ЗАТВЕРДЖУЮ
Голова Державної служби спеціального зв'язку та захисту інформації України
Юрій ЩИГОЛЬ

«___» листопада 2023 року

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі

І. Загальні положення

1. Ці Методичні рекомендації розроблені з метою визначення механізму підготовки проектних загроз критичній інфраструктурі секторального та об'єктового рівнів та оцінки загроз критичній інфраструктурі, що сприятиме забезпеченню уніфікованого підходу для проведення оцінки загроз у сфері захисту критичної інфраструктури, розробки та затвердження проектних загроз.

2. Ці Методичні рекомендації можуть використовуватися секторальними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури під час розроблення проектних загроз секторального та об'єктового рівнів відповідно, а також для оцінки загроз критичній інфраструктурі.

3. У цих Методичних рекомендаціях терміни вживаються в такому значенні:

аналізування загрози – визначення ймовірності реалізації загрози за п'ятибальною шкалою, можливого її впливу на критичну інфраструктуру та можливих наслідків від її реалізації;

вразливість об'єкта критичної інфраструктури (далі – вразливість) – нездатність витримувати обставини непереборної сили; міра чутливості до уражень, пошкоджень; слабке місце одного з елементів об'єкта захисту; фактор реалізації загрози;

ідентифікація загроз – процес визначення, аналізу та опису загроз, які можуть виникнути в певному контексті або від певних дій, явищ, подій або впливів. Кожна сторона, задіяна в підготовці проектної загрози, проводить ідентифікацію загрози на своєму рівні;

оцінка наслідків реалізації загрози - визначення величини впливу загрози на цільові параметри функціонування критичної інфраструктури за п'ятибальною шкалою;

ранжування загроз – визначення загроз у порядку відповідно до загального рівня наслідків її реалізації на об'єктах/об'єкті критичної інфраструктури сектору з визначеною ймовірністю;

рівень загрози – величина, що визначається шляхом перемноження визначеної ймовірності загрози на результат оцінки наслідків реалізації загрози.

Інші терміни вживаються у значенні, наведеному в Законі України «Про критичну інфраструктуру» та постанові Кабінету Міністрів України від 04.08.2023 № 818 «Деякі питання паспортизації об'єктів критичної інфраструктури».

II. Оцінка та ранжування загроз

1. Для оцінки та ранжування загроз можуть використовуватися такі документи та інформаційні матеріали:

інформаційні матеріали про інциденти, що сталися на об'єкті критичної інфраструктури в минулому, наслідки та вжиті заходи щодо їх мінімізації або ліквідації;

документація щодо стану захищеності об'єкта критичної інфраструктури;

інформація щодо порушень режиму функціонування об'єкта критичної інфраструктури;

інформація про надзвичайні ситуації, що сталися на території регіону, де розміщено об'єкт критичної інфраструктури;

дані ситуаційних центрів про події, що можуть вплинути на функціонування об'єкта критичної інфраструктури;

попередження секторальних органів у сфері захисту критичної інфраструктури про загрози операторів критичної інфраструктури;

плани (проєкти) модернізації та розвитку об'єктів критичної інфраструктури.

Зазначений перелік не є вичерпним.

2. Оцінка та ранжування загроз передбачає ідентифікацію загрози, аналізування загрози, оцінку наслідків реалізації загрози, визначення рівня загрози, ранжування загроз відповідно до їх визначених рівнів.

3. Оцінку та ранжування загроз доцільно здійснювати у послідовності, визначеній у додатку 1 до цих Методичних рекомендацій.

4. У ході ідентифікації загроз можливе використання орієнтовного переліку загроз, визначеного у додатку 2 до цих Методичних рекомендацій.

5. Кожна загроза визначається як окремий об'єкт (подія), що має ідентифікатор, назву, опис, характеристики/сценарії та зв'язки із суб'єктами, до яких виникає звернення у випадку реалізації загрози.

6. У ході оцінки загроз необхідно враховувати:

зовнішні та внутрішні чинники, що можуть вплинути на режим функціонування об'єкта критичної інфраструктури;

тип об'єкта/належності до певного сектору;

плани управління об'єкта критичної інфраструктури;

вразливості об'єкта критичної інфраструктури;

наявну інформацію щодо потенційних та реальних загроз, що отримується від суб'єктів національної системи захисту критичної інфраструктури;

відповідні рекомендації функціональних органів у сфері захисту критичної інфраструктури.

7. При розробленні проектних загроз секторального/об'єктового рівня необхідно керуватися принципом функціональної повноти та враховувати повний обсяг можливих негативних впливів на об'єкти критичної інфраструктури.

8. Після проведення оцінки та ранжування загроз критичній інфраструктурі визначається, які саме загрози будуть віднесені до проектних загроз секторального/об'єктового рівня.

9. Результатом оцінки та ранжування загроз критичній інфраструктурі є розроблена та затверджена для кожного сектору та об'єкта критичної інфраструктури відповідна проектна загроза.

10. Проектна загроза враховується при розробленні (перегляді) паспорта безпеки на кожний об'єкт критичної інфраструктури.

ІІІ. Структура та опис проектної загрози

1. Проектні загрози у структурованому вигляді містить перелік загроз для сектора/об'єкта критичної інфраструктури.

2. Форма проектних загроз критичній інфраструктурі секторального та об'єктового рівнів затверджена наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 28.07.2023 № 219/ДСК. При її заповненні необхідно враховувати особливості різних типів об'єктів критичної інфраструктури.

3. Оператори критичної інфраструктури розробляють і затверджують проектні загрози об'єктового рівня з додаванням загроз, властивих конкретному об'єкту критичної інфраструктури.

4. Секторальні органи розробляють і затверджують проектні загрози секторального рівня з додаванням загроз, властивих конкретному сектору критичної інфраструктури.

5. Перегляд проектних загроз критичній інфраструктурі секторального та об'єктового рівнів рекомендується здійснювати на постійній основі не рідше ніж один раз на рік.

Директор Департаменту захисту критичної
інфраструктури Адміністрації Держспецзв'язку
08.11.2023 Андрій ЧОТЧИКОВ

Додаток 1
до Методичних рекомендацій щодо розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі

ПОСЛІДОВНІСТЬ
розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівня та оцінки загроз критичній інфраструктурі

1. Оцінка загроз критичній інфраструктурі секторального рівня та розробка проектних загроз критичній інфраструктурі секторального рівня може здійснюватися структурними підрозділами з питань захисту критичної інфраструктури, створеними у складі секторального органу у сфері захисту критичної інфраструктури.

2. Оцінка загроз критичній інфраструктурі об'єктового рівня та розробка проектних загроз критичній інфраструктурі об'єктового рівня можуть здійснюватися окремими структурними підрозділами з питань захисту критичної інфраструктури, що можуть бути створені операторами критичної інфраструктури.

3. До оцінки загроз критичній інфраструктурі доцільно залучати в установленому порядку інших фахівців сектору/об'єкта, а також представників функціональних органів, місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, наукових установ та організацій.

4. Ідентифікація загрози полягає в її виявленні, аналізі та формалізації у змістовній формі. На секторальному та об'єктовому рівнях формалізація опису загрози здійснюється з урахуванням секторальних особливостей та об'єктових характеристик критичної інфраструктури.

5. Для оцінок ймовірностей загрози та наслідків її реалізації може бути встановлена така градація (у балах):

для загальних ймовірностей: «низька» (1), «помірно низька» (2), «середня» (3), «помірно висока» (4), «висока» (5);

для оцінки наслідків реалізації загрози: «незначні» (1), «неістотні» (2), «помірні» (3), «істотні» (4), «катастрофічні» (5).

6. При визначенні ймовірності необхідно враховувати наявні статистичні дані та дослідження щодо інцидентів, що мали місце на конкретному об'єкті критичної інфраструктури, на аналогічних об'єктах критичної інфраструктури та/або у секторі в цілому.

Продовження додатка 1

7. При оцінці наслідків реалізації загрози необхідно враховувати дані у сукупності щодо наслідків інцидентів, що мали місце на об'єктах критичної інфраструктури в минулому, а також результати прогнозування негативних наслідків та/або моделювання кризових ситуацій, що могли б мати місце у випадку реалізації потенційних загроз.

8. При оцінці наслідків реалізації загрози можуть враховуватися показники шкоди життю та здоров'ю людей, матеріальна шкода, час припинення надання послуг об'єктом критичної інфраструктури та час, необхідний для відновлення штатного режиму функціонування об'єкта.

Орієнтовний перелік критеріїв оцінювання наслідків впливу реалізації загрози:

чисельність постраждалого населення (вимушена міграція чи потреба прихистку, евакуації, допомоги);

зниження рівня надання життєво важливих функцій та/або послуг;

час, необхідний для відновлення надання життєво важливих функцій та/або послуг;

економічні збитки;

шкода довкіллю;

зниження рівня обороноздатності;

вплив на інші сектори/об'єкти критичної інфраструктури;

публічне сприйняття ситуації, спричинене впливом загрози.

Перелік критеріїв може змінюватися/уточнюватися з урахуванням специфіки сектору/об'єкта критичної інфраструктури.

9. Після визначення ймовірності реалізації загрози та оцінки наслідків її реалізації визначається рівень загрози шляхом помноження балу ймовірності на бал наслідків.

10. Отримані значення в балах вносять до таблиці ранжування загроз (таблиця).

Таблиця

Таблиця ранжування загроз

Ранжування №	Назва загрози	Ймовірність загрози	Оцінка наслідків	Рівень загрози

11. На підставі ранжування приймається рішення щодо віднесення визначених загроз до проектних загроз критичній інфраструктурі секторального/об'єктового рівня.

12. Приклад практичного застосування цих Методичних рекомендацій наведено у додатку 3 до Методичних рекомендацій щодо розробки проектних

Продовження додатка 1

загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі.

Додаток 2
до Методичних рекомендацій щодо розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі

ОРІЄНТОВНИЙ ПЕРЕЛІК ЗАГРОЗ

1. Загрози воєнного характеру:
1.1. Застосування зброї масового ураження.
1.2. Ракетні удари.
1.3. Удари із застосуванням авіаційних засобів.
1.4. Артилерійські обстріли.
1.5. Удари із застосуванням безпілотних літальних апаратів.
1.6. Проникнення диверсійно-розвідувальних груп.
1.7. Розвідувально-підривна діяльність іноземних спеціальних служб.
2. Терористичні загрози.
3. Диверсії.
4. Кіберзагрози:
4.1. Загрози порушення цілісності, конфіденційності та доступності інформації, що обробляється в системах об'єкта.
4.2. Загрози пов'язані з відсутністю резервних каналів зв'язку та резервних джерел безперебійного живлення.
5. Інформаційні загрози.
6. Загрози соціального характеру:
6.1. Збройні напади, захоплення й утримування об'єктів критичної інфраструктури або реальна загроза їх здійснення.
6.2. Використання вибухового пристрою на об'єкті критичної інфраструктури.
6.3. Масові заворушення, страйки тощо.
6.4. Завідомо неправдиві (анонімні) повідомленням про загрозу безпеці громадян, знищення чи пошкодження об'єктів критичної інфраструктури.
7. Загрози техногенного характеру:
7.1. Пов'язані з аваріями чи катастрофами на об'єктах критичної інфраструктури.
7.2. Пов'язані з пожежами та/або вибухами на об'єктах критичної інфраструктури.
7.3. Пов'язані з викиданням (загрозою викидання) у навколишнє середовище шкідливих (забруднювальних) і/або радіоактивних речовин.
7.4. Пов'язані із руйнуванням будівель і споруд об'єктів критичної інфраструктури.
7.5. Пов'язані з аваріями у системах життєзабезпечення.
7.6. Пов'язані з аваріями систем електронних комунікацій.
7.7. Пов'язані з аваріями на очисних спорудах.
7.8. Гідродинамічна аварія.
8. Дії персоналу, пов'язані з його недостатньою кваліфікацією або низьким рівнем підготовки.

Продовження додатка 2

9. Загрози природного характеру:
9.1. Геофізичні:
пов'язані із землетрусом.
9.2. Геологічні:
пов'язані зі зсувом;
пов'язані з обвалом або осипом;
пов'язані з осіданням (проваллям) земної поверхні;
пов'язані з карстовими провалами;
пов'язані з підвищенням рівня ґрунтових вод (підтопленням).
9.3. Метеорологічні:
пов'язані з атмосферними опадами;
пов'язані із сильною зливою (кількість опадів 30 мм і більше, тривалістю 1 година і менше);
пов'язані з крупним градом (діаметром 20 мм і більше);
пов'язані з дуже сильним снігопадом (кількість опадів 20 мм і більше, тривалістю 12 годин і менше);
пов'язані з дуже сильним дощем (дощ і мокрий сніг) (кількість опадів 50 мм і більше, тривалістю 12 годин і менше; для гірських районів 30 мм і більше, тривалістю 12 годин і менше);
пов'язані з дуже сильним морозом (температура повітря мінус 30° С і нижче);
пов'язані з дуже сильною спекою (температура повітря 35° С і вище);
пов'язані з масовим засиханням та загибеллю посівів і створених 1 – 3-річних лісових культур унаслідок засухи;
пов'язані з масовим пошкодженням і загибеллю посівів, незібраним урожаєм, унаслідок заморозків;
пов'язані із сильним вітром (швидкістю 25 м/с і більше), охоплюючи шквали та смерчі;
пов'язані із сильною пиловою бурею (за швидкості вітру 15 м/с і більше, тривалістю 12 годин і більше);
пов'язані із сильним налипанням снігу (шар мокрого замерзлого снігу на деревах, стовбурах, дротах електромереж тощо діаметром 35 мм і більше);
пов'язані із сильною ожеледдю (шар льоду на деревах, дротах електромереж тощо діаметром 20 мм і більше);
пов'язані зі сніговими заметами (повне припинення руху транспорту на шляхах);
пов'язані із сильною хуртовиною (за швидкості вітру 15 м/с і більше, тривалістю 12 годин і більше);
пов'язані із сильним туманом (видимість менше 100 м, тривалістю 12 годин і більше).
9.4. Гідрологічні морські:
пов'язані із сильним (високим) хвилюванням моря та на водосховищі;
пов'язані з високим або низьким рівнем моря;
пов'язані з раннім льодоставом або припаєм;
пов'язані із загрозливим обледенінням суден.
9.5. Гідрологічні поверхневих вод:
пов'язані з високим рівнем води (водопілля, паводки);

пов'язані з маловоддям/посухою (маловоддя);
пов'язані із заторами, зажорами;
пов'язані із селем;
пов'язані зі сходом снігової лавини;
пов'язані з низьким рівнем води;
пов'язані з раннім льодоставом та появою льоду на судноплавних водоймах і річках;
пов'язані із затопленням.
9.6. Пов'язані з пожежами в природних екологічних системах.
9.7. Медико-біологічні:
пов'язані з інфекційним захворюванням людей;
пов'язані з екзотичним та особливо небезпечним інфекційним захворюванням людей (окремі випадки);
пов'язані з небезпечною інфекційною хворобою (групові випадки);
пов'язані з епідемічним спалахом небезпечних інфекційних хвороб;
пов'язані з епідемією.
9.8. Пандемія.
9.9. Панзоотія.
9.10. Панфітотія.

Зазначений орієнтовний перелік не є вичерпним. Рекомендується у ході розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівня та оцінки загроз критичній інфраструктурі розглядати всі потенційні та реальні загрози, що можуть бути властиві конкретному сектору/об'єкту критичної інфраструктури.

Додаток 3
до Методичних рекомендацій щодо розробки проектних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі

ПРИКЛАД
практичного застосування Методичних рекомендацій на основі оцінки загроз у сфері захисту критичної інфраструктури об'єктового рівня.

Наведені у прикладі дані є вигадані та застосовуються лише для візуалізації практичного застосування цих Методичних рекомендацій.

Об'єкт критичної інфраструктури – «Комунальне некомерційне підприємство «Обласна лікарня № 1».

Для зазначеного об'єкта критичної інфраструктури ідентифіковано 5 загроз, а саме:

землетрус;

перебої з електропостачанням;

перебої з водопостачанням;

ракетний удар;

службова недбалість (випадкові дії або бездіяльність).

З урахуванням наявних статистичні даних щодо інцидентів, що мали місце на вказаному об'єкті та на аналогічних об'єктах сектору критичної інфраструктури, а також шляхом прогнозування можливості реалізації загроз були присвоєні такі бали:

землетрус: «ймовірність реалізації загрози середня» – 3 бали;

перебої з електропостачанням: «ймовірність реалізації помірно висока» – 4 бали;

перебої з водопостачанням: «ймовірність реалізації помірно висока» – 4 бали;

ракетний удар: «ймовірність реалізації загрози висока» – 5 балів;

службова недбалість (випадкові дії або бездіяльність): «ймовірність реалізації загрози помірно середня» – 2 бали.

З урахуванням сукупних даних щодо наслідків інцидентів, що мали місце на об'єктах критичної інфраструктури в минулому, прогнозування негативних наслідків, що могли б мати місце у випадку реалізації потенційних загроз, а також моделювання кризових ситуацій кожній ідентифікованій загрозі присвоєно такі бали оцінки рівня наслідків її реалізації:

землетрус: «наслідки помірні» – 3 бали;

перебої з електропостачанням: «наслідки незначні» – 1 бал;

перебої з водопостачанням: «наслідки істотні» – 4 бали;

ракетний удар: «наслідки катастрофічні» – 5 балів;

службова недбалість (випадкові дії або бездіяльність): «наслідки неістотні» – 2 бали.

Продовження додатка 3

Після цього проводиться підрахунок рівня загрози шляхом множення умовного балу ймовірності на умовний бал наслідків для кожної загрози окремо.

Землетрус: ймовірність (3 бали) х оцінку наслідків (3 бали) = 9 балів.

НАСЛІДКИ						
	Катастрофічні (5)	5	10	15	20	25
	Істотні (4)	4	8	12	16	20
	Помірні (3)	3	6	9	12	15
	Неістотні (2)	2	4	6	8	10
	Незначні (1)	1	2	3	4	5
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		ЙМОВІРНІСТЬ				

Перебої з електропостачанням: ймовірність (4 бали) х оцінку наслідків (1 бал) = 4 бали.

НАСЛІДКИ						
	Катастрофічні (5)	5	10	15	20	25
	Істотні (4)	4	8	12	16	20
	Помірні (3)	3	6	9	12	15
	Неістотні (2)	2	4	6	8	10
	Незначні (1)	1	2	3	4	5
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		ЙМОВІРНІСТЬ				

Продовження додатка 3

Перебої з водопостачанням: ймовірність (4 бали) х оцінку наслідків (4 бали) = 16 балів

НАСЛІДКИ						
	Катастрофічні (5)	5	10	15	20	25
	Істотні (4)	4	8	12	16	20
	Помірні (3)	3	6	9	12	15
	Неістотні (2)	2	4	6	8	10
	Незначні (1)	1	2	3	4	5
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		ЙМОВІРНІСТЬ				

Ракетний удар: ймовірність (5 балів) х оцінку наслідків (5 балів) = 25 балів.

НАСЛІДКИ						
	Катастрофічні (5)	5	10	15	20	25
	Істотні (4)	4	8	12	16	20
	Помірні (3)	3	6	9	12	15
	Неістотні (2)	2	4	6	8	10
	Незначні (1)	1	2	3	4	5
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		ЙМОВІРНІСТЬ				

Продовження додатка 3

Службова недбалість (випадкові дії або бездіяльність): ймовірність (2 бали) х оцінку наслідків (2 бали) = 4 бали.

НАСЛІДКИ						
	Катастрофічні (5)	5	10	15	20	25
	Істотні (4)	4	8	12	16	20
	Помірні (3)	3	6	9	12	15
	Неістотні (2)	2	4	6	8	10
	Незначні (1)	1	2	3	4	5
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		ЙМОВІРНІСТЬ				

Визначивши рівень загроз у балах, проводиться їх ранжування від більшого до меншого значення. Результати ранжування оцінених загроз наведено в таблиці.

Таблиця

Ранжування №	Назва загрози	Ймовірність загрози	Оцінка наслідків	Рівень загрози
1	Ракетний удар	5	5	25
2	Перебої з водопостачанням	4	4	16
3	Землетрус	3	3	9
4	Перебої з електропостачанням	4	1	4
5	Службова недбалість (випадкові дії або бездіяльність)	2	2	4

Після завершення ранжування загроз приймається рішення про те, які саме загрози мають бути віднесені до проектних загроз секторального/об'єктового рівня.