МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет історії, політології і міжнародних відносин
Кафедра міжнародних відносин

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ

Рівень вищої освіти – магістр

Освітня програма Міжнародні відносини, суспільні комунікації та регіональні студії
Спеціальність С3 Міжнародні відносини
Галузь знань С Соціальні науки, журналістика, інформація
та міжнародні відносини

Затверджено на засіданні
кафедри міжнародних відносин
Протокол No1 від 26 серпня 2025 р.

м. Івано-Франківськ – 2025р.

.

1. Загальна інформація	
Назва дисципліни	Інформаційний тероризм
Викладач (-і)	Струтинська Тетяна Зіновіївна – кандидат політичних наук, доцент кафедри міжнародних відносин
Контактний телефон викладача	(0342) 75 20 27
E-mail викладача	tetiana.strutynska@cnu.edu.ua
Формат дисципліни	очний
Обсяг дисципліни	Лекції – 12 год. Практичні заняття – 18 год. Самостійна робота – 90 год. 3 кредитів ЄКТС, 90 год.
Посилання на сайт дистанційного навчання	https://d-learn.pnu.edu.ua/course/subscription/through/url/304360d9552784aa7f0d
Консультації	Згідно розкладу

2. Анотація до навчальної дисципліни

Дисципліна «Інформаційний тероризм» спрямована на формування у студентів-магістрантів системного розуміння феномену інформаційного тероризму як однієї з ключових загроз міжнародній та національній безпеці в умовах глобалізованого та цифровізованого світового порядку. Курс охоплює теоретичні засади, правові рамки, інституційні механізми та практичні інструменти протидії інформаційним загрозам на світовому, регіональному та національному рівнях.

У межах дисципліни студенти вивчають поняття, ознаки та класифікацію інформаційного тероризму, співвідносячи його з класичними формами тероризму та сучасними загрозами у сфері інформаційно-психологічного та кіберпростору. Особлива увага приділяється інформаційно-психологічним та інформаційно-технічним атакам, медіа-тероризму, кібертероризму та пов’язаним правопорушенням у цифровому середовищі.

Важливим елементом курсу є аналіз світового досвіду протидії інформаційному тероризму, включаючи політики та стратегії ООН, НАТО, Інтерполу, Шанхайської організації співробітництва, Європейського Союзу та ОБСЄ. Студенти опановують міжнародні правові документи, такі як Глобальна контртерористична стратегія ООН, Конвенція Ради Європи про кіберзлочинність, європейська Стратегія кібербезпеки, Директива NIS та інші ключові акти у сфері цифрової безпеки.

Окрема частина курсу присвячена аналізу національних моделей протидії інформаційному тероризму у США, країнах Азії, держав Європейського Союзу, зокрема Естонії, Литві, Великій Британії, Німеччині, Франції, Іспанії та Туреччині. Розглядаються їхні законодавчі підходи, інституційні структури, механізми попередження та реагування на кібер- та інформаційні атаки.

Значну увагу приділено боротьбі з інформаційним тероризмом в Україні, зокрема нормативно-правовому забезпеченню, діяльності Служби безпеки України, Кіберполіції,

Державного центру кіберзахисту та протидії кіберзагрозам. Студенти аналізують Закон України «Про основні засади забезпечення кібербезпеки» та інші ключові документи (Закон України «Про Державну службу спеціального зв'язку та захисту інформації України, Закон України «Про електронні комунікації»).

Дисципліна також передбачає вивчення співробітництва України з міжнародними організаціями у сфері боротьби з інформаційним та кібертероризмом, включаючи виконання міжнародних конвенцій щодо протидії тероризму, фінансуванню терористичної діяльності та протидії відмиванню коштів.

У результаті опанування курсу студенти набувають компетентностей щодо:

– ідентифікації та класифікації інформаційно-терористичних загроз;

– аналізу політики держав і міжнародних інституцій у сфері кібер- та інформаційної безпеки;

– оцінювання ефективності механізмів протидії інформаційному тероризму;

– застосування міжнародних та національних норм у сфері запобігання і боротьби з інформаційно-терористичними проявами;

– вироблення рекомендацій щодо підвищення рівня безпеки держави у цифровому середовищі.

Дисципліна є важливим елементом професійної підготовки фахівців-міжнародників, які працюватимуть у сферах дипломатії, безпеки, аналітики, комунікацій, державного управління та міжнародного співробітництва.

3. Мета та цілі навчальної дисципліни

Метою навчальної дисципліни **«Інформаційний тероризм»** є формування у студентів-магістрантів комплексного розуміння природи, форм та механізмів інформаційного тероризму, а також вироблення знань і навичок з аналізу, прогнозування та протидії інформаційно-терористичним загрозам на міжнародному, регіональному та національному рівнях.

Основні цілі:

- ✓ засвоїти понятійно-категоріальний апарат тероризму та інформаційного тероризму;
- ✓ розкрити зміст, ознаки та види інформаційного тероризму;
- ✓ зрозуміти взаємозв'язок між інформаційним, медіа- та кібертероризмом;
- ✓ осягнути роль інформаційного тероризму як складника загроз міжнародній та національній безпеці.
- ✓ навчитися аналізувати інструменти, методи та наслідки інформаційно-терористичних атак;
- ✓ здійснювати порівняльний аналіз міжнародних, регіональних та національних моделей протидії інформаційному тероризму;
- ✓ оцінювати ефективність діяльності міжнародних організацій у сфері боротьби з інформаційним тероризмом.
- ✓ опанувати міжнародно-правову базу протидії тероризму та кібертероризму (конвенції, стратегії, директиви, рішення міжнародних організацій);
- ✓ набути навичок розпізнавання інформаційних атак, дезінформаційних кампаній і кібератак;
- ✓ розвинути здатність формувати пропозиції щодо удосконалення державної політики у сфері інформаційної та кібербезпеки.
- ✓ підготувати студентів до роботи у структурах міжнародної безпеки, аналітичних центрах, органах державної влади та міжнародних організаціях;
- ✓ сформувати компетентності для участі в розробці інформаційно-безпекових стратегій та заходів протидії інформаційному тероризму;
- ✓ поглибити розуміння ролі України в міжнародній системі кібербезпеки та її співпраці з провідними партнерами.

4. Програмні компетентності та результати навчання

Інтегральна компетентність: здатність розв’язувати складні задачі та проблеми у галузі міжнародних відносин, суспільних комунікації та регіональних студій, що передбачають проведення досліджень та/або здійснення інновацій та характеризуються невизначеністю умов і вимог.

Загальні компетентності:
ЗК 5. Здатність генерувати нові ідеї (креативність).
ЗК 6. Здатність працювати в міжнародному контексті.

Спеціальні компетентності:
СК 9. Здатність виявляти та аналізувати особливості розвитку країн та регіонів, сучасних глобальних, регіональних та локальних процесів, та місця в них України.
СК 10. Здатність до самонавчання, підтримки належного рівня знань, готовність до опанування знань нового рівня, підвищення своєї фаховості та рівня кваліфікації.

Програмні результати навчання:
РН 06. Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.

5. Організація навчання

Обсяг навчальної дисципліни

Вид заняття	Загальна кількість годин
лекції	**12**
семінарські заняття / практичні / лабораторні	**18**
самостійна робота	**90**

Ознаки навчальної дисципліни

Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
1			нормативний

Тематика навчальної дисципліни

Тема	кількість год.		
	лекції	Семінарські заняття	сам. роб.
Тема 1. Поняття та ознаки інформаційного тероризму	1	2	10

Тема 2. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці	1	2	10
Тема 3. Світовий досвід протидії інформаційному тероризму рамках міжнародних організацій	2	2	10
Тема 4. Світовий досвід протидії інформаційному тероризму в Америці та країнах Азії	2	2	10
Тема 5 Засоби протидії інформаційному тероризму держав Європи на регіональному рівні	2	2	10
Тема 6. Засоби протидії інформаційному тероризму держав Європи на національному рівні	2	2	10
Тема 7. Державна політика протидії тероризму в Україні	1	2	10
Тема 8. Інформаційний тероризм як загроза національній безпеці Україні	1	2	10
Тема 9. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму	-	2	10
ЗАГ.:	12	18	90

6. Система оцінювання навчальної дисципліни

Загальна система оцінювання навчальної дисципліни	Поточний контроль з дисципліни «Інформаційний тероризм» відбувається шляхом перевірки засвоєння студентами знань та умінь в ході семінарських занять, написання контрольної роботи, підготовки індивідуальної роботи та контролю самостійного опрацювання додаткової літератури. Перевірка засвоєння студентами знань та умінь в ході семінарських занять здійснюється шляхом оцінювання усних відповідей (в тому числі у формі презентацій), коротких письмових / тестових робіт. За опрацювання тем, визначених для семінарських занять студент може отримати максимально 30 балів. Відповідна форма активності студентів оцінюється за стобальною системою. У кінці семестру сума всіх оцінок ділиться на кількість оцінок та множиться на 6.
Вимоги до письмових робіт	Написання 1 письмової контрольної роботи (оцінюються за 100- бальною шкалою) є обов'язковим для виставлення підсумкової оцінки. У випадку, якщо здобувач не написав контрольну роботу, він вважається таким, що не виконав усі види робіт, що передбачаються силабусом. Контрольна робота включає 20 тестових питань та оцінюються 40 балами.
Семінарські заняття	Оцінювання результатів навчання здійснюється за 100-бальною шкалою. Виступи на семінарських заняттях передбачають перевірку рівня теоретичних знань, уміння працювати з джерелами та аналітичних навичок щодо інформаційного тероризму . **«Відмінно» (90–100 балів)** ✓ Здобувач освіти повно і ґрунтовно опанував теоретичний матеріал та: ✓ демонструє вільне володіння ключовими поняттями інформаційного та кібертероризму; ✓ орієнтується у міжнародних конвенціях, стратегіях, рішеннях ООН, НАТО, ОБСЄ, ЄС, а також українських нормативних актах у сфері інформаційної та кібербезпеки; ✓ вміє логічно, структуровано, доказово і аргументовано вибудовувати відповідь; ✓ здатний застосовувати теоретичні знання для аналізу конкретних кейсів (кібератак, інформаційних операцій, дезінформаційних кампаній);

	✓ уміє порівнювати підходи різних держав і міжнародних організацій, виявляти тенденції та причинно-наслідкові зв'язки; ✓ формулює власне експертне бачення проблематики та пропонує обґрунтовані рекомендації; ✓ демонструє високий рівень практичних навичок аналізу інформаційних загроз, роботи з даними CERT, кіберінцидентами, аналітичними матеріалами. **«Добре» (70–89 балів)** ✓ Здобувач освіти **добре засвоїв основний матеріал**, володіє змістом першоджерел і нормативних документів. Виявляє вміння: ✓ аналізувати основні види та прояви інформаційного і кібертероризму; ✓ пояснювати ключові процеси, спираючись на рекомендовану літературу та офіційні джерела; ✓ аргументовано висловлювати власну думку щодо механізмів протидії; ✓ виконувати аналіз практичних ситуацій, хоча з окремими неточностями; ✓ застосовувати знання на рівні адекватного, але не глибокого розбору кейсів. ✓ Допускаються окремі помилки в логіці викладу, використанні спеціальної термінології або у трактуванні практичних прикладів, однак загальний рівень підготовки є достатнім. **«Задовільно» (50–69 балів)** ✓ Здобувач освіти частково опанував матеріал, орієнтується у ключових джерелах, але: ✓ відповіді є непереконливими, з плутаниною у термінах кібербезпеки та інформаційного тероризму; ✓ демонструє поверхневе розуміння характерних ознак інформаційних атак; ✓ має труднощі з аналізом статистичних даних, кейсів кібератак, матеріалів CERT, аналітичних звітів; ✓ не завжди здатний обґрунтувати висновки або застосувати теоретичний матеріал до практичних ситуацій; ✓ аналітичні навички сформовані на мінімальному рівні. ✓ Практичні завдання виконані формально або поверхнево, без глибокого розуміння суті. **«Незадовільно» (менше 50 балів)** ✓ Здобувач освіти не опанував навчальний матеріал. Спостерігається: ✓ незнання основних термінів (кібертероризм, інформаційно-психологічна операція, кіберінцидент, інформаційна безпека тощо); ✓ відсутність розуміння нормативно-правової бази; ✓ невміння аналізувати кейси, статистику, офіційні дані і документи; ✓ відсутність системності у відповіді або її повна відсутність; ✓ аналітичні та практичні навички не сформовані.
Умови допуску до підсумкового контролю	Форма і терміни підсумкового контролю навчальної дисципліни визначаються навчальним планом. Здобувач(ка) отримує залік на останньому практичному занятті за умови виконання всіх передбачених силабусом навчальних робіт, відпрацювання усіх «заборгованостей» та набору не менше 50 і більше балів за всі види контролю.

Підсумковий контроль	Підсумкова оцінка за вивчення дисципліни складається із математичної суми балів за роботу на семінарах (максимально – 30 балів), отриманих балів за самостійну роботу (максимально – 15), за презентацію проєкту (максимально – 15), за контрольну роботу – максимально 40 балів, що в сумі максимально може скласти 100 балів. Підсумковий семестровий контроль дисципліни здійснюється у формі заліку. На останньому практичному занятті проводиться підсумкова контрольна робота і виставляється залік. Кількість тестових питань становить 20, кожне з яких оцінюється у 2 бали.

7. Політика навчальної дисципліни

Дисципліна базується на принципах академічної доброчесності, що передбачають самостійне виконання студентами навчальних і контрольних завдань, добросовісне використання джерел, відсутність плагіату, фабрикації чи фальсифікації даних. Будь-які порушення академічної доброчесності (списування, несанкціоноване користування під час контрольних робіт, використання чужих текстів без посилання, тощо) тягнуть за собою зниження оцінки або повторне проходження оцінювання. Ознайомитися з Положенням про академічну доброчесність можна на сайті університету: https://cnu.edu.ua/wp-content/uploads/2022/09/%D0%9D%D0%BE%D0%B2%D0%B0-%D1%80%D0%B5%D0%B4%D0%B0%D0%BA%D1%86%D1%96%D1%8F-%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D1%80%D0%BE-%D0%B7%D0%B0%D0%BF%D0%BE%D0%B1%D1%96%D0%B3%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B0%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D0%BE%D0%BC%D1%83-%D0%BF%D0%BB%D0%B0%D0%B3%D1%96%D0%B0%D1%82%D1%83.pdf?utm_source=chatgpt.com

Систематична присутність на лекційних і практичних заняттях є важливою складовою успішного засвоєння матеріалу. У разі пропуску занять студент повинен відпрацювати пропущені теми в установленому порядку. Завдання (тести, індивідуальні, контрольні, презентації) виконуються у визначені строки. Несвоєчасне подання без поважної причини знижує оцінку або може бути не зараховане. Усі виняткові ситуації узгоджуються з викладачем індивідуально. Оцінюється якість участі у дискусіях, здатність аргументовано висловлювати власну думку. Пасивна участь або порушення дисципліни негативно впливають на поточний рейтинг. Студенти зобов’язані дотримуватися правил етичної поведінки, поваги до викладача та одногрупників. Неповага, некоректні висловлювання чи порушення навчального процесу розглядаються як дисциплінарні порушення згідно з положеннями університету. Студенти можуть отримати додаткові бали за участь у наукових конференціях, круглих столах, проєктах, підготовку публікацій або проходження курсів неформальної освіти, пов’язаних із тематикою дисципліни. Такі бали зараховуються за рішенням кафедри міжнародних відносин. Результати неформальної освіти (сертифіковані онлайн-курси, тренінги, воркшопи) можуть бути зараховані в межах дисципліни відповідно до Положення. Викладач відкритий до комунікації зі студентами в межах консультацій, електронної пошти та навчальної платформи https://d-learn.pnu.edu.ua/. Рекомендується завчасно домовлятися про консультації, узгодження тем індивідуальних робіт і порядок відпрацювань.

8. Рекомендована література

1. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико правовий аспект / Р. О. Банк. // Інформація і право. - 2016. – №1. - С. 110-116.

2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок. В. Б. Толубко, В. О. Хорошко, В. О. Толюпа., 2015. - 288 с. 3. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.04 "Дипломатична академія

України при МЗС України" / Валюшко І. О. - К., 2018. - 210 с.

4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України |Електронний ресурс) / 0. В. Глазов // Наукові праці. Політологія. – 2012. – Режим доступу до ресурсу: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf.

5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк. // UkrainianScientificJournalofInformationSecurity. — 2013. — № 2.— С. 118-129.
6. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. / О.О. Грицун // Часопис Київського університету права. 2014. № 4. С. 312 - 317.

7. Гуцалюк М. Кібертероризм та заходи протидії / М. Гуцалюк. // Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матеріали міжнародної науково-практичної конференції. (30 вересня 2016 року, м. Київ). К.: Національна академія прокуратури України. - 2016. - С. 86-88. 8. Давиденко М. О. Протидія СБ України терористичній пропаганді у інформаційному середовищі України / М. О. Давиденко. // Актуальні проблеми управління інформаційною безпекою держави: збірник тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). Київ: Нац. Акад. СБУ,. - 2019. - С. 35-36. Режим доступу до ресурсу: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf

9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька. //LvivPolytechnicNationalUniversityInstitutionalRepository. — 2016. — № l. — С. 27-32. Режим доступу до ресурсу: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf

10. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23 листопада |Електронний ресурс]. - 2001. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_575

12. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. / Я. Малик [Електронний ресурс] // Ефективність державного управління. 2015. Вип. 44. С. 13- 20. Режим доступу до ресурсу: http://www. lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf

13. Мануйлов Є. М. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави / Є. М. Мануйлов, Ю. Ю. Калиновський. // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». - 2016. - № 2. - С. 144-153.

14. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці [Електронний ресурс] / М. Матула // Науковий блог. Національний університет «Острозька з академія». - 2014. – Режим доступу до ресурсу: https://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta mizhnarodnij-bezpetsi/

15 Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-VI[Електронний ресурс] // Верховна Рада – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/638-15

16. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII [Електронний ресуре] // Верховна | Рада України - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#n18 (Дата звернення: 20.08.2019).

17. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05 березня 2019 року № 53/2019. [Електронний ресуре] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/53/2019?lang=ru

18. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2469-19

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19

20. Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/287/2015

21. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016#n2 [Електронний ресуре] // Верховна Рада України - Режим доступу до ресурсу: :https://zakon.rada.gov.ua/laws/show/96/201 6#n2

22. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року 247/2017. № 247/2017[Електронний ресурс] // Верховна Рада України – Режим доступу до ресурсу: :https://zakon.rada.gov.ua/laws/show/47/2017

23. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн / Т. Ткачук [Електронний ресурс] // VisegradJournalonHumanRights. — 2018 - №1. - С 145-150. — Режим доступу до ресурсу: http://vjhr.sk/archive/2018_1/part 2/24.pdf

24. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико правовий аналіз / Т. Ткачук [Електронний ресурсі] // Підприємництво, господарство і право. - 2017. - №10 - С. 182-186. – Режим доступу до ресурсу: :http://pgp-journal. kiev.ua/archive/2017/10/38.

25. Форос А. В. Інформаційний тероризм як загроза національній безпеці України. /АВ. Форос // Правова держава. 2010. № 12. С. 256-261

26. Фролова 0. М. Роль ООН в системі міжнародної інформаційної безпеки. Міжнародні віносини [Електронний ресурс] / О. М. Фролова // Міжнародні віносини. Серія «Політичні науки». - 2018. - № 18-19. Режим доступу до ресурсу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468

27. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу / І. М. Харченко, С. О. Сапогов, В. М. Шамраєва, Л. В. Новікова / Вісник Харківського національного університету імені В. Н. Кразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм. - 2017. - №б. - С. 77-81. Режим доступу ресурсу: http://internationalrelationstourism.karazin.ua/themes/irtb/resources/2c5d772b29c5a9e2139a9f 6aa96834d0.pdt.

28 Яцик Т. П. Особливості інформаційного тероризму як Одного із способів інформаційної війни. / Т. П. Яцик // Науковий вісник Національного університету ДПС

України (економіка, право). 2014. № 2(65). С. 55-60.

29. Яцик Т. П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект) / Т. П. Яцик // Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія і практика). 2017. Вип. 1 (5). С. 111-115.

30. Струтинська Т., Дерещук Т., Романченко В. Виклики на шляху до ефективної протидії кіберзлочинності в Європейському Союзі. Наук. журн. «Філософія та політологія в контексті сучасної культури», 2022, Т. 14, № 2. - С. 110 – 118. https://fip.dp.ua/index.php/FIP/issue/view/38/PHIP%202022%2C%2014%282%29

Інформаційні ресурси

Законодавчі акти, нормативні документи, інструктивні, методичні матеріали та рекомендації міністерств і відомств:

Єдиний веб-портал органів виконавчої влади України. URL: http://www.kmu.gov.ua/

Нормативно-правова база України. URL: http://zakon3.rada.gov.ua

Офіційний сайт Верховної Ради України. URL: http://www.rada.gov.ua/

Наукова бібліотека КНУ. URL: http://lib.pnu.edu.ua/

Національна бібліотека України імені В.І. Вернадського. URL: http://www.nbuv.gov.ua/

Викладач Струтинська Т.З.