МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА

Кафедра міжнародних відносин, міжнародної інформації та безпеки

КОМПЛЕКС НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ

з дисципліни
«ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ»

рівень вищої освіти: другий (магістерський)
галузь знань: 29 «Міжнародні відносини»
спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітня програма: «Міжнародна інформаційна безпека»
вид дисципліни: за вибором
факультет міжнародних економічних відносин та туристичного бізнесу

Укладачі: канд. юрид. наук, доц. Доценко О. М.
канд. юрид. наук Зіняк Л.В.

2020 / 2021 навчальний рік

1. НАВЧАЛЬНИЙ КОНТЕНТ (РОЗШИРЕНИЙ ПЛАН ЛЕКЦІЙ)

РОЗДІЛ 1. ПОНЯТТЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ ТА СПОСОБИ ПРОТИДІЇ ЙОМУ

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

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

Навчальні питання:

1. Тероризм як явище.

Загальна характеристика Закону України «Про боротьбу з тероризмом» від 20.03.2003 року № 638-IV.

Тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних ціле.

Терористична діяльність – діяльність, яка охоплює: планування, організацію, підготовку та реалізацію терористичних актів; підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях; організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах; вербування, озброєння, підготовку та використання терористів; пропаганду і поширення ідеології тероризму; фінансування та інше сприяння тероризму.

Тероризм представляє собою цілеспрямовану дію, отже обов’язковими складовими цієї специфічної дії є: суб’єкт (або суб’єкти); об’єкт (об’єкти); причина і мотив; мета здійснення; часові та просторові характеристики; використовувані інструменти (засоби); наслідки.

Міжнародний тероризм – це здійснювані у світовому чи регіональному масштабі терористичними організаціями, угрупованнями, у тому числі за підтримки державних органів окремих держав, з метою досягнення певних цілей суспільно небезпечні насильницькі діяння, пов’язані з викраденням, захопленням, вбивством ні в чому не винних людей чи загрозою їх життю і здоров’ю, зруйнуванням чи загрозою зруйнування важливих народногосподарських об’єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження.

2. Поняття «інформаційний тероризм» та його характерні риси.

Широкомасштабне використання інформаційно-комунікаційних технологій та підвищення рівня залежності держав, а саме їх критично-важливих інфраструктур, від новітніх технологій спровокували появу нового явища у сфері міжнародної інформаційної безпеки – інформаційного

тероризму. Інформаційний тероризм – злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій.

Суб'єкти інформаційного тероризму: іноземні спецслужби та інституції; вітчизняні та міжнародні ЗМІ; певні екстремістські угрупування.

Характерні риси терористичних актів в інформаційній сфері: 1) прихований характер підготовки та реалізації таких діянь – відсутність проявів та слідів проникнення; 2) масштабність атак – нанесення удару по великій кількості об'єктів; 3) синхронність атак – вони можуть бути здійснені одночасно по багатьом об'єктам; 4) віддаленість – джерело атаки може знаходитись за межами країни, в якій здійснюється напад; 5) інтернаціональність – шкода може поширюватись на території кількох держав

Види інформаційного тероризму: інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій); інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації і т. п.).

Медіа-тероризм, його характерні риси та способи здійснення. Сутність медіа-тероризму полягає у спробах шляхом організації спеціальних медіа-кампаній дестабілізувати суспільство, створити у ньому атмосферу громадянської непокори, недовіри суспільства до дій та намірів влади й особливо – її силових структур, покликаних захищати суспільний порядок.

Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, різноманітні електронні іграшки тощо. Зважаючи на специфічність ЗМІ як особливого інструменту в руках суб'єктів терористичної діяльності, специфіка якого обумовлена власне тим, що одна з основних цілей терористів — швидке поширення інформації серед населення — співпадає власне із призначенням ЗМІ і пояснює їх особливу роль у глобалізації тероризму, подальшого дослідження потребують питання специфіки функціонування медіа-тероризму як особливого виду тероризму в Україні та в інших країнах світу, зокрема суб'єктно-об'єктної структури цього явища, його методів, засобів і функцій тощо.

Кібертероризм, його характерні риси, види та способи здійснення. Кібертероризм – це сукупність дій, що включають інформаційну атаку на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупуваннями або окремими особами.

Кібертероризм спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та здійснення інших деструктивних дій. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж (терористичні акції можуть здійснюватися з будь-якої точки світу) та в проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність через декілька підставних комп'ютерів, що ускладнює його ідентифікацію та визначення місцезнаходження. Зброя «кібертерористів» постійно вдосконалюється залежно від засобів захисту, застосовуваних користувачами комп'ютерних мереж.

Характерні риси кібертероризму: використання високих технологій як зброї; використання відкритості Інтернету для відключення критичної інфраструктури; має за мету створити серед населення паніку; загроза провокації воєнного конфлікту; вплив на уряди країн або міжнародну спільноту в цілому.

Кібертероризм є одним з найнебезпечніших видів злочинності. Кібератаки можуть спричинити величезну шкоду на локальному, державному та навіть міжнародному рівні. Адже, зовнішні кібератаки можуть переслідувати і більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібертероризму можуть бути грошова і секретна інформація, апаратура контролю над космічними приладами, ядерними електростанціями, воєнними комплексами головні комп'ютерні вузли тощо.

3. Види правопорушень в інформаційній сфері.

Правопорушення проти цілісності та доступності комп'ютерних даних і систем (незаконний доступ; нелегальне перехоплення; втручання у дані, втручання у систему; зловживання пристроями).

Правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами).

Правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією).

Правопорушення, пов'язані з порушенням авторських та суміжних прав.

Тема 2. Світовий досвід протидії інформаційному тероризму

ЛЕКЦІЯ 2. Світовий досвід протидії інформаційному тероризму Навчальні питання:

1. **Протидія інформаційному тероризму в рамках міжнародних організацій та форумів.** Протидія інформаційному тероризму в рамках ООН. Резолюція Генеральної Асамблеї ООН A/RES/53/70 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 4 січня 1999 року у практичному плані резолюція рекомендувала державам-членам ООН висловитися щодо доцільності розробки міжнародних принципів, які стали б направлятися на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем і сприяли б боротьбі з

міжнародним тероризмом і криміналом. Резолюція Генеральної Асамблеї ООН A/RES/54/49 «Досягнення
в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 23 грудня 1999 року підтвердила доцільність розробки згаданих вище міжнародних принципів, а також серйозним кроком вперед стало визнання можливості загроз негативного впливу інформаційних технологій безпеці держав не тільки в цивільній, а й у військовій сферах.

Резолюція Генеральної Асамблеї ООН A/RES/56/19 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 7 січня 2002 року передбачала створення Групи урядових експертів, основними завданнями якої були визначені: розгляд існуючих і потенційних загроз у сфері інформаційної безпеки та можливі спільні заходи по їх усуненню.

Резолюція Генеральної Асамблеї ООН A/RES/60/45 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 8 грудня 2005 року, ключовим положенням якої стало рішення про створення в 2009 році групи урядових експертів ООН (її другого складу) для продовження дослідження існуючих і потенційних загроз у сфері інформаційної безпеки і можливих спільних заходів щодо їх усунення. У практичному плані Група націлила світове співтовариство на продовження діалогу між державами з метою обговорення норм, що стосуються державного використання ІКТ, скорочення колективного ризику і захисту критичної національної і міжнародної інфраструктури.

Резолюція Генеральної Асамблеї ООН A/RES/66/24 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 13 грудня 2011 року містила заклик до подальших дій за результатами роботи останньої ГУЕ.

Резолюція Генеральної Асамблеї ООН A/RES/60/288 «Глобальна контртерористична стратегія ООН» від 20 вересня 2006 року визначає, що держави-члени ООН взяли на себе зобов'язання здійснювати співробітництво з ООН з метою вивчення шляхів та засобів «координації зусиль на міжнародному та регіональному рівні з метою боротьби з тероризмом у всіх його формах та проявах в мережі Інтернет, а також використання мережі Інтернет в якості інструменту боротьби з поширенням тероризму, визнаючи той факт, що державам може знадобитись допомога у вирішенні цих питань», дотримуючись при цьому принципів конфіденційності, поваги до прав і свобод людини й громадянина та норм міжнародного права. Відповідно до вищезгаданої Резолюції було створено Робочу групу з питань протидії використання мережі Інтернет в терористичних цілях.

Діяльність ООН у сфері інформаційної безпеки спрямована на розробку міжнародно-правової бази та вироблення документів для протидії протиправному використанню науково-технологічного прогресу терористичними угрупованнями та організованою злочинністю.

Протидія інформаційному тероризму в рамках НАТО. Улистопаді 2002 року під час Празького саміту лідери країн-членів НАТО виявили своє бажання посилювати свої можливості щодо протидії інформаційним атакам.

У січні 2008 р були затверджені напрямки політики з кіберзахисту, націлені на забезпечення швидкого і ефективного реагування в разі кібернападів. Ці напрямки вказують військовим і цивільним органам НАТО на необхідність забезпечення загального узгодженого підходу, а також дає рекомендації окремим країнам щодо захисту національних систем. В рамках Організації Північноатлантичного договору створено Управління з питань забезпечення кібероборони, Центр експертизи з питань кооперативної кібероборони (CCDCOE) у Таллінні, Агентство з питань комунікації та інформації НАТО, а також розпочато впровадження програми кіберзахисту NCIRC (NATO Computer Incident Response Capability).

Крім цього, в Анкарі створено Центр передового досвіду НАТО у боротьбі з тероризмом, що також значну увагу приділяє питанням боротьби з інформаційним тероризмом. У травні 2014 р. експертами центру було опубліковано доповідь «Використання кіберпростору терористами», в якій висвітлювались питання розуміння поняття інформаційного тероризму, оцінки та реагування на кіберзагрози, використання терористами інформаційних технологій, а також питання спроможності новітніх технологій протистояти кібертерористам.

Роль Інтерполу у протидії інформаційному тероризму.

Генеральний секретаріат Інтерполу вирішив скоординувати досвід країн-членів у галузі злочинності в сфері інформаційних технологій (англ. Information Technology Crime, ITC) через створення «робочої групи», тобто групи експертів. Такі робочі групи складаються з начальників чи досвідчених членів національних органів боротьби із комп'ютерною злочинністю, та покликані відображати регіональний досвід країн Європи, Азії, Південної та Північної Америки та Африки. Основним завданням центрального органу є гармонізація ініціатив різних регіональних робочих груп.

У вересні 2002 р., на тлі тривожного зростання кількості міжнародних терористичних атак, Інтерполом була створена так звана Об'єднана цільова група (англ. Fusion Task Force, FTF), направлена саме на боротьбу з міжнародним тероризмом. Основними її завданнями є виявлення активних терористичних груп та їх членів, збирання та обмін інформацією та розвідкою, надання аналітичної підтримки та посилення спроможності країн-членів щодо подолання загроз тероризму та організованої злочинності.

У рамках своєї глобальної антитерористичної стратегії Інтерпол прагне протидіяти терористичним загрозам на цифрових платформах шляхом посилення можливостей аналізу соціальних медіа країн-членів в регіоні Близького Сходу, Північної Африки та в Пакистані.

Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. Ця угода визначає шість основних загроз у сфері міжнародної інформаційної безпеки, однією з яких є

інформаційний тероризм, а також напрями співробітництва держав у сфері забезпечення міжнародної інформаційної безпеки. У Додатку 1 до Угоди ШОС міститься визначення інформаційного тероризму, під яким автори документу розуміють «*використання інформаційних ресурсів та (чи) вплив на них в інформаційному просторі в терористичних цілях*». Додаток 2 до Угоди деталізує це поняття через визначення його джерел та основних ознак.

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.

Незважаючи на те, що визначення інформаційного тероризму, запропоноване у концепції Конвенції про забезпечення міжнародної інформаційної безпеки, повністю відтворює визначення, закріплене в Угоді держав-членів ШОС, автори концепції використовують термін «тероризм в інформаційному просторі», а основною загрозою міжнародному миру та безпеці у цій сфері вважають: «використання міжнародного інформаційного простору державними та недержавними структурами, організаціями, групами та окремими особами в терористичних, екстремістських чи інших злочинних цілях». Вищезгадана концепція ширше підходить до розуміння інформаційного тероризму, але досі не вдалось досягнути консенсусу та прийняти цей нормативно-правовий акт.

Проект «Загального договору з питань кібербезпеки та кіберзлочинності», запропонований професором Штайном Шольбергом, який займав посаду голови Групи Експертів високого рівня з питань кібербезпеки, засновану у 2007 р. задля вивчення можливостей створення загального документа з питань кіберзлочинності в рамках Організації Об'єднаних Націй, та професором Соланж Гернуті-Елі. Автори цього проекту розглядають інформаційний тероризм як один із видів кібератак. Тому стаття, присвячена врегулюванню цього питання, має назву «запобігання тероризму та іншим серйозним кібератакам». Відповідно до положень проекту договору до таких дій належать: публічне підбурювання до вчинення терористичного злочину, пошук та схилення людей для вчинення терористичного акту та проведення терористичних навчань. Також договором передбачено кримінальну відповідальність за такі дії згідно з внутрішнім законодавством держав-членів.

2. Періодизація превентивних заходів та контрзаходів світової спільноти в сфері протидії інформаційному тероризму.

2003 р. – опублікування у США Національної стратегії безпеки у кіберпросторі (є частиною більш загальної Стратегії забезпечення національної безпеки, створеної як реагування на події 11 вересня 2001 р.);

2006 р. – Швеція розробила Стратегію підсилення безпеки Інтернет; США проводять перші глобальні навчання з питань кібербезпеки Cyber Storm I, що вказали на велику вразливість держави до сторонніх кібернетичних впливів;

2008 р. – Естонія опублікувала розширену державну стратегію кібербезпеки (реакція на потужні КбА 2007 р., одна з перших у Європі розширених стратегій, центральним об'єктом є безпека інформаційних систем, а контрзаходи базуються на правовому регулюванні, навчанні та співпраці); США проводять навчання Cyber Storm II, результати яких виявились не набагато кращими за попередні навчання (Cyber Storm I);

2009–2012 рр. – створення загонів кібервійськ у КНР, США, Росії, Індії, Великобританії, Німеччині, Австралії тощо; 2010 р. – США проводять триденні навчання Cyber Storm III, що були присвячені випробуванням нової системи протидії кібератакам із залученням провідних фахівців з Австрії, Великобританії, Японії, Німеччини, Нідерландів, Швеції, Франції та інших держав; проведено перші кібернавчання державами Європейського союзу під назвою Cyber Europe-2010 – перший крок у розробці стратегії комплексної безпеки на території об'єднаної Європи;

2011 р. – прийняття стратегій кібербезпеки у Великобританії, Чехії, Франції, Німеччині, Литві, Люксембурзі, Нідерландах тощо; створення в Україні Управління по боротьбі з кіберзлочинністю МВС України – окремого оперативного підрозділу, що спеціалізується виключно на протидії кіберзлочинності;

2012 р. – під егідою Єврокомісії проведено чергові кібернавчання типу «стрес-тест» під назвою Cyber Europe-2012, де використовувались віртуальні стендові системи, що відтворюють реальні характеристики критичних інформаційних інфраструктур Євросоюзу; створення в Україні та апробація першого навчального курсу під егідою ІКАО, присвяченого захисту цивільної авіації від кіберзагроз;

2013 р. – відкрито Європейський центр по боротьбі з кіберзлочинністю (ЕС3), який став координаційним центром ЄС у боротьбі із кіберзлочинністю.

3. Механізми протидії інформаційному тероризму в США та в провідних державах Азії.

Найбільший обсяг матеріальних збитків по всіх країнах від терористичних актів було зафіксовано у 2014 р. – понад 105,4 6 млрд дол. США (у 2015 р. вони становили 89,6 млрд дол. США, а у 2000 р. – близько 5,3 млрд дол. США). Також це явище створює додаткові ризики для міжнародного бізнесу, туризму та транспортних перевезень. Річні витрати держав G20 на захист від тероризму в 2014 р. оцінювалися у 117 млрд дол. США

Уряд Японії постійно оновлює свою стратегію кібербезпеки. З моменту публікації в 2006 р «Першої національної стратегії інформаційної безпеки» в неї кілька разів вносилися зміни і доповнення. Так, у Стратегії-2015 визначено орган, відповідальний за її реалізацію – Стратегічний штаб із забезпечення кібербезпеки. Створена в 2014 році за допомогою реорганізації Ради з питань політики в області інформаційної безпеки, нова організація діє як командний і контрольний орган в питаннях, пов'язаних з національною кібербезпекою, а також як орган, наділений повноваженнями давати

рекомендації в сфері кібербезпеки іншим держустановам. Нарешті, в серпні 2016 японський Національний центр готовності до надзвичайних ситуацій та стратегії в сфері кібербезпеки (NISC) опублікував документ під назвою «Загальні рамкові положення безпеки систем «інтернету речей» який є додатком до Національної стратегії кібербезпеки.

Тема 3. Механізми протидії інформаційному тероризму держав Європи

ЛЕКЦІЯ 3. Засоби протидії інформаційному тероризму держав Європи на регіональному рівні

Навчальні питання:

1. Поняття регіональної системи безпеки.

Під регіональною системою безпеки розуміється сукупність принципів і норм, що діють в межах визначеного регіону і регулюють співробітництво держав регіону в сфері підтримки миру і безпеки. Початок інституалізації системи європейської безпеки поклали Паризька хартія для нової Європи 1990 року і Додатковий документ до неї 1990 року. Дані документи передбачали створення ряду структур та інститутів, які повинні були стимулювати і спрямовувати загальноєвропейський безпековий процес.

Лісабонська декларація від 1 січня 1996 року «Про моделі загальної і всеосяжної безпеки для Європи XXI століття» конкретизувала й розвинула концептуальні засади європейської безпеки. У ній наголошувалося на необхідності створення єдиного простору безпеки, основними елементами якого є всеосяжний і неподільний характер безпеки, прихильність цінностям, зобов'язанням і нормам поведінки.

Ще одним документом, який визначив основи європейської взаємодії на початок XXI століття стала Хартія європейської безпеки, прийнята на Стамбульській зустрічі ОБСЄ на вищому рівні 19 листопада 1999 року, яка передбачає найширше співробітництво між ОБСЄ та компетентними європейськими організаціями з урахуванням ключової координуючої ролі ОБСЄ як єдиної загальноєвропейської організації безпеки, покликаної забезпечувати мир і стабільність в регіоні.

2. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року.

Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року є єдиним уніфікованим європейським документом, що не тільки визначає види злочинів в інформаційній сфері (кіберзлочинів), а й форму співробітництва у боротьбі із ними. У Конвенції міститься оптимальний комплекс юридичних і технічних норм, які можуть послужити основою для розробки додаткових угод по розширенню регіонального та міжнародного співробітництва в сфері забезпечення кібербезпеки. Вона передбачає здійснення захисних дій на рівні держав-учасників, а також на регіональному та міжнародному рівнях. На сьогоднішній день Конвенція підписана 43 членами ЄС і 15 іншими країнами, включаючи США. Крім того, Конвенція підтримується іншими

організаціями, які посилаються на неї в своїх рішеннях. Це Європейський Союз, Організація Американських держав (ОАД), Організація економічного співробітництва і розвитку (ОЕСР), Організація Азіатсько-Тихоокеанського економічного співробітництва, Інтерпол, а також структури приватного сектору.

3. Роль ОБСЄ у протидії інформаційному тероризму держав Європи.

Рішення Ради Міністрів ОБСЄ № 3/04 «Боротьба з використанням Інтернету в терористичних цілях» 2004 року визначало масштабність використання мережі Інтернет терористичними організаціями для організації терористичних актів, збору фінансів, вербування прихильників та пропаганди і підбурювання до вчинення терористичних дій. Відповідно до цього документа держави зобов'язались обмінюватись інформацією про використання Інтернету в терористичних цілях та про стратегії боротьби з цим явищем.

Також у 2004 р. було проведено спеціальну нараду ОБСЄ про взаємозв'язок між расистською, ксенофобською й антисемітською пропагандою в Інтернеті та злочинами, здійсненими на підставі ненависті. У 2005 р. відбувся експертний семінар ОБСЄ щодо боротьби з використанням Інтернету у терористичних цілях, а у 2006 р. – спільний експертний семінар ОБСЄ та Ради Європи щодо попередження тероризму.

Рішенням Ради Міністрів ОБСЄ № 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року державам-учасницям було запропоновано розширити моніторинг веб-сайтів, що мають терористичне чи екстремістське спрямування та активізувати обмін інформацією з цього питання, залучати інститути громадянського суспільства до протидії використанню Інтернету в терористичних цілях та здійснювати обмін інформацією про можливі загрози у зв'язку з таким використанням через Контртерористичну мережу ОБСЄ.

4. Протидія інформаційному тероризму в рамках ЄС.

Ініціатива «Електронна Європа» була затверджена у грудні 1999 року. Головними напрямками, в рамках яких було розроблено сектори та конкретні завдання ініціативи, є такі: надання доступу до цифрових технологій та Інтернету кожному громадянину, кожній оселі, школі, підприємству та державній установі; подолання цифрової неосвіченості у Європі через культуру підприємництва, відкриту до застосування нових інформаційних технологій; забезпечення соціальної лояльності до інформаційного суспільства. Загальний план дій в рамках ініціативи, затверджений самітом Європейської Ради в Фейрі в червні 2000 року, приділив серйозну увагу безпеці мережі і боротьбі з кіберзлочинністю та його найтяжчою формою – кібертероризмом.

13 березня 2004 році на базі ЄС було створено Агентство з мереж і інформаційної безпеки (ENISA), яке постійно проводить моніторинг користувачів мережі, відповідно до цього вносить поправки до вже прийнятих проектів, які стають законами і дотримуються країнами ЄС. Агентство було створено з метою регулювання та запобігання мережевих та інформаційних загроз, зміцнення багатостороннього діалогу всередині Європи і за його межами з проблеми кіберзлочинності та кібертероризму, розвитку культури мережевої та інформаційної безпеки в інтересах громадян, підприємств і організацій державного сектору Європи для сприяння нормальному функціонуванню Європейського регіону. ENISA надає консультації щодо передової практики, та проводить експертизи аналізу існуючих ризиків та надає допомогу державам-членам та європейським органам влади. Крім того, законодавці проводять щорічні зустрічі з політиками, IT-фахівцями, науковцями для навчання і вдосконалення навичок безпечного користування Інтернетом, а також проводять вчення по протидії та запобіганню кібератакам різного ступеня складності.

Вчення Cyber Europe – це моделювання масштабних інцидентів кібербезпеки, які переростають у кіберкризи. Cyber Europe 2010 була організована державами-членами ЄС, за підтримки Європейського агентства мережевої та інформаційної безпеки (ENISA), а також за підтримки Спільного дослідницького центру (JRC). Навчання пропонують можливість проаналізувати передові технічні інциденти, пов'язані з кібербезпекою, а також розв'язати складні ситуації з безперервністю бізнесу та кризовими ситуаціями. Під час тренувань експерти Cyber Europe 2010 від європейських країн працювали разом, щоб протистояти спробам хакерів паралізувати Інтернет та критичні інфраструктури, особлива увага приділялася захисту інформаційних мереж саме від кібертерористичних атак. Ці вчення були першим, ключовим кроком у боротьбі з потенційними проявами кібертероризму для основної критичної інфраструктури, а також зміцнення безпеки як окремого громадянина європейської держави, так і Європи в цілому. Були проведені вчення за стратегіями Cyber Europe 2012, 2014, 2016 та 2018 року, наразі йде опрацювання нової стратегії Cyber Europe 2020, яка буде мати на меті боротьбу з наростаючою загрозою інформаційного тероризму.

У 2011 році для підтримки різних груп IT-безпеки в установах ЄС в їх боротьбі з кіберзагрозами різних видів була створена Група реагування на надзвичайні ситуації (CERT-EU). Вона діє як центр обміну інформацією про кібербезпеку і координує реагування на кіберінциденти, під якими розуміють події або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого

управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Європейський центр по боротьбі з кіберзлочинністю (ЕС3) спирається на існуючий потенціал правоохоронних органів Європолу, але він також має інші значно розширені можливості, зокрема, надання оперативної та аналітичної підтримки у розслідуванні кібертерористичних атак державами-членами.

Стратегія кібербезпеки ЄС 2013 року встановила «пріоритетну міжнародну політику у сфері кіберпростору для ЄС» у п'яти пріоритетах: забезпечення стійкості кіберпростору Європейського союзу; скорочення кількості кіберзлочинів; розвиток політики кібероборони, яка включає сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії на основі Спільної політики безпеки і оборони Європейського союзу; розвиток виробничо-технологічних ресурсів для забезпечення кібербезпеки; створення узгодженої всіма членами Євросоюзу міжнародної політики з кібербезпеки з іноземними партнерами для підвищення кооперації в цій галузі з третіми країнами.

Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від 06.07.2016 року (NIS Directive) встановлює вимоги безпеки в таких критично важливих сферах як банківська, енергетика, транспорт, охорона здоров'я, інфраструктура фінансового ринку та цифрова інфраструктура, а також вимоги безпеки у сферах онлайн-послуг (торгових майданчиків, пошукових систем, хмарних технологій тощо). Зазначена директива покладає на держави-членів ЄС, наступні обов'язки: прийняття внутрішньодержавних стратегій NIS, які визначать стратегічні цілі у сфері кібербезпеки; формування національного органу, на який будуть покладені обов'язки щодо реалізації та контролю за дотриманням NIS Directive; створення мережі Computer Security Incident Response Teams, відповідальної за інциденти та загрози, які виникають у сферах, визначених директивою.

Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. Євроюст здійснює координацію дій правоохоронних органів різних держав з питань розслідування кіберзлочинів, надає допомогу в проведенні розслідувань за запитом відповідного органу публічної влади держав, надає правоохоронним органам цих країн інформацію про проведені розслідуваннях щодо кіберзлочинців.

Діяльність Європолу обмежена структурами організованої злочинності, в яких задіяні дві чи більше країни ЄС. До пріоритетних сфер повноважень Європолу належать в тому числі тероризм та кіберзлочини. Європол допомагає державам-членам в обміні інформацією; здійснює оперативний аналіз заходів, до яких вдаються держави-члени; готує стратегічні звіти (зокрема, формулює загрози) та дослідження злочинності; виконує

експертизу і надає технічну підтримку в рамках розслідувань і операцій всередині ЄС; а також сприяє гармонізації процедур розслідування у державах-членах. У 2009 році в Києві підписано Угоду між Україною та Європейським поліцейським офісом про стратегічне співробітництво.

ЛЕКЦІЯ 4. Засоби протидії інформаційному тероризму держав Європи на національному рівні

Навчальні питання:

1. Досвід Естонії та Литви у боротьбі з інформаційним тероризмом.

Естонія у 2008 році однією з перших ухвалила національну Стратегію кібербезпеки і переглянула її у 2014 році. Стратегія передбачає забезпечення захисту інформаційних систем, що лежать в основі служб життєзабезпечення, подолання кіберзагроз для державного і приватного сектора, впровадження національної системи контролю в сфері кібербезпеки, забезпечення цілісності цифрових ресурсів держави, посилення міжнародного співробітництва в сфері захисту інфраструктури особливо важливої інформації, вдосконалення боротьби з кібертероризмом, підвищення громадської обізнаності прокіберризики, а також розробка нової законодавчої бази для забезпечення кібербезпеки і інші.

10 травня 2018 року набув чинності Закон про кібербезпеку (Cybersecurity Bill). Він спрямований на зміцнення структур, що надають важливі послуги суспільству, та захист державних та муніципальних мереж та інформаційних систем.

Талліннський центр кіберзахисту НАТО (The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence, CCD COE) – операційно незалежна міжнародна військова організація, створена у 2008 році, що фінансується та керується державами, що добровільно беруть у ній участь. Центр зосереджується на дослідженнях, розробках, навчанні та освіті як у технічних, так і у нетехнічних аспектах кіберзахисту.

В Естонії працює CERT Estonia.

Стратегія кібербезпеки Литви була прийнята в 2011 році: це Програма розвитку електронної інформаційної безпеки (кібербезпеки) на 2011–2019 роки.

Перший закон про кібербезпеку Литви був ухвалений у грудні 2014 року та встановлює положення, що дозволяють компетентним органам вживати заходів для захисту електронно-комунікаційної інфраструктури.

Національний центр кібербезпеки при Міністерстві національної оборони (NCSC), який почав діяти з 1 січня 2018 року, є основним інститутом литовської кібербезпеки, відповідальним за єдине управління кіберінцидами, моніторинг і контроль за виконанням вимог кібербезпеки, акредитацію інформаційних ресурсів.

В Литві працює CERT-LT.

2. Особливості протидії інформаційному тероризму у Великій Британії, Німеччині та Бельгії.

Метою Національної стратегії кібербезпеки 2011 року зазначає, що необхідним є виключення ризиків типу кібератак злочинців та терористів з метою зробити кіберпростір безпечним для громадян та держави. За виконання Національної стратегії кібербезпеки 2011 року відповідають два CERT-и: CERT-UK, що підтримує операторів, які захищають критичну інфраструктуру, та GovCertUK, який працює з державними установами. Окрім цього, існують Національна рада Безпеки та Офіс страхування з питань кібернетичної та інформаційної безпеки.

Головним органом, що відповідає за кібербезпеку Великої Британії є Національний центр кібербезпеки, який самостійно почав функціонувати лише у 2016 році, та має на меті підтримувати найбільш критичні інфраструктури у Великій Британії, громадському секторі, промисловості, а також широкій громадськості. Його батьківською організацією є Центр урядового зв'язку, що відповідальний за ведення радіоелектронної розвідки і забезпечення захисту інформації органів уряду і армії та знаходиться у віданні Міністра закордонних справ Великобританії. Центр несе відповідальність за збір і аналіз інформації в країнах Європи і Африки.

Центр захисту національної інфраструктури (CPNI) є державним органом, що надає захисні рекомендації щодо безпеки національної інфраструктури Великої Британії. Роль Центру полягає в захисті національної безпеки, допомагаючи зменшити вразливість національної інфраструктури до тероризму та інших загроз у кіберпросторі.

Національне агентство з питань злочинності (NCA) Великої Британії координує боротьбу з кіберзлочинністю та кібертероризмом, а також низкою інших злочинів, тісно співпрацюючи з низкою національних і міжнародних партнерів з кібербезпеки.

Загальний центр захисту від тероризму Німеччини покликаний об'єднати роботу понад сорока різних німецьких федеральних і земельних установ з різних напрямків попередження загрози тероризму. Вся діяльність центру розбита на дев'ять робочих груп, в які входять понад 200 представників вищеназваних відомств. Вони ведуть роботу по відповідальним напрямками, постійно обмінюючись інформацією і координуючи свої дії через два аналітичних центру – розвідувальний і поліцейський.

Відповідно до Національної стратегії кібербезпеки в 2011 році була створена Національна рада кібербезпеки, метою якої було дозволити секретаріатам всіх міністерств внести питання кібербезпеки в стратегію реалізації всіх політичних напрямків діяльності в країні.

Також Стратегія визначає Федеральний офіс інформаційної безпеки (BSI) Міністерства внутрішніх справ органом, що є відповідальним за кібербезпеку в країні. BSI створив Національний центр кіберреагування (NCAZ) відповідальний за визначення, аналіз і розробку заходів, необхідних для нівелювання і усунення потенційних загроз.

У липні 2015 р. у Німеччині був прийнятий Акт про інформаційну безпеку (IT Security Act), метою якого стало запобігання шкоди найважливішим IT-системам країни. BSI займається реалізацією положень

цього Акта, який включає в себе мінімальні стандарти кібербезпеки для понад 2000 критично важливих інфраструктурних компаній.

Орган, що контролює інформаційний простір Бельгії – Аудіовізуальна вища рада (CSA) був створений 1987 році і був виключно консультативним. Постанова від 27 лютого 2003 року надала цьому органу статус юридичної особи та контрольних повноважень в діяльності ЗМІ.

Поняття злочинів у кіберпросторі були включені в Закон про кіберзлочинність 2000 року і знайшли своє відображення в кримінальному кодексі Бельгії. Серед них: комп'ютерна підробка, комп'ютерне шахрайство та злочини проти конфіденційності, цілісності комп'ютерних систем і даних, тих, що зберігаються, оброблюються чи передаються.

У Бельгії в березні 2005 року була створена робоча група з проблеми кіберзлочинності та кібертероризму, на рівні Урядового комітету розвідки і безпеки.

У Бельгії працює CERT.be.

3. Особливості протидії Франції та Іспанії.

«Біла книга з питань національної оборони і безпеки» 2008 року була першим основоположним документом, стосовно проблематики національних кіберзагроз як основного ризику для національної безпеки і суверенітету Франції. У ній визначалися нові пріоритети, такі як запобігання і реагування на кібератаки.

У 2009 р. Головне управління комп'ютерної безпеки Франції (DCSSI) було перетворено в Національне агентство безпеки інформаційних систем (ANSSI) і стало органом, відповідальним за безпеку національних інформаційних систем. Після створенням цього органу у 2011 році у Франції була опублікована перша національна кіберстратегія, яка містить чотири основні цілі: забезпечення світового лідерства з питань кібероборони, охорона апарату прийняття рішень у Франції за допомогою захисту суверенної інформації, підвищення рівня кібербезпеки критично-важливих елементів інфраструктури, а також забезпечення безпеки в кіберпросторі.

У 2015 році уряд Франції опублікував другу національну стратегію кібербезпеки як свою реакцію на зростання кількості і серйозності кібератак в найрізноманітніших сферах. Національна кіберстратегія 2015 року підтримує «співпрацю країн ЄС для створення європейської стратегічної цифрової автономії як довгострокової гарантії більш безпечного кіберпростору».

У 2019 році на модернізацію техніки боротьби із кіберзлочинністю уряд Франції виділив 1 млрд. євро.

В іспанській правовій системі існують процедурні норми прямого застосування кримінального переслідування до проявів кібертероризму. Незаконний доступ, втручання в роботу ІКТ-систем, зловмисне використання технологічних пристроїв криміналізуються Кримінальним кодексом країни.

Іспанія ухвалила Національну Стратегію з кібербезпеки у 2013 році. Стратегія є добре узгодженою як з Планом з національної безпеки, так і з чинним законодавством в галузі кібербезпеки.

В Іспанії діють INTECO-CERT та CCN-CERT, а також створено Національний Центр із захисту критичної інфраструктури (CNPIC). Цей Центр
є державною структурою, яка відповідає за інформаційну безпеку та кібербезпеку, тоді як роль CERT-ів зводиться до реагування на кіберінциденти. CNPIC відповідає також за поширення інформації щодо кіберзагроз та кіберінцидентів, а також забезпечує координацію та співпрацю між різними секторами економіки та між державними та приватними інституціями. Він створює також робочі групи, які розробляють секторальні плани з кібербезпеки.

Іспанія створила свої структури, у різних міністерствах, для реагування на кіберзагрози та кібертероризм, наприклад, Національний інститут кібербезпеки (INCIBE), Національний офіс безпеки (ONS), Національний криптологічний центр (CCN), Спільне командування кібероборони, та спеціалізовані підрозділи в органах безпеки, такі як група з телематичних злочинів і група кібертероризму цивільної гвардії.

4. Досвід протидії інформаційному тероризму у Туреччині.

У 2012 році Туреччина сформувала Стратегію кібербезпеки, включає в себе одразу всі види основних загроз у кіберпросторі та методи протидії ним, а також визначає перелік критичної інфраструктури держави. Стратегія кібербезпеки Туреччини направлена на захист громадянина, бізнесу та держави в цілому. Вона була розроблена за такими основними напрямками: а) операції з кіберзахисту та кіберстримування; б) боротьба з кіберзлочинністю та кібертероризмом; в) розвідувальна діяльність і кібершпіонаж; г) кризове управління; ґ) управління мережею Інтернет і кібердипломатія.

У 2012 році був створений Командний центр кіберзахисту, який 30 серпня 2013 року був перетворений в Командування кіберзахисту Збройних Сил Туреччини. Збройні Сили Туреччини є лідерами у сфері розробок турецьких кібертехнологій.

Ще одним значним кроком у реформуванні системи безпеки Туреччини було проведення на державному рівні навчань щодо забезпечення національної кібербезпеки з 2011 по 2013 роки. Проведені навчання значно покращили стан кіберготовності Туреччини до відображення терористичних атак у кіберпросторі.

Туреччина прийняла національну кіберстратегію на 2016–2019 рр., в якій наголошено на важливості кібероборони для боротьби проти ворожої пропаганди, для захисту кордонів, для збережень систем ключових інфраструктур і держустанов, для електронної торгівлі, для промислових об'єктів країни.

Тема 4. Інформаційний тероризм як загроза національній безпеці України

ЛЕКЦІЯ 5. Інформаційний тероризм як загроза національній безпеці України

Навчальні питання:

1. Періодизація та види терористичних атак на інформаційний простір та кіберпростір України.

Хронологія кібертерористичних атак на національний інформаційний та кіберпростір України з 4 лютого 2014 року, коли анонімні хакери з угрупування CyberBerkut завантажили в YouTube телефонну розмову між помічником держсекретаря США і послом США в Україні, який включає в себе висміюють коментарі про ЄС, по 27 червня 2017 року, коли відбулася масштабна хакерська атака за допомогою вірусної програми Petya.A, яка порушила роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ.

2. Нормативно-правова база протидії інформаційному тероризму в Україні.

Основні положення Законів України:

- «Про інформацію» № 2657-XII від 2 жовтня 1992 року (відповідальність за порушення законодавства про інформацію);

- «Про національну безпеку» № 2469-VIII від 21 червня 2018 року:

Державна служба спеціального зв'язку та захисту інформації України є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону;

- «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року:

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Об'єкти кібербезпеки (конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури) та кіберзахисту (1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів

місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу).

Суб'єкти забезпечення кібербезпеки (суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, та суб'єкти забезпечення кібербезпеки у межах своєї компетенції).

До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Принципи забезпечення кібербезпеки: 1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом; 2) забезпечення національних інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі; 4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері; 5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі; 6) пріоритетності запобіжних заходів; 7) невідворотності покарання за вчинення кіберзлочинів; 8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; 9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях; 10) забезпечення демократичного цивільного контролю за утвореними відповідно

до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури;

-«Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року (Повноваження державних органів у сфері захисту інформації в системах).

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».

Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

Національними інтересами України в інформаційній сфері є визначені життєво-важливі інтереси особи, суспільства і держави.

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів

Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Пріоритетами державної політики в інформаційній сфері мають бути пріоритети щодо забезпечення інформаційної безпеки; щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію; щодо відкритості та прозорості держави перед громадянами; щодо формування позитивного міжнародного іміджу 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».

Метою Стратегії кібербезпеки України (далі - Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Пріоритети забезпечення кібербезпеки України: 1) розвиток безпечного, стабільного і надійного кіберпростору; 2) кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом; 3) кіберзахист критичної інфраструктури; 4) розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; 5) боротьба з кіберзлочинністю тощо.

3. Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом.

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак

та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

Антитерористична пропаганда СБ України здійснюється через систему взаємоузгоджених заходів, які застосовуються комплексно. Основними з них є: 1) інформаційно-пропагандистська діяльність органів влади та правоохоронних структур; 2) розвінчування ідеології тероризму (його антологічних і гносеологічних основ); 3) «деромантизація» терористичних лідерів; 4) контроль і протиборство з ідеологією тероризму у мережі Інтернет (блокування сайтів, публікацій на форумах, соціальних мережах); 5) організація інформаційного контролю за середовищем молоді.

5 жовтня 2015 року було створено Кіберполіцію – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює оперативно-розшукову діяльність. Метою діяльності Кіберполіції є забезпечення кібербезпеки України в інформаційному просторі, миттєве реагування та протистояння кіберзагрозам, кіберзлочинам, та їх найтяжчій формі – кібертероризму. Крім того, до завдань підрозділу входить проведення міжнародної співпраці по знешкодженню транснаціональних злочинних угрупувань у даній сфері. Так, за результатом роботи Кіберполіції України у 2018 році було викрито більше 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій.

4. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом.

Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України – державна установа, створена для здійснення

впровадження організаційно-технічної моделі кіберзахисту, забезпечення функціонування якої у межах штатної чисельності та виділених обсягів фінансування здійснює Державна служба спеціального зв'язку та захисту інформації України.

Функції, що виконує ДЦКЗ: координація органів державної влади з питань запобігання та усунення наслідків кіберінцидентів; координація діяльності операторів та провайдерів щодо збору інформації про кіберінциденти; міжнародна координація з питань кіберзахисту.

2 лютого 2018 року у складі Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку відкрито новий підрозділ – Центр реагування на кіберзагрози (Cyber Threat Response Centre – CRC). Основною діяльністю підрозділу є забезпечення кіберзахисту органів державної влади та об'єктів критичної інформаційної інфраструктури України.

У складі ДЦКЗ функціонує спеціалізований структурний підрозділ – Команда реагування на комп'ютерні надзвичайні події України (Computer Emergency Response Team of Ukraine, CERT-UA) для забезпечення кіберзахисту та протидії кіберзагрозам.

5. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CERT-UA) у сфері протидії інформаційному тероризму.

Підрозділ заснований у 2007. У 2009 акредитована у Форуму команд реагування на інциденти інформаційної безпеки (FIRST). Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності.

Завданнями CERT-UA є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

CERT-UA активно взаємодіє з аналогічними командами в усьому світі.

5. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.

З метою розвитку ефективної міжнародної взаємодії з питань боротьби

з тероризмом на сьогодні Україна є стороною 17 базових міжнародних конвенцій і протоколів, що регулюють різні аспекти боротьби з тероризмом. На теперішній час налагоджено дієві партнерські стосунки із правоохоронними органами і спеціальними службами багатьох Європейських держав, США, антитерористичними структурами ООН, ОБСЄ, НАТО, ЄС та іншими міжнародними організаціями, що здійснюють боротьбу з тероризмом.

З січня 2003 року Україна є учасницею всіх міжнародних Конвенцій і протоколів ООН у сфері боротьби з тероризмом. Практика застосування положень, закріплених у Глобальній контртероритстичній стратегії ООН і плані дій до неї, відображена у нормах чинного законодавства нашої держави.

Окрім цього, Україною і її урядом підписано більше 165 міждержавних і міжурядових угод і протоколів у сфері боротьби з тероризмом.

Співробітництво України з Інтерполом. У 1992 році Україна стала членом Інтерполу. Кабінет Міністрів України у 1993 році постановою № 220 затвердив «Положення про Національне центральне бюро Інтерполу». Наказ «Про затвердження Інструкції про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів» № 3/1/2/5/2/2 від 03.01.1997 року.

Співробітництво України з Європолом. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 року, метою якої є встановлення відносин співробітництва між Україною та Європолом з метою підтримки України та держав-членів Європейського Союзу в запобіганні і боротьбі з організованою злочинністю, тероризмом та іншими формами міжнародної злочинності у сферах злочинності, зокрема шляхом обміну інформацією між Україною та Європолом.

Крім обміну інформацією, співробітництво може включати, відповідно до визначених Рішенням Ради Європолу завдань Європолу, обмін спеціальними знаннями, загальними зведеннями, результатами стратегічного аналізу, інформацією щодо процедур кримінальних розслідувань, інформацією про методи запобігання злочинності, участь у навчальних заходах, а також надання консультацій та підтримки в окремих кримінальних розслідуваннях.

2. ПЛАНИ ПРАКТИЧНИХ (СЕМІНАРСЬКИХ) ЗАНЯТЬ, ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ ТА ПОТОЧНОГО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК СТУДЕНТІВ РОЗДІЛ 1. ПОНЯТТЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ ТА СПОСОБИ ПРОТИДІЇ ЙОМУ

Семінарське заняття 1: **Феномен інформаційного тероризму як загрози міжнародній та національній безпеці**

Навчальна мета заняття: формування у студентів базових знань щодо поняття інформаційного тероризму, його характерних рис та видів, видів порушень в інформаційній сфері, а також практичних умінь та навичок визначати поняття інформаційного тероризму, його характерні риси, характеризувати види інформаційного тероризму та види порушень в інформаційній сфері, аналізувати та професійно давати оцінку сучасним міждержавним відносинам у світлі протидії інформаційному тероризму, обґрунтовувати та висловлювати свою точку зору з проблем, пов'язаних з способами боротьби з інформаційним тероризмом та міжнародною інформаційною безпекою в цілому.

Час проведення – 2 год.

Ключові поняття: тероризм, терористична діяльність, міжнародний тероризм, інформаційний тероризм, інформаційно-психологічний тероризм, інформаційно-технічний тероризм, медіа-тероризм, кібертероризм, кібератака, інформаційна сфера, критична інфраструктура, інформаційна безпека.

Навчальні питання:

1. Тероризм як явище.
2. Поняття «інформаційний тероризм» та його характерні риси.
3. Види правопорушень в інформаційній сфері.

Література:

Основна: 1, 3, 4, 5, 7, 10, 16, 17, 18, 19, 29, 31, 33, 34, 35, 40.
Додаткова: 2, 4, 8, 6, 11, 12, 13.

Самостійна робота – 15 год.

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.

Семінарське заняття 2: **Світовий досвід протидії інформаційному тероризму**

Навчальна мета заняття: формування у студентів базових знань щодо особливостей світового досвіду протидії інформаційному тероризму, зокрема в рамках міжнародних організацій, а також практичних умінь та навичок розкривати особливості світового досвіду протидії інформаційному тероризму, зокрема в рамках міжнародних організацій, вирішувати аналітичні завдання та практичні казуси відповідно до програми курсу на підставі аналізу нормативних документів, а також навчальної та монографічної літератури, аналізувати та професійно давати оцінку сучасним міждержавним відносинам у світлі протидії інформаційному тероризму, обґрунтовувати та висловлювати свою точку зору з проблем, пов'язаних з способами боротьби з інформаційним тероризмом та міжнародною інформаційною безпекою в цілому.

Час проведення – 2 год.

Ключові поняття: інформаційний тероризм, міжнародна безпека, міжнародна інформаційна безпека, інформатизація, телекомунікації, ООН, НАТО, Інтерпол, кібербезпека, кіберзлочинність, стратегія кібербезпеки.

Навчальні питання:

1. Протидія інформаційному тероризму в рамках міжнародних організацій та форумів.
2. Періодизація превентивних заходів та контрзаходів світової спільноти

в сфері протидії інформаційному тероризму.

3. Механізми протидії інформаційному тероризму в США та провідних державах Азії.

Література:

Основна: 2, 4, 6, 7, 12, 15, 16, 26, 29, 32, 33, 34, 38, 40.

Додаткова: 2, 3, 5, 7, 11, 12, 13.

Самостійна робота – 15 год.

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:

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 міжнародноїінформаційноїбезпеки» 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 просторівАзіатсько-Тихоокеанськомурегіоні 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.

Семінарське заняття 3: **Засоби протидії інформаційному тероризму держав Європи на регіональному рівні**

Навчальна мета заняття: формування у студентів базових знань щодо механізмів протидії інформаційному тероризму держав Європи на регіональному рівні, зокрема в рамках Ради Європи, ЄС та ОБСЄ, а також практичних умінь та навичок характеризувати механізми протидії інформаційному тероризму держав Європи на регіональному рівні, зокрема в рамках Ради Європи, ЄС та ОБСЄ, визначати позитивні та негативні тенденції міжнародного досвіду протидії інформаційному тероризму та можливість його застосування в Україні, працювати з міжнародними та національними нормативно-правовими актами та документами у сфері протидії інформаційному тероризму.

Час проведення – 2 год.

Ключові поняття: інформаційний тероризм, регіональна система безпеки, Рада Європи, ОБСЄ, Інтернет, «Ініціатива «Електронна Європа», ENISA, «вчення Cyber Europe», CERT-EU, EC3, кіберпростір, кібербезпека, Євроюст, Європол.

Навчальні питання:

1. Поняття регіональної системи безпеки.
2. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року.
2. Роль ОБСЄ у протидії інформаційному тероризму держав Європи.
3. Протидія інформаційному тероризму в рамках ЄС.

.

Література:

Основна: 2, 5, 6, 7, 10, 12, 15, 16, 25, 26, 30, 33, 34, 35, 36, 37, 38, 39, 40.
Додаткова: 2, 6, 8, 10, 11, 12, 13, 14.

Самостійна робота – 15 год.

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.

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.

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.

Семінарське заняття 4: **Засоби протидії інформаційному тероризму держав Європи на національному рівні**

Навчальна мета заняття: формування у студентів базових знань щодо механізмів протидії інформаційному тероризму держав Європи на національному рівні, а також практичних умінь та навичок характеризувати механізми протидії інформаційному тероризму держав Європи на національному рівні, аналізувати та професійно давати оцінку сучасним міждержавним відносинам у світлі протидії інформаційному тероризму, обґрунтовувати та висловлювати свою точку зору з проблем, пов'язаних з способами боротьби з інформаційним тероризмом та міжнародною інформаційною безпекою в цілому.

Час проведення – 2 год.

Ключові поняття: інформаційний тероризм, національна безпека, Стратегія кібербезпеки, кібертероризм, кіберзагроза, кібербезпека, інформаційна безпека, CERT, критична інфраструктура.

Навчальні питання:

1. Досвід протидії інформаційному тероризму в Естонії та Литві.
2. Досвід протидії інформаційному тероризму у Великій Британії, Німеччині та Бельгії.
3. Досвід протидії інформаційному тероризму у Франції та Іспанії.
4. Досвід протидії інформаційному тероризму у Туреччині**.**

Література:

Основна: 2, 5, 6, 7, 10, 12, 15, 16, 25, 26, 28, 29, 30, 32, 33, 34, 36, 38, 40.
Додаткова: 5, 6, 7, 10, 11, 12, 13, 14.

Самостійна робота – 10 год.

Питання для контролю засвоєння знань:

1) Що передбачає Стратегія кібербезпеки Естонії 2014 року у сфері протидії кібертероризму?
2) Визначте роль Таллінського центру кіберзахисту НАТО у боротьбі з кібертероризмом?
3) Що передбачає Стратегія кібербезпеки Литви 2011 року у сфері протидії кібертероризму?
4) Визначте роль Національного центру кібербезпеки при Міністерстві національної оборони (NCSC) у боротьбі з кібертероризмом в Литві?
5) Назвіть основні напрямки Стратегії Кібербезпеки Туреччини 2012 року.

6) Визначте роль Національного Центру із захисту критичної інфраструктури (CNPIC) у боротьбі з інформаційним тероризмом в Іспанії.

7) Визначте роль Національного агентства безпеки інформаційних систем (ANSSI) у боротьбі з інформаційним тероризмом у Франції.

8) Визначте роль Аудіовізуальної вищої ради (CSA) у боротьбі з інформаційним тероризмом у Бельгії.

9) Визначте роль Федерального офісу інформаційної безпеки (BSI) у боротьбі з інформаційним тероризмом у Німеччині.

10) 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 Таллінського центру кіберзахисту НАТО у боротьбі з кібертероризмом.

2) Роль CERT-UK та GovCertUK у протидії кібертероризму у Великій Британії.

3) Досвід протидії інформаційному тероризму у Туреччині.

4) Досвід протидії інформаційному тероризму в Естонії.

2. 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.

3. 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.

Семінарське заняття 5: **Інформаційний тероризм як загроза національній безпеці України**

Навчальна мета заняття: формування у студентів базових знань щодо видів терористичних атак на інформаційний простір України та особливості протидії інформаційному тероризму в Україні, а також практичних умінь та навичок визначати види терористичних атак на інформаційний простір України та особливості протидії інформаційному тероризму в Україні, визначати позитивні та негативні тенденції міжнародного досвіду протидії інформаційному тероризму та можливість його застосування в Україні,

працювати з міжнародними та національними нормативно-правовими актами та документами у сфері протидії інформаційному тероризму, готувати рекомендації та пропозиції до проектів керівних документів у сфері протидії

інформаційному тероризму, спрямованих на адекватну відповідь загрозам національній безпеці України.

Час проведення – 2 год.

Ключові поняття: інформаційний тероризм, національний інформаційний простір, національний кіберпростір,

Навчальні питання:

1. Періодизація та види терористичних атак на інформаційний простір та кіберпростір України.
2. Нормативно-правова база протидії інформаційному тероризму в Україні.
3. Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом.
4. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CERT-UA) у сфері протидії інформаційному тероризму.
5. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом.
6. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.

Література:

Основна: 1, 2, 3, 4, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24, 27, 28, 30, 31, 38.

Додаткова: 1, 5, 8, 9, 12, 15.

Самостійна робота – 15 год.

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 No 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 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.

3. 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. ЗАВДАННЯ ДЛЯ ПІДСУМКОГОВО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК СТУДЕНТІВ, ЗАЛІКОВИХ РОБІТ

Перелік питань до заліку

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

Питання для підготовки:

1. Складові терористичної дії.
2. Поняття «інформаційний тероризм» та його характерні риси.

Медіа-тероризм, його характерні риси та способи здійснення.

3. Кібертероризм, його характерні риси, види та способи здійснення.
4. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами).
5. Види правопорушень в інформаційній сфері (правопорушення, пов'язані зі змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав).
6. Протидія інформаційному тероризму в рамках ООН.
7. Протидія інформаційному тероризму в рамках НАТО.
8. 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.

Приклад екзаменаційного білету

Харківський національний університет імені В. Н. Каразіна
Факультет міжнародних економічних відносин та туристичного бізнесу

Галузь знань: 29 «Міжнародні відносини»
Спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітня програма: «Міжнародна інформаційна безпека»
Семестр: 3
Форма навчання: денна
Рівень вищої освіти: другий (магістерський)
Навчальна дисципліна: «Інформаційний тероризм»

ЗАЛІКОВИЙ БІЛЕТ № 1

1. Медіа-тероризм, його характерні риси та способи здійснення (20 балів).
2. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму (20 балів).

Затверджено на засіданні кафедри міжнародних відносин, міжнародної інформації та безпеки протокол № 1 від “27” серпня 2019 р.

Завідувач кафедри _____ Л. В. Новікова

Екзаменатор _____ Л. В. Зіняк

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 кибератаки 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/2c5d77 2b29c5a9e2139 a9f6aa96834d0.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).

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/