Державно-приватне партнерство в системі забезпечення безпеки та стійкості критичної інфраструктури

О.Суходоля, д.н.держ.упр.,
завідувач відділу енергетичної та техногенної безпеки
Національного інституту стратегічних досліджень

Критична інфраструктура

системи та засоби, фізичні чи віртуальні, *настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів підривало би національну безпеку, національну економіку, загрожувало би здоров'ю чи безпеці населення, чи мало би результатом будь-яку комбінацію із переліченого* - **США** (USA PATRIOT ACT (2001))

активи (матеріальні ресурси, основні фонди), системи чи їх частини, *розташовані в країнах-членах, які є суттєвими для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, захищеності, економічного та соціального благополуччя людей, порушення їхнього функціонування або знищення матимуть значний вплив у країні-члені ЄС та призведуть до нездатності забезпечувати вказані функції* - **ЄС** (EU Directive 2008/114)

системи, мережі, об'єкти, ресурси*, які забезпечують реалізацію життєво важливих функцій та послуг і мають настільки велике значення, що їх знищення, пошкодження або виведення з ладу призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку країни, обороноздатності держави та забезпечення національної безпеки* - *пропозиції НІСД*

Критична інфраструктура

Дається визначення - «*об'єкти критичної інфраструктури* - ***підприємства, установи та організації незалежно від форми власності,*** *діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;*

Стаття 6 уточнює, що «*До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації (за визначеними галузями:….) та об'єкти потенційно небезпечних технологій і виробництв*»

- **Україна** (ЗУ «про основи забезпечення кібербезпеки України 2017/2163)

Критична інфраструктура *– **сукупність об'єктів,** які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;*

Об'єкт *критичної інфраструктури – **визначений у встановленому законодавством порядку** складовий елемент критичної інфраструктури, функціональність …. якого забезпечують реалізацію життєво важливих національних інтересів*

Законопроект «Про критичну інфраструктуру та її захист»

Критична інфраструктура

Власники/оператори *– **особи відповідальні за інвестиції та/або щоденне функціонування окремого об'єкту**, системи або її частини, що визначені як Європейська критична інфраструктура згідно з Directive EU 2008/114.*

Власники/оператори *– державний орган, підприємство, установа, організація, юридична та/або фізична **особа, який/яке/яка на правах власності, оренди, господарського відання, оперативного управління** або на інших законних підставах користується об'єктом критичної інфраструктури та відповідає за його поточне функціонування -*

Законопроект «Про критичну інфраструктуру та її захист»

Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури

Можливість формалізації та регламентації параметрів стійкості системи:

- штатний діапазон, рівень допустимих загроз, штатна процедура реагування;
- параметри критичних загроз системі, процедури допомоги від інших систем, час протидії загрозі;
- процедури реагування на кризу, час реагування;
- вимоги резервування, процедури відновлення, час відновлення
- допустимий діапазон та час обмеження функціональності, адаптація до нової ситуації;

штатний режим (зелений). На даному етапі суб'єктами державної системи захисту критичної інфраструктури здійснюється оцінка можливих загроз та аналіз ризиків їх реалізації, інформування про імовірні загрози. Функціонування інфраструктури здійснюється в нормальному режимі та правовому стані;

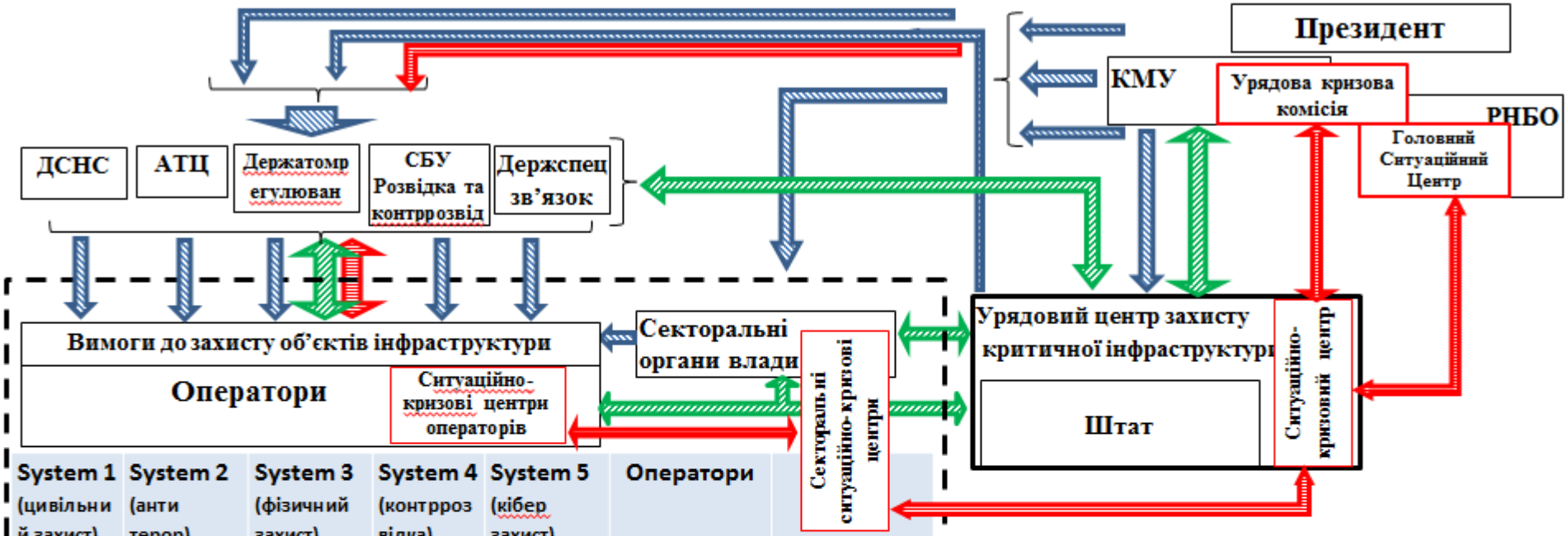
режим готовності та запобігання реалізації загроз (жовтий). На даному етапі суб'єктами державної системи захисту критичної інфраструктури здійснюється перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози, у рамках підготовлених Планів запобігання виникнення кризової ситуації. Функціонування інфраструктури здійснюється в нормальному режимі та правовому стані;

режим реагування на виникнення кризової ситуації (помаранчевий). На даному етапі суб'єктами державної системи захисту критичної інфраструктури застосовуються заходи реагування на кризову ситуацію в рамках планів реагування. Функціонування інфраструктури здійснюється в режимі кризової ситуації (надзвичайної ситуації), вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів.

режим відновлення штатного функціонування (блакитний). На даному етапі суб'єктами державної системи захисту критичної інфраструктури застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до проектного режиму. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи, в нормальному режимі та правовому стані;

Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури

Модель взаємодії в системі захисту критичної енергетичної інфраструктури



System 1 (цивільний захист)	System 2 (анти терор)	System 3 (фізичний захист)	System 4 (контрроз відка)	System 5 (кібер захист)	Оператори	
Об (1)	**Об (2)**	**Об (2)**		Об (3)	Operator 1	Sector 1 (зв'язок)
	Об (1)	Об (2)	Об (3)	Об (2)	Operator 2	
Об (1)	Об (2)		**Об (1)**		Operator 1	Sector 2 (енерго-)
		Об (1)	Об (2)	**Об (3)**	Operator 2	
Об (1)	**Об (2)**			Об (1)	Operator 3	
	Об (1)	**Об (2)**	**Об (2)**	Об (4)	Operator 1	Sector ... (фінанси)
			Об (1)	Об (2)	Operator 2	
Об (1)	Об (2)	**Об (3)**			Operator 1	Sector 10
			Об (1)	**Об (2)**	Operator 2	

Об (х) - Об'єкти, управління якими здійснюють оператори інфраструктури у відповідних секторах.

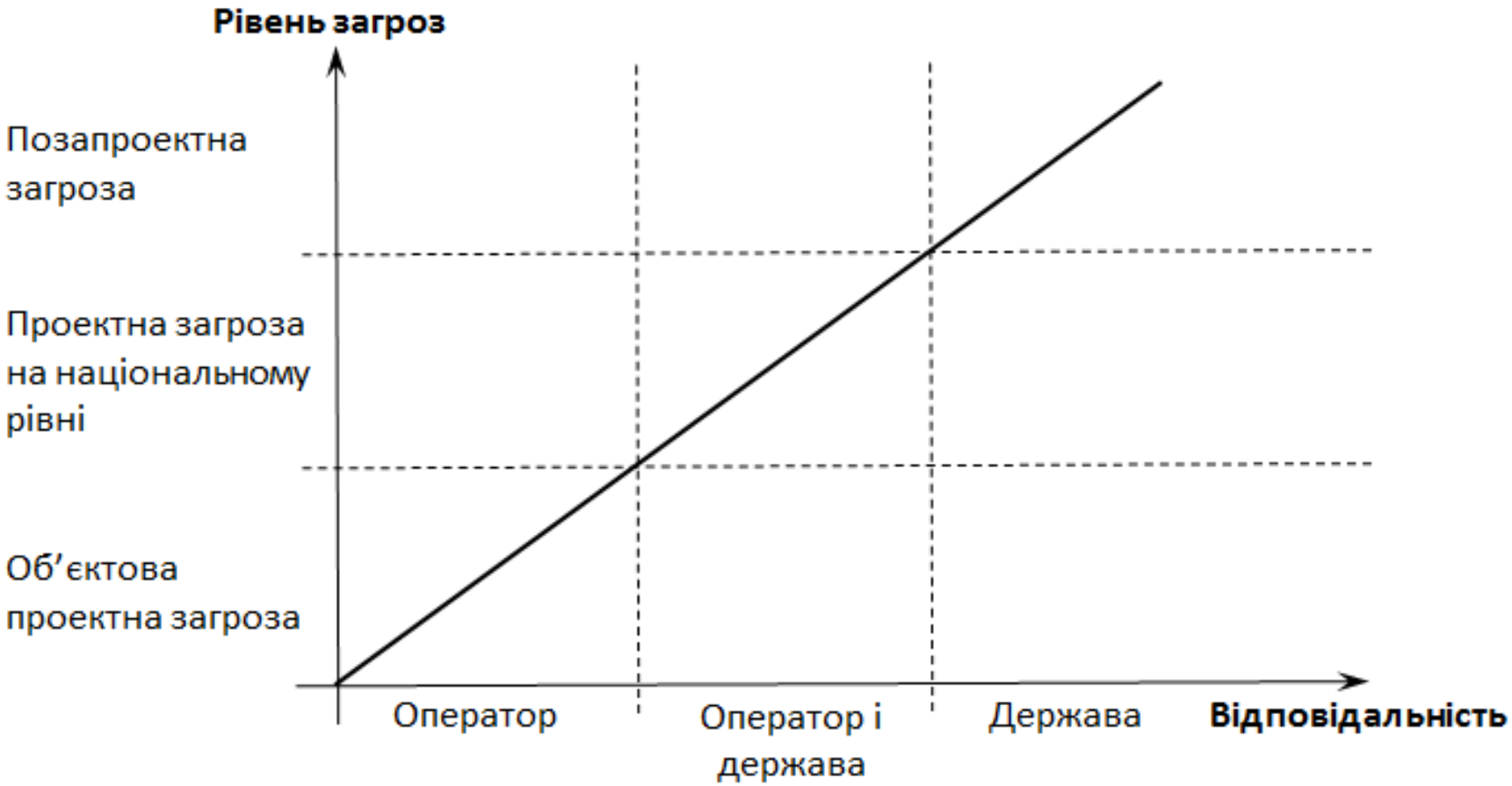
Об (х) виділенні червоним кольором – об'єкти внесені до Переліку критичної інфраструктури

Стрілки синього кольору (заштрихована з нахилом вліво) – основний напрям доведення законодавчих та організаційних вимоги до захисту критичної інфраструктури

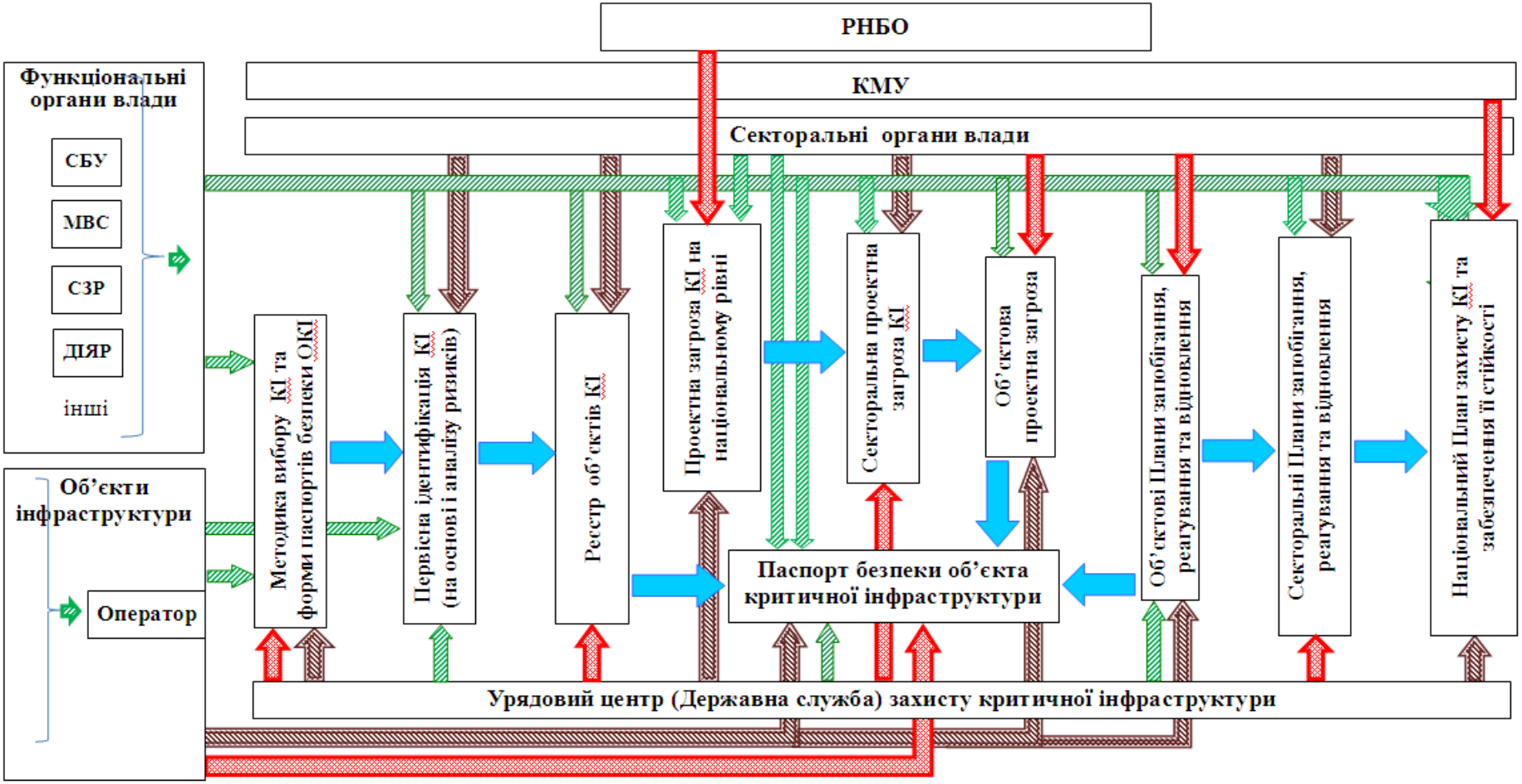
Стрілки зелений колір (заштрихована з нахилом вправо) – основні напрями обміну інформацією та взаємодії у нормальному режимі

Стрілки червоного кольору (заштрихована горизонтально) – основні напрями інформаційних повідомлень в кризовому режимі

Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури



Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури



Пояснення:

Стрілка, заштрихована з нахилом вправо (зелена): суб'єкт системи, що надає інформацію, пропозиції та/або погоджує документ.

Стрілка, заштрихована з нахилом вліво (коричнева): суб'єкт системи, що розробляє проект документу.

Стрілка, заштрихована хрестиком (червона): суб'єкт системи, що затверджує документ.

Стрілка суцільна (синя) – зв'язок між документами.

Вимоги до захисту

Паспорт безпеки

Проектна загроза

Плани реагування

Плани взаємодії

Чутливість інформації

Державна таємниця

Комерційна таємниця

Приватні права на захист інформації

Механізм взаємодії та обміну інформацією

Фінансування заходів безпеки

Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури

ЗМІСТ

Передмова 7

Розділ 1. **Система безпеки та стійкості критичної інфраструктури – невід'ємний елемент системи національної безпеки** 11

Розділ 2. **Світовий досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури** 31

Розділ 3. **Методологічні та організаційні засади забезпечення діяльності системи безпеки та стійкості критичної інфраструктури** 87

3.1. Модель організації взаємодії залучених суб'єктів у рамках державної системи захисту критичної інфраструктури 87

3.2. Ситуаційно-кризові центри в системі захисту критичної інфраструктури 110

3.3. Ризик-аналіз у системі захисту критичної інфраструктури 115

3.4. Методологія віднесення інфраструктурних об'єктів і систем до критичної інфраструктури 124

3.5. Проектна загроза у системі захисту критичної інфраструктури 134

3.5.1. Модель порушника та модель загрози протиправних дій . . . 135

3.5.2. Модель загроз та проектна загроза критичній інфраструктурі 139

3.6. Паспорти безпеки об'єктів критичної інфраструктури 144

3.6.1. Нормативно-правові засади формування вимог до захисту об'єктів критичної інфраструктури 144

3.6.2. Основні вимоги до розробки паспортів безпеки об'єктів критичної інфраструктури 147

3.7. Проведення навчань і тренувань 151

Державно-приватне партнерство в системі забезпечення захисту і стійкості критичної інфраструктури

Додатки 166

Додаток 1. Інструменти формалізації діяльності у сфері захисту критичної інфраструктури 166

1.1. План захисту критичної інфраструктури 166

1.2. План реагування на випадок кризової ситуації 168

1.3. Проведення ризик-аналізу 171

1.4. Перелік секторів критичної інфраструктури 173

1.5. Паспорт безпеки об'єкта/системи критичної інфраструктури . . 176

1.6. Проектна загроза критичній інфраструктури 180

Додаток 2. Пропозиції до Національного плану захисту критичної інфраструктури 184

Додаток 3. Пропозиції до проекту Закону України «Про критичну інфраструктуру» 199

Додаток 4. Глосарій 219

Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:

- обміну інформацією між державними органами, приватним та громадським сектором і громадянами щодо загроз об’єктам критичної інфраструктури та кризових ситуацій на цих об’єктах;
- підвищення комплексних знань, навичок і вмінь громадян з питань захисту критичної інфраструктури;
- залучення експертного потенціалу, наукових установ, професійних об’єднань та громадських організацій до підготовки галузевих проектів та нормативних документів у сфері захисту критичної інфраструктури;
- надання консультативної та практичної допомоги з питань реагування на кризові ситуації на об’єктах критичної інфраструктури;
- запровадження механізму громадського контролю ефективності заходів із захисту критичної інфраструктури;
- створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань захисту критичної інфраструктури;
- організації забезпечення захисту персоналу від можливих загроз;
- забезпечення резервування основних ресурсів для функціонування об’єкта критичної інфраструктури у різних режимах;
- оповіщення місцевого населення про інциденти та кризові ситуації на об’єктах критичної інфраструктури.

Страхування ризиків у сфері критичної інфраструктури

Страхування ризиків у сфері критичної інфраструктури здійснюється шляхом:

- запровадження страхування об'єктів критичної інфраструктури від пошкодження внаслідок впливу стихійних лих або техногенних катастроф та від протиправних дій третіх осіб;
- запровадження цивільної відповідальності операторів критичної інфраструктури за шкоду, яку може бути заподіяно припиненням функціонування та/або аваріями на об'єктах критичної інфраструктури, зумовленими невиконанням операторами критичної інфраструктури вимог законодавства у сфері захисту критичної інфраструктури.

Страхування об'єктів критичної інфраструктури здійснюється у встановленому Кабінетом Міністрів України порядку. Страхування є обов'язковим стосовно об'єктів критичної інфраструктури, включених до Реєстру критичної інфраструктури.

Для створення умов та координації діяльності, пов'язаної із забезпеченням страхування у сфері критичної інфраструктури, забезпечення фінансової надійності страхування створюється страховий фонд безпеки критичної інфраструктури (Страховий пул безпеки інфраструктури).

Порядок проведення розслідувань припинення функціонування та/або аварій на об'єктах критичної інфраструктури встановлюється Кабінетом Міністрів України відповідно до вимог цього та інших законів.

Джерела забезпечення заходів із захисту критичної інфраструктури

Джерелами здійснення заходів із захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредитні та інвестиційні ресурси, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Для фінансування заходів за окремими напрями створюються цільові механізми, а саме:

– для формування власних цільових видатків ресурсів операторів критичної інфраструктури – включення до тарифів (цін) на послуги (продукцію) 50 відсотків видатків суб'єктів господарювання, здійснених на виконання вимог, визначених Законом;

– для заходів, включених до секторальних планів захисту критичної інфраструктури, – включення до валових витрат 50 відсотків видатків суб'єктів господарювання на реалізацію заходів;

– для створення мінімальних запасів ресурсів (обладнання) – залучення приватних ресурсів у рамках державно-приватного партнерства;

– для створення ринкового механізму інвестування у заходи безпеки – створення механізму страхування ризиків у сфері захисту критичної інфраструктури.

Виключний перелік заходів секторальних планів забезпечення захисту критичної інфраструктури та вимог Закону, щодо яких застосовуються вищезазначені механізми фінансування затверджуються Кабінетом Міністрів України.

Дякую за увагу!

Запрошуємо до активної участі до формування засад державно-приватного партнерства в системі забезпечення захисту і стійкості критичної інфраструктури

Суходоля О.М.
sam@niss.gov.ua