Лекція 2_9. ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ.

1.Призначення, функції та завдання видів Державної служби спеціального зв'язку та захисту інформації

2. Структура Державної служби спеціального зв'язку та захисту інформації та напрями розвитку.

Література.

1. Закон України «Про національну безпеку України»
2. Закон України «Про інформацію». ВВР України, 1992, № 48, ст.650.
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» ВВР України, 2006, № 30, ст.258.
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року зі змінами від 17 вересня 2020 року.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» зі змінами від 04 червня 2020 року
6. Закон України «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 року зі змінами від 27 березня 2014 року
7. Закон України «Про радіочастотний ресурс України» від 1 червня 2000 року зі змінами від 14 січня 2020 року
8. Закон України «Про телекомунікації» від 18 листопада 2003 року зі змінами від 17 вересня 2020 року
9. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 рок
10. Указ Президента України Про Стратегію кібербезпеки України м. Київ 26 серпня 2021 року № 447/2021
11. Указ Президента України Про рішення РНБО України від 22 жовтня 2021 року "Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України від 22 жовтня 2021 року № 544/2021.
12. Постанова Кабінету Міністрів України від 24 червня 2006 р. № 868 «Положення Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації»
13. Указ Президента України від 14.09.2020 "Про Стратегію національної безпеки України".
14. Указ Президента України від 21.03.2021 № 121/2021 "Про Стратегію воєнної безпеки України".

АКТУАЛЬНІСТЬ

Інформаційна політика держави є важливою складовою зовнішньої й внутрішньої політики держави та включає усі сфери життя суспільства. Стрімкий розвиток інформаційної сфери викликає появу принципово нових загроз інтересам особи, суспільства, держави та її національній безпеці.

Гостроти проблеми додає той факт, що інформаційна складова є стійким об’єктом маніпуляції в умовах гібридної війни. Так як складна політична ситуація, в якій Україна знаходиться останніми роками, безупинне погіршення репутації держави на міжнародній арені спричинені рядом факторів, серед яких істотним фактором є неналежний стан системи забезпечення інформаційної безпеки. В Україні існує об'єктивна потреба в державно-правовому регулюванні науково-технічної та інформаційної діяльності, яке б відповідало реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищало власні національні інтереси України.

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.

1.ПРИЗНАЧЕННЯ, ФУНКЦІЇ ТА ЗАВДАННЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Призначення Держспецзв’язку

Відповідно до Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» (далі – закон) Державна служба спеціального зв’язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.

Офіційна скорочена назва – Держспецзв’язку

Функції Держспецзв’язку

Захист інформації

Кіберзахист

Держспецзв'язку — один з основних суб'єктів кібербезпеки України, відповідальний за кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, за координацію діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту.

Кіберреформа UA30 в Україні

Кіберреформа UA30 в Україні — заходи з реформування галузі кібербезпеки України, які розпочала Державна служба спеціального зв'язку та захисту інформації України під керівництвом голови Держспецзв'язку Юрія Щиголя за ініціативи Президента України Володимира Зеленського у 2021 році. Мета UA30 — до 2030 року Україна має стати одним зі світових лідерів у сфері кібербезпеки, підтвердити визнанням на міжнародному рівні.

Кіберцентр UA30 — це флагман кіберреформи UA30. Основне завдання Кіберцентру UA30 — забезпечувати кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

До Кіберцентру UA30 входять:

- Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA — це єдина акредитована у FIRST команда з України. CERT-UA має можливість обмінюватись даними з понад 500 командами реагування з 90 країн світу.
- Тренінговий центр — це унікальний майданчик для відпрацювання реальних сценаріїв кібератак у навчальному середовищі та вироблення практичних умінь і навичок, необхідних для практичного реагування на кіберзагрози в сучасних реаліях.

Регіональні центри кіберзахисту

Одне із завдань Держспецзв'язку в галузі кіберзахисту — створення регіональних центрів кіберзахисту.

Національний центр резервування державних інформаційних ресурсів

8 лютого 2021 року КМУ ухвалив постанову «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів».

До НЦ увійдуть єдині основний і резервний захищені центри оброблення даних (дата-центри), призначені для обробки і зберігання державних електронних інформаційних ресурсів.

Створенням компонентів НЦ займається Держспецзв'язку та підприємства, які належать до її сфери управління. Адміністратором безпеки є Державний центр кіберзахисту. Технічним адміністратором — ДП «Українські спеціальні системи». Його зона відповідальності — проєктування, закупівля обладнання і розміщення, придбання програмного забезпечення тощо.

Концерн КРРТ і ДП «Укрспецзв'язок» надаватимуть транспортні мережі, забезпечуватимуть центр резервування електрикою, займатимуться будівництвом, адмініструванням інфраструктури.

Платформа сервісів кіберзахисту

Платформа сервісів кіберзахисту — це один із компонентів Національного центру резервування державних інформаційних ресурсів. Платформа також буде доступною для державних органів як окрема послуга. Завдяки цій платформі органи державної влади отримують захист власних інформаційних ресурсів за найвищими галузевими стандартами.

Платформа для створення і розміщення державних реєстрів

Це уніфікований інструмент для побудови інформаційних систем і реєстрів. Розпорядником платформи є ДП «УСС», що належить до сфери управління Держспецзв'язку.

Модернізація системи захищеного доступу до мережі «Інтернет» для державного сектору

Державний центр кіберзахисту Держспецзв'язку відповідає за розроблення та функціонування системи захищеного доступу до мережі «Інтернет» для державних органів. У 2021 році розпочалась робота над модернізацією системи для 82 ЦОВВ.

Організаційно-технічна модель кіберзахисту (ОТМ)

Держспецзв'язку розробила і впроваджує організаційно-технічну модель кіберзахисту.

Організаційно-технічна модель кіберзахисту — це фундамент для побудови національної системи кібербезпеки. Вона описує правила взаємодії між суб'єктами національної системи кібербезпеки на організаційному, технологічному і базисному рівнях. ОТМ складається з трьох вертикально та горизонтально інтегрованих інфраструктур:

1. Організаційно-керівна інфраструктура

2. Технологічна інфраструктура, яка має три горизонти — національний, галузевий (регіональний) та об'єктовий.

3. Базова інфраструктура, яка складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни)

29 грудня 2021 року Кабінет Міністрів України ухвалив Положення про організаційно-технічну модель кіберзахисту.

Технічний та криптографічний захист інформації

Держспецзв'язку розробляє стандарти криптографічного та технічного захисту, а також визначає, які стандарти захисту інформації визнаються в Україні для різних видів систем.

Держспецзв'язку є повноважним органом ліцензування у сфері криптографічного та технічного захисту інформації, має повноваження проводити планові та позапланові перевірки стану і дотримання ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту державних інформаційних ресурсів та інформації.

У 2020 році Держспецзв'язку ініціювала внесення змін у Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Зокрема, організації дістали можливість будувати захист не тільки за стандартами КСЗІ, а й за міжнародним стандартом ISO 27000, якщо компанія не працює зі службовою інформацією або інформацією, що становить державну таємницю.

У 2021 році Держспецзв'язку розробила, а Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони України ухвалив «Перелік категорій кіберінцидентів» і «Загальні правила обміну інформацією про кіберінциденти. Протокол TLP». Документи слугуватимуть основою для обміну інформацією про кіберінциденти між суб'єктами національної системи кібербезпеки.

«Перелік категорій кіберінцидентів» упроваджує єдину термінологію для обміну інформацією про кіберінциденти, передання звітів до НКЦК, у тому числі за допомогою автоматизованих платформ для обміну інформацією про кіберзагрози.

«Загальні правила обміну інформацією про кіберінциденти. Протокол TLP» визначають спосіб класифікації повідомлень про кіберінциденти з урахуванням того, як і кому може бути надана така інформація. Також протокол може бути застосований для передання індикаторів компрометації урядовій команді

реагування на комп'ютерні надзвичайні події України CERT-UA з метою інформування інших організацій про потенційні загрози.

У 2021 році Держспецзв'язку працює над розробленням пакету документів, що містять вимоги захисту інформації та приватності, розроблені згідно зі стандартами NIST, а також провідними європейськими стандартами. Імплементація цих стандартів має розпочатись у 2022 році.

Захист критичної інформаційної інфраструктури

19 червня 2019 року Кабінетом Міністрів було визначено Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»), реалізація яких покладена на власників таких об'єктів. Наразі застосування таких вимог не тільки на об'єктах критичної інфраструктури дозволяє суттєво підвищити рівень кіберзахисту країни.

9 жовтня 2020 року Кабінет Міністрів України ухвалив Постанови «Деякі питання об'єктів критичної інфраструктури» та «Деякі питання об'єктів критичної інформаційної інфраструктури», які були розроблені фахівцями Служби. Ці Постанови встановлюють:

- Порядок віднесення об'єктів до об'єктів критичної інфраструктури;
- Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;
- Методику категоризації об'єктів критичної інфраструктури;
- Порядок формування переліку об'єктів критичної інформаційної інфраструктури;
- Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

До кінця 2021 року ОКІ мають завершити процес віднесення себе до певного рівня критичності. Наступним кроком Держспецзв'язку запустить процес створення переліку ОКІІ, потім — аудиту інформаційної безпеки ОКІ — та контролюватиме посилення їх кіберзахисту.

У жовтні 2021 року Держспецзв'язку затвердила Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Цей документ базується на підходах Національного інституту стандартів і технологій США та об'єднує найкращі світові практики та чинну нормативну базу, за допомогою яких оператори ОКІІ мають будувати кіберзахист систем.

Документ регулярно переглядатимуть, адже ОКІІ мають бути здатними протистояти ризикам кібербезпеки, які постійно змінюються. Рекомендації можуть бути застосовані на всіх етапах створення комплексної системи захисту

інформації (КСЗІ), системи інформаційної безпеки (на підставі Постанови Кабінету Міністрів України№ 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»), створення системи управління інформаційною безпекою (СУІБ, відповідно до вимог ДСТУ ISO/IEC 27 001) або інших систем захисту інформації, побудованих міжнародними та національними стандартами.

Державний контроль

Держспецзв'язку здійснює державний контроль за станом:

- технічного захисту інформації;
- криптографічного захисту інформації;
- протидії технічним розвідкам;
- захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;
- кіберзахисту об'єктів критичної інфраструктури;
- дотриманням вимог законодавства у сфері електронних довірчих послуг.

Водночас Держспецзв'язку проводить державний інструментальний контроль захищеності інформації, яка циркулює на об'єктах «особливої норми» та в кабінетах абонентів урядового зв'язку.

Крім того, Держспецзв'язку впроваджує постійний державний контроль на об'єктах критичної інфраструктури та державний інструментальний контроль програмного забезпечення на наявність недокументованих функцій.

Аудит інформаційної безпеки

Держспецзв'язку забезпечує впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, їх атестації та переатестації. Також Держспецзв'язку координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість.

Протидія технічним розвідкам

Держспецзв'язку забезпечує нормативно-правове та технічне регулювання, методичне керівництво та координацію органів державного сектору, погоджує проєкти нормативно-правових документів тощо в галузі протидії технічним розвідкам.

Крім того, Держспецзв'язку погоджує і контролює виконання технічних завдань на проєктування, будівництво і реконструкцію особливо важливих об'єктів і на зразках військової та спеціальної техніки в частині протидії технічним розвідкам.

Спеціальний зв'язок

Урядовий зв'язок

Держспецзв'язку забезпечує функціонування та розвиток державної системи урядового зв'язку для Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб державних органів, органів місцевого самоврядування для зв'язку із закордонними дипломатичними установами України, а також для зв'язку із закордонними дипломатичними установами України. Держспецзв'язку здійснює контроль за виконанням вимог законодавства у сфері захисту інформації в приміщеннях абонентів урядового зв'язку.

У 2020 році Держспецзв'язку розпочала модернізацію урядового зв'язку. У рамках реформи Служби, Держспецзв'язку й надалі забезпечуватиме надання надійного, безпечного та своєчасного спеціального зв'язку у мирний час, в умовах надзвичайного стану і в особливий період. А також розширити функціональні можливості Національної телекомунікаційної мережі (НТМ), 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.

Фельд'єгерський зв'язок

Головне управління та підрозділи урядового фельд'єгерського зв'язку Держспецзв'язку призначені для організації і забезпечення урядовим фельд'єгерським зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління та інших юридичних осіб відповідно до законодавства. Забезпечення урядовим фельд'єгерським зв'язком передбачає доставку кореспонденції різного грифу секретності в межах України, а також дипломатичної пошти до інших держав.

Очолює систему урядового фельд'єгерського зв'язку — Головне управління урядового фельд'єгерського зв'язку Держспецзв'язку, яке координує діяльність підрозділів урядового фельд'єгерського зв'язку Держспецзв'язку в обласних центрах.

У рамках реформування Держспецзв'язку буде запущено прототип системи автоматизації контролю за проходженням кореспонденції. Планується, що вже у наступному, 2022 році ця система працюватиме повноцінно.

Урядовий фельд'єгерський зв'язок підвищить надійність, оперативність доставки кореспонденції, яка містить відомості, що становлять державну таємницю, 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.

Спеціальний поштовий зв'язок

Держспецзв'язку здійснює формування та реалізацію державної політики в галузі поштового зв'язку спеціального призначення.

Зв'язок

Як регулятор в галузі зв'язку Держспецзв'язку:

- бере участь у формуванні та реалізації державної тарифної політики і політики державних закупівель у сферах телекомунікацій, користування радіочастотним ресурсом України;
- виконує функції Адміністрації зв'язку та радіочастот України;
- здійснює правовий захист інтересів України в міжнародних і регіональних організаціях з питань телекомунікацій і користування радіочастотним ресурсом;
- забезпечує розвиток у сферах телекомунікацій і користування радіочастотним ресурсом України;
- в межах своїх повноважень розробляє проєкти концепцій розвитку телекомунікацій України та інших проєктів концепцій у сфері користування радіочастотним ресурсом України, а також сприяє їх реалізації;
- забезпечує регулювання у сферах телекомунікацій, користування радіочастотним ресурсом України;
- погоджує проекти нормативно-правових актів з питань телекомунікацій і користування радіочастотним ресурсом України;
- розробляє технічні регламенти, норми, методики розрахунків електромагнітної сумісності радіоелектронних засобів і випромінювальних пристроїв та інші нормативно-правові акти;
- встановлює технічні вимоги до телекомунікаційних мереж, систем і комплексів спеціального зв'язку і загального користування, засобів та об'єктів телекомунікацій;
- визначає перелік технічних засобів, що можуть застосовуватися в телекомунікаційних мережах загального користування;
- встановлює норми, правила і порядки проведення випробувань у сфері користування радіочастотним ресурсом України тощо

Завдання Держспецзв’язку

Основними завданнями Державної служби спеціального зв’язку та захисту інформації України є:

1. формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – інформаційно-комунікаційні

системи) і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, активної протидії агресії у кіберпросторі;

2. участь у формуванні та реалізації державної політики у сферах електронного документообігу в інформаційно-комунікаційних системах, в яких обробляються службова інформація та державна таємниця (в частині захисту інформації державних органів та органів місцевого самоврядування), захисту критичної інформаційної інфраструктури;

3. забезпечення у встановленому порядку та в межах компетенції діяльності суб’єктів, які безпосередньо здійснюють боротьбу з тероризмом;

4. реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах;

5. визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об’єктів критичної інфраструктури, ведення переліку об’єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

6. здійснення контролю за дотриманням вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту критичної інформаційної інфраструктури;

7. створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі;

8. створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі;

виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту.

Принципи діяльності Державної служби спеціального зв’язку та захисту інформації України

1. Діяльність Державної служби спеціального зв’язку та захисту інформації України ґрунтується на принципах верховенства права, забезпечення дотримання прав і свобод людини і громадянина, безперервності, законності, забезпечення єдності державної політики, відкритості для демократичного цивільного контролю, прозорості, позапартійності.

2. Державна служба спеціального зв’язку та захисту інформації України діє за принципом єдиноначальності.

2. СТРУКТУРА ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ ТА НАПРЯМИ ПРЗВИТКУ.

Структура Держспецзв'язку

Керівним органом системи Держспецзв'язку є Адміністрація Держспецзв'язку, яка діє відповідно до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. До складу Адміністрації входять 17 департаментів та відділів, які виконують покладені на службу завдання.

До сфери управління Адміністрації Держспецзв'язку входять державні підприємства, установи та організації, діяльність яких пов'язана із забезпеченням виконанням завдань, покладених на Службу.

Адміністрація Держспецзв'язку

- Департаменти Адміністрації Держспецзв'язку
- Департамент захисту інформації Адміністрації Держспецзв'язку
- Департамент кіберзахисту Адміністрації Держспецзв'язку
- Департамент державного контролю у сфері захисту інформації Адміністрації Держспецзв'язку
- Департамент розвитку електронних комунікацій Адміністрації Держспецзв'язку
- Департамент європейської інтеграції та міжнародного співробітництва Адміністрації Держспецзв'язку
- Режимно-секретне управління Адміністрації Держспецзв'язку
- Відділ інформаційних комунікацій Адміністрації Держспецзв'язку
- Департамент планування застосування органів і підрозділів та спеціального зв'язку Адміністрації Держспецзв'язку
- Інші департаменти та відділи

Територіальні органи

- Головне управління урядового зв'язку

Забезпечує урядовим зв'язком вищих посадових осіб держави в місцях їх постійного та тимчасового перебування на території України та за її межами. Забезпечують функціонування мереж та комплексів державної системи урядового зв'язку.

- Управління Держспецзв'язку в областях

Забезпечує урядовим зв'язком державні органи в областях, реалізують державну політику у сферах криптографічного та технічного захисту інформації, впровадження сервісів кіберзахисту.

Територіальні підрозділи

Забезпечують урядовим зв'язком органи військового управління сил оборони та сектору безпеки на польових пунктах управління.

- 2 територіальний вузол урядового зв'язку
- 3 територіальний вузол урядового зв'язку
- 4 територіальний вузол урядового зв'язку
- 8 територіальний вузол урядового зв'язку
- 10 територіальний вузол урядового зв'язку

Заклади та установи, підприємства, що входять до сфери управління Держспецзв'язку

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації

Інститут[15] є виробничо-орієнтованою[*джерело?*] галузевою науковою установою, розташований у Києві. Результат діяльності ДержНДІ призначений для безпосереднього впровадження у виробництво та/або практичного використання у спеціальних інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності.

Галузі діяльності ДержНДІ:

1. розроблення, дослідження, виробництво і впровадження засобів криптографічного та технічного захисту інформації, а також телекомунікаційного обладнання для спеціальних інформаційно-телекомунікаційних систем;
2. створення засобів криптографічного захисту інформації та засобів спеціального зв'язку в частині забезпечення криптографічних, інженерно-криптографічних, спеціальних вимог;
3. сертифікаційне випробування засобів криптографічного та технічного захисту інформації, наукові експертизи проєктів у сфері захисту інформації, науково-технічні експертизи у сфері криптографічного та технічного захисту інформації;
4. інша діяльність, що не суперечить умовам акредитації випробувальної лабораторії ДержНДІ та умовам ліцензування в галузі криптографічного і технічного захисту інформації.

Інститут спеціального зв'язку та захисту інформації

Інститут[16] розташований у Києві і є закладом освіти Державної служби спеціального зв'язку та захисту інформації України та військовим навчальним підрозділом найбільшого технічного університету України дослідницького

типу — Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Підготовка фахівців у Інституті здійснюється за спеціальностями:

- 122 Комп'ютерні науки;
- 125 Кібербезпека;
- 172 Електронні комунікації та радіотехніка.

Національний центр оперативно-технічного управління мережами телекомунікацій

Державний центр кіберзахисту та протидії кіберзагрозам

Докладніше: Державний центр кіберзахисту

Основним завданням Центру є впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки шляхом:

- забезпечення функціонування та розвитку CERT-UA;
- запровадження комплексу організаційно-технічних заходів із виявлення вразливостей і недоліків у налаштуванні ІТС, в яких обробляють державні інформаційні ресурси;
- відповідно до постанови Кабінету Міністрів України № 94 «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів», забезпечення створення та функціонування складових НЦ у частині, що стосується виконання завдань адміністратора безпеки НЦ;
- забезпечення функціонування, експлуатації та розвитку Тренінгового кіберцентру в інтересах кібербезпеки держави.

ДЦКЗ Держспецзв'язку забезпечує функціонування системи захищеного доступу до мережі Інтернет. Також фахівці ДЦКЗ Держспецзв'язку розробляють платформу сервісів кіберзахисту, яка працюватиме[*коли?*] як послуга на базі Національного центру резервування державних інформаційних ресурсів, так і як окрема послуга для державних органів.

13 травня 2021 року Президент України Володимир Зеленський відкрив Кіберцентр UA30, який також входить до ДЦКЗ Держспецзв'язку.

Державне підприємство «Українські спеціальні системи» (ДП «УСС»)

Державне підприємство «Українські спеціальні системи» є оператором національної мережі конфіденційного зв'язку, спеціальної мережі стільникового зв'язку та захищеного вузла інтернет-доступу; а також надає послуги конфіденційного зв'язку, створення комплексних систем захисту інформації та проведення державної експертизи; електронні довірчі послуги та послуги

захисту інформаційних ресурсів органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій різних форм власності з використанням сучасних технологій.

Від 24 березня 2021 року ДП «УСС», відповідно до розпорядження Кабінету Міністрів України, визначено Централізованою закупівельною організацією у сфері цифровізації. ДП «УСС» було створено окрему філію «Централізована закупівельна організація».

Проведення закупівлі комп'ютерного обладнання та програмного забезпечення під одним дахом дасть можливість мати такі переваги:

- **Прозорість**: об'єднання закупівель допомагає покращити систему громадського контролю за використанням бюджетних коштів. А найголовніше: усі тендери ЦЗО проводить через електронну систему закупівель без жодних винятків.
- **Безпека**: ДП «УСС» перебуває у підпорядкуванні Держспецзв'язку, тому має доступ до найсвіжішої інформації щодо кіберзагроз і здатне перевірити наявність у комп'ютерного обладнання та програмного забезпечення належного рівня захищеності.
- **Ефективність**: ДП «УСС» має багаторічний досвід закупівель у галузі цифровізації, якого немає у більшості інших державних установ та організацій, а також має матеріально-технічну базу та висококваліфікований персонал, що забезпечує високу ефективність закупівель.

Концерн радіомовлення, радіозв'язку та телебачення (Концерн РРТ, КРРТ)

Докладніше: Концерн радіомовлення, радіозв'язку та телебачення

Концерн радіомовлення, радіозв'язку та телебачення — державний оператор телерадіомовлення, радіорелейного й супутникового зв'язку. Замовниками послуг Концерну РРТ є загальнонаціональні телевізійні мовники та радіокомпанії України, обласні, регіональні телерадіокомпанії, комерційні телерадіокомпанії, оператори телекомунікацій та підприємства зв'язку.

Концерн РРТ бере участь у розробленні та реалізації державної політики у сфері телерадіомовлення, аналізі стану телерадіомовлення в Україні, реалізації пропозицій щодо вдосконалення законодавства у цій сфері, забезпечення інформаційної безпеки України в сфері телекомунікацій тощо. Як державне підприємство Концерн РРТ віддає 80 % своїх доходів державі.

Найбільш вагомими замовниками послуг Концерну РРТ є ПАТ «НСТУ», якому надають послуги з трансляції телевізійних програм у аналоговому і цифровому форматі та радіопрограм у діапазонах ультракоротких та середніх хвиль, ТОВ

«Зеонбуд» (цифрове телебачення), оператори стільникового зв'язку (технічне обслуговування телекомунікаційного обладнання).

Концерн РРТ є членом Міжнародної організації супутникового зв'язку «INTELSAT» і акціонером Європейської організації супутникового зв'язку «EUTELSAT S. A.».

У 2019 році Національна рада України з питань телебачення і радіомовлення визначила Концерн РРТ оператором багатоканальної цифрової національної телемережі Multiplex МХ-7. Указом Президента України від 18 травня 2021 року № 198/2021 запроваджено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Щодо окремих заходів із забезпечення інформаційної безпеки», відповідно до якого передбачений механізм матеріально-технічного забезпечення побудови Концерном РРТ загальнонаціональної цифрової багатоканальної телемережі МХ-7.

Мультиплекс МХ-7 зможе розмістити до 12 телевізійних каналів і 3 радіоканали. Передусім це будуть державні канали та суспільний мовник.

Побудова загальнонаціональної цифрової багатоканальної телемережі МХ-7 є суспільно значимою з точки зору забезпечення інформаційної безпеки України. Адже мультиплекс надасть державі можливість контролю над елементом критичної інфраструктури — доступом до національного мовлення. Крім того, поява ще одного оператора національного цифрового мовлення сприятиме розвитку конкуренції на ринку для телеканалів.

Державне підприємство спеціального зв'язку (ДП СЗ)

Державне підприємство «Український науково-дослідний інститут радіо і телебачення» (ДП «УНДІРТ»)

Галузевий державний архів Держспецзв'язку м. Київ

Медичний центр Держспецзв'язку м. Київ

Казенне підприємство «Укрспецзв'язок»

Головне управління та підрозділи урядового фельд'єгерського зв'язку Держспецзв'язку

Перспективи розвитку Держспецзв’язку

У сучасному світі, інформаційна безпека є однією з ключових складових національної безпеки, розвиток Державної служби спеціального зв'язку та захисту інформації України має важливе значення. В умовах зростання кіберзагроз, необхідності захисту державної інформації, а також зростаючих вимог до захищеного зв’язку, Служба постає перед новими викликами і потребує стратегічного розвитку.

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.

ВИСНОВКИ

З метою підвищення національної безпеки України та забезпечення ефективного захисту державної інформаційної інфраструктури, стратегічний розвиток Держспецзв’язку передбачає комплексну модернізацію, удосконалення та посилення захищених систем зв’язку і кіберзахисту. До ключових кроків для досягнення цих цілей належить інтеграція мереж у єдину захищену мультисервісну платформу Національної телекомунікаційної мережі, переоснащення підрозділів сучасними цифровими засобами зв’язку, модернізація систем зв’язку спеціального призначення та оптимізація організаційних структур. Це забезпечить надійну комунікаційну підтримку державних органів, особливо в умовах кризових ситуацій.

Також важливими аспектами є розвиток нормативно-правової бази, проведення акредитації для захисту комунікаційно-інформаційних систем, удосконалення механізмів кіберзахисту та запровадження програм підготовки фахівців із захисту інформації. Водночас необхідно нарощувати спроможності з виробництва ключових документів для криптографічного захисту та впроваджувати системи технічного регулювання для протидії технічним розвідкам. Ці заходи дозволять не лише покращити захищеність інформації, але й підвищити ефективність роботи Держспецзв’язку, забезпечуючи надійний захист від сучасних кіберзагроз і можливість відповідати на них злагоджено та оперативно.