УДК 007:35+005.5

Ю. Г. ДАНИК, *доктор технічних наук, професор, заслужений діяч науки і техніки України, начальник Житомирського військового інституту імені С. П. Корольова Державного університету телекомунікацій, м. Житомир*

В. І. ШЕСТАКОВ, *кандидат технічних наук, доцент, лауреат державної премії України в галузі науки і техніки, заступник начальника Житомирського військового інституту імені С. П. Корольова Державного університету телекомунікаці з навчальної та наукової роботи, м. Житомир*

С. В. ЧЕРНИШУК, *ад'юнкт Житомирського військового інституту імені С. П. Корольова Державного університету телекомунікацій, м. Житомир*

ПІДХІД ДО КЛАСИФІКАЦІЇ КІБЕРНЕТИЧНИХ ЗАГРОЗ

У статті проаналізовано кібернетичні загрози з точки зору забезпечення інформаційної безпеки або захисту інформації без урахування особливостей процесів управління, які відбуваються в інформаційних системах. Пропонується розглядати кібернетичні загрози як загрози процесам управління на різних рівнях. Існуючі класифікації кібернетичних загроз доповнено найбільш суттєвими ознаками з погляду захисту та протидії.

Ключові слова: *класифікація, кібернетичні загрози, ознаки класифікації, протидія.*

Постановка проблеми у загальному вигляді. У низці нормативних документів з питань оборони та безпеки України чільне місце відводиться проблемі протидії кібернетичним загрозам (КЗ). Зокрема у [1, 2] КЗ віднесено до актуальних загроз національній безпеці держави, а створення системи кібернетичної безпеки (КБ) та захист від кібернетичних атак визначено нагальними завданнями.

Забезпечення КБ громадян, суспільства, держави потребує, у першу чергу, завчасного виявлення КЗ об'єкту захисту для прогнозування можливих наслідків прояву таких загроз та своєчасного прийняття рішення про їх нейтралізацію або стримування [3, 4]. За умови успішного виконання зазначених етапів досягається такий стан захищеності кібернетичного простору держави від будь-якого деструктивного впливу, за якого забезпечується його належне функціонування та сталий розвиток.

Виявлення КЗ вимагає глибокого аналізу їх сутності та систематизації таких загроз. Упорядкування всієї множини КЗ за певними класифікаційними ознаками дозволить забезпечити необхідний рівень достовірності їх ідентифікації. Тому завдання класифікації існуючих та потенційних КЗ об'єкту захисту є актуальною з огляду на забезпечення його КБ.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори. Аналіз доступних авторам робіт дозволяє стверджувати, що відомі підходи до класифікації КЗ орієнтовані на дещо звужене розуміння КЗ. У більшості з таких класифікацій розглядаються інформаційні загрози [5], загрози інформації [6], загрози розподіленим системам обробки даних [7], тобто загрози, орієнтовані на інформаційну складову безпеки, а не на кібернетичну в цілому [8].

При цьому автори зазначених праць як класифікаційні ознаки, зазвичай, обирають характеристики загроз, які властиві вузькоспеціалізованим галузям діяльності. Наприклад, у [4] йдеться про загрози спеціальним інформаційно-телекомунікаційним системам, у [5] увага акцентується на інформаційно-психологічних загрозах, у [6] розглядаються загрози у мережі Інтернет, у [7] систематизова-

но загрози, що виникають у процесі обробки персональних даних, у [9] описано загрози у сфері захисту прав інтелектуальної власності тощо. Такі підходи характеризують різні аспекти безпеки процесів управління й обміну інформацією, які відбуваються у переважній більшості систем різних галузей життєдіяльності сучасного суспільства. Відповідно до сучасних уявлень подібні системи належать до класу кібернетичних.

Таким чином, відомі класифікації КЗ розроблено з позицій забезпечення інформаційної безпеки і безпеки інформації, не враховують особливості процесів управління, що відбуваються у кібернетичних системах (КС) різного призначення.

Метою статті є розвиток підходів до класифікації КЗ з урахуванням особливостей процесів управління, що дозволить систематизувати накопичені у даній предметній галузі знання для їх подальшого використання при розробці моделей таких загроз, способів їх виявлення та заходів протидії в інтересах забезпечення КБ громадянина, суспільства, держави.

Виклад основного матеріалу дослідження. За результатами аналізу, наведеного в [10], під КЗ пропонується розуміти фактори (події, явища), які мають місце та відбуваються в інформаційному, комунікаційному, комп'ютерно-мережному, соціальному та соціотехнічному просторах (або їх комбінація у певному поєднанні), які за умови їх умисного цілеспрямованого використання створюють небезпеку порушення процесів управління, обробки та передачі інформації, що відбуваються у КС різних сфер (соціальній, технічній, соціотехнічній), або можуть зашкодити елементам таких систем.

Виходячи з того, що будь-яка класифікація є поділом предметів різного роду на взаємозв'язані класи відповідно до найбільш суттєвих ознак, які властиві предметам цього роду і відрізняють їх від предметів інших родів, до неї висуваються такі вимоги:

повнота поділу: усі категорії класифікації повинні бути перераховані;

чистота: категорії класифікації не повинні перетинатися.

Відповідно розв'язання задачі класифікації КЗ передбачає формування якомога повнішого переліку таких загроз та розподілу їх за найбільш суттєвими та важливими у практичному відношенні ознаками, які не допускають дублювання.

Виходячи із сутності КЗ, при формуванні найбільш повного їх переліку доцільно враховувати: характеристику конкретної КС та її елементів; особливості процесів управління, обробки й обміну інформацією, що відбуваються у КС; властивості середовища (шляхи) поширення сигналів та передачі інформації; можливості джерел (суб'єктів) загрози.

До характеристик КС, що визначають рівень небезпеки її функціонуванню, можна віднести: структуру КС (елементи системи та взаємозв'язки між ними), наявність зв'язків із зовнішнім середовищем та іншими КС, наявність підсистеми захисту.

У загальному випадку КС складається з об'єкта управління, суб'єкта управління і каналів зв'язку та може бути зображена рис. 1, де $\vec{g}_i'(t)$, $\vec{g}_i''(t)$ – кібернетичні загрози; $\vec{x}(t)$ – вхідна (керуюча) дія; $\vec{y}(t)$ – вихідна дія (реакція системи); t – час. Природа всієї системи визначається її призначенням та, зазвичай, є комбінованою, при цьому природа окремих елементів може бути абсолютно різною: біологічною, технічною або соціальною.

Особливості процесів управління, обробки та передачі інформації, які відбуваються у КС, обумовлені специфікою алгоритмів перетворення вхідної дії $\vec{x}(t)$, яка надходить через рецептори, у результат на виході КС $\vec{y}(t)$ (вихідну дію) (див. рис. 1).

Порушення будь-якого з етапів таких алгоритмів у результаті реалізації загрози $\vec{g}_i(t)$ може призвести до дезорганізації функціонування КС та невиконання її призначення. Тому при розгляді кожної конкретної КС важливо чітко визначити учасників процесу управління; множину їх допустимих станів та закони зміни таких станів; сигнали, які вони можуть продукувати; безпечні зв'язки між учасниками процесу управління.

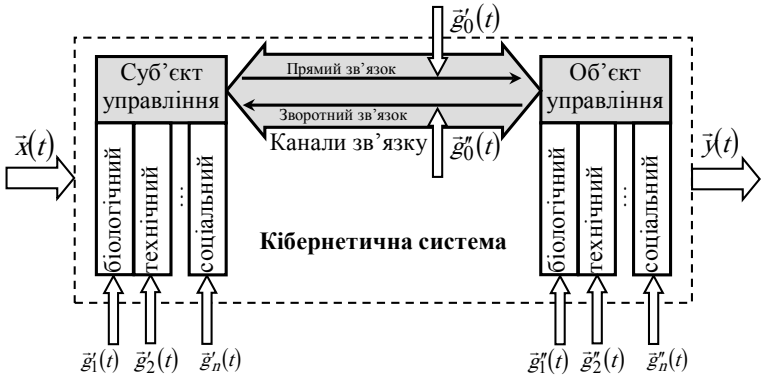

Рис. 1. Модель кібернетичної системи

Канали зв'язку, що являють собою середовище передавання інформації (управляючих сигналів), є одним з найбільш уразливих елементів КС, оскільки під час передавання інформації вона може перехоплюватися, модифікуватися або взагалі знищуватися.

Можливості джерел (суб'єктів) КЗ обумовлені сукупністю способів доступу (проникнення, впливу) до елементів КС, у результаті реалізації яких досягається порушення функціонування таких елементів або виведення їх із працездатного стану.

Ураховуючи особливості функціонування КС, до базових ознак класифікації пропонується віднести такі (рис. 2):

вид КС (V), на яку спрямована загроза;

елемент КС (K), на який безпосередньо націлена реалізація загрози;

уразливості (U) (системи та її елементів), що використовуються;

розташування джерела (суб'єкта) КЗ (S);

спосіб реалізації КЗ (R);

середовище поширення (M);

умисність (B);

походження (N);

повторюваність появи (F);

прихованість прояву (L);

масштаби наслідків від реалізації загрози (O);
ієрархія управління, що відбувається у КС (Q);
доцільність реалізації КЗ (X);
час появи КЗ (T)
умовність реалізації (Y).

За видом *КС* (V) (її фізичною природою), на яку спрямована КЗ, розрізняють: технічні (V_1); біологічні (V_2); соціальні (V_3); комбіновані (V_4).

Слід зазначити, що вид КС, яка підлягає захисту, обмежує не лише діапазон її потенційних загроз, а й значною мірою можливі заходи протидії таким загрозам. Так, наприклад, при розгляді суто технічних КС, можна відкинути загрози біологічної або соціальної природи, що дозволить скоротити перелік можливих заходів захисту та протидії.

За елементом *КС* (K), на який безпосередньо націлена (або через який здійснюється) КЗ, можна виділити такі класи загроз: загрози об'єкту управління (K_1); загрози суб'єкту управління (K_2); загрози каналу зв'язку (інформації, командам, що передаються) (K_3); комплексні загрози (K_4).

Класифікація за такою ознакою як елемент КС, на який спрямована загроза, дозволяє підвищити ефективність протидії за рахунок раціонального використання сил та засобів (ресурсів) захисту. Завчасне зосередження ресурсів захисту на певній складовій КС, щодо якої існує загроза, дозволяє забезпечити необхідний рівень захисту всієї системи із найменшими витратами.

За уразливостями (U) (системи та її елементів), що використовуються, мають місце такі загрози: загрози, що реалізуються за рахунок уразливостей складових КС (U_1); загрози, що реалізуються за рахунок використання уразливостей підсистеми захисту КС (за наявності такої підсистеми) (U_2); загрози, що реалізуються із застосуванням недоліків в алгоритмах управління й обробки інформації (сигналів) (U_3).

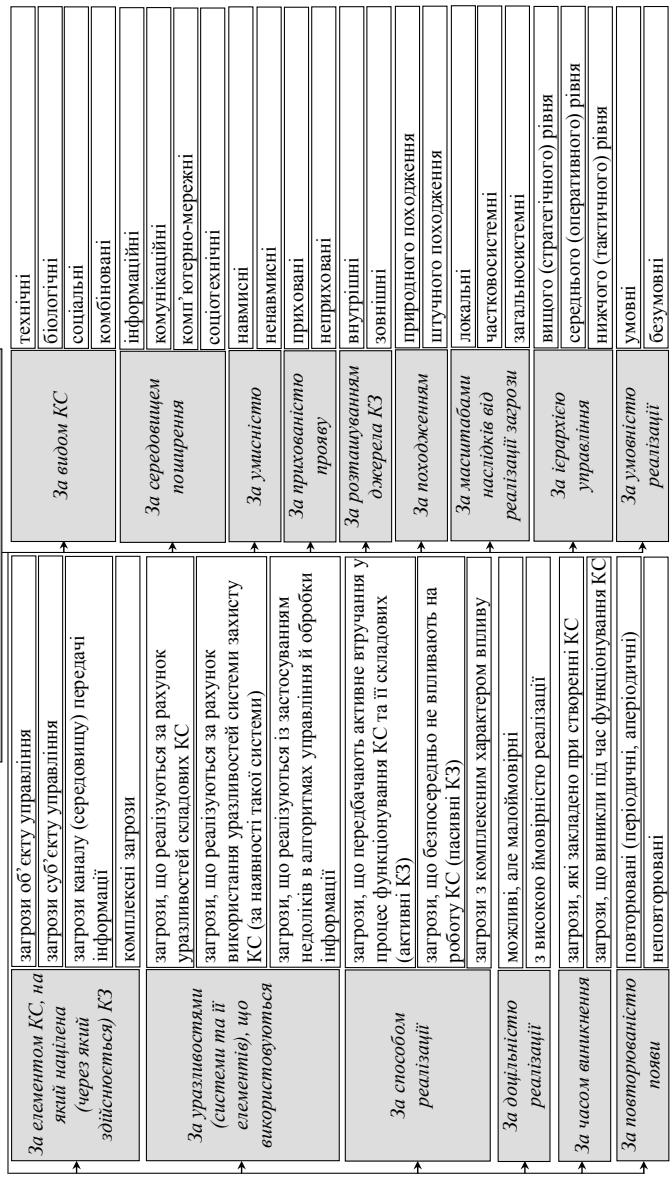

Рис. 2. Класифікаційна схема кібернетичних загроз

Класифікація загроз за уразливістю, що використовується, дозволяє підвищити точність локалізації небезпеки та мінімізувати витрати на проведення заходів захисту КС.

За розташуванням (S) джерела (суб'єкта) КЗ відносно об'єкта, на який вона спрямована, слід виділяти загрози: зовнішні (S_1) та внутрішні (S_2).Об'єкти, з якими взаємодіють КС, що підлягають захисту, виступають джерелом зовнішніх загроз, а складові таких систем – внутрішніх.

Зовнішні КЗ, у свою чергу, поділяються на загрози від середовища функціонування КС та загрози від конкуруючих (протидіючих) систем. До загроз першого підкласу можна віднести стихійні лиха, революції тощо. Прикладом загроз другого підкласу можуть бути загрози протиборчих сторін одна одній у військовому конфлікті.

Клас внутрішніх КЗ розгалужується з урахуванням складу конкретної КС. Наприклад, для сучасних інформаційно-управляючих систем до внутрішніх КЗ можуть належати загрози від носіїв інформації; технічних засобів; програмних засобів; засобів захисту інформації (апаратних, алгоритмічних, програмних); людини-оператора (обслуговуючого персоналу) тощо.

Завчасне визначення джерела загрози дозволяє застосовувати відносно нього активні (превентивні) заходи протидії.

Спосіб реалізації КЗ (R) залежить від конкретного об'єкта та його особливостей (технічних, соціальних, біологічних, психологічних), але в загальному випадку виділяються: загрози, що передбачають активне втручання у процес функціонування КС (активні КЗ) (R_1); загрози, що безпосередньо не впливають на роботу КС (пасивні КЗ) (R_2); загрози із комплексним характером впливу (R_3).

За середовищем поширення загрози (M) виділяються класи, що відповідають існуючим небезпечним середовищам: інформаційному (M_1); комунікаційному (M_2); комп'ютерно-мережному (M_3); соціотехнічному (M_4).

Середовище поширення КЗ не в останню чергу визначає форми та способи протидії таким загрозам. Наприклад, недоцільно (хоча й можливо) застосовувати фізичне знищення комунікацій-

них каналів для захисту від атаки типу "відмова в обслуговуванні", а от завдання превентивного удару по противнику, що готується до збройної агресії, можна вважати ефективним.

За умисністю (B) загрози бувають: навмисними (B_1); ненавмисними (B_2).

Навмисні загрози передбачають цілеспрямований намір заподіяння шкоди КС або її елементам. Ненавмисні загрози виникають і реалізуються безвідносно до волі носія (джерела) загрози.

За походженням (N) можна виділити загрози: штучного походження (антропогенні, техногенні) (N_1); природного походження (N_2).

Загрози штучного походження є наслідком діяльності людини або функціонування технічних систем. Загрози ж природного походження виникають внаслідок природних процесів, що відбуваються у живій та неживій природі.

За повторюваністю появи (F) виділяються загрози: повторювані (періодичні, аперіодичні) (F_1); неповторювані (F_2).

Віднесення тієї або іншої загрози до класу повторюваних дозволяє ефективніше протидіяти їй у майбутньому за рахунок формування образу такої загрози та застосування відпрацьованого алгоритму протидії. Неповторювані ж загрози вимагають залучення більш значних ресурсів для їх усунення через необхідність додаткового вивчення та моделювання. Показник повторюваності f може бути визначений, наприклад, кількістю m випадків появи тієї чи іншої КЗ за деякий проміжок часу t ($f = \frac{m}{t}$).

За прихованістю прояву (L) виділяються: приховані (L_1); неприховані (L_2).

Рівень прихованості загроз визначає складність алгоритмів їх ідентифікації, що неодмінно позначається на тривалості виявлення загроз та врешті решт визначає принципову можливість такого виявлення за допустимий час.

Прихованість КЗ може бути оцінена ймовірністю виявлення її ознак:

$$P_{вияв} = \prod_{j=1}^{N}\left(1 - \prod_{q=1}^{K}\left(1 - P_{вияв_q}\right)\right), \qquad (1)$$

де $P_{вияв_q} = \frac{m_{вияв}}{N \cdot l}$ – ймовірність виявлення q-го етапу реалізації КЗ ($m_{вияв}$ – кількість випадків виявлення q-го етапу, l – кількість ітерацій q-го етапу КЗ у кожній з N спроб її реалізації); K – кількість етапів реалізації КЗ.

Реалізація однієї із КЗ наведених класів або їх сукупності може призвести до наслідків різного масштабу (O) для КС або її елементів. Відповідно й КЗ можна поділити на: локальні (O_1); частковосистемні (O_2); загальносистемні (O_3).

Локальні загрози характеризуються несуттєвим ускладненням роботи окремого елемента КС, що не позначається на функціонуванні КС у цілому.

Загрози частковосистемного характеру призводять до порушення роботи кількох елементів або сегмента КС, що здатне негативно позначитися на виконанні КС частини своїх функції або призначення в цілому з можливістю відновлення ураженого сегмента.

Загальносистемні загрози націлені на ураження кількох сегментів системи або ключових її елементів, що неодмінно призводить до відмови функціонування КС у цілому без можливості відновлення її роботи.

Ступінь тяжкості наслідків реалізації загрози може бути оцінений за виразом

$$O = \sum_{w=1}^{E} \alpha_w P_w, \qquad (2)$$

де α_w – коефіцієнт важливості w-го елемента (сегмента) КС з огляду на функціонування системи в цілому; P_w – ймовірність реалізації КЗ, націленої на w-й елемент (сегмент) КС; E – кількість елементів (сегментів) КС.

За ієрархією управління (Q), що відбувається у КС, виділяються КЗ: вищого (стратегічного) рівня (Q_1); середнього (оперативного) рівня (Q_2); нижчого (тактичного) рівня (Q_3).

На вищому (стратегічному) рівні управління приймаються та реалізуються найбільш важливі рішення для КС у цілому. Очевидно, що загрози цього рівня найбільш небезпечні для функціонування КС.

Проміжний (оперативний) рівень забезпечує управління ходом окремих операцій (оперативне управління), а тому є не просто буфером між вищою та нижчою ланками управління, а відіграє вкрай важливу роль у виконанні КС свого призначення. Порушення управління у проміжній ланці здатне призвести до дезорганізації КС, а тому загрози на проміжному рівні управління також становлять небезпеку.

Нижча (тактична) ланка управління, як правило, найбільш чисельна (що дозволяє застосовувати в управлінні дублювання та резервування), тому загрози на цьому рівні не становлять значної небезпеки, а можуть лише вплинути на реалізацію певної часткової функції КС. Проте одночасна реалізація деякої сукупності КЗ відносно критичних елементів на нижчому рівні управління може призвести до синергетичного ефекту, тому безпекою цієї ланки управління КС також не слід нехтувати.

Прийняття рішення про доцільність (X) реалізації КЗ можливо за критерієм "ефективність/вартість" ($X = \frac{P}{C}$). Тобто, якщо отриманий від реалізації КЗ ефект P перевищує витрати C на її підготовку і здійснення ($X > 1$), є сенс розглядати можливість такої загрози. В іншому випадку ($X \leq 1$) реалізація КЗ недоцільна. Відповідно до цього виділимо такі класи КЗ: гіпотетично можливі, але малоймовірні (X_1); з високою ймовірністю реалізації (X_2).

Важливим чинником, що впливає на ймовірність реалізації тієї чи іншої КЗ, є її залежність від певних подій. Тобто реалізація одних КЗ можлива лише за умови, якщо відбудеться відповідна сприятли-

ва подія ω_s (або група подій $\Omega = \{\omega_1, \omega_2, ..., \omega_p\}$), а реалізація інших не вимагає виконання такої умови.

Відповідно за умовністю реалізації (Y) виділимо КЗ: умовні (Y_1); безумовні (X_2).

Математично безумовні КЗ описуються виразом

$$P(\mathrm{A}|\omega_s) = P(A), \tag{3}$$

а умовні:

$$P(\mathrm{A}) = \sum_{i=1}^{p} P(\omega_s) P(A \,|\, \omega_s), \tag{4}$$

$$P(\mathrm{A}) = \prod_{i=1}^{p} P(A \,|\, \omega_s), \tag{5}$$

де A – реалізація КЗ; ω_s – сприятлива для реалізації КЗ подія, $\sum_{s=1}^{p} P(\omega_s) = 1$; p – кількість сприятливих для реалізації КЗ подій.

При цьому, якщо події ω_s складають повну групу подій Ω, застосовується формула (4), в іншому випадку – формула (5).

За часом появи КЗ (T) виділимо: загрози, які закладено при створенні КС (T_1); загрози, які виникають у процесі функціонування КС (T_2).

Недосконалості у структурі та конструкції КС або її окремих елементів є уразливими місцями, які потенційно можуть використовуватися для порушення сталої роботи системи. Такі уразливості закладаються під час створення системи або проявляються у процесі її функціонування (для комп'ютерних систем це "загрози нульового дня"). Виявлення закладених при створенні КС уразливостей дозволяє значно підвищити захист таких систем від КЗ уже на ранніх етапах експлуатації. Уразливості, що проявляються з часом, більш небезпечні, оскільки їх виникнення складно передбачити чи

спрогнозувати, а тому протидія загрозам, що використовують такі уразливості, украй утруднена.

Застосований для класифікації КЗ ознаковий принцип дозволяє описати будь-яку загрозу $\vec{g}_i$ множиною якісних та кількісних ознак $\vec{g}_i = (V, E, U, S, R, M, B, N, F, L, O, Q, X, Y)$, які можуть бути використані при моделюванні та подальшій ідентифікації такої загрози.

Наведена класифікація КЗ передбачає можливість доповнення та розгалуження на підкласи, що досить зручно при розробці переліку загроз для кожної конкретної КС, залежно від рівня необхідної деталізації.

Висновки. Комплексна природа КЗ вимагає розглядати їх, у першу чергу, як загрози процесам управління, що відбуваються у КС, а не лише інформації, що циркулює у таких системах. Значна різноманітність КС (за природою, структурою, принципами та середовищем функціонування тощо) обумовлює такі вимоги до класифікаційних ознак КЗ: адекватність для будь-яких КС; універсальність з огляду на особливості процесів управління, обробки й обміну інформацією, що відбуваються у КС різних класів; відображення властивостей середовища функціонування КС; урахування можливостей джерел (суб'єктів) загрози.

Запропонована класифікація КЗ не суперечить відомим і враховує при цьому комплексний характер таких загроз. В її основу покладено найбільш значущі для виявлення та протидії КЗ ознаки, які одночасно забезпечують повноту і чистоту класифікації. Наведені ознаки доцільно використати для подальшої формалізації КЗ та розробки їх моделей. Запропонована класифікація може бути покладена в основу розробки методик виявлення КЗ, що дозволить своєчасно реагувати на такі загрози та запобігати їх ескалації.

Перспективи подальших розвідок у даному напрямку. У міру постійної видозміни сучасних КС та процесів, що у них відбуваються, актуальність класифікації КЗ забезпечується тільки за рахунок її постійного доповнення й уточнення, що й передбачається здійснити під час подальших досліджень.

Список використаної літератури

1. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Воєнної доктрини України" : Указ Президента України № 390/2012 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/14824.html

2. Про Доктрину інформаційної безпеки України : Указ Президента України № 514/2009 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/514/2009

3. Корнюшин П. Н. Информационная безопасность / П. Н. Корнюшин, С. С. Костерин. – Владивосток : ТИДОТ ДВГУ, 2003. – 154 с.

4. Бурячок В. Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко. // Наука і оборона. – 2011. – № 3 – С. 35–42.

5. Інформаційна безпека держави: аспект інформаційно-психологічних загроз / [В. Г. Головань, О. М. Дроздов, В. В. Сергєєв, В. М. Герасимов] // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир: ЖВІ НАУ, 2011. – Вип. 5. – С. 33–41.

6. Конев А. А. Подход к построению модели угроз защищаемой информации / А. А. Конев // Доклады ТУСУРа. – Томск, 2012. – № 1 (25). – Часть 2. – С. 34–40.

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. – Режим доступа : http://www.aksimed.ru /download/center/ Bazovaya-model.pdf

8. Wiener N. Cybernetics or Control and Communication in the Animal and the Machine. // N. Wiener – New York : The Technology Press and John Wiley & Sons, Inc. – Paris : Hermann et Cie, 1948.

9. Internal Threats to America: Cyber & Intellectual Property Threat Study Guide Intellectual Takeout [Electronic resource] – Mode of access : http://www.intellectualtakeout.org/ sites/www.intellectualtakeout.org/files/Cyber Threats Study Guide - March 2012_2.pdf

10. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю. Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир : ЖВІ НАУ, 2012. – Спецвип. 2. –С. 5–14.

Стаття надійшла до редакції 7.02.2014.

Даник Ю. Г., Шестаков В. И., Черныщук С. В. **Подход к классификации кибернетических угроз**

В статье проведен анализ кибернетических угроз с точки зрения обеспечения информационной безопасности или защиты информации без учета особенностей, протекающих в информационных системах процессов управления. Предлагается рассматривать кибернетические угрозы как угрозы процессам управления на разных уровнях. Существующие классификации кибернетических угроз дополнены наиболее существенными признаками с точки зрения защиты и противодействия.

Ключевые слова: классификация, кибернетические угрозы, признаки классификации, противодействие.

Danyk Yu. H., Shestakov V. I., Chernyshuk S. V. **Approach to cyberthreats classification**

Nowadays cyberthreats became most dangerous for normal functioning of critical infrastructures of whole countries. Effectively counteraction to these threats demands deep analysis of their nature and systematization. Majority of modern researchers consider cyberthreats in context of information security or data protection and don't take into account peculiarities of management processes witch take place in information systems. But complex nature of cybernetic systems demands to consider such threats as threats to management processes. Purpose of this paper is to develop existing approaches to cyberthreats classification with regard to management process peculiarities in order to systematize existent in this subject area knowledge for their further appliance in cyberthreats modeling and development of methods and countermeasures for cyber security of citizens, society and whole country.

According to accepted definition of cyberthreats it's suggested a set of their classification features witch determined by characteristics of certain cybernetic system and its elements; peculiarities of management, communication and information processing in such systems; properties of signals and information transmission medium (path); capabilities of threat sources. As result we succeessed to singularize following

classification features: cybernetic system type; targeted system element; used for cyberthreat realization vulnerabilities of system or its elements; cyberthreat source placing; method of cyberthreat realization; cyberthreat transmission medium; premeditation; origination; occurrence repetition; hiding; dimensions of treats realization impact; management hierarchy; practicality of realization; time of occurrence; conditionally.

For suggested features noncrossing classes are determined and influence of cyberthreats categorization on determined classes to cybersecurity effectiveness is substantiated. All classes are summarized in general classification scheme for better understanding of their structure.

As result applied classification scheme makes it possible to describe each cyberthreat as a set of quantitative and quality characteristic, witch can be used for modeling and further identification of these threats.

Developed classification provide for possible addition and embranchment to subclasses for convenient determination of cyberthreats list for certain cybernetic system depending from level of necessary detalization. In order to demonstrate mentioned properties of suggested classification the possibility of its application for information and control systems is showed.

Suggested classification is not contradictory to existing one and consider complex nature of these threats. It's based on most important for defense and counteraction features. Chosen features guarantee completeness and clarity of classification.

Developed classification scheme can be take as a basis for further researches in field of cyberthreats detection technologies in order to timely reaction to these threats and eliminate their escalation.

Because of constant transfiguration of modern cybernetic systems and modification of processes, witch take place in these systems, actuality of classification can be achieved only by permanent addition and revision which should be conducted on regular basis.

Keywords: *classification, cyberthreats, criterion of classification, counteraction.*