Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра міжнародних відносин, міжнародної інформації та безпеки

СИЛАБУС
навчальної дисципліни
Інформаційний тероризм

рівень вищої освіти: другий (магістерський)

галузь знань: 29 «Міжнародні відносини»
(шифр і назва)

спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
(шифр і назва)

освітня програма: «Міжнародна інформаційна безпека»
(шифр і назва)

спеціалізація: _____
(шифр і назва)

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

факультет Міжнародних економічних відносин та туристичного бізнесу

2019 / 2020 навчальний рік

РОЗРОБНИК СИЛАБУСУ: к.ю.н., доц. Доценко О. М.

Силабус схвалено на засіданні кафедри міжнародних відносин. міжнародної інформації та безпеки

Протокол від «27» 08 2019 року № 1

Завідувач кафедри _____ Новікова Л. В.
(підпис) (прізвище та ініціали)

1. Дані про викладача, що викладає дисципліну

Прізвище, ім’я по батькові викладача	Доценко Олена Михайлівна
Контактний тел.	0662847282
E-mail:	olena.dotsenko@karazin.ua
Розклад занять	четвер 17.00–18.20, ауд. 383-а
Консультації	вівторок 12.30–13.30, ауд. 264

2. Анотація дисципліни

У сучасних умовах дедалі більшого значення набуває роль інформації. В результаті активних процесів глобалізації та розвитку інформаційно-комунікаційних технологій та як наслідок, змін в соціально-інформаційній сфері, змінюються також інструменти реалізації державної політики, як внутрішньої так і зовнішньої, і поряд з економічними і політичними важелями впливу не менш важливими постають інформаційні. В епоху інформатизації, у XXI столітті, традиційні конфлікти перемістилися із матеріального простору в принципово новий – інформаційний, де маніпулятивні технології набувають дедалі ширшого використання. Завдяки їм ведуться інформаційні війни, знищуються опоненти, здійснюється вплив на маси і багато інших дій. Тому, останнім часом великої популярності набув інформаційний тероризм. Осмислення цього феномену є передумовою формування більш чітких уявлень щодо сутності сучасного міжнародного тероризму, запобігання деструктивного впливу на державні інститути і основи національної безпеки загалом.

Вивчення дисципліни «Інформаційний тероризм» спрямоване на отримання теоретичних знань поняття та характерних рис інформаційного тероризму як загрози міжнародні та національній безпеці держави і практичних умінь та навичок застосовувати механізми протидії йому.

Навчальна дисципліна належить до вибіркових дисциплін.

Пререквізити. Вивчення дисципліни передбачає попереднє засвоєння курсів з актуальних проблем міжнародних відносин та глобального розвитку, інформаційно-аналітичного забезпечення зовнішньої політики, пропаганди та контрпропаганди в міжнародних відносинах, а також міжнародних організацій в сфері безпеки.

Постреквізити. Основні положення навчальної дисципліни можуть застосовуватися при використанні їх у професійній діяльності та у подальшій науковій діяльності.

3. Опис навчальної дисципліни

3.1. ***Метою викладання*** навчальної дисципліни «Інформаційний тероризм» є формування у студенів 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, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

3.2. ***Основними завданнями*** вивчення дисципліни «Інформаційний тероризм» є: отримання та засвоєння студентами знань з певних питань, пов’язаних із теоретичними аспектами інформаційного тероризму та практичними способами протидії йому; формування у студентів практичних умінь та навичок роботи з міжнародними та національними нормативно-правовими актами та документами у сфері інформаційної безпеки; формування у студентів умінь та навичок вирішення аналітичних завдань та практичних казусів відповідно до програми курсу на підставі аналізу нормативних документів, а також навчальної та монографічної літератури; розвиток у студентів навичок аналітичного мислення, уміння логічно та професійно давати оцінку сучасним

міждержавним відносинам у світлі політики інформаційної безпеки держави, обґрунтовувати та висловлювати свою точку зору з проблем, пов'язаних з протидією інформаційному тероризму; вивчення форм, організації та інструментів переговорного процесу на міжнародному рівні; вивчення принципів дипломатичної теорії переговорів.

3.3. Кількість кредитів – 3.

3.4. Загальна кількість годин – 90.

3.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
3-й	-й
Лекції	
10 год.	год.
Практичні, семінарські заняття	
10 год.	год.
Лабораторні заняття	
- год.	год.
Самостійна робота	
70 год.	год.
Індивідуальні завдання	
- год.	

3.6. Заплановані результати навчання.

Перелік предметних компетентностей здобувача вищої освіти

ЗК 7	вміння аргументувати вибір шляхів вирішення завдань професійного характеру, критично оцінювати отримані результати та обґрунтовувати прийняті рішення;
ЗК 11	навички міжособистісної взаємодії, цінування та повага різноманітності та багатокультурності, здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів діяльності).
ФК 1	поглиблені знання про природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики;

У результаті засвоєння навчальної дисципліни здобувач вищої освіти повинен демонструвати такі результати навчання:

Знання:	
ПРН 34	знання природи та особливостей інформаційного тероризму / знання основних прийомів протидії кібертероризму та забезпечення кібербезпеки;
Уміння:	
ПРН 8	демонструвати в умовах усних ділових контактів з використанням прийомів і методів усного спілкування знання в царині міжкультурної комунікації та відповідних комунікативних технологій, застосовувати ситуаційний підхід з метою ефективного виконання професійних обов'язків;
ПРН 41	оцінювати природу та особливості інформаційного тероризму / володіти основними прийомами протидії кібертероризму та забезпечення кібербезпеки;
Навички:	
ПРН 48	мати практичні навички із протидії інформаційному тероризму /

	використовувати сучасні прийоми із протидії кібертероризму та забезпечення кібербезпеки;

4. Теми навчальної дисципліни

Розділ 1. Поняття інформаційного тероризму та способи протидії йому

Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці

Тероризм як явище. Закон України «Про боротьбу з тероризмом» від 20.03.2003 року № 638-IV. Поняття міжнародного тероризму. Складові терористичної дії (суб'єкт, об'єкт, причина і мотив, мета здійснення, часові та просторові характеристики, використовувані інструменти (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). 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 змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав).

Тема 2. 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 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 в сфері протидії інформаційному тероризму. Механізми протидії інформаційному тероризму в США. Механізми протидії інформаційному тероризму в провідних державах Азії.

Тема 3. Механізми протидії інформаційному тероризму держав Європи

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 № 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 (ENISA) у боротьбі з інформаційним тероризмом. Команда Реагування на Комп'ютерні надзвичайні події ЄС (CERT-EU). 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 (NIS Directive). Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. 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.

Тема 4. Інформаційний тероризм як загроза національній безпеці України

Періодизація та види терористичних атак на інформаційний простір та кіберпростір України. Основні положення Законів України: «Про інформацію» № 2657-XII від 2 жовтня 1992 року, «Про національну безпеку» № 2469-VIII від 21 червня 2018 року, «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року. Основні положення Указу Президента України від 25 лютого 2017 року № 247/2017 «Про рішення Ради національної 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 «Про рішення Ради національної безпеки і оборони України від 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 (CERT-UA) у сфері протидії інформаційному тероризму. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.

5. Схема навчальної дисципліни

Назви розділів і тем	Кількість годин/тижнів			
	денна форма			
	усього	у тому числі		
		лекційне заняття	прак. заняття	сам. роб.
2	3	4	5	6
Розділ 1. Основні теоретичні концепції міжнародних відносин				
Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.	19 год	2 год/ 1 тиж	2 год/ 2 тиж	15 год
Тема 2. Світовий досвід протидії інформаційному тероризму.	23 год	2 год/ 3 тиж	2 год/ 4 тиж	15 год
Тема 3. Механізми протидії інформаційному тероризму держав Європи	29 год	4 год/ 5, 7 тиж	4 год/ 6, 8 тиж	25 год
Тема 4. Інформаційний тероризм як загроза національній безпеці України.	19 год	2 год/ 9 тиж	2 год/ 10 тиж	15 год
Усього годин	***90 год***	***10 год***	***10 год***	***70 год***

6. Завдання для самостійної роботи та показники академічної активності здобувачів вищої освіти

№ теми	Види, зміст самостійної роботи
1	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв’язати завдання за темою. **Питання для контролю засвоєння знань:**

	1) Дайте визначення тероризму. 2) Дайте визначення терористичної діяльності**.** 3) Назвіть обов'язкові складові тероризму як цілеспрямованої дії. 4) Дайте визначення поняття «міжнародний тероризм». 5) Дайте визначення інформаційного тероризму. 6) Назвіть характерні риси терористичних актів в інформаційній сфері. 7) Назвіть види інформаційного тероризму. 8) У чому полягає сутність медіа-тероризму? 9) Визначте характерні риси кібертероризму. 10) Назвіть види правопорушень проти цілісності та доступності комп'ютерних даних і систем. **Завдання:** 1. Підготувати доповіді / презентації з наступних тем: 1) Міжнародний тероризм як загроза глобальній безпеці. 2) Медіа-тероризм: сутність та способи протидії. 3) Кібертероризм: сутність та способи протидії. 4) Правопорушення проти цілісності та доступності комп'ютерних даних і систем. 2. Ознайомитися із Законом України «Про боротьбу з тероризмом» від 20.03.2003 року №638-IV https://zakon.rada.gov.ua/laws/show/638-15 та вміти характеризувати основні принципи, організаційні основи боротьби з тероризмом, засади міжнародного співробітництва у сфері боротьби з тероризмом. 3. Ознайомитися з документальним фільмом «Інформаційний тероризм» https://www.youtube.com/watch?v=PziD0tDuxX0 та бути готовим до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у фільмі.
2	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв'язати завдання за темою. **Питання для контролю засвоєння знань:** 1) Визначте роль Резолюцій ГА ООН «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» 1999, 2002, 2005 років у протидії інформаційному тероризму. 2) Визначте роль Резолюції ГА ООН A/RES/60/288 «Глобальна контртерористична стратегія ООН» від 20 вересня 2006 року у протидії інформаційному тероризму. 3) Визначте особливості протидії інформаційному тероризму в рамках НАТО. 4) Визначте роль Інтерполу у протидії інформаційному тероризму. 5) Дайте характеристику Угоди між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. 6) Визначте концептуальні підходи до питання інформаційного тероризму, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. на Конференції з питань кіберпростору. 7) Визначте концептуальні підходи до питання інформаційного тероризму, що закріплені у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга. 8) Дайте періодизацію превентивних заходів та контрзаходів світової спільноти в сфері протидії інформаційному тероризму. 9) Визначте особливості механізмів протидії інформаційному тероризму в

	США. 10) Визначте особливості механізмів протидії інформаційному тероризму в провідних державах Азії. **Завдання:** 1. Підготувати доповіді / презентації з наступних тем: 1) Протидія інформаційному тероризму в рамках ООН. 2) Протидія інформаційному тероризму в рамках НАТО. 3) Роль Інтерполу у протидії інформаційному тероризму. 4) Механізми протидії інформаційному тероризму в США. 5) Механізми протидії інформаційному тероризму в провідних державах Азії. 2. Ознайомитися із статтею Фролової О. М. «Роль ООН в системі міжнародної інформаційної безпеки» http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468/3140 та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті. 3. Ознайомитися із річним звітом 2018 APCERT – Спеціальної групи реагування на надзвичайні ситуації в інформаційному комп'ютерному просторі в Азіатсько-Тихоокеанському регіоні https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2018.pdf та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у звіті.
3	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв’язати завдання за темою. **Питання для контролю засвоєння знань:** 1) Що розуміється під регіональною системою безпеки? 2) Визначте роль Паризької хартії для нової Європи 1990 року і Додаткового документу до неї 1990 року у сфері інституалізації системи європейської регіональної безпеки. 3) Визначте роль Лісабонської декларації від 1 січня 1996 року «Про моделі загальної і всеосяжної безпеки для Європи XXI століття» та Хартії європейської безпеки, прийнятої на Стамбульській зустрічі ОБСЄ на вищому рівні 19 листопада 1999 року у сфері побудови системи європейської регіональної безпеки. 4) Дайте загальну характеристику Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року. 5) Визначте роль ОБСЄ у протидії інформаційному тероризму у державах Європи. 6) Що таке «Ініціатива «Електронна Європа»? 7) Визначте роль Агентства з мереж і інформаційної безпеки (ENISA) у протидії інформаційному тероризму у державах Європи. 8) Що таке «Вчення Cyber Europe»? 9) Визначте роль Групи реагування на надзвичайні ситуації (CERT-EU) у протидії інформаційному тероризму у державах Європи. 10) Визначте роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. 11) Що передбачає Стратегія кібербезпеки Естонії 2014 року у сфері протидії кібертероризму? 12) Визначте роль Таллінського центру кіберзахисту НАТО у боротьбі з кібертероризмом? 13) Що передбачає Стратегія кібербезпеки Литви 2011 року у сфері протидії

	кібертероризму? 14) Визначте роль Національного центру кібербезпеки при Міністерстві національної оборони (NCSC) у боротьбі з кібертероризмом в Литві? 15) Назвіть основні напрямки Стратегії Кібербезпеки Туреччини 2012 року. 16) Визначте роль Національного Центру із захисту критичної інфраструктури (CNPIC) у боротьбі з інформаційним тероризмом в Іспанії. 17) Визначте роль Національного агентства безпеки інформаційних систем (ANSSI) у боротьбі з інформаційним тероризмом у Франції. 18) Визначте роль Аудіовізуальної вищої ради (CSA) у боротьбі з інформаційним тероризмом у Бельгії. 19) Визначте роль Федерального офісу інформаційної безпеки (BSI) у боротьбі з інформаційним тероризмом у Німеччині. 20) Визначте роль Національного агентства з питань злочинності (NCA) у боротьбі з інформаційним тероризмом у Великій Британії. **Завдання:** 1. Підготувати доповіді / презентації з наступних тем: 1) Роль Ради Європи у протидії інформаційному тероризму у державах Європи. 2) Загальна характеристика Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року. 3) Роль ОБСЄ у протидії інформаційному тероризму у державах Європи. 4) Роль Агентства з мереж і інформаційної безпеки (ENISA) у протидії інформаційному тероризму у державах Європи. 5) Роль Групи реагування на надзвичайні ситуації (CERT-EU) у протидії інформаційному тероризму у державах Європи. 6) Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. 7) Роль Таллінського центру кіберзахисту НАТО у боротьбі з кібертероризмом. 8) Роль CERT-UK та GovCertUK у протидії кібертероризму у Великій Британії. 9) Досвід протидії інформаційному тероризму у Туреччині. 10) Досвід протидії інформаційному тероризму в Естонії. 2. Ознайомитися із Директивою Європейського парламенту і ради (ЄС) 2016/1148 від 06.07.2016 року про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем на території Союзу (NIS Directive) https://zakon.rada.gov.ua/laws/show/984_013-16 та бути готовими обговорення її змісту. 3. Ознайомитися із Угодою між Україною та Європейським поліцейським офісом про стратегічне співробітництво від 14.12.2016 року https://zakon.rada.gov.ua/laws/show/984_001-16 та бути готовими обговорення її змісту. 4. Ознайомитися із спеціальним звітом компанії FireEye 2017 щодо кіберзагроз державам Європи https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdfhttps://zakon.rada.gov.ua/laws/show/984_013-16 та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у звіті. 5. Ознайомитися із показниками Глобального індексу кібербезпеки 2018 по Європейському регіону https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf та бути готовими до дискусії та обґрунтування своєї точки зору з цього питання.
4	Ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю

	знань, розв’язати завдання за темою. **Питання для контролю засвоєння знань:** 1) Визначте хронологію терористичних атак на національний інформаційний та кіберпростір України, починаючи з 2014 року. 2) Визначте нормативно-правову базу протидії інформаційному тероризму в Україні. 3) Що може бути віднесено до об’єктів критичної інфраструктури відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2019 року? 4) Визначтне основні повноваження державних органів у сфері захисту інформації в системах відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 року. 5) Охарактеризуйте основні положення Указу Президента України від 25 лютого 2017 року № 247/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». 6) Охарактеризуйте основні положення Указу Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». 7) Назвіть основні завдання Кіберполіції України. 8) Назвіть основні функції Державного центру кіберзахисту та протидії кіберзагрозам в Україні. 9) Назвіть завдання CERT-UA. 10) Визначте роль Державної служби спеціального зв’язку та захисту інформації України в сфері протидії інформаційному тероризму. **Завдання:** 1. Підготувати доповіді / презентації з наступних тем: 1) Роль Служби безпеки України у боротьбі з інформаційним тероризмом. 2) Роль Кіберполіції України у боротьбі з інформаційним тероризмом. 3) Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом. 4) Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CERT-UA) у сфері протидії інформаційному тероризму. 5) Співробітництво України з міжнародними організаціями та інституціями у сфері протидії інформаційному тероризму. 2. Ознайомитися із статтею з порталу BBC Future стосовно кібератаки на Україну https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті. 3. Ознайомитися із статтею Жайворонка О. І. «Вдосконалення механізму протидії інформаційному тероризму в Україні в загальнодержавній системі антикризового реагування» http://www.investplan.com.ua/pdf/17_2018/22.pdf та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

Кафедра міжнародних відносин, міжнародної інформації та безпеки бере до уваги такі показники академічної активності та додаткових освітніх досягнень здобувачів вищої освіти:

- відповіді на питання плану семінарського заняття під час заняття;
- доповіді з проблемних питань семінарського заняття;
- участь в активних формах навчання на семінарських заняттях;

– розробка тематичних презентацій і кейсів;

– участь у роботі наукового гуртка: публікація тез доповідей та участь у конференціях, написання наукових статей, есе, рефератів;

– відпрацювання тем пропущених практичних занять;

– інші здобутки у сфері міжнародних відносин, міжнародної інформації та безпеки, що підтверджені документально (грамоти, дипломи, сертифікати тощо).

7. Вимоги викладача

При вивченні дисципліни «Інформаційний тероризм» необхідно спиратися на конспект лекцій та рекомендовану літературу. Водночас вітається використання інших джерел з альтернативними поглядами на ті чи інші питання задля формування продуктивної дискусії та різнобічного вивчення тем.

Високо оцінюється прагнення здобувачів вищої освіти:

– регулярно відвідувати заняття;

– планомірно та систематично засвоювати навчальний матеріал;

– активно працювати на семінарських заняттях: брати участь в обговоренні дискусійних питань та кейсів;

– повною мірою долучатися до активних форм навчання;

– відпрацьовувати пропущені семінарські заняття.

Обов’язковою вимогою є дотримання норм академічної поведінки та етики.

8. Методи контролю

При вивченні дисципліни застосовується поточний та підсумковий семестровий форми контролю. Також, передбачено обов’язковий контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу.

Поточний контроль (засвоєння окремих тем) проводиться у формі усного опитування, доповідей і повідомлень студентів, розв’язання ситуативних та тестових завдань, навчальних дискусій, виконання творчих завдань.

Підсумковий семестровий контроль з дисципліни є обов’язковою формою контролю навчальних досягнень здобувачів вищої освіти. Він проводиться у письмовій формі у вигляді підсумкового семестрового контролю (залік) (за дворівневою шкалою оцінювання). Терміни проведення підсумкового семестрового контролю встановлюються графіком навчального процесу, а обсяг навчального матеріалу, який виноситься на підсумковий семестровий контроль, визначається робочою програмою дисципліни.

Сумарна кількість рейтингових балів за вивчення дисципліни за семестр розраховується як сума балів, отриманих за результатами поточного контролю та балів, отриманих за результатами підсумкового семестрового контролю. Максимальна сума балів за семестр складає 100 балів.

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання					Залікова робота	Сума
Розділ 1				Разом		
Т1	Т2	Т3	Т4	60	40	100
14	12	20	14			

Т1, Т2 ... – теми розділів.

Критеріями оцінювання знань за поточний контроль є успішність освоювання знань та набутих навичок на лекціях та семінарських заняттях, що включає систематичність їх

відвідування, здатність здобувача вищої освіти засвоювати категорійний апарат, вміння орієнтуватися у сучасних подіях в світі і державі, навички узагальненого мислення, логічність та повноту викладання навчального матеріалу, навички творчо підходити до вирішення поставлених завдань, активність роботи на семінарських заняттях, рівень знань за результатами опитування на семінарських заняттях, самостійне опрацювання тем уцілому чи окремих питань.

Схема нарахування балів за поточним контролем (засвоєння теми дисципліни):

10–14 балів – здобувач вищої освіти цілком і всебічно розкрив сутність питань теми, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, висока активність роботи на семінарському занятті, уміння сформувати своє ставлення до певної проблеми теми та аргументовано його доводити, вміння мислити абстрактно і узагальнено, здатність публічно представити матеріал.

5–9 балів – здобувач вищої освіти розкрив питання теми у загальних рисах, розуміє їхню сутність, вільно оперує поняттями і термінологією, але спостерігаються деякі упущення при відповідях на питання та неточні обґрунтування, активна робота на семінарському занятті, допущення декількох незначних помилок при виконанні завдань, здатність публічно представити матеріал;

1–4 балів – здобувач вищої освіти не повністю розкрив питання теми у загальних рисах, намагається робити висновки, але слабко орієнтується в джерелах, припускається помилок, матеріал викладає нелогічно, пасивна робота на семінарських заняттях (участь у роботі останніх лише за наявності стимулу з боку викладача), наявність певного уявлення щодо матеріалу тем змістовного розділу, неповні відповіді, допущення значної кількості помилок при виконання завдання.

0 балів – здобувач вищої освіти не розкрив питання теми, не розуміє його сутності, не орієнтується в джерелах, пасивність у роботі на семінарських заняттях, відсутність знань за темою дисципліни, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдання, невміння публічно представити матеріал

Підсумковий семестровий контроль з дисципліни проводиться за заліковими завданнями. Кожне із завдань містить 2 теоретичні питання. Максимальна кількість балів, яка може бути нарахована за перше та друге теоретичне питання, дорівнює 20 балів.

Схема нарахування балів за одне теоретичне питання залікового завдання:

17–20 балів – здобувач вищої освіти цілком і всебічно розкрив сутність питання, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідних питань і може аргументовано її доводити;

11–16 балів – здобувач вищої освіти достатньо повно і всебічно розкрив сутність питання, вільно оперує поняттями і термінологією, але спостерігаються деякі упущення при відповідях на питання та неточні обґрунтування;

5–10 балів – здобувач вищої освіти розкрив питання у загальних рисах, розуміє його сутність, намагається робити висновки, але слабко орієнтується в джерелах, припускається помилок, матеріал викладає нелогічно;

0–4 балів – здобувач вищої освіти не розкрив питання навіть у загальних рисах, не розуміє його сутності, слабко орієнтується чи не орієнтується в джерелах, припускається грубих помилок, матеріал викладає нелогічно.

Набрана кількість рейтингових балів є основою для оцінки за національною шкалою. Шкала оцінювання наведена нижче.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90–100	відмінно	

70–89	добре	зараховано
50–69	задовільно	
1–49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* 2016. № 1 (16). С. 110–116.
2. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.
3. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.
4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України. *Наукові праці. Політологія.* 2012. Випуск 185. Том 197. URL: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf (Дата звернення: 22.08.2019).
5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security.* 2013. Vol. 19. Issue 2. С. 118–129.
6. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права.* 2014. № 4. С. 312–317.
7. Гуцалюк М. Кібертероризм та заходи протидії. *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. *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. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення: 22.08.2019).
9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Lviv Polytechnic National University Institutional Repository.* 2016. Vol. 2. No. 1. P. 27–32. URL: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (дата звернення: 20.08.2019).
10. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 22.08.2019).
11. Крупнейшие кибератаки против Украины с 2014 года. Инфографика. *Новое время*. – 2017. URL: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-goda-infografika-1438924.html. (Режим доступа: 24.05.2019).
12. Макаренко Є. Інформаційне протиборство у сучасних міжнародних відносинах. Міжнародні відносини. Серія «Політичні науки». 2017. № 17. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3316/2995 (дата звернення: 20.08.2019).
13. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління. 2015. Вип. 44. С. 13–20. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf (дата звернення: 20.08.2019).

14. Мануйлов Є. М., Ю. Ю. Калиновський. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2016. № 2 (29). С. 144–153.
15. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. *Науковий блог. Національний університет «Острозька академія».* 03.07.2014. URL: https://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (дата звернення: 22.08.2019).
16. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені. *Международный научный журнал «Интернаука».* 2017. № 2 (24). 1 т. С. 65–68.
17. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення 22.05.2019).
18. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#n18 (дата звернення: 20.08.2019).
19. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05 березня 2019 року № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019?lang=ru (дата звернення: 20.08.2019).
20. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 20.08.2019).
21. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.08.2019).
22. 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. URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 20.08.2019).
23. 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. URL: https://zakon.rada.gov.ua/laws/show/96/2016#n2 (дата звернення: 22.08.2019).
24. 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. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 20.08.2019).
25. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими из киберпространства. *ОБСЕ.* 2013. URL: https://www.osce.org/ru/secretariat/110472?download=true (дата звернення: 22.08.2019).
26. Самые громкие кибер-атаки на критические инфраструктуры. *Habr.* 30 ноября 2016. URL: https://habr.com/ru/company/panda/blog/316500/ (дата звернення: 22.08.2019).
27. Семен Н. Ф. Російські Інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): дис. … канд. наук з соц. комун.: 27.00.01 / Міжнародний економіко-гуманітарний університет імені акад. С. Демянчука; Дніпровьский національний університет імені Олеся Гончара. Рівне, 2018. 250 с.
28. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн. *Visegrad Journal on Human Rights.* 2018. № 1 (Volume 2). С. 145–150. URL: http://vjhr.sk/archive/2018_1/part_2/24.pdf (дата звернення: 20.08.2019).
29. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182–186. URL: http://pgp-journal.kiev.ua/archive/2017/10/38.pdf (дата звернення: 20.08.2019).

30. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України: дис. … докт. юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет. Ужгород, 2019. 487 с.
31. Форос А. В. Інформаційний тероризм як загроза національній безпеці України. *Правова держава.* 2010. № 12. С. 256–261.
32. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. Міжнародні віносини. Серія «Політичні науки». 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468 (дата звернення: 22.08.2019).
33. Харченко І. М., Сапогов С. О., Шамраєва В. М., Новікова Л. В. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. Вісник Харківського національного університету імені В. Н. Кразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм. 2017. Випуск 6. С. 77–81. URL: http://international-relations-tourism.karazin.ua/themes/irtb/resources/2c5d772b29c5a9e2139a9f6aa96834d0.pdf (дата звернення: 20.08.2019).
34. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право).* 2014. № 2(65). С. 55–60.
35. Яцик Т. П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект). *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія і практика).* 2017. Вип. 1 (5). С. 111–115.
36. Directive (Eu) 2016/1148 Of The European Parliament and Of The Council concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*. 2016. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Last Accessed: 22.05.2019).
37. European Commission. «eEurope - An information society for all». URL: http://europa.eu/rapid/press-release_SPEECH-01-180_en.htm?locale=ru (Last Accessed: 22.05.2019).
38. Global Cybersecurity Index (GCI) 2018. Studies & Research. ITUPublications, 2019. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Last Accessed: 22.08.2019).
39. Kumar M. European Union Parliament Under Cyber Attack! *The Hacker News.* March 29, 2011. URL: https://thehackernews.com/2011/03/european-union-parliament-under-cyber.html (Last Accessed: 22.08.2019).
40. Lemos R. Cyberterrorism: The Real Risk. *Computer Crime Research Center (CCRC)*. URL: http://www.crime%research.org/library/Robert1.htm (дата звернення: 22.08.2019).

Допоміжна література

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: автореф. дис. ... канд. наук з державного управління: 25.00.02 / Національна академія державного управління при Президентові України. Київ, 2017. 21 с.
2. Возженников А. В. Международный терроризм: борьба за геополитическое господство. *Эксмо.* Москва. 2007. 528 с.
3. Градов А. П. Деятельность Североатлантического союза в сфере кибербезопасности. *Зарубежное военное обозрение*. 2014. Вып. 7. С. 13–16.
4. Григорьев Н. Ю., Родюков Э. Б. Современный кибернетический терроризм и его социальные последствия. *Вестник университета.* 2016. № 5. С. 227–234.
5. Довгань О. Д., Хлань В. Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави.* № 3 (7), 2011. С. 49–53.

6. Журавель В. Противодействие угрозе кибертерроризма. *Зарубежное военное обозрение.* 2018. №5. С. 12–15.
7. Корченко О. Г., Бурячок В. Л., С. О. Гнатюк. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації.* 2013. Т. 19. № 1. С. 40–45.
8. Лазарев Н. Я. Терроризм как социально-политическое явление: истоки, формы и динамика развития в современных условиях: дис. … канд. полит. наук: 23.00.01 / Государственный университет управления. Москва, 2007. 172 с.
9. Негодченко В. Основні напрями державної інформаційної політики в Україні. Підприємництво, господарство і право. 2016. № 4. С. 77–81. URL: http://pgp-journal.kiev.ua/archive/2016/04/15.pdf (дата звернення: 20.08.2019).
10. Правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт Европейского союза / Отв. ред. В. Г. Киютин. А. П. Новиков. Бишкек-Москва, 2010. 239 с.
11. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації.* 2016. № 4. С. 65–70.
12. Широкова-Мурараш О. Г., Акчурін Ю. Р. Кіберзлочинність та кібертероризм як загроза міжнародній інформаційній безпеці: міжнародно-правовий аспект. *Інформація і право.* 2011. № 1. С. 76–81.
13. Collins A. Contemporary Security Studies. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.
14. ENISA. Cyber Europe 2018: After Action Report. 2018. URL: https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report (Last Accessed: 22.08.2019).
15. Petya Ransomware Outbreak: Here's What You Need To Know, Symantec Security Response. *Symantec.* 24 October, 2017. URL: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Last Accessed: 22.08.2019).

11. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Верховна Рада України - www.zakon1.rada.gov.ua.
2. Міністерство закордонних справ - http://mfa.gov.ua/ua
3. Міністерство юстиції - https://minjust.gov.ua/ua
4. Конституційний Суд України - http://www.ccu.gov.ua/uk/index
5. Організація Об'єднаних Націй - http://www.un.org/
6. Європейський суд з прав людини - http://echr.coe.int/
7. Європейський союз - http://eeas.europa.eu/
8. Організація з безпеки та співробітництва в Європі - http://www.osce.org/
9. Рада Європи - http://www.coe.int/web/portal/home
10. Управління Верховного комісара ООН з прав людини - http://www.ohchr.org/
11. Національна парламентська Бібліотека України - http://www.nplu.org/
12. Національна бібліотека України імені В. І. Вернадського - www.nbuv.gov.ua
13. Київська центральна міська публічна бібліотека ім. Лесі Українки - http://lucl.lucl.kiev.ua
14. Центральна наукова бібліотека Харківського національного університету ім. В.Н. Каразіна - http://www.univer.kharkov.ua
15. Харківська державна наукова бібліотека ім. В. Г. Короленка - http://korolenko.kharkov.com
16. European Union Agency For Cybersecurity (ENISA) – https://www.enisa.europa.eu/
17. Computer Emergency Response Team of Ukraine (CERT-UA) – https://cert.gov.ua/
18. Офіційний сайт кіберполіції України – https://cyberpolice.gov.ua/

12. Перелік питань до заліку

Заліковий білет (завдання) містить 2 завдання, які полягають у розгорнутій відповіді на теоретичні питання курсу.

Питання для підготовки:

1. Складові терористичної дії.
2. Поняття «інформаційний тероризм» та його характерні риси.
3. Медіа-тероризм, його характерні риси та способи здійснення.
4. Кібертероризм, його характерні риси, види та способи здійснення.
5. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами).
6. Види правопорушень в інформаційній сфері (правопорушення, пов'язані зі змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав).
7. Протидія інформаційному тероризму в рамках ООН.
8. Протидія інформаційному тероризму в рамках НАТО.
9. Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року.
10. Концептуальні підходи до питання інформаційного тероризму (Конвенція про забезпечення міжнародної інформаційної безпеки та проект «Загального договору з питань кібербезпеки та кіберзлочинності» (Договорі Шольберга).
11. Періодизація превентивних заходів та контрзаходів світової спільноти в сфері протидії інформаційному тероризму.
12. Механізми протидії інформаційному тероризму в США.
13. Механізми протидії інформаційному тероризму в провідних державах Азії.
14. Загальна характеристика Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року.
15. Роль ОБСЄ у протидії інформаційному тероризму держав Європи.
16. Загальна характеристика механізмів протидії інформаційному тероризму в рамках ЄС.
17. Роль Агентства з мереж інформаційної безпеки (ENISA) у боротьбі з інформаційним тероризмом. Команда Реагування на Комп'ютерні надзвичайні події ЄС (CERT-EU).
18. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від 06.07.2016 року (NIS Directive).
19. Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи.
20. Досвід Естонії та Литви у боротьбі з інформаційним тероризмом.
21. Досвід Німеччини та Франції у боротьбі з інформаційним тероризмом.
22. Особливості протидії інформаційному тероризму у Великій Британії та Бельгії.
23. Досвід протидії інформаційному тероризму у Туреччині та Іспанії.
24. Періодизація та види терористичних атак на інформаційний простір та кіберпростір України.
25. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року.
26. Основні положення Указу Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
27. Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом.
28. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CERT-UA) у сфері протидії інформаційному тероризму.

29. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом.
30. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.