МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет історії, політології і міжнародних відносин

Кафедра міжнародних відносин

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційний тероризм

Освітня програма Магістр

Спеціальність 291 Міжнародні відносини, суспільні комунікації та регіональні студії

Галузь знань 29 Міжнародні відносини

Затверджено на засіданні кафедри
Протокол № __ від "_" ___ 2022 р.

м. Івано-Франківськ - 2022

ЗМІСТ

1. Загальна інформація	
Назва дисципліни	**Інформаційний тероризм**
Рівень вищої освіти	Другий (магістерський) рівень
Викладач	Струтинська Тетяна Зіновіївна
Контактний телефон викладача	+380975599132
E-mail викладача	tetiana.z.strutynska@pnu.edu.ua
Формат дисципліни	Цикл загальної підготовки Вибіркова дисципліна
Обсяг дисципліни	3 кредити
Посилання на сайт дистанційного навчання	http://www.d-learn.pnu.edu.ua
Консультації	2 год на тиждень

2. Анотація до курсу

Вибіркова навчальна дисципліна «Інформаційний тероризм» складена відповідно до освітньої програми підготовки магістрів спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань у сфері протидії інформаційному тероризму як загрози міжнародній та національній безпеці, а також практичних умінь та навичок правильного тлумачення та застосування механізмів інформаційної протидії тероризму, необхідних для їх майбутньої професійної діяльності у галузі міжнародних відносин, зовнішньої політики, міжнародних комунікацій та регіональних студій та при проведенні досліджень.

Підсумковий контроль – залік.

3. Мета та цілі курсу

Метою викладання навчальної дисципліни «Інформаційний тероризм» є глибоке усвідомлення студентами інформаційного тероризму. Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань у сфері протидії інформаційному тероризму як загрози міжнародній та національній безпеці, а також практичних умінь та навичок правильного тлумачення та застосування механізмів інформаційної протидії тероризму, необхідних для їх майбутньої професійної діяльності у галузі міжнародних відносин, зовнішньої політики, міжнародних комунікацій та регіональних студій та при проведенні досліджень.

Програма вивчення навчальної дисципліни вільного вибору «Інформаційний тероризм» складена відповідно до освітньої програми підготовки магістрів спеціальності 291 Міжнародні відносини, суспільні комунікації та регіональні студії.

4. Компетентності

Дисципліна покликана розвинути наступні компетентності:

Інтегральна компетентність – здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в сфері міжнародних відносин, суспільних комунікації та регіональних студій, які відповідають меті та завданням навчальної дисципліни

Загальні компетентності – здатність вчитися і оволодівати сучасними знаннями; генерувати нові ідеї (креативність); застосовувати знання у практичних ситуаціях; здатність до абстрактного мислення, аналізу та синтезу; здатність використовувати інформаційні та комунікаційні технології; спілкуватися державною мовою як усно, так і письмово; здатність до пошуку, оброблення та аналізу інформації з різних джерел; здатність бути критичним і самокритичним.

5. Результати навчання

Згідно з вимогами освітньої програми студенти повинні:

знати основні положення всіх тем, передбачених навчально-тематичним планом. Фундаментальні знання щодо природи, джерел та напрямів еволюції

міжнародних відносин, міжнародної політики, зовнішньої політики держав, стану

теоретичних досліджень міжнародних відносин та світової політики.
Поглиблені знання проблем міжнародної та національної безпеки, міжнародних та інтернаціоналізованих конфліктів, підходів, способів та механізмів забезпечення безпеки у міжнародному просторі та у зовнішній політиці держав.
Демонструвати системне сприйняття та розуміння положень, які відносяться до галузі знань «Міжнародні відносини» та є складовою професійної практики.
Визначати та прогнозувати політичні, дипломатичні, безпекові й інші ризики у сфері міжнародних відносин.
Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.
Навчальна дисципліна пов'язана із дисциплінами «Міжнародна інформація», «Міжнародна безпека», «Дипломатія і розвідка» та ін.

6. Організація навчання курсу

Обсяг курсу 90 год

Вид заняття	Загальна кількість годин
Лекції	14
семінарські заняття / практичні / лабораторні	18
самостійна робота	60

Ознаки курсу

Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
1	Міжнародні відносини	1	вибірковий

Тематика курсу

Тема, план	Форма заняття	Література	Завдання, год	Вага оцінки	Термін виконання
Тема 1. **Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.** Тероризм як явище. Характеристика Закону України «Про боротьбу з тероризмом». Поняття міжнародного тероризму. Складові терористичної дії (суб'єкт. об'єкт, причина і мотив, мета здійснення, часові та просторові характеристики. використовувані інструменти	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	Згідно розкладу

(засоби), наслідки). Поняття «інформаційний тероризм» та його характерні риси. Суб'єкти інформаційного тероризму. Характерні риси терористичних актів в інформаційній сфері. Види інформаційного тероризму (інформаційно-психологічний тероризм, інформаційно-технічний тероризм).					
Тема 2. **Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.** Медіа-тероризм, його характерні риси та способи здійснення. Кібертероризм, його характерні риси, види та способи здійснення. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем: правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	Згідно розкладу

змістом: правопорушення, пов'язані з порушенням авторських та суміжних прав).					
Тема 3. **Світовий досвід протидії інформаційному тероризму.** Протидія інформаційному тероризму в рамках міжнародних організацій та форумів. Протидія інформаційному тероризму в рамках ООН. Глобальна контртерористична стратегія ООН 2006 року. Протидія інформаційному тероризму в рамках НАТО. Роль Інтерполу у протидії інформаційному тероризму. Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. Концептуальні підходи до питання інформаційного	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	

тероризму, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. На Конференції з питань кіберпростору, та у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга. Періодизація превентивних заходів та контрзаходів світової спільноти у сфері протидії інформаційному тероризму.					
Тема 4**. Світовий досвід протидії інформаційному тероризму.** Механізми протидії інформаційному тероризму в США. Механізми протидії інформаційному тероризму в провідних державах Азії.	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	Згідно розкладу

Тема 5 **Засоби протидії інформаційному тероризму держав Європи на регіональному рівні**. Поняття регіональної системи безпеки. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року. Роль ОБСЄ у протидії інформаційному тероризму держав Європи. Хартія європейської безпеки 1999 року. Рішення Ради Міністрів ОБСЄ № 3/04 «Боротьба з використанням Інтернету в терористичних цілях» 2004 року. Рішення Ради Міністрів ОБСЄ Ме 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року. Протидія інформаційному тероризму в рамках ЄС. Ініціатива «Електронна Європа». Роль Агентства з мереж інформаційної безпеки (ЕМІЗА) у боротьбі з інформаційним тероризмом.	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	Згідно розкладу

Команда Реагування на Комп'ютерні надзвичайні події ЄС (СЕКТ ЕП). Європейський центр по боротьбі з кіберзлочинністю (ЕС3). Стратегія кібербезпеки ЄС 2013 року. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від 06.07.2016 року. Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи.					
Тема 6. **Засоби протидії інформаційному тероризму держав Європи на національному рівні.** Досвід Естонії та Литви у боротьбі з інформаційним тероризмом. Особливості протидії інформаційному тероризму у Великій Британії, Німеччині, Бельгії, Франції та Іспанії Досвід протидії інформаційному тероризму у Туреччині.	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8		Згідно розкладу

Тема 7. **Інформаційний тероризм як загроза національній безпеці.** Періодизація та види терористичних атак на інформаційний простір та кіберпростір України. Основні положення Законів України: «Про інформацію» «Про національну безпеку» року. «Про основні засади забезпечення кібербезпеки України» «Про захист інформації в інформаційно-телекомунікаційних системах». Основні положення Указу Президента України від 25 лютого 2017 року № 247/2017 «Про рішення Радинаціональної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Основні положення Указу Президента України від 15 березня 2016 року № 96/2016	Лекція Семінар Самостійна робота	Згідно списку літератури	2 2 8	1-5	Згідно розкладу

«Про рішення Ради національної безпеки і оборони Українивід 27 січня 2016 року «Про Стратегію кібербезпеки України ». Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CEBT-Ї А) у сфері протидії інформаційному тероризму. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом.					
Тема 8. **Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.**	Лекція Самостійна робота	Згідно списку літератури	2 4		Згідно розкладу
7. Система оцінювання курсу					
Загальна система оцінювання курсу		Поточний контроль – це оцінювання знань студента під час семінарських та практичних занять, якості виконання домашніх завдань, самостійної роботи та активності студента на занятті. Поточний контроль рівня засвоєння навчального матеріалу дисципліни оцінюється за п’ятибальною шкалою. За семестр студент набирає до 50 балів.			

<table>
<tr><td></td><td>Якщо студент жодного разу не відповідав на семінарських заняттях, матиме за відповідний поточний контроль 0 балів.
Форми участі студентів у навчальному процесі, які підлягають поточному контролю:
- Виступ з основного питання.
- Усна наукова доповідь.
- Доповнення, запитання до виступаючого, рецензія на виступ.
- Участь у дискусіях, інтерактивних формах організації заняття.
- Аналіз джерельної і монографічної літератури.
- Письмові завдання (тестові, контрольні, творчі роботи тощо).
- Реферат, есе (письмові роботи, оформлені відповідно до вимог).
Результати поточного контролю заносяться до журналу обліку роботи академічної групи.
Модульний контроль проводиться під час семінарських занять в академічній групі відповідно до розкладу занять. До контрольного заходу відповідного модульного контролю студент допускається незалежно від результатів поточного контролю. На консультаціях студент може відпрацювати пропущені семінарські заняття, захистити індивідуальні завдання, реферати, а також ліквідувати заборгованості з інших видів навчальної роботи. У разі відсутності студента на тестовому заході модульного контролю або при одержаній незадовільній оцінці за результатами модульного контролю йому надається право на повторне складання в індивідуальному порядку.
Контрольна робота оцінюється максимум 50 балів.
При контролі виконання завдань для самостійного опрацювання оцінці можуть підлягати: всі теми курсу; самостійне опрацювання тем загалом чи окремих питань; написання та публічний захист рефератів, есе; підготовка конспектів навчальних чи наукових текстів тощо.
<table>
<tr><td>Поточний контроль</td><td>Індивідуальна письмова робота</td><td>Залікова контрольна робота</td><td>Самостійна робота</td><td>Всього</td></tr>
<tr><td>20 балів</td><td>20 балів</td><td>50 балів</td><td>10 балів</td><td>100 балів</td></tr>
</table>
</td></tr>
<tr><td>Вимоги до письмової роботи</td><td>Доповіді та індивідуальні завдання за відповідними темами семінарських занять виконуються самостійно при консультуванні викладачем протягом вивчення навчальної дисципліни у відповідності до графіку навчального процесу. Даний вид роботи виконується з метою закріплення, поглиблення і узагальнення знань, одержаних студентами за час навчання та набуття практичних навичок їх застосування при вирішенні проблем публічного адміністрування. Доповіді та індивідуальні завдання допускають наявність</td></tr>
</table>

	наступних елементів наукового дослідження: практичної значущості; комплексного системного підходу до вирішення завдань дослідження; теоретичного використання передової сучасної методології і наукових розробок; наявність елементів творчості. Практична значущість докладів і індивідуальних завдань полягає в обґрунтуванні реальності їх результатів для потреб теорії та практики публічного адміністрування. Реальною вважається робота, яка виконана на основі аналізу результатів досліджень провідних фахівців в галузі публічного адміністрування, теоретичної бази щодо актуальних питань та запропонованої теоретико-методичної і методологічної баз щодо шляхів вирішення проблем, які існують в публічному адмініструванні. Комплексний системний підхід до розкриття теми доповідей і індивідуальних завдань полягає в тому, що предмет дослідження розглядається під різними точками зору – з позицій теоретичної бази і практичних напрацювань його реалізації в суспільній діяльності, в тісній взаємодії та єдиній логіці викладення. Застосування сучасної методології дослідження полягає в тому, що при підготовці докладів індивідуальних завдань студент повинен використовувати існуючу теоретичну базу й апарат наукових методів дослідження. В процесі підготовки доповідей і індивідуальних завдань разом з теоретичними знаннями і практичними навиками за фахом, студент повинен продемонструвати здібності до науково-дослідної роботи і уміння творчо мислити, навчитися вирішувати науково-прикладні актуальні завдання. Написання ІНДЗ на одну із запропонованих викладачем тем згідно наступних вимог: обсяг – 15-20 сторінок, 14 шрифт, 1,5 інтервал, поля: зліва, зверху, знизу – 20 мм, справа – 15 мм. Список літератури подавати наприкінці тексту. Посилання в тексті в квадратних дужках позиції у списку літератури, а друга – номер сторінки. Індивідуальне навчально-дослідне завдання передбачає: систематизацію, закріплення, розширення теоретичних і практичних знань із дисципліни і застосування їх при вирішенні конкретних виробничих завдань; розвиток навичок самостійної роботи з літературними джерелами і звітністю підприємства. Виконане ІНДЗ студент надає наприкінці семестру, але не пізніше терміну проведення підсумкового модульного контролю. Оцінка за виконання ІНДЗ враховується при виставленні загальної оцінки з дисципліни.
Семінарські заняття	На семінарських заняттях оцінці підлягають: рівень знань, продемонстрований у виступах, активність при обговоренні питань, відповіді на питання експрес-

	контролю тощо. Критеріями оцінки при усних відповідях можуть бути: повнота розкриття питання; логіка викладення; впевненість та переконливість, культура мови; використання основної та додаткової літератури (монографій, навчальних посібників, журналів, інших періодичних видань тощо); аналітичність міркування, вміння робити порівняння, висновки. Робота на семінарських заняттях оцінюється в діапазоні від 1 до 5 балів. При переведенні в бали сукупно можна набрати 30 балів.
Умови допуску до підсумкового контролю	Належне виконання: 1) змісту питань планів семінарських занять. Для цього необхідно готувати конспекти семінарських занять. Вітається якісна підготовка візуалізованих презентацій для відповідей на семінарські питання. Візуалізувана презентація на семінарське питання не повинна перевищувати 20 слайдів. Однак слід пам'ятати, що візуалізована презентація тільки доповнює підготовлену основну відповідь студента (-ки). 2) індивідуальної роботи.

8. Політика курсу

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Курс передбачає роботу в колективі. Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики. Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. Під час роботи над завданнями не допустимо порушення академічної доброчесності. Презентації та доповіді мають бути авторськими оригінальними.

Можливе зарахування результатів неформальної освіти у відповідності з про порядок зарахування результатів неформальної освіти у ДВНЗ «Прикарпатський національний університет імені Василя Стефаника».

9. 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. — № 1. — 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
11. Крупнейшие кибератаки против Украины: с 2014 года. Инфографика. [Електронний ресурс] // Новое время. – 2017. – Режим доступу до ресурсу: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-godainfografika1438924. html.
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. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені / В.І. Мітін // Международный научньй журнал «Интернаука». 2017. № 2 (24). 1 т. С. 65-68.
16. 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
17. 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).
18. 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
19. 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
20. 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
21. 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
22. 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
23. 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
24. 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
25. 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.
26. Форос А. В. Інформаційний тероризм як загроза національній безпеці України. /АВ. Форос // Правова держава. 2010. № 12. С. 256-261
27. 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
28. 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/2c5d772b29c5a9e2139a9f6aa96834d0.pdt.
29 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.
30. 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

Викладач Струтинська Т.З.