УДК 354.42

Олександр Миколайович Косогов *(канд. військ. наук, стар. наук. співр.)*
Військова частина А1906, Київ, Україна

МЕТОД АНАЛІЗУ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ДЕРЖАВІ У ВОЄННІЙ СФЕРІ ДЛЯ ВИЗНАЧЕННЯ АДЕКВАТНИХ ЗАХОДІВ ПРОТИДІЇ

На основі аналізу взаємодії логічного ланцюжка джерела загроз – загрози – реалізація загроз (атаки) – уразливості – об'єкти – наслідки (збиток) – заходи протидії розроблено отологічну схему забезпечення інформаційної безпеки. Встановлено, що головними цілями діяльності із забезпечення інформаційної безпеки є попередження, уникнення та ліквідація загроз об'єктам інформаційної безпеки та мінімізація можливого збитку, завданого внаслідок реалізації даних загроз. Запропоновано метода налізу та оцінювання інформаційних загроз для визначення адекватних заходів протидії цим загрозам. У межах наведеного методу оцінка ризиків здійснюється за допомогою оцінювання можливості реалізації загроз безпеці, пов'язаних з уразливостями, властивими тим чи іншим об'єктам інформаційної безпеки. .

Ключові слова: *інформаційна безпека, загрози інформаційній безпеці, джерело загрози, уразливість об'єкта, система протидії, воєнна сфера.*

Вступ

Необхідність створення дієвої системи забезпечення інформаційної безпеки Міністерства оборони України, його структурних підрозділів та Збройних Сил України обумовлюється глобалізацією світових інформаційних процесів, збільшенням ваги інформаційної складової в усіх, без винятку, сферах життєдіяльності держави і, як наслідок, лавинним зростанням різнорідних інформаційних загроз та збільшенням їхньої складності.

Непередбачуваність розвитку обстановки, постійна зміна характеру загроз, мінливість тактики протистояння з боку агресора – все це об'єктивно змушує воєнну організацію держави діяти більш гнучко та ефективно під час виконання поставлених перед ними завдань добування достовірної упереджувальної інформації, передусім військового характеру. Глибокий аналіз отриманих відомостей, аналітична обробка і своєчасне надання їх вищому воєнно-політичному й військовому керівництву держави, створює сприятливі умови для досягнення перемоги у воєнному конфлікті, уникнення зайвих жертв та руйнувань.

З іншого боку, будь-які неконтрольовані зовнішні або внутрішні процеси потенційно можуть призвести до виникнення загроз. Реалізація цих загроз, в свою чергу, негативно впливає на стан інформаційної безпеки у сфері безпеки і оборони України, що викликає різні деструктивні процеси. Порушується нормальне функціонування інформаційно-аналітичної діяльності, в результаті чого аналітики можуть дійти хибних висновків, що може призвести до прийняття вищим керівництвом держави неадекватних рішень або до значного ускладнення та затягування у часі процесу їх прийняття [1].

Тому пошук шляхів надійного виявлення інформаційних загроз державі у воєнній сфері та протидії їм є актуальним науково-практичним завданням.

Постановка проблеми. 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 методу аналізу та оцінювання інформаційних загроз для визначення ефективних заходів протидії їм.

Викладення основного матеріалу

Аналіз основ забезпечення інформаційної безпеки дає змогу зробити висновок про те, що поняття "забезпечення інформаційної безпеки" включає об'єкти інформаційної безпеки, загрози об'єктам інформаційної безпеки та діяльність щодо захисту цих об'єктів, засновану на сукупності сил, засобів, способів і методів забезпечення інформаційної безпеки.

Головними цілями діяльності із забезпечення інформаційної безпеки є попередження, уникнення та ліквідація загроз об'єктам інформаційної безпеки та мінімізація можливого збитку, завданого внаслідок реалізації даних загроз.

Загроза – одне із ключових понять у сфері забезпечення інформаційної безпеки.

Загроза об'єкту інформаційної безпеки сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів (їх елементів), здатних впливати на конкретний об'єкт інформаційної безпеки. Негативні впливи розрізняються за характером завданої шкоди, а саме: за ступенем зміни властивостей об'єкта безпеки та можливості ліквідації наслідків прояву загрози.

До найбільш важливих властивостей загрози слід віднести вибірковість, передбачуваність і шкідливість. Вибірковість характеризує націленість загрози на завдання шкоди тим чи іншим конкретним властивостям об'єкта безпеки. Передбачуваність характеризує наявність ознак виникнення загрози, що дають змогу заздалегідь прогнозувати можливість появи загрози та визначати конкретні об'єкти безпеки, на які вона буде спрямована. Шкідливість характеризує можливість завдання шкоди різної ваги об'єкту безпеки. Шкода, як правило, може бути оцінена вартістю витрат на ліквідацію наслідків прояву загрози або на запобігання її появи.

Необхідно виділити два найбільш важливі типи загроз:

1. Намір завдати шкоди, що з'являється у вигляді наявного мотиву діяльності суб'єкта;

2. Можливість завдання шкоди – існування достатніх для цього умов і факторів.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питання про наявність у загрозливого суб'єкта сил і засобів, достатніх для здійснення наміру.

Можливість завдання шкоди полягає в існуванні достатніх для цього умов і факторів. Особливість загроз цього типу полягає в тому, що оцінити потенціал сукупності факторів, які можуть слугувати перетворенню цих можливостей і умов на шкоду, можуть тільки суб'єкти загроз.

Між загрозою та небезпекою завдання шкоди завжди існує стійкий причинно-наслідковий зв'язок. Загроза завжди породжує небезпеку. Небезпеку також можна представити як стан, в якому перебуває об'єкт безпеки внаслідок виникнення йому загрози. Головна відмінність між ними полягає в тім, що небезпека є властивістю об'єкта інформаційної безпеки та характеризує його здатність протистояти прояву загроз, а загроза – властивістю об'єкта взаємодії або елементів, що перебувають у взаємодії, об'єкта безпеки, які виступають як джерело загроз. Поняття загрози має причинно-наслідковий зв'язок не тільки з поняттям небезпеки, але й з можливою шкодою, як наслідком негативної зміни умов існування об'єкта. Можлива шкода визначає величину небезпеки.

Опираючись на уведені вище поняття, можна побудувати таку онтологічну схему забезпечення інформаційної безпеки (рис.1).

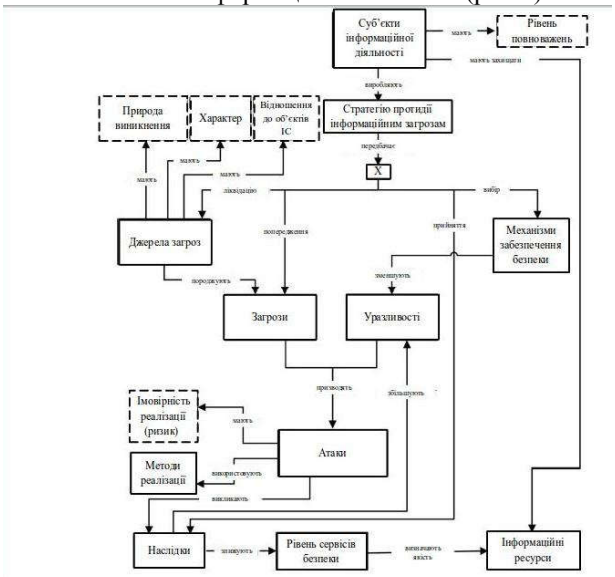

Рис. 1. Онтологічна схема забезпечення інформаційної безпеки

Суб'єкти інформаційної діяльності (джерело, власник або користувач інформації) визначають множину інформаційних ресурсів, які повинні бути захищені від різного роду атак. До активів ІС зазвичай відносять: матеріальні ресурси; інформаційні ресурси (аналітична, службова, керівна інформація на всіх етапах свого життєвого циклу: створення, обробка, зберігання, передача, знищення); інформаційні технологічні процеси життєвого циклу автоматизованих систем; надані інформаційні послуги тощо [4].

Атаки є результатом реалізації загроз, здійснюються через різні уразливості в захисті, і мають імовірність реалізації (ризик атаки).

Основні порушення безпеки: розкриття інформаційних ресурсів (втрата конфіденційності), їхня неавторизована модифікація (втрата цілісності) або неавторизована втрата доступу до цих ресурсів (втрата доступності).

У результаті аналізу уразливостей, властивостей джерел загроз (природи виникнення, характеру, відносини до об'єктів ІС) і ймовірностей їх можливої реалізації в конкретному оточенні, визначаються ризики для даного набору інформаційних ресурсів. Це, у свою чергу, дозволяє визначити стратегію протидії, що є політикою безпеки.

Вироблена суб'єктом інформаційних відносин стратегія протидії може передбачати для кожної із загроз одну з можливих ліній поводження: спробу ліквідації джерела загрози, ухилення від загрози, прийняття загрози,

мінімізація збитку від атаки, викликаного цією загрозою, за допомогою сервісів і механізмів безпеки. При цьому слід враховувати, що окремі уразливості можуть зберегтися й після застосування заходів безпеки.

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.1.

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 1 – 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 Збройних Сил 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. 2.

Таблиця 2 – 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

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.

Висновки

Морфологічний аналіз показує, що можна виділити такі основні складові загрози інформаційній безпеці: джерело впливу на інформаційну систему, спосіб впливу, інформаційні об'єкти впливу, а також результат впливу (заподіяний збиток).

Ці елементи при розробці класифікації можуть бути обрані як базові класифікаційні ознаки для подальшої їхньої декомпозиції.

Розроблений метод аналізу та оцінювання інформаційних загроз держави у воєнній сфері дозволяє визначати заходи протидії інформаційним загрозам на підставі аналізу можливих негативних наслідків загроз, ідентифікації можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей).

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

Література

1. Frank G. Hoffman. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Confict. "Strategic Forum", Institute for National Strategic Studies National Defense University. No. 240. April 2009. [Електронний ресурс.] – Режим доступу: 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 // -Зб. наук. Праць. – Харків: ХУПС, 2015.– Випуск 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. Ю.І.Радковець, О.В.Левченко, Косогов О.М. Погляди на створення системи інформаційної безпеки України та її Збройних Сил // Наука і оборона. – 2014. – № 1. – С. 38–41.

МЕТОД АНАЛИЗА И ОЦЕНКИ ИНФОРМАЦИОННЫХ УГРОЗ ГОСУДАРСТВУ В ВОЕННОЙ СФЕРЕ ДЛЯ ОПРЕДЕЛЕНИЯ АДЕКВАТНЫХ МЕРОПРИЯТИЙ ПРОТИВОДЕЙСТВИЯ

Александр Николаевич Косогов
Войсковая часть А1906, Киев, Украина

На основе анализа взаимодействия логической цепочки источника угроз – угрозы – реализация угроз (атаки) – уязвимости – объекты – следствия (убыток) – мероприятия противодействия разработана онтологическая схема обеспечения информационной безопасности. Установлено, что главными целями деятельности из обеспечения информационной безопасности есть предупреждения, избежание и ликвидация угроз объектам информационной безопасности и минимизация возможного убытка, причиненного вследствие реализации данных угроз. Предложено метод анализа и оценки информационных угроз для определения адекватных мероприятий противодействия этим угрозам. В пределах приведенного метода оценка рисков осуществляется с помощью оценивания возможности реализации угроз безопасности, связанных с уязвимостями присущих тем или другим объектам информационной безопасности.

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

METHOD OF ANALYSIS AND ASSESSMENT OF INFORMATION THREATS TO THE STATE IN THE MILITARY SPHERE TO DETERMINE ADEQUATE ACTIVITIES OF COUNTERACTION

Oleksandr M. Kosogov ***(Candidate of Military Sciences, Senior Research Fellow)***
Military Unit A1906, Kyiv, Ukraine

Based on the analysis of the interaction of the logical chain of the source of threats - threats - the implementation of threats (attacks) - vulnerabilities - objects - effects (loss) - countermeasures developed an ontological scheme for ensuring information security. It was established that the main objectives of the activity of ensuring information security are warnings, avoidance and elimination of threats to information security objects and minimization of possible losses caused by the implementation of these threats. A method of analyzing and assessing information threats is proposed to determine adequate measures to counter these threats. Within the above method, the risk assessment is carried out by assessing the feasibility of implementing security threats related to the vulnerabilities inherent in one or other information security objects.

Key words: *information security, threats to information security, source of threat, vulnerability of the object, counteraction system, military sphere.*

References

1. Frank G. Hoffman. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. Strategic Forum, Institute for National Strategic Studies, National Defense University. No. 240. April 2009. [Electronic resource.] - Access mode: http: // http://www.ndu.edu/inss.

2. Levchenko O.V. A conceptual approach to a comprehensive assessment of the state of information security / O.V. Levchenko // Science and technology of the Air Forces of the Armed Forces of Ukraine. - 2015 # 3 (20). - P. 47 - 50.

3. Lande D. Information operations through the prism of the system of monitoring and integration of Internet resources / D.Lande, V.Furashev // Legal Informatics. - 2009. - No. 2 (22). - P. 49-57.

4. Gorbulin V.P. Information operations and public safety: threats, counteraction, modeling: monogr. / VPGorbulin, O.G.Dodonov, D.V. Lende. - K.: Intertechnology, 2009. - 164 p.

5. Kosogov O.M. Approach to the construction of a state system for counteracting information threats in a special period / O. M. Kosogov // Sb. sciences Work - Kharkiv: HUPPS, 2015. - Issue 4 (45) .- P. 76 - 79.

6. Litvinenko O.V. Information Influences and Transactions: Theoret. -Analyte. Essays Methods, means and measures for ensuring information-psychological security of person, society, country Information Security of the Person, Society and State ● No. 3 (7) ● 2011 77 / O. V. Litvinenko. - K.: Nat. other strategist research, 2003. - 239 pp. - (Gen. 6: National Security).

7. Litvinenko O.V. Special informational operations: monogr. / O. V. Litvinenko. - K. Rada Nats. Security and Defense of Ukraine, National. other strategist Research, 1999. - 163 p. - (Publication 3: National Security).

8. Manoylo AV State information policy in special conditions: monogr. / A.V.Manoyolo - M.: MIFi, 2003. - 388 pp.

9. Yu.I.Radkovets, O.V.Levchenko, O.M. Kosogov Views on the creation of the information security system of Ukraine and its Armed Forces // Science and Defense. - 2014. - No. 1. - P. 38-41.