

Проблеми застосування в Україні норм інформаційної безпеки НАТО

Аналітична записка

Празький самміт, на якому було підтверджено бажання України щодо вступу у НАТО та прийнято План дій між Україною і НАТО став певною віхою в напрямку активізації співробітництва України з НАТО. План дій буде стратегічною рамковою угодою, з метою визначення певних критеріїв, поставлених перед країнами, які уклали з НАТО План дій щодо членства (ПДЧ). Положення ПДЧ доповнюють ті види діяльності, які вже розгорнуто за програмою “Партнерство заради миру”, через розширення діапазону підготовчих заходів, необхідних для набуття членства в НАТО. Одним з таких пріоритетних напрямків є питання інформаційної безпеки та захисту інформації.

I. Нові виклики сучасності та інформаційна безпека держави.

Проблеми ХХІ століття кількісно і якісно відмінні від тих, які були характерні для періоду холодної війни, тому потрібні корінні зміни інститутів національної безпеки, військової стратегії і підходів до питань оборони. Інформаційна та консцієнтна війна, де предметом ураження і знищення є визначені типи свідомості, свідчать, що світ вступив у новий етап боротьби - конкуренції форм організації свідомості. Відбувається перенесення акценту в збройному протистоянні з традиційних його форм ведення в інформаційно-інтелектуальну й інформаційно-технічну сфери, тобто туди, де ведеться підготовка, відбувається прийняття і реалізація військових і політичних рішень. Інформаційний вплив носить різнобічний характер і змінюється в залежності від розв'язуваних завдань і обстановки. Інформаційна і консцієнтна зброя впливають на “ідеальні” об'єкти (знакові системи) або їхні матеріальні носії. Інформаційна війна по суті є комплексом заходів і операцій, здійснюваних у конфліктних ситуаціях, коли інформація є водночас зброєю, ресурсом і ціллю. Закономірним є питання про те, якою мірою реальна і наскільки загрожує національним інтересам інформаційна війна.

Поширення взаємозв'язків і взаємозалежностей у сучасному світі робить його дедалі вразливішим. Нові прояви вразливості з'являються і змінюються в результаті більшої відкритості світового співтовариства, ускладнення технологічних систем, зростаючої залежності від електронних систем інформації та зв'язку, взаємозв'язаних і дедалі більш щільних транспортних мереж. Втрата на тривалий період через терористичні напади, саботаж, технічні збої кількох основних елементів та функцій може викликати широкомасштабні порушення. В основі ключових елементів інфраструктури, ушкодження або виведення з ладу яких матиме руйнівні наслідки для безпеки держави, лежать інформаційні системи, зростання інтеграції яких викликає необхідність забезпечення інформаційної безпеки та захисту інформації.

Поширення використання інформаційних технологій змінило значення державних кордонів в контексті національної безпеки. Сучасні тенденції розвитку суспільства ведуть до розростання міжнародного тероризму, появи на його озброєнні новітніх технологій і виникнення принципово нового високотехнологічного кібертероризму. Міжнародний тероризм є непрямим, потенційно високоефективним засобом дестабілізації й ослаблення держави, не переходячи меж відкритої ворожості. Непрямий і дестабілізуючий вплив як одна з ознак тероризму - убити одного, щоб залякати сотні - виявляється більш суттєвим, ніж прямий вплив терористичних силових актів. Засоби інформації створюють міжнародному тероризму "віртуальний простір", що істотно підсилює непрямий вплив терористичних акцій - оскільки він не має меж у просторовому відношенні, і дестабілізуючий - оскільки чинить реальний політико-психологічний вплив.

Нову якість і значення тероризм і застосовувані ним методи нерегулярного ведення війни придбали ще за часів холодної війни. Приховане ведення війни, включаючи використання терористичних форм боротьби, між наддержавами в очікуванні звичайної або навіть ядерної війни було основою військово-політичних стратегій багатьох країн і військово-політичних блоків. У рамках патової ситуації атомних і неатомних військових потенціалів нерегулярне ведення війни отримало стратегічний пріоритет, оскільки воно було прихованим, непрямим, гнучким і не занадто дорогим.

У військових операціях останнього десятиліття отримали ширше застосування як технічні інформаційні системи, так і спеціальні заходи інформаційної протидії. Так, за кілька тижнів до початку операції "Буря в пустелі" агенти ЦРУ впровадили програмні "віруси-закладки", що у призначений день і годину відключили телефонні станції і радіолокаційні пости, паралізувавши вже в перші хвилини повітряного нальоту систему ППО Іраку. Аналіз бойових дій армії США показав, що інформаційні технології забезпечують скорочення середнього часу підльоту і підготовки до атаки ударних вертольотів з 26 до 18 хвилин і збільшення відсотка ураження цілей ПТКР з 55 до 93 %. Обробка і передача повідомлень у вищестоящі штаби в ланці "рота-батальйон" скорочується з 9 до 5 хвилин, імовірність дублювання телеграм знижується з 30 до 4 %, передачі підтверджуючої інформації з телефонних ліній - з 98 до 22 %.

Інформаційне забезпечення дій сил НАТО в ході військового конфлікту в Косово включало реалізацію основних способів ведення інформаційної війни таких як застосування бойових електронних засобів з метою послідовного ураження всієї інформаційної системи, розрив інформаційних потоків; ослаблення і руйнування системи бойового керування і зв'язку противника, використання відповідних електронних засобів і електромагнітної зброї для заглушування та нейтралізації роботи центрів збору інформації збройних сил Югославії, для виведення з ладу засобів зв'язку і радіолокаційних станцій. Одночасно були задіяні засоби власного інформаційного захисту по забезпеченню оперативної скритності за допомогою суворого дотримання режиму таємності та перешкоджання доступу противника до своєї інформації. Складовою інформаційного протистояння в операції "Союзницька сила" було інформаційно-технічне протистояння об'єднаних збройних сил (ОЗС) НАТО і збройних сил СРЮ. Боротьба за інформаційне домінування розгорнулася насамперед у сфері електронних засобів розвідки, обробки і поширення інформації ОЗС НАТО при активному використанні сучасних засобів і систем розвідки, зв'язку, радіонавігації і цілеуказування. У зв'язку з цим відповідні підрозділи ОЗС НАТО провели широкомасштабні акції по ураженню найважливіших пунктів керування ЗР СРЮ, елементів державної і військової інформаційної інфраструктури Югославії, а також систем, що знаходились на озброєнні югославської армії, засобів радіозв'язку і радіолокаційної розвідки. У ході нанесення авіаційних ударів по об'єктах інформаційної інфраструктури ОЗС Альянсу використовували спеціальні авіабомби для виведення з ладу засобів радіолокації. Отриманий досвід, а також перспективи технічного розвитку дали підстави виділити інформаційну війну в окрему область протистояння. З огляду на великі можливості і досить високу ефективність структур НАТО по інформаційному впливу у військових конфліктах, можна зробити висновок, що роль і значення інформаційної війни у військових конфліктах ХХІ століття буде збільшуватися.

Сьогодні Пентагон це не тільки один з найбільших власників, орендарів і користувачів інформаційних і телекомунікаційних ресурсів, провідних замовників програмного забезпечення, комп'ютерного устаткування і засобів цифрового зв'язку, але й, по суті, законодавець державної політики і промислових стандартів в області інформаційної безпеки. Деякою мірою це позначається і на самих поняттях, зв'язаних із захистом

інформації, що поступово трансформуючись з чисто військових термінів здобувають характер загальнодержавних і промислових стандартів. Виробники устаткування і розроблювачі програмних продуктів, зацікавлені у великих державних і військових замовленнях, починають прислухатися до того, що говорять у коридорах Пентагона про інформаційну безпеку.

У таємній директиві Пентагона S-3600.1 з'явилися зовсім нові поняття - "гарантія інформації" та "інформаційна операція". В основу терміну "інформаційна операція" покладений класичний прийом ведення війни - дезорганізація керування. Гарантія інформації визначається як "інформаційна операція або операції, пов'язані з захистом інформації й інформаційних систем за рахунок забезпечення їхньої готовності (доступності), цілісності, автентичності, конфіденційності і несуперечності. Дані операції містять у собі відновлення інформаційних систем за рахунок об'єднання можливостей захисту, виявлення та реагування. При цьому інформація не повинна бути розкритою особам, процесам або пристроям, які не мають до неї прав доступу, але має бути забезпечена повна вірогідність факту передачі, наявності самого повідомлення та його відправника. Одночасно має бути забезпечена перевірка прав на одержання окремих категорій інформації. Дані залишаються у вихідному виді і не повинні бути випадково або навмисно змінені або знищені. Буде забезпечений своєчасний і надійний (за вимогою) доступ до даних й інформаційних служб установлених користувачів, а відправник даних одержить повідомлення факту доставки, також як одержувач - підтвердження особистості відправника, в такий спосіб ніхто не зможе заперечувати своєї участі в обробці даних. Тим самим класичне поняття інформаційної безпеки як стану інформаційних ресурсів було розширене і доповнене, тобто в політиці інформаційної безпеки чітко позначилося зрушення в напрямку активних організаційно-технічних заходів захисту інформаційних ресурсів.

Україна в силу її геополітичного розташування є об'єктом інтересів багатьох розвинутих держав, що обумовлює велику вірогідність втягування її в інформаційну війну та вимагає розробки методологічних основ інформаційної безпеки як фундаменту для формування і реалізації політики забезпечення національних інтересів на інформаційному рівні і створення національної системи інформаційної безпеки. Тобто забезпечення такого стану захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму можливі збитки через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації.

Таким чином, у зв'язку з появою нових ризиків в сфері безпеки відбувається трансформація традиційних військово-політичних концепцій в напрямку поєднання прямих (силових) та непрямих методів протидії з метою досягнення політичних цілей.

II. Політика НАТО в сфері інформаційної безпеки.

При створенні НАТО в 1949 році системи безпеки країн-учасниць істотно розрізнялися. Загальний підхід до безпеки інформації ґрунтувався на досвіді другої світової війни і методах захисту інформації в умовах воєнного часу. Тому правила безпеки, узгоджені союзниками протягом війни, були прийняті за основу. Перша система засекречування містила вісім рівнів таємності, з них чотири вищих, а також створення в кожній країні двох центральних режимних органів і певна кількість підлеглих. Добір персоналу, що мав доступ до цієї інформації, був дуже суворим, а інформація жорстко контролювалася на всіх стадіях.

Ця система виявилася дуже громіздкою й у 1955 р. основою політики безпеки в НАТО став Меморандум Північноатлантичної Ради “Безпека Організації Північноатлантичного Договору” (С-М(55)15 Final). У цьому документі були зазначені узгоджені та схвалені всіма державами-членами НАТО мінімальні стандарти в області захисту таємної інформації. Основні вимоги стосувались фізичної, процедурної, технічної безпеки і безпеки персоналу як носія інформації. Система засекречування містила чотири рівні таємності: “обмежений доступ”, “конфіденційно”, “таємно”, “абсолютно таємно”. Система обліку була збережена, а система добору персоналу спрощена. Розділ Х додатку “С” цього документа присвячений безпеці таємної інформації, яка зберігається, обробляється та передається в мережах та системах автоматизованої обробки даних (САОД). Обов'язком національного рівня кожної держави Альянсу стала гарантія адекватного захисту таємної (по класифікації НАТО) інформації.

Протягом наступних десятиліть нормативна база Альянсу щодо захисту інформації була розширена укладанням декількох угод: Угоди про взаємне забезпечення гарантій захисту таємниць стосовно винаходів в сфері оборони, на які подані заявки на патентування (Париж, 21 вересня 1960 р.), Угоди НАТО щодо передачі технічної інформації для оборонних цілей (Брюссель, 19 жовтня 1970 р.), а також Угоди про співробітництво стосовно інформації з питань атомної енергії (С-М(64)39 - Основна угода та Адміністративні механізми реалізації угоди (С-М(68)41, 5-а редакція).

На початку 90-х років ХХ ст. НАТО розпочала політичну та військову трансформацію структур безпеки. Первісно система безпеки інформації НАТО була розроблена для документів у виді “твердих копій”, але швидкість розвитку інформаційних технологій спонукала до майже повної заміни паперових носіїв на електронні, що спричиняло не тільки позитивні (скорочення часу обміну, збільшення місткості носіїв, швидкість пошуку, класифікацію, створення баз даних та ін.), а й негативні (втрата конфіденційності, цілісності змісту інформації або цілісності системи, втрата доступу та ін.) наслідки інформатизації. Поява цих ризиків в сфері інформаційної безпеки спричинила необхідність впровадження нових заходів та процедур захисту інформації, а також вдосконалення нормативної бази, адже безпека інформації, тісно пов'язана саме із загальним керуванням потоками інформації. У березні 1997 р. була укладена Угода між Сторонами Північноатлантичного Договору щодо захисту інформації.

Політику Альянсу в галузі безпеки та оборони, оперативні концепції, та систему колективної оборони визначає Стратегічна концепція НАТО. Стратегічна концепція чітко окреслює сучасні виклики і зазначає, що нові ризики, які загрожують миру та стабільності, стають дедалі очевиднішими: утиски та конфлікти на етнічному ґрунті; поширення зброї масового ураження; глобальне поширення технологій виготовлення зброї; тероризм; спроби використати зростаючу залежність Альянсу від інформаційних систем шляхом проведення інформаційних операцій, покликаних зруйнувати такі системи, намагатися використати такі стратегії, аби протистояти перевагам НАТО в галузі звичайних озброєнь.

Після вступу в НАТО, кожна держава повинна провести оцінку співвідношення стосовно Угоди між Сторонами Північноатлантичного Договору щодо захисту інформації даного документу, згідно Плану дій заради членства, та запровадити достатньо заходів перестороги та процедур для гарантування захисту таємної інформації відповідно до положень політики НАТО з питань захисту інформації, а також визначити критерії щодо таємності інформації, якою вона буде і повинна обмінюватись в рамках Альянсу. Відмова з боку однієї або декількох держав від зобов'язання щодо дотримання правил безпеки стосовно захисту інформації може привести до скорочення кількості і якості таємної

інформації усередині НАТО. Польща, наприклад, після вступу внесла свій вклад в інформаційну безпеку Альянсу. Фахівці служби держбезпеки Польщі розробили нову систему електронної безпеки, що спирається на "спеціальні шифрові ключі", для застосування в електронній пошті, якою користуються відповідні структури країн НАТО. Показово, що при розподілі видатків між країнами-членами НАТО по Програмі інвестицій у безпеку Польща посідає шосте місце, вважається навіть, що в Польщі краща система захисту інформації, чим в інших державах-членах НАТО

В процесі підготовки до членства в НАТО були проведені певні заходи в країнах Балтії. Були прийняті Угоди по безпеці, законодавство приведено у відповідність з вимогами НАТО, удосконалений захисний режим для таємної інформації в державних установах, які включатимуться в процес інтеграції в НАТО та система інформаційного обміну і зберігання таємної інформації, встановлений список підприємств та компаній, в майбутньому потенційно здібних до поводження з таємними контрактами НАТО. Але іноді певні заходи мали специфічну форму. В Латвії, наприклад, були внесені зміни в Закон про державну таємницю, в якому з'явилося поняття «інформації обмеженого користування». Це нижчий ступінь таємності, прийнятий спеціально для "створеної в зв'язку з міжнародними договорами або отриманою Латвійською Республікою захищеної інформації, що відноситься до військової, політичної, економічної, наукової, технічної, розвідувальної (контррозвідувальної) і оперативної діяльності держави". Відповідальним за обмін класифікованою інформацією з міжнародними організаціями призначене Бюро по захисту Сатверсме (Конституції), у компетенцію якого ввійшла також акредитація комп'ютерних систем держустанов на предмет їхньої надійності від неконтрольованого доступу, контроль криптографічної системи і розробка таємних кодів. Список осіб, що не можуть одержати доступу до класифікованої інформації включає не тільки тих, хто відмовився від громадянства Латвійської Республіки, колишніх радянських співробітників і агентів служб безпеки, але також тих, "чиї персональні або професійні особливості дають підстави сумніватися в їхній можливості дотримуватись вимог режиму таємності".

Політика НАТО в області безпеки узгоджена всіма країнами-учасниками. В окремих країнах, командуваннях НАТО й агентствах НАТО можуть виникати питання по реалізації політики безпеки. У робочій групі з питань забезпечення безпеки САОД Комітету внутрішньої безпеки НАТО (NSC) за останні п'ять років розроблені і продовжують розроблятися керівні документи по безпеці, які перекривають ряд важливих питань таких як організація і керування безпекою САОД, аналіз ризику і керування ризиком, документація з питань безпеки. Система захисту інформації постійно модернізується.

III. Основні вимоги НАТО щодо захисту інформації.

Основним принципом безпеки інформації НАТО є те, що правила повинні забезпечити доступ до інформації осіб, яким вона потрібна в силу службової необхідності, і те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах, починаючи з джерела, а контроль за розподілом і поширенням інформації повинний забезпечити відсутність її витоку. Присвоєння інформації НАТО того або іншого грифа таємності виробляється відповідно до правил систем безпеки країн-учасниць. Присвоєння інформації НАТО того чи іншого грифу таємності проводиться у відповідності з правилами систем безпеки країн-членів. Власне НАТО як міжнародна організація таємну інформацію не виробляє. Система безпеки НАТО є просто продовженням систем країн-учасниць. Однак, деяка інформація може певний час залишатися конфіденційною, тому що в Альянсі прийнятий консенсус. Всі переговори і дискусії залишаються конфіденційними, поки рішення не прийняте. Наприклад, з метою збереження конфіденційності, при підготовці комюніке зустрічі міністрів, проекти документів мають

бути таємними, поки всі міністри не погодили текст, після чого інформація така перестав бути таємною.

Мінімальні стандарти НАТО по захисту інформації містять вимоги по обробці, збереженню і передачі таємної інформації. Ключовим терміном є "керування ризиком", тобто оцінка загроз і уразливості з однієї сторони і проведення контрзаходів з іншої. При цьому треба чітко уявляти розміри вартості збитку при витоку інформації, відповідність затрат необхідних ресурсів для захисту інформації потребам, та кількість засобів для одержання інформації супротивною стороною.

У зв'язку з діяльністю НАТО і міжнародним військово-політичним співробітництвом, джерелами загроз є служби розвідки інших країн, терористичні організації або окремі терористи, хакери, розроблювачі комп'ютерних вірусів і просто зловмисники. У загальному виді загрозу визначають як можливість випадкового або навмисного порушення безпеки САОД або мережі, джерело цієї загрози, її мотиви та мету. Джерела загроз угруповують таким чином:

а) внутрішні - від персоналу - з метою отримання доступу нелегальним чином до інформації, або пошкодження системи на користь іноземних розвідок, зовнішніх організацій чи терористичних угруповань;

б) зовнішні - нові форми таємної атаки у зв'язку з обробкою інформації електронним способом;

в) фізичні - проти фізичного існування САОД і мереж.

Реалізація загрози відбувається завдяки існуючій уразливості - слабкості або відсутності контролю, що може бути результатом недогляду або недоліку в глибині контролю, у його повноті або сталості, природа якого може бути технічна, функціональна або оперативна. Виходячи з цього, для захисту інформації служба безпеки повинна забезпечити максимальну неможливість:

несанкціонованого розкриття інформації у результаті дій неблагонадійного персоналу (утрата конфіденційності) ;

порушення змісту інформації, її повноти або сталості в САОД чи мережі в результаті несанкціонованих змін (утрата цілісності інформації);

втрати точності устаткування або зниження його функціональних характеристик сталості і надійності (утрата цілісності системи);

порушення доступу до інформації, ресурсів САОД чи мереж, або збільшення часу виконання критичних операцій (утрата доступності).

В залежності від конкретної ситуації питання конфіденційності, цілісності та доступності можуть мати різні пріоритети. В даний час в НАТО основну увагу приділяється питанню конфіденційності, але в майбутньому більша увага має приділятися розробці політики і керівних документів в області захисту від втрати цілісності і доступності.

Виходячи з загроз й уразливості з однієї сторони, оцінки втрат (конфіденційності, цілісності, приступності) - з іншої, необхідна повна, ефективна і збалансована система мір безпеки. З огляду на це найбільш важливими є контроль доступу до інформації, контроль носіїв інформації та звітність. Доступ до інформації контролюється і надається тільки особам з відповідним допуском і при службовій необхідності. В області САОД і мереж для цього застосовуються механізми ідентифікації й аутентифікації, автономний механізм керування доступом у системі, установлений згідно принципу службової необхідності

інформації, механізм керування доступом на основі форми допуску користувача. При цьому система повинна бути здатна розпізнати форму допуску і вирішити, чи достатня вона для доступу до інформації з визначеним рівнем таємності.

Питання забезпечення захисту інформації входять до юрисдикції Комітету внутрішньої безпеки НАТО (NSC), який є дорадчим органом при Північноатлантичній Раді, з питань, що стосуються безпеки НАТО. Головою Комітету є директор Служби безпеки НАТО (NOS), яка надає підтримку Комітету з боку Міжнародного секретаріату НАТО. Комітету внутрішньої безпеки також підпорядкована Робоча група з питань гарантування безпеки автоматичної обробки даних.

Інструкція із таємного діловодства в НАТО вимагає від країни-члена створити національний уповноважений орган, відповідальний за безпеку таємної інформації, через який Служба безпеки НАТО здійснює контакти з країною. Усередині НАТО функції національного уповноваженого органа по безпеці інформації наступні:

забезпечення безпеки таємної інформації НАТО у національних органах, військових і цивільних структурах, як всередині країни, так і за її межами;

керівництво створенням (або ліквідацією) органа управління та режимних відділів;

проведення періодичних інспекцій по перевірці виконання правил захисту таємної інформації НАТО в національних організаціях всіх рівнів, як військових, так і цивільних;

забезпечення лояльності всіх осіб - громадян даної країни, за родом своєї діяльності допущених до таємної інформації, відповідно до стандартів та правил захисту інформації НАТО;

забезпечення розробки планів захисту інформації в надзвичайних обставинах, з метою запобігання втрати конфіденційності таємної інформації НАТО.

Представники національного уповноваженого органа по безпеці інформації беруть участь у нарадах Комітету безпеки НАТО, на яких виробляються політика й інструкції в області безпеки. Обумовлена законом загальна структура системи безпеки країни і розподіл повноважень між органами влади впливають на призначення національного уповноваженого органа по безпеці. Є країни НАТО, в яких уповноважений орган по безпеці інформації знаходиться в міністерстві закордонних справ, оборони і юстиції. В інших країнах керівником уповноваженого органа по безпеці є прем'єр-міністр, міністр оборони або міністр внутрішніх справ. На обсяг функцій відповідального уповноваженого впливають розмір країни і кількість населення, географічне розташування місць обробки таємної інформації і не в останню чергу, розподіл повноважень між органами в області національної безпеки. Часто значна частина функцій відповідального уповноваженого делегується в міністерство оборони.

Пріоритетним є впровадження найсучасніших систем спостереження, засобів обробки інформації і зв'язку, а також високоточної зброї. У звіті корпорації RAND «Майбутнє НАТО: вплив на стан і можливості армії США» підкреслюється, що Альянс зштовхнувся сьогодні з новими загрозами, що змушують зміщати акценти від питань забезпечення територіальної безпеки у бік нарощування технічної моці. Аналітики RAND вважають, що країни НАТО повинні фінансувати процес розвитку інформаційної інфраструктури національних збройних сил, для того щоб зробити їх більш легкими й мобільними.

Витрати на утримання інформаційно-комунікаційних систем покриваються коштами Програми інвестицій у безпеку НАТО. В дослідженні Брукса Ліске (Brooks Lieske) з Frost & Sullivan відзначається зміна орієнтації в реалізації загроз з порушення цілісності системи на порушення конфіденційності, в основному читанням пошти і збором службової інформації. В ході дослідження був виявлений стійкий ріст витрат на

забезпечення інформаційної безпеки в таких структурах як Агентство по національній безпеці (National Security Agency) і НАТО. Витрати урядів і військово-промислових комплексів країн НАТО на технології шифрування протягом 5 років (до 2007 р.) зростуть з \$176 млн. до \$457,6 млн. На думку автора дослідження, уряди стурбовані не стільки зламами систем і вірусами, скільки викраденням інформації.

IV. Співробітництво України та НАТО в сфері інформаційної безпеки.

Співробітництво між НАТО та країнами-партнерами в рамках Ради євроатлантичного партнерства (РЄАП) та Програми "Партнерство заради миру" (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації. Участь країн в оборонному плануванні і військових навчаннях НАТО в рамках програми ПЗМ надає доступ до деяких технічних даних НАТО щодо сумісності. Для збільшення транспарентності військового планування й оборонних бюджетів і забезпечення демократичного контролю над збройними силами сторони можуть брати участь у взаємному обміні інформацією про кроки, що вони почали або починають. Перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи по безпеці інформації повинні бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити захист інформації відповідно до вимог сторони, яка її передає.

Приєднання країни до програми ПЗМ передбачало ратифікацію "Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або програмі ПЗМ". Згідно цієї Угоди, сторони погоджуються консультуватися по політичних питаннях і питаннях безпеки, розширювати й інтенсифікувати політичне і військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах має на увазі обмін "таємною" інформацією і/або інформацією обмеженого доступу серед учасників. Відповідальним органом при захисті таємної інформації, якою обмінюються сторони при співробітництві в рамках РЄАП/ПЗМ, є Служба безпеки НАТО (NOS). Країна-партнер інформує Службу безпеки НАТО про те, який національний орган має повноваження в області безпеки інформації. Указом Президента України від 27 січня 2001 року "Про Державну програму співробітництва України з Організацією Північноатлантичного Договору (НАТО) на 2001-2004 роки" (ДПС-2004) на Державний комітет зв'язку та інформатизації України покладено відповідальність за реалізацію 5 розділу цієї програми, а саме "Співробітництво в галузі телекомунікаційних та інформаційних систем". Також, між НАТО та країною-партнером укладається окрема адміністративна угода по стандартах взаємного забезпечення безпеки інформації, якою обмінюються сторони і призначається офіцер зв'язку між Управлінням безпеки НАТО і національним уповноваженим органом по безпеці інформації. У травні 1998 р. на засіданні Комісії Україна - НАТО на рівні міністрів закордонних справ було погоджено призначення в Київ офіцера НАТО по зв'язках з метою сприяння повномасштабній участі України в ПЗМ і вдосконалення співпраці між військовими НАТО та України в цілому.

Вся інформація, якою обмінюються сторони в рамках РЄАП/ПЗМ, є інформацією обмеженого доступу і тільки для урядового використання. Тому її повинні отримувати тільки організації й особи, які беруть участь у цих програмах і мають з нею справу за родом своєї діяльності. Установлення ступеня таємності документа або зниження ступеня таємності є прерогативою автора документа. На відміну від стандартів щодо захисту інформації, прийнятих в НАТО, де існує чотири рівні захисту, в мінімальних стандартах по обробці і захисту таємної інформації, якою обмінюються сторони в рамках програм РЄАП/ПЗМ, опущений рівень "абсолютно таємно", що спричинено тим, що кількість абсолютно таємної інформації в НАТО є дуже обмеженою, а додаткові вимоги по безпеці в зв'язку з цим рівнем таємності не виправдано ускладнили б правила обміну інформацією між країнами-партнерами і НАТО.

Певним досягненням стала ратифікація Законом України від 12 вересня 2002 р. “Угоди про безпеку між Урядом України та Організацією Північноатлантичного Договору”, яка визначає основні вимоги щодо обміну та захисту таємною та/або конфіденційною інформацією між Україною та НАТО в рамках РЄАП та ПЗМ і може стати основою прийняття відповідних документів в процесі подальшого співробітництва чи повної інтеграції України в Альянс.

V. Інформаційна безпека України: проблеми та перспективи.

Проблема вдосконалення державної інформаційної політики набула сьогодні ваги одного із національних пріоритетів. Якщо розглядати в Україні діяльність щодо захисту інформаційно-телекомунікаційних систем, то наявна нормативна база у сфері захисту інформації відповідає світовим підходам до їх проектування, виробництва, оцінювання та експлуатації. Концепція Національної безпеки України визначає загрози національній безпеці та основні напрями державної політики національної безпеки України щодо інформаційної сфери. Прийняті також документи, які складають нормативну базу в цій сфері: Національна програма інформатизації, Указ Президента "Про міри по забезпеченню інформаційної безпеки держави", Закон України "Про державну таємницю", Закон України "Про захист інформації в автоматизованих системах", Положення "Про технічний захист інформації" та інші.

Однак наявність відповідної нормативної бази - це тільки перший крок в напрямку забезпечення належного рівня безпеки держави в цій сфері. Найбільш важливим є реалізація та впровадження необхідних заходів щодо здійснення політики інформаційної безпеки і особливо захисту інформації.

Найбільш незахищеною ланкою інформаційної інфраструктури України на сьогодні є мережі передачі даних та канали зв'язку. Це обумовлено тим, що сучасне цифрове телекомунікаційне обладнання, яке впроваджується в мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, тобто створює умови для несанкціонованого впливу та контролю за фактом передачі інформації та її змістом. Обов'язковою умовою для забезпечення безпеки зазначених ресурсів є одержання об'єктивної оцінки рівня захищеності інформації в мережах передачі даних, яка може бути одержана шляхом проведення відповідної експертизи. З цих позицій одним з першочергових завдань у сфері забезпечення інформаційної безпеки є створення в державі захищеної мережі передачі інформації, що значно б знизило ймовірність несанкціонованого втручання в функціонування інформаційно-технічних систем державних органів, установ, підприємств і організацій. Можливість та певний досвід побудови такої системи в Україні є, оскільки подібні системи вже довгий час функціонують в державі. До них можна віднести Державну систему урядового зв'язку, систему конфіденційного зв'язку Служби безпеки України, комплекс спеціальних видів зв'язку Міністерства оборони України, системи спеціального зв'язку міністерств та відомств. Використання ефективної шифрувальної техніки гарантованої стійкості, а також обмеження доступу до міжнародних інформаційних мереж є факторами, які суттєво знижують можливості несанкціонованого доступу до вітчизняних мереж. Крім того, відповідними підрозділами Служби безпеки здійснюються заходи, спрямовані на своєчасне виявлення та локалізацію місцезнаходження технічної розвідки ворожих країн і терористичних угруповань.

Зазначені проблеми еволюційні, спричинені постійним розвитком процесу інформатизації. Однак існують проблеми, вирішення яких перебуває у соціальній площині. Згідно висновку Ради національної безпеки і оборони, який зроблено на засіданні з питання "Про

заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" 19 квітня 2002 р. в інформаційній сфері держави залишається неподоланим розвиток низки загроз, що зумовлено недовістю численних державних рішень, спрямованих на впорядкування справ у цій сфері. Численні доручення Президента України і рішення Уряду з питань вдосконалення ситуації в інформаційній сфері держави хронічно не виконуються. Створювані в рамках Національної програми інформатизації інформаційно-аналітичні системи окремих органів виконавчої влади (типовий комплекс Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій, інформаційно-обчислювальна мережа Генерального штабу Збройних Сил України та інші) реалізуються за відсутності системності, єдиної концепції та моделі інформаційних потоків. З метою вирішення даних проблем була створена Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, що свідчить про критичність ситуації і необхідність першочергового вирішення окреслених питань.

В рамках співробітництва Україна-НАТО вже проводяться певні заходи. Зокрема, постійно проводяться курси НАТО "Комунікаційні та інформаційні системи програми ПЗМ", основною метою яких є ознайомлення фахівців країн-партнерів з організаційною структурою, основними принципами роботи та управління комунікаційними та інформаційними системами НАТО, а саме: загальна організаційна структура комунікаційних та інформаційних систем (КІС) НАТО; структура Організації НАТО з питань консультацій, управління та контролю (NATO C3 Organization); бюджет та постачання КІС НАТО; стандартизаційні угоди (STANAGs) та процедурні правила НАТО; забезпечення операцій НАТО зв'язком та обміном інформацією. Відповідні курси з питань безпеки персоналу, фізичної безпеки, захисту документів, промислових таємниць та інформації є одним з додаткових заходів процесу набуття членства. В перспективі заплановані подальша реалізація проекту "Уран" щодо створення та розбудови комп'ютерної мережі установ та закладів науки, освіти і культури та її підключення до загальноєвропейської академічної мережі GEANT, застосування інформаційної системи програми ПЗМ (PRIME). Таким чином, подальше поглиблення та активізація роботи по співробітництву України з НАТО, зокрема проведення заходів, спрямованих на реформування та подальший розвиток систем зв'язку України є необхідними для досягнення рівня відповідності вимогам НАТО.

VI. Вирішення проблемних питань: стратегія і тактика .

На Празькому самміті НАТО були ухвалені основні напрямки подальшої адаптації Альянсу до нових умов та його подальшої трансформації. Розширення відбувається не тільки в напрямку прийняття нових країн-членів, а й шляхом розширення функцій союзу, зокрема визначення як першочергового завдання боротьбу з міжнародним тероризмом і розширення зони відповідальності Альянсу. Здійснення означених функцій потребує комплексної стратегії, що базується не тільки на використанні військової сили, але й на нових формах співпраці, зокрема в сфері внутрішньої безпеки з огляду на трансатлантичний зв'язок. Курс на євроінтеграцію, обраний Україною передбачає не тільки проголошення, але й реалізацію певних заходів. Попри те, що Україна прагне постійно розвивати співробітництво з Альянсом в основному в рамках РСАП та ПЗМ, всі взяті на себе зобов'язання не виконуються в повному обсязі, чим вичерпується ліміт довіри з боку Альянсу. Для того, щоб стати претендентом на вступ необхідно враховувати, що на даний момент, не дивлячись на "особливе партнерство" ступінь відповідності стандартам НАТО у визначених сферах ще далекий від необхідного. Щодо предмету даного дослідження, потрібен всебічний аналіз та вдосконалення стану інформаційної безпеки в Україні, в першу чергу, для забезпечення безпеки держави взагалі, оскільки неспроможність подолати загрози підвищує рівень уразливості держави і

робить потенційним об'єктом прямого чи непрямого нападу. По-друге, з огляду на те, що головним стратегічним напрямом забезпечення національної безпеки та сутнісним орієнтиром зовнішньої політики України є інтеграція у європейські структури, необхідно досягнення відповідності стандартам НАТО по забезпеченню інформаційної безпеки.

Отже, напрямками вирішення проблемних питань мають бути:

- 1.Формування і реалізація єдиної державної політики по забезпеченню захисту національних інтересів від загроз в інформаційній сфері, координація діяльності органів державної влади по забезпеченню інформаційної безпеки та удосконалення законодавства в сфері забезпечення інформаційної безпеки.
- 2.Удосконалення інформаційної структури, прискорення розвитку нових інформаційних технологій та їх поширення.
- 3.Установлення необхідного балансу між потребою у вільному обміні інформацією і припустимими обмеженнями її поширення;
- 4.Розвиток систем електронної сертифікації та криптографії, включаючи підготовку персоналу.
- 5.Уніфікація засобів пошуку, збору, збереження, обробки й аналізу інформації з урахуванням входження України в глобальну інформаційну інфраструктуру та відповідності світовим стандартам, зокрема НАТО.
- 6.Розвиток вітчизняної індустрії телекомунікаційних і інформаційних засобів, їх пріоритетне в порівнянні з закордонними аналогами поширення на внутрішньому ринку, а також прискорення процесів модернізації матеріально-технічної бази та забезпечення захисту інформаційних ресурсів та захист державних інформаційних ресурсів і, насамперед, в органах державної влади, та на підприємствах оборонного комплексу.
- 7.Ефективна протидія інформаційній експансії та спробам використання національного інформаційного простору.