Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Кафедра міжнародних комунікацій та цифрової дипломатії

“**ЗАТВЕРДЖУЮ**”

Завідувач кафедри

_____

“____”_____2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“Інформаційна безпека”

освітній рівень **бакалавр**

галузь знань **29 “Міжнародні відносини”**
(шифр і назва галузі знань)

спеціальність **291 “Міжнародні відносини, суспільні комунікації та регіональні студії”**
(шифр і назва спеціальності)

спеціалізація **“Міжнародна інформація”**

освітня програма **“Міжнародна інформація”**

Факультет міжнародних відносин

2022 – 2023 навчальний рік

Поліщук К.В. Інформаційна безпека. Робоча програма навчальної дисципліни для студентів факультету міжнародних відносин за спеціальністю **291 «Міжнародні відносини, суспільні комунікації та регіональні студії»**. Львівський національний університет імені Івана Франка, Львів, 2022..

Розробник:
Поліщук К.В., кандидат політичних наук, доцент кафедри міжнародних комунікацій та цифрової дипломатії.

Робочу програмусхвалено на засіданні кафедри міжнародних комунікацій та цифрової дипломатії.
Протокол №1 від 29 серпня 2022 р.

(підпис) (прізвище та ініціали)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td><u>денна форма навчання</u></td></tr>
<tr><td>Кількість кредитів – 6</td><td>Галузь знань: 29 Міжнародні відносини</td><td>Рік підготовки:
3-й (бакалавр)</td></tr>
<tr><td>Модулів – 2</td><td>Спеціалізація: міжнародна інформація</td><td>Семестр 5-й</td></tr>
<tr><td>Змістових модулів – 2</td><td rowspan="4">Спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»</td><td>Лекції 32 год.</td></tr>
<tr><td>Курсова робота - х</td><td>Практичні, семінарські
32 год.</td></tr>
<tr><td rowspan="2">Загальна кількість годин -180</td><td>Самостійна робота
116 год.</td></tr>
<tr><td>Індивідуальні завдання</td></tr>
<tr><td>Тижневих годин для денної форми навчання:
аудиторних – 4</td><td>Освітньо-кваліфікаційний рівень:
бакалавр</td><td>Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми здобуття освіти – 16:29

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є вивчення тенденцій розвитку інформаційної безпеки під впливом високих (інформаційно-комунікаційних) технологій; сформувати у студентів розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави.

Завдання курсу спрямовані на ознайомлення студентів з особливостями сучасних міжнародних інформаційних відносин і тенденціями їх розвитку у зрізі інформаційної безпеки. В рамках курсу розглядаються найважливіші аспекти феномена «інформаційна безпека», у контексті якого завданнями є прищепити у студентів навики самостійного аналізу загроз інформаційній безпеці держави; сформувати навики виокремлення тенденцій, які властиві сучасним загрозам інформаційній безпеці у соціальних Інтернет-сервісах; визначити напрями і можливості вдосконалення системи забезпечення інформаційної безпеки України.

У результаті вивчення навчальної дисципліни студент повинен

знати

- основні ознаки інформаційної безпеки на рівні індивіда-суспільства-держави-світу;
- загрози інформаційній безпеці та їх різновиди;
- методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах;
- особливості інформаційно-психологічного протиборства у ХХ – на початкуXXI ст.;
- інститути й інструменти забезпечення інформаційної безпеки України;
- причини та методи ведення інформаційної війни Російської Федерації протиУкраїни;
- стандарти міжнародних організацій у сфері інформаційної безпеки;

вміти:

- 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.

Загальні компетентності (ЗК):

ЗК9. Здатність використовувати інформаційні та комунікаційні технології.
ЗК10. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК11. Здатність спілкуватися іноземною мовою.
ЗК12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові, предметні) компетентності (ФК):

ФК2. Здатність аналізувати міжнародні процеси у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.
ФК8. Усвідомлення національних інтересів України на міжнародній арені.
ФК17. Здатність застосовувати інформаційно-комунікаційні системи і технології у професійній діяльності.

Програмні результати навчання за ОП

ПРН 1. Знати та розуміти природу міжнародних відносин та регіональногорозвитку, еволюцію, стан теоретичних досліджень міжнародних відносин тасвітової політики, а також природу та джерела політики держав на міжнароднійарені і діяльності інших учасників міжнародних відносин.
ПРН 2. Знати та розуміти природу та динаміку міжнародної безпеки, розумітиособливості її забезпечення на глобальному, регіональному та національномурівні, знати природу та підходи до вирішення міжнародних таінтернаціоналізованих конфліктів.
ПРН 3. Знати природу міжнародного співробітництва, характер взаємодії міжміжнародним акторами, співвідношення державних, недержавних акторів усвітовій політиці.
ПРН 4. Знати принципи, механізми та процеси забезпечення зовнішньої політикидержав, взаємодії між зовнішньою та внутрішньою політикою, визначення тареалізації на міжнародній арені національних інтересів держав, процесуформування та реалізації зовнішньополітичних рішень.
ПРН 5.Знати природу та механізми міжнародних комунікацій.
ПРН 7. Здійснювати опис та аналіз міжнародної ситуації, збирати з різних джерелнеобхідну для цього інформацію про міжнародні та зовнішньополітичні події тапроцеси.
ПРН 8. Збирати, обробляти та аналізувати великі обсяги інформації про станміжнародних відносин, зовнішньої політики України та інших держав,регіональних систем, міжнародних комунікацій.
ПРН 9. Досліджувати проблеми міжнародних відносин, регіонального розвитку,зовнішньої політики, міжнародних комунікацій, із використанням сучаснихполітичних, економічних і правових теорій та концепцій, наукових методів таміждисциплінарних підходів, презентувати результати досліджень, надавативідповідні рекомендації**.**

ПРН 11. Здійснювати прикладний аналіз міжнародних відносин, зовнішньоїполітики України та інших держав, міжнародних процесів та міжнародноїситуації відповідно до поставлених цілей, готувати інформаційні та аналітичні документи.
ПРН 12. Володіти навичками професійного усного та письмового перекладу з/наіноземні мови, зокрема, з фахової тематики міжнародного співробітництва,зовнішньої політики, міжнародних комунікацій, регіональних студій, дво- та багатосторонніх міжнародних проектів.
ПРН 13. Вести фахову дискусію із проблем міжнародних відносин, міжнародних комунікацій, регіональних студій, зовнішньополітичної діяльності, аргументувати свою позицію, поважати опонентів і їхню точки зору.
ПРН 15. Розуміти та застосовувати для розв'язання складних спеціалізованих задач міжнародних відносин, суспільних комунікацій та регіональних студій чинне законодавство, міжнародні нормативні документи і угоди, довідкові матеріали, чинні стандарти і технічні умови тощо.
ПРН 16. Розуміти та відстоювати національні інтереси України у міжнародній діяльності.
ПРН 17. Мати навички самостійного визначення освітніх цілей та навчання, пошуку необхідних для їх досягнення освітніх ресурсів.
ПРН 18. Володіти теоретичними відомостями та практичними навичками діяльності у сфері електронної комерції.
ПРН 19. Організовувати та підтримувати зв'язки з громадськістю та міжнародні комунікації.
ПРН 20. Організовувати рекламну діяльність у політичній та соціально-економічній сферах.

3. Програма навчальної дисципліни

Змістовий модуль 1. Тенденції та закономірності становлення та розвитку інформаційної безпеки.

Тема 1. Інформаційна безпека: підходи до концептуалізації таіндикатори визначення

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

Тема 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. Інтернет-ресурси як об'єкти загроз інформаційній безпеці держави. Система моніторингу Інтернет-ресурсів. Актори соціальних Інтернет-сервісів. Контент і дані акторів соціальних Інтернет-сервісів. Методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах.

Тема 3. Теорія і практика інформаційно-психологічного протиборствау XX – на початку XXI ст.

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 ст. Сучасні тренди розвитку засобів масової комунікації як основи інформаційно-психологічного протиборства. Маніпулятивні техніки ведення інформаційно-психологічного протиборства в сучасних умовах.

Тема 4. Правові засади інформаційної безпеки. Захист інформації

Конституційне визначення способів захисту в інформаційних правовідносинах: право на самозахист в інформаційних відносинах; право на юридичну допомогу як інституція захисту прав суб'єктів суспільних відносин; право на захист через громадські утворення; право на звернення до органів державної влади як інституція в захисті інформаційних відносин; судовий захист інформаційних відносин. Правові засади захисту об'єктів інформаційних правовідносин від загроз в інформаційній сфері. Інформаційна безпека людини й суспільства. Правові засади охорони комерційної, банківської таємниці та персональних даних. Правовий захист інформації, інформаційних ресурсів та інформаційних систем від загроз несанкціонованого та неправомірного впливу сторонніх осіб. Забезпечення інформаційної безпеки в мережі Інтернет.

Змістовий модуль 2. Інформаційна безпека України. Міжнародні стандартиу сфері інформаційної безпеки

Тема 5. 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 6. 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.

Тема 7. Стандарти ООН, Європейського Союзу і НАТО у сферіінформаційної безпеки

Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки (програми, директиви тощо): «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» (1995 р.), «Єдині критерії безпеки інформаційних технологій» (1996 р.), «Безпечніший Інтернет» (1999 р.), «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (2007 р.), «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» (2009 р.). Основні засади політики інформаційної безпеки НАТО. Північноатлантична Рада з питань, що стосуються безпеки НАТО, Комітет внутрішньої безпеки НАТО, Комітет з планування використання цивільних систем зв'язку, Орган з управління кібернетичною безпекою НАТО, Комісія з управління діяльністю в галузі кіберзахисту.

Тема 8. Інформаційна безпека особистості. Захист персональних даних

Виникнення й розвиток концепції права на приватність. Право на забуття. Особливості інформаційних правовідносин, що виникають при виробництві, передачі й споживанні персональних даних. Суб'єкти й об'єкти інформаційних правовідносин у сфері персональних даних. Правові

засади роботи зперсональними даними. Права суб'єкта персональних даних. Права й обов'язки власника щодо роботи з масивами персональних даних. Державне регулювання роботи з персональними даними. Захист фізичних осіб щодо автоматизованого опрацювання персональних даних. Правове регулювання захисту права на приватність та транскордонні потоки персональних даних. Досвід ЄС у регулюванні захисту персональних даних

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					х					
		л	п	лаб	інд	ср						
1	2	3	4	5	6	7						
Модуль 1												
Змістовий модуль 1. Тенденції та закономірності становлення та розвитку інформаційної безпеки.												
Тема 1. Інформаційна безпека: підходи до концептуалізації та індикатори визначення	**8**	**4**	**4**			**14**						
Тема 2. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах	**8**	**4**	**4**			**14**						
Тема 3. Теорія і практика інформаційно-психологічного протиборствау XX – на початку XXI ст.	**8**	**4**	**4**			**14**						
Тема 4. Правові засади інформаційної безпеки. Захист інформації	**8**	**4**	**4**			**16**						
Разом – зм. модуль1	**32**	**16**	**16**			**58**						
Змістовий модуль 2. Інформаційна безпека України. Міжнародні стандартиу сфері інформаційної безпеки												
Тема 5. Інститути й інструменти забезпечення інформаційної безпеки України	**8**	**4**	**4**			**14**						
Тема 6 Загрози інформаційній безпеці України	**8**	**4**	**4**			**14**						
Тема 7 Стандарти												

ООН, Європейського Союзу і НАТО у сферіінформаційної безпеки	**8**	**4**	**4**			**14**						
Тема 8 Інформаційна безпека особистості. Захист персональних даних	**8**	**4**	**4**			**16**						
Разом – зм. модуль 2	**32**	**16**	**16**			**58**						
Модуль 2												
Усього годин	64	32	32			116						

5. Плани семінарських занять

№ з/п	Назва теми	Кількість годин
1	Еволюція та сучасний стан розвитку інформаційної безпеки	2
2	Загрози інформаційній безпеці	2
3	Інформаційно-психологічні протиборства	4
4	Кіберзлочинність і кібертероризм	4
5	Технологічний вимір розвитку інформаційної безпеки	2
6	Розвиток глобальної інформаційної та комунікаційної інфраструктури у сфері безпеки	4
7	Інститути й інструменти забезпечення інформаційної безпеки України	4
8	Загрози інформаційній безпеці України	4
9	Індивідуальні завдання	6

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Безпека у кіберпросторі	12
2	Новий міжнародний інформаційний порядок у сфері безпеки	12
3	Глобалізація та міжнародні інформаційні процеси	12
4	Інформаційна безпека: підходи до концептуалізації та індикатори визначення	12
5	Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах	12
6	Теорія і практика інформаційно-психологічного протиборства	12
7	Інститути й інструменти забезпечення інформаційної безпеки України	12
8	Загрози інформаційній безпеці України	12
9	Міжнародні стандарти у сфері інформаційної безпеки	20
	Разом	116

7. Методи навчання

Навчальний процес здійснюється за традиційною технологією: лекції, практичні (семінарські) заняття, самостійна робота.

На лекційних заняттях використовуються: словесні методи (розповідь, бесіда, пояснення, лекція, діалог); наочні та практичні методи (ілюстрація, демонстрація); метод синтезу, аналізу, індукції, дедукції тощо.

На семінарських заняттях використовуються: дискусія, проблемно-пошуковий, репродуктивний, інтерактивний методи тощо.

У межах самостійної роботи застосовуються дослідницькі методи.

8. Критерії оцінювання знань студентів

Оцінка	Критерії оцінювання
E	Студент виявляє знання і розуміння основних положень теоретичного матеріалу. Дає правильні, але недостатньо осмислені відповіді. Вміє застосовувати знання при виконанні завдань за зразком, наводити окремі власні приклади на підтвердження власних думок
D	Студент вміє застосовувати вивчений матеріал у стандартних ситуаціях, намагається аналізувати встановлювати найсуттєвіші зв'язки і залежність між явищами, фактами, робити висновки, загалом дає відповіді логічно, допускаючи при цьому неточності.
C	Студент добре володіє вивченим матеріалом, застосовує знання в стандартних ситуаціях, уміє аналізувати й систематизувати інформацію, використовує основні положення із самостійною і правильною аргументацією.
B	Студент має повні, глибокі знання, здатний застосовувати їх у практичній діяльності, робити висновки, узагальнення. Вміє аргументовано використовувати отримані знання в різних ситуаціях, самостійно знаходити інформацію, ставити і розв'язувати проблеми
A	Студент має системні, міцні знання в обсязі та в межах вимог навчальних програм, усвідомлено використовує їх у стандартних та нестандартних ситуаціях. Уміє самостійно аналізувати, оцінювати, узагальнювати опанований матеріал, самостійно користуватися джерелами інформації, приймати рішення.

9. Розподіл балів, що присвоюється студентам

Розподіл балів, які отримують студенти (для екзамену)

<table>
<tr><td colspan="8">Поточне тестування та самостійна робота</td><td>Підсумковий тест (екзамен)</td><td>Сума</td></tr>
<tr><td colspan="4">Змістовий модуль 1</td><td colspan="4">Змістовий модуль 2</td><td rowspan="3">50</td><td rowspan="3">100</td></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td><td>Т5</td><td>Т6</td><td>Т7</td><td>Т8</td></tr>
<tr><td>5</td><td>5</td><td>5</td><td>10</td><td>5</td><td>5</td><td>5</td><td>10</td></tr>
</table>

Оцінювання знань студента здійснюється за 100-бальною шкалою (для екзаменів і заліків).

- максимальна кількість балів при оцінюванні знань студентів з дисципліни, яка завершується екзаменом, становить за поточну успішність 50 балів, на екзамені – 50 балів;
- при оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань студентів за різними системами.

Шкала оцінювання: вузу, національна та ECTS

Оцінка ECTS	***Оцінка в балах***	***За національною шкалою***		
		Екзаменаційна оцінка, оцінка з диференційованого заліку		***Залік***
A	90 – 100	5	***Відмінно***	***Зараховано***
B	81-89	4	***Дуже добре***	
C	71-80		***Добре***	
D	61-70	3	***Задовільно***	
E	51-60		***Достатньо***	

Протягом семестру проводиться не менше двох модулів або колоквіумів чи контрольних робіт або інших видів контролю. Максимальна кількість балів, яка встановлюється для цих видів контролю, а також відповідність оцінок FX та F у шкалі ECTS, у балах та національній шкалі визначається Вченими радами факультетів або кафедрами, які забезпечують викладання відповідних дисциплін.

10. Рекомендована література
Базова

1. Барабаш О., Грищук Р., Молодецька-Гринчук К. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних Інтернет-сервісів. Наукоємні технології. 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-тстратегічних 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 стратегіїнаціональної безпеки України: монографія. К., 2007. 592 с.
10. Грищук Р., Мамарєв В., Молодецька-Гринчук К. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблоку Twitter). Інформаційні технології та комп'ютерна інженерія. 2017.
№ 2. С. 12–19.
11. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. Захист інформації. 2017. Т. 19. № 4. С. 254–262.
12. Грищук Р., Молодецька-Гринчук К. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. Сучаснийзахист інформації. 2017. № 3. С. 86–96.
13. Дереко В. Теоретико-методологічні засади класифікації загроз об'єктам 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. Глобальна природа інформаційної безпеки. Політологічнийвісник. 2015. Вип. 79. С. 181–189.
17. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства. Гілея: науковий вісник. 2017. Вип. 124. С. 295–299.
18. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки. Мультиверсум. Філософський альманах. 2016. Вип. 1–2. С. 58–70.
19. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки. Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2015. Вип. 34. С. 167–175.
20. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі. Гуманітарний вісник державного вищого навчального закладу

«Переяслав-Хмельницький державний педагогічний університет ім. Г. С.Сковороди». Філософія. 2015. Вип. 37. С. 106–117.

21. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2017. Вип. 48 (1). С. 212–219.
22. Захаренко К. Проблеми формування ефективної державної інформаційної політики. Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2016. Вип. 36. С. 202–209.
23. 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.
24. Качинський А. Індикатори національної безпеки: визначення та застосування їхграничних значень. К.: НІСД, 2013. 104 с.
25. 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.
26. Левченко О. Система заходів протидії інформаційним операціям. Збірник наукових праць Харківського університету Повітряних Сил. 2016. Вип. 3. С. 57–60.
27. Левченко О. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. Наука і оборона. 2013. № 3. С. 21–26.
28. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.
29. Ліпкан В. Національна безпека України: навчальний посібник. Київ: КНТ, 2009.
576 с.
30. Ліпкан В. Теоретико-методологічні засади управління у сфері національної безпеки України. К.: Видавництво Національної академії внутрішніх справ України, 2005. 350 с.
31. Молодецька-Гринчук К. Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. Вісник Житомирського національного агроекологічного університету. 2017. №2 (1). С. 180–187.
32. Молодецька-Гринчук К. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності. Управління розвитком складних систем. 2017. Вип. 30. С. 121–127.
33. Молодецька-Гринчук К. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками. Радіоелектроніка, інформатика, управління. 2017. № 2. С. 117–126.
34. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах.

Автоматизация технологических и бизнес-процессов. 2017. Вип. 9. № 2. С. 36–42.
35. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
36. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
37. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». 2012.Вип. 32. С. 20–27.
38. Панченко В. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16.
39. Панченко В. Інформаційні операції в системі стратегічних комунікацій.
Стратегічні пріоритети. Серія: Політика. 2016. № 4. С. 72–79.
40. Панченко В. Концептуальні вимоги до якості розвідувальної інформації в умовах суспільства знань. Інформаційна безпека людини, суспільства, держави.2013. № 3. С. 6–11.
41. Пелещишин А., Гумінський Р. Загрози інформаційної безпеки держави в соціальних мережах. Наука і техніка Повітряних Сил Збройних Сил України. 2013. № 2. С. 192–199.
42. 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.
43. Пилипчук В. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник. К.: Нац. акад. СБУ, 2017. 260 с.
44. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянськаакадемія», 2015. 497 с.
45. Присяжнюк М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. Військово- спеціальні науки. 2013. Вип. 30. С. 42–46.
46. Прозоров А. Ціннісні основи інформаційної безпеки особи, суспільства та держави. Інформаційна безпека людини, суспільства, держави. 2016. № 1 (20). С. 29–37.
47. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). Грані. 2015. № 3. С. 18–23.
48. Сніцаренко П., Міхєєв Ю., Чернявський Г. Методичний підхід до оцінювання рівня інтенсивності деструктивного інформаційно-психологічного впливу на цільову аудиторію. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2016. Вип. 13. С. 12–19.
49. Сніцаренко П., Саричев Ю. Роль та місце інформаційного забезпечення в системі державного управління. Державне управління:

теорія та практика. 2016.
№ 1. С. 46–56.

50. Сніцаренко П., Саричев Ю. Теоретичні підходи до визначення сутності інформаційного забезпечення в системі державного управління. Науково- інформаційний вісник Академії національної безпеки. 2016. № 1–2. С. 7–19.
51. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства.Юридичний вісник. 2015. № 1 (34). С. 75–80.
52. Ткачук Т. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Наук. вісник УжНУ. Серія: Право. 2017. № 46. Т. 2. С. 39–43.
53. 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.
54. 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.
55. 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.
56. Ткачук Т. Теоретико-правове осмислення інформаційної безпеки держави уконтексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства: мат. наук.-практ. конф. (Київ, 29 листопада 2017 р.). 2017. С. 111–114.
57. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.
58. Штельмах О. Організаційні аспекти протидії інформаційній агресії як складовоїгібридної війни. Актуальні проблеми управління державною безпекою: зб. Матер.наук.-практ. Конф (Київ, 19 березня 2015 р.). К.: Центр навч., наук. та період. видань НА СБ України, 2015. С. 393–396.

Допоміжна

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. 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. 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 податкової служби України (економіка, право). 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

1. Міністерство закордонних справ України: Офіційний веб-сайт. URL:https://mfa.gov.ua/ua (дата звернення: 26.08.2019).
2. Міністерство оборони України: Офіційний веб-сайт. URL
3. Офіційний портал Верховної Ради України. URL: https://rada.gov.ua/ (датазвернення: 26.08.2019).
4. Президент України. Офіційне інтернет-представництво. URL

Законодавство:

1. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // ВідомостіВерховної Ради України. – 1996. – №30 – Ст. 141.
2. Кримінальний кодекс України від 5 квітня 2001 р. // Відомості Верховної Ради України. –2001. – № 25-26 – Ст. 131.
3. Основи законодавства України про культуру: Закон України від 14 лютого 1992 р. № 2117-XII // Відомості Верховної Ради України. – 1992. – № 21. – Ст. 294.
4. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19.
5. Про адвокатуру: Закон України від 19 грудня 1992 р. № 2887-XII // Відомості ВерховноїРади України. – 1993. – № 9. – Ст. 62.
6. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року № 2121-III //Відомості Верховної Ради України. – 2001. – № 5- 6. – Ст. 30.

7. Про бібліотеки і бібліотечну справу: Закон України від 27 січня 1995 р. // ВідомостіВерховної Ради України. – 1995. – № 7. – ст. 45.
8. Про вибори народних депутатів України: Закон України в редакції Закону № 2777-IV від 7липня 2005 р. // Відомості Верховної Ради України. – 2005. – № 38-39. – Ст. 449.
9. Про видавничу справу: Закон України від 5 червня 1997 р. № 318/97-ВР // ВідомостіВерховної Ради України. – 1997. – № 32. – Ст. 206.
10. ро державну службу: Закон України від 16 грудня 1993 року № 3723-XII // ВідомостіВерховної Ради України. – 1993. – № 52. – Ст. 490.
11. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258.