**Тема 4.** **Державні органи в інформаційній сфері**.

1. Інформаційна безпека та механізми її забезпечення.
2. Основні функції Комітету Верховної Ради України з питань гуманітарної та інформаційної політики.
3. Створення Департаменту доступу до публічної інформації Офісу Президента України ( серпень 2019 р.).
4. Міністерство цифрової трансформації України.
5. Державна служба спеціального зв’язку та захисту інформації України.
6. Інформаційна безпека є не лише складовою національної безпеки, а й невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, адже всі типи взаємовідносин між суб’єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією.

З цього приводу В.А. Ліпкан зазначає, що національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу.

Український учений М. Сенченко справедливо відзначає, що Україні для ефективного протистояння інформаційній війні з боку росії потрібно мати хоча б:

1) ефективну систему ведення інформаційної війни;

2) ефективну правову концепцію інформаційної війни;

3) стратегію ведення інформаційної війни.

Лише та держава може розраховувати на лідерство в економічній, військово-політичній чи інших сферах, мати стратегічну й тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби.

Інформаційна безпека України передбачає головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Реалізація такого завдання зумовлює потребу створення системи протидії будь-якій інформаційній загрозі та захисту власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Застосування росією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України росія використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Механізми захисту інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний.

Найважливіше на **законодавчому рівні** – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, що може спричинити послаблення інформаційної безпеки.

**Адміністративний** механізм забезпечення інформаційної безпеки охоплює установи, діяльність яких спрямована на формування та реалізацію інформаційної безпеки. Головне на адміністративному рівні – сформувати програму заходів в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи поточний стан справ.

Сьогодні запорукою створення надійної системи забезпечення охорони інформаційної безпеки може бути тільки зміцнення самої української держави та державних органів, відповідальних за її забезпечення. Реалізація цього завдання зумовлює масштабні завдання, пов’язані з виробленням системи забезпечення інформаційної безпеки, пошуком принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління ризиками та загрозами.

Серед **основних напрямів забезпечення інформаційної безпеки виділяють:**

* підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
* створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки;
* підтримка ринково орієнтованої стандартизації та сертифікації;
* правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
* зміцнення інформаційної безпеки на державному рівні шляхом.

Інформаційна безпека як поняття розглядається у декількох ракурсах. У найзагальнішому вигляді – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави. Оскільки суспільні відносини, що виникають у зв’язку із забезпеченням інформаційної безпеки регулюються нормами права, є необхідним проаналізувати основні принципи і норми, спрямовані на забезпечення інформаційної безпеки.

Український законодавець за роки незалежності сформував потужну правову базу у сфері національної безпеки, основою для якої є чинна Конституція України. Так, у ч. 1 ст. 3 Конституції України сформульовано концептуальні засади забезпечення безпеки людини: “людина, її життя і здоров’я, честь і гідність, недоторканість і безпека визначаються в Україні найвищою цінністю”. У ч. 1 ст. 17 Конституції України передбачено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Загалом, у Конституції України містяться правові норми, пов’язані із забезпеченням інформаційної безпеки, які становлять основу законодавства у цій сфері і мають вищу юридичну силу. У цих нормах закріплено право на інформацію, передбачена охорона відомостей, що становлять державну таємницю. Конституційні норми, пов’язані із забезпеченням інформаційної безпеки, вказують на те, що це питання є настільки багатоаспектним та багатогранним, що кожна з зазначених правових норм може стати окремими темами наукових досліджень.

Правові засади національної безпеки України також регламентуються Законом України “Про національну безпеку України” від 21 червня 2018 р. У різних державах розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного простору. Застосовуючи різні засоби, країни-лідери достатньо ефективно здійснюють національну політику інформаційної безпеки.

На сьогодні кібербезпека є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави.

Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі.

Україна схвалила Стратегію кібербезпеки України. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

На основі вивчення міжнародних правових актів, що стосуються протидії новим викликам та загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, очевидним є висновок про необхідність подальшої імплементації положень міжнародних правових актів та гармонізації з законодавствами іноземних держав.

**Заходи щодо забезпечення інформаційної безпеки України** повинні здійснюватися шляхом:

* забезпечення інформаційного суверенітету України;
* удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
* забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо.

В умовах сучасного розвитку інформаційного суспільства, захист національного інформаційного простору та забезпечення інформаційної безпеки вже стали пріоритетними стратегічними завданнями багатьох держав світу.

1. **Комітет Верховної Ради України з питань гуманітарної та інформаційної політики** — утворений 29 серпня 2019 у [Верховній Раді України IX скликання](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%BD%D0%B0_%D0%A0%D0%B0%D0%B4%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8_IX_%D1%81%D0%BA%D0%BB%D0%B8%D0%BA%D0%B0%D0%BD%D0%BD%D1%8F). У складі комітету 17 депутатів, голова Комітету —[Потураєв Микита Русланович](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%82%D1%83%D1%80%D0%B0%D1%94%D0%B2_%D0%9C%D0%B8%D0%BA%D0%B8%D1%82%D0%B0_%D0%A0%D1%83%D1%81%D0%BB%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8%D1%87) (із 17 червня 2020 року)

Предмети відання Комітету Верховної Ради України з питань гуманітарної та інформаційної політики:

* Культурно-просвітницька діяльність (видавнича справа, бібліотечна справа, народні художні промисли);
* культурно-мистецька діяльність (професійні творчі спілки, театри, музика, школи естетичного виховання, арт-ринок, дизайн, галереї, організація виставок, концертів, фестивалів тощо);
* медійна індустрія (телебачення, ОТТ та IPTV, платформи з розповсюдження інформації, радіо),
* національна кіноіндустрія; аудіовізуальний ринок; рекламна діяльність; охорона історико-культурної спадщини (музейна справа, архівна справа, діяльність заповідників, вивезення, ввезення і повернення культурних цінностей);
* друковані, електронні засоби масової інформації, у тому числі соціальні медіа, мережа Інтернет;
* туризм та туристична діяльність;
* курорти та рекреаційна діяльність; державна політика у сфері свободи совісті та релігійних організацій; державна політика у сфері розвитку та використання державної мови та мов національних меншин в Україні;
* засади благодійної діяльності, у тому числі меценатської;
* IX скликання Верховної Ради України державна політика у сфері інформації та інформаційної безпеки (крім питань, що належать до сфери національної безпеки та оборони);
* висвітлення діяльності Верховної Ради України;
* державна політика у сфері сімейно-шлюбних відносин;
* державна політика сприяння становленню інституту сім’ї, забезпечення надання державної допомоги сім’ям з дітьми, захисту безпритульних дітей, оздоровлення та відпочинку дітей;
* демографічна політика.

1. **Департамент доступу до публічної інформації Офісу Президента України** спеціальним структурним підрозділом, який організовує в установленому порядку доступ до публічної інформації, відповідає за розгляд, опрацювання, облік, систематизацію, аналізування та надання відповідей на запити на інформацію, що надходять до Президента України, Офісу Президента України, а також надає консультації під час оформлення таких запитів.

Цим документом також визначили такими, що втратили чинність: указ президента від 5 травня 2011 року № 548 «Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України» та указ від 17 листопада 2014 року № 883 «Про внесення змін до Указу Президента України від 5 травня 2011 року № 548».

1. **Міністерство цифрової трансформації України є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, розвитку національних електронних інформаційних ресурсів, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії.**

Створене у вересні 2019 р

**Михайло Федоров**

Варто класифікувати повноваження Мінцифри саме за типом повноваження, і тому можна виділити на загальнодержавні, адміністративні, регіональні, соціальні, господарські (підприємницькі).

**Загальнодержавні:**

1) узагальнює практику застосування законодавства з питань, що належать до його

компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України та в установленому порядку вносить їх Кабінетові Міністрів України;

2) розробляє проєкти законів та інших нормативно-правових актів із питань, що належать до його компетенції;

3) здійснює заходи щодо створення та забезпечення функціонування:системи електронної взаємодії державних електронних інформаційних ресурсів

–системи електронної взаємодії органів виконавчої влади;

–інтегрованої системи електронної ідентифікації;

–єдиного веб-порталу електронного урядування;

–єдиного державного веб-порталу від критих даних;

–національного реєстру електронних інформаційних ресурсів;

–єдиного державного веб-порталу електронних послуг;

4) розробляє пропозиції щодо:

–визначення цілей і завдань державної інформаційної політики, інтелектуальної власності та шляхів її реалізації;

–встановлення стандартів, норм, правил, порядків, класифікаторів у сферах, що належить до його компетенції;

–визначення порядку функціонування офіційних веб-сайтів органів виконавчої влади, державних інформаційно

-аналітичних систем, державних інформаційних ресурсів, електронних реєстрів та баз даних;

–прийняття або внесення змін до нормативно-правових актів із питань захисту персональних даних, охорони інтелектуальної власності;

5) бере участь у:

–формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку;

–впровадженні концепції смарт-сіті органами місцевого самоврядування;

–забезпеченні розвитку віртуальних активів, блокчейну та токенізації, штучного інтелекту;

–розробленні норм, стандартів у сферах електронних довірчих послуг та електронної

ідентифікації;

–розробленні критеріїв і порядку проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах; організації та проведенні оцінки стану захищеності державних інформаційних ресурсів, наданні відповідних рекомендацій;

–формуванні і реалізації державної тарифної політики та політики публічних закупівель у сферах телекомунікацій, користування радіочастотним ресурсом України;

–розробленні пропозицій щодо державної політики з питань державного регулювання у сферах телекомунікацій, користування ра-діочастотним ресурсом, надання послуг поштового зв’язку;

– розробленні та впровадженні вимог: до форматів даних електронного документообігу в державних органах; щодо функціонування електронного документообігу; до оформлення документів, організації документообігу, зокрема електронного документообігу;

–розробленні та організації виконання державних програм із питань захисту інформації та кіберзахисту;

–здійсненні заходів щодо забезпечення функціонування Національної системи конфіденційного зв’язку та Національної телекомунікаційної мережі;

6) здійснює управління об’єктами державної власності, що належать до сфери управління Мінцифри;

7) здійснює міжнародне співробітництво, забезпечує виконання зобов’язань, взятих за міжнародними договорами України, з питань, що належать до компетенції Мінцифри.

**Адміністративні**:

1. розробляє нормативно-технічну до-кументацію щодо цифрових трансформацій;

2) виконує функції генерального державного замовника Національної програми інформатизації та інших державних програм цифровізації, зокрема:

–здійснює моніторинг у сфері інформатизації;

–погоджує та координує галузеві, регіональні програми та проекти інформатизації, програми та проєкти інформатизації органів місцевого самоврядування і вносить подання Кабінетові Міністрів України щодо зупинення виконання таких програм і проєктів;

забезпечує:

–методологічну, нормативно-правову, інформаційну та організаційну підтримку процесів формування і виконання Національної програми інформатизації;

–проведення експертизи Національної програми інформатизації та окремих її завдань (проєктів);

3) проводить цифрову експертизу та готує відповідні висновки до проєктів відповідних актів Кабінету Міністрів України, міністерств та інших органів виконавчої влади;

4) проводить погодження в порядку, встановленому законодавством, призначення керівника з питань цифрового розвитку, цифрових трансформацій або цифровізації органу виконавчої влади;

5) розробляє пропозиції щодо визначення основних напрямів розвитку системи надання електронних та адміністративних послуг, здійснює заходи з її реформування;

6) формує та веде Реєстр адміністративних послуг;

7) координує діяльність органів, що утворили центри надання адміністративних послуг із питань підвищення рівня якості надання електронних та адміністративних послуг, розвитку електронної інформаційної взаємодії таких центрів із суб’єктами надання адміністративних послуг, розширення функцій центрів і переліку послуг, які надаються через них;

8) здійснює моніторинг якості надання електронних та адміністративних послуг, широкосмугового доступу до Інтернету, відкри-тих даних;

9) координує діяльність міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих держадміністрацій, а також державних підприємств, установ, організацій та державних господарських об’єднань, навчальних закладів із питань, що належать до компетенції Мінцифри, надає їм необхідну методичну допомогу;

10) організовує та координує діяльність органів виконавчої влади, пов’язану із співпрацею з програмою ЄС «Єдиний цифровий ринок» (DigitalSingleMarket), інших міжнаро-дних програм цифрового співробітництва;

11) здійснює моніторинг даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері;

12) координує адміністрування, функціонування та використання адресного простору українського сегмента Інтернету;

13) здійснює визначені законом повноваження у сферах електронних довірчих послуг та електронної ідентифікації:

–надає адміністративну послугу шляхом внесення юридичних осіб та фізичних осіб

–підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку;

–погоджує розроблені надавачами електронних довірчих послуг порядки синхронізації часу із Всесвітнім координованим часом (UTC);

–погоджує плани припинення діяльності кваліфікованих надавачів електронних довірчих послуг;

–приймає та зберігає документовану інформацію, сформовані сертифікати (у т. ч. посилені, кваліфіковані) відкритих ключів, реєстри чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності кваліфікованого надавача електронних довірчих послуг;

–розглядає пропозиції (зауваження) суб’єктів відносин у сфері електронних довірчих послуг щодо удосконалення державного регулювання сфери електронних довірчих послуг;

–надає суб’єктам відносин у сфері електронних довірчих послуг консультації з пи-тань, пов’язаних із наданням електронних довірчих послуг;

–інформує відповідно до Закону України «Про електронні довірчі послуги» про обставини, які перешкоджають діяльності центрального засвідчуваного органу;

–проводить оцінку стану розвитку сфери електронних довірчих послуг за результатами проведення аналізу інформації про діяльність постачальників електронних довірчих послуг та засвідчуваного центру;

–забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг;

–здійснює інші повноваження у сферах електронних довірчих послуг та електронної ідентифікації, визначені законом;

14) затверджує:

–методику визначення належності бюджетних програм до сфери інформатизації;

–методику формування індикаторів розвитку інформаційного суспільства;

–порядок оброблення інформації в інтегрованій системі електронної ідентифікації, інтеграції інформаційно-телекомунікаційних систем до цієї системи, регламент роботи інтегрованої системи електронної ідентифікації та

примірний договір про приєднання до цієї системи;

–примірний договір про інформаційну взаємодію та примірну угоду про підключення до системи електронної взаємодії державних

електронних інформаційних ресурсів;

–формати електронних повідомлень та обміну даними системи електронної взаємодії державних електронних інформаційних ресурсів;

–вимоги до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування;

15) організовує навчання державних службовців з питань, що належать до компетенції Мінцифри;

16) організовує навчання та готує пропозиції щодо вдосконалення системи розвитку цифрових навичок громадян, підготовки та перепідготовки фахівців з питань, що належать до компетенції Мінцифри.

**Регіональні:**

1. сприяє впровадженню у державних органах та органах місцевого самоврядування технологій цифрових трансформацій.

Соціальні: здійснює розгляд звернень громадян з питань, пов’язаних з діяльністю Мінцифри, підприємств, установ та організацій, що належать до сфери його управління, а також стосовно актів, які видаються Мінцифри

Господарські (підприємницькі): сприяє залученню інвестицій, упровадженню новітніх технологій та використанню управлінського досвіду з питань, що належать до компетенції Мінцифри.

Спостерігаємо, що узагальнення та систематизація повноважень Міністерства цифрової трансформації України дає нам свідчення, що ключовий акцент у діяльності органу виконавчої влади спрямований на реалізацію адміністративно-державних повноважень. Вони найбільш глибоко формально визначені і пояснені.

Висновки.Таким чином, сучасна цифровізація розвивається одночасно за трьома ключовими напрямами: інформаційне суспільство; цифрові економічні відносини; електронний уряд. Зазначені виклики лягли в основу діяльності Міністерства цифрової трансформації України, яке є центральним засвідчувальним органом у сфері електронних довірчих послуг. Також до компетенції Міністерства належить розвиток широкосмугового доступу до інтернету, телекомунікаційних мереж та ІТ-індустрії. Проаналізувавши завдання та повноваження Мінцифри, основними серед них є адміністративні та загальнодержавні, які утворюють основний пласт його діяльності та забезпечують його сутність.

1. **Державна служба спеціального зв’язку та захисту інформації України.**

Держспецзв'язку створено на виконання прийнятого 23 лютого 2006 року Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України.

Держспецзв'язку виконує 93 завдання й функції та формує державну політику в 16 сферах (згідно із Законом України «Про Державну службу спеціального зв'язку та захисту України»).

У штаті Держспецзв'язку та підприємств, що належать до сфери управління Служби, працюють понад 11 тис. фахівців, з-поміж яких 80 % — військовослужбовці.

1 грудня 2023 року розпорядженням Кабінету Міністрів України № 1098-р Головою Державної служби спеціального зв'язку та захисту інформації України призначений [Мироненко Юрій Миколайович](https://uk.wikipedia.org/w/index.php?title=%D0%9C%D0%B8%D1%80%D0%BE%D0%BD%D0%B5%D0%BD%D0%BA%D0%BE_%D0%AE%D1%80%D1%96%D0%B9_%D0%9C%D0%B8%D0%BA%D0%BE%D0%BB%D0%B0%D0%B9%D0%BE%D0%B2%D0%B8%D1%87&action=edit&redlink=1)

22 жовтня 2021 року Президент України Володимир Зеленський затвердив Концепцію реформування Держспецзв'язку (Указ Президента України № 544/2021 "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»"). До 2025 року Державна служба спеціального зв'язку та захисту інформації України буде реформована.

Реформа Держспецзв'язку — це посилення інституційних  спроможностей. Унаслідок реформування Служба стане більш ефективною та прозорою. Будуть розв'язані питання соціального забезпечення військовослужбовців. Відбудеться демілітаризація Служби — виконання деяких військових функцій буде передане цивільним співробітникам.

Основні засади реформування:

**Урядовий зв'язок.** Система урядового зв'язку буде повністю інтегрована до Національної телекомунікаційної мережі, осучаснені та модернізовані системи зв'язку. Фельд'єгерський зв'язок стане оперативнішим і більш захищеним.

**Кібербезпека**. Сучасна система кіберзахисту буде розгорнута на об'єктах критичної інформаційної інфраструктури, посилено захист державних інформаційних ресурсів, буде розширено сучасну нормативно-правову базу у сфері кіберзахисту.

**Захист інформації.** Буде розроблено та імплементовано нові сучасні стандарти технічного і криптографічного захисту інформації, протидії технічним розвідкам.

**Ефективність**. Відбудеться реформування структури Служби, посилення демократичного цивільного контролю. Робота у Держспецзв'язку буде престижною і забезпечуватиме гідний соціальний рівень. Підвищимо якість освіти з кібербезпеки, рівень фахівців із захисту інформації.

**Міжнародна співпраця.** Внаслідок реформи Держспецзв'язку розширить співпрацю з НАТО з метою впровадження стандартів Альянсу у повсякденну діяльність та задля наближення набуття Україною членства у Альянсі. Служба стане акредитаційним центром із питань безпеки національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом.

**Функції Держспецзв'язку:**

* **Захист інформації (кіберзахист). Д**ержспецзв'язок — 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.

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

* **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.

#### 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.

#### 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.

#### 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.