УДК 621.391. **Богданович В.Ю, Алексєєв М.М.**

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ОБҐРУНТУВАННЯ РЕЖИМІВ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Розглянуто методологічний підхід до оцінювання можливості виникнення надзвичайних ситуацій кібернетичного характеру та вибору режимів функціонування системи забезпечення кібернетичної безпеки, які дозволять у межах виділених ресурсів локалізувати відповідні кіберзагрози та зменшити до мінімуму їх негативні наслідки.

Ключові слова: надзвичайна ситуація, кіберзагроза, система забезпечення кібернетичної безпеки, режим функціонування системи.

Постановка проблеми.

Відповідно до [1] новітні інформаційно-телекомунікаційні (ІТ) технології останнім часом стали важливою складовою суспільного розвитку і розвитку світової економіки у цілому. Разом з тим значною мірою вони змінили механізми функціонування багатьох суспільних інститутів та інститутів державної влади. Новітні ІТ технології увійшли до числа найбільш суттєвих факторів, які впливають на формування сучасного високоорганізованого інформаційного середовища та дають можливість на якісно новому рівні вести повсякденну оперативну роботу, здійснювати аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів, а також добувати вихідні дані, необхідні для прийняття раціональних і науково-обґрунтованих управлінських рішень.

Сьогоднішні темпи інформатизації провідних країн та загальносвітовий розвиток ІТ технологій обумовлюють актуальність проблеми побудови та розвитку глобальної системи забезпечення кібернетичної безпеки держави, створення та удосконалення методів, засобів та заходів кібернетичного захисту.

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізовувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів [2] .

У сучасних умовах інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку.

Використання ІТ технологій визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил. Спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку і прогнозування наслідків безпосередньо залежать від ефективності використовуваної інформаційної інфраструктури.

Звісно, рівень інформатизації в Україні ще не такий як в країнах Західної Європи та США. Водночас, як зазначається в [3], наша держава має власну історію розвитку базових засад інформаційного суспільства: діяльність всесвітньо відомої школи кібернетики; формування на початку 90-х років минулого століття концепції та програми інформатизації; створення різноманітних ІТ технологій і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення.

При цьому, сучасні темпи зростання рівня інформатизації в Україні вже випереджають

відповідні показники для деяких східноєвропейських країн, збільшуються кількість та масштаби представлення у кіберпросторі вітчизняних об'єктів критичної інфраструктури, у тому числі в оборонній галузі.

Зважаючи на викладене та враховуючи рівень присутності фізичних і юридичних осіб України у кіберпросторі, доступність Інтернету практично у всіх населених пунктах нашої держави, є всі підстави для того, щоб розглядати питання забезпечення кібернетичної безпеки України в якості актуальної проблеми. Відповідно, завдання оцінки викликів, небезпек та загроз у національному сегменті кіберпростору є не менш важливим, ніж у інших країнах світу.

Аналіз останніх досліджень і публікацій.

Відповідно до [4] створення національної системи кібербезпеки віднесено до одного з ключових завдань політики національної безпеки України у внутрішньополітичній сфері.

Поруч з викладеним, не зважаючи на наявність широкої правової основи у сфері інформаційної безпеки держави, яку становлять Конституція України, Закони України «Про основи національної безпеки України», «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», відповідні міжнародні договори, укази і розпорядження Президента України, постанови та розпорядження Кабінету Міністрів України, інші нормативно-правові акти (НПА), станом на сьогодні, на розгляді у Верховній Раді України залишається ухвалений урядом проект Закону України «Про кібернетичну безпеку України».

Також фахівцями Національного Інституту стратегічних досліджень при Президентові України протягом 2012-2013 рр. напрацьовано проект Стратегії забезпечення кібернетичної безпеки України. Попереднє обговорення її положень відбулось під час Експертних консультацій Україна-НАТО з питань кіберзахисту (м.Ялта, 4-7 листопада 2013 р).

Безпосередньо в цих документах уперше визначаються основні засади державної політики у галузі захисту життєво важливих інтересів особи, суспільства і держави, пов'язаних з належним функціонуванням інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем.

Так, у [5] кібернетична безпека держави визначається як стан захищеності об'єктів критичної інформаційної інфраструктури країни (кіберпростір держави), сформований комплексом технологічних, технічних та інформаційних заходів і засобів кіберзахисту від зовнішніх та внутрішніх несанкціонованих посягань, реальних та потенційних кібернетичних загроз.

При цьому, об'єктами критичної інформаційної інфраструктури (ОКІІ) вважається сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави.

ОКІІ поділяють на такі групи, як:

- державні електронні інформаційні ресурси, автоматизовані системи управління або електронні інформаційні ресурси де обробляється (зберігається) інформація, яка є власністю держави, або інформація, несанкціоновані дії щодо якої можуть створювати загрозу національній безпеці та обороноздатності країни (у тому числі відкрита інформація);

- автоматизовані системи управління, що використовуються суб'єктами Воєнної

організації держави;

- телекомунікаційні системи загального користування та спеціальні телекомунікаційні системи;

- автоматизовані системи управління, що здійснюють керування виробничими та (або) технологічними процесами на об'єктах підвищеної небезпеки;

- інші інформаційно-телекомунікаційні системи та автоматизовані системи управління.

Основні реальні та потенційні загрози національній безпеці України у політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах проявляються у кіберпросторі з урахуванням особливостей використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Серед таких загроз виділяються наступні:

використання кіберпростору у воєнних цілях, створення іншими державами кібервійськ, кіберпідрозділів у традиційних родах військ;

розроблення іноземними державами нових видів зброї кібернетичного характеру;

існування в інших країнах планів наступальних та розвідувальних військових операцій у кіберпросторі;

освоєння іноземними спеціальними службами методів розвідувально-підривної діяльності у кіберпросторі, методів маніпулювання суспільною свідомістю за допомогою кіберпростору;

можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегменту кіберпростору;

спроби втручання у внутрішні справи держави з використанням соціальних мереж, поширення у національному сегменті кіберпростору культу насильства, жорстокості, порнографії;

активізація проявів кібертероризму та поширення фактів кіберзлочинності;

критична залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції, поширення фактів включення у програмно-технічні засоби скритих шкідливих функцій;

зростання ризиків виникнення надзвичайних ситуацій техногенного характеру через зниження рівня захищеності об'єктів критичної інформаційної інфраструктури держави.

Невирішена раніше проблема.

Кожна з перерахованих вище загроз може виникати як самостійно, так і сприяти виникненню іншої, тобто, здатна спричинити ланцюговий процес. Безумовно, кожна з них потребує детального аналізу та організації протидії. На превеликий жаль, відкритих публікацій по даній тематиці автори не виявили.

Мета статті.

У даній статті автори ставлять за мету провести аналіз можливостей виникнення надзвичайних ситуацій кібернетичного характеру в наслідок реалізації визначених загроз та розробити методологічний підхід до встановлення режимів функціонування сил та засобів системи забезпечення кібернетичної безпеки держави для дій з локалізації ситуацій та ліквідації їх негативних наслідків.

Викладення основного матеріалу.

Як показано в [6], ***надзвичайні ситуації кібернетичного характеру в Україні*** **(**рис.1) можуть виникнути за рахунок наступних джерел кібернетичних загроз:

- міжнародні злочинні групи хакерів;
- окремі підготовлені у сфері інформаційних технологій злочинці;
- іноземні державні органи;
- терористичні та екстремістські угруповання;
- транснаціональні корпорації та фінансово-промислові групи тощо.

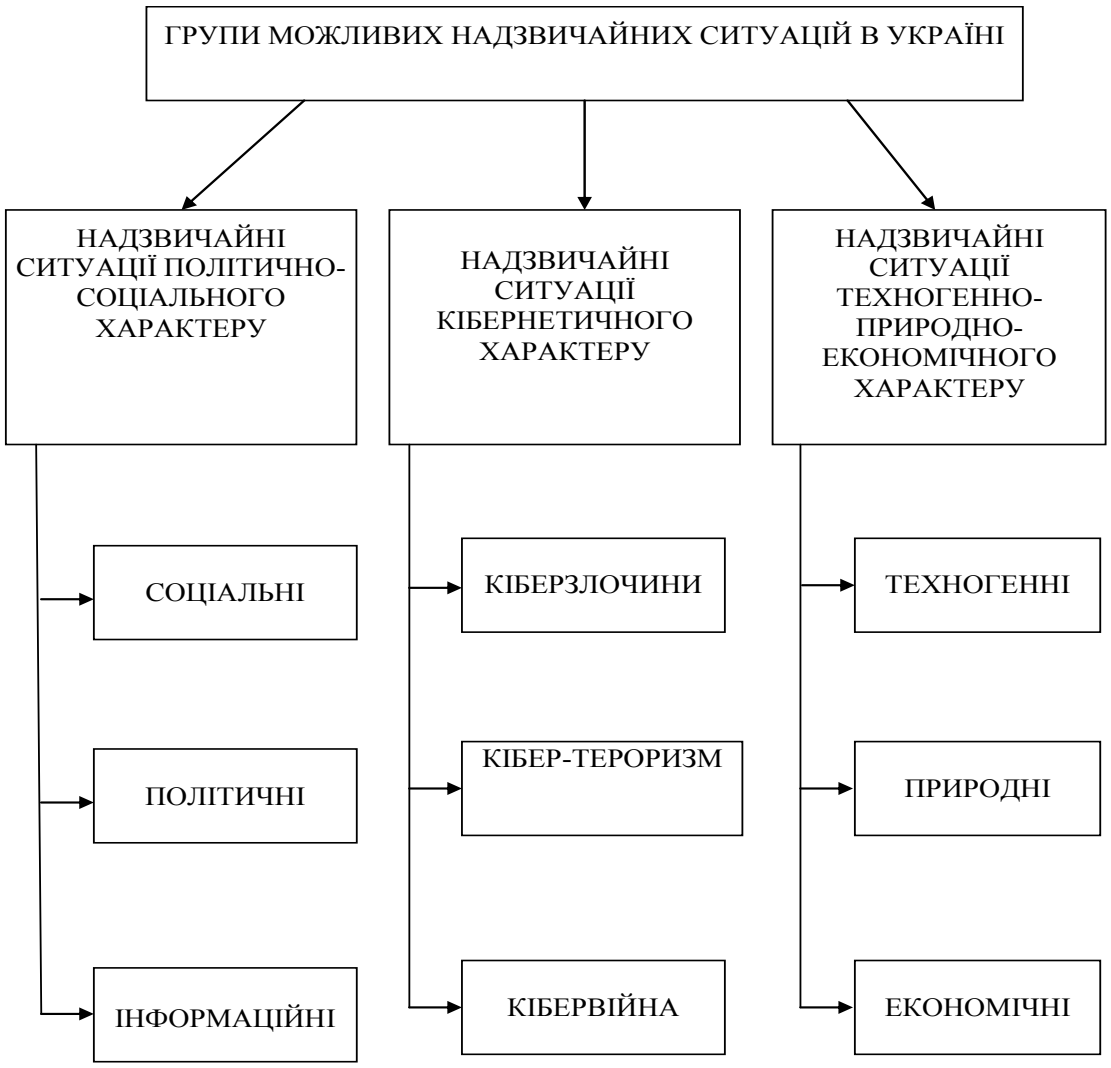

Рис. 1. Класифікація надзвичайних ситуацій, які можуть виникнути в Україні

Кібертероризм. Ціла низка вітчизняних підприємств, порушення роботи яких може становити загрозу життю та здоров'ю громадян, може стати потенційною ціллю для здійснення терористичних актів, в тому числі – із застосуванням сучасних інформаційних технологій. Не меншою загрозою є вчинення протиправних дій на шкоду третім країнам, що здійснюються із використанням вітчизняної інформаційної інфраструктури, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

Кібервійна. Воєнна сфера зазнає чи не найдраматичніших змін внаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформує свої потенціали у сфері оборони в напрямі посилення кібернетичних можливостей ведення бойових дій та захисту від аналогічних дій з боку супротивника, оскільки все актуальнішими стають нові типи загроз. З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема, створення ЄАСУ ЗС України, оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює

кіберпростір на окрему, поряд з традиційними "Земля", "Повітря", "Море", "Космос", сферу ведення бойових дій, а у найближчому майбутньому, рівень обороноздатності країни буде визначатись у т.ч. наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатністю протистояти кіберзагрозам у сфері оборони.

Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків держави в ключових сферах життєдіяльності, що мають особливе значення для забезпечення кібернетичної безпеки. З цією метою, держава, у партнерстві із суспільством, недержавним та приватним сектором, а також громадянами, з метою посилення кібербезпеки України, при формуванні власної політики кібербезпеки повинна керуватись наступними пріоритетами [6]:

у зовнішньополітичній сфері:

підвищувати роль України як активного учасника формування стандартів світової політики по відношенню до кіберпростору;

підтримувати міжнародні ініціативи у сфері кібербезпеки з урахуванням національних інтересів України;

сприяти недопущенню мілітаризації кіберпростору;

неухильно дотримуватись взятих на себе міжнародних зобов'язань у сфері кібернетичної безпеки та боротьби з кібернетичною злочинністю;

підвищувати рівень міжнародного співробітництва у сфері забезпечення кібернетичної безпеки на загальнодержавному та відомчому рівнях;

сприяти створенню міжнародних правил поведінки держав у кіберпросторі та удосконаленню міжнародної нормативно-правової бази у відповідності до кібербезпекових викликів національній та міжнародній безпеці;

підтримувати як існуючі багатосторонні навчання із протидії кібернападам на державну та приватну інформаційну інфраструктуру, так і ініціювати нові види таких навчань;

у сфері державної та внутрішньополітичної безпеки:

створити Національну систему кібернетичної безпеки України;

встановити обов'язкові вимоги щодо кіберзахисту критичних об'єктів національної інформаційної інфраструктури незалежно від форми власності, порядок захисту та контролю за його дотриманням;

здійснювати заходи щодо реформування системи захисту інформації з обмеженим доступом з урахуванням реалій сьогодення задля уникнення її витоків;

посилювати технічні та технологічні можливості, науковий та професійний потенціал Служби безпеки України, розвідувальних органів та Державної служби спеціального зв'язку і захисту інформації у кіберпросторі;

посилювати боротьбу з кібертероризмом та кібершпигунством, захист від їх проявів критичних об'єктів національної інформаційної інфраструктури;

забезпечити імплементацію положень Конвенції Ради Європи про кіберзлочинність [7] у національне законодавство, зокрема, щодо:

- надання повноважень органам дізнання та слідства щодо видачі обов'язкових до виконання провайдерами приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину;
- обов'язковості збереження провайдерами даних про трафік на строк до 90 днів із можливістю дальшого продовження терміну до 3 років;
- зобов'язання суб'єкта, який зберігає комп'ютерні данні, не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом визначеного законодавством періоду;
- надання провайдером органу дізнання або слідства інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

удосконалювати кримінальне законодавство, виділити окремі склади злочинів, де об'єктами протиправних посягань є критичні елементи національної інформаційної інфраструктури;

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

у воєнній сфері:

здійснювати підготовку до застосування ЗС України в умовах кібервійни;

створювати можливості для відбиття збройної агресії в кіберпросторі з урахуванням нових викликів та загроз;

захищати військову інформаційну інфраструктуру від реальних та потенційних кіберзагроз;

створити систему підготовки кадрів у сфері кібербезпеки для потреб ЗС України та інших органів сектору безпеки і оборони України;

у соціальній, гуманітарній та науково-технологічній сферах:

розвивати та координувати науково-дослідні роботи у галузі кібербезпеки;

створювати сприятливі умови для молодих фахівців в ІТ-сфері, що має сприяти їх працевлаштуванню в Україні;

забезпечити внесення змін до навчальних планів та програм середньої та вищої школи, підготовки наукових та науково-педагогічних кадрів, що спрямовані на інформування основних цільових груп про кіберзагрози та методи протидії ним;

розробляти загальнодержавні програми підвищення рівня обізнаності населення щодо кіберзагроз (в тому числі через створення всеукраїнської системи змагань серед молоді, що присвячені проблемі кібербезпеки, запровадження «Національного тижню обізнаності з кібербезпекою»);

підтримувати зусилля громадянського суспільства та бізнесу щодо підвищення обізнаності населення з актуальних кіберзагроз;

стимулювати всі зацікавлені сторони до активної участі у щорічних Днях безпечного інтернету;

сприяти більш активній політиці державних безпекових інституцій щодо інформування населення про кіберзагрози;

забезпечити безперервне підвищення кваліфікації державних службовців та працівників, що задіяні на ключових об'єктах критичної інфраструктури;

сприяти розробці вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави.

Поруч з викладеним, одними з першочергових заходів на шляху побудови системи кібербезпеки держави вважається вдосконалення державного управління у даній сфері та впорядкування нормативно-правового поля. Як вже визначалось вище, з метою забезпечення кібернетичної безпеки України має бути створено цілісну Національну систему кібернетичної безпеки.

До складу Національної системи кібернетичної безпеки мають бути включені: Служба безпеки України; Міністерство внутрішніх справ України; Міністерство оборони України; Генеральний Штаб Збройних Сил України; Державна служба спеціального зв'язку та захисту інформації України.

У разі необхідності до участі у здійсненні заходів, пов'язаних із виявленням, запобіганням і нейтралізацією загроз кібернетичного характеру, можуть бути залучені інші суб'єкти забезпечення кібернетичної безпеки.

З метою координації дій суб'єктів забезпечення кібернетичної безпеки, необхідним є створення Державного агентства з кіберзахисту – державного органу для забезпечення своєчасного виявлення, запобігання і нейтралізації кібернетичних загроз, управління Національною системою кібернетичної безпеки, забезпечення роботи Міжвідомчої колегії з питань протидії кібернетичним загрозам при Президентові України.

При цьому слід пам'ятати історичний досвід, який переконливо свідчить про те, що ефективність забезпечення національної безпеки, у сферах криміналу, тероризму та військовій у своїй більшості визначається якістю оцінки стану у цих сферах і точністю прогнозування тенденцій їх розвитку [8]. Сформульовані на підставі таких оцінок висновки дають відповідним органам можливість завчасно визначити адекватні напрями розвитку

системи безпеки та заходи щодо запобігання та реагування на надзвичайні ситуації в Україні.

Об'єктивність аналізу обстановки, що потребує втручання відповідних структур, є основною вимогою для обґрунтування організаційно-штатної структури системи кібернетичної безпеки держави взагалі й зокрема сил та засобів для ліквідації надзвичайних ситуацій кібернетичного характеру та визначення режимів їх функціонування в залежності від поточного рівня небезпеки.

Усе це обумовлює необхідність постійного моніторингу кримінальної, терористичної та воєнної ситуації в кібернетичному просторі держави, удосконалення методичного апарату її оцінювання й прогнозування з метою розробки конкретних пропозицій щодо підтримки необхідного рівня обороноздатності країни.

У цілому стан і тенденції розвитку надзвичайної ситуації кібернетичного характеру визначаються комплексним впливом стабілізуючих й дестабілізуючих факторів. Наукові підходи до вирішення задач у цій галузі повинні базуватися, у першу чергу, на методології системного аналізу й теорії прогнозування.

Адекватна оцінка поточного стану кібернетичної безпеки (ПСКБ) України можлива тільки на основі всебічного аналізу причинно-наслідкових зв'язків, виділення з усієї різноманітності домінуючих.

Відповідно до [9] центральним моментом ПСКБ, що складається, є визначення ступеня небезпеки переходу ПСКБ у надзвичайний стан, коли виникає потреба в застосуванні сил і засобів з його локалізації з подальшим усуненням його наслідків.

У цілому оцінка ПСКБ з подальшою можливістю прогнозування тривалості загрозливого періоду надзвичайної ситуації може здійснюватися керівництвом Державного агентства з кіберзахисту із залученням аналітиків та експертів від силових відомств у такій послідовності:

1. Визначається множина можливих джерел {**I**}, які в принципі можуть бути потенційними носіями виникнення в державі надзвичайної ситуації кібернетичного характеру.

2. Здійснюється аналіз кожного джерела з множини {**I**}.

3. За результатами аналізу ПСКБ по кожному джерелу з множини {**I**}, визначається пріоритетний ряд потенційних джерел загрозливого характеру з оцінкою масштабу вкладу їх у можливість виникнення надзвичайної ситуації по кожному з них.

4. Визначається й аналізується стан взаємовідносин з кожним джерелом із множини {**I**} з урахуванням особливостей ситуацій кримінального, терористичного та воєнного характеру в кіберпросторі держави. Як правило, це політична, територіальна, історична, етнічна, економічна, воєнна, релігійна та інші сфери відносин. У кожній сфері аналізується характер і оцінюється можливість їх вирішення з використанням спеціальних сил та засобів. У цілому інформаційна технологія оцінювання допускає одночасний розгляд до 9 сфер. Якщо таких набирається більше дев'яти, то доцільно провести композицію (об'єднання) найбільш близьких із тим, що звести їх кількість до дев'яти.

5. На основі аналізу взаємовідносин із кожним ***i-м*** джерелом (i = 1,I) у кожній сфері формується вектор показників рівня кібернетичної небезпеки (кримінальної, терористичної та воєнної) $\{U(t_1)\}$ на момент часу t_1, що аналізується, з оцінкою тенденції їх зміни (наприклад, погіршуються, покращуються, залишаються на колишньому рівні) .

Кількість показників для кожної сфери взаємовідносин повинна бути не більше дев'яти, у противному випадку необхідно або проводити їх композицію, або будувати багаторівневу ієрархію з урахуванням їх взаємозалежності [10] .

6. За інформацією, яка отримана попередньо, проводиться оцінка рівня кібернетичної небезпеки (загрози) з боку ***i-го*** джерела (i = 1,I) [3]. В якості критерію оцінки рівня кібернебезпеки ПСКБ з боку ***i-го*** джерела взято комплексний показник рівня кібернебезпеки ПСКБ:

$$K_i(t_1) = F\{(U_{сф1i}(t_1), (U_{сф2i}(t_1), ..., (U_{сфsi}(t_1)\},$$

де, $\{(U_{сф1i}(t_1), (U_{сф2i}(t_1), ….., (U_{сфsi}(t_1)\} = \{U_i(t_1)\}$ – вектор показників по кожній з $S \leq 9$ сфер взаємовідносин, який описує співвідношення з ***і-м*** джерелом, сумарний вплив якого може привести до надзвичайної ситуації кібернетичного характеру; S – кількість сфер взаємовідносин з ***і-м*** джерелом.

На основі цих міркувань на рис.2 наведено гіпотетичний приклад оцінки ПСКБ ***і-го*** джерела протягом часу $[t_0, t_{ус.\ наслідків\ надзв.\ ситуації}]$.

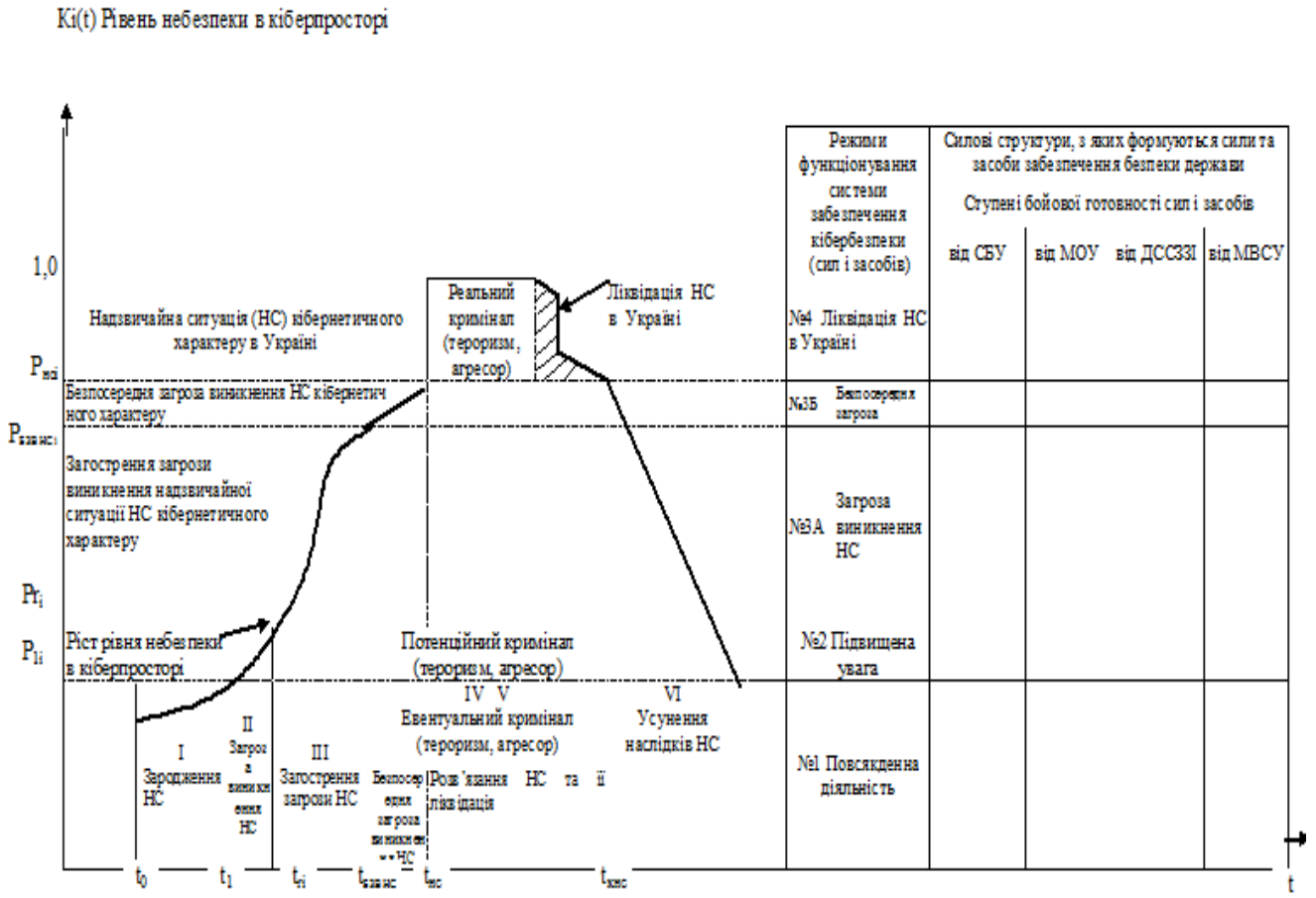

Рис. 2. Етапи розвитку ПСКП до надзвичайної та режими функціонування системи забезпечення кібернетичної безпеки держави.

Аналізуючи рис.2, можна виділити шість етапів у розвитку надзвичайної ситуації кібернетичного характеру, а саме:

перший етап – зародження надзвичайної ситуації кібернетичного характеру. На цьому етапі ПСКБ у державі наближається до надзвичайного, хоча нормальне життя не порушується;

другий етап пов'язаний із загостренням напруги і початком загроз зі сторони криміналітету (терористів, протиборчих сторін);

на третьому етапі конфронтації стосунки загострюються, криміналітет (терористи, протиборчі сторони) переходять до провокацій у кібернетичному просторі, але до прямих протиправних дій справа не доходить;

четвертий етап самий небезпечний і характеризується кризовим станом обстановки в кіберпросторі, безпосередньою загрозою виникнення надзвичайної ситуації кібернетичного характеру в державі;

п'ятий етап – розв'язання надзвичайної ситуації із застосуванням протиборчими сторонами всіх наявних сил та засобів у всіляких проявах;

шостий етап – усунення наслідків надзвичайної ситуації.

При $K_i(t) \leq P_{1i}$ (де P_{1i} – поріг нормальної ПСКБ). В умовах обмеження людських, фінансових, матеріальних й інших ресурсів влада держави не має можливості постійно

тримати свою систему забезпечення кібернетичної безпеки в найвищому ступені бойової готовності. Було б доцільно, щоб стан готовності відповідних сил та засобів адаптувався до рівня небезпеки кібернетичного характеру. [11]

Так ось, саме режим функціонування системи кібернетичної безпеки №1 установлюється при значенні комплексного показника рівня небезпеки не більше P_{1i}. Забезпечення необхідного рівня безпеки здійснюється мінімально визначеною штатною чисельністю сил і засобів системи забезпечення кібернетичної безпеки держави, які знаходяться в постійній бойовій готовності, займаються повсякденною діяльністю у відповідності з визначеними завданнями.

При $P_{1i} < K_i\ (t_1) < P_{ri}$ (де P_{ri} – поріг загрози виникнення надзвичайної ситуації кібернетичного характеру) для системи забезпечення кібернетичної безпеки встановлюється режим №2, тобто, як і в попередньому випадку, забезпечення необхідного рівня безпеки здійснюється мінімально визначеною чисельністю елементів системи. Різниця полягає в залученні додаткових експертів до перевірки аналітичними структурами отриманого значення комплексного показника рівня небезпеки.

У випадку не підтвердження отриманого значення $K_i\ (t)$ система забезпечення кібербезпеки держави повертається в режим №1.

У разі підтвердження отриманого значення $K_i\ (t)$ система залишається в режимі №2. При цьому формулюються додаткові завдання відповідним структурам відносно поглибленого моніторингу кримінальної, терористичної, воєнно-політичної обстановки в кіберпросторі як України, так і сусідніх держав, зі сторони яких зросла відповідна небезпека, і навколо їх. Крім того, більш детально вивчається можливість утворення спільного міждержавного органу з іншими країнами – союзниками для ліквідації можливої наступної надзвичайної ситуації кібернетичного характеру. Активізуються зусилля відповідних міністерств та відомств щодо здобуття інформації, пов'язаної зі зростанням рівня кібернетичної небезпеки.

При $P_{ri} < K_i\ (t_1) < P_{РЗВНСi}$ (де $P_{РЗВНСi}$ – поріг безпосередньої загрози виникнення надзвичайної ситуації кібернетичного характеру) система забезпечення кібербезпеки держави переводиться в режим функціонування №3А. При цьому особлива увага приділяється відслідковуванню ознак безпосередньої загрози виникнення надзвичайної ситуації.

У випадку появи хоча б однієї ознаки безпосередньої загрози виникнення надзвичайної ситуації, тобто при $P_{РЗВНСi} < K_i\ (t_1) < P_{НСi}$ (де – поріг надзвичайної ситуації) система забезпечення кібербезпеки держави переводиться в режим функціонування №3Б, і з цього моменту починається відлік терміну загрозливого періоду виникнення надзвичайної ситуації кібернетичного характеру, а якщо це безпосередня воєнна загроза – то в державі вводиться надзвичайний стан.

У зв'язку з тим, що точність розрахунків комплексного показника рівня небезпеки у кібернетичному просторі держави залежить від точності і повноти вхідної інформації, яка в переважній більшості випадків неповна і не точна, то для запобігання прийняття помилкових рішень вводиться поріг (рівень) підтвердження P_{ri}. При отриманих оцінках $K > P_{ri}$ пропонується додаткова перевірка показника К за допомогою експертів (аналітиків) з тим, щоб або підтвердити розрахункове значення комплексного показника рівня небезпеки, або уточнити його значення. Якщо отримано підтвердження зростання $K_i(t) > P_{ri}$., то за допомогою відомих методів прогнозування здійснюється пролонгація графіка

$$K_i(t) = F[(U_1(t), (U_2(t), \ldots..., (U_s(t)],$$

для, $t = var\ (t_r, t_{БЗВНС})$, де $t_{НС} = arg\ \{Ki(t) = P_{НСi}\}$, $t_{БЗВНС} = arg\ \{Ki(t) = P_{БЗВНСi}\}$.

Загрозливий період у розвитку ситуації кібернетичного характеру має велике значення, особливо для ситуації воєнного характеру. Саме мудра політика керівництва всіх рівнів на цьому етапі може не допустити переходу ситуації до надзвичайної, або розтягнути цей

період до межі, яка дозволить підготувати сили і засоби для більш ефективного їх використання на етапі ліквідації надзвичайної ситуації. Так, наприклад, для воєнної ситуації, цей період може бути використаний для:

звернення до системи регіональної безпеки;

створення воєнних союзів і укладання угод на випадок відбиття збройної агресії;

корегування зусиль розвідки;

попередження держави – ймовірного противника про можливі наслідки агресії;

переведення у вищу ступінь бойової готовності ударних компонентів сил стримування тощо.

Висновки.

Таким чином, запропонована технологія аналізу можливості виникнення надзвичайних ситуацій кібернетичного характеру дає змогу в залежності від отриманого значення комплексного показника рівня небезпеки кібернетичного характеру нарощувати відповідні сили та засоби системи забезпечення кібербезпеки держави та утримувати їх у таких режимах функціонування, які дозволять у межах виділених ресурсів локалізувати відповідні кіберзагрози та зменшити до мінімуму їх негативні наслідки.

Перспективи подальшого розвитку в даному напряму. У подальших публікаціях буде розглянута система показників оцінювання рівня кібернетичного захисту національних інтересів держави в оборонній сфері.

ЛІТЕРАТУРА

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія./ В.Л. Бурячок. – К.: НАУ.- 2013. – 432с.;

2. Указ Президента України «Про Доктрину інформаційної безпеки України» м. Київ, 8 липня 2009 року № 514/2009 [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/514/2009;

3. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки»: за станом на 25.12.2012р./ Затверджений ВР України від 09.01.2007 року № 537-V. - Відомості Верховної Ради України, 2007, № 12, ст.102. -[Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16;

4. Указ Президента України «Про Стратегію національної безпеки України» м. Київ 12 лютого 2007 року № 105/2007 [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007;

5. Проект закону України «Про кібернетичну безпеку України» від 04.06.2013 № 2207а. [Електронний ресурс]. – режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JG1PBA0A.html;

6. Проект «Стратегія забезпечення кібернетичної безпеки України» [Електронний ресурс]. – режим доступу: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf;

7. Конвенція РЄ «Про кіберзлочинність» (*ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005, ВВР, 2006, N 5-6, ст.71)* [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575;

8. Богданович В.Ю. Воєнна безпека України: методологія дослідження та шляхи забезпечення: Монографія.- К.: "Тираж".- 323с.;

9. Богданович В.Ю.Теоретические основы анализа проблем национальной безопасности государства в военной сфере: Монография.- К.: Основа .-2006.-296 с.;

10. Богданович В.Ю., Романченко І.С., Свида І.Ю., Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості : Монографія. - Львів: Академія сухопутних військ. -2011.-414 с.;

11. Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Монографія. : у 7 т..-Т.1.Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.: Наук.-вид. центр НА СБ України, 2012.-548с.

Надійшла: 20.12.2013р.

Рецензент: д.т.н., професор Хорошко В.О.