УДК 354.42

О.М. Косогов

Військова частина 1906

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ ТА ВИЗНАЧЕННЮ ЗАХОДІВ ПРОТИДІЇ ЇМ

На основі аналізу поняття загрози інформаційній безпеці 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. Розроблено отологічну схему забезпечення інформаційної безпеки. Виділено основні складові загрози інформаційній безпеці.

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

Вступ

Постановка проблеми. Аналіз літератури. 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.

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

В наявній літературі, присвяченій даному питанню, запропоновано ряд класифікацій загроз інформаційній безпеці, що відбиває ті або інші аспекти розглянутої проблеми [1 - 4]. Разом з тим, на теперішній час відсутня універсальна методологія, яка б давала змогу визначати джерела загроз, можливість їх реалізації, можливі збитки внаслідок їх реалізації, а також планувати та здійснювати ефективні заходи протидії загрозам.

Метою статті є розробка методологічного підходу до аналізу загроз інформаційній безпеці держави у воєнній сфері та визначенню заходів протидії їм.

Основний матеріал

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 за-

грози 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 важливих типів загроз:

намір завдати шкоди, що з'являється у вигляді наявного мотиву діяльності суб'єкта;

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).

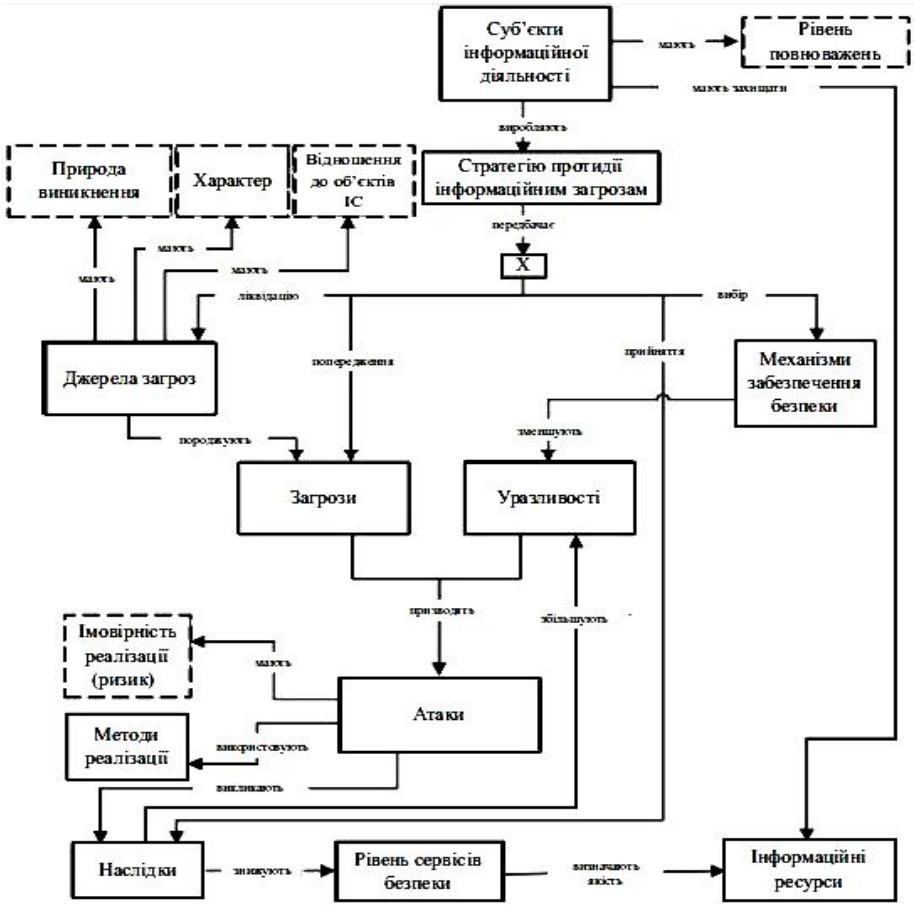

Рис. 1. Онтологічна схема забезпечення інформаційної безпеки

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.

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 безпеці інформації.

Виходячи з такого принципу, моделювання й класифікацію джерел загроз, самих загроз та їх проявів, а також розробку ефективних заходів протидії доцільно проводити на основі аналізу взаємодії логічного ланцюжка: «Джерело загрози» → «Загроза» → «Уразливість» → «Реалізація загрози (атака)» → «Наслідки (збиток)» → «Заходи протидії».

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з ідентифікованими джерелами загроз, а також, що 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.

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.

Список літератури

1. Варфоломеев А.А. Основы информационной безопасности / А.А. Варфоломеев. – М., 2008. – 254 с.

2. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій / В.М. Петрик, О.А. Штоквиш, В.І. Полевий та ін. – К.: Росава, 2006.. – 208 с.

3. Ажмухамедов И.М. Концептуальная модель управления комплексной безопасностью системы / И.М. Ажмухамедов // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика" – 2010. – № 1. – С. 62-66.

4. Белов П.Г. Теоретические основы системной инженерии безопасности / П.Г. Белов. – К.: КМУ ГА, 2006.

Надійшла до редколегії 11.08.2015

Рецензент: д-р техн. наук проф. К.С. Васюта, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К АНАЛИЗУ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В ВОЕННОЙ СФЕРЕ И ОПРЕДЕЛЕНИЕ МЕР ПРОТИВОДЕЙСТВИЯ ИМ

А.Н. Косогов

На основе анализа понятия угрозы информационной безопасности установлено, что главными целями деятельности по обеспечению информационной безопасности являются предупреждение, избегание и ликвидация угроз объектам информационной безопасности и минимизация возможного ущерба, нанесенного вследствие реализации данных угроз. Разработана онтологическая схема обеспечения информационной безопасности. Выделены основные составные части угрозы информационной безопасности.

Ключевые слова: *информационная безопасность, угрозы информационной безопасности, источник угрозы, уязвимость объекта.*

METODOLOGICAL GOING NEAR ANALYSIS OF THREATS OF INFORMATIVE SECURITY OF THE STATE IN MILITARY SPHERE AND DETERMINATION OF MEASURES OF COUNTERACTION TO THEM

O.M. Kosogov

It is set on the basis of analysis of concept of threat of informative security, that the primary objectives of activity on providing of informative security are warning, avoidance and liquidation of threats to the objects of informative security and minimization of the possible damage inflicted because of realization of these threats. The ontological chart of providing of informative security is worked out. Basic component parts of threat of informative security are distinguished.

Keywords: *informative security , threats of informative security, source of threat, vulnerability of object.*