DOI: 10.18372/2310-5461.44.14318

УДК 004.9:629

К. О. Соколов
Управління інформаційних технологій Міністерства оборони України
orcid.org/0000-0002-5182-5569
e-mail: saks555skat@gmail.com;

О. П. Гудима, канд. техн. наук, старш. наук. співроб.
Управління інформаційних технологій Міністерства оборони України
orcid.org/0000-0002-3494-8583
e-mail: Olgud18@gmail.com

ПІДХІД ДО РОЗРОБКИ ЕЛЕМЕНТІВ СТРУКТУРИ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ВПЛИВУ У КІБЕРПРОСТОРІ

Вступ

Світова тенденція щодо зростання кількості користувачів сервісів соціальних інформаційних мереж продовжує зберігати динаміку до зростання.

Це пов'язане з тим, що всесвітнє інформаційне середовище має суттєві переваги над звичайними засобами і технологіями, а саме:

- оперативність (розміщення і регулярне оновлення інформації не потребують значного часу на підготовку матеріалів в електронному вигляді. Користувачі отримують її в режимі реального часу);
- економічність (залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених завдань);
- скритність джерела впливу (як правило, акт агресії в глобальній мережі важко відрізнити від дії звичайних комп'ютерних хуліганів).

Кіберпростір надає широкі можливості для впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації).

Підготувати та провести кібератаку з використанням всесвітнього інформаційного середовища може досить широке коло осіб — від військових і розвідувальних структур іноземних держав до партизанських формувань, злочинців, промислових конкурентів, хакерів або просто озлоблених людей.

Відстежити ж джерело досить складно. Таким чином всесвітнє інформаційне середовище стало новим майданчиком інформаційного впливу, що має ряд суттєвих переваг над класичними методами впливу.

Постановка проблеми в загальному вигляді

Питанням інформаційної та кібернетичної безпеки в електронних засобах масової інформації в країнах світу приділяється суттєва увага.

Відповідно до меморандуму 2017 р. у Гельсінкі (Фінляндія) за участю США, Франції, Німеччини, Швеції, Польщі, Фінляндії, Латвії, Литви створено Європейський центр з протидії гібридним загрозам, який є міждержавним, європейським Центром боротьби з гібридними загрозами — кібератаками, пропагандою та дезінформацією. Передбачається, що Центр формуватиме мережу експертів для країн-учасниць та буде тісно співпрацювати з Євросоюзом і НАТО.

Велика Британія з метою протистояння російській загрозі в 2019–2020 роках має намір створити кібервійська. Кібервійська нараховуватимуть 2 тис. осіб, а фінансування, становитиме понад 250 млн фунтів стерлінгів.

В Україні основні завдання щодо захисту кіберпростору визначені в:

– Законі України від 21.06.2018 № 2469-VIII «Про національну безпеку України»;

– Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII (із змінами), № 2469-VIII від 21.06.2018;

– Указі Президента України від 15 березня 2016 року № 96/2016 «Про Стратегію кібербезпеки України».

Вище зазначене вимагає створення в Міністерстві оборони України та Збройних Силах України відповідної Системи (організаційної структури) з виявлення деструктивного впливу в кіберпросторі та реагування на інформаційні загрози (далі — Система).

На сьогодні, Міністерством оборони України проведена значна робота за даним напрямом.

Результатом проведеної роботи є формування загального вигляду і де-факто організація діяльності окремих складових Системи.

Основними завданнями Системи є:

- виявлення, оцінювання та прогнозування розвитку потенційних та реальних інформаційних загроз у воєнній сфері;
- проведення попереджувальних інформаційних та інших заходів щодо їх нейтралізації;
- протидія зовнішньому інформаційному впливу (інформаційним заходам), спрямованому на послаблення обороноздатності держави;
- забезпечення розвитку і кіберзахисту інформаційної інфраструктури та інформаційних ресурсів МО України та ЗС України;
- підготовка та захист об'єктів критичної інформаційної інфраструктури держави у воєнній сфері (у тому числі від кібератак);
- підготовка і ведення дій в інформаційному просторі, спрямованих на запобігання виникненню воєнних конфліктів, стримування потенційного агресора у разі виникнення передумов застосування проти України воєнної сили та відсічі збройній агресії проти України та ін.

Для реалізації основних завдань Системи формується її структура із ряду підсистем.

У статті зосереджена увага на підсистемі виявлення, оцінювання деструктивного впливу та прогнозування розвитку, планування заходів нейтралізації (протидії) і безпосередньо на її елементі — що здійснює заходи з виявлення та оцінювання деструктивного впливу, що в подальшому може привести до формування інформаційної загрози.

Розглянемо один з підходів, що стосується питання формування структур з моніторингу кіберпростору та виявлення деструктивного впливу.

Аналіз останніх досліджень і публікацій

Теоретичну основу синтезу складних інформаційних систем та систем накопичення, архівації цільової інформації (інформаційних систем (ІС)) становлять праці А. В. Малишевського [1], А. В. Лукацкого [2], Г. Хакена [3], О. В. Палагіна [4], О. Є. Стрижака [5], Г. Бучи [6], О. Г. Славко [7], В. О. Куланова [8].

У наукових працях вітчизняних і зарубіжних учених окремі аспекти даної проблеми ще недостатньо висвітлені.

Як правило, збільшення кількості і щільності потоку деструктивної інформації (деструктивних впливів) та їх типів відпрацьовується збільшенням елементів структури за відповідними призначенням і рівнем, що породжує інформаційну надмірність даних для обробки. Зазначене не дозволяє реалізувати оперативне виявлення деструктивних впливів (деструктивних кібердій), динамічний перерозподіл обмежених сил і засобів спостереження і дій з урахуванням рівня реалізації і ефективності поточних завдань та інформативності і доступності джерел даних про зовнішню обстановку і унеможливлює функціонування інформаційної системи в умовах реального часу, що може призвести до зриву виконання цільових завдань реагування на кібердії противника.

Мета статті

Ураховуючи вище зазначене **метою статті** є висвітлення підходу щодо побудови елементів структури системи виявлення деструктивного впливу (деструктивних кібердій) у кіберпросторі.

Виклад основного матеріалу дослідження

Аналіз відомих методологічних підходів до реалізації процесів та побудови інформаційних систем спрямованих на моніторинг процесів та інформаційних потоків і результати їх практичного застосування переконливо доводить наявність проблем у принципах побудови та методологічній базі обробки в них інформації. Першою причиною цього є інформаційна надмірність даних моніторингу, що породжена самоціллю створення, розвитку та застосування єдиного інформаційного простору. Характерним, при цьому є постійне зростання кількості інформаційних джерел та технічних засобів моніторингу різного типу, формату даних, повнотою, достовірністю та своєчасністю первинної інформації, а також споживачів інформації.

Технологічно побудова відомих інформаційних систем, спрямованих на моніторинг процесів та інформаційних потоків, орієнтована на формуванні статичної надмірної структури системи і алгоритмів їх функціонування з рівномірним розподілом завдань між усіма її складовими та вибірковістю елементів лише за їх призначенням і ієрархією горизонтально-вертикальних зв'язків.

Першочерговим завданням під час побудови структури є здійснення ідентифікації деструктивної інформації (деструктивного впливу, деструктивних кібердій), що потребує встановлення переліку індикаторів, та класифікаційних характеристик. Процес інформаційного впливу в загальному уявленні здійснюється через інформаційні джерела різного типу. Як інформаційні джерела будемо розглядати Інтернет-простір (кіберпростір), окрема особистість чи їх група тощо. Інформаційне джерело вміщує у собі інформаційні повідомлення. Будемо класифікувати індикатори деструктивного впливу за: класами деструктивного впливу; групами деструктивного впливу; видами деструктивного впливу (табл. 1).

Таблиця 1

Класифікація індикаторів деструктивного впливу

Клас деструктивного впливу	Група деструктивного впливу	Види деструктивного впливу
За рівнем та типом об'єкту впливу	Загрози державі	Проведення державної політики
		Цілісність держави
		Науково-технічні ресурси
		Розвиток індустрії та інформаційниї технологій
		Забезпечення потреб внутрішнього ринку в національній продукції
		Забезпечення накопичення, збереження та ефективного використання національних інформаційних ресурсів
	Загрози суспільству та особистості	Забезпечення діяльності суспільних об'єднань, колективів та окремих їх представників
		Загрози правам і свободам людини у галузі духовного життя
		Індивідуальні, групові та суспільні свідомості
	Загрози технічним засобам інформаційно-комунікаційних систем та технологій	Інформаційно-телекомунікаційні системи загального призначення
		Інформаційно-телекомунікаційні системи спеціального призначення

Орієнтовні індикатори деструктивного впливу: класом деструктивного впливу — за рівнем та типом об'єкту впливу, групою деструктивного впливу — загрози державі, вид деструктивного впливу — проведення державної політики представлені в табл. 2.

Таблиця 2

Індикатори деструктивного впливу щодо проведення державної політики

Вид деструктивного впливу	Індикатори деструктивного впливу
Проведення державної політики	Монополізація інформаційного ринку, його окремих секторів національними та закордонними інформаційними структурами
	Деформація системи масового інформування за рахунок монополізації засобів масової інформації та неконтрольованого розширення сектору закордонних засобів масової інформації в національному інформаційному просторі
	Блокування діяльності державних засобів масової інформації щодо інформування національної і закордонної аудиторії
	Зниження ефективності інформаційного забезпечення державної політики внаслідок дефіциту кваліфікованих кадрів, відсутності системи формування і реалізації державної інформаційної політики
	Розповсюдження дезінформації про політику держави, діяльність органів державної влади, події, що відбуваються в країні та за кордоном
	Блокування діяльності національних засобів масової інформації щодо роз'яснення закордонній аудиторії цілей і основних напрямків національної державної політики
	Інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію стратегії зовнішньої і внутрішньої політики держави
	Розповсюдження за кордоном дезінформації про зовнішню та внутрішню політику держави
	Порушення прав громадян та юридичних осіб в інформаційній сфері за кордоном
	Спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфраструктуру національних органів виконавчої влади, що реалізують зовнішню політику держави, національних представництв та організацій за кордоном, національних представництв у міжнародних організаціях

Закінчення табл. 2

Вид деструктивного впливу	Індикатори деструктивного впливу
	Порушення встановленого порядку збору, обробки, зберігання та передачі інформації в національних органах влади, що реалізують зовнішню політику, і на підвідомчих їм підприємствах, в установах і організаціях
	Інформаційно-пропагандистська діяльність політичних сил, громадських об'єднань, засобів масової інформації та окремих осіб, що викривляє стратегію і тактику національної зовнішньополітичної діяльності
	Недостатня інформованість населення про національну зовнішньополітичну діяльність

Дані представлені в табл. 1, 2 будуть використовуватися під час формування елементів структури (формування кількості автоматизованих робочих місць та розподілу завдань за напрямками) виявлення деструктивного впливу у кіберпросторі.

Для виявлення деструктивного впливу в інформаційних повідомленнях здійснюється їх контент-аналіз за одиницею аналізу — елементом тексту, що підлягає виявленню в інформаційних повідомленнях (певне поняття, тема, ситуація, подія).

Одиниця аналізу в інформаційному джерелі відображається числом — кількістю (частотою) появи одиниці аналізу. Окрім кількості (частоти) появи одиниць аналізу, оцінюється частота перегляду інформаційних повідомлень та частота перегляду інформаційних джерел. Реакція об'єкта на контент інформаційного повідомлення фактично оцінюється зазначеними показниками, що мають конкретну об'єктивну числову міру. Кінцевим же результатом є зміна настанов, намірів, суджень, оцінок та (або) поведінки об'єкту впливу (окремого індивіду чи (або) групи).

Оцінку (ознаку) рівня деструктивного впливу слід визначати на основі аналізу інформаційних повідомлень, виходячи з сформованих індикаторів деструкційного впливу, що міститься на конкретному інформаційному джерелі. У табл. 3 наведені сформовані ознаки деструктивного впливу за їх рівнем.

Таблиця 3

Рівні ознак деструктивного впливу

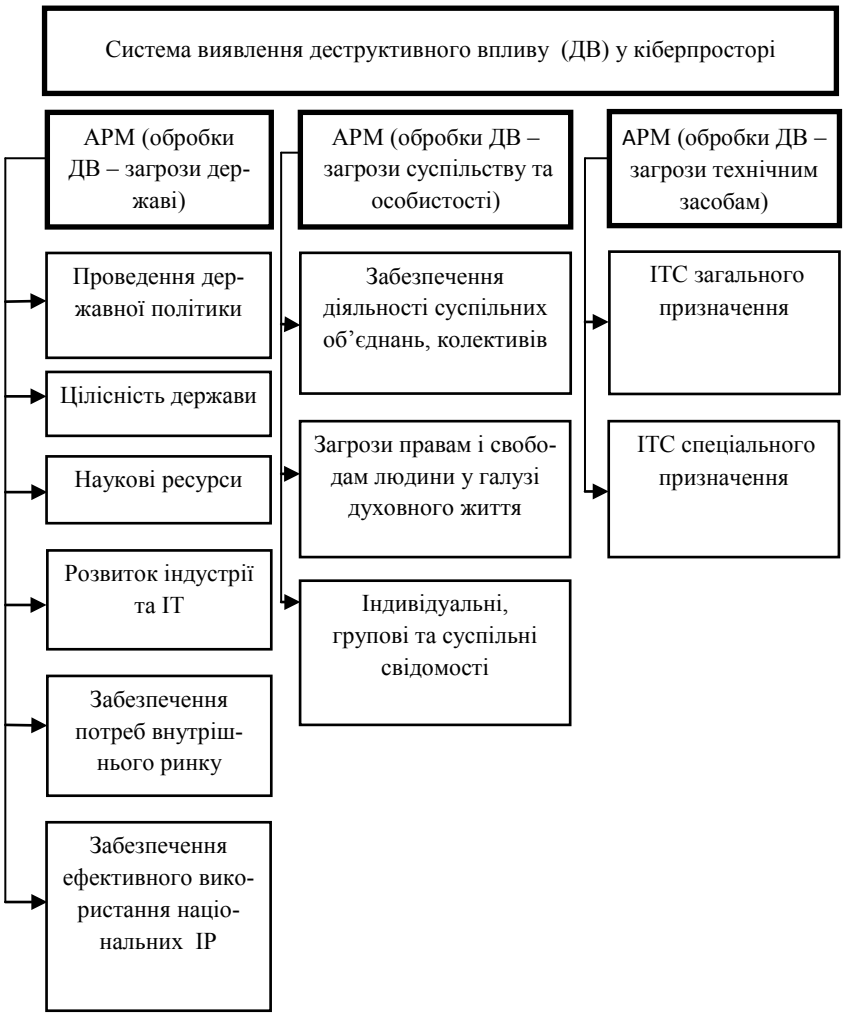
Рівень ознаки	Лінгвістична категорія рівня ознаки	Зміст
5	Високий	Активні усі групи деструктивного впливу
4	Підвищеної уваги	Активні більше 55 % груп деструктивного впливу
3	Середній	Активні 45–55 % груп
2	Застережний	Активні менше за 45 % груп деструктивного впливу
1	Низький	Активна хоча б одна класифікаційна група деструктивного впливу

Основними критеріями при опрацюванні елементів системи, яка буде забезпечувати автоматизоване виявлення деструктивного впливу у кіберпросторі, це забезпечення: виконання найбільшої кількості функцій автоматизованим робочим місцем із заданих математичною моделлю деструктивного впливу $T_{Sj} \to \max$; найбільшу кількість використаних інформаційних джерел для виявлення деструктивного впливу $T_{Sj} \to \max$ з найкращими технічними характеристиками (ТХ) $T_{Sj} \to \max$. Поряд з цим забезпечення (підвищення) необхідної оперативності надання результатів роботи та достовірності.

Виходячи з викладеного вище та спираючись на метод експертних оцінок попередня структура елементу системи виявлення деструктивного впливу в електронних засобах масової інформації (кіберпросторі) з виявлення та оцінювання деструктивного впливу зображена на рисунку.

Висновки

1. Сьогодні на Україну здійснюється потужний інформаційний вплив шляхом поширення неповної або упередженої інформації через інформаційний простір. Це зумовлено, насамперед, прагненням керівництва іноземних держав впливати на зовнішню та внутрішню політику України. Натепер актуальним завданням для України є моніторинг загроз інформаційній безпеці для реалізації інформаційної політики, спрямованої на забезпечення національних інтересів.



Структура елементу системи виявлення деструктивного впливу в електронних засобах масової інформації (кіберпросторі) з виявлення та оцінювання деструктивного впливу

2. Організований інформаційний вплив на людей є специфічним явищем сучасності, важливим і ефективним засобом досягнення різних цілей на тактичному, оперативному і стратегічному рівнях. Негативний інформаційний вплив інформаційних повідомлень все частіше використовується як зброя. Контент-моніторинг кіберпростору з метою виявлення деструктивного впливу дасть змогу підвищити ефективність забезпечення інформаційної безпеки України у воєнній сфері та сприятиме:

- підвищенню ефективності оцінки, прогнозуванню розвитку суспільно-політичної та соціально-економічної обстановки в державі, в регіоні та в світі в цілому;
- оперативній оцінці наслідків різних рішень і вибору з них найбільш раціональних;
- визначенню області ризику з найбільшою можливістю і величиною збитку у випадку реалізації ризиків;
- переходу від прийняття окремих рішень до вироблення комплексних сценаріїв (загальносистемних рішень), коли кожне окреме рішення підпорядковано забезпеченню довгострокових цілей держави.

3. У подальшому буде розроблено метод автоматизованого формування типової структури Системи (організаційної структури) з виявлення деструктивного впливу в кіберпросторі та реагування на інформаційні загрози.

ЛІТЕРАТУРА

1. **Малишевський А. В**. Качественные модели в теории сложных систем. М.: Наука. Физматлит. 1998. 528 с.

2. **Лукацкий А. В.** Обнаружение атак: [Критерии атак и признаки их обнаружения. Источники информации об атаках и методы их анализа. Классификация систем обнаружения атак. Критерии оценки систем обнаружения атак. Выбор и построение инфраструктуры обнаружения атак. Установка, размещение и эксплуатация систем обнаружения атак]. 2. изд. СПб.: БХВ-Петербург, 2003. 596 с.

3. **Хакен Г.** Синергетика. М.: Мир, 1980. 406 с.

4. **Палагін О. В.**, Малахов К. С., Величко В. Ю., Щуров О. С. Проектування та програмна реалізація підсистеми створення та використання онтологічної бази знань публікацій наукового дослідника [Електронний ресурс]. *Проблеми програмування*. 2017. № 2. С. 72-81. URL: http://nbuv.gov.ua/UJRN/Progr_2017_2_8 (дата звернення 11.09.2019).

5. **Стрижак О. Є.** Інструменти інформаційно-аналітичного супроводу процесів моніторингу. *Екологічна безпека та природокористування*. 2014. Вип. 14. С. 180-191. URL: http://nbuv.gov.ua /UJRN/ebpk_2014_14_20 (дата звернення 11.09.2019)

6. **Буч Г.** Обьектно-ориентированное проектирование с примерами применения. М.: ООО «И. Д. Вильямс», 2008. 720 с.

7. **Славко О. Г.** Ідентифікація узагальнених параметрів математичної моделі комп'ютерної мережі в задачі забезпечення QOS. *Радіоелектронні і комп'ютерні системи.* 2010. № 3. С. 68–74. URL: http://nbuv.gov.ua/UJRN/recs_2010_3_13. (дата звернення 11.09.2019)

8. **Куланов В. А.** Об оценке диверсности реализации минимальных форм функций в различных базисах. *Радіоелектронні і комп'ютерні системи.* 2008. Вип. 5(32). С. 34–65.

Соколов К. О., Гудима О. П.

ПІДХІД ДО РОЗРОБКИ ЕЛЕМЕНТІВ СТРУКТУРИ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ВПЛИВУ У КІБЕРПРОСТОРІ

У статті розглянуто питання аналізу інформації та виявлення деструктивного впливу у кіберпросторі. В умовах зростання кількості користувачів сервісів соціальних інформаційних мереж з кожним роком і враховуючи суттєві переваги всесвітнього інформаційного середовища над звичайними засобами і технологіями загострюються питання інформаційної та кібернетичної безпеки в електронних засобах масової інформації (кіберпросторі) в країнах світу, де створюються відповідні організаційні структури з протидії гібридним загрозам. Зазначене вимагає створення відповідних структур в Україні.

Збільшення кількості і щільності потоку деструктивної інформації (деструктивних впливів) та їх типів відпрацьовується збільшенням елементів структури за відповідними призначенням і рівнем, що породжує інформаційну надмірність даних для обробки.

Зазначене не дозволяє реалізувати оперативне виявлення деструктивних впливів (деструктивних кібердій), динамічний перерозподіл обмежених сил і засобів спостереження і дій з урахуванням рівня реалізації і ефективності поточних завдань та інформативності і доступності джерел даних про зовнішню обстановку і унеможливлює функціонування інформаційної системи в умовах реального часу, що може призвести до зриву виконання цільових завдань реагування на кібердії противника. Враховуючи вище зазначене метою статті є висвітлення підходу щодо побудови елементів структури системи виявлення деструктивного впливу (деструктивних кібердій) у кіберпросторі в межах створення в Міністерстві оборони України та Збройних Силах України відповідної Системи (організаційної структури) та буде зосереджена увага на її елементі, що здійснює заходи з виявлення та оцінювання деструктивного впливу.

Базуючись на визначених критеріях та враховуючи індикатори деструктивного впливу сформовано структуру елементу системи виявлення деструктивного впливу в електронних засобах масової інформації (кіберпросторі) з виявлення та оцінювання деструктивного впливу.

Ключові слова: кіберпростір; інформація; вплив; індикатори; система; синтез.

Sokolov K. O., Hudyma O. P.

THE APPROACH TO DEVELOPMENT OF THE ELEMENTS OF THE STRUCTURE OF THE DESTRUCTIVE IMPACT DETECTION SYSTEM IN CYBER SPACE

The article addresses the problematic issue of analyzing information and detecting destructive effects in cyberspace. With the increasing number of users of social information network services every year, and given the significant advantages of the global information environment over conventional media and technologies, issues of information and cyber security in electronic media (cyberspace) in the world where appropriate organizational structures to counteract the hybrid organization Typically, an increase in the amount and density of the destructive information flow (destructive effects) and their types is accomplished by an increase in the structure elements for their intended purpose and the level that generates al structures are created. threats. This requires the creation of appropriate structures in Ukraine.

information redundancy for processing.

The above does not allow to realize prompt detection of destructive effects (destructive cyberdias), dynamic redistribution of limited forces and means of observation and actions taking into account the level of realization and efficiency of current tasks and informativeness and availability of sources of data about the external situation and preventing the functioning of information conditions, can disrupt the adversary's cyber response targets.

Given the above, the purpose of the article is to highlight the approach to building elements of the structure of the system of detection of destructive impact (destructive cyberdias) in cyberspace within the creation in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine of the appropriate System (organizational structure) and will

focus on its element, which implements to identify and evaluate destructive effects. Based on the defined criteria and taking into account the indicators of destructive impact, the structure of the element of the system of detection of destructive influence in electronic media (cyberspace) for the detection and evaluation of destructive influence is formed.

Keywords: cyberspace; information; influence; indicators; system; synthesis.

Соколов К.О., Гудыма О.П.

ПОДХОД К РОЗРАБОТКЕ ЭЛЕМЕНТОВ СТРУКТУРЫ СИСТЕМЫ ОБНАРУЖЕНИЯ ДЕСТРУКТИВНОГО ВЛИЯНИЯ В КИБЕРПРОСТРАНСТВЕ

В статье рассмотрен вопрос анализа информации и выявления деструктивного влияния в киберпространстве. В условиях роста количества пользователей сервисов социальных информационных сетей с каждым годом и учитывая существенные преимущества всемирной информационной среды над обычными средствами и технологиями обостряются вопросы информационной и кибернетической безопасности в электронных средствах массовой информации (киберпространстве) в странах мира, где создаются соответствующие организационные структуры по противодействию гибридным угрозам. Указанное требует создания соответствующих структур в Украине.

Увеличение количества и плотности потока деструктивной информации (деструктивных воздействий) и их типов отрабатывается увеличением элементов структуры по соответствующим назначениям и уровням, порождает информационную избыточность данных для обработки.

Указанное не позволяет реализовать оперативное выявление деструктивных воздействий (деструктивных кибердействий), динамическое перераспределение ограниченных сил и средств наблюдения и действий с учетом уровня реализации и эффективности текущих задач и информативности и доступности источников данных о внешней обстановке и делает невозможным функционирование информационной системы в условиях реального времени, может привести к срыву выполнения целевых задач реагирования на кибердействия противника. Целью статьи является освещение подхода к построению элементов структуры системы выявления деструктивного воздействия (деструктивных кибердействий) в кибепрпространстве в рамках создания в Министерстве обороны Украины и Вооруженных Силах Украины соответствующей Системы (организационной структуры) и будет сосредоточено внимание на ее элементе, который осуществляет мероприятия по выявлению и оценке деструктивного воздействия.

Основываясь на определенных условиях и учитывая индикаторы деструктивного влияния сформирована структура элемента системы обнаружения деструктивного влияния в электронных средствах массовой информации (киберпространстве) по выявлению и оценке деструктивного воздействия.

Ключевые слова: киберпространство; информация; влияние; индикаторы; система; синтез.

Стаття надійшла до редакції 06.11.2019 р.
Прийнято до друку 04.12.2019 р.