НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

Серія «Національна безпека». Випуск 5

КОНЦЕПЦІЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЇЇ ВПРОВАДЖЕННЯ В УКРАЇНІ

Збірник матеріалів міжнародної науково-практичної конференції
(7-8 листопада 2013 р., Київ – Вишгород)

Київ 2014

УДК 32.1:323.28:342.77:519.22(477)
К 65

Серію засновано
у 2013 році

Упорядники:

Д. С. Бірюков, к. т. н.;
С. І. Кондратов

За загальною редакцією заслуженого діяча науки і техніки України, д. м. н., професора *Ю. М. Скалецького*

Електронна версія: http://www.niss.gov.ua

К 65 **Концепція** захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні : зб. матеріалів міжнар. наук.-практ. конф. (7-8 листопада 2013 р., Київ – Вишгород) / упоряд. Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2014. – 148 с. – (Сер. «Національна безпека», вип. 5).

ISBN 978-966-554-222-3

Представлено матеріали міжнародної науково-практичної конференції з теми «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні», проведеної 7-8 листопада 2013 р. Національним інститутом стратегічних досліджень спільно з Офісом зв'язку НАТО в Україні та ПАТ «Укргідроенерго».

Висвітлено актуальні проблеми забезпечення безпеки критично важливих для життєдіяльності держави, здоров'я людей і довкілля об'єктів і систем.

ISBN 978-966-554-222-3

ПЕРЕДМОВА

Наприкінці XX ст. світ стикнувся з тенденцією різкого зростання загрози тероризму, що виявлялося не лише у значному збільшенні кількості терористичних актів (у т.ч. з важкими наслідками), а й в активізації намагань терористів оволодіти зброєю та матеріалами масового знищення, їх намаганні розробляти нові способи здійснення терористичних атак (у т.ч. із використанням новітніх технологій) з метою спричинення максимальної кількості жертв і значних руйнувань.

Рівень і масштаби загрози тероризму були значною мірою усвідомлені в результаті терористичних актів 11 вересня 2001 р. Ці події засвідчили, що терористи здатні на будь-які дії задля досягнення своїх цілей, і тому, за певних умов, найбільш привабливими мішенями для них можуть стати об'єкти, системи й ресурси тієї чи іншої держави, які є критично важливими для забезпечення її життєдіяльності, безпеки її громадян і довкілля. Саме такі об'єкти, системи й ресурси відносять до т.зв. критичної інфраструктури (КІ) держави.

Безумовно, фізичній безпеці таких об'єктів і систем приділялася значна увага з боку урядів більшості країн світу, але у випадку відсутності безпосередньої воєнної загрози забезпечення їх захисту розглядалося переважно з погляду впливу техногенних і природних чинників. Глобальні безпекові зміни наприкінці XX – початку XXI стст. змусили провідні держави світу й міжнародні організації докорінно переглянути свої підходи до забезпечення безпеки, що значно активізувало процес інтеграції відповідних заходів у межах спеціального безпекового напряму – захисту критичної інфраструктури. При цьому системний підхід до такого амбіційного завдання забезпечується, з-поміж іншого, й тим, що критична інфраструктура розглядається як дуже складний, але єдиний об'єкт захисту, здійснюваний компетентними державними органами й іншими суб'єктами процесу, що дає їм змогу більш ефективно застосовувати загальні механізми управління ризиками та наявними ресурсами.

Захист критичної інфраструктури як напрям забезпечення безпеки на національному та міжнародному рівнях набув нормативно-правового

оформлення у таких провідних країнах світу, як США, Канада, Велика Британія, Австралія, Росія, у країнах-членах ЄС, які імплементують відповідні директиви Європейської Комісії. Значна увага приділяється захисту КІ і в діяльності НАТО, що відображено, зокрема, у його Політичних директивах з боротьби проти тероризму, прийнятих у травні 2012 р. на саміті Альянсу в Чикаго (США). Масштаби наслідків терористичних нападів на елементи критичної інфраструктури або інші надзвичайні ситуації, пов'язані з нею, дуже гостро ставлять питання взаємодії та співробітництва у зниженні ризиків таких подій і на національному, і на міжнародному рівнях.

У Національному інституті стратегічних досліджень (НІСД) приділяється значна увага дослідженням різних аспектів протидії тероризму. Із березня 2011 р. при НІСД працює Міжвідомча експертна робоча група (МЕРГ) з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних із ними терористичних загроз і захисту критичної інфраструктури. Із часу створення МЕРГ провела 12 засідань, під час яких неодноразово розглядалися питання, пов'язані з безпекою критичної інфраструктури. Зі звітами про засідання МЕРГ та з аналітичними матеріалами, підготовленими в результаті роботи групи, можна ознайомитися на сайті НІСД.

Саме під час зазначених засідань виникла ідея проведення спільно з НАТО міжнародної конференції з проблематики критичної інфраструктури, на що Офіс зв'язку НАТО в Україні дав згоду.

При підготовці програми конференції організатори виходили із необхідності урахування факту проведення в Україні спільно з НАТО міжнародних консультацій із питань інформаційної та кібербезпеки, тематика яких тісно пов'язана із темою конференції. Таким чином, структурно програма останньої складалася із трьох основних блоків:

• *перший* – виступи (пленарне засідання), присвячені питанням захисту об'єктів і систем критичної інфраструктури України за окремими напрямами й секторами з урахуванням того, що в нашій країні досі не запроваджено інтегрований підхід до захисту національної критичної інфраструктури;

• *другий* блок (друге пленарне засідання) присвячений зарубіжному досвіду захисту критичної інфраструктури на національному та міжнародному рівнях. Під час цього засідання обговорювалися переваги, які надає застосування концепції критичної інфраструктури у країнах НАТО, про діяльність Альянсу у цьому напрямі;

• *третій* блок питань (третє виїзне засідання) об'єднав питання реалізації заходів із фізичної безпеки на окремих об'єктах і системах, а також питання наукових досліджень щодо забезпечення фізичної безпеки критичної інфраструктури.

Крім того, до збірника матеріалів увійшли рішення конференції, використані НІСД при підготовці аналітичних матеріалів для відповідних державних органів.

ВИСТУПИ УЧАСНИКІВ

БЕЗПЕКА ОБ'ЄКТІВ ГІДРОЕНЕРГЕТИКИ УКРАЇНИ: ПРІОРИТЕТ ДІЯЛЬНОСТІ ПАТ «УКРГІДРОЕНЕРГО»

СИРОТА Ігор Миколайович,
генеральний директор
ПАТ «Укргідроенерго»

ПАТ «Укргідроенерго» – найбільша гідрогенеруюча компанія України. До її складу входять дев'ять станцій на річках Дніпро та Дністер. У 2013 р. на станціях нашого товариства працював 101 гідроагрегат сумарною встановленою потужністю 5040 МВт. Наприкінці 2013 р. ми мали отримати додатково ще один гідроагрегат, який мав працювати на Дністровській ГАЕС, тож сумарна потужність буде 5365 МВт.

У середині 90-х років XX ст. було розпочато масштабний проект реконструкції наших станцій (це перший досвід роботи з іноземними інвестиціями). До фінансування зазначеного проекту долучився Світовий банк, який нині залишається нашим надійним партнером і кредитором. П'ять років тому на Всесвітньому форумі керівників у м. Нью-Йорку наша компанія увійшла до списку сотні ліпших компаній світу, що здійснюють реконструкцію обладнання та споруд за кредитні кошти банку. Запорукою тривалого та взаємовигідного співробітництва є не лише розуміння важливості реалізації цього масштабного й амбітного проекту, який дає друге життя українським ГЕС, продовжуючи термін їх безпечної та надійної експлуатації ще на 30–40 років, а й відкритість нашої компанії до співробітництва з міжнародними фінансовими організаціями, прозорість її роботи, фінансової звітності й демонстрація високих якісних показників роботи.

Нині активно реалізується другий етап Проекту реконструкції ГЕС, що технічно реабілітує всі станції. Після завершення матимемо повністю нові в технічному плані станції. Наприклад, на Київській ГЕС уже завершено реконструкцію та модернізацію останнього, 20-го гідроагрегата, й 2014 р. це буде станція з повністю новими 20-ма турбінами й генераторами, електронним і механічним обладнанням, сучасною системою керування та контролю, всіма засобами безпеки найвищого рівня. Зага-

лом по всіх станціях уже завершено понад половину запланованих Проектом реабілітації робіт, і ці темпи лише прискорюються, адже робота має бути завершена до 2017 р., що збільшить потужність діючих ГЕС на 250 МВт.

Звичайно, що в 90-ті роки XX ст. через складну фінансово-економічну ситуацію в державі запустити цей проект без зовнішньої фінансової підтримки було б неможливо. Завдяки коштам Світового банку він став реальністю. Звісно, компанія вкладає і значну частку власних коштів, які вона отримує за рахунок тарифу на вироблену електроенергію. Однак їх недостатньо, тому ми змушені залучати додаткове фінансування у міжнародних фінансових організацій під державні гарантії уряду. Процентна ставка таких кредитів є низькою, умови надання коштів досить привабливі, зважаючи на термін кредитування й пільгові періоди повернення. Крім того, залучення таких інвестицій не створює додаткового навантаження на тариф.

За попередні роки до фінансування проекту реконструкції станцій долучилися ще два банки – Європейський інвестиційний банк і Європейський банк реконструкції та розвитку, які надали два кредити в сумі 400 млн євро. Таким чином, за цим проектом від початку його реалізації ми вже залучили 680 млн дол. США на дуже вигідних пільгових умовах.

Також у 2008–2012 рр. компанія успішно реалізувала проект спільного впровадження за проектом реконструкції ГЕС, що скоротило викиди CO_2 обсягом понад 800 тис. т од., це дало змогу отримати майже 4 млн євро додаткового ресурсу фінансування на заходи з реконструкції станцій.

Реконструкція діючих станцій – це лише один з напрямів діяльності компанії. Значна увага приділяється будівництву нових генеруючих потужностей. Спорудження нових об'єктів у будь-якій галузі економіки привертає увагу банкірів. Так, проектами будівництва Канівської ГАЕС і Каховської ГЕС-2 уже зацікавилися не лише міжнародні фінансові організації, а й комерційні банки Німеччини, Китаю та інших країн. Зараз ми ініціюємо залучення коштів на будівництво Канівської ГАЕС – сподіваємося отримати близько 1 млрд дол. США кредитних коштів, що покриє 70 % необхідного фінансування (решту забезпечимо коштами компанії). Крім того, кілька років тому ЄБРР виділив грант обсягом 1 млн євро на розроблення ТЕО розширення Каховської ГЕС-2. На цей проект сподіваємося залучити понад 500 млн дол. США від МФО, довіру яких ми вже завоювали.

Нині «Укргідроенерго» – це потужна структура, яка разом зі своїми постійними партнерами здатна забезпечити повний цикл реалізації масштабних інфраструктурних проектів – від стадії проектування, будівництва до безпосередньої експлуатації. Ми є прикладом для багатьох іноземних (не лише гідроенергетичних), а й усіх енергетичних та інших компаній щодо спроможності власноруч реалізувати досить амбітні проекти з «нуля», використовуючи виключно власну робочу силу, обладнання українського виробництва та, крім усього, власні оборотні кошти, які вкладаються в економіку України, що стимулює економічний розвиток держави.

Прикладом такої роботи є Дністровська ГАЕС – станція, яка за проектом уже потрапила до п'ятірки найпотужніших у світі й має стати найбільшою в Європі; станція, яку ми будуємо вже чимало років за власні та кредитні кошти державних банків України. І якщо ще 15 років тому цей проект усі називали «покинутим радянським довгобудом», то нині основна увага влади та світового гідроенергетичного товариства прикута до пуску першої черги вже реально працюючої станції, яка за масштабами будівництва не поступається славетному ДніпроГЕСу. Нині будівництво Дністровської ГАЕС – чи не єдиний і чи не найбільший інфраструктурний проект, що реалізується в Україні самими українцями.

Перший гідроагрегат, потужність якого можна порівняти із цілою ГЕС на Дніпрі, було введено у промислову експлуатацію три роки тому. Після коригування проекту було внесено корективи щодо будівництва верхньої водойми. Оскільки Дністровська ГАЕС є маневровою станцією, то було прийнято рішення про збільшення маневрової потужності й перехід від добового на тижневий графік регулювання, а також завершення будівництва верхньої водойми в повному обсязі. Завдання виконано, і тепер за рахунок зменшення споживання газу й мазуту енергетики мають змогу економити близько 800 млн грн щорічно.

Як і було обіцяно керівництву держави та громадськості, поставлене перед нами завдання розпочати пускові операції другого гідроагрегату станції вже у грудні 2013 р. та ввести в експлуатацію першу чергу у складі трьох гідроагрегатів у 2015 р. згідно із затвердженим графіком має бути виконано.

Зараз роботи в шахтах другого і третього гідроагрегату, в машинному залі, на найбільшій штучній водоймі ГАЕС у Європі та інших пускових об'єктах ведуться без зупинки, замовлення на все основне гідросилове обладнання станції вже розміщено та сплачено авансовим платежем. Це

обладнання буде вітчизняного виробництва, а саме державних заводів «Турбоатом», «Електроважмаш», Запорізького трансформаторного заводу, чим відверто пишаємося.

Нині зусилля «Укргідроенерго» разом із Міністерством енергетики та вугільної промисловості України спрямовані на монтаж і пуск обладнання другого гідроагрегату, завершення будівництва житлового будинку та виконання низки взятих на себе зобов'язань перед місцевими мешканцями щодо розвитку регіону. Адже разом із завершенням робіт по другому гідроагрегату людям було обіцяно до кінця року здати в експлуатацію багатоповерховий житловий будинок на 114 квартир.

Звичайно, що реалізуючи проект будівництва і Дністровської ГАЕС, і інших нових об'єктів, «Укргідроенерго» бере участь у розвитку інфраструктури прилеглих територій, для чого у проекти будівництва закладаються відповідні кошти (у випадку із Дністровською та Канівською ГАЕС – по 300 млн грн). Така допомога дає змогу вирішити чимало проблем районів та областей, пов'язаних із будівництвом об'єктів соціально-культурної сфери, житлово-комунального господарства, виконання робіт із благоустрою. Наприклад, у м. Сокиряни, що поблизу будівництва Дністровської ГАЕС, ми профінансували будівництво сучасної районної лікарні, яка нині обслуговує мешканців усього району, також взяли участь у фінансуванні будівництва районного будинку культури в м. Новодністровську. У цьому ж місті ми фінансуємо прокладання водопроводу, здійснюємо капітальне будівництво й реконструкцію електричних і теплових мереж. У таких проектах будівництво позитивно впливає на соціально-економічний розвиток регіону: поліпшується транспортна мережа, збільшується надходження коштів до місцевого бюджету, з'являються додаткові робочі місця тощо.

Наприклад, на будівництві Дністровської ГАЕС задіяно дві тисячі людей і десятки вітчизняних будівельних, монтажних, транспортних, наукових та інших підприємств з усіх куточків України (майже із третини областей). Своїми замовленнями ми допомогли вижити у скрутні часи й вітчизняним виробникам гідросилового та електричного обладнання. Тобто такі проекти необхідно розглядати як рушійні для соціального та економічного розвитку регіонів.

Не на словах і не на папері, а реальною справою ми продемонстрували спроможність самостійно реалізувати такий амбітний і масштабний проект, зрушити з місця процес будівництва та реанімувати радянський довгобуд, переглянути проект і забезпечити його реальним фінансуванням

власними силами, без залучення зовнішніх кредитів, знайти необхідне обладнання та висококваліфікованих фахівців на батьківщині, організувати весь будівельний процес і дати результат – працюючу гідроакумулюючу станцію. Саме це стало домінуючим при прийнятті рішення міжнародними фінансовими організаціями розглянути участь у фінансуванні інших двох об'єктів – Канівської ГАЕС і Каховської ГЕС-2. Ми довели, що спроможні реалізовувати проекти, бути в них надійними партнерами, ефективно використовувати кошти й розвивати галузь, адже ми своєчасно та в повному обсязі виконуємо завдання, визначені в оновленій Енергетичній стратегії до 2030 року, що передбачає за будь-якого сценарію розвитку попиту необхідність будівництва нових гідро- та гідроакумулюючих потужностей. Реалізація всіх зазначених проектів дасть змогу до 2030 р. довести частку маневрених потужностей ГЕС і ГАЕС у загальному балансі галузі із 7 до 16 %. Ми хочемо досягти таких самих показників, які ставлять собі за мету розвинені країни Європейського Союзу.

Будівництво й розвиток гідроенергетики нерозривно пов'язані з розвитком економіки держави та зміцненням її енергетичної незалежності.

ЄВРОПЕЙСЬКИЙ ДОСВІД РОЗБУДОВИ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: УРОКИ ДЛЯ УКРАЇНИ

БІРЮКОВ Дмитро Сергійович,
старший консультант відділу екологічної та техногенної безпеки НІСД

Нині високий ступінь упровадження новітніх технологій є ознакою рівня розвиненості країни, визначальним чинником її економічної конкурентоспроможності, а отже, й необхідною умовою досягнення цілей, що визначаються національними інтересами. Водночас разом із багатьма перевагами технологічний прогрес створив умови безпрецедентної залежності і окремої людини, і суспільства загалом від систем, що надають інформаційні, комунікаційні, транспортні, енергетичні, фінансові й інші послуги. З руйнуванням таких систем нині пов'язують найбільш небезпечні безпекові сценарії для провідних держав світу, зокрема для країн ЄС. Тому, зважаючи на обмеженість ресурсів, об'єктивну неможливість забезпечити абсолютний захист і безпеку всіх інфраструктурних систем, у багатьох країнах світу імплементується концепція критичної інфра-

структури (КІ), що дає змогу сконцентрувати увагу на системах, мережах та окремих об'єктах, знищення або порушення роботи яких матиме суттєві негативні наслідки для національної безпеки цих країн[1].

На початку XXI ст. у наукових роботах почали наголошувати на необхідності подальшого розвитку механізмів захисту європейської КІ на основі трансатлантичних взаємовідносин в економічній і безпековій сферах[2]. На той час у Сполучених Штатах Америки вже були скоєні безпрецедентні терористичні акти й у відповідь на них прийняті законодавчі акти, в яких захист КІ від терористичних загроз визначався як одне з основних завдань системи захисту національної безпеки.

У ЄС, розуміючи рівень загроз і важливість захисту КІ, також ініціювали процеси створення правових та організаційних механізмів у цій сфері. Початком цілеспрямованої роботи можна вважати звернення у 2004 р. Європейської Ради до Європейської Комісії (ЄК) з дорученням щодо підготовки загальної стратегії захисту КІ. Уже в жовтні 2004 р. ЄК оприлюднила офіційне повідомлення[3], в якому містилися і огляд дій, здійснюваних Єврокомісією у цій сфері, і пропозиції стосовно додаткових заходів задля вдосконалення європейської системи запобігання, готовності й реагування на терористичні атаки, спрямовані проти елементів КІ. Також у повідомленні зазначається, що через значну кількість об'єктів, які потенційно можуть бути віднесені до КІ, забезпечити їх захист на загальноєвропейському рівні неможливо, тому, керуючись принципом субсидіарності, загальноєвропейським інституціям потрібно сконцентрувати зусилля на захисті тих об'єктів, припинення функціонування яких матиме транскордонний вплив, залишивши за країнами ЄС відповідальність за інші об'єкти. Водночас наголошується, що підхід до захисту КІ в усіх країнах ЄС має бути загальним. Забезпечити впровадження й реалізацію такого загального підходу мають Європейська програма захисту КІ (ЄПЗКІ) та Європейська інформаційна мережа попередження щодо КІ (*European Critical Infrastructure Warning Information Network*, *CIWIN*).

---

[1] *CEPS* task force report: Protecting critical infrastructure in the EU / B. Hammerly, A. Renda. – Brussels : Centre for European policy studies, 2010. – 100 p.; *Critical* infrastructure protection at the European level // Studia diplomatica. – 2011. – LXIV-1 [Електронний ресурс]. – Режим доступу: http://www.nonproliferation.eu/

[2] *Lembke J.* EU critical infrastructure and security policy / J. Lembke // European economic and political issues. – Nova Science Publishers Inc., 2002. – Vol.6. – P. 49–79.

[3] *Communication* from the Commission to the Council and the European Parliament of 20 October 2004 – Critical infrastructure protection in the fight against terrorism (COM/2004/702 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

В офіційному повідомленні № 786 (2006 р.)[4] ЄК рекомендувала всім країнам ЄС вжити заходів, зазначених у ЄПЗКІ, у національних законодавчих актах і розробити національні програми із захисту КІ. В ЄПЗКІ надано критерій розмежування національної (порушення функціонування її елементів має вплив лише в межах окремої країни ЄС) і загальноєвропейської (виникнення транскордонних наслідків, тобто має вплив щонайменше на дві країни ЄС) КІ. *Основними рекомендаціями із захисту КІ для країн ЄС* є такі:

• розробити національну програму захисту КІ як документ, що має правову силу;

• задовольнити такий рівень охорони здоров'я, технологічної безпеки, національної безпеки, соціально-економічного добробуту, який гарантував би «гнучкість» (стійкість, незламність) нації до загроз;

• уніфікувати зусилля, спрямовані на захист КІ, надавши єдиному державному органу, що звітує із цього питання, функції координації дій державних органів влади, які спеціалізуються й мають тісні відносини з галузями промисловості, до яких належать об'єкти КІ;

• визначити органи державної влади, відповідальні за сектори КІ, та відповідні компанії приватного сектору;

• створити умови для ефективної взаємодії та обміну інформацією, даними й досвідом між країнами-членами ЄС, міжнародного співробітництва і приватним сектором;

• зробити внесок у створення гармонізованого методу на рівні ЄС та європейської системи аналізу ризиків.

Щодо *CIWIN*, то основним завданням цієї мережі є створення засобів координації та інформаційного обміну щодо КІ на загальноєвропейському рівні. *CIWIN* характеризується високими вимогами до забезпечення інформаційної безпеки, оскільки в мережі обробляється інформація, є чутлива щодо забезпечення безпеки об'єктів КІ. Через високі технічні вимоги й унікальність зазначеної інформаційної системи підтримка її функціонування оцінюється в понад 600 тис. євро щорічно[5].

---

[4] *Communication* from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[5] *Accompanying* document to the proposal for a Council decision on creating a Critical Infrastructure Warning Information Network (CIWIN) : commission staff working document / Impact assessment (SEC/2008/2702) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

Установлення критеріїв і визначення показників, за якими певні інфраструктури або їхні елементи можна віднести до КІ, є окремим питанням для вивчення. Пропозиції щодо процедури та критеріїв визначення об'єктів КІ на загальноєвропейському рівні були представлені в Зеленій книзі (2005 р.)[6]. У ній розглядалися 11 секторів КІ, в які було включено 37 підсекторів. Згодом, під час підготовки проекту директиви було внесено ці 11 секторів із 29 підсекторами[7], а вже в ухваленій директиві ЄК[8] згадується тільки два сектори, що складаються з таких восьми підсекторів:

• енергетика (електромережі та об'єкти з генерування та передачі електроенергії; нафтопереробна й нафтовидобувна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали скрапленого газу);

• транспорт (автодорожній; залізничний; авіаційний; річковий флот; океанічний та морський флот і порти).

Елементи всередині КІ, своєю чергою, також можуть бути впорядковані за значимістю. Наприклад, у Швейцарії найвагомішого значення надано двом підсекторам енергетики (постачання газу та електроенергії), банківським установам, інформаційним технологіям і телекомунікаціям, залізничному транспорту й автомобільним шляхам, а також мережі постачання питної води[9].

Визначення категорій об'єктів КІ дає змогу встановити диференційовані вимоги до забезпечення безпеки цих об'єктів з урахуванням, зокрема, ступеня потенційної небезпеки здійснення акту незаконного втручання або теракту і його можливих наслідків.

Функціонування КІ пов'язується з підтриманням життєво важливих функцій у суспільстві, захистом базових потреб і забезпеченням від-

---

[6] *Green* paper on a European programme for critical infrastructure protection (COM/2005/576 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[7] *Proposal* for a Directive of the Council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection (COM/2006/787 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[8] *EU* Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection / Off. J. of the European Union [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[9] *Brem S.* Developing a national CIP strategy: Swiss experiences and results / S. Brem // European CIIP Newsletter. – 2009. – Vol.5, No.2. – P. 13–15; *The Federal* Council's Basic strategy for critical infrastructure protection / Federal Administration [Електронний ресурс]. – Режим доступу: http://www.bevoelkerungsschutz.admin.ch

чуття безпеки й захищеності у населення. Наприклад, у Норвегії цьому питанню було приділено увагу у звіті урядової комісії, яку очолював експрем'єр-міністр Коре Віллок. Серед нових викликів, пов'язаних із безпекою суспільства, були названі, зокрема, технологічні зміни, підвищення економічної ефективності й тиску, зниження повноти державних послуг та аутсорсинг державних послуг для комерційних підприємств[10]. Ці проблеми, разом із появою таких «нових» загроз, як тероризм, організована злочинність і кліматичні зміни, принципово змінили контекст для відомств і спеціалізованих служб, відповідальних за підтримку й захист КІ.

Загрози КІ є різноманітними, а соціально-економічні наслідки їх реалізації складно оцінити через численні каскадні ефекти і взаємопов'язаність різних об'єктів КІ. Яскравим прикладом цього твердження є офіційні оцінки наслідків терактів, скоєних у вересні 2001 р. у США, для авіаційного транспорту в Європі. За оцінками Асоціації європейських авіаліній (*Association of European Airlines*) падіння попиту на пасажирські авіаперевезення становило 15–30 %, що спричинило в останньому кварталі 2001 р. втрати обсягом 3,6 млрд євро та скорочення близько 17 тис. робочих місць (майже 5 % працівників) у європейських авіакомпаніях[11].

Терористичні акти, скоєні в європейських країнах у 2000-х роках, засвідчили, що навіть за наявності розгалуженої системи протидії тероризму на їх території існує значний терористичний ризик. Аналіз офіційного звіту, складеного після теракту в Лондоні (липень 2005 р.), свідчить, що інфраструктурні об'єкти й місця масового скупчення людей є дуже вразливими до терористичних загроз[12].

Інша група загроз (природного характеру), як свідчить статистика міжнародної бази даних з надзвичайних ситуацій[13], характеризується тенденцією до зростання чисельності стихійних метеорологічних явищ і розміру їх наслідків для країн ЄС. Тому дедалі більше уваги приділя-

---

[10] *Protection* of critical infrastructures and critical societal functions in Norway // Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006 [Електронний ресурс]. – Режим доступу: http://www.regjeringen.no/

[11] *The repercussions* of the terrorist attacks in the United States on the air transport industry (COM/2001/574 final) : communication from the Commission to the European Parliament and the Council [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[12] *Report* into the London terrorist attacks on 7 July 2005 / Presented to Parliament by the Prime Minister // Intelligence and Security Committee, 2006.

[13] *EM-DAT :* The OFDA/CRED International Disaster Database / Université Catholique de Louvain, Брюссель, Бельгія [Електронний ресурс]. – Режим доступу: www.emdat.be

ється дослідженням стійкості електроенергетичних мереж, які вважаються найбільш вразливими до кліматичних чинників[14]. Небезпечність останніх, а також стихійних лих викликана одночасним впливом на різні об'єкти й навіть сектори КІ, виникненням аварій через т.зв. відмови із загальної причини, або каскадним впливом таких відмов[15].

Масштабні аварії в електроенергетичних мережах свідчать про щільний взаємозв'язок між різними секторами КІ, різноманітні прояви ефекту каскадних відмов. Наприклад, «затемнення» в Італії, що відбулося у вересні 2003 р., призвело до перебоїв у функціонуванні залізничного транспорту, служб та установ надання медичної допомоги населенню, фінансових електронних сервісів і загалом усіх телекомунікаційних мереж[16]. Проведені дослідження функціонування електроенергетичних мереж також свідчать, що ризики виникають і внаслідок недоліків структурної побудови самої мережі, і вразливостей, що мають її інформаційні та керуючі підсистеми[17].

Беззаперечно, *з-поміж техногенних загроз для КІ особливу небезпеку становлять кіберзагрози*. Кібератак зазнають сервери державних установ, великих компаній, банків, бірж[18]. Найбільш розповсюдженою мережевою кібератакою є *DoS* (*denial of service*) – атака, що спричиняє відмову обслуговування апаратного забезпечення. Така кібератака у грудні 2012 р. спричинила відмову серверів найбільшої в Німеччині компанії з генерування відновлюваної електроенергії[19].

Новітньою тенденцією стали кібератаки на промислові системи автоматизованого управління технологічним процесом. Ще донедавна вважалося, що такі системи не можуть стати ціллю кібератаки, оскіль-

---

[14] *Rubbelke D.* Impacts of climate change on European critical infrastructures: the case of the power sector / D. Rubbelke, S. Vogele // Environmental science and policy. – 2011. – № 14. – P. 53–63.

[15] *Guikema S. D.* Natural disaster risk analysis for critical infrastructure systems: an approach based on statistical learning theory / S. D. Guikema // Reliab. eng-ng and system safety. – 2009. – № 94. – P. 855–860.

[16] *Rosato V.* Modelling interdependent infrastructures using interacting dynamical models / V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni [at al.] // Int. J. of Critical Infrastructures. – 2008. – № 4. – P. 63–79.

[17] *Fridheim H.* En sårbar kraftforsyning : Sluttrapport etter BAS3 / Forsvarets Forskningsinstitutt, Kjeller / H. Fridheim, J. Hagen, S. Henriksen [Крихка влада : заключний звіт для BAS3 / Дослідницький інститут оборони. – Defence Research Establishment, м. Кьеллер], 2001.

[18] *International* CIIP Handbook / edt. A. Wenger, J. Metzger, M. Dunn. – Zurich: Swiss Federal Institute of Technology, 2012. – 218 p.

[19] *European* renewable power grid rocked by cyber-attack [Електронний ресурс]. – Режим доступу: http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-5

ки промислове обладнання (виробничі конвеєри, контролери, датчики й сенсори) зазвичай ізольоване не лише від зовнішніх, а й від локальних інформаційних мереж. Проте у 2010 р. вперше були зареєстровані випадки проникнення шкідливого програмного коду, що змінював параметри режимів контролерів технологічного процесу, збирав і передавав отримані з них дані[20].

Загрози для об'єктів КІ оцінюються за допомогою різноманітних методик і прикладного програмного забезпечення, основою яких є загальна методологія останньої, причому головною особливістю оцінки ризиків для КІ є врахування численних взаємозв'язків і залежностей, про що свідчить звіт Інституту захисту й безпеки громадян (входить до складу Центру спільних досліджень Єврокомісії, розташованого в м. Іспра, Італія)[21].

Варто зазначити, що *в ЄС виділяються значні кошти на проведення науково-дослідних проектів із тематики захисту КІ.* Згадаємо лише кілька з них – найбільш характерних. Відповідно до проекту *MICIE*[22] було розроблено систему оповіщення, яка в режимі реального часу дає змогу визначати рівень можливих загроз для певних секторів та об'єктів КІ небажаними подіями в інших секторах. У проекті *IRRIIS* [23] розроблялися механізми, що підвищують надійність, живучість і стійкість інформаційних систем. Так, було розроблено набір програмних засобів, що дають змогу моделювати і прогнозувати вплив взаємозв'язків між різними елементами КІ[24], високий рівень взаємозалежності між якими продемонстрували також результати проектів *CRUTIAL* і *DOMINO*[25]. Низка наукових проектів розглядали такі пов'язані питання, як захист від терористичних атак (*APENCOT – Analysis of the protection*

---

[20] *Stuxnet* Dossier // Symantec Security Response. – 2011. – February. – 68 p. [Електронний ресурс]. – Режим доступу: http://www.symantec.com/

[21] *Giannopoulos G.* Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art / G. Giannopoulos, R. Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.

[22] *Model* tools for managing interaction between critical infrastructures and related dependability and vulnerabilities (EU FP7 MICIE Project) [Електронний ресурс]. – Режим доступу: http://www.micie.eu

[23] *Integrated* Risk Reduction of Information-based Infrastructure Systems (EU FP6 IRRIIS Project) [Електронний ресурс]. – Режим доступу: http://www.irriis.org

[24] *Usov A. S*imulating interdependent Critical Infrastructures with SimCIP / A. Usov, C. Beyel // European CIIP Newsletter. – 2008. – Vol.4. – No.3 [Електронний ресурс]. – Режим доступу: http://www.irriis.org/

[25] *Verissimo P*. The CRUTIAL architecture for critical information infrastructures / P. Verissimo, N. Neves, M. Correia, Y. Deswarte [at al.] // Architecting Dependable Systems. – 2008. – Vol. 5. – P. 1–27.

of energy networks' crucial objects against terrorism and proposal of security standards), стійкість електроенергетичних мереж (*OCTAVIO – Comprehensive approach definition to improve the security of energy control centers; SEMPOC – Simulation exercise to manage power cut crisis*), вплив систем космічного зв'язку на розвиток економіки країн ЄС і загальноєвропейської безпеки (*SECURESPACE*).

Захист КІ потребує партнерської взаємодії між власниками та операторами КІ, з одного боку, та урядовими структурами країн ЄС – із другого. В офіційному повідомленні ЄК зазначається, що «посилення відповідних заходів безпеки органами державної влади, пов'язаних із хвилею атак, які спрямовані проти суспільства загалом, а не проти окремих діючих гравців промисловості, має бути здійснено за рахунок держави»[26], тобто остання має відігравати головну роль при захисті КІ. Водночас відповідальність за управління ризиком, пов'язаним із промисловими об'єктами, системою постачань, інформаційними технологіями й комунікаційними мережами, мають нести власники та оператори об'єктів КІ. Тому інформаційні попередження, консультативні й дорадчі матеріали мають бути доступними і допомагати громадськості й приватному сектору захищати основні системи інфраструктури.

Водночас забезпечення безпеки та надійності функціонування вимагає значних фінансових витрат, а рішення щодо таких інвестицій приймаються після ретельного економічного аналізу «витрат-вигід». Як свідчать дослідження, компанії, що працюють у телекомунікаційному секторі КІ, приділяють значно більше уваги спроможності технічних систем долати відмови (аварії), що характеризуються високою ймовірністю настання, але низьким рівнем втрат, тоді як аваріям, що характеризуються низькою ймовірністю настання і вкрай високим рівнем наслідків, приділяється менше уваги й ресурсів[27]. Використання такого підходу пояснюється намаганнями компаній створити для себе ринкові переваги (за показником якості послуг) хоча б у середньотерміновій перспективі, залишаючись привабливими для інвесторів.

---

[26] *The repercussions* of the terrorist attacks in the United States on the air transport industry (COM/2001/574 final) : communication from the Commission to the European Parliament and the Council [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[27] *Protection* of critical infrastructures and critical societal functions in Norway : report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006 [Електронний ресурс]. – Режим доступу: http://www.regjeringen.no/

Для України може бути корисним *досвід імплементації концепції захисту КІ в законодавствах деяких східноєвропейських країн*. Наприклад, у нормативно-правовій базі Республіки Польща введено термін «захист критичної інфраструктури», під яким розуміються всі «зусилля, спрямовані на забезпечення функціональності, неперервності й цілісності критично важливих об'єктів інфраструктури з метою запобігання загрозам, ризикам і вразливості та обмеження, а також нейтралізації їх наслідків і швидкого оновлення інфраструктури у випадку відмов, атак та інших випадків, що порушують її належне функціонування»[28].

Подібна ситуація спостерігається в нормативно-правовій базі Словацької Республіки, де у 2007 р. уряд ухвалив Концепцію критичної інфраструктури у Словацькій Республіці, її захисту та оборони[29], а на її основі у 2008 р. розроблено Національну програму захисту та оборони критичної інфраструктури[30]. Ці документи визначають загальні (концептуальні) характеристики стратегії захисту КІ, але не надають детального опису заходів з її здійснення.

У законодавстві Республіки Болгарія термін «критична інфраструктура» визначено в Законі «Про захист від стихійних лих» (жовтень 2011 р.): критична інфраструктура є системою або її частиною, необхідною для підтримки життєво важливих соціальних функцій, здоров'я, безпеки, економічного чи соціального добробуту населення, а її руйнування або знищення матиме суттєвий негативний вплив і спричинить для Болгарії нездатність підтримувати такі функції. Прийнято також Постанову Ради Міністрів «Про порядок, спосіб і компетентні органи для визначення критичної інфраструктури та об'єктів і оцінки ризиків» (жовтень 2012 р.)[31], також діють нормативні документи, що регламентують порядок взаємодії

---

[28] *Act* of 26 April 2007 on Crisis Management / пер. англ. мовою // Урядовий центр з питань безпеки Республіки Польща [Електронний ресурс]. – Режим доступу: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf

[29] *Koncepcia* kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany // Міністерство внутрішніх справ Республіки Словаччина [Електронний ресурс]. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691

[30] *Národný* program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike // Міністерство внутрішніх справ Республіки Словаччина [Електронний ресурс]. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10692

[31] *Наредба* за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях // Българският правен портал [Електронний ресурс]. – Режим доступу: http://www.lex.bg/bg/mobile/ldoc/2135816878http://www.lex.bg/bg/mobile/ldoc/2135816878http://www.lex.bg/bg/mobile/ldoc/2135816878

між окремими відомствами щодо питань захисту КІ (див. інструкцію[32]). Відповідно до положень Директиви ЄК №114 2008 р. Рада Міністрів Республіки Болгарія прийняла постанову, в якій визначається порядок визначення об'єктів КІ у двох секторах (енергетика і транспорт), а також заходів з їх захисту[33].

Отже, можна стверджувати, що нині концепція захисту КІ імплементована і в загальноєвропейському законодавстві, і в національних законодавствах окремих країн-членів ЄС. На рівні Євросоюзу сформовано загальну концепцію вирішення завдань захисту КІ, тоді як на рівні країн ЄС мають бути розроблені й реалізовані національні плани захисту КІ. Загальноєвропейською КІ вважається та, що має транскордонне (в межах ЄС) значення; проте відчувається тенденція до посилення ролі загальноєвропейських структур ЄС щодо забезпечення захищеності КІ, визначення необхідних заходів, забезпечення взаємодії та обміну інформацією у спільній системі раннього реагування.

Україна за своїм географічним положенням є частиною енергетичного і транспортного пан'європейського простору, а отже, де-факто пов'язана з європейською КІ, що відкриває можливості для діалогу з питань безпеки КІ між уповноваженими органами влади України та її європейських сусідів.

CONCEPTION OF CRITICAL INFRASTRUCTURE PROTECTION: LESSONS LEARNING AND CONCLUSIONS FOR UKRAINE

Dmytro BIRIUKOV,
Senior consultant National Institute for Strategic Studies, Ukraine

Nowadays a high level of implementation of modern technologies is an indicator of development level of the state, the factor which determines the possibilities of economic competitiveness and, therefore, a prerequisite for achieving the goals determined by national interests. Simultaneously, along

---

[32] *За взаимодействие* между министерството на отбраната и министерството на вътрешните работи : инструкция от 18.06.2011 г. № М-3 / Министерството на отбраната и Министерството на вътрешните работи (обн. ДВ. бр.60 от 5.08.2011 г.) // Българският правен портал [Електронний ресурс]. – Режим доступу: http://www.lex.bg/bg/laws/ldoc/2135744408

[33] *За установяването* и означаването на европейски критични инфраструктури в Република България и мерки за тяхната защита : постановление от 1.02.2011 г. № 18 // Българският правен портал [Електронний ресурс]. – Режим доступу: http://www.lex.bg/bg/laws/ldoc/2135716127

with the many benefits of technological progress technologies have created unprecedented conditions depending on both the individual and society from systems that provide information, communication, transport, energy, financial and other services. With the destruction of such systems currently connect most dangerous security scenario for the world's leading countries, including EU and NATO Member States. Therefore, given the limited resources, the objective impossibility to provide absolute protection and safety of all infrastructure systems in many countries is implemented the concept of critical infrastructure (CI), which allows to focus on the systems, networks and certain facilities, destruction or disruption of which could lead to the most serious negative consequences for the national security.

Since the middle of 1990s, the term «critical infrastructure» was introduced in the legislative documents and the practice of international communication on a diplomatic level, as well as in academic and business discursions. Meaning of this term differs slightly across countries, but these differences are not so significant. Specifically, pursuant to the current US legislation, critical infrastructure means «systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters» (sec.1016.e)[34].

The establishment of the legal framework for critical infrastructure protection (CIP) is a long process. Perhaps the greatest success in this area has been reached in the US. Also, European experience on CIP concept implementation is very interesting, especially for Ukraine, which expresses their euro-integration intentions. Thus, we will consider US and EU efforts made in this area (fig.1). In the late 1990s, the concept of CI mainly associated with the information and telecommunications infrastructure. Perhaps the first attempt to estimate potential losses on the state level in case of CI failure was made in the report of the US President's Commission on Critical Infrastructure Protection[35], which was established in July, 1996[36]. In its' report Commission emphasized on possible influence on CI from the side of cyber-attacks.

---

[34] *Uniting* and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT, 2001) [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[35] *Economic* Impacts of Infrastructure Failures : report to the President's Commission on Critical Infrastructure Protection, 1997 [Електронний ресурс]. – Режим доступу: http://www.ciao.gov/resource/pccip/EconomicImpacts.pdf

[36] *Critical* Infrastructure Protection : executive Order 13010 of July 15, 1996 [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/FR-199/pdf/96-51.pdf

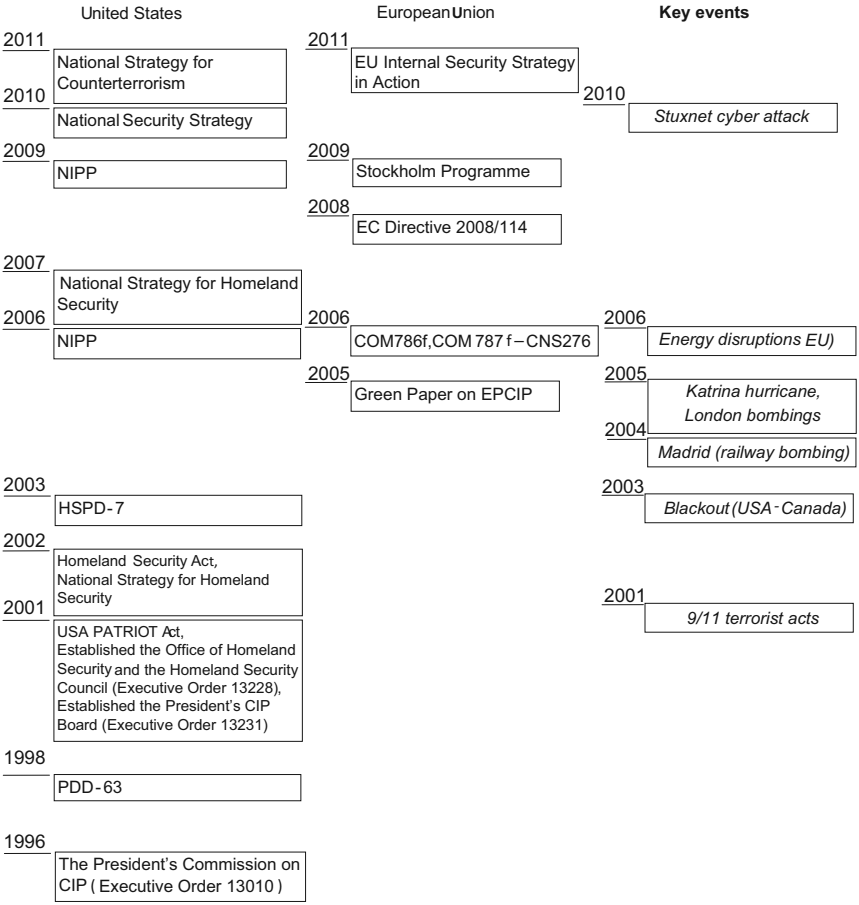


Fig.1. Main legislative acts of US and EU in the field of CIP and key events, which accelerated CIP concept evolution

In May, 1998, the ensuring of CI security was recognized as a component of US security policy. It was noticed in PDD-63[37]: «US will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and

[37] *Presidential* Decision Directive/NSC-63 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

cyber-attacks on our CI, including especially our cyber systems». Therefore national program on CIP was initiated. Continuation of work on strengthening the protection of critical information infrastructure was reflected in administration's National Plan for Information Systems Protection (2000)[38].

But the turning point in establishing the concept of CIP has become the need to respond to acts of terrorism committed in New York on September 11, 2001. After this extraordinary horrible event the US government fundamentally revised approaches to the homeland security protection (legislative, organizational and technological aspects). An important conclusion was made after this tragedy, and that was reflected in US PATRIOT ACT (known by this abbreviation title). In this document the term CI was formulated in its current form.

After 9/11 the US pays serious attention to CIP efforts, and CIP concept is reflected in the recent documents from the field of national security: Executive Order 13228 – Establishing the Office of Homeland Security and the Homeland Security Council (October, 2001)[39]; Executive Order 13231 – Critical Infrastructure Protection in the Information Age (October, 2001)[40]; National Security Strategy (July, 2002); National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February, 2003)[41]; The National Strategy to Secure Cyberspace (February, 2003)[42]; Homeland Security Presidential Directive 7 (December, 2003); National Infrastructure Protection Plan (October, 2006); National Strategy for Homeland Security (October, 2007)[43]; National Infrastructure Protection Plan (October, 2009)[44]; Cyberspace policy review (2009); National Security Strategy (March, 2010)[45].

---

[38] [Електронний ресурс]. – Режим доступу: https://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

[39] *Establishing* the Office of Homeland Security and the Homeland Security Council : executive Order 13228. – 2001. – October 8 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/offdocs/eo/eo-13228.htm

[40] *Critical* Infrastructure Protection in the Information Age : executive Order 13231. – 2001. – October 16 [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/WCPD-2001-10-22/pdf/WCPD-2001-10-22-Pg1485.pdf

[41] *National* Strategy for the Physical Protection of Critical Infrastructures and Key Assets [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[42] *The National* Strategy to Secure Cyberspace [Електронний ресурс]. – Режим доступу: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[43] *National* Strategy for Homeland Security [Електронний ресурс]. – Режим доступу: [http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[44] *Partnering* to enhance protection and resiliency : National Infrastructure Protection Plan. – US Dep. Homeland Security, 2009. – 188 p.

[45] *National* Security Strategy [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

In 2002 Department of Homeland Security (DHS) was established[46]. DHS combined 22 different federal departments and agencies, and it was a major restructuring of US government's military and intelligence agencies since the late 1950s.

Homeland Security Presidential Directive 7[47] defines the responsibilities of the DHS, other ministries and federal agencies that are responsible for specific sectors of CI. DHS has the responsibility to form National Infrastructure Protection Plan (NIPP). Two NIPPs were developed by DHS (in 2006 and 2009), and one may conclude that changes and improvements had been affected overall approach to risk management and security assessments within CI sectors.

The significant amount of funding assigned for CIP in US confirms its' recognized importance for national security. For instance, CIP spends a significant portion of the funds assigned in the Federal Budget for homeland security (it was about 67.9 billion USD in 2012 and 68,9 billion USD was planned for 2013 fiscal year). In 2012 the allocation of budgetary funds for these purposes was held as follows: DHS – 52 % , MoD – 26 % and other 29 entities – 22 %.

Unlike the US, where a single executive authority was created to be responsible for CIP, in EU there is no such body, and appropriate authorities of certain Member States perform CIP within their national borders.

In the EU, realizing the high level of threats and importance of the CIP measures, the process of creating the legal and institutional arrangements in this area was also initiated. As a start point of the focused work can be considered an appeal of European Council to the European Commission (EC) formulated in June 2004 with instructions for the preparation of comprehensive strategy for CIP. Soon in October 2004, in response, the EC published the Communication[48], which contain an overview of actions that the EC carried out in this area, as well as proposals for additional measures to improve the European system of prevention, preparedness and response to terrorist attacks against CI. In this Communication EC underlined that there is a number of

---

[46] *Homeland* Security Act [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

[47] *Critical* Infrastructure Identification, Prioritization, and Protection : homeland Security Presidential Directive 7. – 2003. – December [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/homeland-security-presidential-directive-7

[48] *Critical* infrastructure protection in the fight against terrorism : communication from the Commission to the Council and the European Parliament. – 2004. – 20 October (COM/2004/702 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

facilities which could potentially be attributed to the European CI, but, following the principle of subsidiarity, the European institutions need to focus on protecting only those facilities which disruption will have a transboundary impact, and the other facilities should be left on responsibility of Member States. However, as noted in this Communication, it should be a common approach on CIP in all Member States.

To ensure implementation and realization of a common approach, EC adopted in 2005 a Green Paper on European Programme for Critical Infrastructure Protection (EPCIP)[49]. In December 2006, the Commission presented a proposal for a directive on the identification and designation of European critical infrastructures and a common approach to assess the need to improve their protection[50]. On the same day, EC also adopted Communication[51], which declares the approach of how the EC proposes to address the issue of CIP in the EU. In this Communication EC recommended for all Member States to take measures specified in EPCIP, particularly, establishing the conditions in their national legislation.

A separate issue for consideration is an establishing criteria and indicators on which certain infrastructure or their components can be attributed to the CI. Proposals for the procedures and criteria for defining list of European CI have been presented in the Green Paper (2005). There were considered 11 sectors of CI, which included 37 sub-sectors. But later, in the proposals for the directive the number of subsectors was reduced to 29, and, finally, in the Directive adopted by EC[52], only two sectors (energy and transport) were mentioned. Within these two sectors eight sub-sectors were specified: electricity (infrastructures and facilities for generation and transmission of electricity in respect of supply electricity), oil (oil production, refining, treatment, storage and transmission by pipelines), gas (gas production, refining, treatment, storage and transmis-

[49] *Green* paper on a European programme for critical infrastructure protection (COM/2005/576 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[50] *Proposal* for a Directive of the Council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection (COM/2006/787 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[51] *Communication* from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[52] *EU* Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection Off. J. of the European Union [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

sion by pipelines LNG terminals), road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping and ports.

Besides, the components of CI within certain sectors can be ordered by its' importance. For instance, in Switzerland the highest value given to the two sub-sectors of energy (gas and electricity), banks, information technology and telecommunications, railways and roads, and drinking water supply network[53].

Operation of CI tightly associated with maintaining of vital functions in society, protection of basic needs and providing a feeling of safety and security of the population. In the Working Document of EC Staff[54] was mentioned that: «by ensuring a high degree of protection of EU infrastructures and increasing their resilience (against all threats and hazards), we can minimize the consequences of loss of services to society as a whole». These objectives are correlated with objectives defined in the Stockholm Programme[55] and in the EU Internal Security Strategy[56].

In Norway, this issue was raised in the report of the government commission, headed by Kåre Willoch (former Prime Minister). Among the new challenges related to the safety of society, were specifically identified technological change, increased production efficiency and the pressure of economic competition, reduced public services and outsourcing of public services for business[57]. These problems, along with the appearance of «soft» threats such as terrorism, organized crime and climate change fundamentally changed the context for the specialized agencies and services responsible for maintaining and protecting CI.

Norwegian Defence Research Establishment (http://www.ffi.no) and Norwegian Directorate for Civil Protection (http://www.dsb.no) published a series

---

[53] *Brem S.* Developing a national CIP strategy: Swiss experiences and results / S. Brem // European CIIP Newsletter. – 2009. – Vol.5. – No.2. – P. 13–15.

[54] *SWD* (2013) 318 final: On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure : EC staff working document [Електронний ресурс]. – Режим доступу http://ec.europa.eu/

[55] *The Stockholm* Programme: An Open and Secure Europe Serving and Protecting the Citizens : council Document 17024/09 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:en:HTML

[56] *COM* (2010) 673 final: The EU Internal Security Strategy in Action: Five steps toward a more secure Europe : communication from the Commission to the European Parliament and the Council [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

[57] *Protection* of critical infrastructures and critical societal functions in Norway // Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006 [Електронний ресурс]. – Режим доступу: http://www.regjeringen.no/

of reports (started in 1997) dedicated to «protection of society» subject, whose purpose was to examine how modern society will react, and how it should protect itself under modern warfare conditions. Herewith, the reports identify the key life-support systems that are necessary for modern society live, and examine the interdependence between them. In preparing these reports, expert assessments were used, which allowed to show in simple table-like form the interdependence among life-support systems[58]. Also, it should be noted, that the Scandinavian experts examined the particular long-term impact of «failure» of certain CI system (transport network) to other systems[59].

Examining the experience we can conclude, that the basis for ensuring CIP associated with establishment of following key issues:

• improving coordination and interaction among authorities responsible on separate certain issues or certain sectors of CI;

• fostering of public-private partnership in the field of security;

• using risk-analysis-based «all-hazard» approach for emergency management.

The all hazards approach concerns arrangements for managing the large range of possible effects of risks and emergencies. This concept is useful to the extent that a large range of risks can cause similar problems and such measures as warning, evacuation, medical services and community recovery will be required during and following emergencies. For instance, in US HSPD-8 were noticed that «the term 'all – hazards preparedness' refers to preparedness for domestic terrorism attacks, major disasters, and other emergencies»[60].

It should be warned from delusion. «All-hazards does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation. What it does mean is that there are things that commonly occur in many kinds of disasters, such as the need for emergency warning or mass evacuation, that can be addressed in a general plan and that that plan can provide the basis for responding to unexpected events»[61].

---

[58] *Beskyttelse* av samfunnet: Sluttrapport : заключний звіт «Захист суспільства» / Дослідницький інститут оборони (Норвегія) [Електронний ресурс]. – Режим доступу: http://rapporter.ffi.no/rapporter/97/01459.pdf

[59] *Beskyttelse* av samfunnet med fokus på transportsektoren : звіт 2003/929 «Захист суспільства: в фокусі транспортна мережа» / Дослідницький інститут оборони (Норвегія) [Електронний ресурс]. – Режим доступу: http://www.ffi.no/no/Rapporter/03-00929.pdf

[60] *United* States Homeland Security Presidential Directive 8 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/offdocs/nspd/hspd-8.html

[61] *Waugh W.* Terrorism and the All-Hazards Model 2004 / W. Waugh [Електронний ресурс]. – Режим доступу: http://training.fema.gov/EMIWeb/downloads/Waugh%20-%20Terrorism%20and%20Planning.doc

In its communication on the EU Internal Security Strategy[62] EC calls for uniform risk analyses based on standardized criteria to establish a Common Risk Management Framework, also including risk information and risk-based controls. Based on the Security Strategy and the Communications on the Prevention of Natural and Man-made Disasters[63], the EC developed Risk Assessment und Mapping Guidelines for Disaster Management[64]. These guidelines are aimed to support Member States in their efforts and contributions to a European Risk Atlas and to serve as a further basis for an coherent all-hazard risk policy.

Solving practical problems of CIP requires for accountability of all involved actors (state, owners, society). In the US private sector consists about 85 % of CI. In many European countries such infrastructures as water, energy, and railway transportation have previously often solely been taken care of by the governments. But it was underlined that, while government authorizes responsible for CI resilience, they «lack the technical expertise and the means to monitor or control CI operations»[65].

CIP Concept in Security Studies. Within security studies, how we can see, the CIP isn't conceptualized yet. Indirectly, this thesis confirms the content of scientific papers on CIP, published in most cited journals (IJCIP by Elsevier and IJCIS by Inderscience) and the most cited books[66] and collections of conferences and working groups (like IFIP Working Group 11.10 on CIP)[67].

---

[62] *Communication* from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe / European Commission (2010): COM(2010) 673 final [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

[63] *Communication* from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Community approach on the prevention of natural and man-made disasters. {SEC(2009)202} {SEC(2009)203} / Commission of the European Communities (2009): COM(2009)82 final [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0082:FIN:EN:PDF

[64] *Commission* Staff Working Paper. Risk Assessment and Mapping Guidelines for Disaster Management / European Commission (2010): SEC(2010) 1626 final [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/prevention/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

[65] *De Bruijne M.* Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment / M. De Bruijne, M. Van Eeten // J. of Contingencies and Crisis Management. – 2007. – 15(1). – P. 18–29.

[66] *Lewis T. G.* Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation / T. G. Lewis. – Wiley, 2006. – 486 p.

[67] *Critical* Infrastructure Protection VII / eds. J. Butts; S. Shenoi // 7th IFIP WG 11.10 Int. Conf. (ICCIP 2013) Proceedings, Washington, DC, USA. – 2013. – March 18–20. – 227 p.

For instance, we analyzed 314 paper published in IJCIP and IJCIS during period of 2005–2013 and found following. The main body of these publications (65,5 %) discusses an applied issues of cyber security and physical protection against terrorist attacks or methodological issues of risk assessment, interconnection modeling and vulnerability assessment (fig.2).

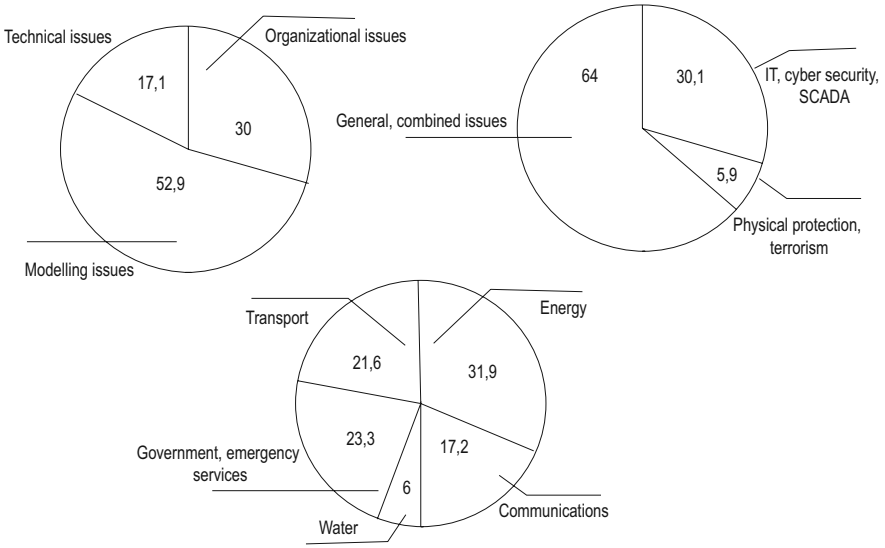


Fig. 2. Distribution of topics of publications from IJCIP and IJCIS

If we refer to CIP as a concept within contemporary security studies, first of all, we should keep in mind that over the past twenty years the focus of security research has shifted, and this shift took place simultaneously in several planes. As it was noted by *Emma Rothschild*[68], that a concept of national security was «extended» in the following four forms: from the security of nations to the security of groups and individuals; from the security of nations to the international security; from pure military to another forms (economic, energy, environmental, or «human» security); the political responsibility of ensuring security was shared among new security ac-

[68] *Rothschild E.* What is Security? / E. Rothschild // Daedalus. – 1995. – 124(3). – P. 53–98.

tors (international institutions, regional or local governments, NGOs and public society).

We have to emphasize, that Ukrainian legislations in the field of national security developed in 1990s–2000s reflects this changes. We propose to use schematic (logical-graphical) analysis of definitions (fig. 3). In the scheme we use following components: key terms (definitions) are contained in rectangles; logical connections (and, or) in circles; connections, which describes action, in hexagons; lists of features (or categories) are contained in angled parallelepipeds; and links of «supplement» are drawn by arrows with appropriate pronoun specified above arrow.

Such a construction (triad: «national security», «national interests» and «national security threats») is hard or even impossible in practice to be operationalized. Despite, *CI gives mechanism to operationalize* relations among security, interests and threats.

Based on the definition of «national interest», which is given in the Law of Ukraine «On the Basics of National Security»[69], it can be argued that the CI includes the physical or virtual (information stored in registers, databases, information systems or transmitted through the government system of confidential communication) facilities and systems which stable operation determines the possibility of achieving national interests.

Relations between political and economic power should be also in the focus of investigation within CIP concept. The problem of conflict of the interests of private owners, state and society in the field of CIP is relevant not only for Ukraine, but also for the developed states. This opinion is confirmed by recent large scale accident (Deepwater Horizon oil spill, Fukushima Daiichi nuclear disaster). Whether we can be protected from such a «normal accident» (this term introduced by *Charles Perrow*[70]), that are caused by technological system complexity?

In Ukraine the privatization of many companies that can be classified as CI and establishment of new companies, which from the beginning were in private ownership (e.g companies in telecommunications, information technology, banking and financial services) brings new challenges to the list of CIP tasks. Among them we should highlight following:

---

[69] *Про основи* національної безпеки : закон України від 19.06.2003 р. № 964-IV // ВВР. – 2003. – № 39. – Ст. 351 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15

[70] *Perrow C.* Normal Accidents: Living with High Risk Technologies / C. Perrow. – 1999. – 386 p.

• sharing the responsibility among the government authorities (regulators), owners of facilities (operators) and society (customers);

• distribution of responsibility for the consequences, compliance mechanisms for mitigation of social responsibility;

• interaction authorities (inspections) to CI owners;

• standardization, regulations, inspections and insurance.

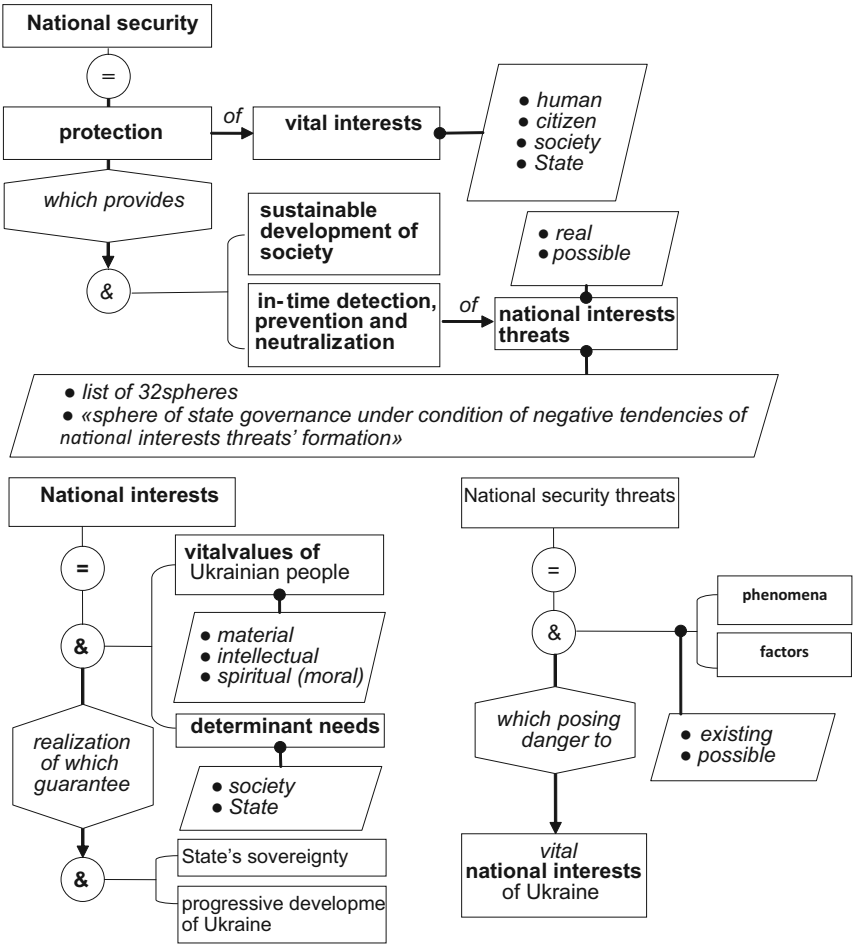


Fig. 3. Investigation of the key definitions: «national security», «national interests» and «national security threats»

Another issue, which should be studied within CIP concept, is *securitization of various threats against CI facilities*. A sporadic research of *Claudia Aradau* (The Open University, Milton Keynes, UK) examines this issue[71].

CI surrogates in Ukrainian legislation. It should be noticed that de facto in Ukraine there are all sectors and elements, which are attributed to CI. These include complex large-scale industrial complexes such as NPP, HPP and dams, chemical industry plants, banking payment systems, transportation networks, oil and gas pipelines, communication networks and so on, and, naturally, government institutions, law enforcement authorities, emergency services, and monuments of cultural heritage included in UNESCO list of world cultural heritage sites.

Several legislative and regulatory acts in Ukrainian legislation establish the special nature of the functioning for certain categories of facilities and systems that usually referred to CI. However, the term «critical infrastructure» or its straight analog (like Objects of critical importance, which used in Russia) is excluded in Ukrainian legislation.

Despite lack of definition of CI in Ukrainian legislation base several official documents produced by Ukrainian authorities (President and Parliament) include this term. The first reference on CI (within the context of information security) was made in 2006 in the text of the Recommendations of the Parliament Hearings on the development of the information society[72]. Unfortunately, further work on implementing of these recommendations in the field of CIP had been stalled.

The National Security Strategy[73] adopted in 2012 contains in the fourth chapter (Strategic aims and main tasks of national security) two references on CI. Among the ways of enhancing energy security an «effective protection of critical infrastructure of fuel and energy complex against ecological and man-made impacts and malicious acts»(item 4.3.4) were specified; and among the ways of ensuring information security «providing security of information and telecommunication systems that operate in the interest of governance, defense

---

[71] *Aradau C.* Security That Matters: Critical Infrastructure and Objects of Protection / C. Aradau // Security Dialogue. – 2010. – 41(5). – P. 491–514.

[72] *Про Рекомендації* парламентських слухань з питань розвитку інформаційного суспільства в Україні : постанова Верховної Ради України // ВВР. – 2006. – № 15. – Ст. 131.

[73] *Про рішення* Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України» : указ Президента України від 8.06.2012 р. № 389/2012 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/389/2012

and national security, banking and other sectors of the economy, control systems of critical infrastructure facilities» (item 4.3.8) were specified. However, the term «CI» was not defined in Ukrainian legislation.

An assessment of importance of certain facilities for national security of Ukraine was carried out in the perspective of certain kinds of threats. For instance, pursuant to the Resolution of the National Security and Defense Council (was put into effect by Presidential Decree from 10.12.2010, No.1119/2010), the Cabinet of Ministers of Ukraine (CMU) was assigned to «develop with assistance of Security Service of Ukraine and approve a list of facilities that are essential to national security and defense of Ukraine and require to be primary protected against cyber-attacks» (item 4.b, paragraph 3)[74].

On today there are two Unified State Systems, which work in parallel:

• unified state system for prevention, response and suppression of terrorist attacks and minimizing their consequences (its' Regulation approved by the Decree of CMU No1051 on 15.08.2007);

• unified state system of civil protection of the population and territories (regulates by the Code of Civil Protection).

These systems were established particularly to protect facilities which are of vital importance for the state against certain threats. This shows the common situation in security sphere that can be defined as dominance of institutional approaches for solving security problems of national scale.

The national legislation of Ukraine has a number of specific definitions (categories of objects) that define the special status of objects and systems regards to protection of national interests and, as a result, to provide sustainable development of the state. These categories, referring to the experience of European countries, more or less correspond to definition of CI. These categories are:

a) enterprises that are of strategic importance to the economy and national security[75];

b) objects that have to be obligatory protected on the basis of contracts by the State Guard Service[76];

---

[74] *Про виклики* та загрози національній безпеці України у 2011 році : рішення Ради національної безпеки і оборони України від 17.11.2010 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua

[75] *Про затвердження* переліку підприємств, які мають стратегічне значення для економіки та безпеки держави : постанова Кабінету Міністрів України від 23.12.04 № 1734 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1BF

[76] *Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами) : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

c) facilities that are included in the State register of potentially dangerous objects[77] and Objects of high danger[78] (including The list of especially hazardous enterprises, the termination of which requires special measures to prevent injury to life and health of citizens, property, constructions and environment[79]);

d) objects of state's importance[80];

e) objects that have to be protected and defensed during emergency situations and the special period[81];

f) objects that belong to categories of civil protection[82];

g) oil and gas industry facilities of highest importance[83];

h) energy facilities of highest importance[84];

i) immovable objects of cultural heritage.

In 2012 we investigated these categories in analytical report[85] and we present some results below (fig. 4, fig. 5).

Decree of CMU (23.12.04 No1734) approved the list of enterprises that are of strategic importance to the economy and national security. This cate-

---

[77] *Про затвердження* Положення про Державний реєстр потенційно небезпечних об'єктів : постанова Кабінету Міністрів України від 29.08.2002 р. № 1288 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1288-2002-%D0%BF

[78] *Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2245-14

[79] *Перелік* особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу / затв. Постановою Кабінету Міністрів України від 6.05.2000 р. № 765 [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?code=765-2000-%EF

[80] *Постанова* Кабінету Міністрів України від 15.08.2007 р. № 1051 (дск).

[81] *Щодо затвердження* Переліку об'єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період : постанова Кабінету Міністрів України від 24.04.99 р. № 675-019.

[82] *Постанова* Кабінету Міністрів України від 2.03.2010 р. № 227 (дск).

[83] *Про затвердження* переліку особливо важливих об'єктів нафтогазової галузі : розпорядження Кабінету Міністрів України від 27.05.2009 р. № 578-р [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/578-2009-%D1%80

[84] *Про електроенергетику :* закон України від 16.10.1997 р. № 575/97-ВР [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/575/97-%D0%B2%D1%80; *Про затвердження* переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 р. № 1170 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1170-2003-%D0%BF

[85] *Бірюков Д. С.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні : аналіт. доп. / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 102 с.

gory includes large industrial facilities, research institutions, design bureaus, scientific and production associations. This list was regularly updated by the ministries and other central executive authorities and submitted annually in order to take a decision by the CMU on amendments. The main purpose of this Decree is obviously a limitation on privatization of enterprises and research institutions.

	Enterprises that are of strategic importance to the economy and national security	Objects that have to be obligatory protected on the basis of contracts by the State Guard Service	Facilities that are included in the State register of potentially dangerous objects and Objects of high danger	Objects that have to be protected and defensed during emergency situations and the special period	Objects that belong to categories of civil protection	Oil and gas industry facilities of highest importance / Energy facilities of highest importance
Primary criterion	Economic and social value, significance for defense industry	composed from categories a,c,g,h (on previous page)	Presence of hazardous materials, explosives, etc.	Preparation of territories for emergencies and defense	Preparation of territories for defense	Control points, large capacities of fuel storage
Primary risks	Lost of control over the strategic enterprise (technologies)	Intrusion, sabotage, heist,hijacking	Depreciation of production assets, equipment failures	Inoperability	Inoperability	Intrusion, sabotage, terrorist attack
Primary protection measures	Restrictions on rivatization	Physical protection	Technological safety inspections	Inspections	Inspections	Physical protection, technological safety inspections

Fig. 4. Main categories, primary criteria and protection measures

The similar problem was raised in new edition of the Military Doctrine of Ukraine which among directions of the military-industrial policy refers to the need to «remain in state ownership the enterprises of strategic importance for the defense»[86], (Article 28).

[86] *Про рішення* Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Воєнної доктрини України» : указ Президента України від 8.06.2012 р. № 390/2012 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/390/2012

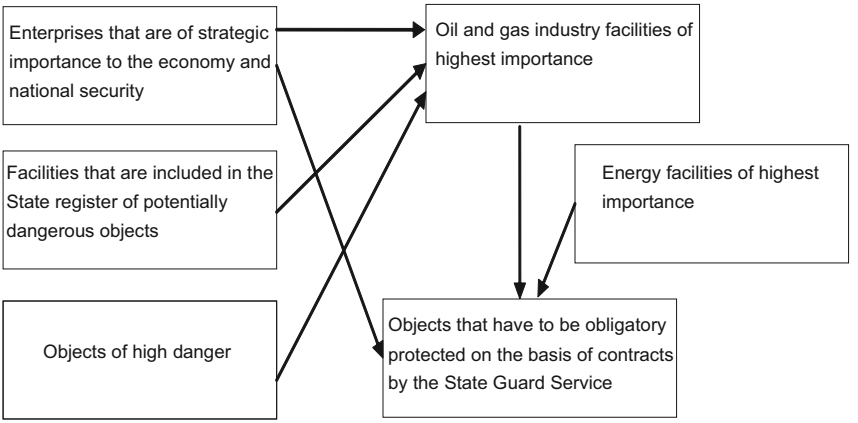


Fig. 5. Relations among main categories

Despite of purely economic orientation of the mentioned above category, this list is used as a baseline to determine the increasing requirements for the physical protection of certain objects. A number of such objects protected by the State Guard Service (SGS), pursuant to Decree of CMU «On measures to improve the protection of objects of state and other forms of property» (10.08.1993 No615)[87]. This decree approved the list of objects that have to be obligatory protected on the basis of contracts by the SGS. There are:

• buildings occupied by authorities (except central executive authorities, which control military forces, State Tax Service and State Customs Service);

• public television, broadcasting and sound recording centers;

• public registers, museums and art galleries, historic and cultural reserves, and other important cultural facilities, which contains historical and cultural values of national significance;

• Ukrainian Stock Exchange and its affiliates, state enterprises of jewelry industry, precious metals warehouses, enterprises that produce state's securities;

[87] *Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами) : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615-93-%EF

• enterprises that produce firearms for sport, hunting weapons, special tools and explosives;

• large warehouses and trading centers;

• mobilization reserve, central and regional pharmaceutical warehouses;

• water supply facilities and reservoirs for drinking water;

• sea ports;

• railway and highway bridges of high importance;

• oil and gas storages of highest importance;

• pipeline, which transports ammonia;

• storage facilities for hazardous substances, radioactive waste, objects located in the zone of alienation and resettlement;

• National exhibition center, National Vernadskii Library, National «Olimpic» Sport Complex, clinical hospital «Pheophania»;

• Ukrainian and regional centers of education quality evaluation.

Besides the SGS, that operates in the structure of the Ministry of Internal Affairs of Ukraine (MIA), other bodies deal with the protection of important objects that belong to their area of responsibility. For instance, Ministry of Transport of Ukraine[88] in 2004 established special guard units to implement and improve the physical protection of shipping locks on the Dnieper River[89]. Similar decision was made by Ministry of Energy and Coal Industry of Ukraine (MEC) in 2007, which established militarized guard units[90]. These activities were made in accordance with the Decree of CMU «On approval of the list of objects that have to be protected and defensed during emergency situations and the special period» (24.04.1999 No.675-019).

Pursuant to Order of CMU (27.05.2009 No.578-r) MEC with MIA and State Service for Emergency Situations of Ukraine (SSES) should ensure physical protection, compliance with technological regulations and fire safety on the oil and gas industry facilities of highest importance. These security and safety measures should be financed by owners of the facilities.

We should emphasize on several trial cases regarding to legality of contracts for physical protection of facilities which SGS tried to provide for cer-

---

[88] Notice: it was reorganized to Ministry of Infrastructure of Ukraine in 2011.

[89] *Про затвердження* Положення про загін відомчої охорони судноплавних шлюзів та Запорізького району гідротехнічних споруд : наказ Міністерства транспорту України від 16.02.2004 р. № 89 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0268-04

[90] *Про організацію* діяльності відомчої воєнізованої охорони Міністерства палива та енергетики України : наказ Мінпаливенерго України від 8.10.2007 р. № 480 [Електронний ресурс].– Режим доступу: http://zakon1.rada.gov.ua/laws/show/z1262-07

tain companies. In these cases companies refuse SGS protection, arguing that protection is already ensured by their own guard units and it is unable to determine the list of objects that have to be protected due to the gap in legislation[91]. Particularly, the trial case «SGS vs. State Enterprise «Prydniprovska Railway»« shows following. Despite the fact that the *List of objects that have to be obligatory protected on the basis of contracts by the SGS* contains reference on railway and highway bridges of high importance, the titles and location of these objects are not specified.

Under the conditions of emergency and special period, pursuant to Decree of CMU (13.12.2000 No.1833-034), a number of railway bridges are subject to mandatory protection. However, under peacetime conditions these bridges are not classified as bridges of high importance. Generally, the category of bridges is determined only by their capacity and length (e.g., large bridge exceeding 100 m, and small bridge is up to 25 m)[92], but the criteria on which we could define the bridges of high importance are nowhere established.

Thus, the lack of regulations that define particularly importance of infrastructure facilities, including railways, under peacetime conditions causes a situation when the importance of the objects are determined by authorities, which responsible for these objects' stable functioning. This does not considered of national or regional significance of the object.

One of the key categories of objects specified in national legislation and could be used in determining the critical facilities and infrastructure in Ukraine is potentially dangerous objects. The procedure of the identification of these objects was established in appropriate methodology[93].

A stage of this procedure is to identify the sources of threats under certain conditions (man-made accidents, violations of the operational regime, natural hazards, etc.) which may cause an emergency, and assessment of possible consequences (number of victims, property damage, etc.) of an emergency for each of the threats.

---

[91] *Постанова* Вищого господарського суду України. Справа № 5005/2220/2011. – 6.10.2011 р. // Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/18544529; *Рішення* Господарського суду Донецької області. Справа № 43/271пд. – 4.03.2010 // Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/8236600

[92] Згідно з Інструкцією по утриманню штучних споруд, затвердженою Наказом Укрзалізниці від 27.04.1999 р. № 124-Ц.

[93] *Про затвердження* Методики ідентифікації потенційно небезпечних об'єктів : наказ МНС України від 23.02.2006 р. № 98 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0286-06

While establishing the level of possible emergencies we should assess:

- spatial distribution of possible emergencies;
- expected number of injuries and death tolls;
- expected economic loses.

Therefore, the main characteristic of which is taken into account in the determination of objects classified as «potentially dangerous objects» is the scale of the possible consequences of the accident at the facility. So this category corresponds to generally accepted definition of the CI in the context of possible negative consequences.

The need of systematization and categorization of objects in certain industries in order to identify those objects, on which requirements for physical protection should be enhanced, is reflected in several regulations. In particular, the Order of CMU (27.05.2009 No.578-r) contains a *List of oil and gas industry facilities of highest importance*[94]. This category contains following facilities of oil and gas industry:

- facility which belongs to enterprise of strategic importance to the economy and national security (which defined in the Decree of CMU 23.12.2004 No.1734);
- facility of enterprise that are object of state's importance (according to the Decree of CMU 24.04.1999 No.675-019);
- facility which are included in the State register of potentially dangerous objects and require continuous maintenance of reliability, operational safety and protection by specialized guarded units.

This list includes: oil-trunk pipelines, the main pipeline outlets, oil pumping stations, production line control station, terminals, marine oil terminals, oil and gas stations with reservoir parks and loading dock, gas lift compressor stations, gas processing plants.

Another legal document – Decree of CMU (28.07.2003 No.1170), approved the *List of energy facilities of highest importance*. These facilities are protected by militarized guard subordinated by MEC[95]. This list includes: dispatching point for operational and technological management, electrical

---

[94] *Про затвердження* переліку особливо важливих об'єктів нафтогазової галузі : розпорядження Кабінету Міністрів України від 27.05.2009 р. № 578-р [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/578-2009-%D1%80

[95] *Про затвердження* переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 р. № 1170 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1170-2003-%D0%BF

substations with voltage over 330kV, hydroelectric power plants, heat and power plants.

Yet another category which is defined in the Ukrainian legislation, and determined, for instance, in the US, as part of the CI taking into account a possible terrorist threat, is immovable monuments of cultural heritage.

The objects of cultural heritage pursuit to Law of Ukraine «On Protection of Cultural Heritage»[96] are landmarks, buildings and constructions, related moving objects and areas (including underwater archaeological areas), other natural or man-made objects, that kept their value of archaeological, aesthetic, ethnological, historical, architectural, artistic, or scientific kind. Objects of cultural heritage are listed in the State Register of Immovable Monuments of Ukraine. To protect immovable cultural heritage the protection zones were established within which a special regime of their use have been set (regulations on building and construction, protected landscape area of archaeological cultural layer, etc.).

In the communication sector we should mention several systems, which operation is vital for governance, finance and emergency management.

The first one is National System of Confidential Communication, which, pursuit to Law of Ukraine «On the National System of Confidential Communication»[97], is a collection of special telecommunication systems (networks), which exchange confidential information among central and local authorities and therefore provide appropriate conditions for their cooperation during peacetime, emergency or warfare. State service of special communications of Ukraine (Derzhspeczv'yazok) maintains this system and ensures its functioning, development, and information protection using cryptographic and other technologies.

The second category of information systems, which we would like to emphasize, is a payment system. Pursuit to the Law of Ukraine «On the National Bank of Ukraine»(Article 7), the NBU provides coordination, development and control over operation of payment systems in Ukraine. There are already established and ensured the functioning of the Electronic Payment System (payments performed among banks) and the National System of Mass Elec-

---

[96] *Про охорону* культурної спадщини : закон України від 8.06.2000 р. № 1805-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1834105-14

[97] *Про Національну* систему конфіденційного зв'язку : закон України від 10.01.2002 р. № 2919-III (із змінами) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2919-14

tronic Payments (retail payments). Besides the payment system oversight[98], a considerable attention is paid to technical support of reliable operation and ensuring of information security.

So, at the moment may appear a new category of objects – those that require urgent protection against cyber-attacks.

It is important to note that according to international experience the Emergency and rescue service are considered as a part of CI. The Law of Ukraine «On the emergency services» declares that the emergency services operate on the certain area and provides services for enterprises, institutions and organizations regardless of their ownership, where there is a risk of natural disasters or manmade accidents. The list of objects, which should be served by emergency services, is defined by the Decree of CMU (04.08.2000 No.1214)[99]. This list includes objects of geological exploration, coal and other non-metallic mining, oil industry, chemical and petrochemical industry (including main pipelines, ammonia and ethylene pipelines), metallurgy, machinery, energy, transport system, etc.

In pursuance of the Order of CMU (02.10.2003 No.589-r) Ministry of Emergency Situations (predecessor of SSES) developed «Procedure for maintenance of facilities and some areas of public rescue services»[100]. Number of staff and professional composition of public rescue service unit which serves on facility under contract are determined by the head of the unit considering source of danger, scale of possible emergency and actual accident statistics. The cost of rescue maintenance on the facilities, including reimbursement of costs associated with the liquidation of emergency, determined by the appropriate Procedure[101].

---

[98] *Концепція* запровадження нагляду (оверсайта) за платіжними системами в Україні : постанова Правління Національного банку України від 15.09.2010 р. № 426 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/v0500-10

[99] *Про затвердження* переліку об'єктів та окремих територій, які підлягають постійному та обов'язковому на договірній основі обслуговуванню державними аварійно-рятувальними службами : постанова Кабінету Міністрів України від 4.08.2000 р. № 1214 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1

[100] *Про Порядок* обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами : наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 17.11.2003 р. № 440 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show

[101] *Про затвердження* Порядку визначення розмірів оплати за обслуговування об'єктів та окремих територій державними аварійно-рятувальними службами : наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерства економіки та з питань європейської інтеграції України від 15.12.2003 р. № 495/369 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1222-03

Thus, *the amounts of resources and tools (organizational, technical, engineering, information, etc.) allocated for emergency services units are defined by management of the certain units, and there is any claim concerning national (or even regional) significance of the object, the scale and nature of the possible consequences and impacts on other infrastructures*.

Another issue is the ability of State to allocate sufficient resources for the maintenance and modernization of safety and security on CI. On today, planning in this field is carried out without taking into account the scale of the possible consequences of accidents.

Unfortunately, the cost of safety and security measures can completely lie on the shoulders of users of infrastructure. For instance, the committee that was formed by MEC (Order No.365, 08.07.2008)[102], recognized that the protection of structural units of «Crimean generating system» does not meet the requirements of current legislation on the protection of energy facilities of high importance, and therefore this committee has proposed to send proposition to National Commission for the State Regulation of Energy to include all expenses of the security guard unit to the tariff for electricity generation.

Summary of this section. We have to conclude that measures to protect critical facilities, systems and resources in Ukraine are fragmented, they carried out by a number of authorities within their objectives and competences, that is reflected in the parallel functioning of systems intended to protect facilities and people against certain types of threats (man-made, natural or socio-political). This parallel existence of the protection of critical facilities and infrastructure posed a threat of problem «bureaucratization» and inefficient use of resources.

FROM CRITICAL INFRASTRUCTURE PROTECTION TOWARDS SECURING VITAL FUNCTIONS OF SOCIETY: CASE PROJECT ANVIL

Dr. Timo HELLENBERG,
CEO and Chairman, Hellenberg International Limited
(international government advocacy)

I would like to thank organizers for this kind possibility to be here today. I am grateful to the National Institute for Strategic Studies, which I have vi-

[102] *Про організацію* охорони об'єктів Державного підприємства «Кримські генеруючі системи» : наказ Мінекерговугілля від 8.07.2008 р. № 365 [Електронний ресурс]. – Режим доступу: http://mpe.kmu.gov.ua/fuel/doccatalog/document?id=136192

sited earlier, and the NATO Liaison Office in Ukraine, and particularly, Kersti Kelder. Thank you for this very interesting opportunity.

Before I go to my presentation about the Finnish system in critical infrastructure protection (CIP), I would like to come back a little bit to the earlier presentation, in particularly, the presentation made by Dmytro Biriukov. Here you can see a small picture of the landscape taken a few minutes before Hurricane Katrina hit New Orleans in 2005. Mr Biriukov pointed out at a very interesting comparison between the United States and Europe. What is critical? What is infrastructure? Should we consider, for instance, river based groundwater as a part of critical infrastructure? Also, should we consider human health as an element of critical infrastructure and so forth?

In Finland we have learned a lot of things about the American system of CIP. We have been particularly interested in the role of a private sector in this field. How should we engage private companies to protect critical infrastructure (CI)?

After 9/11, i.e., 11 September 2001 terrorist attacks, there was a new initiative launched in the U.S. in order to engage private entities. They established 16 working groups on both sides – the public sector and the private sector – and tried to identify those critical areas which are essential for business continuity in different fields: finance, energy, logistics and so forth. That was one attempt to attract interest from the private sector to this common goal, CIP, but I believe that it is not enough, because one of the problems is that the private companies tried to think on a quarterly or half-yearly basis, whereas we, who work with public agencies, tend to think in a-few-years timeframe. That is why we have different expectations and different mechanisms at place.

There is also one thing, which was not mentioned in the previous presentation – I mean prevention. How much should we be concentrated on prevention? And, on the other hand, on consequences and response? These things also require different approaches. What is the most important part of our mechanism aiming at CIP? I belong to the camp of experts who believe that the timely response is everything we need. It is more important than preparedness or consequences management.

Who has to make a decision in the right time to mobilize all response resources? From my experience, this is the most important thing.

And the other critical thing is resilience. In our country people are prone to think that the government will protect CI. «If something happens to me, it is governmental agencies who will come and help to rescue me», – is a typical viewpoint. For example, in Helsinki, the capital of the country, the average

time to arrive for fire service is seven minutes. But the fact remains, that if I call to countryside, it might take two hours to get a first response. What does it mean for such country as Finland where we have large distances separating cities and settlements, population of five million and the territory of a size of France. I believe, that it means that people have to have resilience provided themselves. They have to be risk-aware, i.e. knowing answers to questions: «What are the risks? And, «What can I do myself to reduce them?»

I am very happy to sit here, beside Kersti Kelder, because I often pointed out at Estonia, as a very good example of its citizens' resilience. The more the citizens are risk-aware the more they invest themselves – having two telephones, a standby aggregate in a garage, possibilities to withstand storms – the less money should be paid from the state budget. In Estonia there is a very interesting model called Naabrivalve (Neighborhood watch). It demonstrates, how neighbors should be connected with each other to create a risk awareness network, how they inform each other, and, the most important, how they transfer relevant information to the public agencies. This is a very small, micro-level experience, but it is worth to think it over very carefully. It shows us, what can be done, if we push responsibility to citizens themselves and let them think, how to share information with public agencies.

Ok, let me go further to the next part of my presentation. Here are some projects, in which our small team of experts has been engaged with EU. Basically, our work has been concentrated on CIP. For Nordic and Baltic countries governments we have done simulations of ship hijackings. We tried to map the risks for CI of the Baltic Sea Region, and, the most important, we have tried to develop some joined exercises. The above mentioned exercises addressed not only security of the nuclear facilities but also facilities assigned to CI (aviation industry, airports, seaports, and so forth).

Now, a few words about a crisis management system directly related to CIP. Historically, the current Finnish system for crisis management has been derived from the Cold War era. That means, that country has to be prepared to total defense. I would like to say, that the present crisis management system in Finland can be characterized as that based on high-degree decentralization, i.e. the system is decentralized. All the public agencies, all the public services will continue normal, routine work under emergency conditions. When an exceptional situation like a terrorist act, natural hazard or whatever occurs, all the agencies shall to carry on their normal routines. We have not created any specialized or ad hoc task forces. We used to have such a model in 1970s, but then we learned that it would be better if the public agencies would carry on

their normal routines. Thus, in that way, the system has been decentralized. I don't want to say that it is an optimal model: actually, a lot of difficulties have arisen from it. For instance, one of the difficulties is the following: when there is any kind of aggression against or interruption of CI systems or, like we say in Finland, the vital functions of society, who should define the nature of a crisis? I believe, that the answer appears to be very important, because basing on it, a decision shall be made, which an agency is in charge with a crisis response mission. Whether it is police, or fire and rescue service, or environmental protection ministry? Which one? Instead of losing hours and even days to decide who is responsible, we should response to a crisis without any delay.

This kind of an immediate response of an upper level decision making system is mobilized in the situation when a large scale crisis (like a nuclear disaster or a large scale flooding) occurs which affects the most part of society. Now, I would like to tell you more about it.

I have already mentioned about our tradition in this field: the system is mostly stemmed from the Cold War era. We have had quite a lot of reforms in our country in the recent decade. Three major reforms have been implemented in our crisis management system.

They are the following:

• erstablishment of the Emergency Management Administration 112. At the moment we have one emergency number, while previously we had six or even seven emergency numbers. But the situation is rather chaotic. We have established this new authority connecting, for instance police, and a client. Earlier, we used to have 15 alarm centres in our country, but we have scaled down our system to only two centres, and, probably, we shall be able to reduce it to one center, because modern technologies give us possibility to do so and to reduce the costs. Again, I am not saying, that it is the best system. On the contrary, I believe that we should have those 15 emergency centres and use them in case of exceptional situations as local emergency response centres as well as command and control centres;

• the second reform which has taken place in the past ten years is the total reform of our fire and rescue service. Previously we used to have a municipal system, thus we had 440 fire and rescue stations in Finland. Each municipality, each village had its own fire and rescue service. Instead of having 440 we have now 22 rescue regions. This reform brought more capacity, more personnel exchange and higher training possibilities. I believe that this is a very good reform in total.

Besides 112 system reform, fire and rescue service system regionalization we have also launched a new radio network. So, instead of a situation when all authorities were speaking to the telephones or radio network in case of emergency, now we have «Tetra» system, about which, as I know, Ukraine has been negotiated to purchase it. The use of this system means that if several authorities entering the same situation they are quickly connected with the same network, and that is a very positive development.

I am not very fond to bother you talking about legal documents, but I would like to state that the Finnish system is derived from its main goal – security of vital functions of society. That means, CIP is a hard core our civil security system in our country. It addresses the livelihood of the population, security of the society and national sovereignty. These three objectives are in the hard core of our system, and when we go to the project conceptualization it means international interaction management of the state activities, psychological crisis tolerance and, of course, resilience, what I have already mentioned.

This is a system created after the tsunami disaster occurred in 2004 in the South-Eastern Asia. It was the biggest civilian disaster affecting Finland. One could ask, why do you speak about this tsunami while we are considering CI? I think that the 2004 tsunami disaster is relevant because it was a kind of a landmark event for our country. After it we somewhat abolished the old crisis management system, instead it we have created a new one where a competent authority whether it is a local sheriff or local fire and rescue service always be in charge in case of emergency. If resources are insufficient, if there is no full awareness of an emergency situation, there are no enough data on an incident, and then responsibility is to be transferred to a higher level, i.e. the Governmental First Response Committee. In case of presence of a political dimension of a crisis connected with, for example, hijacking of a passenger ferry or a tsunami, CBRN threats involvement, then the responsibility might be transferred to the meeting of the permanent ministries secretaries and, finally, to the governmental level and to President. This is our new system in brief.

We also have a security strategy for society. The latest one has been published this year, and as I mentioned before, this is the first time this year when cyber security has been mentioned as part of measures aiming at CIP. Besides, we have created our cyber security strategy as well.

You can see the diagram of our new system of crisis management which looks rather extensive. If I don't fully understand it I cannot require you to do so. I still want to show it to you in order to have imagination about the administration process might look. So, here is the competent authority and, as I

mentioned earlier, a local response body, whatever it is (police, fire and rescue service, border guard, the newly created emergency call service), then – Security and Defense Committee facilitated by the Ministry of Defense. At the same time we have the Governmental Situation Centre at the Prime Minister's office designed for operational leadership in the case when a competent authority does not manage a deal with the emergency situation like it happened in case of swine flu epidemic in 2011 which presented a very good example. Then one ministry could not deal with the whole situation and had to transfer responsibility to the upper level.

As I outlined before, in our country we have a wording somewhat different from «critical infrastructure protection». Actually, we use a kind of its substitute, namely, «security of the functions vital to society». That means, that instead of focusing on protection of infrastructure assets we are focusing on guaranteeing the security of livelihood, security of sovereignty, security of population. It is a slightly different approach, but it is very close to those applied by other countries.

When considering sectors of our system, they are the following:

- management of the governmental affairs;
- international activities;
- military defense;
- internal security;
- functioning of the economy;
- population income security;
- psychological crisis tolerance.

These wordings sound very academically, but there is quite a lot of focus on resilience in this strategy. Of course, one could ask «Why I am still surprised with our system?» The matter is that, for instance, the Finnish government has multiple crisis scenarios developed to which our country is prepared to response. But, as we all know, a crisis is always unique, its conditions are different. It should be noted that today some political dimension is involved in crisis management. In this connection, I would like to say that a system is never fully ready to response. So, we have to improve it further, and that is why I also have some critical points on the Finnish crisis management system.

Here are some current problems. We still have a problem in sharing information among different agencies. And this is one of the biggest handicaps of our system. Actually, in case of the crisis situation we have a problem of transferring information and awareness of the situation from bottom to up, while, on the other hand, there are problems in sharing information among agencies.

The reason of this difficulty is that it is a voluntary business for the civil services to share information with other agencies. There is no a legal basis for such a legally binding requirement to different ministries.

Probably, you remember the ship hijacking in 2009 of the «Arctic Sea» merchant vessel. In that case, for instance, the Finnish Prime Minister was not able to get critical information from the Finnish police because they were not obliged to inform the Prime Minister. It was a very interesting situation, since our Prime Minister at that time was travelling to Moscow to have a meeting with then Russian Prime Minister Vladimir Putin. So our Prime Minister had to ask his Russian colleague whether or not he had any information on the hijacking since he could not get information from the Finnish authorities. And we are still in the situation where we have to resolve this issue, and this is, I think, a very interesting and informative case.

Now, I would like to talk about some cases clearly affecting CIP in Finland in the aftermath of the Cold War. In that period of time we had the ship hijacking occurred between Finland and Estonia. That was a horrified situation for both countries.

Almost 1000 became casualties due to the sinking of the MS Estonia of 1994 in the Baltic Sea. Actually, that was the first serious test for cross border civil security systems of three countries – Estonia, Finland and Sweden. We learned a lot of lessons from that accident. And, the situation was particularly aggravated due to the fact that the accident occurred in international waters, and it was extremely difficult to identify who was responsible for rescue operations.

As for tsunami of 2004 in South-Eastern Asia, our country lost almost two hundred people in this disaster. I am sure, that Ukraine also lost a lot of people. After that we have created a new crisis management system which I described earlier. When creating it, the main idea was that, basically, the crisis management leadership had to be clear defined. Besides, one more objective was to provide conditions in which situational awareness can move smoothly across the bureaucratic borders.

The flooding of 2005 at the Gulf of Finland also belongs to major disasters shaping our crisis management system. At that time the sea water level rose by two meters within one day. That was a very disastrous incident not only for Finland, but also for our neighbors, Estonia and Russia. I have to say that the disaster was very close to end up with somewhat like Finnish Fukushima. I suppose, that you can think that I am exaggerating the situation, but, actually, we did not have a holistic downscaling system in our nuclear reactor in this

part of sea near Loviisa. Really, at some moment of that flooding the level of sea water was 2 cm from the critical level defined for our nuclear reactor. In this connection, I am curious, here, in Ukraine, you did not build your nuclear reactors by the sea? They are inland. On the contrary, we built our 6 reactors by the sea. This is just a small example outlining our situation.

The next one incident is Nokia water crisis. The crisis was not connected with a well-known company Nokia. This is about a small town called Nokia where the above company was established two hundred years ago. There we had the water crisis caused by accidental leakages of polluted water to drinking water. Consequently, eight thousand people got symptoms of a very serious sickness through, basically, drinking the totally wasted water. One person died in the incident. What we learned when we considered resilience and CIP was that response and early reaction were everything that we needed in that case.

We had also two cases of shooting in schools in Finland. In both cases several young people died. Those cases gave us very dramatic experience. Most of the lessons learned from them related to the response of police and other law enforcement bodies.

One more disaster in this list is connected with the Russian forest fires in 2010. They affected directly Finnish CI. That was a very serious situation caused by the worst natural catastrophe in the modern Russian history. I saw figures provided by the UN that showed 56 000 deaths due to that disaster. This is a very high quantity. I used to live in Moscow at that time, and according to one of the very concrete estimations, in Moscow 700 people died every day during the disaster period. Exactly at the same time we had in Karelia the summer storms. You can see how the winds led to very big devastations, to destruction of electric grids, communication networks, etc. Basically, a half of Finland was cut off from power supply and communication. Some of the territories were without electricity for two weeks. You can imagine how, for example, some people were living on the island of a big lake. There was no electricity, no communication and the boat was at the bottom of the lake. That was a very serious situation for our country.

We also suffered from the winter storms which have affected our CI networks on a continuous basis. To be prepared to emergencies we carry out annual exercises for our authorities. The last one was in December 2011.

One more case was caused by the electric grid disabled for several days during the flooding. That created communication problems like I mentioned earlier, i.e. cell phones were disabled. Luckily, at that time there was not the

severe frost. If that flooding water would be frozen, we would have been, very likely, in an emergency of a national level.

My time is out, but I would like to present very quickly the ANVIL project[103]. I am providing you with a web-address where you can get relevant information. We have practiced under this project thanks to EU for 2 years and done a very extensive research of CIP systems in Europe. I would like to urge you to visit our web-site after December, when the reports for all these countries will be available, and you will be able to have free access to them. We have tried to study, what is an optimal CIP system for each country and, of course, to provide some valuable aid to EU countries and all associated countries basing on the project results. The partner countries within the project framework are Poland, Sweden and Norway. Besides, most of European countries are involved in the project. I would like to give these reports to the Institute which is hosting this conference.

CRITICAL INFRASTRUCTURE PROTECTION IN POLAND

Krzysztof BRZOZOWSKI,
Chief expert, Critical Infrastructure Protection Unit, Government Centre for Security, Poland

I would like to speak a little bit about critical infrastructure protection (CIP) in Poland, about our system, designation of our CI and the CI systems.

So, some words about the historical background of the subject matter. Before we had defined such terms as critical infrastructure (CI) and critical infrastructure protection (CIP) there were different legal acts in this field, in particular, acts about the protection of special objects. But we found that this protection system was not adequate to threats. For example, the system was focused only on physical protection of the objects and there was lack of clear criteria for defining such objects.

So, we have shifted to a modern approach to define such objects and systems. The first two steps in this direction were done in 2007. They were: establishment of the Government Centre for Security, a governmental body responsible for crisis management and CIP planning and programming; and creation of a relevant law, namely, the Act of 26 April 2007 on Crisis Manage-

[103] *Detailed* information can be obtained from [Електронний ресурс]. – Режим доступу: www.anvil-project.net

ment. This act contains the definitions of critical infrastructure and critical infrastructure protection.

So, according to the above mentioned act, critical infrastructure shall be understood «as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises».

There are 11 CI systems:

a) Energy, fuel and energy resources supply system (we recognize this system as especially important for our country);

b) Communication system (including phones, mobile phones, TV stations, radiobroadcasting stations, Internet, post offices, etc.);

c) Tele-information network system (for example: systems used by the government and administrations);

d) Financial system (including state budget banking system, stock exchange, etc.);

e) Food supply system (including various facilities for food production and storage);

f) Water supply system (the name of these systems is a little bit tricky, since they include not only fresh water facilities but also those of waste water management);

g) Health protection system;

h) Transportation systems (including roads, trains, trucks and other means of transportation);

i) Rescue system;

j) Systems ensuring the continuity of public administration activities;

k) System of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

Thus, any object assigned to CI in Poland is included in one of the system mentioned above.

According to already mentioned Act of 26 April 2007, protection of critical infrastructure shall be understood as «all steps aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to prevent threats, risks or vulnerabilities and limitations as well as neutralizing their effects and quick reconstruction of the infrastructure in case of failures, attacks and other events disrupting its appropriate functioning». So, the main goal is to protect all CI objects and systems so that to ensure their normal functioning.

The CIP is based on risk analysis. For this purpose we ask all actors involved in the process to carry out a high quality risk analysis.

All protection measures have been divided into 6 types. One of them is physical protection which deals with walls, fences, guards, guns, etc. Technical measures are about process and construction safety. The next one is security personnel and aimed at persons who are authorized to enter our buildings, sites, etc. and could do some unauthorized acts within the protected areas. The IT measures, obviously, are aimed at software and hardware security. The legal ones mean special law in some specific areas and, obviously, all things about ownership of buildings, ground and other elements of CI. Last thing is recovery plans. They are important because even if we have protection on a very high level, some things can go wrong and we should be prepared to respond. For example, if we have a special pump and it is broken, it is likely that we will not able to buy it at the market within a few days or weeks. So, under such a plan we should prepare our systems to identify, what are crucial elements in their process chains and purchase some of them in advance and then put in storage, or to make some arrangements with producers.

Now, I would like to show you, how CI is designated in Poland. In the CI designation process we have three stages and only if a CI goes through all the stages of designation it is recognized as a CI element. So, during the first stage sectorial criteria are taken into account. It is, in reality, a pre-selection stage. Every system has its own specific numeric criteria. If an object or system meets a certain numeric criteria then it is considered that the first step is completed. The criteria are classified as a «restricted» information. After the first step we compare our object with the definition of CI which I mentioned before to determine whether the object is critical for the state and its citizens. And the third step associated with application of cross-cutting criteria. Within this stage we have to assess potential effects of infrastructure system dysfunction. When doing so we apply the following categories of criteria:

- casualties;
- economic effects;
- necessity of evacuation;
- service loss;
- recovery time;
- international effects;
- uniqueness.

If an object passes all three stages then it can be designated as CI. These criteria are also «restricted» information. The output from the last stage is the list of CI of Poland. The complete list of CI are classified «secret». After the list is complete the Director of the Government Centre for Security sends notifications to operators of CI put on the list. With this, certain obligations are put on operators. The first is the preparation of a CI protection plan. And it is not an easy task. The first step on this route of course, is to understand the role of your facility, plant or other object, and then to perform risk analysis allowing to answer the question: «What should I do to mitigate the risks for our CI?» Without a good risk analysis you can spend a lot of money for elements which have no direct influence on security.

The second obligation put on an operator is the designation of a contact person responsible for maintaining relations with public administration on issues dealing with CI protection.

One very important thing is that in Poland protection of critical infrastructure is the operator's duty. So, it is not government's or other body's duty. Of course, all the services should help operators but the obligation of protection is on operator's side.

So, what government and administration do to help operators? These activities are based on provisions of Article 5b of the Act on Crisis Management according to which «The Council of Ministers shall adopt, by a resolution, the National Critical Infrastructure Protection Programme… which aims at creating conditions for improving the security of critical infrastructure…» The Programme is prepared by the Government Centre for Security. The Programme is a short document, but has three annexes. Of them Annex 3 contains the CI criteria and is classified. So, only the main document and Annexes 1 and 2 are printed out and publicly available.

As for the main actors of CIP in Poland, first of all we, should note the ministers. Each minister is responsible for one or more CI systems. We also have the Government Centre for Security which ensures information exchange between operators and administration. And, of course, we should mention operators of CI.

In our activities we answer the following question: «What for we are doing all these things?» The answer is: «To create conditions for improving security of CI». So, when somebody asks: «Why should I do some things?» or, «Why should I go through all Poland to attend, for example, a seminar or training course?» Our answer is following: «It is for security of your CI and we think that the CI is crucial for security of our country and our people. It is crucial

too, even if it is in private ownership. It should be in good condition, protected, and it is you that should think about it. It is not only government's services task to protect your object.»

The main objectives of our Programme are achieved by the following measures:

- designating ministers responsible for the specific CI systems;
- defining criteria to drawin up the List of CI;
- outlining priorities, objectives, requirements and standards, which are to ensure the functioning of critical infrastructure.

Programme implementation is based on the following main principles:

- joint responsibility;
- trust;
- cooperation.

As I mentioned before, the responsibility for CI protection is on the operator's side, but we know that all governmental services – police, fire fighters and so on – should cooperate, provide warning, establish information exchange, etc.

Trust is especially important in exchanging sensitive information. Sometimes public administration has sensitive information and sends it to operators, and sometimes operators provide the government, for example our Centre for Security, with sensitive data about their bussines. When doing so, we should trust each other. Operator should be sure we shall not disseminate information to unappropriated people, especially, when it includes data on CI security issues.

And, of course, efficient cooperation is of great importance in our efforts. Without it, obviously, we cannot reach good results.

As for annexes to the Programme, Annex 1 contains characteristics of all eleven CI systems. But for operators, we believe, especially interesting is Annex 2 which contains standards ensuring efficient functioning of critical infrastructure – best practices and recommendations. Ultimately, Annex 3 contains criteria for identifying CI, and this Annex is not a publicly available document.

The National Programme for Critical Infrastructure Protection can be downloaded from the RCB (the title abbreviation of the Government Centre for Security in Polish) web-page, where some national legislative acts on CI in English are also available.

NATIONAL ASPECTS OF THE CRITICAL INFRASTRUCTURE PROTECTION: CASE OF HUNGARY

Lt-Col. Dr. Katalin GÖRÖG,
Deputy Head of Department for Critical Infrastructure Coordination
National Directorate General for Disaster Management
Ministry of the Interior, Hungary

Thank for host country for kind invitation. It is possibility for me to share all my experience in this special issue which is called Critical Infrastructure Protection (CIP).

Primarily I would like to show you a video which was made last year, 2012. That date was very remarkable for our national disaster management system, because this year we have prepared more than 100 pieces of legislation regarding to disaster management, and in addition to it a totally new disaster management structure was established, which completely broke the past organization and structural setup. This video – which will take about 5 minutes, will give you a short insight of our daily routine work in disaster management.

Returning to my presentation which will be divided into 3 parts. First, I would like to concentrate on the past events regarding to this topic. Then I'll focus on recent activities and measures. And the third part will be on our future plans regarding to CIP.

The first question that can be raised is that «What do we mean under infrastructure?»

In a very simple way we should say that infrastructure equals with our social environment around us. Infrastructures can contribute to satisfy our human needs. They are accompanied with technologies all the time. And they provide different kinds of services for us. (fig.1)

What the difference between «ordinary» and «critical» infrastructure? What make the infrastructure to be critical?

We should consider several principles, which are given from the EU legislation:

- interdependence;
- cyber security;
- operation;
- cascade effect;
- the weakest link & part-whole concept.

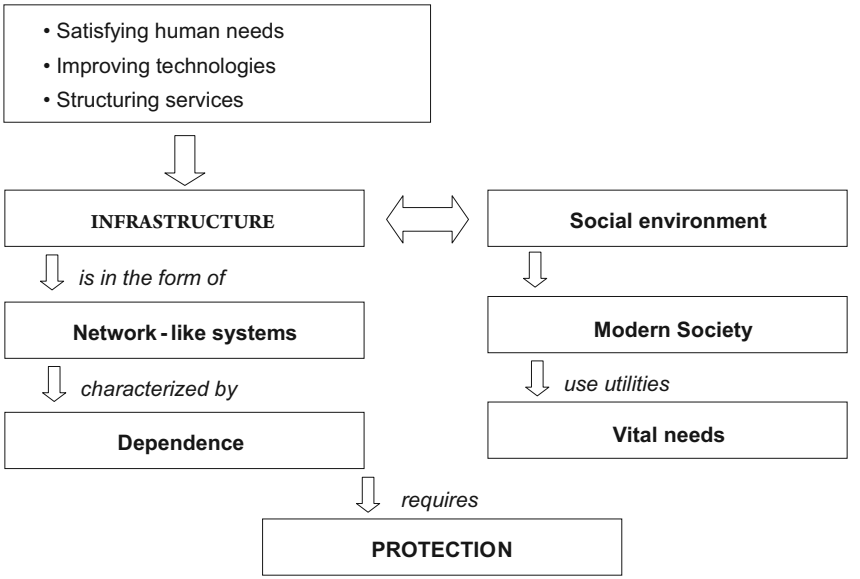


Fig. 1. Infrastructures in the everyday life

Along examination of these principles, you have to pay attention to infrastructures which are essential for the maintenance of public service, and if public service provision failure or disruption deficiency happens then it can have significant negative impact or a harmful impact on environment. If an infrastructure acts this way in a case of its failure or disoperation than it can be designated as CI.

According to its definition, CI means «an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions»[104].

Why do we have to deal with CI? Because such things could happen in the past, and happened in the near past as well. Bhopal (India) – chemical

[104] *EU Council* Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection Off. J. of the European Union [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

incident. Sumatra. Hungarian example – Kolontar – that's a sad tragedy. Everybody heard about that. NY remarkable day, Madrid – terrorist attack and London.

Based on these accidents and based on these disasters International organization are paying special focus on CIP issues. Beyond NATO the EU put this topic into his agenda. As everybody knows EU has an EPCIP (European Program for CIP) aiming at the prevention, preparedness and resilience principles. This European program doesn't consist only of the directive but it includes financial background project, member-states assistance, action plans and so on in itself.

What about Hungary? Our security environment was changed when we had the accession to the NATO in March 1999. And obviously becoming of the member of EU (May 2004) already changed our security environment. There is a movement (a change) which can be perceived if we compare happening and problems which were arises during political regime change in 1989–1990 th. Then we had to face with illegal migration and Balkan conflicts. And now we have to face with different kind of disasters and CI threats.

As I said in 1990-th when political regime changed along with this the term «security» the approach regarding to security was reinterpreted (fig.2). We had Disaster Management Act from 1990-th which was amended in 2006.

We had a Green Paper regarding to CIP in Hungary (Government Decision No.2080/2008 (VI. 30).

I would like to pay your attention on 2 government decisions (Government Decision 1249/2010. (XI. 19) on the governmental tasks).

The first from 2008 – its aim to adopt a national Green Paper of CIP Program. The second decision, that I would like to emphasize is from 2010 – its main point was to designate the Ministry of Interior of Hungary to coordinate tasks in CIP. And he became an EPCIP contact point, and has the rights and obligations to take part in international discussion regarding to European CI.

The other element that can be emphasized in this decision is that it defines the set of CIP Working Groups. On fig.3 you can see the composition of inter-ministry Working Groups. It involves a Ministry of Interior, Minister for Administration and Justice, Minister for Economics and Minister for National Defense. This Working Group made very fruitful activity (they were very active) in reporting, classifying different criteria and discussion matters.

In 2012 we had a new Act on Disaster Management (No.CXXVIII of 2011) and several Decrees on covering issues. In last year we had visible change of

attitude toward disasters. And CIP became a prime area; I would say it became a trendy task.

Relevant legislation regarding to CIP starts from Fundamental Law of Hungary. We have Strategy of National Security and National Military Security as well. We have a Disaster Management Act as I said.

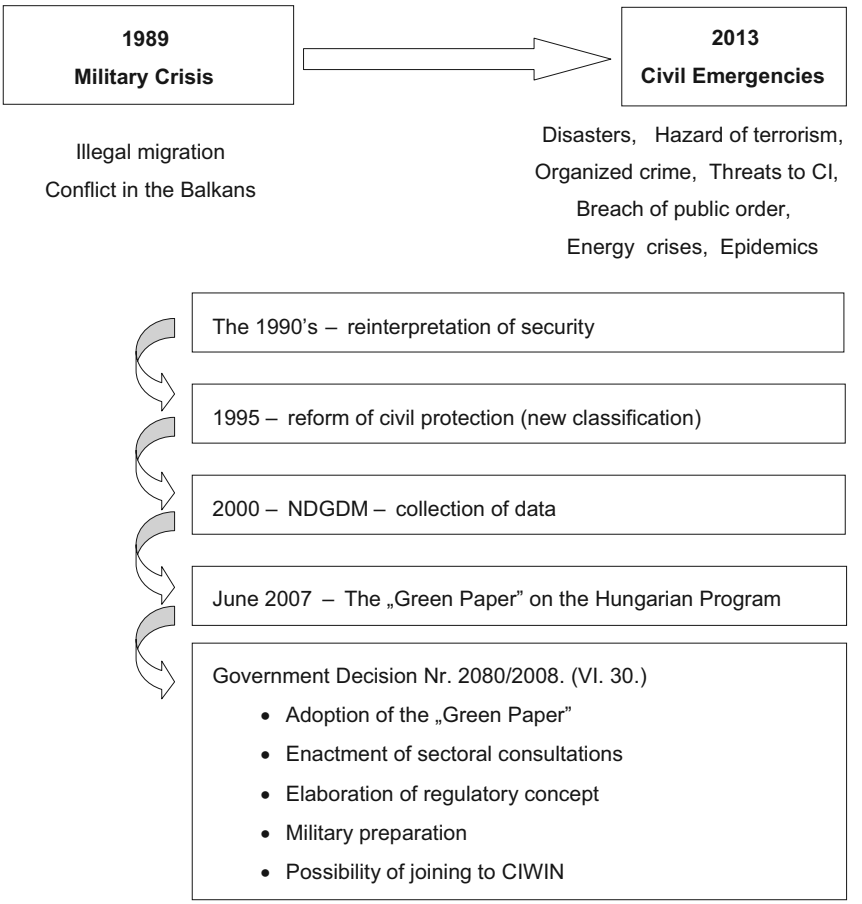


Fig. 2. Changes of challenges and risks affecting Hungary: «change of approach!»

Fig. 3. Composition of the CIP Inter-ministerial Working Group

And what is new – from the last year we have a special Act on the identification, designation and protection of critical infrastructures (No.CLXVI. of 2012). And this year on March its detailed and general Government Decree belonging this Act became to affect. And we have sectoral legislation as well. In the energy sector the Government Decree No.360/2013 was published in Official Journal in 11 October 2013, so it's quite fresh.

Examining the main elements of CIP Act. It consists of 16 paragraphs and 3 annexes. It starts with explanatory provision, definitions which are very important for the interpretation of the law. And then it lays down (describes) the identification and designation process of the National European CI. And its determines the common rules which covers the registration, operation security plans, the rule of qualification of security liaison officers and its speaks about control and inspection.

We can find special rules for the energy sector. And it closed by authorization and closing provisions.

In annexes. We have 10 sectors of CI. Designated CI shall be belonged to one of these sectors. And to this sectors 2 or more subsectors joins. All together we have 42 subsectors.

We have already legislation regarding to Energy sector. A kind of delay for legislation can be perceived. But for the next year (January 2014) each of the sectors have to be ready with their legislation process (Fig. 4).

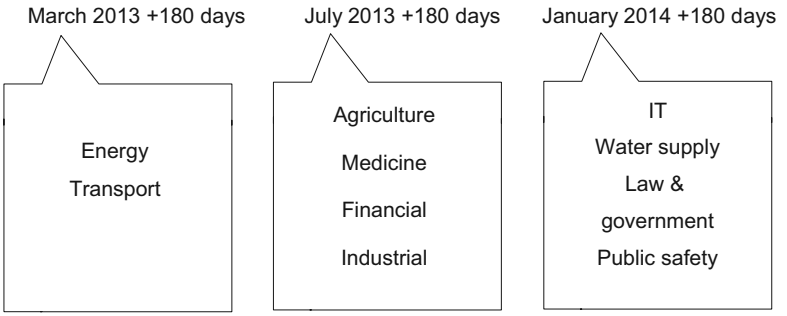


Fig. 4. Legislation process deadlines for each sector of CI

What is the content of Government Decree No.65/2013 (III.08.) on Critical Infrastructure? It contains the detailed information on different kind of legislation pieces:

- detailed general rules;
- complementary explanatory definitions;
- complemenary identification and designation process of the national and European CI;
- content requirements of the Operational Security Plan;
- education and qualification of the security officer;
- registration, data protection, controls on site, coordinated control, supervision, management of extraordinary events;
- special rules for the energy sector.

Two kinds of control and inspection systems that we use.

The missing sectoral decrees have to contain the determination of the sectoral authorities involving identification and designation of CI. In those sectoral decrees the legislative determination of sectoral conditions, criteria, content requirements for Operation Security Plans, and it has to set the reference to the qualification of the officers.

Main elements of the sectoral decrees:

- determination of the sectoral authorities involved in identification and designation;

- determination of sectoral conditions;
- detailed content requirement of the sectoral Operational Security Plan;
- sectorally accepted education and qualification of the security officer.

If we sum this national legislation up, it can be very similar to a piece of cake or Egyptian pyramid. The covering (or the top) is the Act on CIP, together with the general Executive Decree (Government Decree), and the slices are the sectoral decrees which are still missing, except for the regulation on the energy sector.

Disaster management organs play an important role in CIP. The tasks are listed as below:

- monitoring;
- keeping critical infrastructures under authoritative control;
- coordination;
- registration;
- network Safety;
- incident management;
- CIP CERT;
- CIP Point of Contact (POC).

Monitoring. Above the individual sector we have the monitoring authority (a supervisor).

The National Directorate for Disaster Management – we are the main registration office in this respect: keeping the operation safety plans, keeping the official decisions on designated CI, and keeping some data regarding to the liaison officers. Our role is to keep CI under authorities' control. We coordinate for example the sectorial legislation process. We have incident management process as well. We would like to create a CIP emergency response team, with 24 hours on duty. And we are the contact point in this field.

Network Safety Center. Because we are considering that not only the systems (establishment) shall be protected but their network as well.

The disaster management organs have very close cooperative methods with other organizations as law enforcement, educational and scientific institutions.

A bit about the future. We are still waiting for publishing of the sectoral legislations. We would like to expand our cooperation and collaboration. I would say that the public-private partnership (PPP) is working quite well in Hungary on the basis of «give-receive balance». We concentrate on trainings and in the near future we would like to train our staff to handle CIP cases in a more efficient way. We are planning to have more information about international practice, because we are members of EU and we are working with Joint Research Centre (JRC, Ispra, Italy) in ERNCIP project.

And we would like to pay more attention to our bilateral and multilateral discussions. And here I would like to offer you, if you accept, as you know we have an Ukrainian – Hungarian Joint Committee on Disaster Management. And for the next meeting I would suggest to put CIP issue on the agenda, because in that meeting we will have more time for the deeper consultations.

For example, in the energy sector we can have future collaboration in designating European CI.

About Kolontar. I think that the criminal procedure is still going on. The process against persons who can be accused for not doing anything is still going on.

What about foreign owner, the German one – he left the company without any consequences. One of the Hungarian boss was sent into prison, but not for a long time just a kind of preliminary prisoning was happened.

About the damages. The government did a huge effort to compensate the inhabitants somehow. For those peoples, whose houses were ruined (destroyed) or their environment are hazardous for the health had a choice to choose between leaving the house and in this case the government will buy a new one in another city or decide to wait for reconstruction. Some inhabitants were insisted to stay, in spite of that as you know not only the red sludge when it is fluid and liquid is dangerous but also when it becomes dry and its color can turn to be grey and may cause problems to human health.

That is PPP. It was the first case in Hungary when the government directly had an influence into the operation of a private company as a supervisory body because of to maintain the working places, and of economic and financial reasons. Considering these reasons the government decided to supervise the operation of the MAL company. Experts, lawyers and engineers were involved on behalf on the government to handle this case.

The changes were happened not in the ownership but in the daily operation when checking all documentations, security measures were happened every day. We inspected and controlled all the activity that owners made.

In addition, it was the first case when an economically important private company was almost went into bankruptcy if the government doesn't stand beside the company. If the company will pay all compensations for harm brought for inhabitants and environment it will definitely lead to bankruptcy.

Learning from this accident we made pieces of legislation to think such a situation will not happen again. We wrote down if such accident in the private sector will happen than the Government will supervise company if economically or socially is necessary to invite the Government.

ЗАВДАННЯ ВНУТРІШНІХ ВІЙСЬК ЩОДО ЗАХИСТУ ОБ'ЄКТІВ ОКРЕМИХ КАТЕГОРІЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

КРИВЕНКО Олександр Васильович,
заступник командувача
Внутрішніх військ МВС України[105]

Військові частини й підрозділи Внутрішніх військ МВС України відіграють важливу роль у захисті окремих категорій критичної інфраструктури (КІ) і в мирний час, і в особливий період. Звичайно, вони діють в існуючому правовому полі. Відповідно до Закону України «Про Внутрішні війська МВС України» від 26 березня 1992 р. № 2235-XII (зі змінами та доповненнями від 30 жовтня 1995 р. № 407/95-ВР) на Внутрішні війська покладено такі завдання:

• охорона та оборона важливих державних об'єктів, об'єктів матеріально-технічного та військового забезпечення Міністерства внутрішніх справ України;

• супроводження спеціальних вантажів;

• здійснення пропускного режиму на об'єктах, що охороняються;

• конвоювання заарештованих і засуджених;

• охорона підсудних під час судового процесу;

• переслідування й затримання заарештованих і засуджених осіб, які втекли з-під варти;

• участь в охороні громадського порядку та боротьбі зі злочинністю;

• участь у ліквідації наслідків надзвичайних ситуацій на об'єктах, що охороняються;

• охорона дипломатичних представництв і консульських установ іноземних держав на території України.

Крім зазначених завдань, Внутрішні війська беруть участь у таких заходах:

• протидія терористичним проявам (стст. 5 та 6 Закону України «Про боротьбу з тероризмом»);

• забезпечення заходів правового режиму надзвичайного стану (Закон України «Про правовий режим надзвичайного стану»);

---

[105] Станом на 7-8.11.2013 р. (дата проведення міжнародної науково-практичної конференції).

• охорона вищих посадових осіб держави;

• територіальна оборона (Закон України «Про оборону України», Указ Президента України «Про внесення змін до Положення про територіальну оборону України»).

В умовах загострення небезпеки міжнародного тероризму виконання службово-бойових завдань з охорони ядерних об'єктів та об'єктів оборонно-промислового комплексу держави, що належать до КІ, є одними з головних для Внутрішніх військ.

Відповідно до законів України «Про Внутрішні війська МВС України», «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» та постанов Кабінету Міністрів України Внутрішні війська виконують службово-бойові завдання з охорони та оборони таких об'єктів:

• чотири атомних електростанції з 15 діючими реакторами;

• Запорізька АЕС (6 реакторів);

• Хмельницька АЕС (2 реактори);

• Южно-Українська АЕС (3 реактори);

• Рівненська АЕС (4 реактори);

• Державне спеціалізоване підприємство «Чорнобильська АЕС» та об'єкт «Укриття»;

• три науково-дослідницьких інститути:

  – Інститут ядерних досліджень Національної академії наук України (м. Київ);

  – Національний науковий центр «Харківський фізико-технічний інститут»;

  – науково-дослідна лабораторія Севастопольського національного університету ядерної енергії і промисловості Міністерства енергетики та вугільної промисловості України (м. Севастополь);

• 7 підприємств оборонно-промислового комплексу України:

  – державне підприємство «Південний машинобудівний завод» ім. Макарова (м. Дніпропетровськ);

  – казенний завод «Зірка» (м. Шостка);

  – казенний завод «Імпульс» (м. Шостка);

  – казенний завод хімічних виробів (м. Донецьк);

  – казенний завод «Зоря» (м. Рубіжне);

  – державне підприємство «Павлоградський механічний завод» (м. Павлоград);

– державне підприємство «Павлоградський хімічний завод» (м. Павлоград).

Периметр об'єктів, що охороняються Внутрішніми військами, становить понад 125 км, щодобово на бойову службу призначається 41 варта із залученням близько 1 тис. військовослужбовців.

Для виконання службово-бойових завдань з охорони спеціальних вантажів під час їх перевезення територією України у Внутрішніх військах створено спеціальний підрозділ, який забезпечує безпеку перевезення свіжого та відпрацьованого ядерного палива; комплектуючих частин для енергоблоків ядерних реакторів АЕС України; продукції ракетно-космічного призначення; транзитного свіжого та відпрацьованого ядерного палива під час його перевезення з Російської Федерації до атомних електростанцій Болгарії, Словаччини, Чехії та Угорщини й у зворотному напрямку.

Тільки у 2013 р. під час виконання зазначених завдань бойової служби військовослужбовцями Внутрішніх військ МВС затримано 7118 порушників, з-поміж яких за такі порушення та злочини:

- порушення пропускного режиму – 6 898 ос.;
- крадіжка матеріальних цінностей – 209 ос.;
- спроба проникнення на об'єкт – 11 ос.

Вилучено й повернуто державі матеріальних цінностей на загальну суму понад 124 тис. грн.

Виконано 22 завдання з охорони та оборони спеціальних вантажів під час їх перевезення територією України, зокрема таких:

- свіжого ядерного палива – 13;
- відпрацьованого ядерного палива – 7;
- продукції ракетно-космічного комплексу – 2.

При цьому варто зазначити, що завдання, покладені на Внутрішні війська МВС України, виконуються ними в інтересах 17 міністерств і відомств.

Серед об'єктів, що охороняються Внутрішніми військами, є підприємства, що належать до об'єктів I і II категорії режиму таємності і є казенними об'єктами, на яких виконуються роботи щодо розроблення зброї та утилізації артилерійських, інженерних, морських та авіаційних боєприпасів.

На об'єктах, що охороняються Внутрішніми військами, зберігається понад 130 ешелонів із вибуховими речовинами й небезпечними отруйними відходами виробництва, шкідливими для життя та здоров'я людей (у т.ч. 2 ешелони з високотоксичним речовинами).

Командуванням Внутрішніх військ МВС України у 2013 р. проведено робочі зустрічі з адміністрацією об'єктів, що охороняються, визначено способи вдосконалення взаємодії за всіма напрямами службово-бойової діяльності.

Командувач Внутрішніх військ МВС України доповідав міністру внутрішніх справ про проблемні питання щодо виконання службово-бойових завдань з охорони об'єктів, які охороняють внутрішні війська.

Останнім часом поширюються посягання терористичних організацій на безпеку об'єктів ядерної енергетики, що викликає стурбованість міжнародної спільноти. Акти тероризму на ядерних установках можуть завдати значного економічного збитку державі, призвести до радіаційного, хімічного забруднення місцевості на великій території, руйнування значної кількості будівель у населених пунктах і людських втрат. Для ліквідації наслідків необхідно буде залучати значні матеріальні та людські ресурси. Наслідки актів тероризму (аварій) негативно вплинуть на авторитет держави через невиконання взятих нею міжнародних зобов'язань щодо забезпечення безпеки радіаційно-небезпечних об'єктів.

Командування Внутрішніх військ МВС України, усвідомлюючи сучасні загрози ядерним установкам і ядерним матеріалам під час їх використання на ядерних установках, а також під час перевезення, зважаючи на міжнародні зобов'язання, які взяла на себе Україна, та вимоги законодавчих актів у сфері фізичного захисту, розуміючи відповідальність за здійснення охоронних функцій у системі фізичного захисту ядерних установок і ядерного матеріалу, заявляє про готовність запроваджувати у службово-бойову діяльність принципи фізичного захисту, визначені в Поправці до Конвенцій про фізичний захист ядерного матеріалу, та визнає пріоритет культури захищеності.

Діяльність командування Внутрішніх військ МВС України у сфері виконання охоронних функцій у системі фізичного захисту спрямована на забезпечення надійної охорони та оборони ядерних установок і ядерного матеріалу, запровадження й розвиток культури захищеності.

У своїй діяльності щодо здійснення охоронних функцій у системі фізичного захисту ядерних установок і ядерного матеріалу Внутрішні війська МВС України основні зусилля зосереджують на таких аспектах:

• системний підхід при підготовці особового складу до виконання службово-бойових завдань і за нормальної обстановки, і за умов виникнення надзвичайних та кризових ситуацій на території ядерних установок (на маршрутах перевезення ядерного матеріалу);

• адекватна підготовка та оснащення особового складу військових частин (підрозділів охорони) відповідно до загроз, визначених у державній та об'єктових проектних загрозах ядерним установкам і ядерним матеріалам;

• організація та підтримання тісної й дієвої взаємодії з усіма відомствами, задіяними в системі фізичного захисту ядерних установок і ядерних матеріалів під час їх перевезення;

• адекватне та своєчасне реагування на вимоги сьогодення щодо виникнення загроз інтересам України, спробам підриву її авторитету в міжнародному співтоваристві з використанням об'єктів ядерної енергетики або ядерного матеріалу, що використовується (перевозиться) на території України;

• усебічне й повне забезпечення життєдіяльності військових частини (підрозділів охорони);

• збереження кадрового потенціалу військових частин (підрозділів охорони), стимулювання особового складу щодо вдосконалення професійних якостей задля підвищення рівня захищеності ядерних установок і ядерного матеріалу;

• глибоке розуміння всіма військовослужбовцями реальності існуючих загроз;

• усвідомлення особовим складом наслідків, що можуть виникнути внаслідок недбалого ставлення до виконання завдань бойової служби.

Під час запровадження й розвитку культури захищеності командування Внутрішніх військ МВС України дотримується:

• персональної відповідальності кожного військовослужбовця за виконання своїх посадових обов'язків у сфері здійснення охоронних функцій у системі фізичного захисту;

• компетентності, згідно з якою весь особовий склад військових частин (підрозділів охорони) проходить відповідний відбір перед прийняттям на службу і призначенням на посади, початкове навчання й постійно працює над підвищенням професійного рівня в системі бойової і спеціальної підготовки та під час підвищення кваліфікації відповідно до посадових обов'язків;

• контролю, відповідно до якого з боку посадових осіб військових частин (підрозділів охорони) виконання охоронних функцій у системі фізичного захисту знаходиться під постійним контролем керівного складу та самоконтролем особового складу (відповідно до ст. 11 Статуту Внутрішньої служби Збройних сил України);

• мотивації, відповідно до якої встановлюється система заохочень і стягнень, що спонукає особовий склад добровільно доповідати керівництву про всі випадки порушень при здійсненні охоронних функцій у системі фізичного захисту і своїх, і залучених співпрацівників.

Відповідно до переліку об'єктів, затвердженого головою Служби безпеки України, атомні електростанції та підприємства оборонно-промислового комплексу належать до найбільш небезпечних у терористичному відношенні. З метою протидії актам ядерного тероризму відпрацьовано відповідні плани спільних дій підрозділів Служби безпеки України та спеціальних військових частин Внутрішніх військ МВС України.

Щорічно на атомних електростанціях під керівництвом штабу АТЦ при СБУ із запрошенням міжнародних спостерігачів проводяться командно-штабні й тактико-спеціальні навчання для відпрацювання питань щодо перевірки готовності сил і засобів підрозділів та військових частин Внутрішніх військ до боротьби з тероризмом під час проведення антитерористичної операції та ліквідації наслідків терористичного акту.

Також варто зазначити, що Розпорядженням Кабінету Міністрів України від 4 вересня 2013 р. № 684-р затверджено Комплексний план заходів щодо реалізації положень нової редакції Проектної загрози ядерним установкам, ядерним матеріалам, радіоактивним відходам, іншим джерелам іонізуючого випромінювання в Україні.

У зазначеному документі визначено заходи з підвищення рівня фізичного захисту ядерних об'єктів держави, що підлягають виконанню протягом 2014 р.:

• організація перегляду актів міжвідомчих комісій з охорони ядерних установок і ядерних матеріалів. Для реалізації зазначеного заходу командування ВВ МВС України ініціюватиме питання перед Міністерством енергетики та вугільної промисловості України, Міністерством екології та природних ресурсів України, Національною академією наук України, до сфери управління яких належать ядерні об'єкти, щодо створення міжвідомчих комісій та організації їх роботи протягом 2014 р. з питань перегляду актів Міжвідомчої комісії (МВК) з охорони ядерних установок та ядерних матеріалів з урахуванням об'єктових проектних загроз і результатів проведення оцінки вразливості;

• планування проведення спільних тактико-спеціальних навчань на 2014 р., відпрацювання тактики дій військових частин з охорони атомних електростанцій і сил допомоги ззовні у надзвичайних і кризових ситуаціях. Для виконання цього завдання проаналізовано підсумки проведення

тактико-спеціальних навчань на ВП «Хмельницька АЕС», що проводилися в жовтні 2013 р. Запропоновано врахувати результати проведення зазначених навчань при їх плануванні на 2014 р. і відпрацюванні тактики дій військових частин з охорони атомних електростанцій та сил допомоги ззовні у надзвичайних і кризових ситуаціях;

• забезпечення поетапного переозброєння новітніми зразками техніки та озброєння військових частин з охорони атомних електростанцій. З урахуванням нових тенденцій підготовки до тактики дій підрозділів і військових частин з охорони атомних електростанцій та сил допомоги ззовні у надзвичайних і кризових ситуаціях техніка та озброєння мають відповідати сучасним вимогам. При обґрунтуванні кошторису на утримання військових частин з охорони атомних електростанцій в Національній комісії України з регулювання електроенергетики знайдено порозуміння та підтримку щодо поетапного виділення коштів у розмірі 25 % від потреби на закупівлю новітніх зразків військової техніки та озброєння. Це дасть змогу протягом чотирьох років оновити парк техніки та озброєння військових частин з охорони АЕС;

• забезпечення підвищення кваліфікації фахівців із фізичного захисту на навчальних курсах на базі Навчального центру з фізичного захисту, обліку та контролю ядерних матеріалів ім. Джорджа Кузьмича ІЯД НАН України. Командувачем Внутрішніх військ МВС України прийнято рішення щодо проведення перепідготовки та підвищення кваліфікації військовослужбовців за контрактом військових частин з охорони АЕС на базі Навчального центру з фізичного захисту, обліку та контролю ядерних матеріалів ІЯД НАН України. Фахівцями ГУВВ МВС України та викладацьким складом Навчального центру ведеться робота щодо отримання відповідних ліцензій, розроблення тематичних програм і навчальних дисциплін за рівнями підготовки. Надано пропозиції до кошторисних видатків на утримання військових частин з охорони АЕС, а також щодо виділення коштів на навчання особового складу;

• забезпечення реконструкції й технічного переоснащення інженерно-технічних засобів систем фізичного захисту ядерних установок і ядерних матеріалів. Стан інженерно-технічних засобів системи фізичного захисту засобів на деяких об'єктах не відповідає повною мірою встановленим вимогам наказів Державної інспекції ядерного регулювання України №№ 176 і 177. Близько 40 % інженерно-технічних засобів фізичного захисту на атомних електростанціях виробили встановлені терміни експлуатації. Потребують заміни засоби виявлення в заборонених зонах об'єктів.

Нині в Україні відпрацьовується питання реформування правоохоронної системи, під час якого важливо вирішити існуючі проблеми та не допустити зниження рівня захисту об'єктів КІ. До оприлюднення Концепції керівництвом Внутрішніх військ МВС України підготовлено низку змін до Закону України «Про Внутрішні війська МВС України», згідно з якими розширюються повноваження щодо організації взаємодії і з державними органами, і з громадськими організаціями. Є проблемні питання, на вирішення яких сплановано заходи на 2014 р. Якість і обсяг виконання цих заходів значною мірою залежить від обсягів фінансування.

На завершення зазначу, що своєю щоденною службою військовослужбовці Внутрішніх військ МВС України надійно охороняють визначені об'єкти критичної інфраструктури.

ПРОБЛЕМИ РЕГУЛЮВАННЯ ТЕХНОГЕННОЇ БЕЗПЕКИ В УКРАЇНІ

ГРЕЧАНІНОВ Віктор Федорович,
начальник відділу забезпечення діяльності голови Державної служби України з надзвичайних ситуацій;
БЄГУН Василь Васильович,
завідувач відділу Інституту проблем математичних машин та систем НАН України

Численні техногенні загрози нині дедалі більше впливають на спроможність держави стало розвиватися, що зумовлює необхідність удосконалення законодавчих, організаційних, технологічних та інших аспектів у сфері техногенної та екологічної безпеки.

Варто зазначити, що основні нормативно-правові акти, які регулюють зазначену безпекову сферу, були прийняті переважно на початку сторіччя, зокрема:

• Про об'єкти підвищеної небезпеки (ОПН) (2001 р.)[106];

• Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру (2000 р., втратив чинність у 2013 р.)[107];

---

[106] *Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2245-14

[107] *Про захист* населення і територій від надзвичайних ситуацій техногенного та природного характеру» : закон України від 8.06.2000 р. № 1809-III [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1809-14

• Про правові засади цивільного захисту (2004 р., втратив чинність у 2013 р.)[108];

• Про основні засади державного нагляду (контролю) у сфері господарської діяльності (2007 р.)[109].

У липні 2013 р. набув чинності Кодекс цивільного захисту України[110], який врегульовує частину питань із вказаних вище законів.

Постанова Кабінету Міністрів «Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки» від 11 липня 2002 р. № 956 є тією основою законодавчої бази, що визначає процедурні питання та основні документи потенційно небезпечних об'єктів (ПНО), які мають бути розроблені. На жаль, навіть у цьому невеликому масиві норм існують невизначеності, а іноді й протиріччя, причому такі невідповідності починаються на рівні основних визначень. Наприклад, у Законі про ОПН (2001 р., із поправками до 2012 р.) визначено, що «ризик – ступінь імовірності певної негативної події, яка може відбутися в певний час або за певних обставин на території об'єкта підвищеної небезпеки і/або за його межами», а Закон № 877-V (2007 р., із поправками до 4 липня 2013 р.) дає таке визначення: «Ризик – кількісна міра небезпеки, що враховує ймовірність виникнення негативних наслідків від здійснення господарської діяльності та можливий розмір втрат від них». Зрозуміло, що останнє визначення правильне, відповідає сучасним уявленням і міжнародним стандартам, але ці й інші невідповідності досі не виправлені в чинних законах.

Складається враження, що закони не дуже затребувані, оскільки неоднозначності й суперечності не виправлені протягом тривалого часу, а це може означати лише одне: відносини у сфері безпеки реально відбуваються не в законодавчій площині, а на рівні особистих стосунків підприємців і державних службовців, що не сприяє зміцненню безпеки.

Спроби змін законодавства таки були. Зокрема, варто згадати Державну цільову соціальну програму розвитку цивільного захисту на 2009–2013 роки[111] і розроблення та прийняття Кодексу цивільного за-

---

[108] *Про правові* засади цивільного захисту : закон України від 24.06.2004 р. №1859-IV [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1859-15

[109] *Про основні* засади державного нагляду (контролю) у сфері господарської діяльності : закон України від 05.04.2007 р. № 877-V [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/877-16

[110] *Кодекс* цивільного захисту України [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/5403-17

[111] *Про затвердження* Державної цільової соціальної програми розвитку цивільного захисту на 2009–2013 роки : постанова Кабінету Міністрів України № 156 [Електронний ресурс].. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/156-2009-п

хисту. На жаль, більшість задумів з удосконалення законодавства, передбачених Програмою, не виконані, а положення Кодексу найчастіше повторюють помилки законів, нові положення кодексу не впроваджуються. Нова Програма ДСНС України, затверджена Законом України «Про затвердження Загальнодержавної цільової програми захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру на 2013–2017 роки» від 7 червня 2012 р. № 4909 не передбачає принципових змін управління безпекою. Ресурси Програми, призначені для здійснення першочергових заходів щодо захисту населення й територій від надзвичайних ситуацій, стосуються насамперед оновлення матеріальної бази й захисних споруд. Це, безумовно, важливо, але не сприяє вирішенню принципових питань управління безпекою на основі світового досвіду.

Як відомо, основою сучасних уявлень про управління безпекою є концепція ризик-орієнтованого підходу (РОП). Вітчизняні спроби вписатися в рамки цієї концепції не є успішними, навпаки, нещодавно прийнята Постанова КМУ[112] «Про затвердження методик розроблення критеріїв, за якими оцінюється ступінь ризику» висуває такі вимоги до віднесення суб'єктів господарювання до ступенів ризику: «п. 11. До кожного ступеня ризику має бути віднесено:

- до високого ступеня ризику – до 10 % суб'єктів господарювання;
- до середнього ступеня ризику – до 30 % суб'єктів господарювання;
- до незначного ступеня ризику – 60 % і більше суб'єктів господарювання».

Ці вимоги, по перше, необ'єктивні, навіть абсурдні. Дійсно, як можна заздалегідь класифікувати суб'єкти господарювання за ступенем ризику, не оцінюючи його? Ця проблема не вирішується просто. На наш погляд, має бути робота на перспективу: критерії ризику мають бути динамічними, з поступовим зниженням ризику протягом визначеного періоду адаптації до міжнародних норм від значень сьогодення, а саме до європейських норм (рис. 1). Якщо ж прийняти цю умову, то легко можна порахувати критерії на кожен рік періоду адаптації відповідно до вимог ВООЗ. Тобто потрібно було вказати механізм розрахунків критеріїв та методи чи методології оцінок ризиків підприємств.

---

[112] *Про затвердження* методик розроблення критеріїв, за якими оцінюється ступінь ризику : постанова Кабінету Міністрів України від 28.08.2013 р. № 752 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/752-2013-п

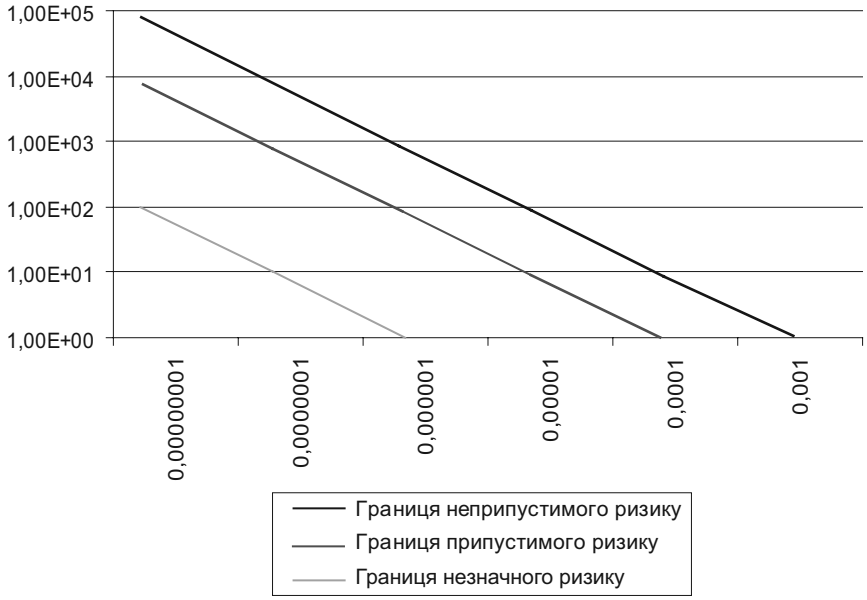


Рис.1. Європейські норми діапазонів ризику

В Україні значення прийнятого ризику законодавчо не встановлені, але світові товариства ВООЗ і МООП рекомендують такі значення: *незначний ризик – $R \leq 1 \cdot 10^{-6}$; припустимий ризик – $1 \cdot 10^{-6} \leq R \leq 5 \cdot 10^{-5}$; високий (терпимий) ризик – $5 \cdot 10^{-5} \leq R \leq 5 \cdot 10^{-4}$; неприпустимий ризик – $R \geq 5 \cdot 10^{-4}$, що відображується діаграмою «ймовірність-наслідки»* (рис. 1). Тут і далі ризик *R* визначаємо відповідно до Концептуального підхіду до управління ризиками надзвичайних ситуацій техногенного і природного характеру[113] як добуток:

$$R = P \cdot U,$$

де *P* – ймовірність небажаної події,

U – збиток.

За збиток у наведених значеннях приймається можлива кількість *загиблих* за результатами ймовірних аварій.

---

[113] *Хміль Г. А.* Концептуальний підхід до управління ризиками надзвичайних ситуацій техногенного і природного характеру / Г. А. Хміль., Є. П. Буравльов., В. В. Гетьман., В. В. Бєгун // Екологія і ресурси. : зб. наук. праць. – К. : ІПНБ РНБО, 2007. – С. 53–64.

У зв'язку зі значною кількістю недоліків і в реальних процесах регулювання безпеки, і в нормативній базі, логічними є запитання: «Чому так?», «Чому ми відстали від цивілізованого суспільства?» На наш погляд, відповідь криється в корені розуміння основних понять, а саме у «філософії безпеки». Про важливість цього поняття для безпеки свідчить висновок академіка В. А. Легасова про причини аварії на ЧАЕС (мовою оригіналу): «Дело именно в философии безопасности. Если бы философия безопасности была правильной, то технические решения под эту философию, конечно же, наши специалисты находили, потому что они грамотные специалисты, толковые люди, умеют считать и делать прочие вещи»[114].

У світовому суспільстві протягом досить тривалого часу панує філософія «запобігання ризиків», яка, своєю чергою, базується на принципах оцінок ризиків, кількісних аналізів тощо. Саме останні дають кількісні покажчики ризику, дають змогу розробляти науково обґрунтовані заходи для зниження ризику і встановлювати періодичність державного контролю, а саме:

- 5 років (якщо на об'єкті задекларовано незначний ризик);
- 3 роки (за припустимого ризику);
- 1 рік (за високого ризику).

Зазначена практика поширена в розвинених країнах із середини 70-х років XX ст., у Росії застосовується з початку нового тисячоріччя, що дає значний економічний ефект і істотно знижує ризики для персоналу небезпечних підприємств, населення й довкілля.

Важливу роль відіграє нове законодавство:

- Постанова КМУ «Про затвердження Порядку розподілу суб'єктів господарювання за ступенем ризику їх господарської діяльності для безпеки життя і здоров'я населення, навколишнього природного середовища щодо пожежної безпеки» від 14 листопада 2007 р. № 1324 й наступні постанови (№ 306, 431 та ін.);
- Наказ МНС (погоджений з Мін'юстом) «Про затвердження Правил улаштування, експлуатації та технічного обслуговування систем раннього виявлення надзвичайних ситуацій та оповіщення людей у разі їх виникнення» від 15 травня 2006 р. № 288;
- Постанова Кабінету Міністрів «Про затвердження Порядку проведення державної експертизи з питань техногенної безпеки…» від 20 серпня 2008 р. № 767.

---

[114] *Текс*т из пяти магнитофонных кассет, надиктованных академиком Легасовым В. А. «Об аварии на Чернобыльской АЭС» [Електронний ресурс]. – Режим доступу: http://www.pseudology.org/

Однак це законодавство є неефективним, не працює і не працюватиме, оскільки його основою є стара концепція регулювання безпеки, заснована на «забезпеченні 100 % безпеки» та постійному державному нагляді. Також не використовуються сучасні економічні механізми управління безпекою.

Так, вказаний першим документ нанівець зводить сучасні передові норми Закону № 877-V. Він, власне, є старою інструкцією радянських часів, оскільки всі ПНО та ОПН опинилися в одній ланці високого ризику, незважаючи на розрахунки.

«За визначенням об'єкти з високим ступенем ризику:

• потенційно небезпечні об'єкти та об'єкти підвищеної небезпеки;

• промислові та складські будівлі (споруди), які належать до категорій «А» або «Б» за вибухопожежною небезпекою незалежно від площі, та <…> категорії «В» площею 500 м^2 і більше;

• підприємства, які мають стратегічне значення для економіки та безпеки держави, перелік яких затверджений Постановою Кабінету Міністрів України № 1734 від 23.12.04 р.»[115].

Тобто це є декларація безпеки, яка за таких обставин втрачає будь-який сенс. Дійсно, навіщо розраховувати ризик (вимоги законів), якщо від цього частота перевірок не змінюється? У Наказі МНС № 288, що є обов'язковим для усіх ОПН, також простежується неадекватність і протиріччя світовому досвіду в головному, а саме: заходи безпеки розробляє і впроваджує господар, вказівки навіть центральних органів влади є некоректними, тим більше у примусовому порядку. Це або протекціонізм, або інший елемент корупційної схеми, що заважає розвитку бізнесу. Не менш значним є і наступний документ, який допускає можливість виконання важливої процедури безпеки (експертизи) виконавцями з недостатніми спеціальними знаннями, тобто вкотре спостерігається невідповідність світовому досвіду. Ще однією проблемою у впровадженні зазначеної норми є відсутність чітко сформульованих вимог до експертів та громадських експертиз.

Як наслідок, несучасні методи управління безпекою відкидають країну у світовому рейтингу в цій сфері на майже останні місця, а за деякими показниками сфери безпеки Україна має найгірші результати (рис. 2–5).

---

[115] *Про затвердження* переліку підприємств, які мають стратегічне значення для економіки та безпеки держави : постанова Кабінету Міністрів України від 23.12.04 р. № 1734 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1734-2004-%D0%BF

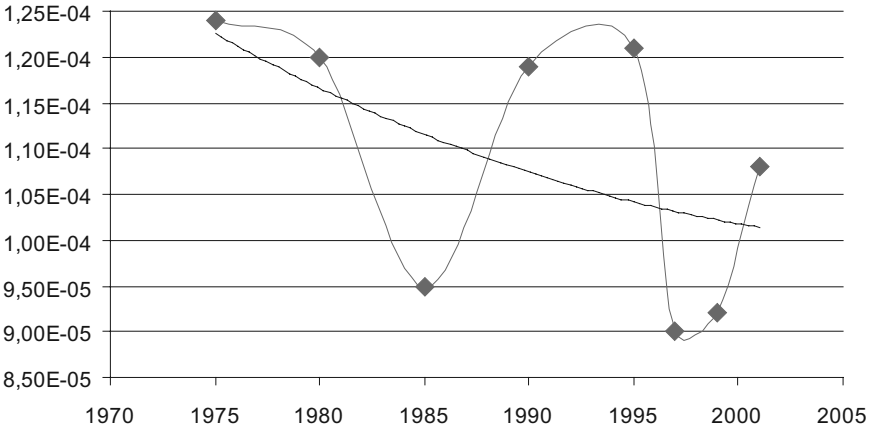


Рис. 2. Ризик смертності на виробництві

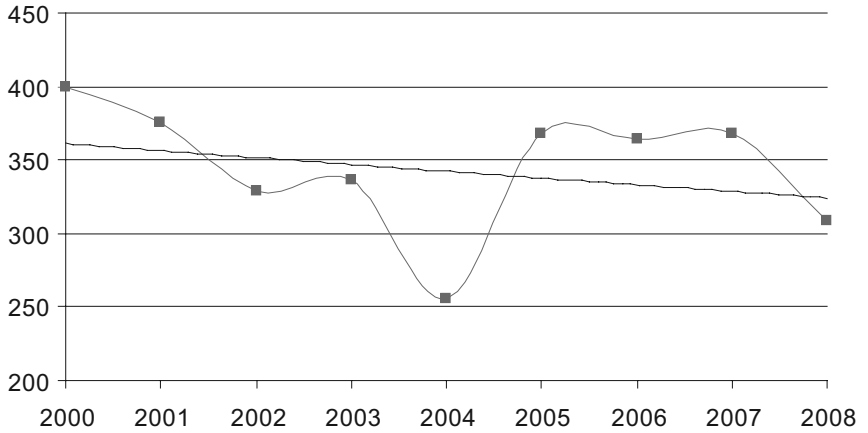


Рис. 3. Кількість надзвичайних ситуацій

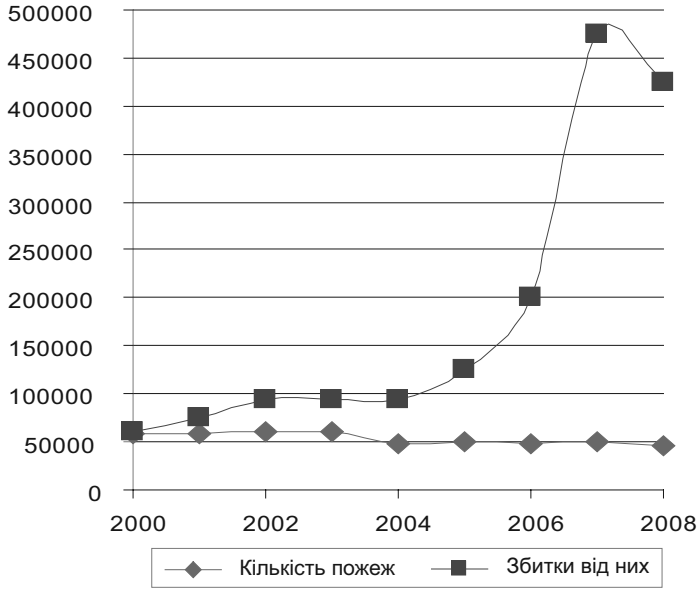


Рис. 4. Кількість пожеж та збитки від них

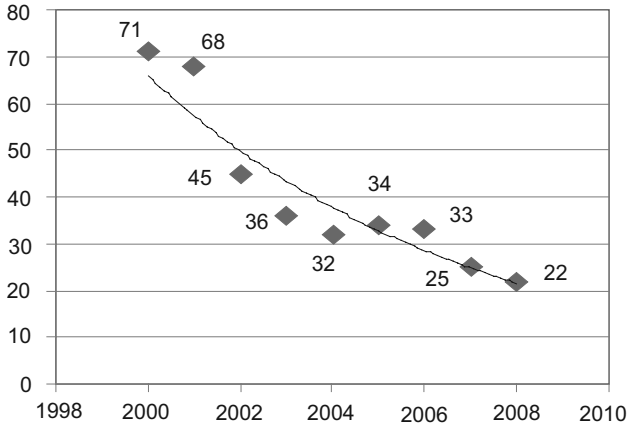


Рис. 5. Кількість порушень на АЕС України

Як видно, основні показники безпеки за порівняльний період або не змінюються (чи слабко змінюються), або зростають; лише в ядерній галузі спостерігається позитивна динаміка, що має експоненціальний характер.

Отже, передові принципи безпеки успішно впроваджуються поки що лише в ядерній галузі, в інших сферах безпеки (безпека охорони праці, техногенна, пожежна безпека тощо) залишаються старі концепції управління. Нонсенс, але факт: Україна за понад 20 років панування нібито ринкових принципів господарювання так і не змогла, крім як у ядерній галузі, змінити світогляд щодо методів управління безпекою. Інтеграція України в європейські структури неминуче приведе до зміни стратегії управління безпекою, адже в ЄС прийнято стратегію упередження надзвичайних ситуацій (НС), що знижує рівень небезпек і значно дешевше для держави загалом (у 7–30 разів).

Низьку ефективність управління безпекою в усіх її сферах порівняно з безпекою АЕС демонструють тренди основних показників із безпеки (рис. 2–5), якими обрано інтегральні показники небезпек: ризик смертності на виробництві – сфера охорони праці (за матеріалами підручника з охорони праці) (рис. 2); кількість надзвичайних ситуацій – сфера цивільного захисту (за матеріалами національної доповіді МНС) (рис. 3); пожежна безпека – кількість пожеж і розмір збитків від пожеж (за матеріалами статистики пожежного нагляду) (рис. 4); кількість порушень нормальної експлуатації на АЕС (за матеріалами щорічних звітів з безпеки) (рис. 5).

Із рис. 2 видно, що ймовірність летального випадку на виробництві, значно не змінилася протягом 30 років, незважаючи на зміни кількох поколінь обладнання й навіть державного устрою та форми власності. Тренд цього показника перебуває в досить вузькому діапазоні. Аналогічною є і поведінка двох інших показників – кількості надзвичайних ситуацій (рис. 3) і пожеж (рис. 4). Стосовно останніх, крім слабо спадаючого тренду кількості пожеж, маємо зростання майже в десять разів прямих збитків. Ці об'єктивні статистичні дані свідчать про низьку ефективність регулювання безпеки у цих сферах, неправильний вибір стратегії управління (перевага реагування на НС), відсутність системної роботи щодо запобігання надзвичайних ситуацій, застарілість основних принципів регулювання безпеки, їх невідповідність сучасним світовим нормам та інші недоліки у цих сферах діяльності.

Протилежна ситуація спостерігається в атомній галузі: упроваджено сучасні міжнародні принципи регулювання безпеки, її діяльність перебуває під пильним міжнародним контролем. За показник безпеки обрано

кількість порушень (навіть не аварій, а порушень – відхилень від нормальних умов експлуатації) за той самий період (рис. 5). За період незалежності відбулося скорочення числа порушень на АЕС майже в десять разів(!), а за порівняльний період – у чотири рази.

Отже, ситуацію з регулювання безпеки у сфері цивільного захисту потрібно змінювати докорінно. Стратегія управління безпекою має відповідати новому державному устрою та приватній формі власності. Про необхідність зміни стратегії державного контролю безпеки йдеться і в Програмі економічних реформ на 2010–2014 роки, в якій зазначено, що одним з основних завдань у сфері державного нагляду й контролю має бути «завершення розроблення та впровадження критеріїв оцінювання ступеня ризику від ведення суб'єктами господарської діяльності й періодичності проведення планових заходів державного нагляду (контролю)»[116].

Отже, все сказане стосовно регулювання безпеки у програмі відповідає і принципам концепції управління ризиками. Але докорінно змінити управління безпекою, як того вимагає уряд, непросто: потрібно змінювати світогляд, філософію і ставлення до безпеки, по-новому навчати фахівців. До цього спонукає час і наш європейський вибір. Навіть із короткого огляду можна дійти висновку щодо низької ефективності управління безпекою в Україні, неузгодженості нормативної бази з безпеки, її невідповідності державному устрою та сучасному міжнародному законодавству. До того ж, як уже зазначалося, неузгодженість розпочинається на рівні основних визначень. Упровадження передових технологій в ядерній галузі може бути прикладом для інших потенційно небезпечних галузей.

Концепція управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру вперше була розроблена у 2005 р. і схвалена Рішенням Ради регіонів щодо забезпечення ефективного реагування на виникнення ризику надзвичайних ситуацій від 20 червня 2013 р. Документ розроблений на основі європейської нормативної бази та передбачає впровадження ризик-орієнтованого підходу (РОП). На цьому шляху постають такі проблеми:

- чинна законодавча база недосконала;
- відповідні закони майже не впроваджені;
- методичний і науковий складники РОП відсутні та не розробляються.

---

[116] *Програма* економічних реформ на 2010–2014 роки. – С. 39 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/docs/Programa_reform_FINAL_1.pdf

Разом з тим можливості РОП значні: визначення ймовірності подій та можливих наслідків, розроблення заходів запобігання на основі моделювання. Наукоємна технологія управління безпекою потребує розрахунків. Зміст розрахунків ризику в загальному вигляді можна представити як знаходження функції шісти змінних:

$$R = F(X1,X2,X3,X4,X5,X6),$$

де *X1* – урахування усіх імовірних сценаріїв аварій для всіх режимів роботи;
X2 – всі можливі вихідні події, природного характеру тощо;
X3 – урахування зношеності основного обладнання та статистики його відмов;
X4 – урахування типів захисного обладнання та його стану;
X5 – урахування навченості персоналу;
X6 – розрахунок наслідків з урахуванням природно-кліматичних умов.

Загальний алгоритм кількісних розрахунків може бути таким (на прикладі аналізів ризиків АЕС)[117]:

1) побудова ймовірнісних моделей усіх систем, що беруть участь у можливих сценаріях аварій;

2) розрахунки імовірності відмов кожної системи;

3) розрахунки можливих кінцевих станів для всіх сценаріїв з урахуванням можливих відмов систем і помилок персоналу;

4) аналіз кінцевих станів з урахуванням усіх сценаріїв, а саме: визначення імовірності кінцевого стану та значимості базисних подій для кожного кінцевого стану.

Для впровадження цифрових технологій у сферу техногенної безпеки в Україні потрібно розробити такі документи:

- положення з організації ризик-менеджменту;
- положення з інформаційної підтримки ризик-менеджменту;
- стратегії контролю (розрахунку) ризику;
- стратегії страхового захисту об'єктів контролю;
- методики оцінки поточних значень ризику;
- методики оцінки пожежного ризику.

Критично важливі інфраструктури (КВІ) є окремим класом об'єктів, що потребують особливої уваги. Тому має бути забезпечено наявність:

---

[117] *Бегун В. В.* Вероятностный анализ безопасности атомных станций / В. В. Бегун, О. В. Горбунов, И. Н. Каденко и др. – К. : Випол, 2000. – 558 с.

• національної законодавчої та нормативно-правової бази щодо КВІ;

• державного нагляду за безпекою на основі ризик-орієнтованого підходу;

• методик визначення ризиків для населення;

• методик державного моніторингу КВІ;

• планів реагування на випадок загроз.

Відношення до ризик-орієнтованих підходів і КВІ у наших північних сусідів більш свідоме. У провідних документах записано (мовою оригіналу): «Целями создания системы мониторинга являются последовательное снижение до *минимального уровня риска воздействия на объекты* и угрозы факторов террористического, техногенного и природного характера, а также минимизация ущерба от кризисных ситуаций для населения страны и окружающей среды»[118]. Важливе значення має те, що в РФ діють стандарти ризик-менеджменту, які є адаптованими європейськими стандартами серій *ISO* або *МЕК,* зокрема: ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения (1.01.2003); ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты (1.01.2003); ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем (1.09.2003); ГОСТ Р 51901.4-2005 Менеджмент риска. Руководство по применению при проектировании (1.02.2006); ГОСТ Р 50779.10-2000 (ИСО 3534-1-93) Статистические методы. Вероятность и основы статистики. Термины и определения; ГОСТ Р 51901.5-2005 Менеджмент риска. Руководство по применению методов анализа надежности (1.02.2006); ГОСТ Р 51901.6-2005 Менеджмент риска. Программа повышения надежности (1.02.2006); ГОСТ Р 51901.11-2005 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство (1.01.2006); ГОСТ Р 51901.13-2005 Менеджмент риска. Анализ дерева неисправностей (1.09.2005); ГОСТ Р 51901.14-2005 Менеджмент риска. Метод структурной схемы надежности (1.09.2005); ГОСТ Р 51901.15-2005 Менеджмент риска. Применение марковских методов (1.02.2006); ГОСТ Р 51901.16-2005 Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки (1.01.2006).

Функції системи моніторингу КВІ прописані так (мовою оригіналу): «…сбор, обработка, анализ, хранение и передача информации о место-

---

[118] *Об одобрении* Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов : распоряжение Правительства Российской Федерации от 27.08.2005 г. №1314-р [Електронний ресурс]. – Режим доступу: http://www.consultant.ru

положении, обобщенных параметрах состояния защищенности объектов и грузов, маршрутах транспортировки грузов и других необходимых данных; информационная поддержка работ, выполняемых в целях подготовки и реализации мер по обеспечению безопасного функционирования объектов (безопасной транспортировки грузов), предупреждению и локализации кризисных ситуаций, а также ликвидации их последствий»[119].

Отже, проблеми, що існують у сфері техногенної безпеки України загалом і критично-важливих інфраструктур зокрема, мають бути розв'язані на шляху до євроінтеграції. Принциповим є перехід на нову концепцію управління ризиками, яка має бути затверджена (прийнята) як базова філософія управління безпекою. До розроблення відповідних документів повинні залучатися вчені, спеціалісти з безпеки; робота має бути відкритою і прозорою та ґрунтуватися на основі світового досвіду.

ГРІД-ЦЕНТР ІЗ ПИТАНЬ ЕНЕРГЕТИКИ Й ТЕХНІЧНІ ЗАСОБИ ДОДАТКОВОГО ЗАХИСТУ ДАНИХ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

ЄВДОКИМОВ Віктор Федорович,
директор Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;
ДАВИДЕНКО Анатолій Миколайович,
заступник директора з наукової роботи Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;
ЧЕМЕРИС Олександр Анатольович,
старший науковий співробітник Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;
ГІЛЬГУРТ Сергій Якович,
старший науковий співробітник Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України

Упровадження нових технологій моделювання на основі високопродуктивних обчислень, зокрема на основі грід-систем, сприяє збільшенню можливостей об'єднаної енергетичної системи (ОЕС) України

[119] *Об одобрении* Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов : распоряжение Правительства Российской Федерации от 27.08.2005 г. №1314-р [Електронний ресурс]. – Режим доступу: http://www.consultant.ru

з урахуванням вимог до рівня маневреності, експлуатаційної безпеки, живучості та стійкості функціонування енергооб'єднання, спостережливості й керованості електроенергетичних систем та об'єктів, зменшення впливу на навколишнє середовище[120]. Предметом досліджень у цьому напрямі є високопродуктивні методи моделювання режимів роботи ОЕС України та енергетичних об'єктів; вирішення завдань економіки, екології та інформаційної безпеки галузі в нових умовах; розроблення систем інформаційного забезпечення, моніторингу, обліку, контролю, керування тощо; моделювання технологій, систем та устаткування для підвищення експлуатаційної надійності, стійкості й живучості електроенергетичних систем; перевірка сценаріїв виникнення надзвичайних ситуацій на об'єктах ОЕС України та зменшення їх впливу на навколишнє середовище. З метою проведення згаданих вище досліджень на базі Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАНУ було створено ресурсно-операційний грід-центр із питань енергетики[121].

У процесі вирішення поставлених перед грід-центром завдань було виявлено проблему: як засвідчили дослідження, механізми інформаційної безпеки сучасних грід-мереж орієнтовані на протидію зовнішнім стосовно грід-інфраструктури чинникам. При цьому питання захисту програмного забезпечення грід-вузлів і даних грід-користувачів від інших авторизованих користувачів грід-системи, у т.ч. обслуговуючий персонал грід-вузлів, залишаються відкритими. Із цієї причини вирішення у грід-середовищі задач моделювання, у процесі якого використовуються конфіденційні дані, стає проблематичним, оскільки однією зі специфічних особливостей енергетики є підвищена небезпека технічних об'єктів.

Тому виникає необхідність у розширенні штатних засобів інформаційної безпеки грід-систем, зокрема у введенні додаткових функцій закриття даних, а також у підвищенні швидкодії при вирішенні завдань закриття інформації в грід-мережі. У результаті проведеного аналізу відомих загроз у комп'ютерних системах і відповідних засобів протидії їм

---

[120] *Петренко А. І.* Практикум з грід-технологій : навч. посіб. / А. І. Петренко, С. Я. Свістунов, Г. Д. Кисельов. – К. : НТУУ «КПІ», 2011. – 580 с.

[121] *Евдокимов В. Ф.* Информационно-аналитический центр по проблемам энергетики на базе грид-узла ИПМЭ НАНУ / В. Ф. Евдокимов, А. Н. Давиденко, А. А. Чемерис, С. Я. Гильгурт [та ін.] // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – Київ, 2009. – Вип. 53. – С. 3–8.

з урахуванням специфіки грід-середовища були сформульовані вимоги до функціонального складу створюваної системи внутрішньої безпеки грід-середовища (СВБГС), яка має включати такі підсистеми[122]:

• додатковий криптографічний захист інформації грід-користувачів;

• контроль цілісності інформації на грід-вузлі;

• виявлення вторгнень сигнатурного типу.

Реалізація перерахованих функцій забезпечить на віддалених грід-вузлах інформаційний захист від внутрішніх загроз і небезпек. Підсистема додаткового криптозахисту грід-користувачів призначена для додаткового захисту конфіденційних даних віддалених користувачів способом застосування відомих алгоритмів закриття інформації[123].

Найбільш уразливою з погляду закриття даних від авторизованих користувачів і технічного персоналу грід-вузлів інформація є під час зберігання у вигляді файлів даних на тривалих носіях інформації обчислювальних кластерів грід-системи.

Самостійне застосування грід-користувачем відомих засобів закриття інформації відволікає його від вирішення основних завдань, вимагає певної кваліфікації та не гарантує достатнього рівня захищеності. До того ж застосування тільки програмних засобів підвищує уразливість рішення та збільшує час обробки, тому пропонується використовувати рішення на основі реконфігуровних уніфікованих обчислювачів (РУО) – типових пристроїв, побудованих на базі програмованих мікросхем – ПЛІС[124]. У такому пристрої може бути синтезована довільна цифрова схема, наприклад високопродуктивний спецпроцесор закриття інформації.

Основою РУО є інтегральна схема програмованої логіки. Обов'язковою вимогою є наявність виділеного контролера системної шини або іншого засобу обміну інформацією із центральним процесором; на цей контролер покладається також функція завантаження конфігурації в

---

[122] *Давиденко А. Н.* Анализ вопросов внутренней безопасности в распределенных компьютерных сетях / А. Н. Давиденко, С. Я. Гильгурт, В. В. Душеба, А. К. Гиранова // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – Київ, 2011. – Вип. 62. – С. 57–62.

[123] *Гильгурт С. Я.* Программно-аппаратная защита данных в распределенных интеллектуальных системах / С. Я. Гильгурт, А. К. Гиранова // Искусственный интеллект. – Донецк : НАН Украины, Институт проблем ИИ, 2010. – № 3. – С. 706–711.

[124] *Гильгурт С. Я.* Обзор современных реконфигурируемых унифицированных вычислителей / С. Я. Гильгурт // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – Київ, 2008. – Вип. 49. – С. 17–24.

ПЛІС. Необхідною є наявність пристрою двопортової пам'яті для зберігання проміжних результатів; спрощують роботу налагоджувальні світлодіодні індикатори та перемикачі.

Функціонує апаратно-програмна підсистема додаткового криптозахисту таким чином. Перед початком роботи із грід-системою в РУО, яким оснащений комп'ютер користувача, завантажується конфігурація спецпроцесора, що реалізує необхідні алгоритми закриття інформації. Дані, призначені для обробки у грід-середовищі, зашифровуються на синтезованому в ПЛІС реконфігуровному обчислювачі та передаються комунікаційними каналами на цільовий грід-вузол, де зберігаються в закритому вигляді. Після запуску користувачем обчислювального завдання у грід-середовище дані розшифровуються безпосередньо перед його виконанням на грід-вузлі або за допомогою РУО, або програмним способом за його відсутності у складі устаткування грід-вузла. Результати обчислень, отримані у процесі виконання завдання, також зашифровуються апаратним або програмним способом і записуються на носії інформації грід-вузла для подальшої передачі грід-користувачу та розшифрування на РУО, встановленому на його комп'ютері.

Підсистема контролю цілісності призначена контролювати цілісність критично важливої інформації на грід-вузлах[125]. Основою механізмів контролю є перевірка відповідності контрольованого об'єкта еталонному зразку. При цьому можуть використовуватися контрольні суми, а також низка інших ознак, таких як дата останньої модифікації об'єкта тощо. У разі необхідності дотримання строгої відповідності контрольованого об'єкта еталонному стану зазначені механізми можуть здійснювати автоматичне або автоматизоване (під керівництвом користувача або адміністратора безпеки) відновлення несанкціоновано зміненого файлового об'єкта з резервної копії. Під час розроблення згадуваної підсистеми були враховані специфічні особливості функціональних послуг безпеки у грід-середовищі (зокрема, контролю цілісності підлягають і системні компоненти, і програми й дані грід-користувачів).

Остання підсистема – виявлення вторгнень сигнатурного типу. Системи виявлення вторгнення (СВВ) є невід'ємними компонентами інформаційного захисту в сучасних комп'ютерних системах, у т.ч. розподілених.

---

[125] *Гильгурт С. Я.* Анализ вопросов контроля целостности информации в распределенных компьютерных сетях / С. Я. Гильгурт, А. Н. Давиденко, В. В. Душеба // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – Київ, 2011. – Вип. 60. – С. 42–46.

Через стрімке зростання обсягів мережевого трафіку при побудові таких систем також використовують апаратне прискорення із застосуванням реконфігуровних пристроїв на базі ПЛІС[126].

Залежно від методу аналізу подій розрізняють два класи СВВ: ті, що використовують сигнатури; ті, що виявляють аномалії. Системи першого класу аналізують потік даних на відповідність сигнатурам – унікальним описам набору подій, що однозначно характеризує конкретну атаку. Системи виявлення аномалій розкривають атаки, ідентифікуючи незвичайну поведінку користувачів, додатків або мережевих інтерфейсів, задля чого часто використовують статистичні методи.

Перевагою систем, що виявляють аномалії, є здатність ідентифікувати раніше невідомі атаки, але на практиці це спричиняє значну кількість помилкових спрацьовувань. До того ж, такі системи вимагають постійних зусиль з боку системних адміністраторів для коректного налаштування в динамічно змінюваних умовах, що робить їх непридатними для використання у складі СВБГС.

При апаратній реалізації СВВ на базі РУО застосовуються різні підходи. Найбільш відомими з яких є такі[127]:

- цифрові автомати;
- паралельні дискретні компаратори;
- пристрої асоціативної пам'яті та її різновиди;
- різні варіанти використання хеш-функцій, зокрема фільтру Блума.

Кожен зі згаданих підходів має і певні переваги перед іншими, і недоліки. Так, цифрові автомати, синтезовані у ПЛІС, не забезпечують високу пропускну спроможність, складні в побудові та конфігуруванні. Паралельні компаратори за більшої продуктивності призводять до підвищених витрат на устаткування та недостатньої масштабованості. Рішення, що базуються на асоціативній пам'яті, менш вимогливі до ПЛІС, ніж цифрові компаратори за сумарної продуктивності, але дорожчі та споживають більше енергії. Фільтр Блума і стискування бази сигнатур функціями хешування дають змогу зменшити кількість порівнянь, але за-

---

[126] *Коростиль Ю. М.* Принципы построения сетевых систем обнаружения вторжений на базе ПЛИС / Ю. М. Коростиль, С. Я. Гильгурт // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – Київ, 2010. – Вип. 57. – С. 87–94.

[127] *Давиденко А. Н.* Алгоритмы распознавания строк в системах обнаружения вторжений на ПЛИС / А. Н. Давиденко, С. Я. Гильгурт // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є.Пухова НАН України. – Київ, 2010. – Вип. 58. – С. 103–109.

безпечують імовірнісне розпізнавання, що вимагає додаткових витрат на доуточнення результатів збігу. Таким чином, жоден зі згаданих підходів не задовольняє вимогам, що пред'являються до сучасних систем виявлення вторгнення. Отже, наукова проблема побудови високопродуктивних СВВ вимагає подальшого вирішення.

На нашу думку, підсистема внутрішнього захисту інформації, побудована на основі запропонованих підходів, забезпечить потрібний ступінь захищеності оброблюваних даних, а також пришвидшить процедури закриття великих обсягів інформації, що дасть змогу розширити коло завдань, що вирішуються грід-центром із питань енергетики[128].

ПРОБЛЕМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ МІСТА КИЄВА

РОМАНЕЦЬ Микола Павлович,
директор з розвитку та інвестицій ПрАТ «СТЕК»

Нині у великих містах сконцентрована більшість продуктивних і людських ресурсів, тому їх стабільний розвиток стає дедалі більш визначальною умовою для функціонування держави. Своєю чергою, інженерна інфраструктура великих міст відіграє критичну роль для їх життєдіяльності. На прикладі м. Києва розглянемо питання розвитку інженерної інфраструктури міста, визначення пріоритетів, першочергових заходів із модернізації інфраструктурних об'єктів і мереж.

Завдання може бути сформульване так: створити систему, в якій навіть за умов виникнення критичних ситуацій з інженерною інфраструктурою негативні наслідки будуть мінімальними. Для цього розроблено «комунікаційний колектор» м. Києва, в межах якого розглядалися всі мережі, за винятком каналізації та газопостачання. На жаль, ця розробка залишилася на стадії концепції через відмову у фінансуванні. Яких результатів було досягнуто і які висновки зроблено під час цієї роботи?

Розпочнемо із системи електропостачання міста: можна стверджувати, що столиця на сьогодні дефіцитна за електропостачанням (за винятком одного житлового масиву – Троєщини), тобто подальше збільшення споживання без інженерних рішень є неможливим. Ми запропонували

---

[128] [Електронний ресурс]. – Режим доступу: http://www.ipme.kiev.ua/ukr/energrid.htm

вирішення цієї проблеми – схему «повного кільця 330кВ», будівництва нових підстанцій «Західна» та реконструкції підстанцій «Північна», «Новокиївська» та «Броварська», а також реконструкції відкритих майданчиків, на яких розташовані підстанції «110-330», на ТЕЦ-5 та ТЕЦ-6. Крім того, разом із Київенерго було створено проектну програму щодо функціонування 32 підстанцій 110кВ, яка, на жаль, була реалізована тільки на кількох підстанціях.

Схема газопостачання у столиці вже давно розбалансована. Весь лівий берег відділений від правого по газопостачанню, не завершено будівництво півкільця на півночі міста. Крім того, мережі високого тиску потрапили до сельбищної території, що є порушенням державних будівельних норм. Через невирішені проблеми газопостачання такі райони, як Березняки та Осокорки, що активно забудовуються, не мають достатнього газопостачання.

Якщо електропостачання знаходиться на критичній межі, то теплопостачання має дефіцит 1000 МВ (для порівняння – половина потужності ТЕЦ-5). Переважна частина правобережних районів міста залежить від ТЕЦ-5, і, за винятком Біличів і Теремків, є дефіцитною (за розрахункової температури – 22^0 С). Як вихід із ситуації – утеплення будинків, що, за нашими підрахунками, дасть змогу вдвічі зменшити споживання газу для теплопостачання, та встановлення локальних джерел теплопостачання там, де це просто необхідно.

Ще однією із критичних систем життєзабезпечення міста є система водопостачання, основними критичними точками якої є джерела (Дніпровська та Деснянська водоочисні станції). Протягом останніх тридцяти років збільшувалася пропускна спроможність мереж, а водопостачання, починаючи з 2000 р., зменшувалося. Як результат, у мережі не вистачає тиску, що призводить до негативних екологічних наслідків. Складна ситуація склалася з найбільшими насосними станціями – їх треба реконструювати.

Щодо каналізації міста, то основні проблеми пов'язані з Бортницькою станцією аерації. Варто нагадати, що 2/3 населення мешкають на правому березі р. Дніпро, а станція знаходиться на лівому; і на сьогодні з погляду техногенної небезпеки вона є критичним об'єктом для міста.

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ОЦІНКИ ТА ВРАХУВАННЯ РИЗИКУ В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ Й БЕЗПЕКИ ГРЕБЕЛЬ

СТЕФАНИШИН Дмитро Володимирович,
провідний науковий співробітник
Інституту телекомунікацій
і глобального інформаційного простору НАН України;

ТРОФИМЧУК Олександр Миколайович,
заступник директора Інституту телекомунікацій
і глобального інформаційного простору НАН України

Пропонуємо розглянути загальну характеристику гребель як об'єктів критичної інфраструктури, проаналізувати проблему аварійності на греблях та ознайомитися зі сформульованими методологічними підходами до оцінки та врахування ризику в завданнях забезпечення надійності й безпеки гребель як об'єктів підвищеної небезпеки.

Греблі є одними з найбільш розповсюджених інженерних споруд з-поміж об'єктів КІ і у світі загалом, і в Україні зокрема. За даними Міжнародної комісії з великих гребель (*ICOLD*), у світі побудовано та експлуатується понад 45 тис. лише т.зв. великих гребель різного типу і призначення, до яких належать споруди висотою 15 м і вище та греблі з водосховищами об'ємом не менше 1 млн м^3. Загальна кількість усіх гребель на Землі перевищує 800 тис.[129]; в Україні ж загальна кількість гребель сягає 1150 споруд[130].

Греблі як інфраструктурні об'єкти застосовуються в різних галузях народного господарства та сферах життєдіяльності людини і значною мірою визначають рівень соціально-економічного розвитку більшості країн світу. Майже всі розвинені країни світу в XX ст. переживали бум греблебудування на своїх територіях. Нині спостерігається нова хвиля масового будівництва у країнах, що стрімко розвиваються, зокрема у Бразилії, В'єтнамі, Китаї.

---

[129] *Hoeg K.* Dams: essential infrastructure for future water management / K. Hoeg // Hydropower and Dams, World Atlas and Industry Guide. – Aqua-Media International, UK, 2001. – 37 p.; *Гидроэнергетика* и окружающая середа / под общ. ред. Ю. Ландау и Л. А. Сиренко. – К. : Либра, 2004. – 484 с.

[130] *Яцик А. В.* Екологічна безпека в Україні / А. В. Яцик. – К. : Генеза, 2001. – 216 с.

Крім корисних ефектів, греблі містять небезпеку для довкілля та людини. Під час будівництва й експлуатації у значних об'ємах використовуються і трансформуються природні ресурси – територіальні й водні, екологічні, матеріальні тощо – зі значним екологічним впливом на навколишнє середовище[131]. У багатьох відношеннях потенційна небезпека для населення, яке проживає в нижніх б'єфах гребель, може бути не меншою, ніж для людей, що живуть біля атомних чи хімічних виробництв – об'єктів, з якими спеціалісти і громадськість зазвичай пов'язують проблеми техногенної безпеки[132].

У різних сферах використання гребель має такі корисні ефекти:

Соціально-економічні	Соціально-екологічні
• гідроенергетика (ГЕС, ГАЕС); • питне водопостачання; • промислове водопостачання; • водовідведення; • водоочищення; • водний транспорт; • іригація; • водосховища-охолоджувачі ТЕС, АЕС; • риборозведення; • транспортні переходи; • наливні ставкові господарства; • лісосплав	• рекреація; • водний спорт; • туризм; • екскурсії; • аматорське рибальство; • урбанізація територій; • боротьба з повенями; • рекультивація ландшафтів; • охорона природи; • охорона вод; • санітарні попуски; • меліорація

В історії світового греблебудування траплялися непоодинокі випадки аварій на греблях, у т.ч. й катастрофічних – із людськими жертвами. У табл. 1 наведено кілька прикладів найбільш відомих катастрофічних аварій на греблях, що сталися в різні роки в різних країнах світу, які можуть свідчити про значний аварійний потенціал гребель.

За статистичними даними, протягом останніх 150 років суттєві аварійні ситуації траплялися майже на кожній із 36 великих гребель, зареєстрованих *ICOLD*. При цьому майже на кожній зі 158 великих гребель аварії супроводжувалися проривами напірного фронту і майже на кожній із 76 руйнувань вдавалося уникнути лише завдяки екстреному (аварійному) спорожненню водосховищ[133].

---

[131] *Гидроэнергетика* и окружающая середа / под общ. ред. Ю. Ландау и Л. А. Сиренко. – К. : Либра, 2004. – 484 с.

[132] *Векслер А. Б.* Надежность, социальная и экологическая безопасность гидротехнических объектов: оценка риска и принятие решений / А. Б. Векслер, Д. А. Ивашинцов, Д. В. Стефанишин. – СПб. : ВНИИГ им. Б. Е. Веденеева, 2002. – 591 с.

[133] *ICOLD* Bulletin 99. Dam Failures : Statistical Analysis. – Paris, 1995. – 73 p.

При цьому важливою особливістю гребель (порівняно з іншими техногенними об'єктами, що ідентифікуються як об'єкти підвищеної небезпеки[134] й підпадають під дію Закону України «Про об'єкти підвищеної безпеки») є необхідність забезпечення неперервності їх експлуатації, навіть у випадках аварійних ситуацій, адже за аварійної ситуації греблю не можна автоматично вивести з експлуатації. У багатьох випадках греблі відіграють роль останнього резерву, здатного у форсованому режимі експлуатації відвернути техногенну катастрофу. Своєю чергою, аварійне спрацювання водосховища зі скидом наносів і забруднень, накопичених у ньому, може призвести до не менш катастрофічних наслідків, ніж власне руйнація гідроспоруди[135].

Таблиця 1

Приклади найвідоміших катастрофічних аварій на греблях

Рік аварії	Гребля (країна)	Тип греблі * / висота, м	Основні причини аварії	Кількість загиблих
1864	Дейл Дайк (Англія)	Гр/ 29,0	Перелив води через гребінь унаслідок повені	238
1889	Саус Форк (США)	Гр/ 21,5	Перелив води через гребінь унаслідок повені	2500
1911	Аустін (США)	Г/ 15,2	Втрата стійкості споруди	100
1923	Глено (Італія)	К/ 52,0	Втрата стійкості споруди	500
1928	Сент Френсіс (США)	Г/ 62,6	Руйнування основи греблі внаслідок хімічної суфозії	400
1959	Мальпасе (Франція)	А/ 66,0	Втрата стійкості берегового межування	421
1960	Оруш (Бразилія)	Гр/ 54,0	Перелив води через гребінь унаслідок несправності водоскиду	1000
1963	Вайонт (Італія)	А/ 262,0	Катастрофічний зсув у водосховище	2600
1967	Семпор (Індонезія)	Гр/ 54,0	Перелив води через гребінь унаслідок несправності водоскиду	200

[134] *Методика* ідентифікації потенційно небезпечних об'єктів / затверджена наказом МНС України від 23.02.2006 р. № 98. Зареєстровано в Міністерстві юстиції України від 20.03.2006 р. за № 286/12160 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/ http://zakon1.rada.gov.ua/laws/show/z0286-06

[135] *Яцик А. В.* До питання щодо спуску Київського водосховища / А. В. Яцик, Є. О. Яковлєв, В. О. Осадчук. – К. : Оріяни, 2002. – 52 с.

Закінчення табл. 1

Рік аварії	Гребля (країна)	Тип греблі * / висота, м	Основні причини аварії	Кількість загиблих
1972	Буфало Крик (США)	Ґр/ 32,0	Перелив води через гребінь унаслідок повені	125
1976	Титон (США)	Ґр/ 93,0	Суфозія на контакті тіла греблі з основою	11
1979	Мачху-2 (Індія)	Ґр/ 26,0	Перелив води через гребінь унаслідок несправності водоскиду	2000

* Греблі: Ґр – ґрунтові, Г – бетонні гравітаційні, А – аркові, К – контрфорсні

Як свідчить статистика, відносна частота аварій на греблях, особливо руйнівних, зі збільшенням кількості побудованих гребель поступово знижується. За даними *ICOLD*, статистична ймовірність аварій на великих греблях протягом XX ст. зменшилася у п'ять разів (із 0,05 до 0,01)[136]. Очікується подальше зниження ймовірності аварій на великих греблях навіть за збільшення їх кількості (рис. 1, 2). Однак, незважаючи на накопичений віками досвід вишукувань, проектування, розрахунків, будівництва й експлуатації гребель, удосконалення технологій, підвищення якості матеріалів, запровадження сучасних засобів автоматизації виробничих процесів, контролю й моніторингу стану споруд, підвищення загального рівня знань та інженерних рішень, аварії на греблях відбуваються й нині. Про це свідчить і аварія на Саяно-Шушенській ГЕС у 2009 р. у Росії, під час якої загинуло 75 осіб. Небезпека катастрофічних аварій на греблях не лише не відійшла в минуле, а й залишатиметься актуальною в майбутньому.

У документах *ICOLD*[137] ризик рекомендується оцінювати як математичне сподівання наслідків реалізації небажаної події (наприклад, як добуток імовірності реалізації негативної події на математичне сподівання величини наслідків цієї події) або як певну комбінацію ймовірностей реалізації подій і пов'язаних з ними наслідків. Відповідно, і необхідність

---

[136] *Hoeg K.* Dams: essential infrastructure for future water management / K. Hoeg // Hydropower and Dams. – 2001, World Atlas and Industry Guide. Aqua-Media International, UK. – 37 p.; *Векслер А. Б.* Надежность, социальная и экологическая безопасность гидротехнических объектов: оценка риска и принятие решений / А. Б. Векслер, Д. А. Ивашинцов, Д. В. Стефанишин. – СПб. : ВНИИГ им. Б. Е. Веденеева, 2002. – 591 с.

[137] *Risk* Assessment in Dam Safety Management : ICOLD Bulletin on Risk Assessment. – Paris, 2003. – 120 p.

оцінки та врахування ризику в задачах забезпечення надійності й безпеки гребель обумовлюють двома основними причинами, пов'язаними з невизначеністю: по-перше, даних щодо навантажень і впливів на споруди й недостатністю знань щодо їх реакцій на ці навантаження і впливи; по-друге, наслідків аварій на греблях.

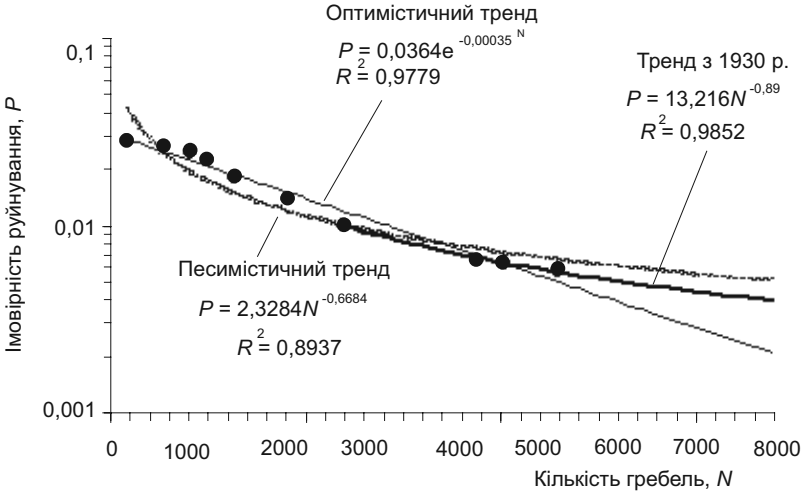


Рис. 1. Тренди очікуваної ймовірності руйнівних аварій на великих бетонних греблях залежно від їх кількості

У матеріалах IX Конгресу *ICOLD*[138] наводилися дані, згідно з якими матеріальні збитки від проривної повені оцінювалися від от 1 до 100 млн дол. США на 1 км^2 площі затоплень або від 1 до 10 дол. США на 1 м^3 води, що прориває́ться в нижній б'єф. За даними XX Конгресу *ICOLD*[139], загальні збитки від аварії на великій греблі можуть варіюватися від сотень мільйонів до десятків мільярдів доларів США. У середньому на 1 дол. США вартості греблі може припадати 10 дол. США лише прямих збитків від її прориву.

Аварії на греблях завжди відбувалися із цілком конкретних причин, і в багатьох випадках, як засвідчував аналіз причин їх виникнення, були

[138] *The behavior* and deterioration of dams : trans. of the 9-th Int. Congress on Large Dams. – Vol. 3. – Q. 34. – Istanbul–Turkey, 1967. – 758 p.

[139] *The use* of risk analysis to support dam safety decisions and management : trans. of the 20-th Int. Congress on Large Dams. – Vol. 1. – Q. 76. – Beijing–China, 2000. – 896 p.

неминучими. Однак навіть тоді, коли аварія на греблі була невідворотною, не всі чинники на момент її виникнення були відомими. Знання реальних причин аварії на одній греблі не завжди унеможливлювало аварію з тих самих причин на іншій споруді. Перевірочні розрахунки аварійних гребель за допомогою контрольних, більш «точних» методів (із використанням «ліпших» моделей тощо) часто засвідчували, що попередні розрахунки цих споруд здійснювалися за методами, не гіршими за контрольні. Здебільшого причина аварії полягала не стільки в неправильному виборі моделі споруди, розрахункового методу чи розрахункової схеми, скільки в неточності вхідних даних, зокрема в помилковому призначенні розрахункових значень показників властивостей матеріалів, ґрунтів, параметрів навантажень.

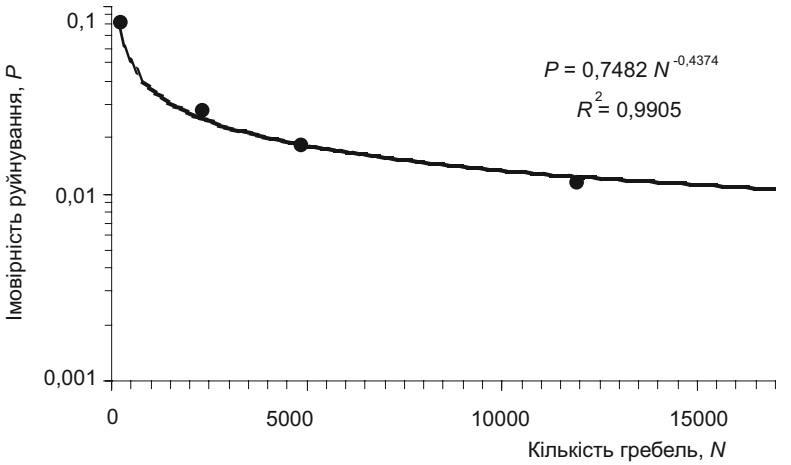


Рис. 2. Тренд очікуваної ймовірності руйнівних аварій на великих грунтових греблях залежно від їх кількості

Про невизначеність даних інженерно-геологічних досліджень професор де Мелло (Бразилія) на XX Конгресі *ICOLD* висловився як про «жахаючу диспропорцію між даними, що отримують за допомогою трьох дюймових свердловин, виконаних із кроком в десятки й сотні метрів, за переважно геометричної, з розміщенням свердловин у певному геометричному порядку, а не за геологічної орієнтації досліджень

ґрунтових товщ, та оцінками за цими даними стану масивів геологічних порід»[140].

Гідрологічні дослідження максимального стоку (одного з основних чинників безпеки гребель) свідчать, що при збільшенні тривалості спостережень не завжди можна отримати суттєве уточнення статистичних параметрів максимальних гідрологічних характеристик, а похибка визначення коефіцієнта асиметрії, що вказує на відмінність кривої розподілу ймовірності від нормального закону, при цьому може навіть зростати[141].

На рис. 3 продемонстровано результати прогнозування (на інтервалі до 1000 років) максимальних витрат води р. Дніпро у створі Київського гідровузла, яке виконувалося за допомогою різних функцій розподілу ймовірності, що враховують асиметрію. Показано, що залежно від закону розподілу одній і тій самій щорічній імовірності перевищення 0,1 % відповідають різні значення максимальної витрати, а прийнятому розрахунковому значенню максимальної витрати води – різні ймовірності перевищення. При цьому всі наведені закони розподілу ймовірності під час перевірки статистичних гіпотез за критерієм Пірсона χ^2 для рівня значущості 0,1 % виявилися гіпотезами, що погоджуються з емпіричними даними, а статистично «найліпшим» виявився розподіл Пірсона III типу для логарифмів.

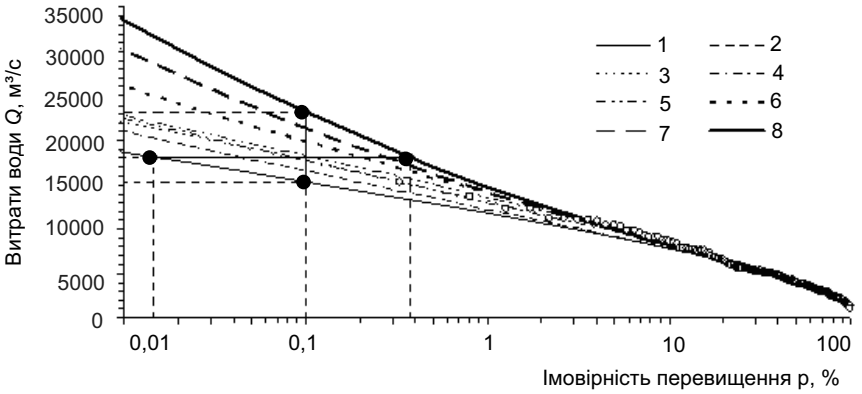
Невизначеність даних є типовою ситуацією під час вибору розрахункових значень для більшості характеристик, параметрів і показників, якими описують властивості матеріалів і ґрунтів гідроспоруд та їх основ, навантаження і впливи на греблі. При цьому невизначеність даних досить часто може призводити і до вибору неадекватних методів розрахунку, розрахункових схем і моделей.

Методологія оцінки та врахування ризику в задачах про забезпечення надійності і безпеки гребель. Адаптація поняття «ризик» при вирішенні задач, обтяжених невизначеністю, зазвичай ґрунтується на тій загальній у всіх визначеннях ідеї, що ризик включає невизначеність результату, невпевненість у майбутньому.

---

[140] *The use* of risk analysis to support dam safety decisions and management : trans. of the 20-th Int. Congress on Large Dams. – Vol. 1. – Q. 76. – Beijing–China, 2000. – 896 p.

[141] *Бортников Ю. А.* Гидрологические аспекты безопасности гидротехнических сооружений / Ю. А. Бортников // Гидротехническое строительство. – 2003. – № 9. – С. 31–33.



Розподіл імовірності: 1 – трипараметричний гама-розподіл Крицького-Менкеля ($C_V = 0{,}5;\ C_S = 2\ C_V$); 2 – те саме за ($C_V = 0{,}5;\ C_S = 2{,}5\ C_V$); 3 – Пірсона III типу (арифметичний); 4 – Гумбеля I типу; 5 – трипараметричний гама-розподіл Крицького-Менкеля ($C_V = 0{,}6;\ C_S = 2\ C_V$); 6 – те саме за ($C_V = 0{,}6;\ C_S = 2{,}5\ C_V$); 7 – логарифмічно нормальний; 8 – Пірсона III типу (логарифмічний); C_V – коефіцієнт варіації, C_S – коефіцієнт асиметрії.

Рис. 3. «Хрест невизначеності» прогнозування максимальних витрат води р. Дніпро (створ Київського гідровузла, гідрометричний пост «Вишгород») за допомогою різних аналітичних законів розподілу ймовірності

Джерело: Stefanyshyn D. V. Application of risk analysis to support safety of dams and flooded territories against floods / D. V. Stefanyshyn // Proc. of Int. Scientific School «Modelling and Analysis of Safety and Risk in Complex Systems». – S.-Petersburg, 2008. – P. 371–376.

Заходи, спрямовані на підвищення надійності й безпеки гребель, як і будь-яких інших потенційно небезпечних об'єктів, апріорі потребують додаткових затрат. Тому з погляду ефективності останніх вони мають виправдовуватися зниженням імовірних втрат (ризиків збитків) від аварій на цих об'єктах.

В умовах, коли роль економічного складника при вирішенні проблем, пов'язаних із безпекою життєдіяльності населення, зростає, основним

принципом обґрунтування рішень щодо техногенної безпеки, зокрема і гребель, може стати принцип розумно досяжного низького рівня ризику (*risk as low as reasonably practicable, ALARP*)[142]. Згідно із принципом *ALARP* підвищення надійності й безпеки потенційно небезпечних об'єктів необхідно погоджувати з економічними можливостями: рівні ризику аварій на греблях можуть вважатися прийнятними в усіх випадках, якщо вони є меншими за встановлену межу терпимості, і коли подальше їх зменшення стає або майже неможливим (за наявних економічних, технологічних та інших умов), або ціна такого зменшення стає непропорційно великою порівняно з отриманим при цьому підвищенням безпеки.

Принцип *ALARP* дає змогу враховувати складну природу ризику аварій на греблях як об'єктивно-суб'єктивної категорії: не лише як очікування можливої розплати за нехтування небезпекою аварії, а і як нехтування можливою вигодою, яку можна отримати від переборення страху перед цією небезпекою. При цьому зниження ймовірних втрат від можливої аварії на греблі можна розглядати як майбутній ефект, а додаткові затрати на заходи щодо забезпечення надійності й безпеки греблі варто трактувати як складники ризику.

Під час прийняття рішень принцип *ALARP* щодо оцінювання заходів із забезпечення надійності й безпеки гребель можна повною мірою застосувати в межах запропонованого методу оцінки повного ризику альтернатив на основі їх парного порівняння з урахуванням ризику невикористаних можливостей[143].

Повний ризик варіанта щодо тих чи інших заходів (альтернативи), спрямованих на забезпечення надійності й безпеки греблі, при цьому міститиме два складники:

• власний ризик *i*-ї альтернативи, що формується додатковими порівняно з певним базовим (нульовим) варіантом узагальненими приведеними затратами $\Delta C_i - C_0$ на реалізацію відповідних заходів;

• ризик невикористаних можливостей, що визначається додатковим порівняно з базовим варіантом зниженням імовірних втрат (ризиків збитків) від аварії на греблі $\Delta L_j\, L_0 - L_j$ за альтернативних *j*-х заходів.

---

[142] *Маршалл В.* Основные опасности химических производств / В. Маршалл. – М. : Мир, 1989. – 672 с.

[143] *Stefanyshyn D. V.* A method of decision making at risk in natural resources use by pairwise comparison of alternatives with taking account of risks of lost opportunities / D. V. Stefanyshyn, Y. D. Stefanyshyna // Proc. of Int. Scientific School «Modelling and Analysis of Safety and Risk in Complex Systems». – S.-Petersburg, 2009. – P. 435–439.

Повний ризик *i*-ї альтернативи при її порівнянні з *j*-ю при цьому буде:

$$R_{ij} = \Delta C_i + \Delta L_j ; \quad (1)$$

відповідно повний ризик *j*-ї альтернативи порівняно з *i*-ю:

$$R_{ji} = \Delta C_j + \Delta L_i . \quad (2)$$

де $\Delta C_i = C_i - C_0$, $\Delta L_j = L_0 - L_j$, $\Delta C_j - C_0$, $\Delta L_i = L_0 - L_i$;
C_0, C_i, C_j – узагальнені приведені затрати на реалізацію відповідних альтернатив;
L_0, L_i, L_j – імовірні втрати (ризики збитків) при аварії тощо.

При цьому ймовірні втрати при аварії L_0, L_i, L_j можуть визначатися через добутки ймовірностей аварії на греблі та збитків, пов'язаних із наслідками аварії[144].

Рис. 4 містить фрагмент таблиці рішень для порівняння різних заходів m_i, m_j, спрямованих на забезпечення надійності й безпеки греблі, за ризиком при $C_0 = 0$.

$m_i \backslash m_j$	m_0	...	m_i	m_j	...
m_0	–	...	ΔL_i	ΔL_j	...
...	...	–	...	...	...
m_i	C_i	...	–	$C_i+\Delta L_j$	...
m_j	C_j	...	$C_j+\Delta L_i$	–	...
...	...	...	...	...	–

Рис. 4. Фрагмент таблиці рішень $||R_{ij}||$ при $C_0 = 0$

Залежно від кількості (n) альтернативних заходів для кожного з варіантів може задаватися $n-1$ значень повного ризику R_{ij}, $i, j = \overline{0,n}$, $i \neq j$. Таблицю рішень (рис. 4) зручно будувати з упорядкуванням альтернатив m_i, i= $\overline{0,n}$ за зростанням затрат ΔC_i. У результаті попарного порівняння альтернатив, починаючи з пари (m_0, m_1) з ризиками $R_{0,1}$, $R_{1,0}$ відповідно і так далі, з відбором на кожному кроці варіанта з меншим повним ризиком R_{ij}, може бути підібраний такий варіант забезпечення надійності й

[144] *The use* of risk analysis to support dam safety decisions and management. Trans. of the 20-th Int. Congress on Large Dams. – Vol. 1. – Q. 76. – Beijing-China, 2000. – 896 p.; *Стефанишин Д. В.* Прогнозування аварій на греблях в задачах оцінки й забезпечення їх надійності та безпеки / Д. В. Стефанишин // Гідроенергетика України. – 2011. – № 3-4. – С. 52–60.

безпеки греблі, який отримуватиме менший ризик при попарному його порівнянні з усіма альтернативами, що розглядаються у процесі прийняття рішення.

Висновки

1. Цінність досліджень ризику виявляється насамперед при розв'язанні задач прийняття рішень в умовах невизначеності, причому потреба в коректних, адекватних оцінках ризику виникає тільки з усвідомленням того, що врахування ризику при прийнятті рішення сприяє розкриттю невизначеності, а вирішення задачі з ризиком передбачає наявність альтернатив і свободу вибору.

2. Дослідження ризику варто розглядати як процес, що повторюється, коли надходить нова інформація, виникає нова задача. Знання ризиків допомагає сформулювати альтернативи, здатні ефективно знижувати ідентифіковані ризики, оскільки наявні ресурси для забезпечення безпеки греблі зазвичай обмежені, а це може вплинути на поточний стан греблі, стан інших споруд гідровузла (насамперед водоскидних споруд), готовність персоналу виконувати необхідні функції в нештатній ситуації тощо. Можуть обмежуватися обсяги фінансування, час. У кожному з випадків вибір на користь того або іншого рішення може бути зроблений з урахуванням пріоритету різних ризиків.

3. Із новими даними оцінки ризику модифікуються, виявляються нові визначальні чинники й параметри. Ефективність заходів, спрямованих на зменшення ризику, оцінюється при співставленні ризиків, що прогнозуються до і після запровадження відповідних заходів. У такому вигляді дослідження стають інтегральним складником процесу забезпечення надійності й безпеки греблі.

4. Запропоновані методологічні підходи до оцінки й урахування ризику дають змогу формалізувати процес прийняття рішень щодо заходів, спрямованих на забезпечення надійності й безпеки гребель, з урахуванням різних чинників ризику: чинників, з якими пов'язуються безпосередні затрати на відповідні заходи (а ці затрати, безперечно, також є чинниками ризику), і чинників, з якими можуть пов'язуватися невикористані можливості, заради чого, власне, заходи й мають здійснюватися. Зрештою, такий підхід стимулюватиме отримання адекватних кількісних оцінок ризиків аварій на греблях, адже саме у процесі прийняття рішень оцінки ризиків набувають реального практичного значення.

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ВЗАЄМОЗВ'ЯЗКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЗАСЛАВСЬКИЙ Володимир Анатолійович,
професор кафедри математичної інформатики
факультету кібернетики
Київського національного університету
імені Тараса Шевченка

Забезпечення безпеки суспільства й держави нині значною мірою залежить від функціонування об'єктів критичної інфраструктури. Згідно із Зеленою книгою, опублікованою Європейською Комісією 2005 р.[145], до КІ мають бути віднесені основні об'єкти енергетики, транспорту, зв'язку та ІТ, хімічної промисловості, життєзабезпечення та охорони здоров'я, дослідницькі центри, урядові та правоохоронні структури. Для таких об'єктів характерною є висока складність, вони є масштабними системами із високою ціною відмови, а їх функціонування впливає на національну економіку, безпеку, стан навколишнього середовища, функціонування установ і життєдіяльність населення країни.

Окремі об'єкти КІ є взаємопов'язаними і фізично (комп'ютерними мережами, забезпеченням електроенергією, транспортними перевезеннями), і різноманітними організаційними регламентами[146]. Прийнято розглядати такі чотири основні види взаємозалежностей між об'єктами КІ[147]:

• *фізична* (від поставок матеріалів чи надання послуг);

• *інформаційна* (від командних сигналів, управління, передачі даних, геопозиціонування тощо);

• *геопросторова* (між територіально розподіленими елементами КІ, що виникають безпосередньо через близьке просторове розміщення об'єктів);

---

[145] *Green* Paper of 17 November 2005 on a European programme for critical infrastructure protection (COM(2005) 576 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[146] *Lewis T .G.* Critical infrastructure protection in homeland security: defending a networked nation / T. G. Lewis. – John Wiley & Sons, Inc., 2006. – 474 p.

[147] *Rinaldi S.* Identifying, understanding and analyzing critical infrastructure interdependencies / S. Rinaldi, J. Peerenboom, T. Kelly // IEEE Control Systems. – 2001. – № 21(6).– P. 11–25.; *Robert B.* Modelling interdependencies among critical infrastructures / B. Robert, R. De Calan, L. Morabito // Int. J. of CI. – 2008. – № 4. – P. 392–408.

• *логічна* (взаємозалежність, яка виникає через нормативні регламенти).

Фахівці підкреслюють те, що саме необхідність урахування багатьох відмов і каскадних ефектів спричиняє неможливість точної оцінки наслідків непрацездатності об'єктів КІ, а отже, знижує точність оцінки ризиків відмови таких об'єктів[148]. Так, британські дослідники, розглядаючи дві найзначніші надзвичайні ситуації, що відбулися на території Великої Британії за останнє десятиріччя (повені 2007 р., пожежа та вибухи в м. Банчфілд), зазначають, що неможливо простежити всі каскадні ефекти. Зокрема, під час повеней були автоматично відключені мережі електропостачання, а внаслідок другої надзвичайної ситуації було пошкоджено устаткування ІТ-компанії, на якому зберігалася інформація про картки медичного обслуговування на загальну суму 1,4 млрд фунтів стерлінгів[149].

Прикладом масштабних аварій на об'єктах КІ та каскадних ефектів, спричинених ними, є відмова мережі енергопостачання в північно-східних штатах США та східних провінціях Канади, що сталися у 2003 р. В офіційному звіті комісії з розслідування причин і наслідків цієї аварії зазначається, що саме помилки при регулюванні в мережі електроенергетики спричинили аварійну ситуацію, яка викликала низку негативних наслідків для економіки, безпеки та соціального добробуту населення[150]. Розслідування причин каскадних аварій свідчить про те, що для їх запобігання потрібні спеціальні методи (технологічні та організаційні), подібно до того, як використовується резервування (структурне, функціональне та резервування за часом), що є методом забезпечення (підвищення) надійності складних технічних систем.

Через значну складність взаємозв'язків між елементами КІ та її системами потрібні спеціалізовані математичні інструменти (моделі та алгоритми) для їх адекватного опису, здійснення аналізу та моделювання безпеки. Системним є підхід, що отримав назву «системи, що склада-

---

[148] *Cozzani V.* The assessment of risk caused by domino effect in quantitative area risk analysis / V. Cozzani, G. Gubinelli, G. Antonioni, G. Spadoni [at al.] // J. Hazardous Materials. – 2005. – No.127. – P. 14–30.

[149] *Bloomfield R.* UK Interdependency Analysis feasibility study: the present and future state of research and practice / R. Bloomfield, N. Chozos // European CIIP Newsletter. – 2008. – № 4(3). – P. 17–20.

[150] *Blackout* in the United States and Canada: Causes and Recommendations : final report on the August 14, 2003 / U.S.–Canada Power System Outage Task Force. – 2004. – April [Електронний ресурс]. – Режим доступу: https://reports.energy.gov/BlackoutFinal-Web.pdf

ються із систем» (*system-of-systems*)[151]. Використання принципу ієрархії при структурному представленні моделі складної системи дають змогу здійснювати декомпозицію до рівня підсистем (модулів, елементів), які, своєю чергою, теж розглядаються як складні системи. При такому розгляді об'єктів КІ моделі й методи аналізу ризику для системи загалом та її елементів є однаковими й узгодженими.

Функціонування об'єктів КІ, а також характер впливу на них зовнішніх і внутрішніх чинників часто не можуть бути описані на основі детермінованих моделей. Тому при моделюванні взаємодії елементів та об'єктів КІ застосовуються методи статистичного моделювання[152]. Разом з тим інформація про характер загроз об'єктам КІ нерідко або взагалі відсутня, або знаходиться під грифом «таємно», а її обсяг недостатній для проведення достовірних статистичних розрахунків[153].

Кожна галузь економіки, до якої належать ті чи інші об'єкти КІ, привносить свої специфічні риси, які необхідно враховувати під час моделювання взаємозв'язків між об'єктами КІ. Зокрема, проаналізовано моделі, використовувані при дослідженні об'єктів енергетичної інфраструктури[154]. Окремо розглянуто взаємозв'язки між різними секторами КІ, наприклад між телекомунікаційними системами й електромережами[155].

Дослідженню й моделюванню каскадних аварій приділяється значна увага у спеціалізованій вітчизняній науковій літературі[156]. Каскадні аварії виникають через автоматичне відключення одних пристроїв чи підсистем унаслідок відмов інших. Така вбудована логіка у багатьох технічних системах військового й цивільного призначення дає змогу уникати перевантаження приладів, економити електроенергію тощо.

---

[151] *Eusgeld I. «*System-of-systems» approach for interdependent critical infrastructures / I. Eusgeld, C. Nan, S. Dietz // Reliab. Eng-ng & Sys. Safety. – 2011. – 96(6). – P. 679–686.

[152] *Pederson P.* Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research / P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann. – Idaho National Laboratory. – U.S. Department of Energy, 2006. – 116 p.

[153] *Paté-Cornell M. E.* Risk and Uncertainty Analysis in Government Safety Decisions / M. E. Paté-Cornell // Risk Analysis. – 2002. – 22(3). – P. 633–646.

[154] *Yusta J. M.* Methodologies and applications for critical infrastructure protection: State-of-the-art / J. M. Yusta, G. J. Correa, R. Lacal-Arantegui // Energy Policy. – 2011. – 39. – P. 6100–6119.

[155] *Beccutia M.* Quantification of dependencies between electrical and information infrastructures / M. Beccutia, S. Chiaradonnac, F. Di Giandomenicoc, S. Donatellia, G. Dondossolad [et al] // Int. J. Critical Infrastructure Protection. – 2012. – Vol. 5. – P. 14–27.

[156] *Безопасность* критических инфраструктур: математические и инженерные методы анализа и обеспечения / под ред. Харченко В. С. – Харьков : МОНУ, Нац. аэрокосм. ун-т «ХАИ». – 2011. – 641 с.

Аналізувати взаємозв'язки між об'єктами й елементами КІ неможливо без застосування спеціалізованого програмного забезпечення. Важливу роль у процесі аналізу об'єктів КІ відіграють засоби візуалізації[157]. Можна виокремити такі програмні засоби, як ГІС, що застосовуються для аналізу та візуалізації у просторі й часі залежностей між елементами КІ[158]. Із низкою програмних продуктів, розроблених для вирішення таких задач, можна ознайомитися на веб-сторінках відомої Лос-Аламоської національної лабораторії[159] та Дослідницького центру з питань оборони та безпеки Школи підвищення кваліфікації офіцерського складу ВМС США[160].

Корисним для опису взаємозв'язків у складних структурах є застосування різноманітних засобів формального опису мережевих моделей, зокрема відкритого стандарту (*IEEE High Level Architecture standard* 1516), розробленого в Інституті інженерів з електротехніки та радіоелектроніки[161].

Необхідно також брати до уваги те, що моделювання взаємозв'язків є лише складником оцінки ризиків об'єктів і систем КІ. Тому, крім взаємозв'язків між самими об'єктами критичної інфраструктури, потрібно розглядати зв'язки із чинниками зовнішнього середовища, що впливають на функціонування об'єктів КІ, та зв'язки із показниками, за якими оцінюється вплив стану функціонування КІ на економіку, стан навколишнього середовища та соціальну сферу[162].

---

[157] *Tolone W. J.* Interactive visualizations for critical infrastructure analysis / W. J. Tolone // Int. J. Critical Infrastructure Protection. – 2009. – Vol.2. – P. 124–134.

[158] *Robert B.* The operational tools for managing physical interdependencies among critical infrastructures / B. Robert, L. Morabito // Int. J. of Critical Infrastructures. – 2008. – № 4(4). – P. 353–367.

[159] *National* Infrastructure Simulation and Analysis Center [Електронний ресурс]. – Режим доступу: http://www.lanl.gov/programs/nisac/

[160] *SIMULATIONS*: CIP Simulations, Tools and Software [Електронний ресурс]. – Режим доступу: https://www.chds.us/?media/resources&collection=53&type=SIMULATION

[161] *Nan C.* Adopting HLA standard for interdependency study / C. Nan, I. Eusgeld // Reliab. Eng-ng & Sys. Safety. – 2011. – Vol.96. – P. 149–159.

[162] *Biriukov D.* Risk models for critical infrastructute protection planning / D. Biriukov, V. Zaslavkii // Problems of Decision Making under Uncertainties : XX Int. Conf. (September 17–21, 2012, Brno, Czech Rep). – P. 23–24.

ОЦІНКА ВРАЗЛИВОСТІ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПОСТАНОВКА ПИТАННЯ

КОНДРАТОВ Сергій Іванович,
старший науковий співробітник
Національного інституту стратегічних досліджень

У зв'язку із глобальним процесом зростання терористичних загроз на сьогодні одним із пріоритетних завдань є забезпечення високого рівня захищеності критично важливих для тієї чи іншої держави систем, об'єктів і ресурсів, які найчастіше об'єднують терміном «*критична інфраструктура»* (КІ), рідше – «*критично важливі об'єкти»* (КВО). Основною ознакою елементів КІ або об'єктів, віднесених до КВО, є те, що їх відмова або виведення з ладу можуть призвести до важких або навіть катастрофічних наслідків для економіки, соціального добробуту населення та стабільності політичної системи держави[163].

Для забезпечення *захищеності* або *фізичної безпеки* елементів КІ та об'єктів, віднесених до КВО, створюють системи фізичного захисту (СФЗ), кожна з яких є сукупністю організаційно-правових, оперативно-розшукових та інженерно-технічних заходів, зокрема використання інженерно-технічних засобів (ІТЗ), і призначена для зведення до прийнятного мінімуму ризику здійснення терористичного нападу або акту тероризму.

Оцінка ризику тероризму є необхідним елементом створення ефективної СФЗ. За твердженням одного із провідних експертів США у цій сфері, «є аксіомою тероризму, що терористи можуть атакувати будь-що, будь-де і в будь-який момент, тоді як уряди не мають можливості захищати все, всюди і весь час»[164]. При побудові СФЗ, зважаючи на обмеженість ресурсів, постає необхідність у визначенні пріоритетних з погляду захисту об'єктів, а також того, що, своєю чергою, доцільно виконувати, спираючись на оцінку ризиків реалізації тих чи інших загроз.

---

[163] *Моторный И. Д.* Современный терроризм и оценка диверсионно-террористической уязвимости гражданских объектов / И. Д. Моторный. – М. : Изд-во И. И. Шумилова, 2004. – 104 с.

[164] *Jenkins Brian Michael.* New Challenges to U.S. Counterterrorism Efforts, Testimony presented before the Senate Homeland Security and Governmental Committee on July11, 2012 / Brian Michael Jenkins // RAND Co. [Електронний ресурс]. – Режим доступу: http://www.rand.org/pubs/testimonies/CT377.html

У публікації *RAND Co*[165] ризик тероризму пропонується розглядати як такий, що має *три компоненти*:

• загрозу можливій цілі терористів (англ. – *the threat to a target*);

• уразливість можливої цілі стосовно цієї конкретної загрози (англ. – *target's vulnerability*);

• наслідки (англ. – *consequences*) у випадку, якщо згадана ціль буде успішно атакована терористами.

Відповідно до цього підходу ризик – це передбачувані (очікувані) наслідки упродовж певного періоду часу для певного типу цілей, які можуть мати місце в результаті реалізацій певного набору загроз. Для конкретної загрози, конкретного об'єкта (цілі) й типу наслідків ризик можна визначити за такою формулою:

$$R=P_З \times Pв \times C_{Н,}$$

де R – ризик;

$P_З$ – загроза (ймовірність здійснення нападу);

Pв – вразливість (ймовірність того, що напад призведе до шкоди у випадку його здійснення);

$C_Н$ – наслідки (коефіцієнт, що характеризує величину й категорію шкоди у випадку здійснення такого нападу).

Таким чином, відповідно до запропонованого *RAND Co* підходу, величина уразливості є ймовірністю того, що в результаті певного нападу терористів даному об'єкту буде завдано шкоду певної категорії. Категорії шкоди можуть включати смерті, поранення, пошкодження власності або інші матеріальні втрати, що мали місце в конкретний проміжок часу.

Більш загальні моделі (часто використовуються при аналізі у військовій сфері) враховують наявність цілого діапазону рівнів шкоди, для кожного з яких існує своя ймовірність при визначенні уразливості.

Зважаючи на викладене, можна стверджувати, що уразливість того чи іншого об'єкта з погляду терористичної загрози є однією з основних характеристик контртерористичної захищеності елемента КІ або КВО, а її оцінка є одним із суттєвих етапів оцінки ризику терористичного нападу.

Оцінка вразливості (ОВ) СФЗ дається з використанням таких інструментів, як аналіз документації, тренування та навчання, експертне оцінювання, комп'ютерне моделювання, випробування ІТЗ у різних їх ком-

---

[165] *Willis Henry H.* Estimating Terrorism Risk / Henry H. Willis [et al.] // RAND Corporation. – Santa-Monica, CA, U.S. – 2005.

бінаціях[166]. При цьому роботи з ОВ характеризуються високою вартістю. Наприклад, у США витрати на виявлення вразливостей об'єктів і підготовку рекомендацій щодо їх усунення коштують операторам у середньому від 50 до 100 тис. дол. США[167].

Стосовно комп'ютерного моделювання СФЗ, то модулі ОВ здебільшого є частиною програмних продуктів, широко використовуваних у створенні сучасних СФЗ, і базуються на використанні математичних методів моделювання сценаріїв загроз[168]. Зрозуміло, що під час розроблення сценаріїв реалізації загроз необхідно враховувати конкретні умови, в яких можуть розгортатися події, у т.ч. розподіл повноважень і відповідальності при забезпеченні фізичного захисту об'єкта, наявність відповідних ресурсів, процедури реагування на надзвичайні події, пов'язані з фізичною безпекою, чинну нормативно-правову базу, на основі якої діють державні органи та оператори.

Щодо нашої країни, то тут необхідно згадати, що в Україні діє Положення, на основі якого здійснюється ОВ ядерних установок і ядерних матеріалів, які беззаперечно належать до категорії об'єктів КІ[169]. Тобто в нашій країні при розробці методів і процедур ОВ елементів КІ для інших секторів є можливість використання напрацювань ядерної галузі.

Загалом з-поміж методів ОВ СФЗ найпопулярнішими є ті, що базуються на підході, який визначає характеристики системи з погляду виконання основних цілей СФЗ (*a system performance-based approach to meeting the PPS objectives*), до яких відносять виявлення (*detection*), затримку (*delay*) та реагування (*response*)[170]. Кожній із перерахованих цілей відповідає певна функціональна підсистема СФЗ. Для оцінки функціонування компонент СФЗ об'єкта використовують і кількісний, і якісний методи. Як зазначає М. Л. Гарсіа, перший із вказаних методів зазвичай

---

[166] *Garcia M. L.* Vulnerability assessment of physical protection systems / M. L. Garcia. – Butterworth-Heinemann, 2005. – 382 p.

[167] *AVERT* evaluates vulnerabilities, assess solutions // Homeland Security NewsWire. – 2011. – January [Електронний ресурс]. – Режим доступу: http://homelandsecuritynewswire.com

[168] *Боровский А. С.* Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов / А. С. Боровский, А. Д. Тарасов // Труды ИСА РАН. – 2011. – Т. 61(1). – С. 3–13.

[169] *Про затвердження* Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів : наказ Державного комітету ядерного регулювання від 30.11.2010 р. № 169 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/z1309-10

[170] *Garcia M. L.* Vulnerability assessment of physical protection systems / M. L. Garcia. – Butterworth-Heinemann, 2005. – 382 p.

використовують для об'єктів і систем, що характеризуються дуже важкими наслідками при виведенні їх із ладу, тоді як другий є прийнятним для об'єктів, цінність яких є значно нижчою[171].

При ОВ загальним завданням є оцінити функціонування кожного компонента СФЗ, встановленого на об'єкті. Коли це виконано, здійснюється оцінка функціонування системи загалом. При використанні кількісних методів перевіряються значення функціональних параметрів СФЗ, тоді як при використанні якісних методів результатом оцінки ефективності функціонування компонента є така її характеристика, як «висока», «середня» або «низька».

При всій складності завдань, що постають під час ОВ елементів КІ або КВО, варто зазначити, що, на відміну від оцінки терористичних загроз, у цьому процесі можуть бути використані вже розроблені моделі та розрахунки для природних і техногенних надзвичайних ситуацій, що дещо спрощує ситуацію. З огляду на увагу, яка приділяється проблемі ОВ елементів КІ та КВО у провідних країнах світу, Україні необхідно не менш активно проводити дослідження у цій сфері задля посилення науково-методологічної підтримки контртерористичних заходів на національному рівні.

РЕАЛІЗАЦІЯ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАХОДІВ ЦИВІЛЬНОГО ЗАХИСТУ В МІСТОБУДІВНІЙ І ПРОЕКТНІЙ ДОКУМЕНТАЦІЇ ЯК ЕФЕКТИВНИЙ МЕХАНІЗМ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЕЩЕНКО Олександр Якович,
головний спеціаліст
Державної служби України з надзвичайних ситуацій

Аналіз виникнення й розвитку надзвичайних ситуацій (НС), що мали місце на території нашої держави та у світі, свідчить про необхідність здійснення комплексу превентивних заходів щодо зниження ризику їх виникнення, а також захисту населення, об'єктів і територій (передусім об'єктів КІ) від їх наслідків. Здійсненням комплексу запобіжних організаційних та

[171] *Garcia M. L.* Vulnerability assessment of physical protection systems / M. L. Garcia. – Butterworth-Heinemann, 2005. – 382 p.

інженерно-технічних заходів, їх ефективною реалізацією можна значно зменшити вірогідність виникнення НС і мінімізувати вартість заходів з ліквідації їх наслідків, підвищити рівень готовності персоналу й виробництва об'єктів КІ до функціонування в умовах НС. Науковими розрахунками та існуючим досвідом доведено, що кошти, які направляються на реалізацію цих заходів, значно менші за необхідні на ліквідацію наслідків НС.

Зважаючи на важливість проблеми протидії можливим техногенним аваріям і катастрофам, стихійним лихам, органами державної влади останнім часом розроблено та введено в дію низку законодавчих і нормативних документів, які регламентують основні аспекти проблеми стійкого функціонування об'єктів КІ в умовах НС. Нині в Україні діє низка законодавчих, нормативно-правових актів і методичних документів, що регламентують вимоги стосовно виконання заходів щодо попередження НС, організації інженерного захисту населення й територій. Так, ст. 34 Кодексу цивільного захисту передбачено реалізацію низки заходів інженерного захисту територій, з-поміж яких:

• розроблення та включення вимог інженерно-технічних заходів цивільного захисту до відповідних видів містобудівної та проектної документації, їх реалізація під час будівництва й експлуатації;

• розміщення об'єктів підвищеної небезпеки з урахуванням наслідків аварій, що можуть статися на таких об'єктах;

• розроблення та вжиття заходів щодо безаварійного функціонування об'єктів підвищеної небезпеки;

• будівництво споруд, будівель, інженерних мереж і транспортних комунікацій із заданими рівнями безпеки та надійності.

Найбільш ефективними та перспективними для розвитку є заходи, що реалізуються на етапі розроблення містобудівної документації, проектування й будівництва об'єктів, у т.ч. об'єктів КІ. Основним складником цих заходів є *інженерно-технічні заходи цивільного захисту* (ІТЗ ЦЗ) – комплекс інженерно-технічних рішень, спрямованих на запобігання виникненню НС, забезпечення захисту населення й територій від них і небезпеки, що може виникнути під час воєнних (бойових) дій або внаслідок таких дій, а також створення умов для забезпечення сталого функціонування суб'єктів господарювання й територій.

У главі 4 ст. 34 Кодексу цивільного захисту визначено, що «розроблення містобудівної документації та проектування об'єктів, що належать суб'єктам господарювання і можуть спричинити виникнення надзвичайних ситуацій та вплинути на стан захисту населення і територій, здій-

снюються з урахуванням вимог інженерно-технічних заходів цивільного захисту»[172].

Відповідно до глави 5 цього Кодексу об'єкти, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту, визначаються Кабінетом Міністрів України. Проект відповідної постанови Кабінету Міністрів України розроблено Державною службою України з надзвичайних ситуацій, погоджено із зацікавленими центральними органами виконавчої влади та у листопаді 2013 р. внесено на розгляд уряду. Із проектом цього нормативного акта можна ознайомитися на офіційному сайті ДСНС України[173].

Відповідно до зазначеного проекту нормативного акта до переліку об'єктів, проектування яких здійснюється з урахуванням вимог ІТЗ ЦЗ, відносяться:

• об'єкти, що можуть спричинити виникнення надзвичайних ситуацій техногенного та природного характеру і вплинути на стан захисту населення й територій;

• об'єкти національної економіки, що забезпечують стійке (або стале) функціонування держави в умовах надзвичайних ситуацій техногенного та природного характеру і в особливий період;

• інші об'єкти національної економіки, що належать до відповідної категорії із цивільного захисту згідно із законодавчо визначеним Порядком[174].

Тобто це об'єкти, що підпадають під визначення «критична інфраструктура», причому в тому розумінні даного терміна, яке прийнято в розвинених країнах світу: «системи та об'єкти, фізичні чи віртуальні, настільки важливі для держави, що їх недієздатність або знищення загрожують національній безпеці, економіці, здоров'ю або безпеці життєдіяльності населення»[175].

---

[172] *Кодекс* цивільного захисту України [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/5403-17

[173] *Про затвердження* переліку об'єктів, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту : проект постанови Кабінету Міністрів [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/public_discus.html

[174] *Про затвердження* Порядку віднесення суб'єктів господарювання до категорій цивільного захисту : постанова Кабінету Міністрів України від 2.03.2010 р. № 227 (для службового користування).

[175] *Бірюков Д. С.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні : аналіт. доп. / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 102 с.

У разі розроблення ІТЗ ЦЗ включення їх до проектів будівництва цих об'єктів та реалізації при їх спорудженні створюється необхідна інфраструктура організаційних та інженерно-технічних заходів, що дають змогу протидіяти техногенній небезпеці, стихійним лихам, іншим ризикам та ефективно ліквідовувати наслідки НС, захищати персонал і населення, а також забезпечувати стале функціонування об'єктів критичної інфраструктури в цих умовах.

Зміст і конкретні вимоги щодо розроблення ІТЗ ЦЗ у містобудівній і проектній документації викладено в нормативних документах, введених у дію Міністерством регіонального розвитку та будівництва відповідно до вимог Закону України «Про державні будівельні норми»[176], а саме:

• ДБН В.1.2-4-2006 «Інженерно-технічні заходи цивільного захисту (цивільної оборони)»;

• ДБН Б.1.1-5-2007 «Склад, зміст, порядок розроблення, погодження та затвердження розділу інженерно-технічних заходів цивільного захисту (цивільної оборони) в містобудівній документації»;

• ДСТУ Б А.2.2-7:2010 «Розділ інженерно-технічних заходів цивільного захисту (цивільної оборони) у складі проектної документації об'єктів. Основні положення».

Варто детальніше розглянути проектні рішення ІТЗ ЦЗ, визначені ДСТУ Б А.2.2-7:2010, залежно від економічної значимості об'єкта, а також його потенційної небезпеки. Вони зазвичай складаються із двох частин:

• проектні рішення у сфері цивільного захисту, що розробляються з урахуванням розміщення виробничих сил і розселення населення, відповідних груп міст і категорій об'єктів із цивільного захисту щодо зон можливих небезпек, а також необхідності створення містобудівних умов для забезпечення стійкого функціонування цих об'єктів;

• проектні рішення щодо попередження надзвичайних ситуацій техногенного та природного характеру, які розробляються з урахуванням потенційної небезпеки на об'єкті, що проектується, а також на поряд розташованих об'єктах, і результатів інженерних вишукувань, оцінки природних умов і навколишнього середовища.

До розділу ІТЗ ЦЗ у складі проектної документації всіх об'єктів включаються:

---

[176] *Про державні* будівельні норми : закон України від 5.11.2009 р. № 1704-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1704-17

• обґрунтування віднесення об'єкта до відповідної категорії із цивільного захисту;

• визначення меж зон можливої небезпеки, передбачених ДБН В.1.2–4;

• обґрунтування відстані об'єкта від категорованих міст та об'єктів із цивільного захисту, зон катастрофічного затоплення від прориву гідротехнічних споруд тощо;

• дані про вогнестійкість будинків і споруд відповідно до вимог ДБН В.1.1–7;

• обґрунтування чисельності чергового та лінійного персоналу об'єктів, що забезпечують життєдіяльність категорованих міст і об'єктів цивільного захисту;

• рішення щодо влаштування системи раннього виявлення НС і локальної системи оповіщення населення, яке проживає в зонах можливого ураження, та персоналу цього об'єкта;

• рішення стосовно безаварійної зупинки технологічних процесів;

• рішення щодо підвищення надійності електропостачання об'єктів і технологічного устаткування, що не підлягають відключенню від електропостачання;

• рішення щодо підвищення стійкості роботи джерел водопостачання та їх захисту від радіоактивних і небезпечних хімічних речовин.

Рішення ІТЗ ЦЗ щодо попередження можливих НС у зв'язку із прогнозованими аваріями на об'єкті будівництва та мінімізацією їх наслідків включають:

• перелік особливо небезпечних виробництв із вказівкою небезпечних речовин та їх кількості для кожного виробництва;

• визначення зон дії основних небезпечних чинників при аваріях (із розрахунками меж цих зон і вказівкою методик, на підставі яких проводилися ці розрахунки);

• відомості про чисельність і розміщення персоналу об'єкта, що проектується, інших об'єктів (організацій), що можуть потрапити в зону дії небезпечних чинників у випадках аварій на об'єкті будівництва;

• відомості про чисельність і розміщення населення на прилягаючій території, що може опинитися в зоні дії небезпечних чинників у випадку аварій на об'єкті;

• рішення щодо недопущення розгерметизації технологічного обладнання та попередження аварійних викидів небезпечних хімічних речовин, вибухових речовин і матеріалів, займистих і горючих речовин;

• відомості про наявність і характеристики систем контролю радіаційної, хімічної обстановки, виявлення вибухонебезпечних концентрацій;

• рішення, спрямовані на попередження розвитку аварій і локалізацію викидів (виливів) небезпечних хімічних речовин, вибухових речовин і матеріалів, займистих і горючих речовин;

• рішення щодо забезпечення вибухопожежобезпечності будівель, споруд і технологічного обладнання об'єкта;

• відомості про наявність і характеристики систем автоматичного управління, блокувань, сигналізації, а також безаварійної зупинки технологічного процесу;

• рішення щодо забезпечення протиаварійної стійкості пунктів (систем) управління виробничим процесом, безпеки персоналу, який перебуває в них, і можливості управління процесом під час аварії;

• відомості про наявність, місця розміщення та характеристики основних (резервних) джерел електро-, тепло-, газо- і водопостачання, а також систем зв'язку;

• відомості про потребу та розміщення резервів матеріальних засобів для ліквідації наслідків аварій на об'єкті, що проектується;

• рішення щодо запобігання стороннього втручання в діяльність об'єкта (системи фізичного захисту та охорони об'єкта);

• проектні рішення щодо систем раннього виявлення НС і локальної системи оповіщення про НС;

• проектні рішення щодо забезпечення евакуації працівників і службовців із території об'єкта;

• проектні рішення щодо забезпечення проведення аварійно-рятувальних робіт, безперешкодного пересування на об'єкті сил і засобів для ліквідації наслідків аварій.

Додаткові рішення ІТЗ ЦЗ щодо попередження можливих НС, джерелами яких є небезпечні природні процеси, включають:

• відомості про природно-кліматичні умови в районі розташування об'єкта будівництва;

• оцінку частоти й інтенсивності проявів небезпечних природних процесів (явищ), а також категорію їх небезпеки;

• заходи щодо інженерного захисту території об'єкта (будинків, споруд і устаткування) від небезпечних геологічних процесів, затоплень і підтоплень, екстремальних вітрових і снігових навантажень, обледеніння, природних пожеж тощо;

• заходи щодо захисту від блискавки;

• опис і характеристики існуючих і розроблених у проекті систем моніторингу небезпечних природних процесів та оповіщення про НС природного характеру;

• відомості про наявність і характеристики систем безаварійної зупинки технологічного процесу у випадку НС, джерелами яких є небезпечні природні процеси;

• рішення щодо забезпечення протиаварійної стійкості пунктів (систем) управління виробничим процесом, безпеки персоналу, який перебуває в них, і можливості управління процесом під час НС;

• відомості про наявність, місця розміщення та характеристики основних (резервних) джерел електро-, тепло-, газо- і водопостачання, а також систем зв'язку.

Отже, комплекс проектних рішень ІТЗ ЦЗ, що реалізуються під час проектування, будівництва та експлуатації об'єктів різного призначення (у т.ч. об'єктів КІ), дає змогу встановити диференційовані вимоги до забезпечення безпеки цих об'єктів з урахуванням впливу різних чинників техногенного і природного характеру, зокрема ступеня потенційної небезпеки здійснення акту незаконного втручання або теракту і його можливих наслідків.

Із січня 2010 р. органами управління МНС України (з початку 2013 р. – ДСНС України) видано замовникам будівництв понад 450 вихідних даних і технічних умов для проектування розділу ІТЗ ЦЗ у складі проектної документації об'єктів різного функціонального призначення. Значну їх частку становлять об'єкти КІ. Наприклад, нові енергоблоки Рівненської та Хмельницької АЕС, Дністровська ГАЕС, лінійні і трансформаторні об'єкти магістральних електромереж держави, об'єкти газопостачання АК «Укртрансгаз», нові станції метрополітенів у містах Києві та Дніпропетровську й низка інших важливих об'єктів.

Висновок

Обов'язкова реалізація вимог інженерно-технічних заходів цивільного захисту при розробленні містобудівної та проектної документації, проведення її експертизи із питань цивільного захисту й техногенної безпеки є ефективним складником процедури управління ризиками надзвичайних ситуацій, захисту об'єктів різного призначення (у т.ч. об'єктів критичної інфраструктури) від наслідків можливих надзвичайних ситуацій різного характеру.

ПОБУДОВА СИСТЕМИ ЕКСТРЕНОЇ ДОПОМОГИ НАСЕЛЕННЮ ЗА ЄДИНИМ ТЕЛЕФОННИМ НОМЕРОМ 112 В УКРАЇНІ

КОВАЛЬ Сергій Михайлович,
перший заступник директора
ДП «Центр громадської безпеки 112»

Основи діючої в Україні системи надання екстреної допомоги населенню були закладені ще у середині XX ст. Нині ця система не відповідає сучасному рівню розвитку технологій екстреної допомоги, не забезпечує надання ефективної допомоги людині в екстреній ситуації, а отже, вимагає модернізації. Значна кількість телефонних номерів служб екстреної допомоги призводить до того, що людина в екстреній ситуації не завжди має змогу швидко знайти потрібну службу екстреної допомоги. Звертаючись до однієї зі служб у разі загрози або виникнення надзвичайної ситуації чи події, аварії, катастрофи, позаштатної побутової ситуації тощо, найчастіше людина не усвідомлює необхідності залучення інших служб екстреного виклику для швидкого й ефективного надання допомоги або може перебільшувати серйозність екстреної ситуації, тому в результаті «хибних викликів» залучаються служби, допомога яких не потрібна.

Отже, в Україні виникла гостра необхідність створення абсолютно нової системи екстреної допомоги людині з використанням єдиного телефонного номера – 112. Правові засади розвитку Системи 112 були закладені в Законі України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112», який визначає Державну службу України з надзвичайних ситуацій головним органом, що має забезпечувати створення Системи 112. Відповідною постановою Кабінету Міністрів України затверджено порядок її функціонування та регламент проходження інформації в системі[177].

Головною метою створення Системи 112 є введення в Україні уніфікованого механізму прийому та обробки екстрених викликів за єдиним но-

[177] *Про затвердження* Порядку функціонування системи екстреної допомоги населенню за єдиним телефонним номером 112 : постанова Кабінету Міністрів України від 17.10.2012 р. № 1031 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/go/1031-2012-%D0%BF

мером 112 і приведення якості надання екстреної допомоги у відповідність до європейських норм. Таким чином, одним із головних завдань створення системи є побудова комплексного й ефективного механізму координації дій усіх служб екстреного виклику, який дає змогу своєчасно надавати допомогу людині при виникненні екстреної (надзвичайної) ситуації.

Відповідно до завдань, покладених на систему, остання має забезпечити збір інформації про екстрені ситуації, автоматизовану ідентифікацію номера телефону й координат місцезнаходження абонента, а також передачу цієї інформації оперативно-диспетчерським службам (правоохоронних органів, центрів екстреної медичної допомоги та медицини катастроф) або до інших аварійних служб, які мають доводити її до відповідних підрозділів для надання екстреної допомоги.

З метою побудови Системи 112 ДСНС України та ДП «Центр громадської безпеки 112», на яке покладено функції головного виконавця робіт (інтегратора) з її впровадження, вживаються такі організаційні та практичні заходи:

• готуються відповідні зміни до чинних законодавчих актів щодо функціонування системи та розробляються проекти нових нормативно-технічних документів;

• проводяться засідання робочих груп із питань створення й упровадження системи екстреної допомоги населенню за єдиним телефонним номером 112;

• розроблено техніко-економічне обґрунтування створення Системи 112 в Україні;

• опрацьовано й затверджено технічне завдання й технічний проект створення Системи 112 в Україні;

• розроблено рекомендації операторам телекомунікації для здійснення маршрутизації екстрених викликів за номером 112 у відповідні центри[178];

• визначено порядок організації доступу абонентів мереж рухомого (мобільного) зв'язку в службу екстреної допомоги[179].

---

[178] *Про використання* єдиного тризначного номера 112 : рішення Національної комісії з питань регулювання зв'язку та інформатизації від 15.03.2012 р. № 125 [Електронний ресурс]. – Режим доступу: http://www.nkrz.gov.ua/uk/activities_nkrzi/ruling2012/1332163647/

[179] *Про затвердження* Порядку організації доступу абонентів мереж рухомого (мобільного) зв'язку до служб екстреної допомоги : наказ Міністерства транспорту та зв'язку України від 7.10.2009 р. № 1034 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/z1002-09

Система 112 забезпечує інформаційну взаємодію служб, номери яких (101, 102, 103, 104) ще деякий час діятимуть паралельно з номером 112 і після введення в дію Системи 112, та отримуватиме від них інформацію про результати реагування. При цьому оператори 112 не втручатимуться у специфічну діяльність цих структур та інших підрозділів, що залучаються до надання екстреної допомоги.

Згідно із законодавством оператори телекомунікації повинні здійснювати маршрутизацію екстрених викликів за єдиним номером 112 до центрів 112 і надавати (за запитом системи) необхідну інформацію про абонента та його місцезнаходження на момент з'єднання з оператором 112. Варто зазначити, що в нашій країні дзвінки на номер 112 з телефонів усіх операторів фіксованого та мобільного зв'язку безкоштовні.

Зважаючи на особливості інфраструктури служб екстреної допомоги України для побудови Системи 112, за основу було обрано дворівневу (децентралізовану) модель обробки екстреного виклику в Системі 112, яка базується на єдиному програмно-апаратному комплексі та функціонує під керівництвом органу управління Державної служби України з надзвичайних ситуацій, на який покладено завдання реалізації державної політики у сфері цивільного захисту населення країни. Саме тому центри екстреної допомоги населенню за єдиним телефонним номером 112 (центри 112, або *PSAP* за європейською термінологією) планується розгорнути в її територіальних управліннях.

Технічні рішення, пропоновані Європейською асоціацією екстрених номерів (*EENA* 112) для реалізації при побудові Системи 112 наступного покоління (*Next Generation* 112), будуть використані в Україні. Їх реалізація передбачає можливість системи обробляти екстрені виклики, отримані через *SMS*, *MMS*-повідомлення, електронну пошту. Архітектура побудови Системи 112 передбачає створення основних структурних елементів Системи 112 – центрів 112 у кожній адміністративній одиниці держави (в АР Крим, областях, містах Київ та Севастополь). Взаємодію центрів 112 з органами управління інших міністерств і відомств (з питань охорони здоров'я, внутрішніх справ, житлово-комунального господарства, із диспетчерськими й аварійними службами органів місцевого самоврядування) передбачається організувати через сучасні телекомунікаційні мережі центрів 112.

У центрі 112 розміщуватимуться оператори, які ідентифікуватимуть екстрені виклики (із залученням геоінформаційної підсистеми та баз да-

них абонентів фіксованого зв'язку), їх класифікацію через систему підтримки та прийняття рішень, інформаційно-довідкову базу й базу знань, а також використовуватимуть інші допоміжні підсистеми. Зазначені системи надають оператору можливість оптимально розподілити завдання, об'єднати зусилля, скоординувати дії кількох або всіх служб екстреної допомоги залежно від конкретної екстреної ситуації.

Оператор 112, до якого буде цілодобово надходити інформація з усіх можливих джерел (у т.ч. з інтернету, інших автоматизованих систем), після оброблення екстреного виклику заповнює електронну картку екстреної ситуації та передає її у відповідні оперативно-диспетчерські служби для організації надання екстреної допомоги. До електронної картки автоматично вноситься аудіозапис екстреного виклику й електронна карта із позначенням місця екстреної ситуації, а також додаткова інформація, що міститься в базах даних операторів телекомунікацій. Для уточнення інформації про екстрену ситуацію оператор 112 зможе безпосередньо з'єднати диспетчера оперативно-диспетчерської служби з людиною, яка здійснює екстрений виклик або організувати конференц-зв'язок за участю перекладача або психолога.

У результаті спеціальних досліджень, проведених задля вивчення обсягів максимальних навантажень каналів екстрених викликів у мережі та обладнання основних операторів телекомунікації України, встановлено, що для стійкої роботи Системи 112 після розгортання всіх її елементів необхідно 550 автоматизованих робочих місць операторів центрів 112. Оптимальне навантаження на одного оператора 112, що також підтверджується досвідом роботи існуючих екстрених служб, – це обслуговування 100 тис. осіб.

Ядром системи є дата-центри, які планується розмістити в містах Києві, Донецьку, Львові та Миколаєві. Кожен дата-центр є взаємозамінним і за потреби зможе виконувати функції сусіднього аналогічного дата-центру. Організовувати взаємодії центрів 112 і дата-центрів передбачається через єдину телекомунікаційну мережу Системи 112. Завдяки такій архітектурі побудови кожен дата-центр обмінюватиметься інформацією із центрами 112, які територіально розташовані в регіоні, та з іншими дата-центрами. Передбачається, що після завершення побудови Система 112 буде створено 27 центрів «112», 4 дата-центри, телекомунікаційну мережу Системи 112.

Таким чином, побудова й упровадження української національної Системи 112 – це створення «барометра якості життя нашого суспіль-

ства», який дасть змогу державі довести, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Створений після впровадження системи комплексний, ефективний і дієздатний механізм координації дій усіх екстрених служб дасть змогу підняти рівень надання екстреної допомоги в нашій країні до рівня європейських вимог.

СУЧАСНИЙ СТАН УПРОВАДЖЕННЯ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО ПОЖЕЖНОГО Й ТЕХНОГЕННОГО СПОСТЕРІГАННЯ

КОВАЛЬ Сергій Михайлович,
перший заступник директора
ДП «Центр громадської безпеки 112»;
КОЦЮБА Віктор Іванович,
начальник відділу системного адміністрування
ДП «Центр громадської безпеки 112»

На сьогодні захист від техногенних аварій і катастроф є одним з найбільш актуальних питань безпеки суспільства. Ризик виникнення надзвичайних ситуацій і пожеж в Україні зумовлений, зокрема, експлуатацією вибухо- й пожежонебезпечних об'єктів на значній кількості промислових підприємств. Більшість із них працює на застарілому обладнанні, що, своєю чергою, підвищує ймовірність виникнення пожеж та аварій на цих об'єктах.

Статистика пожеж в Україні є невтішною. Так, протягом 2012 р. було зареєстровано понад 70 тис. пожеж, унаслідок яких загинула 2751 ос., а збитки на підприємствах, в установах та організаціях сягнули близько 1 млрд грн[180].

Безпечна ситуація в Україні, яка характеризується, зокрема, зростанням загроз пожежного й техногенного характеру, вимагає застосування нових підходів до забезпечення безпечного існування нашої держави. Це зумовлює необхідність надійного захисту особливо важливих із цього погляду об'єктів і ресурсів держави за допомогою підсистеми централізованого пожежного й техногенного спостерігання як елемента «системи захисту критичної інфраструктури».

---

[180] *УкрНДІЦЗ* [Електронний ресурс]. – Режим доступу: http://www.undicz.mns.gov.ua/content/statistics.html

Поодинокі системи пожежної автоматики (ПА), сигналізації, автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення (АСРВО), що встановлюються на різних об'єктах в Україні й не є замкнутими в єдину автоматизовану систему, ускладнюють надання дієвої та своєчасної допомоги пожежно-рятувальними підрозділами.

Головною метою створення системи централізованого пожежного й техногенного спостерігання (СЦПТС) є раннє виявлення пожеж і ситуацій техногенного характеру на об'єктах критичної інфраструктури та сповіщення про них пожежно-рятувальних підрозділів Державної служби України з надзвичайних ситуацій (ДСНС України) для відповідного реагування.

Відповідно до Постанови Кабінету Міністрів України від 21 жовтня 1999 р. № 1943[181] ДСНС має забезпечити здійснення державного пожежного нагляду за станом пожежної безпеки в населених пунктах і на об'єктах незалежно від форм власності з використанням сучасних технологій. Одним із напрямів щодо підвищення рівня державного пожежного нагляду за станом пожежної безпеки є створення й упровадження ПА та виведення її сигналів до оперативно-диспетчерської служби оперативно-координаційного центру Головного управління (Управління) (ОДС ОКЦ ГУ (У)) ДСНС України.

Побудова та впровадження системи централізованого пожежного й техногенного спостерігання здійснюється відповідно до таких нормативних документів: Наказу МНС України від 20 квітня 2011 № 436[182], ДБН В.2.5-56:2010 Інженерне обладнання будинків і споруд «Системи протипожежного захисту», Правил з пожежного спостерігання, затверджених Наказом МНС України від 7 квітня 2011 р. № 351 (зареєстрований у Мін'юсті 22 червня 2011 р. № 477/19482), Ліцензійних умов провадження господарської діяльності з надання послуг і виконання робіт протипожежного призначення, затверджених Наказом МНС від 29 вересня 2011 р. № 1037, ДСТУ-П *CLC/TS* 50136-4:2010 Системи тривожної сигналізації. Системи передавання тривожних сповіщень та устаткування. Частина 4. Устаткування індикації центрів приймання тривожних сповіщень.

---

[181] *Про стан* забезпечення пожежної безпеки та заходи щодо її поліпшення : постанова Кабінету Міністрів України від 21.10.1999 р. № 1943 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1943-99-%D0%BF

[182] *Про затвердження* документації щодо створення та впровадження системи централізованого пожежного та техногенного спостерігання : наказ МНС України від 20.04.2011 р. № 436 [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/files/2011/4/22/436.pdf

Також відповідно до вказаної чинної нормативної бази передача сигналів пожежної тривоги від центрів приймання тривожних сповіщень до точки доступу Центру спостерігання (ЦС) ДСНС України має здійснюватися в автоматичному режимі в єдиному протоколі та форматі передачі даних (формат *XML*, протоколу *SOS ACCESS V*3).

Створення, впровадження та організація безперервного функціонування системи централізованого пожежного спостерігання передбачено Наказом МНС України від 6 грудня 2011 р. № 1274 «з метою забезпечення пожежної та техногенної безпеки об'єктів і територій та оптимізації структури підрозділів МНС України, на яких покладено функції з пожежного й техногенного спостерігання і передачу тривожних сповіщень» [183]. Відповідальним за організацію виконання заходів зі створення, впровадження та функціонування системи централізованого пожежного й техногенного спостерігання визначено ДП «Центр громадської безпеки 112». Також Наказом МНС України «Про організацію централізованого пожежного та техногенного спостерігання» від 30 липня 2012 р. № 1060 ДП «ЦГБ 112» стало Центром спостерігання МНС України й набуло прав укладати договори із суб'єктами господарювання в АР Крим, областях, містах Києві та Севастополі та, відповідно, взяло на себе основні обов'язки щодо впровадження цієї системи протягом найближчого часу та щодо нагляду (контролю) зі сторони Держави за функціонуванням ПА та АСРВО.

Кількість систем ПА та АСРВО, що монтуються на різних об'єктах, неухильно зростає. Нині, якщо об'єкт обладнаний сучасною ПА, то сигнал від неї, у ліпшому випадку, надійде в комерційні центри прийому тривожних сповіщень, а здебільшого – на автономні світлозвукові сповіщувачі систем ПА. У випадку з АСРВО інформація про загрозу виникнення або виникнення НС надається в ГУ(У) ДСНС України здійсненням автоматичного телефонування та передачею тривожного мовного сповіщення, інформативність та оперативність якого є недостатньою для прийняття оперативних управлінських рішень щодо ефективних дій з локалізації та ліквідації надзвичайної ситуації.

Отже, процес отримання, оброблення та реагування на тривожні сповіщення не замкнутий в єдину систему, тому маємо запізніле над-

---

[183] *Про створення* системи централізованого пожежного та техногенного спостерігання та визнання таким, що втратив чинність (наказ МНС від 20.04.2011 р. № 435) : наказ МНС України від 6.12.2011 р. № 1274 [Електронний ресурс]. – Режим доступу: http://mns.gov.ua/files/2011/12/7/1274.pdf

ходження до оперативно-диспетчерської служби інформації про НС і відповідне реагування на подію. Однак ані оснащення підрозділів новою технікою, ані високий професіоналізм рятівників не дадуть досягти успіху при гасінні пожеж і локалізації та ліквідації надзвичайних ситуацій без надійної системи централізованого пожежного й техногенного спостерігання.

Функціонування системи централізованого пожежного й техногенного спостерігання здійснюється за таким принципом: усі сигнали про спрацювання ПА та АСРВО від об'єктів надходять до центру приймання тривожних сповіщень (ЦПТС), потім в автоматичному режимі тривожне сповіщення передається до ЦС ДСНС України у протоколі *SOS ACCESS V*3. Центром спостерігання автоматично формується картка тривожного сповіщення і в автоматичному режимі передається до відповідного за територіальністю ОДС ОКЦ ГУ(У) ДСНС України, в зоні якого знаходиться об'єкт.

Державним підприємством «Центр громадської безпеки 112» вжито низку організаційно-технічних заходів зі створення й упровадження СЦПТС, а саме:

• встановлено та налагоджено програмно-апаратний комплекс для забезпечення виконання функцій, покладених на СЦПТС;

• створено відомчу телекомунікаційну мережу СЦПТС;

• установлено цифрові канали зв'язку для передачі тривожних сповіщень до відповідного за територіальністю ОДС ОКЦ ГУ (У) ДСНС України;

• організовано захищений *WEB*-доступ до порталу СЦПТС для дистанційного введення ліцензіатами карток і план-схем об'єктів спостерігання;

• проводяться випробування щодо можливості приймання тривожних сповіщень СЦПТС від устаткування індикації ЦПТС пультової організації у протоколі *SOS ACCESS V*3 з видачею відповідного висновку про випробування;

• розроблено картку події про надзвичайну ситуацію, що автоматично формується при надходженні тривожного сповіщення;

• проводиться реєстрування, архівування та зберігання інформації про тривожні сповіщення та об'єкти спостерігання в єдиній базі даних об'єктів спостерігання (ЄБД);

• здійснюється реєстрація комерційних пультів пожежного й техногенного спостерігання в ЄБД з видачею посвідчення про реєстрацію;

• проведено дослідну експлуатацію апаратно-програмних засобів Центру спостерігання та АРМ СЦПТС ОДС ОКЦ ГУ(У) ДСНС України;

• упровадження СЦПТС допоможе підвищити рівень захисту критичної інфраструктури, а також дасть змогу пожежно-рятувальним підрозділам ДСНС України більш оперативно реагувати на надзвичайні ситуації, що, своєю чергою, зменшить матеріальні збитки та людські жертви.

ОЦІНКА ГЕОЛОГІЧНИХ ЗАГРОЗ ДЛЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ УКРАЇНИ

ІВАНЮТА Сергій Петрович,
старший консультант відділу екологічної та техногенної безпеки НІСД

На сьогодні в Україні залізничний транспорт займає провідні позиції і щодо вантажних перевезень (за даними Укрстату частка залізниці за цим показником сягає 58,8 % за 9 місяців 2013 р. та 59,2 % – за 2012 р.), і за пасажирообороотом (39,5 і 37,3 % відповідно). Тому забезпечення безпеки функціонування залізничного транспорту є досить важливим для економіки країни завданням, практичне вирішення якого потребує виявлення найбільш імовірних загроз для утримання в належному стані залізничних колій. Складність вирішення такого завдання пов'язана і зі значною експлуатаційною протяжністю головних колій Укрзалізниці (22,3 тис. км, розгорнута протяжність колій – 30,3 тис. км, електрифікованих колій – 9,2 тис. км), і з низкою чинників техногенного та природного характеру.

Однією з вагомих причин пошкоджень конструктивних елементів залізничних колій є вплив небезпечних екзогенних геологічних процесів (НЕГП)[184]. Висока середня просторова щільність експлуатаційної мережі залізниць України ($22{,}3 \cdot 10^3 / 603 \cdot 10^3 \approx 0{,}037$ км/км^2) підвищує ризики ураження залізничної мережі НЕГП. Природна й техногенна активізація таких процесів може відбуватися внаслідок дії різних чинників, що ускладнює контроль за ними та їх прогнозування, тобто змінювання

[184] *Про стан* техногенної та природної безпеки в Україні у 2012 р. : нац. доп. [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/nasdopovid2012.html

геомеханічних, фізико-хімічних, інженерно-геофізичних параметрів породного масиву. За даними Державної служби геології та надр України, значна частина залізничних колій розташована на територіях, уражених НЕГП, з-поміж яких найбільшу загрозу становлять карст, підтоплення та зсуви.

Загроза прояву карсту зумовлена тим, що на 38 % території України поширені породи, в яких можуть відбуватися процеси і природного, і техногенно активізованого карстоутворення, а на 24 % території карст може безпосередньо впливати на господарську діяльність[185] (рис. 1).

Рис. 1. Загрози карсту для функціонування залізниці в Україні

Дані досліджень свідчать, що найбільша загроза прояву карстових процесів існує насамперед на території Волинської, Луганської, Терно-

[185] *Биченок М. М.* Про вплив екзогенних геологічних процесів на рівень техногенних ризиків життєдіяльності / М. М. Биченок, С. П. Іванюта, Є. О. Яковлєв // Зб. наук. праць Українського державного геологорозвідувального інституту. – К. : УкрДГРІ, 2006. – № 1. – С. 85–91.

пільської, Рівненської та Миколаївської областей[186] (табл. 1). За результатами оцінок, у середньому понад 50 % довжини залізничних колій у цих областях перебувають під загрозою прояву карсту. Крім того, залізничні колії Луганської, Волинської й Тернопільської областей майже по всій довжині перебувають у зонах карстових загроз, які останніми роками мають підвищену тенденцію впливу на безпеку експлуатації залізничного комплексу.

Отже, динаміка процесу підтоплення території України є прогресуючою зі стійкою тенденцією до його активізації на регіональному рівні за постійного збільшення площ підтоплення (рис. 2). За даними МНС України, станом на 2011 р. найбільш несприятливі умови з підтоплення територій склалися у Дніпропетровській, Донецькій, Запорізькій, Миколаївській, Одеській та Херсонській областях, де середній приріст підтоплення становить 300 км/рік[187]. Крім того, у цих областях у структурі верхньої зони порід геологічного середовища переважають слабоводостійкі лесові горизонти, що підсилює негативний вплив підтоплення на безпеку функціонування залізничного комплексу. У цьому контексті доцільно зазначити, що одна з найбільш резонансних аварій на залізничному транспорті останнього часу – поблизу с. Ожидова Львівської обл. (т.зв. фосфорна аварія) – трапилася в зоні багаторічного підтоплення, яке могло додатково вплинути на погіршення геодинамічної стійкості ґрунтів.

Результати оцінки загроз від підтоплення, здійсненої з використанням ГІС-технологій, свідчать, що найбільшою ця загроза для функціонування залізниці є на території Житомирської, Донецької, Рівненської, Волинської, Дніпропетровської, Миколаївської, Одеської та Полтавської областей.

Зсуви є одними з найбільш небезпечних екзогенних геологічних процесів, поширених на території України[188]. Хоча здебільшого зсувні деформації виявляються на відносно незначній території, проте внаслідок

---

[186] *Демчишин М. Г.* Регіональні інженерно-геологічні умови території України : інформ. бюл. / М. Г. Демчишин, Л. М. Климчик, Л. М. Красноок [та ін.] // гол. ред. Є. О. Яковлєв – К. : ДІГФ «Геоінформ» Держгеолслужби Мінприроди, 1997. – Вип. 1. – 92 с.

[187] *Про стан* техногенної та природної безпеки в Україні у 2011 р. : нац. доп. // МНС України [Електронний ресурс]. – Режим доступу: http://mns.gov.ua/content/nas-dopovid2011.html

[188] *Yakovlev Y. A.* The geological aspects of environmental systems monitoring the geological medium of Ukraine. UNESCO Regional Office for Science and Technology for Europe : Technical Report 21 / Y. A. Yakovlev. – 1995. – P. 184–191.

регіонального розповсюдження зсувних об'єктів вони можуть мати значні негативні наслідки, спричинені здатністю до швидких деформацій та руйнувань відповідальних елементів інженерно-господарських і потенційно небезпечних об'єктів. Крім того, останніми роками внаслідок довгострокового техногенного підтоплення лесово-суглинистих порід і збільшення опадів відбувається зниження їх міцності й розвиток зсувів на схилах зі стрімкістю 3^0–5^0, що суттєво розширює в Україні площі зсувоутворення.

Рис. 2. Загрози підтоплення для функціонування залізниці в Україні

Наведені в табл. 1 дані свідчать про те, що найбільшою загроза внаслідок можливого прояву зсувів для функціонування залізниці є на території Харківської, Чернівецької, Закарпатської областей.

Таким чином, нагальною є необхідність проведення більш детальних і цілеспрямованих досліджень впливу НЕГП на безпеку функціонування залізничного транспорту України з урахуванням імовірності прояву цих процесів у місцях спорудження нових залізничних колій.

Таблиця 1

Загрози НЕГП для безпеки функціонування залізниці (регіональний розріз)

Назва регіону	Протяжність залізничних колій, км	Протяжність колій у зоні розвитку карсту, км	Частка протяжності колії в зоні розвитку карсту, %	Протяжність колій у зоні зсувів, км	Частка протяжності колії у зоні зсувів, %
АР Крим	594,1	289,9	0,49	62,2	0,10
Вінницька	1391,2	289,4	0,21	211,6	0,15
Волинська	608,5	608,5	1,00	0,0	0,00
Дніпропетровська	1681,8	373,4	0,22	156,6	0,09
Донецька	1985,9	1386,2	0,70	141,3	0,07
Житомирська	1128,6	0,0	0,00	8,0	0,01
Закарпатська	735,8	46,4	0,06	205,1	0,28
Запорізька	931,9	257,2	0,28	70,1	0,08
Івано-Франківська	738,6	265,2	0,36	118,6	0,16
Київська	818,2	0,0	0,00	54,9	0,07
Кіровоградська	930,2	14,9	0,02	38,1	0,04
Луганська	1278,2	1273,1	1,00	228,9	0,18
Львівська	1246,3	726,6	0,58	166,6	0,13
Миколаївська	784,4	554,6	0,71	10,8	0,01
Одеська	1017,3	161,8	0,16	153,9	0,15
Полтавська	815,1	8,2	0,01	123,0	0,15
Рівненська	668,0	534,4	0,80	0,0	0,00
Сумська	878,3	368,9	0,42	103,9	0,12
Тернопільська	534,3	534,3	1,00	42,1	0,08
Харківська	1404,7	483,2	0,34	516,5	0,37
Херсонська	461,6	246,0	0,53	6,0	0,01
Хмельницька	774,8	507,5	0,66	113,9	0,15
Черкаська	750,2	0,0	0,00	148,4	0,20
Чернівецька	420,4	197,2	0,47	130,8	0,31
Чернігівська	920,0	121,4	0,13	23,3	0,03

Отже, результати дослідження свідчать, що першочергової оцінки загроз від НЕГП на безпеку функціонування залізного комплексу потребують залізниці Донецької, Дніпропетровської, Львівської, Одеської, Житомирської та Рівненської областей.

РОЛЬ І МІСЦЕ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В СУЧАСНИХ ВОЄННИХ КОНФЛІКТАХ

ПУНДА Юрій Васильович,
докторант кафедри стратегії національної безпеки і оборони Національного університету оборони України імені Івана Черняховського

Сучасні умови ведення збройної боротьби та можливості сучасного озброєння вимагають перегляду основ підготовки держави до оборони, особливо підготовки об'єктів критичної інфраструктури до функціонування в умовах особливого періоду. Це пов'язано насамперед із тим, що на території України немає ділянок місцевості, недосяжних для вогневого впливу зброєю імовірного противника, а сучасні тенденції ведення бойових дій передбачають перенесення пріоритетів вогневого ураження саме на об'єкти національної економіки та об'єкти систем життєзабезпечення населення.

Під час останніх воєнних конфліктів цей чинник був одним із вирішальних під час планування воєнних дій і брався за основу концепції «стратегічного сковування»[189]. Сутністю зазначеної концепції є порушення функціонування заздалегідь визначеної сукупності головних об'єктів противника, що може перешкодити йому виконати основне завдання, тобто виведення з-під його контролю життєво важливих ресурсів. Досягнути стратегічного сковування противника можна у випадку одночасного завдання т.зв. паралельних ударів по максимальній кількості об'єктів критичної інфраструктури.

Підвищення точності й масове виробництво крилатих ракет і компонентів розвідувально-ударних комплексів у повному обсязі дало змогу реалізувати концепцію стратегічного сковування в операціях «Свобода

[189] *Fadok D. S.* Air Power Quest for Strategic Paralysis / D. S. Fadok, J. Boyd, J. Warden // A Thesis presented to the faculty of the School of Advanced Airpower Studies. – Air University Maxwell Air Force Base, Alabama, 1994. – June.

Іраку» та «Союзницька сила». В Іраку впродовж перших годин операції війська коаліції уразили сотні найважливіших цілей – було повністю порушено телефонний зв'язок, припинено енергопостачання, центри протиповітряної оборони втратили управління над бойовими позиціями, знищено основні пункти управління. Крім порушення управління іракськими військами, знищення об'єктів критичної інфраструктури дало змогу значно знизити готовність населення Іраку до збройного опору.

Вказані зміни у веденні збройної боротьби, на жаль, не повною мірою враховуються в національній практиці підготовки критичної інфраструктури до функціонування в умовах особливого періоду. Усталені погляди на цей процес передбачають, що національна економіка з початком особливого періоду починає перебудову задля функціонування в умовах особливого періоду й за певний проміжок часу значно наростить випуск озброєння в особливий період. Як приклад, на рис. 1 графічно зображено динаміку задоволення воєнно-економічних потреб, що була основою воєнно-стратегічних розрахунків у Радянському Союзі.

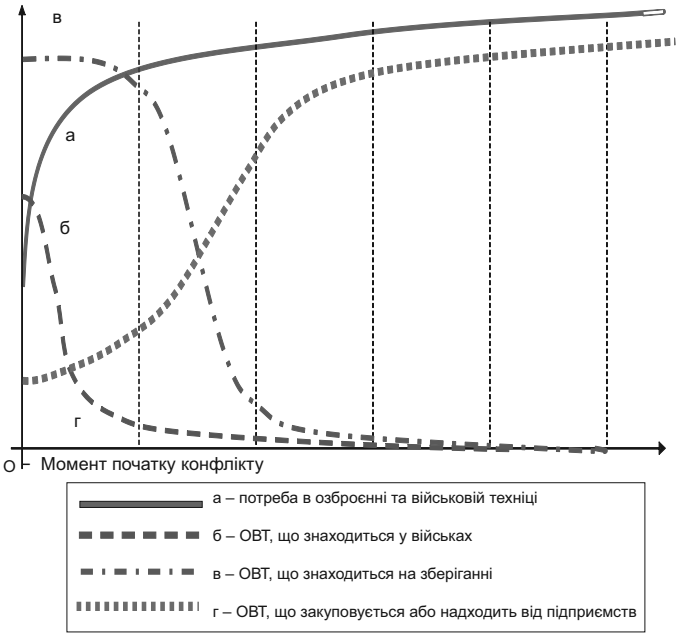


Рис. 1. Графік задоволення воєнно-економічних потреб у минулому

Із графіка видно, що різниця між воєнно-економічними потребами та можливостями національної економіки компенсувалася за рахунок резервів. Проте в сучасних умовах об'єкти критичної інфраструктури, у т.ч. оборонно-промислового комплексу України, є стаціонарними, їх дислокація відома і керівництву інших держав, і потенційним учасникам незаконних збройних формувань. Тому після початку воєнного конфлікту в умовах постійного вогневого впливу противника (або ж можливих асиметричних атак на об'єкти оборонно-промислового комплексу по всій території України) значно зросте час на відновлення оборонної промисловості, а випуск ресурсо- й енергоємної продукції буде неможливий. Тому без зміни поглядів на підготовку об'єктів критичної інфраструктури до функціонування в умовах особливого періоду, графік задоволення воєнно-економічних потреб можна відобразити таким чином (рис. 2).

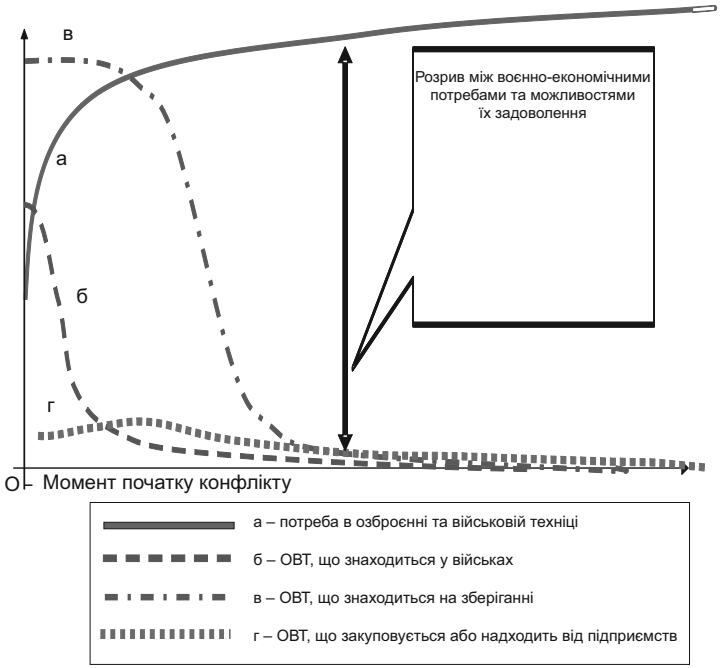


Рис. 2. Графік задоволення воєнно-економічних потреб у сучасних воєнних конфліктах

Отже, в сучасних воєнних конфліктах основною причиною поразки у збройному конфлікті може стати розрив між воєнно-економічними потребами та можливостями їх задоволення, а також готовністю населення до збройного опору через приведення у нефункціональний стан об'єктів критичної інфраструктури. Таким чином, знищення об'єктів критичної інфраструктури руйнує не лише економічний, а й військовий, соціальний і морально-політичний потенціал, що в сукупності є основою обороноздатності країни[190].

У цих умовах у провідних державах світу приділяється значна увага питанням підготовки об'єктів критичної інфраструктури до функціонування в умовах кризових ситуацій різного характеру, в т.ч. і воєнного. Наприклад, у Міністерстві оборони США в Центрі управління оцінюванням оборонних ресурсів (*Test Resource Management Center*) є посада заступника директора з питань оцінювання інфраструктури (*Deputy Director Test Infrastructure*), до посадових обов'язків якого належить перевірка стану й готовності об'єктів інфраструктури до використання в інтересах оборони країни та застосування і розгортання військ. У Директораті національного захисту та програм (*National Protection and Programs Directorate*) Міністерства внутрішньої безпеки США, який очолює заступник міністра, з-поміж інших функціонує управління захисту інфраструктури (*Office of Infrastructure Protection*), головним завданням якого є підвищення рівня готовності до виникнення, відповіді й відновлення після випадків атак, стихійних лих чи інших надзвичайних ситуацій. На виконання Директиви президента з питань внутрішньої безпеки (*Homeland Security Presidential Directive*) управлінням у 2009 р. розроблено План захисту національної інфраструктури[191], відповідно до якого об'єкти інфраструктури розбито на 12 секторів і кожному міністерству визначено сектор відповідальності за напрямом діяльності. Зокрема, Міністерство оборони відповідає за імплементацію заходів плану на об'єктах оборонно-промислового комплексу з урахуванням їх особливостей.

Отже, необхідно зазначити, що в України існує значний потенціал для вдосконалення підготовки об'єктів критичної інфраструктури для функ-

---

[190] *Про оборону* України : закон України від 6.12.1991 р. № 1932-XII // ВВР. – 1992. – № 9. – Ст. 106 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12

[191] *National* Infrastructure Protection Plan [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

ціонування в умовах впливу всього спектра загроз, у т.ч. і воєнного характеру.

СПОСОБИ ВДОСКОНАЛЕННЯ ПРОЦЕСУ ПЛАНУВАННЯ РОЗВИТКУ ІНФРАСТРУКТУРИ КРАЇНИ ДО ФУНКЦІОНУВАННЯ В УМОВАХ КРИЗОВИХ СИТУАЦІЙ

ГРИЩЕНКО Володимир Павлович,
професор кафедри стратегії національної безпеки та оборони Національного університету оборони України імені Івана Черняховського;
ГОЛДА Олександр Леонідович,
старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

На тлі посилення загроз і зростання нестабільності у світі постають нові виклики міжнародній безпеці в сировинній, енергетичній, фінансовій, інформаційній, екологічній, продовольчій сферах, які змушують заново оцінити рівень і вплив загроз життєво важливим інтересам України, визначити стратегічні пріоритети політики національної безпеки та напрями вдосконалення механізмів її реалізації, зокрема способи підвищення ступеня готовності інфраструктури країни до функціонування в умовах кризових ситуацій. Варто зазначити, що у Воєнній доктрині України з-поміж пріоритетних напрямів підготовки держави до збройного захисту національних інтересів визначено «розвиток інфраструктури регіонів з урахуванням потреб підготовки території держави до оборони»[192]. Своєю чергою, ефективний розвиток інфраструктури можливий лише на основі ретельно розробленої комплексної державної цільової програми.

Як відомо, державна цільова програма – це комплекс взаємопов'язаних завдань і заходів, спрямованих на розв'язання найважливіших проблем розвитку держави, окремих галузей економіки або адміністративно-територіальних одиниць, здійснюваних із використанням коштів

[192] *Про нову* редакцію Воєнної доктрини України : указ Президента України від 8.06.2012 р. № 390 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/14824.html

державного бюджету України та узгоджених за строками виконання, складом виконавців, ресурсним забезпеченням. Цільові програми, розроблені за допомогою програмно-цільового методу, дають змогу концентрувати ресурси й зусилля на вирішенні головних завдань – оборонних, соціальних, науково-технологічних, екологічних тощо[193]. Оскільки в цільових програмах передбачаються також завдання й заходи, що забезпечують їх виконання, то вони є не тільки засобом планування, а й інструментом управління. Саме тому для підвищення ступеня готовності критичної інфраструктури країни до функціонування в умовах кризових ситуацій необхідно, на нашу думку, передбачити розроблення *державної цільової програми підготовки критичної інфраструктури*. Така програма має бути спрямована на розв'язання проблеми розвитку критичної інфраструктури загалом, мати довгостроковий період виконання та виконуватися центральними й місцевими органами виконавчої влади. Підставою для її ініціювання є невідповідність ступеня готовності інфраструктури країни до функціонування в умовах кризових ситуацій, а також розуміння того, що цю проблему потрібно вирішити не засобами територіального чи галузевого управління, а завдяки державній підтримці, координації діяльності центральних і місцевих органів виконавчої влади й органів місцевого самоврядування. При цьому розроблення програми має відповідати таким вимогам:

• бути ініційованим відповідно до визначеного у Воєнній доктрині України пріоритетного напряму підготовки держави до збройного захисту національних інтересів;

• виходити із потреби забезпечення міжгалузевих і міжрегіональних зв'язків між суб'єктами підготовки території України до оборони;

• передбачати наявність реальних можливостей для забезпечення виконання програми (фінансових ресурсів – коштів державного, місцевих бюджетів та інших джерел; матеріально-технічних і трудових ресурсів).

Згідно із Порядком розроблення та виконання державних цільових програм[194] на початковому етапі ініціатор розроблення програми має підготувати проект концепції програми, де буде визначено такі основні моменти:

---

[193] *Программно-целевое* планирование и управление : учеб. / Б. А. Райзберг, А. Г. Лобко. – М. : ИНФРА-М, 2002. – 428 с.

[194] *Про затвердження* Порядку розроблення та виконання державних цільових програм : постанова Кабінету Міністрів України від 31.01.2007 р. № 106 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/106-2007-%D0%BF

• аналіз стану існуючої інфраструктури та обґрунтування необхідності його поліпшення;

• мета комплексної цільової програми;

• визначення проблем підготовки критичної інфраструктури до функціонування в умовах кризових ситуацій;

• визначення раціонального варіанта вирішення проблеми підготовленості критичної інфраструктури на основі порівняльного аналізу можливих варіантів;

• способи підвищення ступеня підготовленості критичної інфраструктури до функціонування в умовах кризових ситуацій, а також строки виконання програми;

• очікувані результати виконання програми, визначення її ефективності;

• оцінювання фінансових, матеріально-технічних, трудових та інших ресурсів, необхідних для виконання програми.

Відповідно до вказаного Порядку розроблення державної цільової програми проходить кілька етапів (рис. 1).

Державний замовник програми у процесі її виконання здійснює моніторинг виконання передбачених завдань і заходів; має подавати в установленому порядку фінансову звітність; за потреби подавати щороку до кінця березня Міністерству фінансів України та Міністерству економічного розвитку і торгівлі України пропозиції щодо уточнення переліку завдань і заходів на наступний бюджетний період.

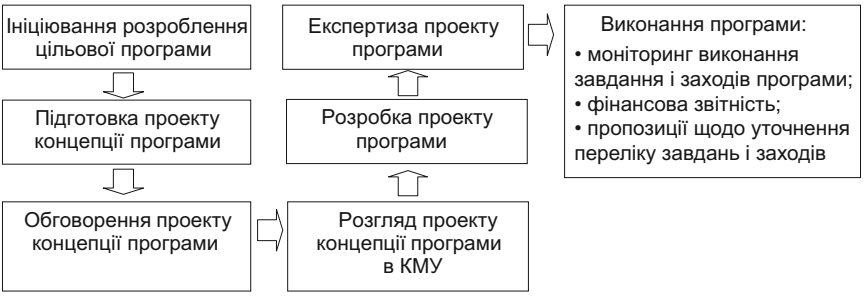


Рис. 1. Етапи розроблення державної цільової програми

Державний замовник програми визначає обсяги видатків на виконання завдань і заходів програми у складі бюджетних програм під час фор-

мування Проекту закону України «Про Державний бюджет України» на відповідний рік. Міністерство фінансів України під час розроблення останнього має враховувати обсяги видатків на виконання завдань і заходів програми у відповідних бюджетних програмах з урахуванням можливостей державного бюджету.

Відповідно до чинного законодавства[195] виконавцями заходів програми можуть бути і державні, і підприємства інших форм власності, установи й організації.

Державний замовник програми має аналізувати й комплексно оцінювати результати виконання передбачених завдань і заходів, цільове використання коштів, а також готувати щорічні (а за потреби і проміжні) звіти про перебіг виконання програми на основі звітів, поданих іншими державними замовниками в установлений строк.

Запропонований підхід до процесу планування ресурсного забезпечення підготовки критичної інфраструктури до функціонування в умовах кризових ситуацій дасть змогу більш ефективно й цілеспрямовано використовувати державні кошти для утримання, модернізації та будівництва об'єктів критичної інфраструктури, що позитивно вплине на всі групи показників ступеня готовності критичної інфраструктури до функціонування в умовах кризових ситуацій.

---

[195] *Про здійснення* державних закупівель : закон України від 1.06.2010 № 2289-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2289-17

РІШЕННЯ
міжнародної науково-практичної конференції з теми «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні» (Київ – Вишгород, Україна, 7-8 листопада)

Міжнародна науково-практична конференція з теми «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні» була присвячена актуальним проблемам забезпечення безпеки критично важливих для життєдіяльності держави, здоров'я людей і довкілля об'єктів та систем. Організатори конференції: Національний інститут стратегічних досліджень, Офіс зв'язку НАТО в Україні та ПАТ «Укргідроенерго». У роботі конференції взяли участь представники державних органів України, державних і приватних компаній та підприємств, науково-дослідних установ Національної академії наук України, учбових закладів, а також представники акредитованих в Україні дипломатичних представництв, міжнародних організацій і зарубіжні експерти.

За результатами представлених доповідей і загальної дискусії учасники конференції *підкреслюють:*

• актуальність проблем захисту критичної інфраструктури для країн Європи, у т.ч. у межах їх членства в НАТО, а також для України з огляду на тенденцію до зростання терористичних загроз у світі, збільшення кількості надзвичайних ситуацій, викликаних природними й техногенними чинниками;

• останнім часом окремими міністерствами й відомствами України здійснено певні кроки з метою підвищення надійності та безпеки функціонування життєво важливих для країни систем і об'єктів;

• зусилля Національного інституту стратегічних досліджень спрямовувалися на запровадження передового зарубіжного досвіду у сфері захисту критичної інфраструктури держави способом сприяння контактам експертів і фахівців, обміну відкритою інформацією, публікації аналітичних матеріалів із зазначеного напряму;

• необхідність подальшої гармонізації безпекових підходів на національному рівні з підходами до захисту критичної інфраструктури, прийнятими провідними країнами світу, зокрема країнами-членами ЄС і НАТО;

• переваги концептуального підходу, заснованого на понятті «критична інфраструктура», який дає змогу системно вирішувати питання захисту критично важливих для життєдіяльності держави, безпеки її громадян та довкілля систем і об'єктів та регіональної безпеки, створює можливості для більш ефективного управління ризиками на глобальному, регіональному та національному рівнях;

• недостатність науково-методичної й технологічної підтримки діяльності суб'єктів процесу запровадження концепції критичної інфраструктури;

• нагальну необхідність пошуку форм і механізмів взаємодії компетентних органів держави, державних і приватних компаній, з одного боку, та науково-дослідних і науково-виробничих організацій – з другого;

• суттєве відставання в розвитку державно-приватного партнерства у сфері безпеки порівняно з таким партнерством в економічній сфері.

Учасники конференції рекомендували:

• *Раді національної безпеки та оборони України* розглянути можливість включення до плану засідань Ради національної безпеки і оборони України у період 2014–2015 рр. питання захисту критично важливих для існування держави, безпеки населення і довкілля систем та об'єктів, які на сьогодні визначаються поняттям «критична інфраструктура», що за останнє десятиріччя широко використовується у провідних країнах;

• *Суб'єктам боротьби з тероризмом в Україні* сприяти запровадженню концептуального поняття «критична інфраструктура» у сферу протидії тероризму, в т.ч. через вивчення та запровадження передового зарубіжного досвіду;

• *Міністерству оборони України та Міністерству закордонних справ України* під час підготовки Плану дій Україна – НАТО на 2015 р. розглянути пропозиції щодо вжиття заходів стосовно захисту критичної інфраструктури серед пріоритетних для їх включення до Плану;

• *Міністерству енергетики та вугільної промисловості України та Міністерству інфраструктури України* сприяти запровадженню поняття «критична інфраструктура» в Україні, в т.ч. з огляду на Директиву Європейської Комісії № 114 за 2008 р., якою встановлений порядок визначення загальноєвропейської критичної інфраструктури;

• *Національному інституту стратегічних досліджень* спираючись на доповіді, представлені на конференції, а також на результати їх обговорень, підготувати:

– аналітичний матеріал для Апарату Ради національної безпеки і оборони України з обґрунтуванням переваг запровадження концептуального підходу до захисту життєво важливих для існування держави, безпеки населення та довкілля систем і об'єктів, основою якого є поняття «критична інфраструктура»;
– пропозиції щодо включення заходів, спрямованих на запровадження концепції критичної інфраструктури, до щорічного Плану дій Україна – НАТО на 2015 р.;
– збірник матеріалів конференції;

• *Національній академії наук України* розглянути можливість започаткування комплексної науково-дослідної програми з питань захисту критичної інфраструктури, врахування взаємозв'язків окремих об'єктів і секторів інфраструктури, впливу зовнішніх чинників природного й соціально-політичного характеру, техногенних чинників, оцінки ризиків і на рівні окремих об'єктів, і для регіонів та держави загалом;

• *Офісу зв'язку НАТО в Україні* продовжити спільні зусилля з українськими державними органами та недержавними організаціями з метою розвитку міжнародного співробітництва, обміну досвідом і знаннями з питань захисту критичної інфраструктури в Україні.

СПИСОК УЧАСНИКІВ

БАКАЛИНСЬКИЙ Олександр Олегович	заступник завідувача спеціальної кафедри № 2 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
БАРАБАШ Сергій Дмитрович	головний спеціаліст Департаменту спеціальних інформаційно-телекомунікаційних систем Адміністрації Держспецзв'язку
БЕНАТОВ Данило Емілович	старший викладач кафедри екології та технології рослинних полімерів ІХФ НТУУ «КПІ», завідувач лабораторії міжнародних науково-освітніх проектів Світового центру даних з геоінформатики та сталого розвитку
БЄГУН Василь Васильович	завідувач відділу Інституту проблем математичних машин і систем НАН України
БЖОЗОВСКІ Кшиштоф	головний експерт відділу захисту критичної інфраструктури Урядового центру з питань безпеки, Польща
БІРЮКОВ Дмитро Сергійович	старший консультант відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
БОГДАНОВ Олександр Михайлович	завідувач спеціальної кафедри №2 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
БОНДАРЕНКО Олег Олександрович	заступник директора департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Держспецзв'язку
БУГЕРА Валерій Фотійович	головний інспектор Міністерства внутрішніх справ України

БУРЛАКОВ Володимир Михайлович	директор департаменту спеціальної безпеки, начальник відділу технічного та криптографічного захисту інформації ДП НАЕК «Енергоатом»
ВАВРИК Олександр Богданович	співробітник Антитерористичного центру при СБУ
ВАСИЛИШИН Андрій Вікторович	співробітник Антитерористичного центру при СБУ
ГАВРИЛЕНКО Олексій Вадимович	начальник управління департаменту технічного захисту інформації Адміністрації Держспецзв'язку
ГЕРЕГ Каталін	заступник начальника відділу Департаменту координації захисту критичної інфраструктури Генерального директорату з питань ліквідації наслідків стихійних лих Міністерства внутрішніх справ Угорщини
ГЛУШКО Іван Миколайович	головний фахівець відділу організації та контролю охорони Управління контролю за охоронною діяльністю та режимом департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
ГОЛДА Олександр Леонідович	центр воєнно-стратегічних досліджень Національного університету оборони України
ГРАНОВСЬКИЙ Едуард Олексійович	президент ТОВ «Ризикон»
ГРЕЧАНІНОВ Віктор Федорович	начальник відділу забезпечення діяльності голови Державної служби України з надзвичайних ситуацій

ДАВИДЕНКО Анатолій Миколайович	заступник директора Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України
ДЕЗІРОН Олександр Вікторович	завідувач сектору забезпечення діяльності адміністрації та зв'язків із громадськістю Укргідромету України
ДІДЕЙЧУК Ігор Вікторович	старший офіцер відділу планування управління територіальної оборони Головного оперативного управління Генерального штабу ЗС України
ЄВДИН Олександр Миколайович	перший заступник начальника Українського науково-дослідного інституту цивільного захисту
ЖЕЛЕЗНЯК Марк Йосипович	завідувач відділу математичного моделювання оточуючого середовища Інституту проблем математичних машин і систем НАН України
ЗАДИРАКА Валерій Костянтинович	член-кореспондент НАН України, завідувач відділом № 140 Інституту кібернетики ім. В. М. Глушкова НАН України
ЗАСЛАВСЬКИЙ Володимир Анатолійович	професор кафедри математичної інформатики факультету кібернетики Київського національного університету імені Тараса Шевченка
ЗЕЛЬ Володимир Іванович	головний інженер КП «Київський метрополітен»
ІВАНЮТА Сергій Петрович	старший консультант відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
КАЧИНСЬКИЙ Анатолій Броніславович	головний науковий співробітник Національного інституту стратегічних досліджень
КЕЛДЕР Керсті	керівник Програми професійної підготовки Офісу зв'язку НАТО в Україні

КОВАЛЬ Сергій Михайлович	перший заступник директора ДП «Центру громадської безпеки 112» Державної служби з надзвичайних ситуацій
КОЛЕСНИК Вікторія Анатоліївна	головний інспектор Міністерства внутрішніх справ України
КОНДРАТОВ Сергій Іванович	старший науковий співробітник відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
КОЦЮБА Віктор Іванович	начальник відділу системного адміністрування ДП «Центр громадської безпеки 112» Державної служби з надзвичайних ситуацій
КРИВЕНКО Олександр Васильович	заступник командувача внутрішніх військ МВС України
КУДРИЦЬКА Наталія Василівна	старший науковий співробітник відділу виробничої інфраструктури Інституту економіки та прогнозування НАН України
КУЗЬМЕНКО Юрій Ігоревич	старший науковий співробітник Інституту проблем безпеки атомних електростанцій НАН України
КУНИЦЬКИЙ Ігор Миколайович	начальник відділу протидії актам ядерного тероризму, спеціальної перевірки та охорони об'єктів життєзабезпечення ДФЗ ЯУ та ЯМ ДФЗСБ ДП НАЕК «Енергоатом»
КУСЛІЙ Ігор Іванович	заступник директора департаменту цивільного захисту ДСНС
КУШКА Віктор Миколайович	начальник управління з питань ядерної захищеності Держатомрегулювання
ЛЕВЧЕНКО Олег Євгенович	начальник кафедри військової токсикології, радіології, медичного захисту Української військово-медичної академії

ЛИСЮК Микола Олександрович	заступник директора Національного НДІ охорони праці
ЛИТВИНЕНКО Олександр Валерійович	заступник директора Національного інституту стратегічних досліджень
ЛИТВИНОВ Віталій Васильович	завідувач кафедрою Чернігівського державного технологічного університету
ЛИФАР Володимир Олексійович	доцент Донецького національного технічного університету
ЛУЧКОВ В'ячеслав Іванович	головний спеціаліст відділу фізичного захисту, антитерористичної діяльності та охорони об'єктів Міненерговугілля
МАЙКО Віталій Іванович	віце-президент Всеукраїнської громадської організації «Український союз промисловців і підприємців»
МАКСИМЕНКО Євген Васильович	заступник завідувача спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
МАРКЄЄВА Оксана Дмитрівна	завідувач відділу стратегій реформування сектору безпеки Національного інституту стратегічних досліджень
МАТЯШЕНКО Валентин Михайлович	начальник відділу департаменту спеціальних інформаційно-телекомунікаційних систем Адміністрації Держспецзв'язку
МОЙСЄЄНКО Віктор Миколайович	начальник басейнової лабораторії моніторингу Дніпровського басейнового управління водних ресурсів Держводагентства України
МОРОЗОВ Анатолій Олексійович	директор Інституту проблем математичних машин і систем НАН України

МОХОР Володимир Володимирович	завідувач спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»
НІКІФОРУК Олена Ігорівна	старший науковий співробітник відділу виробничої інфраструктури Інституту економіки та прогнозування НАН України
ОВЕРЧЕНКО Сергій Миколайович	начальник Управління контролю за охоронною діяльністю та режимом Департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
ПІНЧУК Михайло Георгійович	заступник директора філії Каскад Київських ГЕС і ГАЕС ПАТ «Укргідроенерго»
ПОЛІЩУК Тарас Васильович	заступник директора департаменту запобігання надзвичайним ситуаціям та державного нагляду (контролю), начальник управління техногенної безпеки Державної служби України з надзвичайних ситуацій
ПОПОВ Юрій Вікторович	начальник відділу перепускного режиму Управління контролю за охоронною діяльністю та режимом департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
ПУНДА Юрій Васильович	кафедра стратегії національної безпеки і оборони Національного університету оборони України
РАССОВСЬКИЙ Вадим Леонідович	головний інженер, заступник генерального директора ПАТ «Укргідроенерго»
РАСТОПЧІН Сергій Олексійович	головний спеціаліст департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Держспецзв'язку

РОМАНЕЦЬ Микола Павлович	директор з розвитку та інвестицій ПрАТ «СТЕК»
РТІЩЕВ Олександр Сергійович	начальник відділу впровадження інформаційно-телекомунікаційних систем ДП «Центру громадської безпеки 112» Державної служби з надзвичайних ситуацій
РУДЕНКО Володимир Володимирович	директор філії Каскад Київських ГЕС і ГАЕС ПАТ «Укргідроенерго»
СИРОТА Олена Петрівна	начальник відділу нових викликів і роззброєння, МЗС
СКАЛЕЦЬКИЙ Юрій Миколайович	завідувач відділу екологічної та техногенної безпеки Національного інституту стратегічних досліджень
СЛОБОДЯНЮК Олександр Вікторович	головний фахівець відділу організації та контролю охорони Управління контролю за охоронною діяльністю та режимом Департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
СТЕФАНИШИН Дмитро Володимирович	провідний науковий співробітник Інституту телекомунікацій і глобального інформаційного простору НАН України
СТЕЦЕНКО Анатолій Анатолійович	президент ТОВ «Діагностика»
СУСЛОВ Сергій Миколайович	головний спеціаліст відділу нагляду у сфері техногенної безпеки управління техногенної безпеки Державної служби України з надзвичайних ситуацій
ТІЩЕНКО Андрій Володимирович	начальник відділу планування та моніторингу заходів цивільного захисту департаменту організації заходів цивільного захисту Державної служби України з надзвичайних ситуацій

ТОРБІН Владислав Федорович	професор кафедри військової токсикології, радіології, медичного захисту Української військово-медичної академії
ТРИГОЛОВ Олександр Іванович	головний фахівець відділу організації та контролю охорони Управління контролю за охоронною діяльністю та режимом департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»
ТРОФИМЧУК Олександр Миколайович	заступник директора з наукової роботи Інституту телекомунікацій і глобального інформаційного простору НАН України
ТУРУКІН Юрій Мстиславович	заступник начальника відділу охорони лінійної частини та стаціонарних об'єктів Управління охорони об'єктів та режиму ПАТ «Укртранснафта»
УСТИМЕНКО Олександр Володимирович	старший науковий співробітник Центру воєнно-стратегічних досліджень Національний університет оборони
ХЕЛЛЕНБЕРГ Тімо	генеральний директор *Hellenberg International*, Фінляндія
ЧЕНЧИК Андрій Миколайович	начальник відділу цивільного захисту, пожежної та загальної безпеки департаменту безпеки Міністерства інфраструктури України
ЯКОВЛЄВ Євген Олександрович	головний науковий співробітник Національного інституту стратегічних досліджень
ЯЦЕНКО Степан Степанович	заступник начальника Управління контролю за охоронною діяльністю та режимом Департаменту економічної безпеки та управління ризиками НАК «Нафтогаз України»

ЗМІСТ

Наукове видання

КОНЦЕПЦІЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЇЇ ВПРОВАДЖЕННЯ В УКРАЇНІ

Збірник матеріалів міжнародної науково-практичної конференції
(7-8 листопада 2013 р., Київ – Вишгород)

Науковий редактор: *М. Л. Рубанець*
Літературний редактор: *О. В. Москаленко*
Коректор: *О. В. Москаленко*
Комп'ютерне верстання: *Є. Ю. Стрижеус, Н. І. Палій*

Відповідальна за випуск: *Н. І. Палій*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел/факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua

Формат 60x84/16. Ум. друк. арк. 8,61.
Тираж 200 пр. Зам. № 170

ДП «НВЦ «Пріоритети»
01014, м. Київ, вул. Командарма Каменєва, 8, корп. 6
тел./факс: 254-51-51

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 3862 від 18.08.2010