УДК 354.42

О.М. Косогов

Військова частина 1906, Київ

МЕТОДИКА ВИЗНАЧЕННЯ ЗАХОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ ДЕРЖАВІ У ВОЄННІЙ СФЕРІ

На основі аналізу взаємодії логічного ланцюжка джерела загроз – загрози – реалізація загроз (атаки) – уразливості – об'єкти – наслідки (збиток) – заходи протидії розроблено методику визначення заходів протидії інформаційним загрозам державі у воєнній сфері. У межах наведеної методики оцінка ризиків здійснюється за допомогою оцінювання можливості реалізації загроз безпеці, пов'язаних з уразливостями, властивими тим чи іншим об'єктам інформаційної безпеки. Наведено варіант графу аналізу інформаційних загроз та протидії їм, який складається за результатами аналізу.

Ключові слова: *інформаційна безпека, загрози інформаційній безпеці, система протидії, воєнна сфера.*

Введение

Постановка проблеми. Аналіз літератури. На сьогодні світовий геополітичний простір та внутрішньодержавні відносини формуються в умовах інформаційного протиборства. Для нашої держави ця проблема особливо актуальна: зважаючи на певну невизначеність геополітичного статусу, політичну нестабільність, нестійкість вітчизняного інформаційного простору, Україна перебуває під систематичним інформаційним тиском.

В умовах збройної агресії Росії проти України, а саме анексії Криму, підбурювання, організації та всебічного забезпечення збройного протистояння на Сході нашої держави, проявляється нова тенденція ведення Росією воєнних дій.

Відомий американський військовий теоретик Френк Хоффман одним з перших зазначив: "…війни сучасної епохи характеризує процес гібридизації, у рамках якого змішуються традиційні форми війни, кібервійни, організованої злочинності, іррегулярних конфліктів, тероризму тощо" [1].

Водночас всі ці заходи супроводжуються цілеспрямованою потужною інформаційною кампанією. В часи інтенсивного розвитку інформаційних технологій, наявності глобальних інформаційних мереж і не менш глобалізованих засобів масової інформації, складова "інформаційного супроводу" у гібридних війнах має надзвичайно важливе, якщо не вирішальне, значення. У цих умовах гостро постає проблема захисту національного інформаційного простору.

Враховуючи викладене, пошук шляхів надійного виявлення інформаційних загроз та протидії їм є актуальним науковим та практичним завданням.

Процес забезпечення безпеки інформації повинен носити комплексний характер і має ґрунтуватися на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їхньому прояву (уразливостей) і, як наслідок, визначення актуальних загроз інформаційній безпеці [2].

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з ідентифікованими джерелами загроз, всім ідентифікованим джерелам загроз і уразливостям (факторам) зіставлені методи реалізації.

При цьому важливо мати можливість, у разі потреби, не міняючи самого методичного інструментарію, вводити нові види джерел загроз, методів їх реалізації, уразливостей, які стануть відомі в результаті подальшого отримання знань у цій сфері.

Виходячи з такого принципу, моделювання й класифікацію джерел загроз, загроз та їх проявів, а також розробку ефективних заходів протидії доцільно проводити на основі аналізу взаємодії логічного ланцюжка: Джерела загроз → Загрози → Реалізація загроз (атаки) → Уразливості →Об'єкти → Наслідки (збиток) → Заходи протидії.

Виявлення та аналіз загроз інформаційній безпеці є першим етапом у розробці стратегії протидії інформаційних загроз (політики безпеки). При цьому процес виявлення та аналізу загроз слід розглядати в органічному зв'язку з процесом протидії загрозам.

Аналіз спеціалізованої літератури, наприклад [2-5], показує, що на сьогодні у нашій державі та її Збройних Силах триває інтенсивний процес її формування, а саме у Міністерстві оборони України розроблені концептуальні документи та плани щодо розгортання такої системи, у Збройних Силах України створюються відповідні підрозділи. Разом з тим, методичне забезпечення ефективної протидії інформаційним загрозам державі в особливий період, в умовах якого цільовою аудиторією такого впливу розглядається особовий склад військ (сил) та органи військового управління, а об'єктами інформаційно-технічного впливу – засоби управління військами та

зброєю, вивчено недостатньою мірою [6–9].

Тому розробка методики визначення заходів протидії інформаційним загрозам державі у воєнній сфері є актуальним науково-практичним завданням.

Метою статті є викладення методики визначення заходів протидії інформаційним загрозам державі у воєнній сфері.

Основний матеріал

Процес забезпечення безпеки інформації повинен носити комплексний характер і має ґрунтуватися на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їхньому прояву (уразливостей) і, як наслідок, визначення актуальних загроз інформаційній безпеці.

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з ідентифікованими джерелами загроз, всім ідентифікованим джерелам загроз і уразливостям (факторам) зіставлені методи реалізації.

При цьому важливо мати можливість, у разі потреби, не міняючи самого методичного інструментарію, вводити нові види джерел загроз, методів їх реалізації, уразливостей, які стануть відомі в результаті подальшого отримання знань у цій сфері.

Виходячи з такого принципу, моделювання й класифікацію джерел загроз, загроз та їх проявів, а також розробку ефективних заходів протидії доцільно проводити на основі аналізу взаємодії логічного ланцюжка: Джерела загроз → Загрози → Реалізація загроз (атаки) → Уразливості → →Об'єкти → Наслідки (збиток) → Заходи протидії.

Виявлення та аналіз загроз інформаційній безпеці є першим етапом у розробці стратегії протидії інформаційних загроз (політики безпеки). При цьому процес виявлення та аналізу загроз слід розглядати в органічному зв'язку з процесом протидії загрозам. Процес аналізу починається з визначення основних загроз та їх джерел (табл. 1, 2) .

Таблиця 1

Зразок таблиці
переліку загроз інформаційній безпеці

№ загрози	Зміст загрози
1	Загроза 1
…	…
n	Загроза n

Таблиця 2

Зразок таблиці
переліку джерел загроз інформаційній безпеці

№ джерела	Джерело
1	Джерело 1
…	…
n	Джерело n

На основі ідентифікованих загроз та їх джерел аналогічним чином складаються таблиці методів реалізації загроз (атак), можливих у даній сфері, уразливостей об'єктів, якими ці атаки можуть скористатися, переліку об'єктів забезпечення інформаційної безпеки та заходів забезпечення інформаційної безпеки.

Таким чином, на першому етапі аналізу загроз ідентифікуються всі елементи множин загроз, джерел, об'єктів і заходів забезпечення інформаційної безпеки.

На другому етапі необхідно експертним методом встановити відносини між такими видами елементів.

"Джерела загроз – загрози□, тобто встановити, яке джерело породжує які загрози.

"Загрози – атаки", – встановити, яка загроза через яку атаку реалізується.

"Атаки – уразливості", – встановити, яка атака використовує які уразливості.

"Уразливості – об'єкти захисту", – встановити, яка уразливість належить до якого об'єкту захисту.

"Заходи протидії – загрози", – встановити який захід протистоїть якій загрозі.

Результати такого аналізу представляються в матричній формі на основі припущення, що між елементами множин можна встановити певне бінарне відношення "є причиною".

На цьому етапі здійснюється аналіз визначення відносин між елементами наведених множин. Джерело загроз 1 (наприклад, спеціальні служби іноземних держав) мають пряму зацікавленість як в отриманні конфіденційної інформації про діяльність Збройних Сил України, так і у впливі на цю діяльність.

Таким чином, джерело 1 має відносини з першими трьома загрозами (наприклад, розвідувальною діяльністю іноземних спецслужб, інформаційно-технічними та інформаційно-психологічними впливами з боку ймовірних (можливо неявних) противників).

Аналогічно аналізуються відносини між усіма джерелами та загрозами.

У табл. 3 наведено варіант матриці відносин "Джерела загроз – загрози" ("1" відповідає припущенню, що дане джерело породжує дану загрозу; "0" – відсутність відносин між цими елементами множин. За таким же принципом складаються матриці відносин загроз і атак, атак і уразливостей. Аналіз відносин атак і уразливостей особливо важливий, тому що ілюструє відносини об'єкта забезпечення з оточуючим середовищем, показуючи, які уразливості, можуть використовувати реалізації загроз.

У подальшому складаються матриці відносин "Уразливості – об'єкти забезпечення ІБ'', "Заходи протидії – загрози".

Таблиця 3

Матриця відносин
"Джерела загроз – загрози" (варіант)

		Загрози								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Джерела загроз	**1**	1	1	1	0	0	0	0	0	0
	2	0	0	0	1	0	0	0	0	1
	3	0	0	0	0	1	1	1	0	0
	4	0	0	0	0	0	0	1	0	0
	5	0	0	0	0	0	0	0	1	0

Після аналізу відносин між елементами множин, виділених у процесі ідентифікації, проводиться оцінка ризиків. Цей процес дозволяє мінімізувати витрати ресурсів на заходи протидії. У процесі аналізу можливих і виявлення актуальних загроз оцінюється ризик, що виникає внаслідок потенційного впливу певної загрози.

Відомо декілька різних методик аналізу та оцінки ризиків (переважно закордонних). Усі вони дозволяють отримати лише якісну їх оцінку на основі експертних методів.

У межах наведеної методики оцінка ризиків здійснюється за допомогою оцінювання можливості реалізації загроз безпеці, пов'язаних з уразливими, властивими тим чи іншим об'єктам інформаційної безпеки. На основі аналізу впливу загроз, їм приписується високий, середній або низький рівень ризику по кожній зоні локалізації уразливостей.

При проведенні оцінки ризиків розглядаються три основні категорії втрат. Вони самі та їх опис наведено в табл. 4.

Матриця оцінки ризиків розділена на зони локалізації уразливостей. У межах кожної уразливості перераховуються потенційні загрози. Праворуч від кожної загрози наводяться рівні в рамках категорій втрат.

Матриця заповнюється доданням рівня ризику – високого (В), середнього (С) або низького (Н) - щоб показувати залежність кожної загрози від кожної із зон локалізації уразливості з урахуванням заповнення раніше матриці "Загрози – об'єкт забезпечення інформаційної безпеки".

Таблиця 4

Категорії наслідків реалізації загроз

Категорії наслідків	Опис
Фінансові збитки	Визначаються збільшенням витрат на відновлення та удосконалення технічних (програмних) засобів елементів інформаційної інфраструктури МО України та Збройних Сил України
Зниження ефективності функціонування МО	Визначається неспроможністю структурних підрозділів МО України та Збройних Сил України ефективно виконувати покладені на них завдання внаслідок: - зниження морально-психологічного стану співробітників, а також зміни в стані психіки (психічного здоров'я); - зниження мотивації співробітників до військової служби та їх невпевненість у завтрашньому дні; - зниження боєздатності військових колективів (зниження службової активності, дезертирство, симуляція хвороб, відхилення від виконання наказів начальників, зрада, подавлення волі, неадекватна поведінка); - порушення функціонування системи управління структурними підрозділами; - несправності (виведення з ладу) технічних (програмних) засобів інформаційної інфраструктури; - порушення властивостей інформації, яка циркулює в кібернетичному просторі МО України та Збройних Сил України (конфіденційність, доступність, цілісність, спостережність)
Ускладнення діяльності МО України та ЗС України	Стосується ситуацій, що впливають на втрату суспільної довіри до МО України та Збройних Сил України, погіршення їх іміджу

Оцінка рівнів ризику може здійснюватись за такими ознаками:

високий: значна грошова втрата, втрата продуктивності або значне ускладнення діяльності, що є результатом реалізації загрози, внаслідок наявності відповідної уразливості;

середній: номінальна грошова втрата, втрата продуктивності або виникають певні ускладнення діяльності;

низький: або мінімальна можливість грошової втрати, втрати продуктивності мінімальні або не існують.

Варіант матриці оцінки ризиків наведений в табл. 5.

Таблиця 5

Матриця оцінки ризиків (варіант)

Об'єкти інформаційної безпеки	Ризик грошової втрати	Ризик втрати продуктивності	Ризик ускладнення діяльності
Об'єкт 1	Н	С	В
Об'єкт 2	С	В	Н
…	…	…	…
Об'єкт n	В	Н	С

Після заповнення матриці оцінки ризиків стає зрозумілою картина розподілу загроз і втрат від їх можливої реалізації за всіма об'єктами безпеки.

Подальшим етапом оцінки ризиків є своєрідне підбиття підсумку - складання таблиці оцінки ризиків. Таблиця оцінки ризиків заповнюється за допомогою додання об'єднаного рівня ризику кожної із зон уразливості. Об'єднаний рівень ризику слід отримувати з усіх загроз, попередньо ідентифікованих, виходячи з матриці оцінки ризиків.

Варіант оцінки ризиків наведений в табл. 6. За результатами аналізу складається граф аналізу інформаційних загроз та протидії їм (рис. 1).

Таблиця 6

Оцінка ризиків (варіант)

Об'єкти інформаційної безпеки	Категорія наслідків			
	Фінансові збитки	Зниження ефективності функціонування МО України та ЗС України	Ускладнення діяльності МО України та ЗС України	Загальний ризик
Мережа МО України та ГШ ЗС України	Середній	Високий	Високий	Високий
ЛОМ структурних підрозділів, об'єднань ЗС України	Середній	Високий	Середній	Середній
Окремі АРМ	Середній	Середній	Середній	Середній
Програмно-технічні засоби системи зв'язку	Середній	Середній	Середній	Середній
Військовослужбовці та працівники ЗС України	Високий	Високий	Високий	Високий

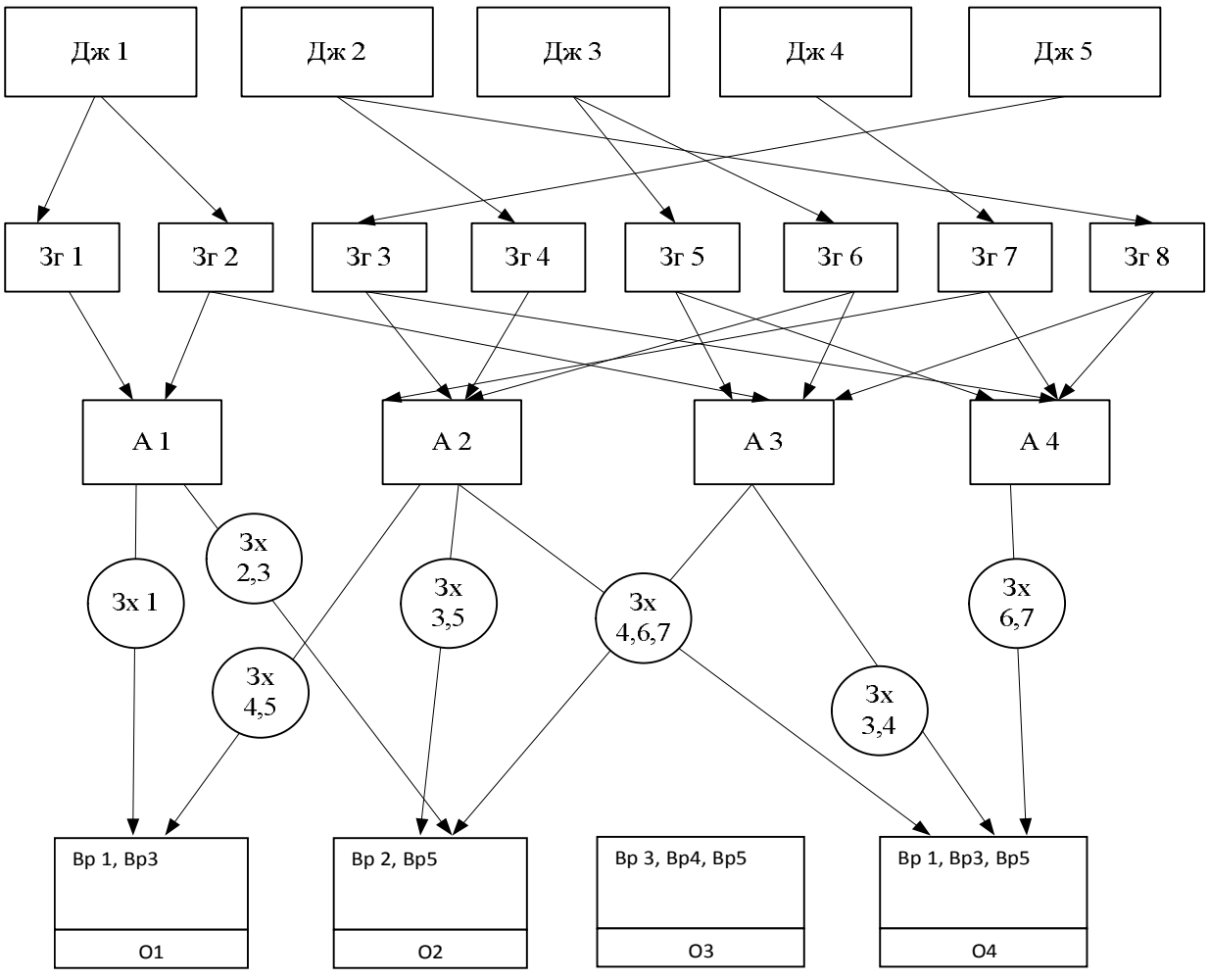

Рис. 1. Граф аналізу інформаційних загроз та протидії їм

На рис.1 позначено:

Дж – джерело загрози;

З – загроза;

А – атака;

О – об'єкт інформаційної безпеки;

Вр – уразливість об'єкту інформаційної безпеки;

Зх – захід протидії.

Висновки

Розроблено методику та алгоритм протидії інформаційним загрозам держави у воєнній сфері, яка дозволяє визначати заходи протидії інформаційним загрозам на підставі аналізу можливих негативних наслідків загроз, ідентифікації можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей).

Наведена методика є універсальною та може застосовуватись як для розробки концептуальних документів у сфері інформаційної безпеки, так і для визначення заходів протидії інформаційним загрозам конкретним інформаційним системам.

Список літератури

1. Frank G. Hoffman. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict [Електронний ресурс] / Frank G. Hoffman. – Strategic Forum. Institute for National Strategic Studies National Defense University. – No. 240. – April, 2009. – Режим доступу до матеріалу: http:// http://www.ndu.edu/inss.

2. Левченко О.В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки/ О.В Левченко//Наука і техніка Повітряних Сил Збройних Сил України. – 2015.№3(20). – С.47 – 50.

3. Ланде Д. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет-ресурсів / Д. Ланде, В. Фурашев // Правова інформатика. – 2009. – № 2 (22). – С. 49-57.

4. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: моногр. / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

5. Косогов О.М. Підхід до побудови державної системи протидії інформаційним загрозам в особливий період / О.М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2015.– Вип. 4 (45).– С. 76 – 79.

6. Литвиненко О.В. Інформаційні впливи та операції: теорет.-аналіт. нариси. Methods, means and measures for ensuring information-psychological security of person, society, country Information Security of the Person, Society and State.· № 3 (7). 2011 77 / О.В. Литвиненко. – К. : Нац. ін-т стратег.дослідж., 2003. – 239 с. – (Вип. 6 : Сер. Нац. безпека).

7. Литвиненко О.В. Спеціальні інформаційні операції : моногр. / О.В. Литвиненко. – К.: Рада нац. безпеки і оборони України, Нац. ін-т стратег. дослідж., 1999. – 163 с. – (Вип. 3 : Нац. безпека).

8. Манойло А.В. Государственная информационная политика в особых условиях : моногр. / А.В. Манойло. – М. : МИФИ, 2003. – 388 с.

9. Радковець Ю.І.Погляди на створення системи інформаційної безпеки України та її Збройних Сил / І. Радковець, О.В. Левченко, О.М. Косогов // Наука і оборона. – 2014. – № 1. – С. 38–41.

Надійшла до редколегії 29.01.2016

Рецензент: д-р техн. наук, проф. О.Б. Леонтьєв, Харківський університет Повітряних Сил імені Івана Кожедуба, Харків.

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕРОПРИЯТИЙ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ УГРОЗАМ ГОСУДАРСТВУ В ВОЕННОЙ СФЕРЕ

А.Н. Косогов

На основе анализа взаимодействия логической цепочки источники угроз – угрозы – реализация угроз (атаки) – уязвимости – объекты – последствия (ущерб) – мероприятия противодействия разработана методика определения мероприятий противодействия информационным угрозам государству в военной сфере. В рамках приведенной методики оценка рисков осуществляется с помощью оценивания возможности реализации угроз безопасности, связанных с уязвимостями, присущими тем или иным объектам информационной безопасности. Приведен вариант графа анализа информационных угроз и противодействия им, который строится по результатам анализа.

Ключевые слова: *информационная безопасность, угрозы информационной безопасности, система противодействия, военная сфера.*

METHODS OF THE DETERMINATION INFORMATION THREATS RELUCTANCES ACTIONS TO STATE IN MILITARY SPHERE

O.M. Kosogov

On base of the analysis of the interaction of the logical chain of the source of the threats - a threats - a realization of the threats (the attacks) - a criticality - an objects - a consequences (the damage) - an actions of the reluctance is designed methods of the determination action reluctances information threat state in military sphere. Within the framework of brought methods estimation risk is realized by means of risk assessment *possibility of the realization of the threats to safety, in accordance with criticality, inherent that or other object to information safety. The brought variant column analysis of the information threats and reluctances to him, which is built on result of the analysis.*

Keywords: *information security, threats to information security, system of the reluctance, military sphere.*