ТЕМА 11. СТРАТЕГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КРАЇНАХ СВІТУ

План лекції

1. Національні суб’єкти реагування та протидії кіберзагрозам
2. Міжнародні інституції забезпечення інформаційної безпеки
3. Вітчизняні суб’єкти запобігання та протидії кіберзагрозам
4. Стратегії кібербезпеки зарубіжних країн

Суб’єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки:

- ✓ міністерства та інші центральні органи виконавчої влади;
- ✓ місцеві державні адміністрації;
- ✓ органи місцевого самоврядування;
- ✓ правоохоронні, розвідувальні та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;
- ✓ Збройні Сили (ЗС) України, інші військові формування, утворені відповідно до закону;
- ✓ Національний банк України;
- ✓ підприємства, установи й організації, віднесені до об’єктів критичної інфраструктури;
- ✓ суб’єкти господарювання, громадяни України й об’єднання громадян, інші особи, які провадять діяльність та / або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом

Суб’єкти забезпечення кібербезпеки здійснюють:

- заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;
- виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
- інформаційний обмін щодо реалізованих і потенційних кіберзагроз;
- розробку і реалізацію запобіжних, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;
- проведення аудиту інформаційної безпеки, у т. ч. на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;
- інші заходи із забезпечення розвитку та безпеки кіберпростору

Розв’язання основних завдань кібербезпеки неможливе без створення:

- ✓ міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки;

- ✓ центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення й оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад і надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін і впливу на їх інформаційно-телекомунікаційні системи;

- ✓ органів власної інформаційної та кібербезпеки – державних установ (відомств) і комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів

Сучасні пріоритети ООН спрямовані на координацію зусиль щодо забезпечення комплексного підходу до розв’язання міжнародних проблем.

Для цього необхідним є:

– перебудова Секретаріату ООН, який непомірно розрісся і хибує на дублювання, паралелізм, невиправдані фінансові витрати;

– вдосконалення системи фінансування, що проявляється у хронічній фінансовій кризі ООН;

– вирішення проблем у напрямі безпеки у сфері міжнародної інформації тощо.

Таблиця 1

Основні резолюції ГА ООН у сфері інформаційної безпеки

Рік, № резолюції	Назва	Зміст
1986 р., № 41/92	«Про створення всеосяжної системи міжнародного миру і безпеки»	Визнання міжнародної інформаційної безпеки як складника в системі міжнародної безпеки
1999 р., № 54/50	«Роль науки і техніки в контексті міжнародної безпеки та роззброєння»	Визнання можливостей застосування досягнень науки і техніки як чинника впливу на міжнародну безпеку
2001 р., № 56/164	«Загальна оцінка проблем інформаційної безпеки. Загрози міжнародній інформаційній безпеці»	Виділення основних чинників, що створюють небезпеку основним інтересам особи, суспільству і державі в інформаційному просторі
2002 р., № 57/239	«Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур»	Прийняття рішень щодо захисту інформаційного суспільства. Кіберзлочини і кібертероризм були визнані серйозною проблемою для загального миру і безпеки
2004 р., № 59/454	«Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки»	Сприяння розгляду на міжнародному рівні існуючих та потенційних угод у сфері інформаційної безпеки, спрямованих на боротьбу з інформаційним тероризмом і криміналом
2010 р., № 65/141	«Застосування інформаційно-комунікаційних технологій у цілях розвитку»	Визнання необхідності застосування інформаційно-комунікаційних технологій для активізації співробітництва у сфері безпеки на міжнародному рівні
2018 р., № 73/678	«Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки»	Затвердження необхідності усіх держав проводити політику роззброєння та міжнародної безпеки в кіберпросторі

Джерело: Резолюції Генеральної Асамблеї ООН (1946-2020). URL: https://www.un.org/ru/sections/documents/general-assemblyresolutions/index.html

ОБСЄ сприяє внеску в процес зміцнення європейської безпеки завдяки політичним механізмам та інструментам, а також за рахунок зацікавленості нинішнього керівництва в подальшому поглибленні конструктивного співробітництва з Україною з метою стабілізації ситуації на Сході і недопущення розповсюдження проявів російської агресії в інших регіонах Європи

Нині багато міжнародних організацій займаються проблемами війни та миру, вирішенням військових конфліктів і проблемами в галузі інформаційної безпеки. Серед таких міжнародних організацій треба виділити НАТО – Північноатлантичний Альянс.

Країни-члени НАТО можуть сподіватися, що реакція на порушення інформаційної безпеки, а саме порушення кібербезпеки, не залишиться без допомоги міжнародної організації. Україна потребує адекватної системи інформаційної безпеки. Питання захисту у кіберпросторі є питаннями національної безпеки. Найкращим варіантом для України є приєднання до НАТО з метою розбудови та застосування систем колективної безпеки від кібератак та інформаційної війни. Завдяки спільним зусиллям з іншими членами Альянсу Україна не залишиться наодинці у складному протистоянні російській агресії на Донбасі.

Міжнародний союз електрозв’язку (МСЕ) нині є спеціалізованим агентством ООН і займається питаннями в галузі телекомунікацій. Україна стала членом міжнародної організації у 1947 році. В умовах незалежності наша країна стала ще більш активно співпрацювати з цією організацією в напрямі подолання «цифрового розриву» в телекомунікаційних технологіях на національному і на міжнародному рівнях

Ставлення Європейського Союзу до колективної безпеки в напрямі забезпечення захисту економічної політики та політики розвитку нині носить зовнішній характер. Для виконання Спільної політики у сфері інформаційної безпеки органи керівництва ЄС мають забезпечити гарантію виконання таких умов, як: необхідність створення правової основи для розвитку міжнародної торгівлі; формування та функціонування спільного ринку між країнами-членами; застосування політики безпеки та спільної зовнішньої політики, які повинні бути у тандемі, а також наявність співробітництва у внутрішніх справах та юстиції.

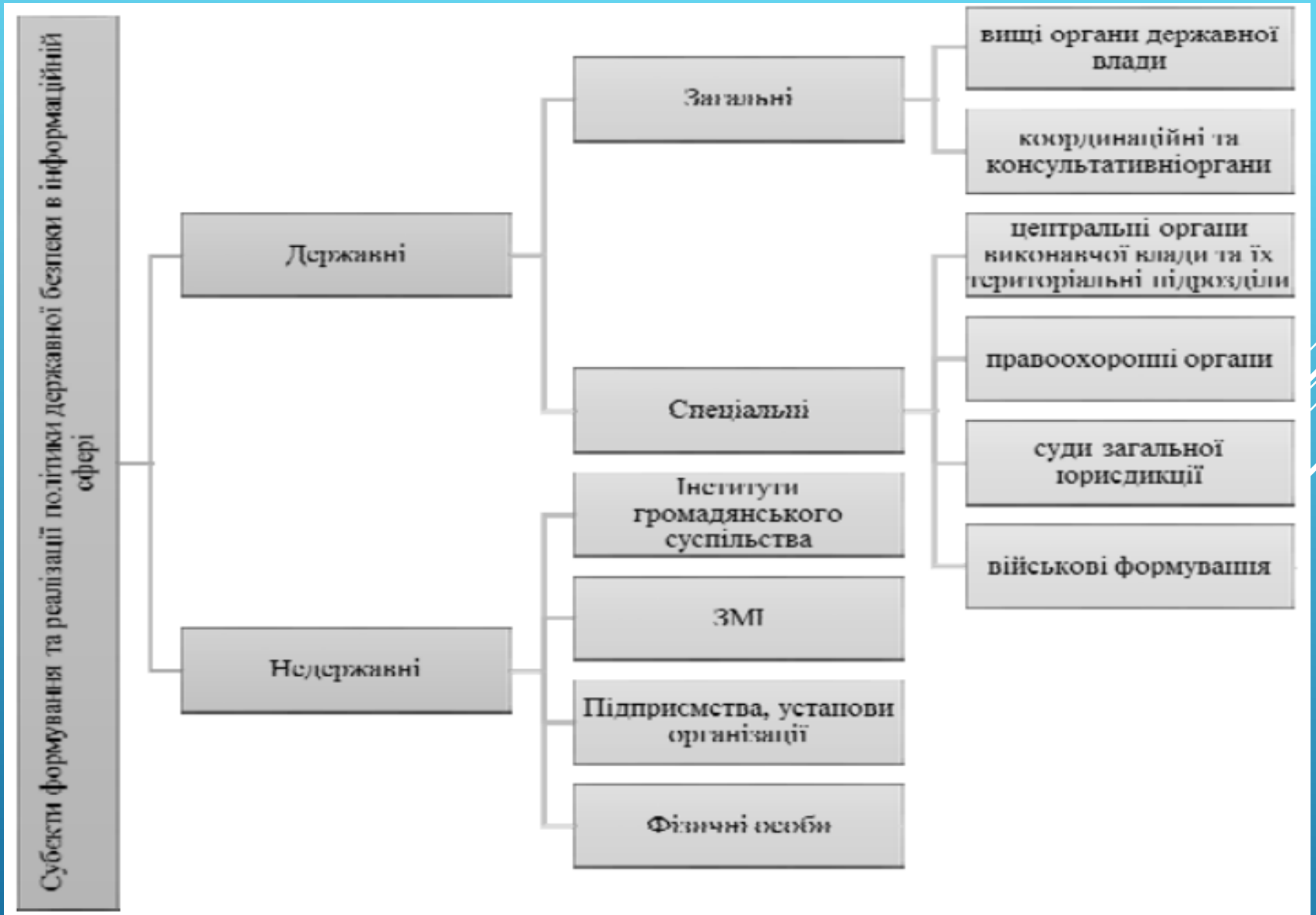

Рис. 1. Система суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері

Джерело: Прав Р.Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. Державне управління: удосконалення та розвиток. URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf

Суб’єкти формування та реалізації політики державної безпеки в інформаційній сфері можна розділити на дві основні категорії:

– органи державної влади України (різних рівнів та сфер життєдіяльності, органи місцевого самоврядування);

– суб’єкти, що функціонують поза системою державного управління: підприємства та організації різних форм власності і господарювання, громадські об’єднання, асоціації та інші організації громадянського суспільства.

Між визначеними суб’єктами формування та реалізації політики державної безпеки в інформаційній сфері існує тісний зв'язок: якщо суспільство має можливість сприяти реалізації інформаційної політики, то органи виконавчої влади є єдиними суб’єктом, що забезпечує її формування та від якого залежить ефективність її реалізації.

Органи державної влади здійснюють формування системи інформаційної безпеки на декількох рівнях:

– законодавчому;

– адміністративному;

– процедурному;

– програмно-технічному