



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

СТРАТЕГІЯ РОЗВИТКУ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ НА 2025-2030 РОКИ



ЗМІСТ

Преамбула	3
Розділ 1. Візія, місія, цінності та принципи	5
Розділ 2. Пріоритетні напрями діяльності	6
Розділ 3. Наші цілі та завдання	16
Розділ 4. Очікувані результати	18
Розділ 5. Механізм реалізації та фінансування стратегії	18
Додаток 1. Правове поле для трансформації СБУ	19



ПРЕАМБУЛА

Стратегія розвитку Служби безпеки України розроблена відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392, Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16.02.2022 № 56, інших стратегічних програмних документів, а також враховує положення Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11.05.2023 № 273, та Плану заходів, спрямованого на його виконання, затвердженого розпорядженням Кабінету Міністрів України від 23.08.2024 № 792-р.

СТРАТЕГІЯ

- ♦ визначає основні напрями трансформації СБУ у єдиний національний контррозвідувальний орган, здатний завчасно та ефективно протидіяти зовнішнім і внутрішнім загрозам державній безпеці;
- ♦ передбачає впровадження сучасних підходів до управління кадрами та їх професійної підготовки, ризик-орієнтованих методів реагування на загрози, новітніх технологічних рішень в оперативну та бойову діяльність, у тому числі розвиток озброєння та впровадження військових інновацій, удосконалення інформаційно-аналітичної складової, покращення ресурсного забезпечення, цифрової трансформації, розширення міжнародної співпраці;
- ♦ враховує більш ніж 30-річний досвід роботи СБУ, у тому числі здобутий у 10-річній боротьбі з російською гібридною та збройною агресією проти України, революційні зміни у військових та інформаційних технологіях, трансформацію законодавства України, положення міжнародних безпекових договорів, зміни глобального безпекового середовища та реалізовані Україною заходи в рамках європейської інтеграції.

Окремі положення Стратегії можуть переглядатися та адаптуватися залежно від змін безпекового середовища.



ВІЗІЯ, МІСІЯ, ЦІННОСТІ ТА ПРИНЦИПИ

ВІЗІЯ

Ми – ефективна спецслужба сильної України, якій довіряє українське суспільство, надійний партнер у захисті демократії.

МІСІЯ

- ◆ ми захищаємо Український народ та національні інтереси України;
- ◆ відстоюємо конституційний лад, забезпечуємо державну безпеку;
- ◆ створюємо умови стратегічної переваги нашої держави в світі.

ЦІННОСТІ

- ◆ довіра Українського народу;
- ◆ повага до прав та свобод людини і громадянина;
- ◆ патріотизм, професіоналізм і постійне вдосконалення;
- ◆ унікальний досвід, здобутий під час війни;
- ◆ ефективна взаємодія зі спецслужбами країн-партнерів;
- ◆ корпоративна єдність.

ПРИНЦИПИ

- ◆ верховенство права та законність;
- ◆ відповідальність і підзвітність;
- ◆ політична нейтральність;
- ◆ оперативність, інноваційність, гнучкість та адаптивність;
- ◆ готовність до викликів;
- ◆ доброчесність та відданість служінню Українському народу.

**ОСНОВИ РЕАЛІЗАЦІЇ СТРАТЕГІЇ – ЛЮДИ,
ПРОЦЕСИ, ІННОВАЦІЇ, ПАРТНЕРСТВО.**

ПРІОРИТЕТНІ НАПРЯМИ ДІЯЛЬНОСТІ

ПРИ ВИЗНАЧЕННІ ПРІОРИТЕТІВ НАШОЇ МІСІЇ МИ ПОВИННІ НАДАВАТИ ВІДПОВІДІ НА ТАКІ ЗАПИТАННЯ:

- ♦ Які загрози безпеці України є актуальними та потенційно можуть виникнути?
- ♦ Яким із цих загроз має протидіяти СБУ?
- ♦ Які загрози на цей час становлять найбільшу небезпеку?
- ♦ Які сили, засоби, ресурси, технології та організаційно-правові заходи необхідні для реагування на загрози?

Найбільшою загрозою суверенітету, конституційному ладу та територіальній цілісності України залишається агресивна війна, яка ведеться російською федерацією за підтримки її союзників.

Ми робимо все можливе для звільнення тимчасово окупованих українських територій від ворога, ефективного знищення його ресурсів для ведення війни, нейтралізації шпигунів та агентури, притягнення до відповідальності зрадників, колаборантів і воєнних злочинців, протидії диверсіям, тероризму, інформаційним та кібератакам, захисту оборонно-промислового комплексу, об'єктів критичної інфраструктури, ланцюгів постачання від можливих терористичних посягань, охорони державної таємниці, а також підвищення довіри українського суспільства.

Інтегруємо інновації в оперативно-бойову діяльність, удосконалюємо ресурсне забезпечення та налагоджуємо взаємодію і координацію з іншими складовими сектору безпеки і оборони та безпековими інституціями країн-партнерів під час проведення спільних операцій.

Для ефективного захисту національних інтересів України в умовах війни та у відбудовний період нам потрібні сучасні технологічні рішення та інструментарій, зброя та озброєння, підготовлений персонал, достатня кількість ресурсів.

У воєнний час та відбудовний період наша діяльність зосереджуватиметься на виконанні завдань за такими напрямками.

БОЙОВІ ОПЕРАЦІЇ



Для СБУ війна розпочалася ще у 2014 році, хоча мала дещо інший характер – це була гібридна агресія з локальними зонами бойових дій. Повномасштабне вторгнення росії в 2022 році стало загрозою набагато більшого масштабу, а фронт простягнувся на тисячі кілометрів. Тому підходи до ведення війни та технічне оснащення, які застосовувались десять років тому, неможливо порівнювати з сучасними реаліями.

Під час війни з росією СБУ стала генератором нових військових ідей, технологій та компетенцій.

Ми активно використовуємо високоточну зброю, сучасні системи розвідки, автоматизовані системи керування, різні типи ударних безпілотних систем. Це дає нам перевагу – бути завжди на крок попереду ворога і завдавати ударів там, де він цього не очікує, у тому числі по об'єктах військово-промислового сектору та центрах забезпечення російської армії у глибокому тилу рф.

З цією метою ми постійно працюємо над покращенням оперативно-бойового забезпечення, у тому числі інтеграцією штучного інтелекту у військові технології, які здатні змінити розстановку сил на полі бою.

ПРІОРИТЕТИ

- ♦ *розвиток роботизованих наземних систем, розвідувально-ударних безпілотних комплексів у поєднанні зі штучним інтелектом, комплексами радіоелектронної розвідки і боротьби як потужного інструменту протидії ворогу на всіх фронтах – у морі, повітрі та на суші;*
- ♦ *розроблення новітніх засобів управління та захисту сил і засобів;*
- ♦ *підвищення мобільності і захищеності підрозділів завдяки використанню броньованого наземного транспорту, авіації, морських та річкових суден;*
- ♦ *взаємодія з оборонно-промисловим комплексом в інтересах розробки та виробництва сучасних видів зброї, озброєння, техніки;*
- ♦ *використання SIGINT, OSINT, IMINT, технології штучного інтелекту для оперативного виявлення і знищення ворожих цілей за будь-яких умов;*
- ♦ *покращення матеріально-технічного, медичного та логістичного забезпечення оперативно-бойових заходів незалежно від місця їх проведення.*

КОНТРРОЗВІДКА



Від часів здобуття незалежності України наші супротивники проводять переважно приховані розвідувальні та підривні операції (акції).

У сучасних геополітичних реаліях та в умовах розвитку технологій частина цілеспрямованих дій іноземних держав проти України залишається непомітною.

Для більш ефективної протидії супротивникам нам потрібно завчасно здобувати достовірну інформацію про їхні плани, наміри, методи, тактику дій, залучених осіб, вразливі місця. Також необхідно зосередитися на здійсненні агентурної розвідки (HUMINT), розвідки з відкритих джерел (OSINT), науково-технічної розвідки (MASINT), радіоелектронної розвідки (SIGINT) та розвідки на основі зображень (IMINT), автоматизації обробки та аналізу здобутої інформації з використанням новітніх інструментів і технологій, які допоможуть краще зрозуміти масштаб і характер загроз.

Ми повинні вийти за межі існуючого підходу до виявлення та передбачення дій наших супротивників і побудувати сучасну дієву систему завчасного впливу на їхню діяльність, спрямовану проти України.

ПРІОРИТЕТИ

- ♦ протидія розвідувально-підривній та іншій діяльності спеціальних служб іноземних держав, інших суб'єктів на шкоду Україні;
- ♦ контррозвідувальне забезпечення оборонного, економічного, інформаційного, науково-технічного потенціалу, об'єктів критичної інфраструктури, ланцюгів постачання, складових сектору безпеки і оборони, закордонних дипломатичних установ України, безпеки співробітників цих установ та членів їх сімей у державі перебування;
- ♦ сприяння дотриманню міжнародних санкцій, міжнародних режимів нерозповсюдження, державному контролю за міжнародними передачами товарів військового призначення та подвійного використання;
- ♦ розмежування контррозвідувальної, оперативно-розшукової діяльності (кримінальної розвідки), кримінального процесу, унормування процедур здійснення контррозвідувальної діяльності;
- ♦ розбудова системи забезпечення контррозвідувального режиму в Україні;
- ♦ запровадження гнучкої структури, здатної оперативно реагувати на загрози державній безпеці України;
- ♦ забезпечення власної безпеки.

ЗАХИСТ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ



Захист державного суверенітету, територіальної цілісності та конституційного ладу є одним із найважливіших пріоритетів Служби.

Основним джерелом загроз національній державності залишаються антиукраїнська політика, економічна експансія, територіальні зазіхання, розпалювання релігійної, ідеологічної, етнічної та іншої ворожнечі.

ПРІОРИТЕТИ

- ♦ нівелювання деструктивного впливу на суспільно-політичну, культурну, наукову, освітню та інформаційну сфери;
- ♦ удосконалення системи виявлення та протидії деструктивному інформацій-

Для цього іноземні держави широко використовують усі можливості – від зовнішньополітичних майданчиків до поширення фейкової інформації у соціальних мережах.

Ми повинні завчасно виявляти ознаки підготовки ворожих акцій, основну мету та спрямованість, причетних до них структур та осіб, залучені ресурси, форми і методи їх проведення та адекватно протидіяти їм.

норму впливу, у тому числі шляхом запобігання його організації, координації та фінансуванню;

- ♦ участь у загальнодержавних заходах із підвищення медіаграмотності населення.

БОРОТЬБА З ТЕРОРИЗМОМ

Служба безпеки України з перших днів створення надає пріоритетне значення боротьбі з тероризмом.

Ми протидіємо проявам тероризму та його фінансуванню, координуємо цю діяльність на державному рівні. Саме для такої координації функціонує Антитерористичний центр при СБУ.

На сьогодні терористична загроза еволюціонує: поряд із діяльністю організованих терористичних груп зросла загроза атак терористів-одинаків, які діють автономно, але часто під ідеологічним чи інформаційним впливом. Ці особи радикалізуються через мережу і можуть швидко мобілізуватися для вчинення насильницьких дій. Відсутність чіткої приналежності до терористичних організацій ускладнює їх ідентифікацію, виявлення і нейтралізацію підготовки терактів, а також розслідування таких діянь.

Міжнародні терористичні організації широко використовують Інтернет та соціальні мережі для поширення своїх ідеологій, радикалізації та вербування осіб, координації вчинення терактів.

На виконання міжнародних зобов'язань у сфері боротьби з тероризмом ми поєднуємо зусилля з іноземними партнерами для нейтралізації терористичних організацій (груп), виявлення ознак підготовки терористичних актів та осіб, яких вербують або спонукають до їх вчинення, ланцюгів постачання вибухівки й інших знарядь, міжнародних каналів переправлення виконавців, фінансування, навчання тероризму.

У воєнний час та після закінчення воєнних дій незаконний обіг зброї, озброєння, боєприпасів та вибухівки прогнозовано буде зростати і використовуватися терористичними організаціями (групами, терористами) та іншими складовими кримінального середовища.



ПРІОРИТЕТИ

- ♦ підвищення ефективності взаємодії СБУ з іншими суб'єктами боротьби з тероризмом та міжнародними партнерами;
- ♦ приведення національного законодавства у сфері боротьби з тероризмом у відповідність до міжнародного законодавства;
- ♦ запровадження ефективних механізмів моніторингу, обробки та обміну інформацією про виявлені ознаки підготовки терористичного акту (діяльності), осіб, причетних до них, форми, методи і засоби терористичної діяльності, джерела її фінансування;
- ♦ забезпечення професійного навчання для представників цивільного сектору, органів державної влади та місцевого самоврядування з питань протидії тероризму, залучення відповідних представників до антитерористичних навчань.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ

Світ швидкоплинно змінюється внаслідок прискорення процесів цифрової трансформації, інтенсивного розвитку інформаційно-комунікаційних технологій та очікуваного збільшення ролі інтелектуальних можливостей комп'ютерних систем.

Саме кіберпростір та його інструментарій відкривають супротивнику широкі можливості для здійснення різноманітних деструктивних діянь без ризику для себе – від збору потрібної інформації, зокрема шляхом поглибленого моніторингу інформаційного сегменту, несанкціонованих технічних проникнень, до вчинення кібератак на об'єкти критичної інфраструктури, сфер військового та державного управління, поширення деструктивної пропаганди та дезінформації.

Наші супротивники широко використовують інформаційний та кіберпростір, сучасні технології, у тому числі призначені для втручання в автоматизоване керування процесами життєдіяльності та прийняття



управлінських рішень. Це несе нові ризики і загрози для держави та людини.

Ми повинні в межах повноважень спільно з іншими суб'єктами забезпечення інформаційної безпеки та кібербезпеки створити умови для унеможливлення деструктивного впливу на інформаційний та кіберпростір держави, а також для формування потенціалу стримування, забезпечення стійкості та взаємодії.

ПРІОРИТЕТИ

- ♦ протидія деструктивним впливам (спеціальним інформаційним, інформаційно-психологічним спеціальним операціям) в інформаційному просторі;
- ♦ удосконалення системи протидії і реагування на кіберінциденти, кібератаки, кіберзагрози, у тому числі шляхом внесення змін до національного законодавства у сфері боротьби з кіберзлочинністю;
- ♦ посилення спроможностей контррозвідувального забезпечення сфери електронних комунікацій, IT-сфери, афілійованого з ними середовища, проведення розвідувальних заходів у кіберпросторі, розслідування кіберінцидентів та кібератак, актів кібершпигунства, кібертероризму та кібердиверсій;
- ♦ запровадження координації діяльності суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям та іншим кіберзагрозам у сфері державної безпеки;
- ♦ удосконалення процедури використання електронних (цифрових) доказів у кримінальному провадженні, часткового розкриття даних про рух інформації та застосування термінового збереження інформації, спрямованих на повну імплементацію Конвенції про кіберзлочинність;
- ♦ розробка і впровадження сучасних засобів кібербезпеки та IT-технологій в контррозвідувальному забезпеченні кібербезпеки та інформаційної безпеки держави;
- ♦ запровадження системи проведення перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;
- ♦ розширення співробітництва з іноземними партнерами щодо розслідування кіберінцидентів, кібератак, кібершпигунства та кібертероризму, а також притягнення винних до відповідальності.

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЛАНЦЮГІВ ПОСТАЧАННЯ



Належний захист критичної інфраструктури та ланцюгів постачання є важливим для розвитку та функціонування будь-якої держави в сучасному світі. Порушення роботи об'єктів критичної інфраструктури може загрожувати стабільності діяльності секторів економіки та національній безпеці.

Контррозвідувальне забезпечення стійкості критичної інфраструктури, зокрема об'єктів енергетики, промисловості, транспортних систем, інших об'єктів критичної інфраструктури, є складовою такого захисту.

Ворожими та недружніми країнами активно вживаються заходи зі здобуття інформації про об'єкти критичної інфраструктури, їх захист та організацію

життєзабезпечення. Їх цікавлять технології та оснащення, елементи допомоги, що надана Україні країнами-партнерами, ланцюги постачання такої допомоги та інших критично важливих товарів, робіт і послуг.

Одночасно із цілеспрямованим руйнуванням об'єктів критичної інфраструктури тривають спроби промислового шпигунства, блокування зовнішніх інвестицій, уникнення санкцій, зниження конкурентоздатності української продукції.

Спільно з іншими суб'єктами національної системи захисту критичної інфраструктури нам необхідно побудувати стійку та ефективну систему виявлення і протидії загрозам критичній інфраструктурі та ланцюгам постачання.

ПРІОРИТЕТИ

- ♦ підвищення рівня безпеки і стійкості національної критичної інфраструктури;
- ♦ сприяння у створенні платформ реагування на прояви і втручання у функціонування об'єктів критичної інфраструктури, удосконалення чинних систем міжвідомчого реагування;
- ♦ зменшення ризиків терористичного і диверсійного характеру щодо об'єктів

критичної інфраструктури та ланцюгів постачання, у тому числі шляхом розвитку взаємодії між суб'єктами національної системи захисту критичної інфраструктури;

- ♦ контррозвідувальний захист інновацій побудови, функціонування та відновлення об'єктів критичної інфраструктури.

ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Україна, як і кожна інша держава, захищає інформацію, витік якої може завдати шкоди національним інтересам.

З початком гібридної та повномасштабної війни зросла важливість цієї роботи.

Іноземні спецслужби активно здійснюють агентурну, легальну та технічну розвідку для отримання відомостей, зокрема, про обороноздатність держави, функціонування оборонно-промислового, енергетичного та транспортного комплексів, оборонні науково-технічні розробки та їх впровадження, потреби,

пов'язані із життєзабезпеченням, зовнішні відносини, у тому числі міжнародно-технічне співробітництво.

Ми постійно відстежуємо розвідувальні спрямування іноземних спецслужб та їхньої агентури, локалізуємо передумови для витіку секретної та чутливої інформації.

Охорона державної таємниці та інформації з обмеженим доступом, а також виконання міжнародних зобов'язань про захист такої інформації залишається для нас ключовим напрямом діяльності.



ПРІОРИТЕТИ

- ♦ удосконалення системи контррозвідувального забезпечення охорони державної таємниці та службової інформації, у тому числі, що обробляється в інформаційно-комунікаційних системах, з урахуванням стандартів безпеки НАТО та ЄС;
- ♦ удосконалення дозвільного порядку провадження діяльності, пов'язаної з державною таємницею, порядку надання

та припинення громадянам допуску та доступу до державної таємниці, а також порядку засекречування інформації;

- ♦ адаптація системи захисту інформації з обмеженим доступом до актуальних загроз державній безпеці;
- ♦ запровадження механізмів захисту інформації, витік та поширення якої може завдати шкоди національним інтересам.

АНАЛІТИКА

Прийняття своєчасних і виважених рішень керівництвом держави та Служби безпеки України залежить від забезпечення їх точними, актуальними аналітично-інформаційними продуктами.

Ми постійно моніторимо стан безпекового середовища, досліджуємо загрози і ризики державній безпеці, прогнозуємо імовірний розвиток ситуацій.

Для обробки й аналізу інформації використовуємо сучасний інструментарій та технології, які допомагають швидше та якісніше опрацьовувати великі обсяги даних, розуміти масштаби і характер загроз, забезпечувати оперативне реагування на них.

Активно впроваджуємо новітні методи та засоби аналітичної розвідки, у тому числі розвідки з відкритих джерел (OSINT), можливості штучного інтелекту та машинного навчання.

Нам потрібно більше інвестувати в розвиток інформаційно-аналітичної діяльності.

Для ефективної протидії загрозам у швидкоплинному та багатовимірному безпековому середовищі нам необхідно впроваджувати сучасні IT-технології та рішення. Це забезпечить комплексне посилення спроможностей СБУ з виконання всього спектру покладених завдань.



ПРІОРИТЕТИ

- ♦ розвиток технологічної складової інформаційно-аналітичної роботи, цифровізація процесів службової діяльності, вдосконалення інформаційно-комунікаційних систем та інших IT-послуг і сервісів, автоматизація процедур добування (збору), обробки, аналізу та відображення інформації;
- ♦ постійна колаборація аналітичних та оперативної складових діяльності СБУ в інтересах посилення спроможностей із своєчасного виявлення і реагування на загрози;
- ♦ впровадження інноваційних методів аналітичної розвідки та OSINT-діяльності із застосуванням інструментів штучного інтелекту й машинного навчання;
- ♦ вдосконалення підходів і засобів моніторингу та ситуаційного аналізу оперативної обстановки, а також взаємодії у рамках мережі ситуаційних центрів державних органів;
- ♦ систематичне підвищення професійних компетентностей аналітиків та їх взаємодії з експертним середовищем.

РОЗСЛІДУВАННЯ

З початком російської гібридної агресії ми зіткнулися з новими злочинами, що завдають значної шкоди державній безпеці.

Російські окупаційні війська та спецслужби систематично вчиняють велику кількість злочинів, спрямованих на знищення нас як нації та посягання на національну безпеку України. Звільнені від тимчасової окупації території та населені пункти відкривають світові докази жорстоких та нелюдських злочинів загарбників, серед яких – злочини геноциду, проти людяності, а також воєнні злочини.

Наша діяльність спрямована на досудове розслідування злочинів, спрямованих на посягання на основи національної та державної безпеки, злочинів проти миру, безпеки людства та міжнародного правопорядку, тероризму, а також у сфері охорони державної таємниці.

Кожен факт злочинної діяльності детально документується не лише в інтересах українського, а й для здійснення міжнародного правосуддя. Справедливу відповідальність перед Міжнародним кримінальним судом мають понести як безпосередні виконавці скоєного, так і військово-політична верхівка держави-агресора.



ПРІОРИТЕТИ

- ♦ впровадження інформаційно-комунікаційних систем у процеси досудового розслідування, новітніх технологій та сучасного інструментарію для збору і збереження первинних доказів з місця події;
- ♦ удосконалення методів збору, обробки, структурування, криміналістичного аналізу доказів;
- ♦ удосконалення процесу фіксації та використання цифрових доказів у кримінальному процесі;
- ♦ посилення техніко-криміналістичних та судово-експертних спроможностей

для забезпечення ефективного досудового розслідування;

- ♦ удосконалення правової основи для міжнародної співпраці у сфері кримінального судочинства між Україною та країнами-партнерами;
- ♦ забезпечення мобільної та автономної роботи підрозділів досудового розслідування, у тому числі в зоні бойових дій, створення умов для належного та безпечного документування злочинів, вчинених на тимчасово окупованих територіях.

ІНСТИТУЦІЙНА СТІЙКІСТЬ

- ♦ розмежування повноважень з іншими складовими сектору безпеки і оборони України;
- ♦ посилення ролі СБУ як єдиного національного контррозвідального органу в складі сектору безпеки і оборони;
- ♦ подальший розвиток бойової компоненти СБУ, як складової сил безпеки і оборони, що здатна застосовувати всі види зброї, озброєння, військової та спеціальної техніки;
- ♦ підвищення рівня координації суб'єктів боротьби з тероризмом;
- ♦ удосконалення системи протидії і реагування на кіберзагрози, розмежування завдань та повноважень між суб'єктами національної системи кібербезпеки, розслідування кіберінцидентів і кібератак, впровадження сучасних засобів кібербезпеки та IT-технологій, а також створення інструментарію кіберспроможностей СБУ;
- ♦ посилення контррозвідальної складової у сфері захисту національної критичної інфраструктури та ланцюгів постачання, а також координації і взаємодії між уповноваженими суб'єктами;
- ♦ удосконалення форм і методів аналітичного прогнозування ризиків та загроз національній і державній безпеці, планування заходів з протидії їм;
- ♦ створення дієвої системи правового регулювання забезпечення державної безпеки з урахуванням геополітичних змін;
- ♦ запровадження гнучкої та адаптивної структури СБУ, ризикорієнтованих підходів;
- ♦ досягнення збалансованого поєднання демократичного цивільного контролю та підзвітності, внутрішнього контролю, забезпечення дотримання принципу доброчесності;
- ♦ впровадження системи стратегічного менеджменту;
- ♦ визначення спроможностей та потреб відповідно до функцій і завдань СБУ в мирний час, на особливий період.

ОПЕРАЦІЙНІ ПРОЦЕСИ

- ♦ розвиток системи внутрішніх комунікацій та ефективної взаємодії між співробітниками і підрозділами, у тому числі на горизонтальних рівнях;
- ♦ уніфікація та стандартизація основних процесів службової діяльності;
- ♦ удосконалення процесів та інструментів оперативно-бойової діяльності підрозділів Служби;
- ♦ модернізація форм, методів і засобів, що використовуються для виконання завдань, функцій та реалізації повноважень Служби;
- ♦ актуалізація механізмів та інструментарію моніторингу безпекового середовища, виявлення загроз і оцінки ризиків національній безпеці, реагування на них;
- ♦ впровадження передових алгоритмів логістичного, матеріально-технічного та іншого забезпечення.

ЛЮДСЬКИЙ КАПІТАЛ

- ♦ упровадження прозорого управління людськими ресурсами з дотриманням принципів гендерної рівності, за якого добір і кар'єрне зростання співробітників здійснюється на основі їх професійних компетентностей та доброчесності;
- ♦ модернізація відомчої освіти відповідно до актуальних потреб Служби безпеки України;
- ♦ забезпечення адаптації особового складу до змін безпекового середовища шляхом постійного навчання та розвитку професійних компетентностей, у тому числі володіння англійською мовою як засобу міжнародного спілкування;
- ♦ створення резерву військово-навчених людських ресурсів, забезпечення їх підготовки, накопичення та утримання;
- ♦ розбудова системного моніторингу ефективності кадрів, створення умов для мотивації та планування кар'єри;
- ♦ розвиток корпоративної культури, професійної етики та доброчесності;
- ♦ підвищення рівня соціально-правового захисту, грошового забезпечення особового складу, медичного забезпечення співробітників та членів сімей, ветеранів;
- ♦ реінтеграція до цивільного життя військовослужбовців, які підлягають звільненню з військової служби.

ІНФРАСТРУКТУРА І ТЕХНОЛОГІЇ

- ♦ розробка та впровадження новітніх засобів управління та захисту, підтримка інновацій у сфері озброєння та техніки;
- ♦ цифрова трансформація та модернізація технологічної інфраструктури, впровадження сучасних IT-технологій і рішень у процеси збору, обробки та аналізу інформації за пріоритетними напрямками діяльності;
- ♦ розбудова єдиного захищеного інформаційного простору з використанням передових безпекових технологій;
- ♦ удосконалення системи технічного захисту інформації, впровадження новітніх засобів е-комунікації та спеціального зв'язку;
- ♦ забезпечення відмовостійкого функціонування та використання інформаційно-комунікаційних систем, реєстрів, банків даних, довідкових ресурсів та інших IT-послуг/сервісів.

КООРДИНАЦІЯ, ВЗАЄМОДІЯ ТА ПАРТНЕРСТВО

- ♦ удосконалення механізмів взаємодії СБУ зі складовими сектору безпеки і оборони, іншими державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями;
- ♦ співпраця з громадянами та їх об'єднаннями на засадах довіри в інтересах спільного забезпечення національної безпеки та національних інтересів;
- ♦ підготовка персоналу складових сектору безпеки і оборони України з питань забезпечення національної безпеки;
- ♦ антитерористична підготовка населення до дій в умовах терористичної загрози;
- ♦ розширення співпраці зі спецслужбами та правоохоронними органами інших держав, безпековими структурами міжнародних організацій.

ОЧІКУВАНІ РЕЗУЛЬТАТИ

ЗАВДЯКИ ВПРОВАДЖЕННЮ СТРАТЕГІЇ СЛУЖБА БЕЗПЕКИ УКРАЇНИ:

сучасна та ефективна національна спеціальна служба, зосереджена на виконанні завдань за такими напрямками діяльності: контррозвідка; виконання спеціальних та бойових завдань; захист національної державності; боротьба з тероризмом та протидія його фінансуванню; контррозвідувальне забезпечення інформаційної безпеки та кібербезпеки держави; контррозвідувальне забезпечення критичної інфраструктури та ланцюгів постачання, оборонного і науково-технічного потенціалу; охорона державної таємниці; інформаційно-аналітична робота; розслідування злочинів відповідно до компетенції;

єдиний національний контррозвідувальний орган, який спрямовує діяльність інших суб'єктів забезпечення державної безпеки;

ефективна бойова складова сил безпеки і оборони, яка має функції, повноваження, сучасний інструментарій та ресурси для своєчасного виявлення та ефективного реагування на виклики

і загрози державній безпеці;

застосовує в діяльності ризик-орієнтовані підходи, формує організаційно-штатну структуру з урахуванням безпекової ситуації та ресурсів;

використовує сучасні стратегічні, зовнішні та внутрішні комунікації, має ефективну систему внутрішнього контролю та антикорупційну програму; політично нейтральна та незалежна спецслужба;

користується довірою та авторитетом в українському суспільстві;

перебуває під прозорим цивільним демократичним контролем;

є надійним міжнародним партнером; ефективно обмінюється інформацією та координує спільні дії, у тому числі через визначені механізми взаємодії між Україною та країнами-партнерами; використовує осучаснену систему управління людськими ресурсами.

Співробітники Служби безпеки України професіонали, які у повсякденній діяльності керуються принципами доброчесності та професійної етики, віддано стоять на захисті прав і свобод людини і громадянина.

МЕХАНІЗМ РЕАЛІЗАЦІЇ ТА ФІНАНСУВАННЯ СТРАТЕГІЇ

СТРАТЕГІЯ ВПРОВАДЖУЄТЬСЯ ШЛЯХОМ:

розробки та впровадження необхідних законодавчих змін у сфері національної безпеки, забезпечення державної безпеки, контррозвідувальної діяльності, боротьби з тероризмом, охорони державної таємниці, оперативно-розшукової діяльності (кримінальної розвідки), інформаційної безпеки та кібербезпеки держави, електронних комунікацій, інформації та захисту персональних даних, демократичного цивільного контролю, соціально-правового захисту;

підготовки та реалізації проєктів, необхідних для досягнення цілей.

Проєкти можуть щороку переглядатися для актуалізації.

Оцінювання стану реалізації Стратегії включає поточний моніторинг та щорічну оцінку успішності виконання запланованих проєктів на підставі визначених індикаторів.

Основним джерелом фінансування реалізації Стратегії є Державний бюджет України, яким визначаються видатки для забезпечення належного функціонування і сталого розвитку СБУ. Джерелами фінансування також можуть бути міжнародна технічна допомога та інші джерела, не заборонені законодавством.

ПРАВОВЕ ПОЛЕ ДЛЯ ТРАНСФОРМАЦІЇ СБУ

ДОДАТОК 1

КОНСТИТУЦІЯ УКРАЇНИ

КОДЕКСИ

- ◆ Кримінальний кодекс України
- ◆ Кримінальний процесуальний кодекс України
- ◆ Кодекс України про адміністративні правопорушення
- ◆ Кодекс адміністративного судочинства України

ЗАКОНИ УКРАЇНИ

- ◆ «Про Службу безпеки України»
- ◆ «Про контррозвідувальну діяльність»
- ◆ «Про оперативно-розшукову діяльність»
- ◆ «Про національну безпеку України»
- ◆ «Про боротьбу з тероризмом»
- ◆ «Про критичну інфраструктуру»
- ◆ «Про розвідку»
- ◆ «Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України»
- ◆ «Про основні засади забезпечення кібербезпеки України»
- ◆ «Про державну таємницю»
- ◆ «Про інформацію»
- ◆ «Про доступ до публічної інформації»
- ◆ «Про звернення громадян»
- ◆ «Про захист персональних даних»
- ◆ «Про захист інформації в інформаційно-комунікаційних системах»
- ◆ «Про засади внутрішньої і зовнішньої політики»
- ◆ «Про запобігання корупції»
- ◆ «Про санкції»
- ◆ «Про електронні комунікації»
- ◆ «Про судову експертизу»
- ◆ «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»
- ◆ «Про загальну структуру і чисельність Служби безпеки України»
- ◆ «Про соціальний і правовий захист військовослужбовців та членів їх сімей»
- ◆ «Про державний захист працівників суду і правоохоронних органів»
- ◆ «Про організаційно-правові основи боротьби з організованою злочинністю»
- ◆ «Про військовий обов'язок і військову службу»
- ◆ «Про державну службу»
- ◆ «Про Державну програму авіаційної безпеки цивільної авіації»

НАЦІОНАЛЬНІ СТРАТЕГІЇ / КОНЦЕПЦІЇ

- ◆ Концепція боротьби з тероризмом в Україні (Указ Президента України від 05.03.2019 № 53)
- ◆ Стратегія національної безпеки України (Указ Президента України від 14.09.2020 № 392)
- ◆ Стратегія боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р)
- ◆ Стратегія кібербезпеки України (Указ Президента України від 26.08.2021 № 447)
- ◆ Стратегічний оборонний бюлетень України (Указ Президента України від 17.09.2021 № 473)
- ◆ Концепція забезпечення національної системи стійкості (Указ Президента України від 27.09.2021 № 479)
- ◆ Стратегія інформаційної безпеки (Указ Президента України від 28.12.2021 № 685)
- ◆ Стратегія забезпечення державної безпеки (Указ Президента України від 16.02.2022 № 56)
- ◆ Стратегія комунікації з питань європейської інтеграції України на період до 2026 року (розпорядження Кабінету Міністрів України від 09.12.2022 № 1155-р)
- ◆ Стратегія комунікацій у сфері запобігання та протидії корупції на період до 2025 року (розпорядження Кабінету Міністрів України від 22.12.2023 № 1203-р)
- ◆ Стратегія морської безпеки України (Указ Президента України від 17.07.2024 № 468)
- ◆ Стратегія формування системи повернення з військової служби до цивільного життя на період до 2033 року (розпорядження Кабінету Міністрів України від 31.12.2024 № 1350-р)

УГОДИ ПРО СПІВРОБІТНИЦТВО У СФЕРІ БЕЗПЕКИ ТА ДОВГОСТРОКОВУ ПІДТРИМКУ МІЖ УКРАЇНОЮ, ІНОЗЕМНИМИ ДЕРЖАВАМИ ТА МІЖНАРОДНИМИ ОРГАНІЗАЦІЯМИ

ПРОГРАМНІ ДОКУМЕНТИ УКРАЇНА – ЄС

- ◆ Дорожня карта за сферою «Верховенство права і безпека»
- ◆ Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки (Указ Президента України від 11.05.2023 № 273)
- ◆ План заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки (розпорядження Кабінету Міністрів України від 23.08.2024 № 792-р)

ПРОГРАМНІ ДОКУМЕНТИ УКРАЇНА – НАТО

- ◆ Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору (09.07.1997, Мадрид)
- ◆ Адаптована Річна національна програма співробітництва Україна – НАТО на 2024 р.
- ◆ Стратегічна концепція НАТО – 2022 (ухвалена главами держав і урядів на Мадридському саміті НАТО 29 червня 2022 року)
- ◆ Дорожня карта взаємосумісності Україна–НАТО
- ◆ Вимоги взаємосумісності з НАТО

ЕЛЕКТРОННА ВЕРСІЯ СТРАТЕГІЇ
УКРАЇНСЬКОЮ МОВОЮ:



E-VERSION OF THE STRATEGY
IN ENGLISH:



СЛУЖБА БЕЗПЕКИ УКРАЇНИ