином оперувати такими поняттями як “інформація”, “знання”, “інформаційне суспільство”;
* користуватися знанням підходів до визначення інформаційної безпеки;
* розуміти проблематику і специфіку загроз інформаційній безпеці;
* знати основні різновиди загроз інформаційній безпеці;
* розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти;
* виявляти причини інформаційних воєн;
* оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн.

У результаті вивчення навчальної дисципліни студент повинен набути таких **компетентностей:**

# Загальні компетентності:

* ЗК04. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
* ЗК05. Навички використання інформаційних і комунікаційних технологій.
* ЗК07. Здатність працювати в команді.
* ЗК08. Здатність навчатися і оволодівати сучасними знаннями.
* ЗК09. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

**Спеціальні (фахові, предметні) компетентності:**

* СК06. Здатність до провадження безпечної медіадіяльності.
* СК07. Здатність володіти технологіями цифрової безпеки.
* СК09. Здатність застосовувати технології медіа-аналізу в умовах інформаційних війн.
* Після вивчення дисципліни студенти повинні показати такі **результати навчання:**
* ПР04 Виконувати пошук, оброблення та аналіз інформації з різних джерел.
* ПР05 Використовувати сучасні інформаційні й комунікаційні технології та спеціалізоване програмне забезпечення для вирішення професійних завдань.
* ПР07 Координувати виконання особистого завдання із завданнями колег.
* ПР08 Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань.
* ПР09 Оцінювати діяльність колег як носіїв прав і обов’язків членів суспільства, представників громадянського суспільства.
* ПР18 Використовувати необхідні знання й технології для виходу з кризових комунікаційний ситуацій на засадах толерантності, діалогу й співробітництва.
* ПР19 Застосовувати знання технологій цифрової безпеки для створення якісного медіа продукту.
* ПР21 Застосовувати знання в своїй професійній діяльності.

**Змістовий модуль 1.**

**Теоретико-методологічні засади дослідження інформаційної війни.**

**Теорія і практика інформаційно-психологічного протиборства**

**Тема 1.1. Інформація в житті людини.**

**Інформаційний вплив та інформаційні війни**

Визначення поняття «інформація». Інформаційне середовище. Інформація явища. Порогові й безпорогові явища. Вплив інформаційного поля життєвого середовища людини. Найважливіші властивості розумної системи: сприйняття, збереження та обробка інформації. Сприйняття інформації — певна зміна системи під тим чи іншим впливом. Поняття інформаційного ресурсу, інформаційного простору та інформаційного суверенітету. Поняття інформаційного впливу. Інформаційні технології як засіб інформаційного впливу. Цілі та завдання інформаційно-психологічного впливу. Інформаційний вплив на моральну та духовну стійкість супротивника, вплив на його психіку. Інформаційна складова: актуальність, своєчасність, достовірність, якість, обсяг. Інформаційна протидія. Поняття інформаційної війни. Інформаційні війни в історії.

Тема 1.2. Типи інформаційної війни

Основи ведення інформаційної війни. Інформаційна війна — складова частина ідеологічної боротьби. Політичні інформаційні війни: головна мета — дискредитація і деморалізація політичного опонента. Типові тактики та стратегії. Мета інформаційної війни. Чинники інформаційної війни. Психологія інформаційної війни.

**Тема 1.3. Специфіка ведення інформаційної війни.**

**Електронна війна — війна третього тисячоліття**

Інформаційні війни в сучасному соціально-політичному вимірі. Технології проведення інформаційних операцій. Основні принципи, завдання, цілі та методи геополітичного стратегічного аналізу та прогнозування. Глобальні інформаційні мережі. Сучасна світова/регіональна політика та Інтернет. Особливості інформаційно-психологічного впливу через Інтернет.

Комп’ютерні інформаційні технології як невід’ємна частина озброєння сучасних армій, принципово важливий компонент, від якого залежить діяльність багатьох військових структур і чим при нагоді може скористатися супротивник.

Тема 1.4. Національна безпека в умовах інформаційної війни

Інформаційні потоки в політико-соціальних системах. Деформація механізмів збору розсіяної інформації. Поняття "національна безпека". Види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна.

Взаємозв'язок інформаційної та інших видів безпеки. Основні види загроз національній безпеці: загрози інформаційній інфраструктурі, загрози безпеці інформації, загрози духовному життю суспільства, загрози правам і свободам громадян. Інформаційна безпека як складова національної безпеки. Зовнішні і внутрішні загрози інформаційній безпеці: типи і класи загроз, джерела, засоби реалізації загроз та їхні наслідки. Роль держави в забезпеченні інформаційної безпеки країни. Українська державність як об’єкт інформаційної агресії. Державна мова як важливий елемент національної безпеки країни. Методи запобігання і ліквідації загроз інформаційній безпеці держави. Поняття політики безпеки. Принципи побудови політики безпеки та її впровадження.

**Змістовий модуль 2.**

**Теоретико-методологічні засади дослідження інформаційної безпеки**

**Тема 2.1. Інформаційна безпека:**

**підходи до концептуалізації та індикатори визначення**

Інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека. Інформаційне суспільство. Підходи до дослідження інформаційної безпеки. Статичний, діяльнісний, комплексний підходи. Система забезпечення інформаційної безпеки. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.

Тема 2.2. Загрози інформаційній безпеці.

Методики оцінювання загроз інформаційній безпеці

в соціальних Інтернет-сервісах

Поняття і різновиди загроз інформаційній безпеці. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів. Принципи інформаційної війни. Логіка інформаційної війни. Моделі інформаційної війни. Різновиди інформаційних воєн. Засоби, методи і технології інформаційних воєн. Механізми реагування на загрози інформаційній безпеці.

Тема 2.3. Теорія і практика інформаційно-психологічного

протиборства у XX – на початку XXI cт.

Інформаційно-психологічне протиборство під час Першої світової війни та у міжвоєнний період (1919–1939). Інформаційно-психологічне протиборство в роки Другої світової війни (1939–1945). Інформаційно-психологічне протиборство в умовах «Холодної війни» (1946–1991). Специфіка глобального інформаційно- психологічного протиборства на початку XXI cт. Сучасні тренди розвитку засобів масової комунікації як основи інформаційно-психологічного протиборства. Маніпулятивні техніки ведення інформаційно-психологічного протиборства в сучасних умовах.

**Тема 2.4. Інститути й інструменти**

**забезпечення інформаційної безпеки України**

Правові засади організації системи інформаційної безпеки в Україні. Державна політика забезпечення інформаційної безпеки України. Інститути забезпечення інформаційної безпеки України. Механізми реагування на загрози інформаційній безпеці України. ЗМІ як інструмент інформаційної безпеки України. Громадські організації в контексті інформаційної безпеки України.

Тема 2.5. Загрози інформаційній безпеці України

Різновиди загроз інформаційній безпеці України. Патерни інформаційних операцій Російської Федерації проти України. Інформаційна війна Російської Федерації проти України. Дипломатія України в контексті інформаційної війни Російської Федерації проти України. Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.

**ЛІТЕРАТУРНІ ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА КУРСУ**

**Базова література:**

1. [Барабаш О.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%91%D0%B0%D1%80%D0%B0%D0%B1%D0%B0%D1%88%20%D0%9E%24), Грищук Р., Молодецька-Гринчук К. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних Інтернет-сервісів. [Наукоємні технології](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100325). 2018. № 2. С. 232–239.
2. Бєлоусова Н., Афанасьєва П. Основні вимоги НАТО щодо забезпеченння безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Вип. 102. Ч. І. 2011. С. 196–202.
3. Валюшко І. Дипломатія України у вимірі інформаційної безпеки країни. Вісник Львівського університету. Серія філос.-політолог. студії. 2017. Вип. 13. С. 137– 142.
4. Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико- політичні студії. Збірник наукових праць. 2015. №2. С. 127–134.
5. Валюшко І. Кібербезпека України: наукові та практичні виміри сучасності. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2016. № 3/4 (31–32). С. 117–124.
6. Гнатюк С. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. К.: Нац. ін-т стратегічних досліджень, 2013. 51 с.
7. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.
8. Горбулін В., Качинський А. Засади національної безпеки України: підручник. К.: Інтертехнологія, 2009. 272 с.
9. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України: монографія. К., 2007. 592 с.
10. [Грищук Р.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%93%D1%80%D0%B8%D1%89%D1%83%D0%BA%20%D0%A0%24), Мамарєв В., Молодецька-Гринчук К. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблоку Twitter). [Інформаційні технології та комп’ютерна інженерія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9625260). 2017. № 2. С. 12–19.
11. [Грищук Р.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%93%D1%80%D0%B8%D1%89%D1%83%D0%BA%20%D0%A0%24), Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. [Захист інформації](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9622801). 2017. Т. 19. № 4. С. 254–262.
12. [Грищук Р.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%93%D1%80%D0%B8%D1%89%D1%83%D0%BA%20%D0%A0%24), Молодецька-Гринчук К. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. [Сучасний](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100435) [захист інформації](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100435). 2017. № 3. С. 86–96.
13. Дереко В. Теоретико-методологічні засади класифікації загроз обʼєктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С.16–22.
14. Дмитренко М. Спеціальні заходи впливу як механізм протистояння зовнішньополітичним впливам в інформаційних війнах. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2016. № 12. С. 21–37.
15. Дмитренко М. Спеціальні інформаційні впливи. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2014. № 8. С. 156–167.
16. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Глобальна природа інформаційної безпеки. [Політологічний](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9668683) [вісник](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9668683). 2015. Вип. 79. С. 181–189.
17. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Держава як суб’єкт інформаційної безпеки суспільства. [Гілея:](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9625326) [науковий вісник](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9625326). 2017. Вип. 124. С. 295–299.
18. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Ефективність використання потенціалу недержавних суб’єктів інформаційної безпеки. [Мультиверсум. Філософський альманах](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670616). 2016. Вип. 1– 2. С. 58–70.
19. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Інформаційні впливи як джерела загострення інформаційної небезпеки. [Науковий часопис НПУ імені М. П. Драгоманова. Серія 7:](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9672786%3A%D0%A1.7) [Релігієзнавство. Культурологія. Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9672786%3A%D0%A1.7). 2015. Вип. 34. С. 167–175.
20. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі. [Гуманітарний вісник державного вищого навчального закладу](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9671961%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81)

[«Переяслав-Хмельницький державний педагогічний університет ім. Г. С.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9671961%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81) [Сковороди». Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9671961%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81). 2015. Вип. 37. С. 106–117.

1. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Основні суб’єкти та інститути інформаційної безпеки. [Вісник](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9669749%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81) [Харківського національного педагогічного університету імені Г. С. Сковороди.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9669749%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81) [Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9669749%3A%D0%A4%D1%96%D0%BB%D0%BE%D1%81). 2017. Вип. 48 (1). С. 212–219.
2. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A%24) Проблеми формування ефективної державної інформаційної політики. [Науковий часопис НПУ імені М. П. Драгоманова. Серія 7:](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9672786%3A%D0%A1.7) [Релігієзнавство. Культурологія. Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9672786%3A%D0%A1.7). 2016. Вип. 36. С. 202–209.
3. Зозуля О. Зарубіжний досвід державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства. Науково-інформаційний вісник Академії національної безпеки. 2016. № 1–2. С. 28–38.
4. Качинський А. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с.
5. Куцька О. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С.180–190.
6. [Левченко О.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%9B%D0%B5%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9E%24) Система заходів протидії інформаційним операціям. [Збірник](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670455) [наукових праць Харківського університету Повітряних Сил](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670455). 2016. Вип. 3. С. 57–60.
7. [Левченко О.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%9B%D0%B5%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9E%24) Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. [Наука і оборона](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9615759). 2013. № 3. С. 21–26.
8. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.
9. Ліпкан В. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с.
10. Ліпкан В. Теоретико-методологічні засади управління у сфері національної безпеки України. К.: Видавництво Національної академії внутрішніх справ України, 2005. 350 с.
11. Молодецька-Гринчук К. Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. [Вісник Житомирського національного агроекологічного університету](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9669750). 2017. № 2 (1). С. 180–187.
12. Молодецька-Гринчук К. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності. [Управління](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9673886) [розвитком складних систем](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9673886). 2017. Вип. 30. С. 121–127.
13. Молодецька-Гринчук К. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками. [Радіоелектроніка,](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9616683) [інформатика, управління](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9616683). 2017. № 2. С. 117–126.
14. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. [Автоматизация технологических и](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100466) [бизнес-процессов](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100466). 2017. Вип. 9. № 2. С. 36–42.
15. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
16. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
17. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». 2012. Вип. 32. С. 20–27.
18. Панченко В. Інформаційні операції в асиметричній війні Росії проти України*:* підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16.
19. Панченко В. Інформаційні операції в системі стратегічних комунікацій.

[Стратегічні пріоритети. Серія: Політика](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9625775%3A%D0%9F). 2016. № 4. С. 72–79.

1. Панченко В. Концептуальні вимоги до якості розвідувальної інформації в умовах суспільства знань. [Інформаційна безпека людини, суспільства, держави](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100315). 2013. № 3. С. 6–11.
2. Пелещишин А., Гумінський Р. Загрози інформаційної безпеки держави в соціальних мережах. [Наука і техніка Повітряних Сил Збройних Сил України](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96100320). 2013. № 2. С. 192–199.
3. Пилипчук В. Інформаційна сфера як складова гібридної війни. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. 408 с.
4. Пилипчук В. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник. К.: Нац. акад. СБУ, 2017. 260 с.
5. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.
6. Присяжнюк М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. Військово- спеціальні науки. 2013. Вип. 30. С. 42–46.
7. Прозоров А. Ціннісні основи інформаційної безпеки особи, суспільства та держави. Інформаційна безпека людини, суспільства, держави. 2016. № 1 (20). С. 29–37.
8. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). [Грані](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9669893). 2015. № 3. С. 18–23.
9. Сніцаренко П., Міхєєв Ю., Чернявський Г. Методичний підхід до оцінювання рівня інтенсивності деструктивного інформаційно-психологічного впливу на цільову аудиторію. [Проблеми створення, випробування, застосування та](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670384) [експлуатації складних інформаційних систем](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670384). 2016. Вип. 13. С. 12–19.
10. Сніцаренко П., Саричев Ю. Роль та місце інформаційного забезпечення в системі державного управління. [Державне управління: теорія та практика](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=EJ000066). 2016. № 1. С. 46–56.
11. Сніцаренко П., Саричев Ю. Теоретичні підходи до визначення сутності інформаційного забезпечення в системі державного управління. [Науково-](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96101280) [інформаційний вісник Академії національної безпеки](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%96101280). 2016. № 1–2. С. 7–19.
12. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С. 75–80.
13. Ткачук Т. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Наук. вісник УжНУ. Серія: Право. 2017. № 46. Т. 2. С. 39–43.
14. Ткачук Т. Захист національних інформаційних ресурсів як пріоритетна складова інформаційної політики держави в умовах глобалізації. Розвиток України в 21 ст.: економічні, соціальні, екологічні, гуманітарні та правові проблеми: мат. міжнарод. наук.-практ. конф. (Тернопіль, 30 березня 2012 р.). С. 209–212.
15. Ткачук Т. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку: мат. наук. круглого столу (Маріуполь, 26 квітня 2018 р.). МДУ, 2018. С. 39–42.
16. Ткачук Т. Кібербезпека: підходи до визначення в окремих країнах. Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 24 травня 2017 р.). 2017. С. 142–144.
17. Ткачук Т. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства: мат. наук.-практ. конф. (Київ, 29 листопада 2017 р.). 2017. С. 111–114.
18. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.
19. Штельмах О. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Актуальні проблеми управління державною безпекою: зб. Матер.наук.-практ. Конф (Київ, 19 березня 2015 р.). К.: Центр навч., наук. та період. видань

# Допоміжна література:

1. Дмитренко М. Зовнішньополітичні впливи як пріоритети діяльності зовнішньої розвідки. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2013. № 5. С. 31−46.
2. Климчук О. Ткачук Н. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С.75–83.
3. Коваленко Є., Плетньов О. Діяльність контррозвідувальних органів в державній системі забезпечення інформаційної безпеки: досвід країн НАТО та українські реалії. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право». 2018. Вип. 26. С. 136–139.
4. [Левченко О.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%9B%D0%B5%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9E%24) Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел. Системи обробки інформації. 2016. Вип. 1 (138). С. 100–102.
5. Молодецька-Гринчук К. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня. [Системи обробки інформації](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670474). 2017. Вип. 5. С. 122–129.
6. Пономаренко Л. Інноваційні підходи до попередження радикалізації настроїв і проявів екстремізму в контексті забезпечення сталого демократичного розвитку. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 74–81.
7. Снитко О. Проекти тотального зомбування в інформаційному просторі України. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 207– 215.
8. Ярема О. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісник Львівського державного університету внутрішніх справ. Серія: Право. 2016. № 2. С. 244–252.
9. Яцик Т. Особливості інформаційного тероризму як одного із способів інформаційної війни. [Науковий вісник Національного університету державної](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670599) [податкової служби України (економіка, право)](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ%3D&S21COLORTERMS=1&S21STR=%D0%9670599). 2014. № 2. С. 55–60.
10. Rasmussen M. The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century. Cambridge: Cambridge University Press, 2007. 234 p.

**Інформаційні ресурси:**

|  |  |
| --- | --- |
| **Назва ресурсу або організації** | **Електронна адреса** |
| Законодавство України | <http://zakon1.rada.gov.ua/laws/main> |
| Міністерство освіти і науки України | <http://www.mon.gov.ua/index.php/ua/> |
| Сайт про медіа | <https://ms.detector.media> |
| Національна бібліотека України імені В.І.Вернадського | <http://www.nbuv.gov.ua/> |
| Харківська державна наукова бібліотека | <http://korolenko.kharkov.com/> |
| Національна парламентська бібліотека України | <http://www.nplu.kiev.ua/> |
| Наукова бібліотека ім. М. МаксимовичаКиївського національного університету імені Тараса Шевченка | <http://lib-gw.univ.kiev.ua/> |
| Галицький коледж імені В. Чорновола | <http://moodle.gi.edu.ua/> |