Указ
Президента України

Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року "Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України"

Відповідно до статті 107 Конституції України постановляю:

1. Увести в дію рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року "Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України" (додається).

2. Затвердити Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України (додається).

3. Кабінету Міністрів України забезпечити реалізацію Концепції реформування Державної служби спеціального зв'язку та захисту інформації України.

4. Цей Указ набирає чинності з дня його опублікування.

Президент України В.ЗЕЛЕНСЬКИЙ
м. Київ
22 жовтня 2021 року
№ 544/2021

ЗАТВЕРДЖЕНО
Указом Президента України
від 22 жовтня 2021 року № 544/2021

КОНЦЕПЦІЯ
реформування Державної служби спеціального зв'язку та захисту інформації України

Загальні положення

До напрямів реалізації пріоритетів національних інтересів України та забезпечення національної безпеки, визначених Стратегією національної безпеки України, затвердженою Указом Президента України від 14 вересня 2020 року № 392, віднесено посилення спроможностей суб'єктів сектору безпеки і оборони та національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі.

Стан безпекового середовища навколо та всередині України на сьогодні характеризується такими основними чинниками:

стрімкі технологічні зміни, насамперед в інформаційних, енергетичних і біотехнологіях, розробки у сфері штучного інтелекту тощо, трансформують економіку і суспільство в цілому. Помітно зросла частка послуг інформаційних технологій, що надаються дистанційно. Наслідки таких трансформацій важко спрогнозувати;

зростає запит на нові ефективні інструменти глобального управління. Трансформується роль міждержавних та міжнародних структур, змінюється модель глобалізації з помітним посиленням тенденцій до регіоналізму. Сучасна система міжнародної безпеки перебуває у кризі, профіль нової на сьогодні не окреслено;

Російська Федерація системно застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби проти України, порушуючи її незалежність, державний суверенітет і територіальну цілісність;

нарощуються угруповання військ Російської Федерації поблизу державного кордону України. Діяльність окупаційної адміністрації Російської Федерації в окремих районах Донецької та Луганської областей, в Автономній Республіці Крим та місті Севастополі грубо порушує права і свободи людини і громадянина, становить загрозу економічній та екологічній безпеці України;

темпи переозброєння сил оборони України на новітні (модернізовані) зразки озброєння не забезпечують потреби у заміні основних видів озброєння та військової техніки радянського виробництва. Стан економіки ускладнює виділення коштів для виробництва та закупівлі у необхідних обсягах сучасних зразків озброєння та військової техніки, що поглиблює дисбаланс воєнних потенціалів України та Російської Федерації;

посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, несанкціонованим втручанням у її функціонування, зокрема фізичним і кіберхарактеру.

За таких умов посилення спроможностей суб'єктів сектору безпеки і оборони та національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі насамперед вимагає посилення інституційної спроможності Державної служби спеціального зв'язку та захисту інформації України.

Актуальність реформування Державної служби спеціального зв'язку та захисту інформації України зумовлена необхідністю:

підвищення ефективності виконання покладених на неї завдань;

приведення інформаційно-телекомунікаційної інфраструктури системи управління державою у відповідність із сучасним рівнем інформаційно-комунікаційних технологій;

запровадження сучасних захищених послуг з обміну і обробки інформації з обмеженим доступом та сучасних ризик-орієнтованих підходів до захисту інформації;

вирішення питань соціального забезпечення особового складу Державної служби спеціального зв'язку та захисту інформації України;

посилення демократичного цивільного контролю за діяльністю Державної служби спеціального зв'язку та захисту інформації України.

В результаті реформування місія Державної служби спеціального зв'язку та захисту інформації України має полягати у забезпеченні сталого функціонування та розвитку інформаційно-телекомунікаційної інфраструктури системи управління державою, що діє в умовах мирного часу, кризових ситуацій, що загрожують національній безпеці, особливого періоду.

Концепція реформування Державної служби спеціального зв'язку та захисту інформації України (далі - Концепція) визначає мету, завдання, етапи, основні пріоритети, напрями, механізми, а також очікувані результати реформування Державної служби спеціального зв'язку та захисту інформації України, які повинні дати їй змогу окремо та у взаємодії з іншими складовими сектору безпеки і оборони ефективно протидіяти загрозам національній безпеці.

Концепція базується на положеннях Конституції України, законів України "Про національну безпеку України" та "Про Державну службу спеціального зв'язку та захисту інформації України", Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, та інших актів законодавства України з питань національної безпеки і оборони.

Мета та завдання Концепції

Метою Концепції є реформування та розвиток Державної служби спеціального зв'язку та захисту інформації України як суб'єкта сектору безпеки і оборони із запровадженням уніфікованої системи планування та управління ресурсами на основі сучасних європейських та євроатлантичних підходів, що дасть змогу підвищити інституційну спроможність, а також оптимізувати організаційну структуру Державної служби спеціального зв'язку та захисту інформації України.

Основним завданням Концепції є підвищення інституційної спроможності Державної служби спеціального зв'язку та захисту інформації України та подальший її розвиток як складової національної системи кібербезпеки держави та суб'єкта сектору безпеки і оборони з урахуванням:

поточного стану та тенденцій розвитку безпекової ситуації навколо України;

стратегічних та концептуальних документів з питань розвитку сектору безпеки і оборони;

міжнародних стандартів у сфері спеціального зв'язку та захисту інформації.

Етапи реалізації Концепції

Реалізація Концепції розрахована на період до 2025 року та складається з двох етапів.

Перший етап (січень 2022 року - грудень 2023 року) передбачає:

удосконалення з урахуванням міжнародних стандартів та кращих світових практик законодавства України з питань організації та діяльності Державної служби спеціального зв'язку та захисту інформації України, зокрема, у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

розроблення пропозицій щодо скорочення кількості відомчих телекомунікаційних мереж спеціального зв'язку поза межами сектору безпеки і оборони з урахуванням нарощування можливостей єдиної захищеної мультисервісної платформи Національної телекомунікаційної мережі;

удосконалення законодавства України в частині порядку функціонування державної системи урядового зв'язку, процедур внесення клопотань та вирішення питань забезпечення урядовим зв'язком посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ та організацій;

реалізацію заходів зі становлення та розвитку Державної служби спеціального зв'язку та захисту інформації України як Безпекового акредитаційного органу, що здійснює організацію акредитації з питань безпеки усіх національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом;

подальший розвиток систем спеціального зв'язку, зокрема в інтересах мережі ситуаційних центрів державних органів, розгортання радіосегмента транспортної платформи Національної телекомунікаційної мережі;

реформування та розвиток систем криптографічного і технічного захисту інформації, протидії технічним розвідкам, проведення оцінки ефективності запроваджених новацій;

започаткування широкого спектра наукових досліджень у сфері кібербезпеки та розробки прикладних систем і засобів кіберзахисту;

збереження та розвиток кадрового потенціалу з урахуванням змін завдань і функцій Державної служби спеціального зв'язку та захисту інформації України, його адаптація відповідно до сучасних умов служби, збереження інституційної пам'яті.

Результатом першого етапу має стати актуалізація законодавства України з питань організації та діяльності Державної служби спеціального зв'язку та захисту інформації України, реалізація пріоритетних проектів у сфері спеціального зв'язку та початок оптимізації організаційної структури Державної служби спеціального зв'язку та захисту інформації України.

Другий етап (січень 2024 року - грудень 2025 року) передбачає:

модернізацію державної системи урядового зв'язку шляхом інтеграції її мереж в єдину захищену мультисервісну платформу Національної телекомунікаційної мережі та перехід до надання споживачам широкого спектра сучасних сервісів;

переоснащення підрозділів урядового польового зв'язку сучасними цифровими засобами спеціального зв'язку;

оптимізацію організаційних структур органів та підрозділів Державної служби спеціального зв'язку та захисту інформації України з урахуванням визначених функцій та спроможностей;

модернізацію системи вузлів зв'язку спеціального призначення позаміських пунктів управління державних органів;

завершення розгортання системи оперативно-технічного управління телекомунікаційними мережами в умовах мирного часу, кризових ситуацій, що загрожують національній безпеці, особливого періоду;

забезпечення реалізації новацій законодавства у сфері захисту інформації;

проведення акредитації з питань безпеки національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом;

впровадження системи технічного регулювання у сфері протидії технічним розвідкам та удосконалення державного контролю за станом протидії технічним розвідкам;

удосконалення системи підготовки фахівців у сфері захисту інформації;

нарощування потужностей з виробництва ключових документів до засобів криптографічного захисту інформації для гарантованого забезпечення потреб державних органів;

впровадження заходів та розроблення засобів кіберзахисту на основі результатів наукових досліджень у сфері кібербезпеки;

впровадження програм короткострокової підготовки (тренування) у сфері кіберзахисту (кібербезпеки) для працівників суб'єктів забезпечення кібербезпеки держави.

За результатами другого етапу має бути модернізовано державну систему урядового зв'язку та впроваджено ключові новації у сфері захисту інформації, завершено оптимізацію організаційних структур органів та підрозділів Державної служби спеціального зв'язку та захисту інформації України.

Основні пріоритети та напрями реформування Державної служби спеціального зв'язку та захисту інформації України

Реформування Державної служби спеціального зв'язку та захисту інформації України передбачається здійснити за такими пріоритетами та напрямами:

1) удосконалення організаційно-правових засад функціонування Державної служби спеціального зв'язку та захисту інформації України, що передбачає:

адаптацію законодавства України до вимог законодавства ЄС у сфері захисту інформації;

перегляд покладених на Державну службу спеціального зв'язку та захисту інформації України завдань та обов'язків;

оптимізацію організаційної структури Державної служби спеціального зв'язку та захисту інформації України;

удосконалення процедури внесення клопотань та вирішення питань забезпечення урядовим зв'язком посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ та організацій;

удосконалення системи контролю за діяльністю Державної служби спеціального зв'язку та захисту інформації України з дотриманням засад демократичного цивільного контролю та порядку, визначеного Конституцією України, законами України "Про Державну службу спеціального зв'язку та захисту інформації України", "Про національну безпеку України", "Про Кабінет Міністрів України" та іншими актами законодавства;

2) розвиток спеціального зв'язку як складової інформаційно-телекомунікаційної інфраструктури в системі управління державою в умовах мирного часу, кризових ситуацій, що загрожують національній безпеці, особливого періоду, що передбачає:

розвиток спеціального зв'язку в інтересах системи державного управління;

розширення функціональних можливостей Національної телекомунікаційної мережі;

подальшу модернізацію державної системи урядового зв'язку, яка буде здійснюватися з урахуванням можливостей Національної телекомунікаційної мережі та передбачатиме впровадження нових комплексів спеціального зв'язку, насамперед сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку;

розвиток спроможностей системи урядового фельд'єгерського зв'язку, спрямований на підвищення надійності та оперативності доставки кореспонденції, що містить відомості, які становлять державну таємницю, та/або службову інформацію, офіційної кореспонденції та дипломатичної пошти Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління, закордонних дипломатичних установ України, зокрема шляхом впровадження автоматизованої системи контролю за її проходженням;

розвиток Національної системи конфіденційного зв'язку, який спрямовуватиметься на впровадження механізмів для функціонування ринку конфіденційних послуг; створення захищених точок взаємоз'єднання спеціальних інформаційно-телекомунікаційних систем для забезпечення захищеного міжвідомчого обміну державними електронними інформаційними ресурсами; модернізацію систем для надання сучасних захищених телекомунікаційних послуг IP-телефонії, електронної пошти, Інтернет-доступу, мобільного зв'язку, розгортання та функціонування захищених центрів обробки даних;

3) удосконалення підходів до захисту інформації з урахуванням сучасних ризик-орієнтованих підходів, що передбачає:

перехід від регулювання створення комплексних систем захисту інформації для електронних публічних сервісів (зокрема реєстрів) до систем управління безпекою інформації та оцінки їх відповідності за міжнародними стандартами, NIS-директивами, безпековими питаннями регламенту eIDAS щодо електронної ідентифікації;

розширення моделі застосування ризик-орієнтованих механізмів захисту інформації та систем управління безпекою інформації;

перехід від ліцензування до залучення для виконання робіт зі створення та оцінки відповідності систем управління безпекою інформації спеціалізованих підприємств, створення відповідного реєстру виконавців таких робіт;

реалізацію заходів зі становлення та розвитку Державної служби спеціального зв'язку та захисту інформації України як Безпекового акредитаційного органу, що здійснює організацію акредитації з питань безпеки усіх національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом, забезпечення проведення акредитації з питань безпеки таких систем;

продовження розроблення та впровадження криптографічних стандартів, що забезпечить необхідний рівень захисту інформації у перехідний від традиційного до квантового та у постквантовий періоди;

вдосконалення законодавства з питань криптографічного та технічного захисту інформації з обмеженим доступом в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, завершення впровадження (розширення номенклатури) технічних рішень, засобів захисту інформації вітчизняного виробництва;

набуття системою урядового польового зв'язку спроможності щодо інтероперабельності, шляхом завершення переоснащення територіальних підрозділів сучасними комплексами спеціального зв'язку, сумісними з наявними системами спеціального зв'язку Збройних Сил України;

розвиток міжнародного співробітництва та імплементацію кращих світових практик та стандартів;

впровадження механізмів державно-приватного партнерства у сфері оцінки відповідності, обговорення та визнання схем сертифікації з безпеки продукції, процесів та систем приватного та публічного застосування;

започаткування співробітництва з Агентством ЄС з питань мережевої та інформаційної безпеки (ENISA);

запровадження альтернативних механізмів моніторингу стану безпеки інформації;

4) формування та реалізація державної політики у сфері кіберзахисту, що передбачає:

створення та розвиток спроможностей щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахист об'єктів критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

удосконалення та розвиток організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки;

впровадження системи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

стимулювання розвитку мережі команд реагування на комп'ютерні надзвичайні події CERT (CSIRT);

розвиток функціональних спроможностей Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України на принципах фаховості, відповідальності, довіри та демілітаризації;

створення механізму державно-приватного партнерства та ефективної системи взаємодії зацікавлених сторін для вирішення питань кіберзахисту;

оновлення технологічної бази кіберполігону (тренінгової кіберплатформи) та проведення кібернавчань в інтересах суб'єктів забезпечення кібербезпеки державного сектору та критичної інфраструктури;

розвиток міжнародного співробітництва та підтримка міжнародних ініціатив у сфері кібербезпеки, поглиблення співпраці з ЄС та НАТО;

розвиток стратегічних комунікацій для підвищення рівня обізнаності суб'єктів забезпечення кібербезпеки з питань кіберзахисту;

5) подальший розвиток системи протидії технічним розвідкам, спрямований на захист національних інтересів у сферах безпеки і оборони, зниження вірогідності негативного впливу противника на систему управління державою, важливі об'єкти критичної інфраструктури, зменшення втрат особового складу, озброєння та військової техніки, що передбачає:

удосконалення нормативно-правової бази у сфері протидії технічним розвідкам та супроводження моделі технічних розвідок (ТР-2030);

впровадження системи технічного регулювання у сфері протидії технічним розвідкам;

покращення підготовки фахівців за напрямом протидії технічним розвідкам;

удосконалення державного контролю за станом протидії технічним розвідкам в інтересах сектору безпеки і оборони;

6) оптимізація структури та модернізація матеріально-технічної бази Державної служби спеціального зв'язку та захисту інформації України;

7) удосконалення системи підготовки фахівців, що передбачає:

удосконалення матеріально-технічного та інформаційно-програмного забезпечення профільного закладу освіти Державної служби спеціального зв'язку та захисту інформації України відповідно до новітніх зразків засобів спеціального зв'язку та захисту інформації;

підвищення кваліфікації науково-педагогічного складу профільного закладу освіти Державної служби спеціального зв'язку та захисту інформації України шляхом співпраці із закордонними освітніми і науковими закладами, участі у міжнародних навчаннях та стажуванні;

розробку та впровадження інноваційних технологій навчання на основі кращих світових практик та стандартів, оновлення методичного забезпечення навчального процесу, посилення практичної складової освітніх програм;

підготовку фахівців у сфері спеціального зв'язку та захисту інформації для складових сектору безпеки і оборони;

створення умов для перепідготовки кадрів та підвищення їх кваліфікації за системою "навчання протягом життя";

запровадження національної програми з підвищення цифрової грамотності та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації проектів з підвищення рівня обізнаності щодо кіберзагроз та кіберзахисту;

8) покращення соціального захисту особового складу Державної служби спеціального зв'язку та захисту інформації України та його мотивації до служби, а також посилення демократичного цивільного контролю, що передбачає:

поліпшення умов грошового забезпечення (оплати праці) особового складу, зокрема, шляхом подолання диспропорції в грошовому забезпеченні (оплаті праці) порівняно з іншими складовими сектору безпеки і оборони,

встановлення розмірів грошового забезпечення (оплати праці) на рівні, який забезпечуватиме достатні матеріальні умови для належного виконання особовим складом службових обов'язків з урахуванням специфіки, інтенсивності та особливого характеру роботи, а також стимулюватиме досягнення високих результатів у службовій діяльності, компенсуватиме фізичні та інтелектуальні затрати особового складу;

покращення стану забезпечення особового складу житлом;

здійснення на принципах верховенства права, законності, підзвітності, прозорості, ефективності та результативності демократичного цивільного контролю за діяльністю Державної служби спеціального зв'язку та захисту інформації України.

Механізми реалізації Концепції

Реалізація Концепції здійснюватиметься шляхом розроблення та виконання відповідних планів заходів з реалізації положень Концепції, що затверджуються Кабінетом Міністрів України. Плани заходів з реалізації положень Концепції мають містити визначені цілі, нормативно-правові й організаційно-управлінські способи їх досягнення, заходи моніторингу та оцінки ефективності реалізації Концепції.

Очікувані результати

Реалізація Концепції дасть змогу:

забезпечити надання надійного, безпечного та своєчасного спеціального зв'язку у мирний час, в умовах надзвичайного стану і в особливий період;

посилити демократичний цивільний контроль за діяльністю Державної служби спеціального зв'язку та захисту інформації України та підвищити рівень довіри суспільства до її діяльності;

розширити функціональні можливості Національної телекомунікаційної мережі, що дасть можливість забезпечити інтеграцію наявних систем спеціального зв'язку та уніфікацію захищених електронних комунікацій різних державних органів у загальному безпековому контурі з використанням сучасних цифрових технологій;

розширити напрями співробітництва з Організацією Північноатлантичного договору з метою набуття повноправного членства України в НАТО;

забезпечити виконання національних зобов'язань щодо акредитації з питань безпеки національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом;

впровадити механізми державно-приватного партнерства у сфері кібербезпеки;

розгорнути систему кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури;

захистити національні інтереси у сфері безпеки та оборони, знизити ймовірність негативного впливу зовнішніх та внутрішніх чинників на телекомунікаційну складову системи управління державою, забезпечити кіберзахист державних інформаційних ресурсів та об'єктів критичної інфраструктури, зменшити втрати особового складу, озброєння та військової техніки;

реформувати організаційну структуру Державної служби спеціального зв'язку та захисту інформації України, дерегулювати та спростити окремі процедури;

підвищити ефективність виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань;

забезпечити на належному рівні підготовку фахівців із захисту інформації, кіберзахисту (кібербезпеки);

організовувати та проводити курси (тренування) короткострокової підготовки у сфері кіберзахисту (кібербезпеки) для працівників суб'єктів забезпечення кібербезпеки держави;

гарантувати належне матеріальне забезпечення особового складу Державної служби спеціального зв'язку та захисту інформації України;

підвищити надійність, оперативність доставки кореспонденції, що містить відомості, які становлять державну таємницю, та/або службову інформацію, офіційної кореспонденції та дипломатичної пошти Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління, закордонних дипломатичних установ України;

підвищити престиж служби (роботи) в Державній службі спеціального зв'язку та захисту інформації України.

Фінансове забезпечення

Фінансування заходів з реалізації Концепції здійснюватиметься за рахунок і в межах видатків, визначених для Адміністрації Державної служби спеціального зв'язку та захисту інформації України в законі про Державний

бюджет України на відповідний рік, а також інших джерел, не заборонених законодавством.

Керівник Офісу
Президента України А.ЄРМАК