



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

вул. Володимирська, 33, м. Київ, 01601, тел./факс: (044) 226-34-31, тел. 256-99-05
www.sbu.gov.ua, e-mail: sbu_cu@ssu.gov.ua Код ЄДРПОУ 00034074

24.01.22 № 33/5-373 м

На № _____ від _____

**Голові Державної регуляторної служби України
Олексію КУЧЕРУ**

*Щодо погодження проекту
регуляторного акта*

Шановний пане Олексію!

Службою безпеки України розроблено проекти Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження.

Відповідно до статті 21 Закону України “Про засади державної регуляторної політики у сфері господарської діяльності” направляємо на погодження зазначені проекти актів.

- Додатки:
1. Проект Правил антитерористичної безпеки на 16 арк.
 2. Проект постанови Кабінету Міністрів України “Про затвердження Правил антитерористичної безпеки” на 1 арк.
 3. Пояснювальна записка до проекту постанови Кабінету Міністрів України “Про затвердження Правил антитерористичної безпеки” на 2 арк.
 4. Аналіз регуляторного впливу до проекту Правил антитерористичної безпеки, прим. № 1 на 15 арк., підлягає поверненню.
 5. Копія повідомлення про оприлюднення проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження на 1 арк.
 6. Скріншот з вебсайту Служби безпеки України зі змінами до Плану діяльності Служби безпеки України з підготовки проектів регуляторних актів на 2022 рік на 1 арк.

З повагою

Голова Служби

Іван БАКАНОВ

Олександр ТЕЛЬНІК
503-05-21

0.31

Державна регуляторна служба України
№ 832/0/19-22 від 26.01.2022



ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2022 р. № _____

Правила антитерористичної безпеки

І. Загальні положення

1.1. Правила антитерористичної безпеки встановлюють механізм віднесення об'єктів нерухомості до об'єктів можливих терористичних посягань та загальні обов'язкові вимоги щодо цих об'єктів, спрямовані на забезпечення їх антитерористичної захищеності.

1.2. У цих Правилах терміни вживаються у такому значенні:

антитерористична безпека - захищеність об'єктів можливих терористичних посягань від терористичних загроз;

антитерористичний захист - діяльність, спрямована на забезпечення захищеності об'єктів можливих терористичних посягань, запобігання та припинення терористичних посягань, мінімізацію їх наслідків шляхом запровадження системи координованих організаційних, правових, адміністративних, охоронних, режимних, технічних та інших антитерористичних заходів;

втрати безпеки життєдіяльності - втрати, що полягають у забрудненні, зіпсуванні, знищенні або зараженні в результаті терористичних посягань довкілля та природних ресурсів (земель, надр, водних ресурсів, атмосферного повітря, рослинного і тваринного світу, об'єктів та територій природно-заповідного фонду, сільськогосподарських угідь, посівів, поголів'я тварин тощо), і відображаються у відповідних кількісних показниках;

екологічна шкода - шкода, пов'язана із забрудненням, псуванням, знищенням або зараженням внаслідок терористичних посягань навколишнього природного середовища та природних ресурсів (земель, надр, вод, атмосферного повітря, лісу та іншої рослинності, тваринного світу), ландшафтів та інших природних комплексів, територій та об'єктів природно-заповідного фонду України, а також із здоров'ям та життям людей; попередження та ліквідація наслідків екологічної шкоди запроваджується із застосуванням принципу "забруднювач-платник", а також із дотриманням принципу довготривалого розвитку;

економічні втрати - втрати, виражені у вартісному (грошовому) вигляді, які пов'язані з прямими та непрямими фінансовими, матеріально-ресурсними, майновими, виробничими та іншими збитками, завданими власнику об'єкта внаслідок терористичних посягань;

ідентифікація - це процес віднесення будь-якого об'єкта нерухомості до об'єкта можливих терористичних посягань та визначення його категорії з урахуванням масштабів і видів імовірних втрат відповідно до прогнозованої загрози;

людські втрати - втрати, пов'язані із загибеллю (позбавленням життя) і травмуванням (завданням тілесних ушкоджень різного ступеня тяжкості) людей внаслідок терористичних посягань

об'єкт можливих терористичних посягань - визначені в постанові Кабінету Міністрів України від 18 лютого 2016 р. № 92 "Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків" (Офіційний вісник України, 2016 р., № 16, ст. 655) об'єкти нерухомого майна, захоплення, блокування роботи, пошкодження або руйнування яких може використовуватися для досягнення терористичних цілей;

паспорт антитерористичної захищеності об'єкта можливих терористичних посягань - документ із відомостями про призначення такого об'єкта, особливості його розташування, основні технічні характеристики та систему захисту тощо, обов'язковий для врахування під час побудови системи забезпечення антитерористичної захищеності;

прогнозована загроза - модель можливих максимально негативних наслідків терористичних посягань відповідно до наявних терористичних загроз, визначених відповідно до цих Правил, щодо об'єкта можливих терористичних посягань;

система забезпечення антитерористичної захищеності - комплекс організаційно-правових, режимних та інших заходів, спрямованих на захист об'єктів від можливих терористичних посягань;

соціально-політична реакція суспільства - зміна соціально-політичних настроїв, інші події, що виникають в суспільстві, в т.ч. соціальні конфлікти та загрози з явно вираженими масовими негативними настроями суспільства;

суспільно-політичні втрати - критичне зниження рівня забезпечення охорони громадського порядку та громадської безпеки, захищеності основ національної безпеки (масові заворушення, дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади тощо), втрата довіри населення до державної влади, порушення керованості держави або регіону, нанесення шкоди авторитету держави та її органів, у тому числі на міжнародній арені, деморалізація, що призводить до зниження рівня боєготовності та боездатності Збройних Сил, інших утворених відповідно до закону військових формувань та правоохоронних органів;

терористична загроза - існуючі та потенційно можливі чинники, що створюють небезпеку вчинення терористичного акту щодо об'єкта можливих терористичних посягань та настання негативних наслідків від нього, в тому числі приховані або відкриті (висловлені) наміри вчинити терористичний акт;

терористичне посягання - підготовка, замах або вчинення суспільно небезпечної дії, такої як застосування зброї, вчинення вибуху, підпалу чи

інших суспільно небезпечних дій для досягнення терористичних цілей;

уразливі місця - критичні елементи об'єкта, місця використання або зберігання вибухо-, пожежо-, хімічно- або біологічно небезпечних речовин, а також виробничого устаткування об'єкта, дії у відношенні яких можуть привести до аварійної (надзвичайної) ситуації або створювати загрозу здоров'ю чи життю людей у результаті здійснення терористичного акту.

У цих правилах терміни вживаються у значенні, наведеному у Законі України "Про електронні комунікації".

1.3. Головною метою забезпечення антитерористичної безпеки є збереження життя та здоров'я громадян, майна фізичних або юридичних осіб, державного або комунального майна, навколишнього природного середовища, життя або здоров'я тварин і рослин, що знаходяться на цих об'єктах або на прилеглий до них місцевості.

1.4. Антитерористична безпека ґрунтується на принципах:

законності та неухильного додержання прав і свобод людини і громадянина – забезпечення антитерористичної захищеності об'єктів повинно забезпечуватися відповідно до національного та міжнародного законодавства і за дотримання при цьому основоположних прав і свобод людини і громадянина;

загальної обов'язковості – забезпечення антитерористичної захищеності об'єктів повинно бути обов'язковим завданням відповідних органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій незалежно від форм власності у підпорядкуванні або користуванні яких перебувають об'єкти, а також кожного громадянина, який перебуває на об'єкті;

правової обумовленості – забезпечення антитерористичної захищеності об'єктів повинно здійснюватися у відповідності з законодавчими та іншими нормативними актами, технічними стандартами, інструкціями й правилами;

превентивності – заходи щодо забезпечення антитерористичної захищеності об'єктів слід організовувати насамперед з метою запобігання загрозам, здійснювати такі заходи завчасно у поєднанні з нарощуванням їхнього обсягу та інтенсивності;

пріоритетності захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності – забезпечення антитерористичної захищеності об'єктів повинно здійснюватися з урахуванням необхідності, насамперед, захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності.

1.5. З метою зниження ризику реалізації терористичних загроз на об'єкті повинна бути створена система забезпечення антитерористичної захищеності.

1.6. Система забезпечення антитерористичної захищеності повинна забезпечувати реалізацію таких цілей:

1) в умовах повсякденного функціонування:

підтримку заданих умов комфортності життєдіяльності людей, що знаходяться на об'єкті;

виявлення і усунення причин та умов, що сприяють вчиненню терористичних актів;

завчасне виявлення терористичних загроз та терористичних посягань на об'єкті та передачу інформації суб'єктам боротьби з тероризмом для вжиття відповідних заходів;

здійснення підготовки, навчань і тренувань керівників та інших працівників об'єкта з питань реагування на терористичні загрози та посягань (як теоретичного, так і практичного), а також навчання населення, яке може потрапити в зону ураження (проведення підготовки, навчань і тренувань керівників об'єктів з питань реагування на терористичні загрози та посягань здійснюється закладами вищої освіти Служби безпеки України).

2) в умовах загрози вчинення або вчинення терористичного акту:

зниження ризику завдання шкоди життю та здоров'ю людей, обладнанню, а також самому об'єкту в цілому;

організацію оповіщення та евакуації людей з об'єкта та прилеглої місцевості;

мінімізацію та ліквідацію наслідків терористичного акту.

Для досягнення зазначених цілей система забезпечення антитерористичної захищеності повинна включати:

санкціонований (контрольований) прохід (проїзд) осіб (транспортних засобів) на територію об'єкта і в його режимні території і приміщення, у тому числі в періоди пікових навантажень;

запобігання несанкціонованому проникненню порушника в зони загального й обмеженого доступів (в окремі функціональні зони, поверхи, приміщення, до критично важливих точок тощо);

запобігання створенню передумов до вчинення актів кібертероризму за рахунок несанкціонованого отримання будь-якими особами, групами осіб та організаціями віддаленого чи безпосереднього доступу до комунікаційних та технологічних систем об'єкта з метою порушення конфіденційності, цілісності та доступності інформації, що в них обробляється (для об'єктів, які підлягають кіберзахисту відповідно до вимог Закону України "Про основні засади забезпечення кібербезпеки України");

запобігання витоку технічними каналами за межі території об'єкта інформації з обмеженим доступом;

запобігання спробам пронесення і провезення заборонених речовин і предметів, які можуть бути використані для вчинення терористичного акту;

виключення можливості використання порушниками надзвичайних подій для проникнення на об'єкт;

виявлення змін обстановки, які можуть бути пов'язані з підготовкою до протиправних дій на об'єкті та прилеглої до нього місцевості;

своєчасну передачу інформації до відповідальних осіб охорони об'єкта та до регіональних органів Служби безпеки України, Національної поліції України, Державної служби України з надзвичайних ситуацій, у разі необхідності – до інших суб'єктів боротьби з тероризмом;

своєчасне реагування на виникнення надзвичайних подій;

термінове оповіщення людей для їхньої безпечної та безперешкодної евакуації;

організацію об'єктивного контролю за діями обслуговуючого персоналу, у тому числі з числа можливих орендарів об'єкта;

відновлення штатного режиму функціонування (відбудови) об'єкта після терористичного акту.

Зазначені цілі повинні досягатися шляхом створення керівниками об'єктів протягом усього життєвого циклу об'єктів систем управління доступу та контролю дій виробничих та інших підрозділів, застосування превентивних дій, використання технічних систем, підсистем і засобів, реалізації на об'єктах заходів з криптографічного та технічного захисту інформації, кіберзахисту комунікаційних та технологічних систем, протидії технічним розвідкам (за наявності об'єктів протидії), передбачених законодавством України у сферах забезпечення кібербезпеки, захисту інформації, електронних довірчих послуг. Вимоги до системи контролю й управління доступом визначаються керівником відповідного об'єкта.

Система забезпечення антитерористичної захищеності функціонує у взаємодії із системою фізичного захисту об'єкта та враховує вимоги чинних законодавчих та нормативно-правових актів у сфері фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання.

1.7. Ці Правила застосовуються щодо усіх об'єктів нерухомості, віднесених у встановленому порядку до об'єктів можливих терористичних посягань.

1.8. Відповідальність за забезпечення антитерористичної захищеності об'єкта покладається на керівника юридичної особи, що є власником об'єкта або використовує його відповідно до законодавства, чи фізичну особу, що є власником об'єкта або використовує його на іншій законній підставі, якщо інше не передбачено законодавством.

1.9. Антитерористична захищеність об'єктів, які належать до сфери управління державних органів та органів місцевого самоврядування має забезпечуватись за рахунок коштів державного та місцевого бюджетів, передбачених для цих органів, а також інших джерел, не заборонених законодавством (власних коштів суб'єктів господарювання, коштів міжнародної технічної допомоги та інших).

Антитерористична захищеність об'єктів, які не належать до сфери управління державних органів та органів місцевого самоврядування забезпечується за рахунок власних коштів суб'єктів господарювання, коштів міжнародної технічної допомоги та інших джерел, не заборонених

законодавством.

2.0. З метою встановлення диференційованих вимог щодо забезпечення антитерористичної захищеності об'єктів проводиться їх ідентифікація відповідно встановленої цими Правилами методики.

II. Методика ідентифікації об'єктів можливих терористичних посягань

2.1. Ідентифікація полягає у віднесенні будь-якого об'єкта нерухомості до об'єкта можливих терористичних посягань та визначенні його категорії з урахуванням масштабів і видів імовірних втрат відповідно до прогнозованої загрози.

Критерієм віднесення до об'єкта можливого терористичного посягання є суб'єктивна оцінка державними органами, органами місцевого самоврядування або Антитерористичним центром при Службі безпеки України соціально-політичної реакції суспільства на небезпеку внаслідок сукупного впливу терористичних загроз на відповідний об'єкт.

Цей критерій характеризує ефективність терористичного впливу на суспільство, ступінь досягнення мети терористичного акту та надає можливість відрізнити терористичні загрози від інших.

2.2. Відповідальними за ідентифікацію об'єкта є керівник юридичної особи, яка є власником об'єкта або використовує його відповідно до законодавства, чи фізична особа, яка є власником об'єкта або використовує його на інших законних підставах, якщо інше не передбачено законодавством.

2.3. З метою проведення аналізу уразливості об'єкта при формуванні прогнозованої загрози керівництвом об'єкта можливих терористичних посягань із залученням спеціально утвореної для цієї мети комісії у складі працівників різних підрозділів (служб) та, за необхідності, із залученням представників інших підприємств, установ та організацій і відповідних місцевих органів виконавчої влади організується, процес виявлення уразливих місць, визначення загроз для об'єкта можливих терористичних посягань, ймовірних способів їхнього здійснення й моделей порушників.

2.4. Формування прогнозованої загрози та ідентифікація здійснюються:
на підставі письмового рішення відповідного державного органу або органу місцевого самоврядування - стосовно об'єктів, які належать до сфери управління державних органів та органів місцевого самоврядування;

на підставі розпорядження керівника Антитерористичного центру при Службі безпеки України - стосовно об'єктів, які не належать до сфери управління державних органів та органів місцевого самоврядування.

2.5. Формування прогнозованої загрози та проведення ідентифікації об'єкта здійснюється комісією, що утворюється наказом керівника (органу управління) об'єкта.

До складу комісії входять:

керівник об'єкта або його заступник (голова комісії);

представник Антитерористичного центру при Службі безпеки України, а у разі потреби представники інших суб'єктів боротьби з тероризмом у межах своєї компетенції та інших державних органів, що здійснюють охорону об'єктів;

фахівець з організації заходів охорони, працівники об'єкта, що відповідають за пожежну безпеку, цивільний захист, охорону та інженерно-технічне оснащення, секретне діловодство, криптографічний та технічний захист інформації, кіберзахист, протидію технічним розвідкам (за наявності об'єктів протидії);

технічний, криптографічний і кіберзахист інформації;

представники органів державної влади та/або органів місцевого самоврядування.

У зазначеному наказі встановлюються строки (не більше трьох місяців) для формування прогнозованої загрози та проведення ідентифікації об'єкта.

2.6. Ідентифікація об'єкта проводиться з урахуванням масштабів і видів можливих втрат згідно з таблицею 1.

Таблиця 1

Показник масштабу втрат, П _і	Коефіцієнт значущості втрат, К _і			
	людські втрати	економічні втрати	втрати безпеки життєдіяльності	суспільно-політичні втрати
	К ₁	К ₂	К ₃	К ₄
Об'єктовий – 1	1	1	1	4
Місцевий – 1	2	2	2	
Регіональний – 1	3	3	3	
Державний – 1	4	4	4	

Масштаб втрат визначається залежно від територіального критерію та відповідно до кількісних показників, які поділяються на такі види:

А) державний – обов'язкова наявність паспорта антитерористичної захищеності об'єкта можливих терористичних посягань, здійснення державної охорони, здійснення відомчої або приватної охорони, контррозвідувальне забезпечення об'єкта можливих терористичних посягань, оперативне забезпечення об'єкта можливих терористичних посягань, визначення в превентивних планах організації антитерористичної захищеності об'єкта можливих терористичних посягань можливості залучення сил реагування з інших областей та з інших районів в межах певної області;

В) регіональний – обов'язкова наявність паспорта антитерористичної захищеності об'єкта можливих терористичних посягань, здійснення відомчої або приватної охорони, оперативне забезпечення об'єкта можливих

терористичних посягань, визначення в превентивних планах організації антитерористичної захищеності об'єкта можливих терористичних посягань можливості залучення сил реагування з інших областей та інших районів в межах певної області;

С) місцевий – визначення в превентивних планах організації антитерористичної захищеності об'єкта можливих терористичних посягань можливості залучення сил реагування з інших областей та з інших районів в межах певної області ;

Д) об'єктовий - визначення в превентивних планах організації антитерористичної захищеності об'єкта можливих терористичних посягань можливості залучення сил реагування з інших районів в межах певної області.

Прогнозована оцінка втрат (за масштабами та їх видами) порівнюється з межовими значеннями, наведеними у кількісних показниках масштабів втрат згідно з додатками 2-4. Остаточне рішення приймається за максимальним значенням отриманих параметрів.

Оцінка коефіцієнта значущості суспільно-політичних втрат здійснюється комісією та проводиться за наявності державного масштабу втрат.

Загальний рівень потенційних втрат (S) від можливих терористичних посягань визначається як сума всіх коефіцієнтів значущості втрат (K_i) відповідно до кількісних показників масштабу втрат (П_j) за такою формулою:

$$S = K_1\Pi_j + K_2\Pi_j + K_3\Pi_j + K_4\Pi_j$$

Категорія об'єкта під час його ідентифікації визначається відповідно до значення загального рівня потенційних втрат (S) згідно з таблицею 2.

Таблиця 2

Категорія об'єкта	Значення показника S
Перша (А)	4–6
Друга (В)	7–9
Третя (С)	10–13
Четверта (D)	14–16

У разі коли значення показника S не перевищує 4, об'єкт нерухомості не відноситься до об'єкта можливих терористичних посягань.

Ідентифікація об'єкта з урахуванням прогнозованих людських, економічних втрат і зниження рівня безпеки життєдіяльності визначається відповідно до кількісних показників масштабів втрат згідно з додатками 2-4.

2.7. Прогнозована загроза формується у порядку, встановленому з урахуванням вимог законодавчих та інших нормативних актів на підставі аналізу характеристик об'єкта, проектної документації, технологічних регламентів та інших документів, пов'язаних з експлуатацією об'єкта.

Під час формування прогнозованої загрози враховуються такі прогнозні показники:

- вид та кількість небезпечних речовин, які перебувають на об'єкті;
- рівень зношеності основних промислово-виробничих фондів;

зона можливого ураження;

кількість працівників на об'єкті, а також населення, яке проживає в зоні можливого ураження;

значення об'єкта для життєзабезпечення, самоідентифікації, задоволення культурних та духовних потреб населення;

час та ресурси, необхідні для відновлення роботи об'єкта та усунення наслідків терористичних посягань;

рівень ефективності системи забезпечення антитерористичної захищеності об'єкта (за результатами аналізу уразливості об'єкта).

Під час формування прогнозованої загрози використовується модель терористичних посягань, спрямованих в найбільш уразливе місце об'єкта, що призводить до максимально можливих втрат, в найбільш незручний час з точки зору функціонування (виробничого циклу) об'єкта та стану його системи забезпечення антитерористичної захищеності, та результати розрахунку потенційних людських, економічних, суспільно-політичних втрат, втрат безпеки життєдіяльності (екологічної шкоди) внаслідок терористичних посягань щодо відповідного об'єкта.

2.8. За результатами здійснення заходів з ідентифікації об'єкта та формування прогнозованої загрози комісією готується висновок за формою, визначеною керівником Антитерористичного центру при Службі безпеки України.

У висновку зазначається категорія об'єкта за результатами його ідентифікації та інші необхідні відомості щодо прогнозованої загрози.

Висновок підписується членами комісії та передається на затвердження до державного органу або органу місцевого самоврядування, до сфери управління якого належить об'єкт, або до відповідної координаційної групи Антитерористичного центру при регіональному органі Служби безпеки України, якщо об'єкт не належить до сфери управління державних органів, органів місцевого самоврядування.

Комісія провадить свою діяльність, зокрема готує висновок, з дотриманням вимог законодавства у сфері захисту інформації з обмеженим доступом.

Антитерористичний центр при Службі безпеки України надає методичну допомогу, рекомендації та роз'яснення комісіям з питань ідентифікації об'єкта і формування прогнозованої загрози.

2.9. Затверджений державним органом або органом місцевого самоврядування висновок надсилається ним до відповідної координаційної групи Антитерористичного центру при регіональному органі Служби безпеки України або до Штабу Антитерористичного центру при Службі безпеки України (на його вимогу) для перевірки допустимості та обґрунтованості віднесення об'єкта нерухомості до об'єкта можливих терористичних посягань та формування регіонального переліку об'єктів можливих терористичних посягань.

До такої перевірки можуть залучатися відповідні фахівці Служби безпеки України у сфері забезпечення державної безпеки.

2.10. Координаційні групи Антитерористичного центру при регіональному органі Служби безпеки України подають регіональні переліки до Штабу Антитерористичного центру при Службі безпеки України, який на основі аналізу поданих матеріалів за наявності підстав вносить відповідні корективи, формує загальнодержавний перелік об'єктів можливих терористичних посягань, що затверджується керівником Антитерористичного центру при Службі безпеки України.

2.11. Антитерористичний центр при Службі безпеки України інформує державні органи, органи місцевого самоврядування, а також громадськість, зокрема шляхом розміщення відповідної інформації на веб-сайті Служби безпеки України, про включення об'єктів, які належать до сфери їх управління, до загальнодержавного переліку об'єктів можливих терористичних посягань із зазначенням категорії об'єкта за результатами його ідентифікації.

Включення об'єкта до загальнодержавного переліку об'єктів можливих терористичних посягань є обов'язковою підставою для подальшої організації антитерористичного захисту об'єкта.

2.12. Державні органи, органи місцевого самоврядування, до сфери управління яких належать об'єкти, включені до загальнодержавного переліку об'єктів можливих терористичних посягань, відповідно до своєї компетенції відстежують обставини, що можуть вплинути на прогнозовану загрозу та ідентифікацію об'єкта, та у разі їх виникнення невідкладно інформують Антитерористичний центр при Службі безпеки України.

Антитерористичний центр при Службі безпеки України аналізує та оцінює надану інформацію, за потреби одержує від державних органів, органів місцевого самоврядування додаткову інформацію з питань антитерористичного захисту об'єкта.

Обставини, що можуть вплинути на прогнозовану загрозу та ідентифікацію об'єктів, які не належать до сфери управління державних органів, органів місцевого самоврядування та включені до загальнодержавного переліку об'єктів можливих терористичних посягань, відстежуються Антитерористичним центром при Службі безпеки України.

За результатами аналізу та оцінки інформації з питань антитерористичного захисту об'єкта Антитерористичний центр при Службі безпеки України ініціює внесення відповідних змін до висновку визначеної прогнозованої загрози та ідентифікації об'єкта відповідно до порядку, встановленого цими Правилами.

III. Організаційні та технічні умови системи забезпечення антитерористичної захищеності об'єктів можливих терористичних посягань

3.1. Безпосередньо на об'єкті система забезпечення антитерористичної захищеності спрямована на:

1) запобігання неправомірному проникненню на об'єкт, включаючи його територію;

2) виявлення потенційних порушників пропускнуго і внутрішньо об'єктового режимів, ознак підготовки або вчинення терористичного акту;

3) оперативного припинення спроб підготовки або вчинення терористичного акту на об'єкті або прилеглій місцевості;

4) мінімізацію та ліквідацію наслідків терористичного акту на об'єкті або прилеглій місцевості;

5) забезпечення захисту інформації з обмеженим доступом, у тому числі тієї, що міститься в паспорті антитерористичної захищеності найбільш уразливого об'єкта можливих терористичних посягань.

6) забезпечення сталого функціонування комунікаційних та технологічних систем об'єкта, цілісності і доступності інформації, що в них обробляється, та їх кіберзахист.

3.2. З метою забезпечення антитерористичної захищеності об'єкта органами, підприємствами, установами, організаціями можуть вживатися наступні заходи:

1) організація пропускнуго і внутрішньо об'єктового режимів об'єкта, контроль за їх функціонуванням, організація санкціонованого допуску осіб і транспортних засобів на об'єкт;

2) визначення кола службових осіб, відповідальних за проведення заходів із забезпечення антитерористичного захисту об'єкта;

3) розробка і реалізація плану заходів, спрямованих на виявлення, і усунення причин та умов, що сприяють неправомірному проникненню сторонніх осіб на об'єкт;

4) чітка організація виробничого процесу, що зменшує кількість випадків перебування працівників в режимних приміщеннях та на режимних територіях об'єкта без нагальної потреби;

5) забезпечення охорони об'єкта шляхом залучення співробітників спеціалізованих охоронних служб (поліції охорони Національної поліції України, Національної гвардії України, недержавних охоронних структур), оснащення об'єкта необхідними інженерно-технічними засобами і системами охорони;

6) постійного контролю за відповідністю експлуатації об'єкта вимогам пожежної безпеки, державним технічним стандартам, будівельним та санітарним нормам або іншим нормативним вимогам;

7) організація забезпечення криптографічного та технічного захисту інформації, кіберзахисту комунікаційних і технологічних систем, протидію технічним розвідкам на об'єкті (за наявності об'єктів протидії), а також реалізація заходів, що виключають несанкціонований доступ до інформаційних ресурсів об'єкта;

8) забезпечення захисту інформації з обмеженим доступом, що міститься в паспорті антитерористичної захищеності найбільш уразливого об'єкта можливих терористичних посягань, інших документах та матеріальних носіях, у тому числі інформації про заходи, що вживаються для антитерористичного захисту об'єкта;

9) попередження фактів порушення пропускнуго і внутрішньо об'єктового режимів, спроб проносу і провезення заборонених предметів (радіоактивних, вибухових, отруйних речовин, зброї, боєприпасів, наркотичних засобів і інших небезпечних предметів і речовин, тощо) на об'єкт;

10) розробка алгоритму перевірки спільно з підрозділами Національної поліції України, Національної гвардії України, Служби безпеки України підозрілих транспортних засобів і осіб, що перебувають у безпосередній близькості до об'єкта;

11) підтримка в справному стані інженерно-технічних засобів і систем охорони, оснащення об'єкта безперебійним зв'язком;

12) контроль за станом підземних комунікацій, стоянок автотранспорту, складських приміщень;

13) своєчасне виявлення і негайне доведення інформації про загрозу здійснення терористичного акту або про його здійснення до суб'єктів боротьби з тероризмом;

14) розробка планів евакуації працівників об'єкта, а також відвідувачів у разі отримання інформації про загрозу вчинення або вчинення терористичного акту;

15) з урахуванням спеціалізації об'єкта організація постійного навчання працівників щодо дій у нестандартних ситуаціях при загрозі здійснення терористичного акту або при його здійсненні;

16) проведення тренувань стосовно евакуації працівників і відвідувачів об'єкта;

17) організація діяльності з пошуку та фіксації фактичних даних про терористичні загрози з боку окремих осіб та груп, у тому числі працівників об'єкта.

IV. Заходи системи забезпечення антитерористичної захищеності об'єктів можливих терористичних посягань

4.1. Для об'єктів встановлюється комплекс основних і додаткових заходів системи забезпечення антитерористичної захищеності у відповідності до прогнозованої загрози та рівня терористичної загрози, встановленого керівником Антитерористичного центру при Службі безпеки України.

4.2. До комплексу основних заходів системи забезпечення антитерористичної захищеності об'єкта належать:

зонування прилеглої території та приміщень об'єкта;

розроблення раціональної структури і штатного розпису експлуатуючої організації, у тому числі, за необхідності, охоронних служб об'єкта;

розробка порядку огляду і санкціонованого допуску на об'єкт людей, транспортних засобів та вантажів;

затвердження правил експлуатації об'єкта відповідно до нормативних вимог (правил пожежної безпеки, санітарних норм, технічних вимог, державних будівельних норм, актів про охорону праці, стандартів з ядерної та радіаційної безпеки, стандартів і нормативних документів, що регулюють питання у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (за наявності об'єктів протидії));

визначення порядку взаємодії власників об'єктів і керівників органів, підприємств, установ та організацій незалежно від форм власності з іншими працівниками об'єктів, а також з представниками правоохоронних органів та сторонніх організацій.

4.3. Система забезпечення антитерористичної захищеності об'єкта складається із:

належного інженерно-технічного оснащення об'єкта в поєднанні з наявними системами безпеки та охорони в інших органах, підприємствах, установах, організаціях, що розташовані на прилеглих до об'єкта територіях;

забезпечення органами, підприємствами, установами, організаціями належного регулювання порядку дій у разі виникнення загрози або вчинення терористичного акту на об'єкті;

підготовленого персоналу служби експлуатації об'єкта;

комплексу охоронних, організаційних і технічних заходів, спрямованих на забезпечення антитерористичної безпеки.

Інженерно-технічне оснащення об'єкта та його охоронна система повинні виконувати такі завдання:

а) система криптографічного та технічного захисту інформації, кіберзахисту комунікаційних і технологічних систем на об'єкті:

забезпечення на об'єкті конфіденційності, цілісності і доступності інформації, які можуть бути порушені шляхом утворення технічних каналів витоку або впливу на інформацію, - насамперед, критично важливих електронних інформаційних ресурсів, що обробляються у комунікаційних та технологічних системах об'єкта.

б) система охоронного відеоспостереження:

контроль території об'єкта та прилеглої до нього території, виділених зон всередині об'єкта, а також під'їзних шляхів;

контрольований доступ людей на територію об'єкта й у виділені приміщення;

контроль переміщення людей всередині об'єкта;

розмежування доступу у виділені зони і приміщення всередині об'єкта;

контроль стану (відкриті/закриті) дверей виділених приміщень;

контроль переміщення по об'єкту, а також виносу з об'єкта обладнання, що пройшло спецперевірку й оснащене чипами з електронною міткою;

управління пристроями загородження й оповіщення, виконавчими пристроями інженерних систем захисту;

взаємодія з іншими системами на апаратному та програмному рівнях;

в) система охоронно-тривожної сигналізації:

контроль за несанкціонованим доступом на територію об'єкта, у виділені приміщення тощо;

оповіщення про проникнення в охоронювані зони;

централізована або децентралізована постановка приміщень під охорону;

сполучення на апаратному рівні системи контролю й управління доступом з системою охоронного відеоспостереження;

г) система контролю повітряно-газового середовища в системах вентиляції та кондиціонування:

виявлення отруйних та інших небезпечних речовин, горючих та токсичних газів, перелік яких повинен уточнюватися при проектуванні;

г) система автономного електроживлення:

забезпечення об'єкта джерелами автономного енергозабезпечення критично важливих електронних інформаційних ресурсів, не пов'язаними з лініями основного та резервного електропостачання.

Особи, відповідальні за забезпечення антитерористичної захищеності об'єкта, забезпечують підготовку та затвердження інструкцій з питань реагування на загрозу вчинення або вчинення терористичного акта на об'єкті.

Такі інструкції повинні визначати:

взаємодію об'єкта або його служби охорони з суб'єктами боротьби з тероризмом, органами місцевого самоврядування;

взаємодію об'єкта або його служби охорони з оперативними службами державних органів та органів місцевого самоврядування, що прибули на об'єкт за фактом події з ознаками терористичного акту;

взаємодію внутрішніх служб об'єкта між собою;

порядок дій працівників служби охорони об'єкта в умовах реалізації тієї чи іншої загрози;

порядок відновлення штатного режиму роботи об'єкта, усунення причин та умов, що сприяли терористичному акту або виникненню надзвичайної події, ліквідації їх наслідків;

порядок організації і здійснення криптографічного та технічного захисту інформації на об'єкті;

права, обов'язки посадових осіб і заходи забезпечення кіберзахисту об'єкта, який підлягає такому захисту відповідно до законодавства;

порядок дій працівників та особливості функціонування об'єкта у разі:

встановлення керівником Антитерористичного центру при Службі безпеки України відповідних рівнів терористичної загрози;

отримання керівником або іншими працівниками об'єкта погроз терористичного характеру по телефону, у вигляді анонімних листів або через інші засоби комунікації;

виявлення підозрілих предметів з ознаками вибухового чи іншого небезпечного пристрою, а також тих, що вимагають перевірки з метою встановлення їхньої реальної вибухової, радіаційної, хімічної і біологічної безпеки;

вчинення терористичного акту на об'єкті або прилеглий території шляхом вибуху чи інших дій, що спричинили людські жертви, знищення і пошкодження матеріальних цінностей, паніку, серйозні збитки, тривале відключення електроенергії, опалення, газу тощо;

вчинення терористичного акту шляхом захоплення й утримання заручників на об'єкті;

несанкціонованого паркування транспортного засобу в безпосередній близькості до об'єкта;

несанкціонованого проїзду чи прориву транспортного засобу на територію об'єкта;

надходження адресату, що знаходиться на об'єкті, поштового відправлення з ймовірним вкладенням вибухового чи іншого небезпечного пристрою або речовини;

пошкодження або спроби пошкодження технічних систем життєзабезпечення об'єкта шляхом вибуху, підпалу або іншим способом;

вчинення кібератаки на комунікаційну або технологічну систему об'єкта, вчинення несанкціонованих дій, виникнення кіберінцидентів, що можуть призвести до порушення конфіденційності, цілісності чи доступності інформації за рахунок утворення технічних каналів витоку (впливу), якщо зазначені кібератаки, кіберінциденти або несанкціоновані дії можуть спричинити чи спричинили людські, економічні, суспільно-політичні втрати або екологічну шкоду;

виникнення інших небезпечних ситуацій, пов'язаних з протиправними діями та аварійними подіями в системах життєзабезпечення об'єкта.

4.4. Державний контроль за станом криптографічного і технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам (за наявності об'єктів протидії), дотриманням вимог законодавства у сфері електронних довірчих послуг, станом захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури на об'єктах можливих терористичних посягань здійснюється у встановленому законодавством порядку.

4.5. Комплекс додаткових заходів системи забезпечення антитерористичної захищеності на конкретних об'єктах можуть також

визначатись центральними органами виконавчої влади, що забезпечують формування та реалізують державну політику у відповідних сферах.

V. Особливості організації заходів з інформування про терористичну загрозу на об'єктах можливих терористичних посягань

5.1. При виявленні загрози вчинення терористичного акту на об'єкті (місцевості), отриманні інформації про загрозу вчинення терористичного акту на об'єкті (місцевості) або при вчиненні терористичного акту на об'єкті (місцевості) службова особа, яка здійснює безпосереднє керівництво діяльністю працівників об'єкта, або уповноважена ним особа негайно інформує про це підрозділи суб'єктів боротьби з тероризмом, до компетенції яких віднесено запобігання, виявлення, припинення, мінімізацію відповідних наслідків терористичної діяльності.

5.2. У разі передачі інформації про загрозу вчинення або вчинення терористичного акту на об'єкті (місцевості) із застосуванням технічних засобів телекомунікацій або кінцевого обладнання уповноважена службова особа об'єкта повинна надати відповідним підрозділам суб'єктів боротьби з тероризмом таку інформацію:

своє прізвище, ім'я, по батькові і займану посаду;

найменування об'єкта, його юридичну та фактичну адреси;

дату і час отримання інформації про загрозу вчинення або вчинення терористичного акту;

повну інформацію про відомі обставини загрози вчинення або вчинення терористичного акту;

орієнтовану кількість осіб, що знаходиться на об'єкті (місцевості);

інші значимі відомості за запитом суб'єктів боротьби з тероризмом.

5.3. Особа, яка передала інформацію про загрозу вчинення або вчинення терористичного акту, робить письмову відмітку про прізвище, ім'я, по батькові, займану посаду співробітника підрозділу суб'єкта боротьби з тероризмом, що отримав інформацію та фіксує дату і час контакту.

При передачі такої інформації з використанням комп'ютерної мережі особа, що передає інформацію, зберігає відповідний електронний лист у папці вихідної кореспонденції.

5.4. При виявленні загрози вчинення терористичного акту на об'єкті або отриманні інформації про загрозу вчинення або вчинення терористичного акту посадова особа, що відповідає на цей час за функціонування об'єкта або безпосередньо керує підрозділом охорони, повинна забезпечити:

посилення охорони, а також пропускнуго і внутрішньо об'єктового режимів;

вжиття заходів своєчасного і оперативного реагування на загрозу вчинення терористичного акту, його попередження;

терміновий збір керівництва та працівників режимних, охоронних, аварійно-рятувальних служб (за наявності);

оповіщення осіб, що знаходяться на об'єкті (місцевості) про загрозу вчинення терористичного акту;

у встановленому порядку евакуацію людей та обладнання;

організацію доступу на об'єкт співробітників суб'єктів боротьби з тероризмом;

у разі вчинення акту кібертероризму, спроби його вчинення у формі кібератаки або інших несанкціонованих дій, виникнення кіберінциденту - невідкладне інформування Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України у порядку, встановленому законодавством.

5.5. На об'єктах має бути розроблена, затверджена та доведена до відома всіх працівників Інструкція щодо реагування працівниками об'єкта на отриману інформацію про загрозу вчинення або вчинення терористичного акту.

VI. Паспорт антитерористичної захищеності об'єкта можливих терористичних посягань

6.1. На кожний об'єкт можливих терористичних посягань протягом 3 місяців після проведення його ідентифікації складається паспорт антитерористичної захищеності найбільш уразливого об'єкта можливих терористичних посягань (далі – паспорт).

На інші об'єкти паспорт може складатися у разі підвищеного ризику вчинення терористичного акту на об'єкті за рішенням координаційної групи Антитерористичного центру при регіональному органі Служби безпеки України.

Відповідальними за розробку паспорта є службові особи, що визначаються керівником юридичної особи, яка є власником об'єкта або використовує його відповідно до законодавства, як правило з числа працівників адміністрації об'єкта, або фізична особа, яка є власником об'єкта або використовує його на інших законних підставах.

Особи, відповідальні за розробку паспорта, несуть персональну відповідальність за повноту та достовірність внесених до нього відомостей, зокрема тих, що передбачені пунктом 6.3. цих Правил.

Невід'ємною частиною паспорта є акти ідентифікації об'єкта, що оформлюються за результатами роботи комісії, утвореної відповідно до Розділу II цих Правил.

6.2. Паспорт розробляється для вирішення наступних завдань:

зниження ризику заподіяння шкоди життю або здоров'ю громадян, майну фізичних або юридичних осіб, державного або комунального майна, що знаходиться на об'єкті або в безпосередній близькості від нього;

визначення показників загального рівня потенційних втрат об'єкта та

можливості виникнення надзвичайних подій, пов'язаних з терористичними проявами;

поточного контролю за антитерористичною захищеністю об'єкта, зниження ризику і зменшення наслідків можливих терористичних актів;

оцінки результату здійснюваних заходів із запобігання, реагування і припинення терористичних актів, мінімізації та ліквідації їх наслідків.

6.3. Паспорт повинен містити наступні розділи:

загальні відомості про об'єкт;

характеристика об'єкта;

відомості про персонал;

відомості про сили й засоби, залучені для охорони об'єкта;

забезпечення пожежної безпеки;

прогнозовані моделі терористичних посягань відносно об'єкта;

заходи, які виконуються або плануються щодо зміцнення антитерористичного захисту та зниження уразливості об'єкта;

відомості щодо інформації і ресурсів, уразливих по технічних каналах витоку (впливу) (заповнюється тільки для об'єктів, які підлягають кіберзахисту відповідно до вимог Закону України "Про основні засади забезпечення кібербезпеки України"), а також дані про виконання на такому об'єкті Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518;

ситуаційні плани дій при виникненні надзвичайних ситуацій на об'єкті;

забезпечення режиму секретності (заповнюється тільки у разі провадження діяльності, пов'язаної з державною таємницею).

Заповнення паспорта здійснюється відповідно додатку 1.

6.4. Паспорт є документом, що містить інформацію з обмеженим доступом та має відмітку "Конфіденційно" або гриф "Для службового користування" чи гриф секретності "Таємно" (згідно відповідної статті Зводу відомостей, що становлять державну таємницю) якщо немає підстав для присвоєння йому відповідного грифу секретності.

Копіювання паспорта та передача його особам, органам, підприємствам, установам, організаціям, що не мають повноважень, пов'язаних із забезпеченням антитерористичного захисту відповідних об'єктів забороняється.

6.5. Паспорт складається в трьох примірниках, погоджується з координаційною групою Антитерористичного центру при регіональному органі Служби безпеки України та затверджується її керівником.

6.6. Погодження та затвердження паспорта забезпечується координаційною групою Антитерористичного центру при регіональному органі Служби безпеки України в строки, що не перевищують 30 діб з дня його надання до координаційної групи.

Відмова в погодженні та затвердженні паспорта повинна бути

вмотивована і складена у письмовій формі.

6.7. Після затвердження паспорта перший примірник зберігається у відповідальній особи органу, підприємства, установи, організації, а другий – в режимно-секретному відділі регіонального органу Служби безпеки України.

Погоджений та затверджений паспорт в електронному вигляді також передається координаційною групою до Штабу Антитерористичного центру при Службі безпеки України.

6.8. Новий паспорт розробляється в таких випадках:

а) зміни або встановлення нормативно-правовими актами додаткових вимог щодо забезпечення антитерористичної захищеності населення та об'єктів;

б) зміни загальних відомостей про об'єкт, що зазначені в пункті 6.3. цих Правил;

в) суттєвої забудови території об'єкта чи завершення робіт по капітальній реконструкції об'єкта;

г) зміни схеми охорони об'єкта, його додаткового оснащення чи забезпечення новими технічними засобами.

6.9. Паспорт підлягає актуалізації не рідше 1 разу на рік.

Актуалізація паспорта полягає у визначенні наявності обставин, передбачених пунктом 6.8. цих Правил.

У разі, якщо при актуалізації паспорта відсутні зміни у порівнянні з існуючим паспортом, керівник органу, підприємства, установи або організації письмово повідомляє про це керівника координаційної групи Антитерористичного центру при регіональному органі Служби безпеки України.

У разі наявності змін здійснюється розробка нового паспорта.

Відповідальність за актуалізацію паспорта несе керівник юридичної особи, що є власником об'єкта або використовує його відповідно до законодавства, чи фізична особа, що є власником об'єкта або використовує його на іншій законній підставі.

6.10. Паспорт об'єктів, щодо яких здійснюється державна охорона, розробляється адміністраціями цих об'єктів у взаємодії з Управлінням державної охорони України у трьох примірниках, погоджується у строк, що не перевищує 30 діб з дня його подачі та затверджується керівником координаційної групи Антитерористичного центру при регіональному органі Служби безпеки України. Після затвердження паспорта перший примірник зберігається на об'єкті, щодо якого здійснюється державна охорона, другий – в Управлінні державної охорони України, третій – в режимно-секретному підрозділі регіонального органу Служби безпеки України.

Погоджений та затверджений паспорт в електронному вигляді також передається координаційною групою до Штабу Антитерористичного центру при Службі безпеки України.

VII. Контроль за ефективністю заходів із антитерористичної захищеності об'єктів можливих терористичних посягань

7.1. Контроль за ефективністю заходів із забезпечення антитерористичної захищеності об'єктів здійснюється шляхом проведення координаційними групами Антитерористичного центру при регіональних органах Служби безпеки України тактико-спеціальних навчань та тренувань.

Керівники органів, підприємств, установ і організацій, незалежно від форм власності, зобов'язані всебічно сприяти координаційним групам Антитерористичного центру при регіональних органах Служби безпеки України в організації та проведенні таких навчань і тренувань.

У разі виявлення недоліків в антитерористичній захищеності об'єкта координаційними групами Антитерористичного центру при регіональних органах Служби безпеки України готується інформування на адресу керівництва об'єкта (або його власника чи органу управління) та Штабу Антитерористичного центру при Службі безпеки України із зазначенням конкретних причин та умов, що негативно впливають на їх терористичну захищеність та пропозицій щодо їх усунення.

Про усунення недоліків та вжиті заходи керівництво об'єкта письмово повідомляє координаційну групу Антитерористичного центру при регіональних органах Служби безпеки України у місячний термін.

7.2. За навмисне невиконання або порушення цих Правил в частині відповідних правил безпеки (протипожежних норм, санітарно-епідемічних норм, умов праці) посадові особи об'єкта притягуються до відповідальності згідно із законодавством.

Голова Служби безпеки України

Іван БАКАНОВ

“ ____ ” _____ 2022 року

Гриф секретності

ЗАТВЕРДЖУЮ

(посада, ім'я та прізвище)

підпис керівника

__._20__ р.

ПАСПОРТ
антитерористичної захищеності об'єкта
можливого терористичного посягання

(найменування об'єкта)

Анотація

1. Відомості про розробників паспорта.
2. Джерела інформації для розробки паспорта.
3. Дата розробки паспорта або оновлення включених в нього відомостей.

Розділ 1. Загальні відомості про об'єкт

- 1.1. Профіль діяльності об'єкта.
- 1.2. Повне і скорочене найменування об'єкта:
 - 1.2.1. Наявність і номер дозволу (ліцензії) на право ведення спеціалізованої діяльності й виду послуг, що надаються;
 - 1.2.2. Зразок підпису керівника, відбитку печатки.
- 1.3. Поштова адреса, телефон, факс, електронна адреса тощо.
- 1.4. Відомча приналежність, організаційно-правова форма:
 - 1.4.1. Повне найменування;
 - 1.4.2. Поштова адреса, телефон, факс, електронна адреса тощо.
- 1.5. Форма власності (державна, приватна та ін.); для акціонерних товариств - частка органів державної влади в статутному фонді об'єкта.
- 1.6. Посадові особи об'єкта із зазначенням прізвища, імені, по батькові, номерів робочих, домашніх і мобільних телефонів:
 - 1.6.1. Керівник об'єкта (директор, генеральний директор, начальник);
 - 1.6.2. Заступник керівника об'єкта по безпеці;
 - 1.6.3. Інші керівники об'єкта;
 - 1.6.4. Відповідальний за цивільну оборону на об'єкті;
 - 1.6.5. Відповідальний за охорону і пропускний режим об'єкта;
 - 1.6.6. Відповідальний за криптографічний та технічний захист інформації, протидію технічним розвідкам на об'єкті (за наявності об'єктів протидії);
 - 1.6.7. Відповідальний за кіберзахист об'єкта;
 - 1.6.8. Відповідальний за протипожежну безпеку об'єкта;
 - 1.6.9. Посадові особи і працівники об'єкта, відповідальні за проведення

заходів щодо попередження надзвичайних ситуацій, у т.ч. викликаних терористичними актами, ліквідації їх наслідків, інших протиправних діянь, аварійних і надзвичайних ситуацій, надання необхідної допомоги потерпілим у процесі надзвичайної ситуації.

1.7. Розміщення об'єкта відносно транспортних комунікацій:

1.7.1. Найменування найближчої залізничної станції та відстань до неї (км);

1.7.2. Найменування найближчого аеропорту, вертолітної площадки та відстань до них (км);

1.7.3. Найменування найближчого морського порту (пристані) і відстань до нього (км).

Розділ 2. Характеристика об'єкта

2.1. Відвідуваність (чисельність персоналу та відвідувачів) за добу.

2.2. Кількість приміщень (одиниць, загальна площа).

2.3. Параметри та особливості охоронюваної території, будинку, об'єкта:

2.3.1. Площа території, займаної об'єктом, з будівлями та подвір'ям (кв. м);

2.3.2. Периметр всієї території у (кв. м);

2.3.3. Характеристика та особливості будинку (будинків об'єкта).

2.4. Інженерні спорудження:

2.4.1. Огородження по периметру території об'єкта (в т.ч. із якого матеріалу вироблено);

2.4.2. Оснащення огороження по всій довжині додатковими захисними засобами;

2.4.3. Наявність на території та у прилеглому оточенні об'єкта автостоянок:

місце розташування;

площа стоянки;

кількість місць для паркування;

наявність системи пропуску та охорони;

маршрути руху;

місця вантажно-розвантажувальних робіт;

прилеглі транспортні магістралі;

2.4.4. Пропускний режим для персоналу та відвідувачів на територію об'єкта.

2.5. Розміщення об'єкта відносно об'єктів інфраструктури:

з чим граничить територія об'єкта;

2.6. Системи і засоби технічного і криптографічного захисту інформації з посиланням на документи, що засвідчують їх відповідність, і місце (підрозділ) зберігання організаційно-технічної документації (для об'єктів кіберзахисту).

2.7. Системи і засоби кіберзахисту з посиланням на документи, що засвідчують їх відповідність і місце (підрозділ) зберігання організаційно-технічної документації (для об'єктів кіберзахисту).

2.8. Інженерні системи об'єкта:

- 2.8.1. Основне та резервне електропостачання об'єкта, наявність автономного електроживлення;
 - 2.8.2. Газопостачання об'єкта;
 - 2.8.3. Водопостачання об'єкта;
 - 2.8.4. Теплопостачання (опалення) об'єкта (центральне, автономне);
 - 2.8.5. Системи вентиляції, кондиціонування повітря об'єкта, пульт керування і засувки;
 - 2.8.6. Місце зберігання проектної та експлуатаційної документації на зазначені системи, відповідальна посадова особа (особи) і номери телефонів;
 - 2.8.7. Місце зберігання сигнальної стрічки (для обмеження небезпечної зони), попереджувальні та обмежувальні знаки і таблички.
- 2.9. Системи і засоби протидії технічним розвідкам (за наявності об'єктів протидії) з посиланням на документи, що засвідчують їх відповідність, і місце (підрозділ) зберігання організаційно-технічної документації (для об'єктів протидії).

Розділ 3. Відомості про персонал

- 3.1. Чисельність персоналу.
- 3.2. Чисельність персоналу за межами об'єкта.
- 3.3. Кількість підрозділів та їх структура.
- 3.4. Телефонні номери керівників об'єкта.

Розділ 4. Відомості про сили та засоби, залучені для охорони об'єкта

- 4.1. Огородження по периметру території об'єкта (матеріал огороження).
- 4.2. Устаткування огороження по всій довжині додатковими захисними засобами.
- 4.3. Сили фізичної охорони об'єкта:
 - 4.3.1. Вид і чисельність охорони об'єкта;
- 4.4. Порядок взаємодії (за допомогою радіо- та телефонного зв'язку).
- 4.5. Режим охорони об'єкта підрозділом охорони.
- 4.6. Заходи щодо посилення охорони.
- 4.7. Технічні засоби охорони об'єкта.
 - 4.7.1. Наявність на території об'єкта технічних засобів: виявлення та сигналізації; оповіщення; стаціонарних, ручних металодетекторів, інтроскопів; засобів локалізації вибуху, примусової зупинки автотранспорту, інших засобів контролю доступу, охорони та захисту з відміткою найменування обладнання, їхньої кількості, виробника, року виготовлення, строку експлуатації;
 - 4.7.2. Обладнання постів (приміщень) кнопками екстреного виклику поліції, підрозділів охорони (тривожної сигналізації);
 - 4.7.3. Обладнання корпусів (приміщень) об'єкта охоронно-пожежною

сигналізацією.

4.8. Засоби озброєння, спеціальні та інші засоби співробітників фізичної охорони об'єкта:

4.8.1. Службова табельна вогнепальна та холодна зброя;

4.8.2. Захисні засоби (бронежилет, шолом та інше);

4.8.3. Спеціальні засоби (кийок гумовий, газовий пістолет, аерозольний балончик зі сльозоточивим (перцевим) газом, інше);

4.8.4. Службові собаки на об'єкті.

4.9. Організація зв'язку:

4.9.1. Засоби зв'язку між постами та центральним пунктом, включаючи резервні канали радіозв'язку (при наявності центрального пункту);

4.9.2. Телефонний зв'язок з керівництвом підрозділів охорони.

4.10. Територіальні підрозділи Служби безпеки України, Національної поліції України, Державної служби з надзвичайних ситуацій України, що забезпечують безпеку об'єкта та ліквідацію надзвичайних ситуацій:

4.10.1. Найближче відділення поліції;

4.10.2. Найближчий територіальний підрозділ Управління Служби безпеки України;

4.10.3. Найближчий територіальний підрозділ Державної служби з надзвичайних ситуацій України.

Розділ 5. Забезпечення пожежної безпеки

5.1. Наявність правил протипожежної безпеки та іншої документації з питань забезпечення пожежної безпеки на об'єкті.

5.2. Наявність та стан із вказівкою в додатку на схемі:

5.2.1. Шляхів евакуації;

5.2.2. Під'їздів для протипожежних машин;

5.2.3. Систем пожежної сигналізації;

5.2.4. Обладнання пожежогасіння;

5.2.5. Обладнання для поглинання диму;

5.2.6. Засобів та обладнання:

протипожежних щитів;

протипожежних внутрішніх водопроводів;

протипожежних гідрантів;

протипожежних кранів і рукавів;

вогнегасників;

аварійного освітлення виходів;

автоматичних довідників на дверях евакуаційних виходів у будинках об'єкта;

інформаційних щитів та інструкцій з дотримання заходів і правил протипожежної безпеки.

Розділ 6. Прогнозовані моделі терористичних актів відносно об'єкта

6.1. Відомості про терористичні акти, що мали місце на об'єкті із проведенням короткого аналізу причин їхнього виникнення.

6.2. Інформація про можливі акти тероризму.

- 6.2.1. Загроза вибуху (підпалу) або вибух (підпал) на об'єкті;
- 6.2.2. Захоплення заручників із числа обслуговуючого персоналу та осіб, що відвідують об'єкт із зазначенням приблизної кількості осіб;
- 6.2.3. Виведення з ладу або несанкціоноване втручання в роботу систем газо-, водо-, електропостачання та інших комунікацій об'єкта (з прив'язкою до приміщень та території об'єкта);
- 6.2.4. Вчинення кібератаки на комунікаційну або технологічну систему об'єкта, вчинення несанкціонованих дій, виникнення кіберінцидентів, що можуть призвести до порушення конфіденційності, цілісності чи доступності інформації за рахунок утворення технічних каналів витоку (впливу);
- 6.2.5. Інші можливості для здійснення терористичних актів (розробляється на розсуд розробника паспорта);
- 6.2.6. Можливі наслідки в результаті здійснення терористичного акту на об'єкті та на прилеглій території:
 - приблизна кількість загиблих;
 - приблизна кількість потерпілих (поранених), заражених;
 - інші наслідки (ситуації) у результаті терористичних актів.
- 6.2.7. Найменування найближчих лікувальних закладів для розміщення потерпілих та відстань до них (км).

Розділ 7. Заходи, які виконуються та плануються щодо зміцнення антитерористичного захисту та зниження уразливості об'єкта

7.1. Першочергові, невідкладні заходи:

- 7.1.1. Посилення охорони периметру об'єкта, уразливих ділянок та споруджень;
- 7.1.2. Обладнання локальних зон безпеки;
- 7.1.3. Збільшення чисельності та озброєння охоронних підрозділів;
- 7.1.4. Інші заходи.

7.2. Довгострокові заходи, що вимагають тривалого часу та значних затрат:

- 7.2.1. Переобладнання системи охорони;
- 7.2.2. Обладнання сучасних систем інженерно-технічних засобів охорони:
 - оснащення комплексом охоронної сигналізації та системи відеоспостереження;
 - забезпечення на об'єкті конфіденційності, цілісності і доступності інформації, які можуть бути порушені шляхом утворення технічних каналів витоку або впливу на інформацію, вжиття інших заходів спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак;
- 7.2.3. Інші заходи (у т.ч. загородження території, створення зон безпеки, збільшення чисельності співробітників охорони, придбання захисних засобів та ін.).

Розділ 8. Відомості щодо інформації і ресурсів, уразливих по технічних каналах витоку (впливу)

8.1. Режимні приміщення, інформаційні засоби і системи, в яких обробляється інформація з обмеженим доступом із зазначенням їх категорії (I-IV) і класу (1-3).

8.2. Комунікаційні та технологічні системи, критично-важливі для функціонування об'єкта, із зазначенням фактичного місцезнаходження серверного обладнання, IP-адрес, операторів/провайдерів комунікаційних послуг.

8.3. Інформаційні ресурси (реєстри, бази даних, програмне забезпечення тощо), критично важливі для функціонування об'єкта, із зазначенням серверів і клієнтських комп'ютерів, де вони зберігаються (інстальовані).

8.4. Відомості щодо виконання на такому об'єкті Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518.

Розділ 9. Ситуаційні плани дій при виникненні надзвичайних ситуацій на об'єкті

9.1. Ситуаційні плани, що містять позначення:

9.1.1. Ділянок і установок об'єкта, можливі підходи до них, у тому числі прихованих у підземних комунікаціях;

9.1.2. Розміщення інженерних споруд охорони об'єкта;

9.1.3. Розташування постів охорони;

9.1.4. Місця прихованого зосередження резервних груп і маршрутів висунення до елементів інженерних споруд та уразливих елементів об'єкта;

9.1.5. Місця розташування штабу операції;

9.1.6. Загальні схеми інженерних комунікацій (теплотрас, прохідних тунелів з комунікаціями, каналізації та ін.);

9.1.7. Загальні схеми комунікаційних і технологічних (телекомунікаційних, інформаційно-телекомунікаційних) мереж об'єкта;

9.1.8. Секторів і ділянок об'єкта, на яких заборонено застосовувати вогнепальну зброю, вибухові та спеціальні засоби;

9.1.9. Приміщень і споруд об'єкта, в яких неможливе використання радіозв'язку.

Розділ 10. Забезпечення режиму секретності

10.1. Наявність на об'єкті режимно-секретного органу, його чисельність (штатна, фактична).

10.2. Заходи щодо забезпечення режиму секретності та збереження секретних відомостей в умовах надзвичайної ситуації на об'єкті.

Додаток 2
до Правил антитерористичної безпеки

Кількісний показник масштабів людських втрат

Масштаб	Кількість загиблих	Кількість поранених
Об'єктовий	до 10	до 100
Місцевий	від 11 до 50	від 101 до 500
Регіональний	від 51 до 300	від 501 до 1000
Державний	від 301 та більше	від 1001 та більше

Додаток 3
до Правил антитерористичної безпеки

Кількісний показник масштабів економічних втрат

Масштаб	Ступінь порушення виробничих зв'язків (функціонування)	Фінансові втрати, неоподаткованих мінімумів доходів громадян
Об'єктовий	не порушено виробничі зв'язки з іншими підприємствами, установами та організаціями	до 1 тис
Місцевий	порушено виробничі зв'язки (функціонування) підприємств населеного пункту, в якому розташований об'єкт	від 1 тис до 50 тис
Регіональний	порушено виробничі зв'язки (функціонування) підприємств у межах області	понад 50 тис до 250 тис
Державний	порушено виробничі зв'язки (функціонування) підприємств двох і більше областей	понад 250 тис та більше

Додаток 4
до Правил антитерористичної безпеки

Кількісний показник зниження рівня безпеки життєдіяльності

Масштаб	Розміри території забруднення (зараження)	Кількість осіб, що перебувають у зоні ураження
Об'єктовий	шкода, завдана навколишньому природному середовищу в межах території об'єкта	до 100
Місцевий	шкода, завдана навколишньому природному середовищу в межах одного або кількох населених пунктів	від 101 до 5000
Регіональний	шкода, завдана навколишньому природному середовищу в межах області	від 5001 до 50 000
Державний	шкода, завдана навколишньому природному середовищу в межах двох і більше областей	від 50 001 та більше



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від

2022 р. №

Київ

Про затвердження Правил антитерористичної безпеки

Кабінет Міністрів України **постановляє:**

Затвердити Правила антитерористичної безпеки, що додаються.

Прем'єр-міністр України

Д. Шмигаль

Голова Служби безпеки України

Іван БАКАНОВ

“ ___ ” _____ 2022 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проекту постанови Кабінету Міністрів України
“Про затвердження Правил антитерористичної безпеки”

1. Мета

Проект постанови Кабінету Міністрів України “Про затвердження Правил антитерористичної безпеки” розроблено Службою безпеки України в межах законодавчо визначених повноважень з метою встановлення загальних обов’язкових вимог для об’єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності, а також критеріїв та методики ідентифікації об’єктів можливих терористичних посягань.

2. Обґрунтування необхідності прийняття акта

Прийняття вказаного нормативно-правового акта спрямоване на забезпечення антитерористичної захищеності об’єктів можливих терористичних посягань, підвищення ефективності систем та режимів охорони об’єктів можливих терористичних посягань та зниження ризику реалізації терористичних загроз на таких об’єктах.

Головною метою забезпечення антитерористичної безпеки є збереження життя та здоров’я громадян, майна фізичних або юридичних осіб, державного або комунального майна, навколишнього природного середовища, тварин і рослин, що знаходяться на цих об’єктах або на прилеглий до них місцевості.

Прийняття акта дозволить підготувати Антитерористичному центру при Службі безпеки України повний перелік об’єктів нерухомості, які потребують належного антитерористичного захисту та сприятиме впровадженню особливих правил антитерористичної безпеки щодо цих об’єктів.

3. Основні положення проекту акта

Проектом акта пропонується встановити загальні обов’язкові вимоги щодо антитерористичної захищеності об’єктів можливих терористичних посягань, організаційні та технічні умови забезпечення їх антитерористичної захищеності, особливості організації заходів з інформування про терористичну загрозу на таких об’єктах та контроль за ефективністю вживаних заходів із антитерористичної захищеності об’єктів.

Актом пропонується визначити методику ідентифікації та механізм віднесення об’єктів нерухомості до об’єктів можливих терористичних посягань.

Також нормативно-правовим актом встановлюються обов'язкове оформлення паспортів антитерористичної захищеності найбільш уразливих об'єктів можливих терористичних посягань та зразок такого паспорту.

4. Правові аспекти

У цій сфері правового регулювання діють:

Конституція України;

Закон України “Про національну безпеку”;

Закон України “Про боротьбу з тероризмом”;

Указ Президента України від 05.03.2019 № 53/2019 “Про Концепцію боротьби з тероризмом в Україні”;

Указ Президента України від 14.04.1999 № 379 “Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України”;

постанова Кабінету Міністрів України від 18.02.2016 № 92 “Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків”;

розпорядження Кабінету Міністрів України від 05.01.2021 № 7-р “Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом в Україні”;

Проект не належить до пріоритетних сфер адаптації законодавства України до законодавства Європейського Союзу.

5. Фінансово-економічне обґрунтування

Реалізацію проекту пропонується здійснювати за рахунок коштів Державного бюджету України, в межах бюджетів установ, які будуть реалізовувати концепцію, а також інших фінансових джерел, що не заборонені законодавством.

6. Позиція заінтересованих сторін

Проект акта погоджено без зауважень з Державною митною службою України (лист від 30.09.2021 № 08-1/21-01/8.6/9065), з Міністерством оборони України (лист від 13.09.2021 № 220/6101), Міністерством фінансів України (лист від 13.09.2021 № 10040-17-10/27967), Міністерством аграрної політики та продовольства України (лист від 13.09.2021 № 21-2900-05.1/7367), Міністерством економіки України (лист від 20.09.2021 № 2712-11/46070), Державною податковою службою України (лист від 20.09.2021 № 12910/5/99-00-10-05-05), Міністерством інфраструктури України (лист від 16.09.2021 № 12055/39/10-21), Міністерством цифрової трансформації України (лист від

09.09.2021 № 1/04-2-10030), Службою зовнішньої розвідки України (лист від 09.09.2021 № 11/3/8033дск), Адміністрацією Державної прикордонної служби України (лист від 18.10.2021 № 251-30517/0/6-21), Фондом державного майна України (лист від 10.09.2021 №10-18-21165), Державною інспекцією ядерного регулювання України (лист від 27.08.2021 № 13-27/12770).

Проект акта вважається погодженим без зауважень Міністерством закордонних справ України та Міністерством охорони здоров'я України.

Проект акта погоджено із зауваженнями, які враховано, Міністерством захисту довкілля та природних ресурсів України (лист від 31.08.2021 № 25/1-31/18565-21), Міністерством енергетики України (лист від 20.09.2021 № 26/1.1-10.1-14778), Державною службою України з надзвичайних ситуацій (лист від 08.10.2021 №01-17195/262-1), Міністерством внутрішніх справ України (лист від 28.09.2021 № 44739/1/14-2021), Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (лист від 17.09.2021 № 05/04-913).

Проект акта погоджено із зауваженнями, які враховано частково, Управлінням державної охорони України (лист від 07.09.2021 № 2/22-1682), Національною поліцією України (лист від 08.10.2021 № 46659/1/38-2021).

Проект не потребує проведення публічних консультацій з громадськістю.

7. Оцінка відповідності

У проекті відсутні положення, що стосуються зобов'язань України у сфері європейської інтеграції, прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод, впливають на забезпечення рівних прав та можливостей жінок і чоловіків, містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією, створюють підстави для дискримінації.

8. Прогноз результатів

Прийняття акта сприятиме впровадженню особливих правил антитерористичної безпеки, дозволить визначити перелік об'єктів можливих терористичних посягань, підвищити ефективність охорони таких об'єктів та знизити ризик реалізації терористичних загроз на них.

Голова Служби безпеки України

Іван БАКАНОВ

“ ___ ” _____ 2022 року

Аналіз регуляторного впливу до проекту Правил антитерористичної безпеки

I. Визначення проблеми

Проект Правил антитерористичної безпеки, що затверджуватиметься постановою Кабінету Міністрів України, розроблено Службою безпеки України в межах законодавчо визначених повноважень з метою вирішення наявних проблем у сфері боротьби з тероризмом, зокрема необхідності:

встановлення загальних обов'язкових вимог для об'єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності;

визначення критеріїв та методики ідентифікації об'єктів можливих терористичних посягань (ОМТП);

забезпечення антитерористичної захищеності ОМТП;

підвищення ефективності систем та режимів охорони ОМТП;

зниження ризику реалізації терористичних загроз на таких об'єктах.

Відповідно до Закону України "Про боротьбу з тероризмом" боротьба з тероризмом ґрунтується, зокрема, на законності та неухильному виконанні прав і свобод людини і громадянина, пріоритетності попереджувальних заходів та захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності. При цьому Служба безпеки України здійснює через Антитерористичний центр при Службі безпеки України координацію діяльності суб'єктів боротьби з тероризмом відповідно до визначеної законодавством України компетенції, а на вказаний Центр покладається розроблення концептуальних засад та програм боротьби з тероризмом.

З огляду на це вбачається, що головною метою забезпечення антитерористичної безпеки, що визначатиметься відповідними Правилами, є збереження життя та здоров'я громадян, майна фізичних або юридичних осіб, державного або комунального майна, навколишнього природного середовища, тварин і рослин, що знаходяться на цих об'єктах або на прилеглих до них місцевості.

Розроблення Правил антитерористичної безпеки обумовлене аналізом ситуації, яка склалася у сфері боротьби з тероризмом, а саме відсутність в Україні уніфікованого переліку об'єктів нерухомості, які потребують належного антитерористичного захисту, ускладнює можливість організації ефективної системи протидії можливим терористичним посяганням на такі об'єкти.

Водночас прийняття акта дозволить підготувати Антитерористичному центру при Службі безпеки України повний перелік об'єктів нерухомості, які потребують належного антитерористичного захисту, та впровадити особливі правила антитерористичної безпеки щодо цих об'єктів.

Відповідно до наявної інформації станом на 2021 рік дія регуляторного акта поширюється на суб'єктів господарювання, що є власниками об'єкта (об'єктів) можливих терористичних посягань або використовують його (їх) відповідно до законодавства. На даний час загальна кількість ОМТП складає

1499, в т.ч. у державній власності перебувають 912 ОМТП, в комунальній власності – 231 ОМТП, в приватній (акціонерній) власності – 275 ОМТП.

Основні групи (підгрупи), на які проблема має вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	-
Держава	+	-
Суб'єкти господарювання	+	-
У тому числі суб'єкти малого підприємництва	-	-

Урегулювання зазначених проблемних питань не може бути здійснено за допомогою:

ринкових механізмів, оскільки такі питання регулюються виключно нормативно-правовими актами;

діючих регуляторних актів, оскільки Закон України “Про боротьбу з тероризмом”, постанова Кабінету Міністрів України від 18.02.2016 № 92 “Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків”, та інші нормативно-правові акти у відповідній сфері регулювання не деталізують порядку віднесення об'єктів нерухомості до ОМТП.

Розв'язати наявну проблему можливо лише шляхом державного регулювання – розроблення регуляторного акта, положення якого заповнюють наявну правову прогалину у відповідній сфері боротьби з тероризмом.

II. Цілі державного регулювання

Основними цілями державного регулювання є визначення чітких, прозорих, однозначних для застосування суб'єктами господарської діяльності вимог щодо:

антитерористичної захищеності ОМТП;

організаційних та технічних умов забезпечення антитерористичної захищеності ОМТП;

особливостей організації заходів з інформування про терористичну загрозу на таких об'єктах;

контролю за ефективністю вжитих заходів із антитерористичної захищеності ОМТП.

III. Визначення та оцінка альтернативних способів досягнення цілей

Альтернативні способи розроблено за результатами обговорення на робочих зустрічах представників головного розробника проекту з заінтересованими органами та в ході проведених консультацій (*п'ять консультацій*).

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	<p>Залишення існуючого у сфері боротьби з тероризмом законодавства без змін.</p> <p>Проблемні питання, що стосуються виконання вимог Закону України “Про боротьбу з тероризмом”, не вирішуються.</p> <p>Продовжують існувати ризики неналежного забезпечення антитерористичної безпеки об’єктів можливих терористичних посягань, що ускладнюватиме організацію ефективної системи протидії можливим терористичним посяганням на такі об’єкти.</p>
Альтернатива 2	<p>Прийняття проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження.</p> <p>Запропонований спосіб забезпечує досягнення визначених цілей щодо нормативно-правового врегулювання питань, пов’язаних з підготовкою повного переліку об’єктів нерухомості, які потребують належного антитерористичного захисту, впровадженням особливих правил антитерористичної безпеки цих об’єктів та виконанням суб’єктами господарської діяльності, що є власниками ОМТП або використовують їх відповідно до законодавства, відповідних нормативних вимог забезпечення антитерористичної безпеки на цих об’єктах.</p>

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні	<p>1. Існуючі на сьогодні підзаконні нормативно-правові акти не повною мірою деталізують положення Закону України “Про боротьбу з тероризмом” в частині пріоритетності попереджувальних заходів та захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності, розроблення АТЦ при СБУ концептуальних засад та програм боротьби з тероризмом.</p>

		2. Залишаються ризики неналежного забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань, що негативним чином позначається на організації ефективної системи протидії можливим терористичним посяганням на такі об'єкти та призводить до неприйняттого підвищення матеріальних втрат в результаті терористичних нападів.
Альтернатива 2	<p>Запобігання ризикам, які спричиняє неналежне забезпечення антитерористичної безпеки ОМТП.</p> <p>Забезпечення антитерористичної захищеності ОМТП.</p> <p>Визначення критеріїв та методики ідентифікації ОМТП.</p> <p>Підвищення ефективності систем та режимів охорони ОМТП.</p> <p>Зниження ризику реалізації терористичних загроз на таких об'єктах.</p> <p>Встановлення загальних обов'язкових вимог для об'єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності.</p> <p>Організація і проведення командно-штабних і тактико-спеціальних навчань та тренувань на ОМТП.</p>	<p>Реалізація Правил антитерористичної безпеки в частині забезпечення антитерористичної захищеності ОМТП потребуватиме витрат за наведеними розрахунками в межах річних кошторисів суб'єктів господарювання та АТЦ при СБУ.</p>

Оцінка впливу на сферу інтересів громадян

Проект Правил антитерористичної безпеки не поширюється на сферу інтересів громадян, але опосередковано позитивно впливатиме на них в разі організації їхнього захисту від терористичної загрози

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник за розміром		Великі	Середні	Малі	Разом
Кількість	суб'єктів	1076	423	-	1499

господарювання, що підпадають під дію регулювання (одиниць)				
Питома вага групи в загальній кількості, відсотків	71%	29%	-	100%

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні	Неналежне забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань може призвести до критичних матеріальних втрат в результаті терористичних актів.
Альтернатива 2	Встановлення загальних обов'язкових вимог для об'єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності, позитивним чином вплине на стан забезпечення антитерористичної безпеки.	Витрати на реалізацію зазначеної альтернативи не перебільшують розмір потенційних матеріальних втрат внаслідок терористичних атак.

Вплив на сферу інтересів суб'єктів господарювання великого і середнього підприємництва (згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта, затвердженої постановою Кабінету Міністрів України від 11 березня 2004 року № 308).

Додаток 2 до Методики

Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1.	Організація робіт комісії з виявлення уразливих місць,	8 годин*36,11грн* 6 членів комісії*0.17 грн	8 годин*36,11грн* 6 членів комісії*0.17

	визначення загроз для ОМТП, ймовірних способів їхнього здійснення й моделей порушників та документального оформлення даної роботи ¹	*10 аркушів* = 1 734,98 грн	грн *10 аркушів* = 1 734,98 грн
2.	За результатами отриманих даних комісія здійснює заходи з ідентифікації об'єкта та формування прогнозованої загрози, готує висновок, передає його на затвердження до державного органу або органу місцевого самоврядування, до сфери управління якого належить об'єкт	4 години*36,11грн *12 членів комісії*0.17 грн*10аркушів = 1 733,28 грн	4 години*36,11грн *12 членів комісії*0.17 грн*10аркушів = 1 733,28 грн
3.	Розробка паспорта антитерористичної захищеності найбільш уразливого об'єкта можливих терористичних посягань, в т.ч. актів ідентифікації об'єкта як його невід'ємної частини, направлення його на погодження до КГ регіонального органу СБУ та до органу, до сфери управління якого належить об'єкт	8 годин*36,11грн = 288,88 грн	8 годин*36,11грн = 288,88 грн
4.	Матеріальні витрати	476,17 грн.	2380,85 грн.
5.	Повідомлення Антитерористичного центру при Службі безпеки України, а у разі необхідності інших суб'єктів боротьби з тероризмом, органів державної влади та/або органів місцевого самоврядування про необхідність включення їхніх представників до складу комісії, що здійснює формування прогнозованої загрози та проведення ідентифікації об'єкта	2 год.*36,11грн = 72,22 грн	361,1 грн
6.	Всього:	4.401,53 грн.	22007,65 грн.
7.	Повідомлення в разі необхідності підприємств, установ та організацій і відповідних місцевих органів виконавчої влади про необхідність залучення їхніх представників до процесу виявлення уразливих місць, визначення загроз для об'єкта можливих терористичних посягань, ймовірних способів їхнього здійснення й моделей	2 год. * 36,11грн = 72,22 грн	361,1 грн

	порушників**		
8.	Кількість суб'єктів великого і середнього підприємництва, на яких буде поширено регулювання.	1499	1499
9.	Сумарні витрати суб'єктів великого і середнього підприємництва на виконання регулювання	1 210 420,75 грн.	6052103,75 грн.
10.	Всього з урахуванням повідомлення в разі необхідності визначених суб'єктів про необхідність включення їхніх представників до складу комісії, що здійснює формування прогнозованої загрози та проведення ідентифікації об'єкта	4 473,75 грн.	22368,75 грн.

¹Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України "Про Державний бюджет України на 2021 рік"; час, який витрачається суб'єктами господарювання на пошук нормативно-правових актів в мережі Інтернет, – 0,5 год. (за результатами консультацій).

²Для обрахунку: вартість пачки паперу формату А4 становить 86 грн за 500 аркушів (0,17 грн 1 аркуш) https://rozetka.com.ua/ua/canon_8713878092269/p5002507/.

³Для обрахунку: ціна 1 конверта на 30 аркушів складає 6 грн. <https://www.ukrposhta.ua/ua/upakuvannia>.

⁴Для обрахунку: ціна пересилання в межах України 1 конверта складає 32 грн <https://www.ukrposhta.ua/ua/taryfy-ukrposhta-ekspres>.

**Такий захід може здійснюватися в разі необхідності виявлення уразливих місць ОМТП, визначення загроз для ОМТП, ймовірних способів їхнього здійснення й моделей порушників.

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1. Сумарні витрати для суб'єктів господарювання великого і середнього підприємництва згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта (рядок 1 пункту 8 таблиці «Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта) відсутні з огляду на відсутність регуляторного акта, що визначає правила антитерористичної безпеки для об'єктів можливих терористичних посягань	1. Існуючі на сьогодні підзаконні нормативно-правові акти не повною мірою деталізують положення Закону України "Про боротьбу з тероризмом" в частині пріоритетності попереджувальних заходів та захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності, та розроблення АТЦ при СБУ концептуальних засад та програм боротьби з тероризмом. 2. Залишаються ризики неналежного забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань, що негативним чином позначається на організації ефективної системи протидії можливим терористичним посяганням на такі

	об'єкти та призводить до неприйняттого підвищення матеріальних втрат в результаті терористичних актів.
<p>Альтернатива 2. Сумарні витрати для суб'єктів господарювання великого і середнього підприємництва згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта</p> <p>(рядок 2 пункту 8 таблиці “Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта”).</p> <p>Зазначені витрати є незначними порівняно з необхідністю належного забезпечення життя та безпеки громадян, що можуть постраждати внаслідок терористичних атак.</p>	<p>Зменшення ризиків від неналежного забезпечення антитерористичної безпеки ОМТП.</p> <p>Забезпечення антитерористичної захищеності ОМТП.</p> <p>Визначення критеріїв та методики ідентифікації ОМТП.</p> <p>Підвищення ефективності систем та режимів охорони ОМТП.</p> <p>Зниження ризику реалізації терористичних загроз на таких об'єктах.</p> <p>Встановлення загальних обов'язкових вимог для об'єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності.</p> <p>Щорічні витрати складають: 1 210 420,75грн.</p>

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Залишення існуючого у сфері боротьби з тероризмом законодавства без змін.	1	Проблемні питання, що стосуються виконання вимог Закону України “Про боротьбу з тероризмом”, не вирішуються. Продовжують існувати ризики неналежного забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань, що ускладнюватиме організацію ефективної системи протидії можливим терористичним посяганням на такі об'єкти.
Прийняття проекту Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження.	4	Прийняття нормативно-правового акта забезпечить повною мірою досягнення поставлених цілей. Проблема більше існувати не буде.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи в рейтингу
Альтернатива 1	Відсутні	Залишаються ризики неналежного забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань, що негативним чином позначається на організації ефективної системи протидії можливим терористичним посяганням на такі об'єкти та призводить до неприйняттого підвищення матеріальних втрат в результаті терористичних нападів	Проблема продовжуватиме існувати, що не забезпечить досягнення поставленої цілі. Проблемні питання, що стосуються виконання вимог Закону України "Про боротьбу з тероризмом", не вирішуються.
Альтернатива 2	Зменшуються ризики неналежного забезпечення антитерористичної безпеки об'єктів можливих терористичних посягань. В результаті прийняття проектів нормативно-правових актів встановлюються загальні обов'язкові вимоги для об'єктів можливих терористичних посягань, спрямовані на забезпечення їх антитерористичної захищеності. Підвищується ефективність систем та	Відсутні	Прийняття акта дозволить досягнути задекларованих цілей. Встановлюються чіткі, зрозумілі, прозорі вимоги для суб'єктів господарської діяльності, що є власниками об'єктів можливих терористичних посягань ОМТП або використовують їх відповідно до законодавства. Запроваджуються відповідні нормативні вимоги забезпечення антитерористичної безпеки на цих об'єктах.

	режимів охорони об'єктів можливих терористичних посягань, знижується ризик реалізації терористичних загроз на таких об'єктах.		
--	---	--	--

Рейтинг	Аргументи щодо переваги обраної альтернативи/ причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Залишення без змін чинних нормативно-правових актів у сфері боротьби з тероризмом.	Основна причина відмови – незабезпечення належної реалізації положень Закону України “Про боротьбу з тероризмом”, а також неможливість удосконалення нормативно-правових актів у сфері боротьби з тероризмом.	Немає.
Прийняття проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження.	Прийняття даного регуляторного акта сприятиме вдосконаленню нормативно-правових актів у сфері боротьби з тероризмом, дозволить підготувати АТЦ при СБУ повний перелік об'єктів нерухомості, які потребують належного антитерористичного захисту, та впровадити особливі правила антитерористичної безпеки щодо цих об'єктів. Підвищується ефективність систем та режимів охорони об'єктів можливих терористичних посягань, знижується ризик реалізації терористичних загроз на таких об'єктах.	Вплив зовнішніх факторів на дію регуляторного акта не очікується

Негативних наслідків від прийняття регуляторного акта не очікується.

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Реалізувати встановлену мету пропонується шляхом прийняття Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження.

Прийняття актів дозволить:

- встановити загальні обов'язкові вимоги для об'єктів можливих терористичних посягань, спрямовані на забезпечення їх антитерористичної захищеності;
- визначити критерії та методики ідентифікації об'єктів можливих терористичних посягань (ОМТП);
- забезпечити антитерористичну захищеність ОМТП;
- підвищити ефективність систем та режимів охорони ОМТП;
- знизити ризик реалізації терористичних загроз на таких об'єктах.

Ефективність запропонованого регуляторного акта забезпечуватиметься за рахунок встановлення чітких вимог до суб'єктів господарювання, що є власниками об'єктів можливих терористичних посягань або використовують їх відповідно до законодавства, та запровадження відповідних нормативних вимог забезпечення антитерористичної безпеки на цих об'єктах.

Проектом Правил антитерористичної безпеки передбачено викладення вичерпної інформації стосовно відомостей, що містить паспорт антитерористичної захищеності найбільш уразливого ОМТП, кількісних показників масштабів людських та економічних втрат.

Для впровадження цього регуляторного акта, проект якого погоджений із заінтересованими органами, необхідно здійснити інформування суб'єктів господарювання про вимоги проекту регуляторного акта шляхом оприлюднення його на офіційному вебсайті Служби безпеки України, налагодження інформаційного забезпечення між ланками системи антитерористичної безпеки.

Ризиків впливу зовнішніх факторів на дію регуляторного акта немає.

Досягнення цілей не передбачає додаткових організаційних заходів.

Прийняття акта не приведе до неочікуваних результатів і не потребуватиме додаткових витрат з державного бюджету.

Можлива шкода у разі очікуваних наслідків дії акта не прогнозується.

Реалізація акта матиме наслідком вчинення суб'єктами господарювання, що є власниками ОМТП або використовують їх відповідно до законодавства, додаткових дій по забезпеченню антитерористичної захищеності таких об'єктів.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні впроваджувати або виконувати ці вимоги

Прийняття проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження не призведе до неочікуваних результатів. Шкода від очікуваних наслідків дії регуляторного акта не прогнозується.

Прийняття зазначених проектів нормативно-правових актів не впливатиме на розмір надходжень до бюджету.

Державне регулювання не передбачає утворення нового державного органу (або нового структурного підрозділу діючого органу).

Сфера державного регулювання регуляторного акта стосуватиметься визначених суб'єктів господарювання та передбачатиме здійснення додаткових витрат за наведеними розрахунками. М-Тест не проводився, оскільки відсутня питома вага суб'єктів малого підприємництва у загальній кількості суб'єктів господарювання, на яких впливає проблема, що потребує розв'язання. Реалізація проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження має забезпечуватись за рахунок коштів державного та місцевого бюджетів, а також інших джерел, не заборонених законодавством (власних коштів суб'єктів господарювання, коштів міжнародної технічної допомоги та інших), в межах річних кошторисів суб'єктів господарської діяльності, на яких поширюватиметься дія відповідних нормативно-правових актів.

Бюджетні витрати на адміністрування регулювання для суб'єктів господарювання

Державний орган, для якого здійснюється розрахунок адміністрування регулювання: Антитерористичний центр при Службі безпеки України, його координаційні групи при регіональних органах Служби безпеки України, заклади вищої освіти Служби безпеки України, фахівці Служби безпеки України у сфері забезпечення державної безпеки.

Процедура регулювання суб'єктів господарювання (розрахунок на одного типового суб'єкта господарювання)	Планові витрати часу на процедуру	Вартість часу співробітника органу державної влади відповідної категорії (заробітна плата) ¹	Оцінка кількості процедур за рік, що припадають на одного суб'єкта господарювання	Оцінка кількості суб'єктів господарювання, що підпадають під дію процедури регулювання	Витрати на адміністрування регулювання (за рік), гривень ²
1.Формування прогнозованої загрози та ідентифікація об'єкта	2 год.	36,11 грн	1	275	19 860,5 грн (36,11 грн* 2 год.*1 процедура*275 суб'єктів господарювання)
2.Затвердження висновку комісії за результатами здійснення заходів з ідентифікації об'єкта та формування прогнозованої загрози	1 год.	36,11 грн	1	275	9 930,25 грн (36,11 грн* *1 год.* грн* 1 процедура*275 суб'єктів господарювання)

3.Надання методичної допомоги, рекомендацій та роз'яснень комісіям з питань ідентифікації об'єкта і формування прогнозованої загрози	1 год.	36,11 грн	1	500	18 055 грн (36,11 грн* *1 год.*36,11 грн*1 процедура*500 суб'єктів господарювання)
4.Перевірка затвердженого державним органом або органом місцевого самоврядування висновку за результатами ідентифікації об'єкта та формування прогнозованої загрози на допустимість та обґрунтованість віднесення об'єктів нерухомості до ОМТП та формування регіонального переліку ОМТП	1 год.	36,11 грн	1	1499	54 128, 89 грн (36,11 грн* *1 год.*36,11 грн*1 процедура*1499 суб'єктів господарювання)
5.Погодження та затвердження поданого паспорта антитерористичної захищеності ОМТП	2 год.	36,11 грн	1	1499	108 257, 78 грн (36,11 грн* *2 год.*36,11 грн*1 процедура*1499 суб'єктів господарювання)
6.Опрацювання письмових повідомлень керівництва об'єктів про усунення недоліків та вжиті заходи	2 год.	36,11 грн	1	150	10 833 грн (36,11 грн.* *2 год.*36,11 грн*1 процедура*150 суб'єктів господарювання)
Разом за рік	X	X	X	X	19860,5грн+ 9930,25грн+ 18055грн+ 54128,89грн+ 108257,78грн+ 10833грн =221065,42грн*

¹Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 36,11 грн/год відповідно до Закону України “Про Державний бюджет України на 2021 рік”.

²Вартість витрат, пов'язаних з адмініструванням процесу регулювання державними органами, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації та на кількість суб'єктів, що підпадають під дію процедури регулювання, та на кількість процедур за рік.

*Всі розрахунки, які наведені в аналізі регуляторного впливу, здійснюються в допустимо мінімальному значенні, є приблизними та можуть бути визначені після прийняття, набуття чинності та застосування норм регуляторного акта.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Регуляторний акт набирає чинності через два місяці з дня його офіційного опублікування, що дозволить здійснити суб'єктам, на яких поширюватиметься його дія, необхідні підготовчі заходи. Строк дії акта визначається як безстроковий з огляду на необхідність постійного забезпечення антитерористичної безпеки ОМТП.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозованими значеннями показників результативності регуляторного акта є:

- кількість суб'єктів господарювання, на яких поширюється дія акта;
- розмір коштів і час, що витратимуться суб'єктами господарювання, пов'язаними з виконанням вимог акта;
- рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта.

Звіт про відстеження результативності Правил антитерористичної безпеки міститиме:

- кількісні та якісні значення показників результативності, що є результатами відстеження результативності;
- дані та припущення, на основі яких здійснено відстеження результативності, а також способи їх одержання;
- використані методи одержання результатів відстеження результативності.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

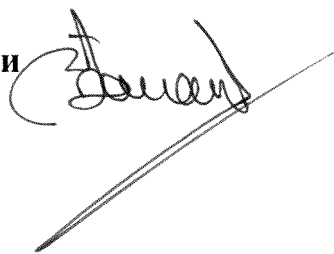
Базове відстеження результативності здійснюватиметься після набрання чинності цим регуляторним актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності акта здійснюватиметься впродовж двох років після набрання ним чинності шляхом здійснення моніторингу після прийняття запропонованого акта.

Періодичне відстеження результативності здійснюватиметься через кожні три роки, починаючи з дня виконання заходів із повторного відстеження.

Метод проведення відстеження результативності – статистичний. Відповідні відстеження будуть проводитись Службою безпеки України шляхом аналізу статистичних даних. Цільові групи, які залучатимуться для проведення відстеження, – суб'єкти господарювання, що є власниками ОМТП або використовують їх відповідно до законодавства.

Голова Служби безпеки України



Іван БАКАНОВ

“ 13 ” 12 2021 року

[Signature]
06.12.21

[Signature] 05.12.21
B. Асқаров 9173
СІТАРҒА

D.A. Corbett
03.12.2021

[Signature]
03.12.2021

[Signature] Ш. Ш. Керемет

ПОВІДОМЛЕННЯ

про оприлюднення проектів Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження

Службою безпеки України в межах законодавчо визначених повноважень розроблено проекти Правил антитерористичної безпеки та постанови Кабінету Міністрів України про їх затвердження з метою встановлення загальних обов'язкових вимог для об'єктів можливих терористичних посягань, спрямованих на забезпечення їх антитерористичної захищеності, а також критеріїв та методики ідентифікації об'єктів можливих терористичних посягань.

Ці проекти, а також аналіз регуляторного впливу акта буде розміщено на вебсайті Служби безпеки України у підпідрозділі "Регуляторна діяльність" підрозділу "Законодавство" розділу "Нормативно-правова база", на вкладці "Громадянам".

Зауваження і пропозиції до зазначених проектів нормативно-правових актів приймаються в письмовому вигляді та електронною поштою протягом місяця за адресами:

Служба безпеки України, вул. Володимирська, 33, м. Київ, 01601;

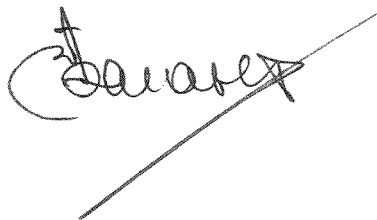
e-mail: atc@ssu.gov.ua;

тел.: (044) 288-50-29.

Державна регуляторна служба України, вул. Арсенальна, 9/11, м. Київ, 01011;

e-mail: inform@drs.gov.ua.

Голова Служби безпеки України



Іван БАКАНОВ

"13" грудня 2021 року

Скріншоти з вебсайту Служби безпеки України зі змінами до Плану діяльності Служби безпеки України з підготовки регуляторних актів на 2022 рік

AA  ssu.gov.ua 

ЗАТВЕРДЖУЮ
Голова Служби
безпеки України

Іван
БАКАНОВ

“ ” сінця 2022 року

ЗМІНИ до ПЛАНУ діяльності Служби безпеки України з підготовки проектів регуляторних актів на 2022 рік


№	Вид плану проекту регуляторного акта	Ціль прийняття проекту регуляторного акта	Строк відповідної інформації, відомостей та розроблення проекту регуляторного акта	Функціональні підрозділи, відповідальні за розроблення проекту регуляторного акта
2	Проект постанови Кабінету Міністрів України Визначення назв інших об'єктів, для яких здійснюється об'єктно-територіальна спеціалізована діяльність Служби безпеки України	Ціль прийняття проекту регуляторного акта	Екстрено	Штаб АТЦ при СБУ
	Проект постанови Кабінету Міністрів України Визначення назв інших об'єктів, для яких здійснюється об'єктно-територіальна спеціалізована діяльність Служби безпеки України	Ціль прийняття проекту регуляторного акта	Екстрено	Штаб АТЦ при СБУ


**Т.в.о. начальника Штабу – заступника керівника Антитерористичного центру
при Службі безпеки України**
Максим ЮРЧИШЕН

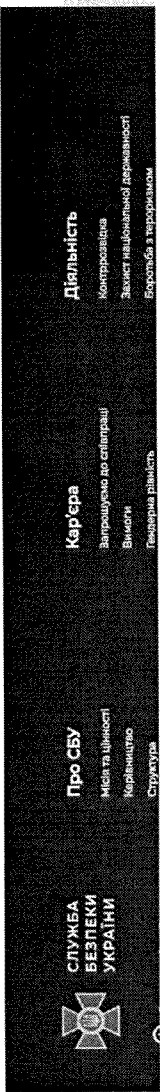
“ ” сінця 2022 року
“ПОГОДЖЕНО”
Перший заступник Голови СБ України –
керівник АТЦ при СБ України
Сергій АНДРУЩЕНКО
“ ” сінця 2022 року



внесення змін до Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації”

 **План діяльності Служби безпеки України з підготовки проектів регуляторних актів на 2022 рік**

 **Зміни до Плану регуляторних актів на 2022 рік**



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Про СБУ
Місія та цінності
Керівництво
Структура

Кар'єра
Запрошуємо до співпраці
Вимоги
Гарантія рівності

Діяльність
Контактна інформація
Заявка національної діяльності
Боротьба з тероризмом