ПРОБЛЕМА РОЗБУДОВИ СИСТЕМИ ПІДГОТОВКИ КАДРІВ І НАСЕЛЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Анотація

У записці розглянуто проблему створення системи підготовки кадрів і населення для захисту та забезпечення стійкості критичної інфраструктури в Україні на основі передового зарубіжного досвіду та найкращої практики, зокрема досвіду діяльності у рамках Міністерства внутрішньої безпеки США (U.S. Department of Homeland Security, DHS) та Всесвітнього інституту з фізичної ядерної безпеки (World Institute for Nuclear Security).

На основі аналізу передового зарубіжного досвіду в цій сфері та узагальненої інформації про наявні національні можливості щодо розбудови системи підготовки кадрів і населення з питань захисту критичної інфраструктури та забезпечення її стійкості сформульована низка конкретних рекомендацій для міністерств і відомств України.

При підготовці записки були також проаналізовано та узагальнено результати дискусії на цю тему, що відбулася 9 листопада 2016 р. у ході проведеного в НІСД комунікаційного заходу з обговорення питання підготовки кадрів з питань захисту критичної інфраструктури за участі експертів з деяких країн-членів Альянсу.

ПРОБЛЕМА РОЗБУДОВИ СИСТЕМИ ПІДГОТОВКИ КАДРІВ І НАСЕЛЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Вступ

Добре відомо, що у проведенні реформ і запровадженні нових підходів у тому чи іншому напрямі діяльності, вирішальну роль відіграє людський фактор. І захист або забезпечення безпеки критичної інфраструктури (КІ) від усіх видів загроз, звичайно, не може бути винятком.

З огляду на безпекову ситуацію, в якій перебуває Україна, а також на ті світові тенденції, які формують нові загрози та виклики безпеці у глобальному та регіональному вимірах, проблематику захисту критичної інфраструктури (ЗКІ), взагалі, та підготовки кадрів для системи ЗКІ, зокрема, не можна не визнати як актуальну.

Слід зазначити, що у світі ЗКІ, як концептуальний підхід до захисту критично важливих систем і об'єктів, активно розвивається вже протягом останніх, приблизно, 15 років (після терактів 11 вересня 2001 року). Що стосується нашої країни, то після тривалого періоду деградації сектору безпеки зараз відбувається його докорінне реформування. Тому у напрямі запровадження сучасних підходів до ЗКІ зроблені лише перші кроки. З іншого боку є й серйозні приводи для оптимізму. Зокрема, той факт, що «*21 листопада за ініціативи делегації України відбулося засідання Ради Безпеки ООН у форматі Арріа* щодо захисту об'єктів критичної інфраструктури від терористичних атак*»[1], свідчить про те, що на вищому політичному рівні держави сформовано чітке уявлення про необхідність розвитку цього безпекового напряму. При цьому очевидно, що винесення саме Україною проблематики ЗКІ на міжнародний рівень дозволяє з упевненістю розраховувати на те, що й у подальшому питанням міжнародної співпраці та обміну передовим досвідом у цій сфері, у т.ч. щодо підготовки кадрів, в нашій країні буде приділятися належна увага.

Національний інститут стратегічних досліджень (далі – НІСД) упродовж кількох останніх років веде активну роботу, спрямовану на сприяння запровадженню концепції ЗКІ в Україні, використовуючи при цьому можливості співпраці з Програмою професійної підготовки НАТО

[1] З повідомлення на сайті *Міністерства закордонних справ України* від 22 листопада 2016р.

* Засідання Ради Безпеки ООН за формулою Арріа проводяться за ініціативою делегацій держав-членів РБ ООН з метою надання членам Ради можливості отримати інформацію з того чи іншого питання від широкого кола учасників, які зазвичай позбавлені можливості бути заслуханими Радою Безпеки. Такі засідання можуть проводитися в закритому (за участю лише членів РБ ООН) та відкритому (для усіх держав-членів ООН) форматах і дозволяють їхнім учасниками вести прямий діалог з представниками урядів, міжнародних організацій та недержавними акторами з питань, які входять до сфери компетенції РБ ООН. [Електронний ресурс]. – Режим доступу: http://mfa.gov.ua/ua/press-center/news/52602-za-iniciativi-ukrajini-vidbulosy-zasidannya-rb-oon-u-formati-arria-shhodo-zahistu-kritichnoji-infrastrukturi-vid-terorizmu

(ППП). Ось і при підготовці цієї записки були враховані матеріали засідання *Міжвідомчої експертної робочої групи з питань протидії розповсюдженню зброї масового знищення, тероризму та захисту критичної інфраструктури* та *Робочої групи щодо співробітництва з НАТО з питань енергетичної безпеки*[2], яке пройшло за участі експертів з країн-членів Альянсу і було організовано спільно НІСД і ППП.

Короткий огляд форм і форматів навчальних курсів щодо захисту КІ та забезпечення її стійкості

Незважаючи на те, що ЗКІ є порівняно новою безпековою концепцією, наразі в світі існує безліч інформації з цієї проблематики, у т.ч. стосовно підготовки кадрів та підвищення інформованості населення щодо захисту та забезпечення стійкості КІ.

Найбільший інтерес викликає досвід таких країн, як США, визнаного лідера у запровадженні сучасних підходів у сфері безпеки. Що стосується галузевих підходів, то тут належну увагу слід приділити ядерному сектору КІ, в якому історія захисту ядерних установок та ядерних матеріалів поза військовими програмами налічує вже кілька десятків років. У зв'язку з цим у записці використані інформаційні матеріали та досвід діяльності *Всесвітнього інституту з фізичної ядерної безпеки*[3], провідної спеціалізованої неприбуткової міжнародної організації, одним із головних завдань якої є поширення знань та підготовка кадрів для сфери фізичної ядерної безпеки (ФЯБ).

Крім ядерної галузі багатий досвід у забезпеченні фізичної безпеки (захищеності) відповідних об'єктів, персоналу та матеріальних цінностей, зменшенні ризиків, пов'язаних із загрозами злочинних дій, включаючи тероризм, мають авіатранспорт і банківсько-фінансова сфера.

---

[2] Див. звіт про захід на сайті НІСД. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2392/

[3] *World Institute for Nuclear Security, WINS* - спеціалізована неурядова міжнародна організація (Відень Австрія), однією з місій якої є поширення знань та підготовка кадрів для сфери фізичної ядерної безпеки (ФЯБ). [Електронний ресурс]. – Режим доступу: (www.wins.org)

Водночас, слід зазначити, що система підготовки кадрів та населення щодо ЗКІ для кожної країни завжди буде унікальною. На конфігурацію та функціонування такої системи впливає цілий комплекс чинників: від особливостей національного законодавства до розподілу повноважень між державними органами, від менталітету та рівня освіти населення до його комп'ютерної грамотності, від соціальної відповідальності бізнесу до розвитку державно-приватного партнерства у цій сфері тощо.

При цьому, комплексний характер завдань, пов'язаних зі створенням такої системи вимагає забезпечення потреб у навчанні в широкому діапазоні цільових аудиторій для різних секторів КІ, створення можливостей як для розповсюдження серед населення базових понять знань (підвищення інформованості) про КІ, так і отримання спеціалізованої вищої освіти.

Ефективному виконанню цих вимог безумовно може сприяти те, що у теперішній час триває процес бурхливого розвитку ІТ-технологій, результати якого дозволяють провідним країнам світу, корпораціям, неурядовим організаціям, залученим до цього процесу, значно урізноманітнити форми і методи навчання і на усіх рівнях та в усіх напрямах. У рамках цього процесу все більшої популярності набувають дистанційні форми навчання з використанням можливостей Інтернету, що дає змогу суттєво зменшити витрати на організацію та проведення учбових та освітніх курсів, а також розширює доступ до необхідних інформаційних ресурсів і створює додаткові можливості для залучення до цього процесу висококваліфікованих викладачів та експертів. Навіть побіжний огляд форм, форматів і методів підготовки кадрів і освітньої діяльності щодо ЗКІ дозволяє зробити попередній висновок, що на даний момент ***на цьому напрямі використовуються практично усі види, форми та інструменти навчання, які притаманні системам загальної освіти та підготовки кадрів*** у провідних країнах світу.

Нижче представлений огляд різних форм, форматів та організаційних підходів у залежності від ряду деяких ключових параметрів процесу

навчання та підготовки кадрів і населення щодо захисту КІ та забезпечення її стійкості (далі – коротко, *підготовка кадрів і населення*).

Досвід організації підготовки кадрів і населення в частині загальних питань захисту КІ на прикладі досвіду США

Відомо, що кожна країна, що запроваджує концепцію захисту КІ, як правило, визначає сектори, які мають відповідні об'єкти, системи і ресурси. Кількість секторів КІ змінюється від країни до країни, але найчастіше це число становить 10 – 12. Ця кількість залежить від багатьох факторів, зокрема, від можливостей (ресурсів) держави забезпечити захист відповідних об'єктів і систем. Найбільш потужна у всіх відношеннях держава світу, США, забезпечує захист 16 секторів КІ[4], визначених директивою Президента. Причому кожний сектор закріплено за одним (іноді двома) державними органами (агентствами), на який (які) покладено відповідальність за діяльність та координацію дій усіх сторін, причетних до захисту систем і об'єктів, віднесених до цього сектору (див. Додаток 1). Підготовка кадрів і населення до захисту від специфічних для даного сектору загроз і ризиків є одним із напрямів діяльності відповідальних міністерств (відомств).

Огляд доступних у мережі Інтернет відкритих інформаційних ресурсів дозволяє зробити попередній висновок про те, що у чітко структурованому вигляді підготовка кадрів та населення щодо захисту об'єктів та систем КІ, які віднесені до того чи іншого її сектору, на даний момент існує лише у США. При цьому можна констатувати, що організаційні підходи до виконання цього завдання перебувають у стадії динамічного розвитку, і про певну завершеність обґрунтовано можна говорити лише для секторів КІ, відповідальність за які покладено на Міністерство внутрішньої безпеки США (*U.S. Department of Homeland Security, DHS)*. Це міністерство одноосібно відповідає за 7 з 16 секторів КІ США, а ще стосовно двох секторів воно

[4] У попередні роки їх число сягало 18.

ділить свою відповідальність з двома іншими державними агентствами (див додаток І)[5].

Відповідно, міністерство, на даний час забезпечує реалізацію програм підготовки персоналу та навчанню з питань ЗКІ (див. Додаток 2)[6] за такими напрямами:

- *Навчання щодо хімічного сектору*;
- *Навчання щодо комерційних об'єктів*[7];
- *Серія з отримання знань про КІ*[8];
- *Навчання щодо сектору гідротехнічних споруд*;
- *Навчання щодо служб надання екстреної допомоги*;
- *Навчання щодо ядерного сектору* (*ядерні реактори, ядерні та радіоактивні матеріали, відходи*).

Звертає на себе увагу, що у цьому списку відсутні сектори зв'язку (*Communications*) та інформаційних технологій (*Information Technology*), що належать до сфери відповідальності *DHS*, а також сектори, стосовно яких *DHS* несе спільну відповідальність: *за урядові об'єкти* (разом з Адміністрацією загальних служб, *General Services Administration*), та *за транспортну систему* (*Transporting System*) (разом з Міністерством транспорту, *Department of Transport*). Саме цей факт дозволяє припустити, що навіть у США процес формування секторальних систем підготовки персоналу та населення щодо ЗКІ ще триває.

Крім того, головна сторінка сайту *DHS,* присвячена навчанню з питань ЗКІ, інформує про широкий набір безкоштовних навчальних програм для

---

[5] Слід зазначити, що на національному рівні в організаційному плані ключову роль щодо захисту КІ, включаючи підготовку кадрів і населення, відіграє *Офіс захисту інфраструктури (Office of Infrastructure Protection) DHS,* який було створено для керування національними зусиллями з метою захисту КІ від усіх видів загроз шляхом управління ризиками та забезпечення стійкості КІ, співпрацюючи з усіма заінтересованими сторонами процесу (детальніше див. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/office-infrastructure-protection).

[6] [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/critical-infrastructure-training

[7] Маються на увазі торгівельно-розважальні центри, стадіони, концертні зали, музеї та інші місця проведення масових заходів.

[8] Серія навчальних одногодинних веб-семінарів щодо ЗКІ, які проводяться експертами з метою ознайомлення із засобами, тенденціями, проблемами та передовим досвідом забезпечення безпеки та стійкості КІ. Участь у семінарах є безкоштовною. *DHS* особливо рекомендує проходження такого навчання своїм партнерам з уряду та з приватного сектору, які несуть відповідальність за управління ризиками, безпекою та кризовими ситуаціями.

урядовців та представників приватного сектору, включаючи курси незалежного вивчення з використанням веб-технологій, курси під керівництвом інструкторів, а також про доступ до необхідних учбових матеріалів, призначених для державних чиновників, власників і операторів об'єктів і систем КІ.

Набір учбових курсів, які пропонує *DHS,* включає таке:

- ***Загальні онлайн курси для секторів КІ***

  Ця категорія включає курси та учбові матеріали, загальні для всіх секторів КІ, у т.ч. інформацію про нормативно-правову базу ЗКІ, про засади партнерства та співпраці у ЗКІ тощо. Крім того, для всіх секторів КІ пропонуються курси з підвищення загальної інформованості з питань фізичної безпеки, у т.ч. такі:

  - *Підвищення інформованості про фізичну безпеку на робочому місці (workplace security awareness);*
  - *Ситуація з «активним стрільцем» (an active shooter situation): що потрібно робити;*
  - *Підвищення інформованості про безпеку на об'єктах роздрібної торгівлі (retail security awareness): усвідомлення прихованих небезпек;*
  - *Підвищення інформованості про (незаконне) стеження (surveillance awareness): що потрібно робити;*
  - *Захист критичної інфраструктури проти загроз внутрішнього порушника (insider threats);*
  - *Фізична безпека критичної інфраструктури: крадіжки та переключення*[9] *(theft and diversion), що потрібно робити.*

- ***Курси для конкретних секторів КІ***

  У цьому розділі згруповано курси для перелічених вище окремих секторів КІ, за які несе відповідальність DHS.

[9] Під «переключенням» тут мається на увазі переключення використання матеріалів та обладнання на злочинні цілі.

Крім того, основна сторінка сайту *DHS* з питань навчання і підготовки кадрів для захисту і забезпечення стійкості КІ містить посилання на спеціальний учбовий портал (*Critical Infrastructure Security and Resilience Training Portal*), з корисними посиланнями щодо інших можливостей для навчання з цієї проблематики. Окремий розділ присвячений курсам, підготовленим *Міжвідомчим комітетом з фізичної безпеки* міністерства (*The Interagency Security Committee)* для професіоналів з безпеки, інженерів, власників будівель, архітекторів та населення з метою надати базову інформацію про стандарти фізичної безпеки для урядових об'єктів, процедури забезпечення та найкращу практику досягнення цих стандартів.

Слід також згадати напрям навчання щодо КІ присвячений комплексу навчальних інструментів (*Counter-Improvised Explosive Device (IED) Training and Awareness)*, розроблених міністерським *Офісом із запобігання підривів* (*DHS Office for Bombing Prevention)* з метою ***створення в державі базових можливостей з протидії застосуванню саморобних вибухових пристроїв*** (СВП) та посилення інформованості про терористичні загрози. Навчальні курси розраховані на представників державних органів, починаючи з федерального рівня, чиновників місцевих органів влади, правоохоронців та менеджерів і співробітників служб екстреного реагування, власників і операторів об'єктів КІ, співробітників служб безпеки на підприємствах тощо.

Інший важливий напрям, присвяченій навчанню щодо безпеки КІ, стосується загроз, пов'язаних з ***так званими «активними стрільцями».*** *DHS* пропонує на безоплатній основі семінари (*Active Shooter Preparedness Workshops*) з підвищення готовності до ситуацій, що виникають в результаті дій «активних стрільців», а також відповідні курси та учбові матеріали, які спрямовані на ознайомлення з індикаторами поведінки, що можуть свідчити про намір вчинити напад, а також з моделями поведінки злочинців.

Також слід відзначити наявність спеціального розділу щодо ***навчання для уповноважених користувачів*** (*Authorized User Training*). Відповідні навчальні курси містять інформацію з обмеженим доступом і для участі в них

допускаються особи, яким це необхідно за їх службовими обов'язками. До цієї категорії, наприклад, належить курс з вивчення *інформації про уразливості з точки зору хімічного тероризму* (*Chemical-Terrorism Vulnerability Information*).

На сторінці *DHS*, у розділі «*Інші навчальні ресурси*» (*Other Training Resources)* слід виділити такий важливий напрям підготовки кадрів і населення до захисту КІ і забезпечення її стійкості, як *сприяння відповідній діяльності місцевих громад та місцевого бізнесу*. Ця робота ведеться під девізом «*Безпека батьківщини починається з безпеки рідного міста*». У розділі надане посилання на спеціальну сторінку «*Безпека рідного міста*» (*Hometown Security)*[10], яка містить розроблені настанови із застосування чотирикрокового підходу за формулою: *Встановлюй зв'язок, Плануй, Тренуйся, Доповідай (Connect, Plan, Train, Report)*. У цьому ж розділі необхідно відзначити наявність такого вкрай актуального напряму підготовки кадрів і населення, як *Планування і тренування для забезпечення безпеки шкіл (School Safety Planning and Training),* що є особливо важливим для країн з високим рівнем терористичної загрози.

Основні форми та інструменти підготовки кадрів і населення у рамках окремого сектору КІ на прикладі США

Значний інтерес представляє організація підготовка кадрів і населення для конкретного сектору КІ. Розглянемо досвід США у цьому питанні на прикладі хімічного сектору КІ (Додаток 3). Система підготовки кадрів і населення для хімічного сектору включає як загальні для усіх секторів КІ, так і специфічні для кожного сектору інструменти та напрями діяльності, зокрема:

- Навчання з підвищення інформованості з питань безпеки з використанням Інтернету (*Web-based Security Awareness Training*);

[10] [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/hometown-security

- Навчання та підвищення інформованості щодо протидії загрозам, пов'язаним із саморобними вибуховими пристроями (*Counter-Improvised Explosive Device Training and Awareness*);
- Серія (заходів) з вивчення проблематики безпеки критичної інфраструктури (*Critical Infrastructure Learning Series).*
- ***Семінари та тренування для представників хімічної промисловості та інших заінтересованих сторін галузі*** (*Security Seminars & Exercises for Chemical Industry Stakeholders*);

DHS також надає інформацію щодо додаткових програм через розділ сайту «*Знайди додаткові можливості для навчання*» (*Find Additional Training Opportunities),* який надає інформацію про курси, семінари і учбові програми, що стосуються інших аспектів безпеки КІ, включаючи її ***кібербезпеку***.

Основні форми та інструменти підготовки кадрів і населення з проблематики кібербезпеки КІ

Сучасні підходи до забезпечення безпеки КІ враховують її нерозривний зв'язок з кібербезпекою, і усвідомлення цього факту знаходить своє відображення у національних законодавствах, включаючи українське[11]. З упевненістю можна стверджувати, що значення проблематики кібербезпеки у захисті КІ у подальшому буде лише збільшуватися. Що стосується конкретних форм та інструментів навчання з питань кібербезпеки, то цей розділ діяльності *DHS* містить посилання на такі спеціалізовані сайти:

- Сайт *Національної ініціативи щодо кар'єри та досліджень у сфері кібербезпеки* (*National Initiative for Cybersecurity Careers and Studies, NICSS*)[12], який пропонує у США більш ніж 3000 курсів з цієї тематики, і ця кількість постійно зростає.

[11] ПКМУ від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» http://zakon2.rada.gov.ua/laws/show/563-2016-п

[12] [Електронний ресурс]. – Режим доступу: http://nicss.cert.gov

- Сайт *Програми безпеки систем управління* (*Control Systems Security Program*[13], який підтримує *Група реагування на надзвичайні кібер-події*, пов'язані з промисловими системами управління (*The Industrial Control Systems Cyber Emergency Response Team, ICS-CERT).*
- Сайт заходів під назвою «*Кібер-шторм: захищаючи кібер-простір*» (*cyber-storm-securing-cyber-space*)[14] .

  На цьому сайті розміщено інформацію про фінансовані урядом та схвалені конгресом США тренування національного рівня для підвищення готовності державного та приватного сектора до кібер-атак. Такі тренування проводяться кожні 2 роки, починаючи з 2006 р.

Необхідність підготовки спеціалістів із захисту КІ питанням кібербезпеки добре усвідомлюється не тільки у США, а й в інших розвинутих країнах та їх об'єднаннях. Цьому, зокрема, була присвячена доповідь радника Офісу зв'язку НАТО в Україні Бели Тецеі (*Béla Téczely*) на міжнародному засіданні експертів у листопаді ц.р. у Києві[15].

Попередні результати короткого огляду підходів до організації підготовки кадрів і населення щодо захисту та забезпечення стійкості КІ.

Як зазначалося, захист і забезпечення належної стійкості КІ є комплексним завданням, до виконання якого, у тій або іншій мірі, має бути залучено широке коло осіб, починаючи від керівників вищих ланок державних органів та корпорацій до широких верств населення. Очевидно, що цільові аудиторії процесу підготовки кадрів і населення щодо проблематики КІ доцільно визначати в залежності від обов'язків та ролі тієї чи іншої категорії осіб у процесі захисту та забезпечення стійкості КІ.

---

[13] [Електронний ресурс]. – Режим доступу: http://ics-cert.us-cert.gov

[14] [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/cyber-storm-i

[15] *Бела Тецеі (Béla Téczely)* «*Cyber Defence and Critical Infrastructure Protection: Why it is vital to include Cyber Defence into education when it comes to Critical Infrastructure Protection*», НІСД, інформаційний огляд заходу. http://www.niss.gov.ua/public/File/2016_table/Teczely.pdf

На прикладі хімічного сектору КІ в США, до найкращої практики підготовки кадрів і населення слід віднести таке:

1. Увесь комплекс навчальних курсів та інших навчальних інструментів та відповідної інформації ділиться на дві основні модулі: *загальний для усіх секторів КІ* та *специфічний для кожного окремого сектору.*
2. *Загальний модуль* включає навчальні курси та інформаційні матеріали, що стосуються актуальних питань:

   a. підвищення безпеки на робочому місці;

   b. настанов для ситуацій, викликаних діями «активного стрільця»;

   c. виявлення незаконного стеження та реагування на нього;

   d. протидія застосування саморобних вибухових пристроїв;

   e. забезпечення безпеки на об'єктах роздрібної торгівлі;

   f. захисту критичної інфраструктури проти внутрішніх порушників;

   g. протидії крадіжкам та переключенню матеріалів та обладнання тощо.

   Як правило навчання та надання інформації для заходів та інструментів *загального модулю* здійснюється на безоплатній основі або за дуже низькими цінами.
3. *Специфічний для кожного сектору модуль* обов'язково має включати навчальні заходи щодо підвищення інформованості з питань ЗКІ ключових суб'єктів цього процесу – представників керівної ланки компетентних державних органів, у т.ч. органів управління; правоохоронних органів; служб екстреної допомоги, власників та операторів об'єктів КІ тощо.
4. Подальше зростання ролі ІТ-технологій у житті окремої людини, суспільства і держави в цілому обумовлює виключне значення, якого набувають питання *кібербезпеки* для забезпечення безпеки та стійкості КІ. У провідних країнах світу це знаходить своє

відображення в активному розвитку навчальних курсів та інших учбових інструментів з питань кібербезпеки у рамках підготовки кадрів і населення для ЗКІ.

Стосовно підвищення інформованості щодо основ захисту та забезпечення стійкості КІ (іншими словами, ознайомлення з базовими знаннями щодо КІ) бажано, щоб через таке навчання пройшло якомога більше представників населення, робітників підприємств та компаній, керівників та управлінців різного рівня та з різними функціональними обов'язками, то спеціалізоване навчання потребує адресності навчальних матеріалів та більш-менш чіткого визначення цільової аудиторії.

У цьому питанні має сенс послатися на передовий досвід *Всесвітнього інституту з фізичної ядерної безпеки (WINS)*[16], який набув багатий досвід у підготовці кадрів для одного із секторів КІ, а саме – ядерного. При *WINS* створено академію, яка пропонує цілу низку навчальних курсів і матеріалів стосовно різних аспектів забезпечення фізичної ядерної безпеки. Усі, категорії учасників курсів мають пройти базовий курс[17] (*foundation module)* з ФЯБ, та, крім того, хоча б один зі спеціальних курсів, розроблених для таких категорій осіб (цільових аудиторій)[18]:

a. *державних управлінців вищої ланки та членів рад директорів великих компаній;*
b. *керівники компаній, що мають ядерні матеріали та ядерні технології;*
c. *наукових співробітників та інженерно-технічного персоналу;*
d. *управлінців з питань реагування на інциденти, пов'язані з фізичною безпекою ядерних об'єктів;*
e. *осіб, відповідальних за підтримання зв'язку з населенням та громадянським суспільством;*

[16] Див. посилання 3.
[17] Англ. – *foundation module.*
[18] *WINS Academy Nuclear Security Management Certification Programme. Reference Guide.* November 2014. [Електронний ресурс]. – Режим доступу: https://www.wins.org/files/2014_11_24-wins_academy_referenceguide_version1.pdf

f. *управлінців, які несуть відповідальність за фізичну безпеку радіоактивних джерел;*

g. *управлінців з питань виконання програм з фізичної безпеки;*

h. *регуляторів фізичної ядерної безпеки;*

i. *управлінців з питань безпеки перевезень ядерних матеріалів.*

У наведеному списку відображено, що є цілком зрозумілим, специфіку ядерної галузі, але аналогічний загальний підхід до формування цільових аудиторій для підготовки кадрів і навчання достатньо просто можна адаптувати для більшості інших секторів КІ, враховуючи безпекові умови, загрози та ризики, характерні для кожного конкретного сектору.

Пріоритетні завдання щодо запровадження навчальної та освітньої діяльності стосовно ЗКІ в Україні

В Україні існує ціла низка установ і організацій системи загальної освіти, а також спеціалізованої (професійної) підготовки кадрів з питань, які у розвинутих країнах безпосередньо пов'язують із захистом та забезпеченням стійкості КІ. Крім того, в країні функціонує ряд наукових та науково-дослідних організацій, які потенційно спроможні зробити належний внесок у створення та функціонування відповідної системи.

До цих установ слід віднести, насамперед, провідні українські університети – *Київський національний університет імені Т.Г. Шевченка* та *Національний технічний університет України «Київський політехнічний інститут» ім. Ігоря Сікорського»*; учбові заклади системи правоохоронних і силових органів – *Національну академію Служби безпеки України*, *Національну академію внутрішніх справ України*, *Інститут спецзв'язку Держспецзв'язку України*, *Національний університет оборони України імені Івана Черняховського*, учбові та науково-дослідні заклади національної системи цивільного захисту Україну, наукові установи *Національної академії наук України*, *Національну академію державного управління при Президентові України*, *Національний інститут стратегічних досліджень*.

Враховуючи широкий спектр питань, які слід вирішувати для забезпечення захисту та стійкості усіх секторів КІ стосовно усіх видів загроз, зрозуміло, що до підготовки кадрів і населення крім перелічених вище навчальних і науково-дослідних закладів необхідно буде залучати інші галузеві установи, які мають специфічну компетенцію у тому чи іншому секторі КІ, а також використовувати можливості експертної спільноти, для чого необхідно створювати відповідні бази даних.

При цьому, констатуючи той факт, що Україна володіє неабияким потенціалом щодо підготовки і перепідготовки професійних кадрів для системи ЗКІ, необхідно зазначити, що ***практика систематичної роботи з населенням з безпекової проблематики в нашій країні фактично відсутня***. Тому цей компонент загальнонаціональної системи підготовки кадрів і населення слід буде створювати фактично з нуля, беручи до уваги, що, як правило, населенню надається можливість отримувати необхідні знання з цієї проблематики на безоплатній основі.

Зрозуміло, що проведення цілеспрямованої, скоординованої роботи з підготовки кадрів та населення щодо ЗКІ потребує відповідної нормативно-правової бази. Найближчим часом для нашої країни можливість досягнення суттєвого прогресу в цьому безпековому напрямі, взагалі, та у підготовці кадрів і населення для ЗКІ, зокрема, буде значною мірою обмежуватися швидкістю, з якою будуть прийняті необхідні нормативно-правові акти.

Разом з тим, слід враховувати, що теперішня безпекова ситуація, в якій перебуває Україна, а також швидкість змін у безпековій сфері, що відбуваються на усіх рівнях – глобальному, регіональному та національному – роблять вкрай непродуктивною позицію, яку відкрито або приховано займають деякі відомства та організації стосовно ЗКІ, вимагаючи спочатку прийняти відповідні законодавчі акти.

Слід зазначити, що Україна має певний позитивний досвід розвитку системи підготовки і перепідготовки кадрів в сфері критичної інфраструктури, до кінцевого врегулювання питання на законодавчому рівні.

Мається на увазі фізичний захист ядерних матеріалів та ядерних установок. Дійсно, *Навчальний центр з фізичного захисту, обліку та контролю ядерного матеріалу ім. Джорджа Кузмича*, який відповідає усім сучасним вимогам до навчального процесу, було відкрито в *Інституті ядерних досліджень* НАНУ в жовтні 1998 р., тобто за два роки до того, як було прийнято профільний закон України про фізичний захист ядерних матеріалів та ядерних установок.

Висновки

Виходячи з наведеного вище, а також спираючись на зарубіжний передовий досвід та кращу практику в цій сфері, можна сформулювати такі висновки:

1. З огляду на зростання терористичних та інших загроз національній безпеці України й, у зв'язку з цим, нагальну необхідність у підвищенні рівня захисту та стійкості національної критичної інфраструктури, слід значно прискорити створення відповідної нормативно-правової бази, визначивши найвищим пріоритетом у цьому напрямі розробку та прийняття у 2017 році профільного закону.
2. Паралельно із зусиллями щодо розвитку національної нормативно-правової бази необхідно вживати заходів у напрямі забезпечення інституційної підтримки запровадження концепції захисту КІ в Україні, включаючи розбудову відповідної системи підготовки кадрів і населення.
3. Визнання вищим політичним керівництвом держави пріоритетності питань захисту критичної інфраструктури для національної безпеки і винесення Україною цього питання на засідання Ради безпеки ООН має бути підкріплено, насамперед, енергійними діями на рівні керівництва суб'єктів забезпечення національної безпеки, а також керівників, операторів/ власників крупних компаній, об'єкти та системи яких, як правило, відносять до критичної інфраструктури.

4. Зважаючи на реальні загрози критичній інфраструктурі держави у теперішніх безпекових умовах, створення системи підготовки кадрів і населення щодо підвищення рівня захисту та стійкості критичної інфраструктури повинно і може здійснюватися випереджувальними темпами, адже людський фактор є ключовим чинником успішності реформування сектору безпеки держави.
5. Державна політика у сфері підготовки кадрів та населення щодо захисту та забезпечення стійкості критичної інфраструктури має визначити одним із своїх пріоритетів системну роботу з населенням із загальної проблематики захисту критичної інфраструктури та забезпечення її стійкості зі створенням можливостей для отримання необхідних знань на безоплатній основі, у т.ч. шляхом використання Інтернету та інших сучасних технологій.
6. Програми підготовки кадрів та населення щодо захисту та забезпечення стійкості критичної інфраструктури обов’язково мають включати проблематику кібербезпеки.

Рекомендації та пропозиції

З метою розбудови системи підготовки кадрів та населення до захисту та забезпечення стійкості КІ в Україні та спираючись на сформульовані вище висновки, вважаємо за доцільне зробити такі рекомендації та пропозиції:

1. Апарату РНБОУ:

   розглянути можливість винесення у першому півріччі 2017 року питання про захист критичної інфраструктури в Україні на засідання Ради національної безпеки і оборони України, підготувавши до цього засідання конкретні пропозиції щодо розробки профільного законопроекту.
2. Кабінету Міністрів України:

   запропонувати міністерствам і відомствам, перелік яких визначити, виходячи із визначення термінів «критична інфраструктура» та

«об'єкти критичної інфраструктури»[19] підготувати пропозиції щодо створення у своїй структурі підрозділів, які б опікувалися проблематикою захисту критичної інфраструктури, включаючи питання підготовки кадрів та населення.

3. Міністерству освіти і науки України:

   запропонувати вищим навчальним закладом України розробити та подати у встановленому порядку пропозиції щодо включення проблематики захисту критичної інфраструктури до навчальної програми.

4. Національному агентству з питань державної служби та Національній академії державного управління при Президентові України:

   опрацювати питання щодо включення проблематики захисту критичної інфраструктури у навчальні програми підготовки та перепідготовки державних службовців.[20]

5. Службі безпеки України, Міністерству оборони України та Міністерству внутрішніх справ України забезпечити запровадження у підвідомчих навчальних закладах:

   - навчальні програми для працівників сектору безпеки і оборони з питань захисту критичної інфраструктури;
   - навчальні курси для населення, які забезпечують настанови на теми:
     - фізична безпека на робочому місці;
     - поведінка у ситуаціях з «активним стрільцем»;
     - захист критичної інфраструктури проти загроз внутрішніх порушників;
     - виявлення незаконного стеження щодо об'єктів критичної інфраструктури;
     - протидії використанню саморобних вибухових пристроїв.

[19] «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» Постанова Кабінету міністрів України від 23 серпня 2016 р. за №563.

[20] Пропозиції щодо відповідної програм підготовлені НІСД. Дивись презентацію: О.Суходоля «*Навчання керівного складу державних органів та інших організацій у сфері захисту критичної інфраструктури*», НІСД, інформаційний огляд заходу. http://www.niss.gov.ua/public/File/2016_table/Suhodolya.pdf

Відділ енергетичної та техногенної безпеки

(С.І. Кондратов)

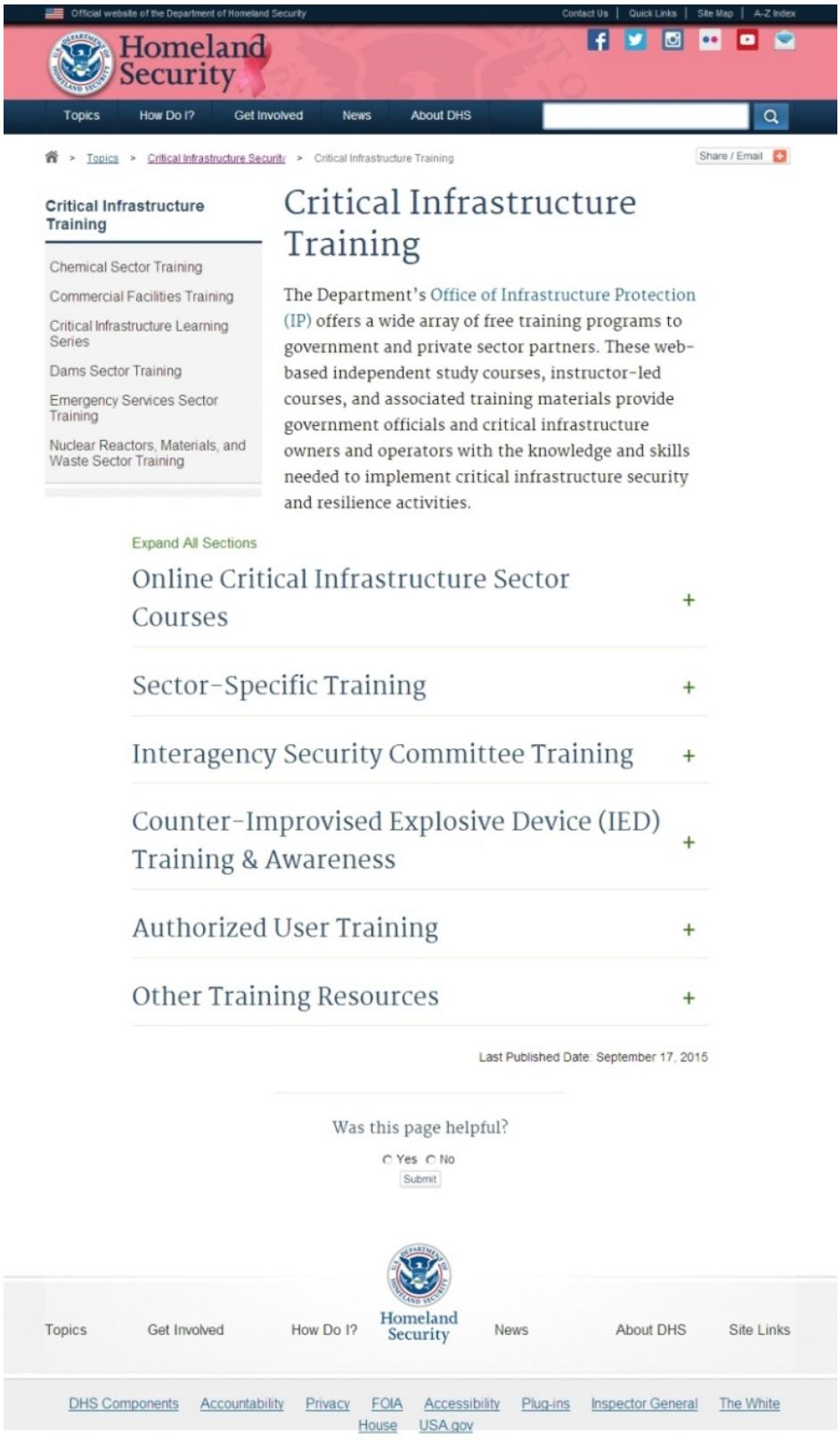
Додаток 1

Розподіл відповідальності за сектори КІ між урядовими органами США

1. Хімічний *Chemical)*	Міністерство внутрішньої безпеки
2. Комерційні об’єкти *(Commercial Facilities)*	Міністерство внутрішньої безпеки
3. Зв'язок *(Communications)*	Міністерство внутрішньої безпеки
4. Критичне виробництво *(Critical Manufacturing)*	Міністерство внутрішньої безпеки
5. Гідротехнічні споруди *(Dams)*	Міністерство внутрішньої безпеки
6. Військово-промислова база *(Defense Industrial Base)*	Міністерство оборони
7. Аварійно-рятувальні служби *(Emergency Services)*	Міністерство внутрішньої безпеки
8. Енергетичний *(Energy)*	Міністерство енергетики
9. Сектор фінансових послуг (*Financial Services)*	Міністерство фінансів
10. Сектор продовольства та сільського господарства *(Food and Agriculture)*	Міністерство сільського господарства + Міністерство охорони здоров’я та соціальних служб
11. Урядові об’єкти (*Government Facilities*)	Міністерство внутрішньої безпеки + Адміністрація загальних служб
12. Медицина та охорона здоров’я (*Healthcare and Public Health)*	Міністерство охорони здоров’я та соціальних служб
13. Інформаційні технології *(Information Technology)*	Міністерство внутрішньої безпеки
14. Ядерні реактори, матеріали та відходи (*Nuclear Reactors, Materials, and Waste)*	Міністерство внутрішньої безпеки
15. Транспортна система (*Transporting System*)	Міністерство внутрішньої безпеки + Міністерство транспорту
16. Системи водопостачання та відведення стічних вод (*Water and Wastewater Systems*)	Агентство з охорони навколишнього середовища

Додаток 2

Сторінка офіційного сайту DHS, присвячена навчанню з питань КІ



Додаток 3

Сторінка сайту DHS, присвячена навчанню з питань захисту КІ для хімічного сектору