УДК 004.738

**А. А. Шиян, Л. О. Нікіфорова,
І. О. Дьогтєва, Я. Ю. Яремчук**
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Модель управління протидією інформаційним атакам у кіберпросторі

Представлено модель управління протидією інформаційним атакам у кіберпросторі сучасного інформаційного суспільства. Вона ґрунтується на виокремлених інструментах щодо протидії негативним інформаційно-психологічним процесам як у соціальних стратах, так і у суспільстві в цілому. Досліджено динаміку кількості суб'єктів, які підпадають під вплив інформаційних атак, з використанням відповідного математичного апарату, основою якого є нелінійні диференційні рівняння. Вони описують як зміну кількості у часі суб'єктів, так і відповідні задачі, поставлені перед службою кібербезпеки для запобігання негативним наслідкам потенційних чи реалізованих інформаційних атак. Виділено та проаналізовано чотири сценарії можливих варіантів інформаційних атак, які залежать від типу обраної функції, і представлено відповідні варіанти розгортання можливих сценаріїв протидії інформаційним атакам. Також виділено окремі аспекти та чинники, за допомогою яких можна управляти даним процесом.

Ключові слова: *модель, кіберпростір, інформаційна атака, протидія, наслідки, управління, безпека.*

Вступ

В останні роки все більше уваги світового співтовариства спрямовано до проблем кібербезпеки. Інформаційні атаки на окремі верстви суспільства, цільові інформаційні атаки на суспільно-економічні процеси, які впливають на життя цілих держав, — усе це сьогодні стало вже типовим наповненням новин.

Важливим аспектом інформаційних атак у кіберпросторі є реакція цільових груп і суспільства у цілому на їхнє розгортання у часі. Все більша увага на рівні органів державної і регіональної влади та управління приділяється саме реакції суспільства. Також стрімко зростає кількість та чисельність спеціалізованих державних і громадських структур, які покликані активно протидіяти таким інформаційним атакам.

Огляд літератури

У роботі [1] здійснено огляд переважно організаційних напрямків діяльності у сфері кібербезпеки в Україні. Підкреслюється необхідність комплексних підходів до вирішення задач кібербезпеки. Це означає, що навіть у рамках одного методу захисту потрібно використовувати системний підхід.

У [2] підкреслюється, що індивідуалізація систем безпеки є важливим елементом інформаційного захисту як на рівні держави, так і окремих цільових об'єктів. Звертається увага на те, що інформаційні атаки найчастіше використовують вразливі особливості саме конкретного об'єкту. Внаслідок цього і управління протидією таким інформаційним атакам повинно враховувати ці специфічні особливості.

Сьогодні на передній план серед можливих загроз інформаційній безпеці держави виходять інформаційно-психологічні впливи через ЗМІ, соціальні медіа тощо [3–8]. Саме такі джерела використовуються сьогодні як засоби інформаційних атак на існуючі у суспільстві ідеї, погляди, уявлення, переконання. В результаті окремі верстви суспільства (цільові групи) будуть спонукатися до певних дій, а, в ряді випадків, і до бездіяльності.

Сьогодні все більш чітко усвідомлюється необхідність аналізу соціальних наслідків від інформаційних атак. Так, у [9] звертається увага на такі їхні специфічні особливості: «Змагальні військові кібероперації, що проводяться під час збройного конфлікту, можуть безпрецедентно впливати на функціонування цивільних суспільств, ставлячи під загрозу захищений обсяг міжнародного гуманітарного права (МГП). У світлі цього у статті підкреслюється необхідність нового захисту для критичних суспільних процесів від кіберзагроз у конфліктних ситуаціях. Хоча експерти та держави загалом погоджуються з тим, що кібер-операції підпадають під дію МГП, цифрова трансформація додала нові вразливості, які нелегко відобразити традиційним обґрунтуванням закону щодо забезпечення базового захисту від наслідків кібернетичної війни, таких як мінімізація смерті, травм і руйнування серед цивільного населення. Сучасні військові кібернетичні засоби та можливості можуть мати серйозний вплив на основні суспільні процеси в економічній, фінансовій, науковій, культурній сферах та сферах охорони здоров'я, а також у просторах публічної інформації. Хоча такі наслідки можуть бути більш розмитими та нематеріальними, у взаємопов'язаному світі вони можуть впливати на цілі суспільства та спричиняти системні зриви в основному».

Унаслідок наведеного вище задачі формування активної протидії інформаційним атакам у кіберпросторі стають все більш актуальними.

Уже існує досить великий обсяг моделей і методів, які переважно сфокусовані на проблемі ідентифікації інформаційної атаки. Наприклад, у [10] розглянуто задачу виявлення кібернетичної атаки на фоні білого гаусівського шуму за умови неперервного спостереження. В [11] розроблено методику кількісно-якісного аналізу та визначення рівня кібербезпеки інформаційних систем держави.

Проте при цьому все ще залишаються актуальними дослідження, пов'язані як із прогнозуванням впливу інформаційних атак у кіберпросторі на поведінку соціальних верств і суспільства у цілому, так і з розробкою ефективного управління протидії виявленим негативним процесам.

Мета роботи

Метою роботи є розробка моделі для управління протидією інформаційним атакам у кіберпросторі, яка орієнтована на удосконалення методів запобігання негативним інформаційно-психологічним процесам у соціальних групах та у суспільстві в цілому.

Буде розглянуто розгортання у часі кількості людей, які знаходяться під впливом інформаційної атаки, та запропоновано параметри, за допомогою яких можна управляти процесом.

Загальна модель для управління

Кожна інформаційна атака у кіберпросторі спрямована на зміну існуючої суспільної думки. Суспільна думка локалізована серед певної сукупності людей. Зі зростанням кількості людей, які поділяють цю нову суспільну думку, вона закріплюється в суспільстві (тобто «завойовує» своїх прихильників).

Розглянемо сукупність людей $n > 0$, які мають певну сформовану раніше суспільну думку. Під впливом інформаційної атаки ця кількість буде змінюватися. Зауважимо, що метою інформаційної атаки у кіберпросторі може бути як збільшення цієї кількості людей (наприклад, які поділяють неприйнятні для суспільства думки), так і зменшення цієї кількості людей (наприклад, патріотично налаштованого населення країни).

Цей процес зміни з часом кількості людей, які будуть поділяти дану суспільну думку, може бути описано таким диференціальним рівнянням:

$$\frac{dn}{dt} = F(n,t),\ n(t=0) = n_0 . \tag{1}$$

Тут n_0 — кількість людей, які поділяють цю суспільну думку на початку розгляду (початкова кількість цих людей).

Функція $F(n,t)$ повинна задовольняти таким вимогам: при малих значеннях часу ця функція повинна бути зростаючою. Проте можливі ситуації, коли вона буде спадаючою (наприклад, для задач зменшення кількості людей).

Загальна задача на управління процесом зміни кількості людей структурами кіберзахисту країни може бути записана у такому вигляді:

$$\frac{dn}{dt} = F(n,t) + u(t),\ n(t=0) = n_0 . \tag{2}$$

Тут $u(t)$ — управляюча функція. Нею моделюється система заходів з боку структур кібербезпеки та тих структур країни, діяльність яких спрямована на протидію інформаційним атакам з боку як зовнішніх, так і внутрішніх агентів впливу.

Зміни суспільної думки людей, як правило, нелінійно залежать від кількості її прихильників (див. [1–3]). Викликано це тим, що процес її зміни залежить від кількості контактів, а кількість контактів зростає нелінійно, залежно від кількості учасників n. Таким чином, функція $F(n,t)$ є нелінійною.

Інформаційна атака, як правило, триває відносно нетривалий період часу. Тому в першому наближенні можна прийняти наближення $F(n,t) = F(n)$. Таким чином, приходимо до такої задачі:

$$\frac{dn}{dt} = F(n) + u(t),\ n(t=0) = n_0 . \tag{3}$$

В управляючій функції $u(t)$ можна, в рамках цього ж наближення, також знехтувати залежністю від часу $u(t) = u$. Таким чином, задача управління протидією інформаційній атаці спрощується до такої:

$$\frac{dn}{dt} = F(n) + u,\ n(t=0) = n_0 . \tag{4}$$

Для аналітичного дослідження задачі необхідно її подальше спрощення. Для цього розкладемо функцію $F(n)$ у ряд та обмежимося лише квадратичним по n членом. Тоді диференціальне рівняння (4) можна привести до такого вигляду:

$$\begin{cases} \dfrac{dn}{dt} = a + bn + cn^2, \\ n(t=0) = n_0, \end{cases}$$
$$F(n) = F_0 + bn + cn^2, \tag{4}$$
$$a = F_0 + u.$$

Тут a, b, c, F_0 та u — константи.

У подальшому, не зменшуючи загальності розгляду, будемо називати a управляючою функцією.

Відмітимо, що коли $n << 1$, то n є часткою людей, які починають реагувати на інформаційну атаку в кіберпросторі. Тоді задача (4) є коректною на початку атаки, тобто при достатньо малих відрізках часу, коли розкладення функції $F(n)$ у ряд та обмеження лише квадратичними членами буде коректним.

Аналіз моделі

Модель (4) може бути використана для аналізування багатьох задач з управління протидією інформаційним атакам у кіберпросторі. Розглянемо декілька можливих сценаріїв таких атак.

Поведінка рішення моделі (4) буде залежати від вигляду такої функції:

$$G(n) = a + bn + cn^2 . \tag{5}$$

У загальному випадку можливі варіанти поведінки функції $G(n)$ наведено на рис. 1–4.

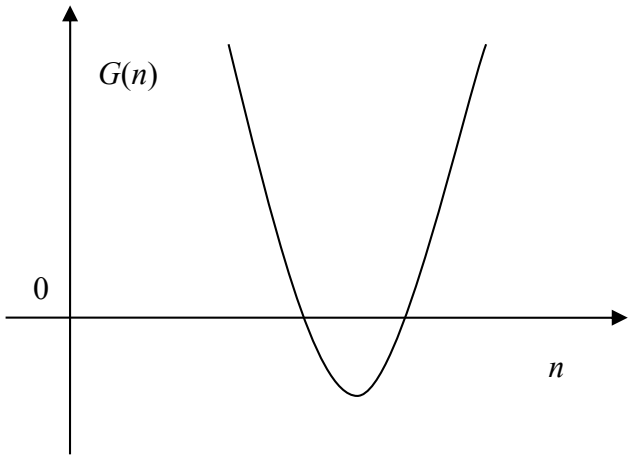

Рис. 1. Загальний вигляд функції $G(n)$ при $c > 0$ за наявності двох дійсних коренів

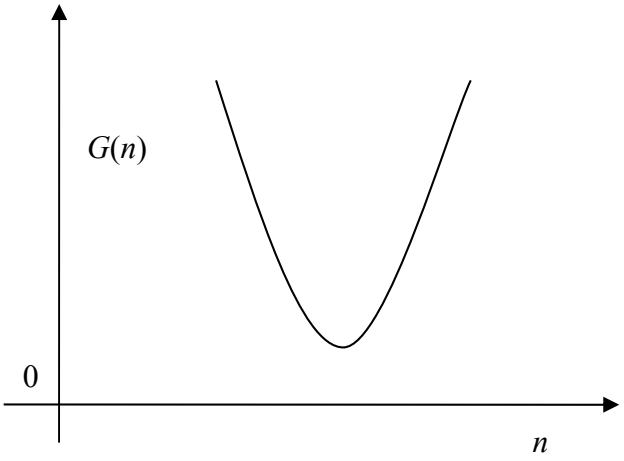

Рис. 2. Загальний вигляд функції $G(n)$ при c > 0 без дійсних коренів

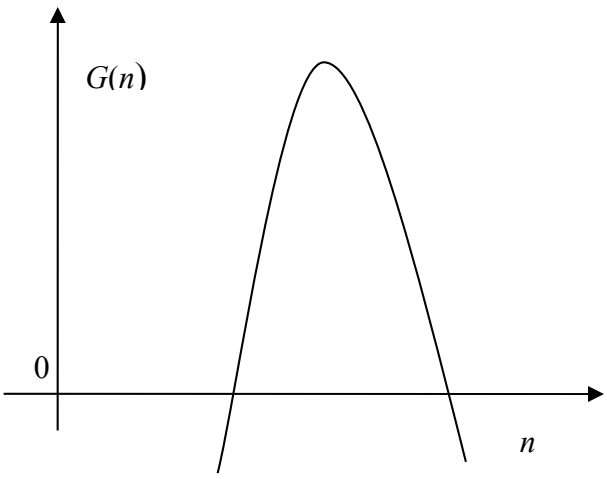

Рис. 3. Загальний вигляд функції $G(n)$ при $c < 0$ за наявності двох дійсних коренів

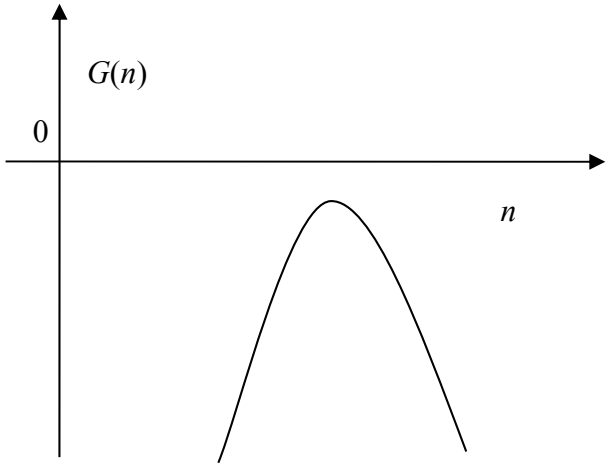

Рис. 4. Загальний вигляд функції $G(n)$ при $c < 0$ без дійсних коренів

Рис. 1–4 ілюструють усі можливі ситуації поведінки рівняння (4). Можна виділити такі сценарії поведінки для задачі (4).

Рис. 1. Функція $n(t)$ має, загалом кажучи, дві стаціонарні точки, які відповідають співвідношенню $G(n) = 0$. «Ліва» стаціонарна точка (при менших значеннях n) є стійкою до малих відхилень, а «права» — нестійкою.

Ця ситуація може відповідати переходу від початкового стану n_0 охоплення суспільства певною думкою до нового стану.

Рис. 2. Функція $n(t)$ буде постійно зростати.

Така ситуація може відповідати тільки початковому стану (відносно нетривалому) переходу суспільства до нового стану (з урахуванням, як видно із (4), як інформаційної атаки, так і протидії їй).

Рис. 3. Функція $n(t)$ має дві стаціонарні точки. Стабільною є стаціонарна точка з більшим значенням змінної n.

Інтерпретація аналогічна інтерпретації рис. 1.

Рис. 4. Функція $n(t)$ буде постійно спадати протягом того часу, допоки не буде досягнуто максимально можливого значення n.

Інтерпретація аналогічна інтерпретації рис. 3.

Таким чином, управління протидією інформаційним атакам у кіберпросторі, сформоване на основі моделі (4), може бути застосовано для широкого кола задач.

Інтерпретація моделі

В рамках моделі можливе здійснення управління протидією інформаційним атакам у кіберпросторі за такими сценаріями. Розглянемо ці чотири сценарії більш детально. Зазначимо, що всі ці сценарії цілком можуть мати місце під час виборчих процесів.

Сценарій 1. Атака у кіберпросторі може бути описана таким чином:

1) постійно йде сталий потік *нової* деструктивної інформації ($F_0 > 0$);

2) ця інформація зачіпає інтереси цільової групи, на яку здійснюється атака ($b > 0$);

3) ця інформація активно обговорюється у цільовій групі ($c > 0$).

Ці умови інформаційної атаки відповідають рис. 1. Але в цьому випадку додатнім (коли $n(t) > 0$) буде лише більший корінь рівняння $G(n) = 0$. Йому відповідає *нестійке* стаціонарне рішення. Розглянемо таку інформаційну атаку, яка спрямована на формування нової «негативної» для суспільства думки. В цьому випадку, без активної протидії інформаційній атаці, кількість носіїв негативної інформації буде зростати, завойовуючи все більшу кількість суспільства.

У цьому випадку, як видно із моделі, протидія такій атаці є неможливою.

З точки зору суспільства це означає, що суспільство сприймає інформаційну атаку як «істину в останній інстанції». А кожен член суспільства підтримує цю інформацію і готовий її як розповсюджувати, так і захищати в дискусіях.

Така ситуація здається парадоксальною, але вона цілком може мати місце.

У рамках запропонованої моделі введено параметри ($F_0 > 0$, $b > 0$ та $c > 0$), які дозволяють визначити успішність атаки на ранніх етапах її розгортання. Ці характеристики можуть бути отримані експериментальним шляхом, наприклад з аналізу реакції суспільства на різні новини.

Сценарій 2. Атака у кіберпросторі може бути описана наступним чином:

1) постійно йде сталий потік *нової* деструктивної інформації ($F_0 > 0$);

2) ця інформація зачіпає інтереси цільової групи, на яку здійснюється атака ($b > 0$);

3) ця інформація активно не обговорюється (швидко «забувається», стає неактуальною, не підтримується тощо) в цільовій групі ($c < 0$).

Такі умови інформаційної атаки відповідають рис. 3. У цьому випадку сама атака (без протидії), формує один стійкий стан у суспільстві із кількістю прихильників

$$n_s = \frac{b + \sqrt{b^2 + 4F_0|c|}}{2|c|}. \tag{6}$$

Якщо застосовувати протидію інформаційній атаці у кіберпросторі з управляючим параметром u , то (6) можна переписати у вигляді

$$n_{su} = \frac{b + \sqrt{b^2 + 4(F_0 + u)|c|}}{2|c|}. \tag{7}$$

Зрозуміло, що, за умови очевидного прагнення зменшити вплив інформаційної атаки, управляючий параметр u може приймати тільки від'ємні значення.

Із (7) видно, що в діапазоні

$$-\frac{b^2}{4|c|} - F_0 \le u \le 0 \tag{8}$$

величина n_{su} при цьому буде зменшуватися до $b/2|c|$.

У випадку, коли виконана нерівність

$$u < u_c = -\frac{b}{4|c|} - F_0, \tag{9}$$

величина $n(t)$ буде постійно спадати. Ця умова відповідає рис. 4.

Таким чином, у цьому випадку, змінюючи управляючий параметр u, ми можемо досягти або зменшення n_{su} від n_s до величини $b/2|c|$, або —повного знищення результатів інформаційної атаки.

Така задача може виникати у випадку, коли інформаційною атакою є тема та інформація, яка має ознаки «неприйнятної» у даному суспільстві («політично некоректної», «забороненої владою», «некультурної», «неетичної», «вульгарної» тощо). Тоді члени суспільства можуть поширювати *чужі* пости та коментарі, але коментувати їх будуть негативно (бо це «забороняється» культурою даного суспільства, наприклад, непристойні пісні чи анекдоти).

Сценарій 3. Атака у кіберпросторі може бути описана таким чином.

1) постійно йде сталий потік *нової* деструктивної інформації ($F_0 > 0$);

2) ця інформація не зачіпає інтереси цільової групи (не поширюється нею), на яку здійснюється атака ($b < 0$);

3) ця інформація активно обговорюється у цільовій групі ($c > 0$).

Такі умови відповідають рис. 1 та 2.

При управляючому параметрі u, який знаходиться в області

$$-F_0 < u < \frac{b^2}{4c} - F_0, \tag{10}$$

існує стаціонарне рішення, яке має вигляд

$$n_{su} = \frac{|b| - \sqrt{b^2 - 4c(F_0 + u)}}{2c}. \tag{11}$$

Із (11) можна зробити висновок, що коли потік шкідливої інформації F_0 стає більшим ніж $b^2/4c$, то стаціонарного значення не буде, і $n(t)$ буде постійно зростати. Те ж буде за умови $u < -F_0$ на управляючий параметр.

Таким чином, у цьому випадку управління зводиться просто до того, щоб зменшити шкоду від інформаційної атаки. Повна ліквідація шкоди від інформаційної атаки у кіберпросторі в цьому випадку досягається при $u = -F_0$.

Ситуація цього сценарію має місце в тому випадку, коли інформація, з якої складається атака, активно вилучається самими користувачами, але вона, тим не менше, активно обговорюється цільовою аудиторією. При цьому таке обговорення носить позитивний характер (підтримується) щодо інформації, яка розповсюджується цією інформаційною атакою.

Сценарій 4. Атака у кіберпросторі може бути описана таким чином:

1) постійно йде сталий потік *нової* деструктивної інформації ($F_0 > 0$).

2) ця інформація не зачіпає інтереси цільової групи (не поширюється нею), на яку здійснюється атака ($b < 0$);

3) ця інформація активно не обговорюється (швидко «забувається», стає неактуальною, не підтримується тощо) у цільовій групі ($c < 0$).

Ці умови відповідають рис. 3 та 4.

При управляючому параметрі u, який знаходиться в області

$$-F_0 < u < 0, \tag{12}$$

існує стаціонарне рішення, яке має вигляд

$$n_{su} = \frac{|b| - \sqrt{b^2 + 4|c|(F_0 + u)}}{2|c|}. \tag{13}$$

За умови $u < -F_0$ стаціонарного значення не буде, і $n(t)$ буде постійно зменшуватися до нуля за скінчений проміжок часу.

Ситуація цього сценарію має місце тоді, коли суспільство у цілому не сприймає теми чи контент, які покладені в основу інформаційної атаки. Проте навіть у цьому випадку, як видно із (13), деяка частина суспільства все-таки стає жертвою цієї атаки. Це означає, що навіть у «фоновому режимі» системи протидії інформаційним атакам у кіберпросторі повинні активно працювати.

Перспективи подальших досліджень.

Побудована модель та отримані результати дозволяють здійснити захист суспільства у кіберпросторі в двох напрямках.

По-перше, можна виявляти сценарії інформаційних атак, які є найбільш шкідливі для суспільства та країни. При цьому слід врахувати, що зловмисники цілком можуть здійснювати комплексні атаки, впорядковуючи у часі, наприклад, проаналізовані вище сценарії.

По друге, після ідентифікації сценарію атаки, можна, використовуючи отримані в статті результати, розробити оптимальні заходи протидії шкідливій інформаційній атаці у кіберпросторі.

Реальні теми, контенти, фейки та штучно зроблені інформаційні події, які можуть бути використані для інформаційних атак у кіберпросторі, дають можливість здійснити класифікацію характеристик інформаційних атак у рамках описаної моделі та отриманих у статті результатів. Це дозволить сформувати базу оптимальних рішень для протидії інформаційним атакам. Також, у результаті таких досліджень, можна буде побудувати комп'ютерну систему для підтримки прийняття рішень у структурах кібербезпеки країни.

Ще один напрямок діяльності полягає у створенні методів для виявлення тих характеристик і параметрів інформаційних атак у кіберпросторі, які можуть бути виражені через кількісні значення параметрів запропонованої моделі.

Нарешті, можна сформувати постійно діючу систему соціологічних досліджень суспільства, яка в результаті дозволить виявити характеристики та параметри реакції суспільства на ті інформаційні «подразники», якими можуть скористатися зловмисники для інформаційних атак у кіберпросторі.

Висновки

В останні роки стрімко збільшується кількість інформаційних атак не лише на окремо виділені страти суспільства, але й спостерігається значний стрибок кількості цільових інформаційних атак на суспільно-психологічні процеси. Вони спричиняють, як правило, паніку та негативний вплив на життя не лише окремих

верств суспільства, але й цілих держав. У результаті виникла нагальна необхідність у розробці моделі управління протидією інформаційним атакам у кіберпросторі сучасного інформаційного суспільства. Представлена в статті модель ґрунтується на виокремлених інструментах щодо протидії негативним інформаційно-психологічним процесам як у соціальних верствах, так і у суспільстві в цілому.

Розроблена модель основана на нелінійному диференційному рівнянні, яке описує як зміну у часі кількості суб'єктів, так і відповідні задачі, поставленні перед службою кіберпезпеки для запобігання негативним наслідкам потенційних чи реалізованих кібератак. Це дало змогу дослідити в динаміці кількість суб'єктів, які підпадають під вплив інформаційної атаки. Виділено та детально проаналізовано чотири можливі варіанти (сценарії) поведінки запропонованої моделі. Це надало можливість сформувати ефективні методи для ефективного управління процесом протидії інформаційним атакам. Також у роботі, залежно від обраного поведінкового варіанту розробленої моделі, було представлено інтерпретацію чотирьох можливих варіантів (сценаріїв) розгортання протидії негативним наслідкам потенційних чи реалізованих інформаційних атак у кіберпросторі сучасного інформаційного суспільства.

На основі отриманих результатів можна розробити потужні методи для виявлення характеристик і параметрів інформаційних атак у кіберпросторі, через які можуть бути виражені кількісні значення параметрів запропонованої моделі. Таким чином, відкриваються можливості для розробки комп'ютерної системи для підтримки прийняття рішень на їхній основі для структур управління кібербезпекою країни в цілому.

1. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150–157.

2. Хорошко В.О., Хохлачова Ю.Є., Кібальчич І.В. Концепція кібербезпеки та моделювання процесів оптимального управління системою кіберзахисту держави. *Інформатика та математичні методи в моделюванні*. 2020. Т. 10, № 3–4. С. 230–242.

3. Манойло А.В. Государственная информационная политика в особых условиях. Москва: МИФИ, 2003. 388 с.

4. Улічев О., Мелешко Є. Моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі. *Захист інформації*. 2020. Т. 22, № 3. С. 166–176.

5. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Київ: «МК-Прес», 2005. 432 с.

6. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. Москва: МЦНМО, 2010. 228 с.

7. Курносов Ю.В. Аналитика как интеллектуальное оружие. Москва: РУСАКИ, 2012. 613 с.

8. Mistakes, Errors and Failures across Cultures. Eds E. Vanderheiden, C.-H. Mayer. Switzerland: Springer Nature AG, 2020. 624 p.

9. Geiss R., Lahmann H. Protecting Societies: Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats (February 01, 2021). 20 p. Available at SSRN URL: https://ssrn.com/abstract=3851137 or http://dx.doi.org/10.2139/ssrn.3851137.

10. Опірський І.Р., Ткач Ю.М., Хорошко В.О. Виявлення кібератак в інформаційних мережах. *Інформатика та математичні методи в моделюванні*. 2020. Т. 10, № 3-4. С. 177–189.

11. Pyskun I., Tkach Yu., Khoroshko V., Khokhlachova Yu., Ayasrah A., Al-Dalvash A. Quantitative assessment and determination of the level of cyber security of state information systems. *Ukrainian Scientific Journal of Information Security*. 2020. Vol. 26, No. 3. P. 131–138.

Надійшла до редакції 10.06.2021