Інформаційна безпека держави

УДК 354.42

О.М. Косогов

Військова частина 1906, Київ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

На основі аналізу методів забезпечення безпеки інформаційної інфраструктури держави визначено основні напрями забезпечення інформаційної безпеки. Зазначено, що обрання цілей і методів протидії конкретним загрозам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми запропоновано можливі форми діяльності органів державного управління. Визначено концептуальну модель безпеки інформаційної інфраструктури держави.

Ключові слова: *інформаційна безпека, інформаційна інфраструктура, методи забезпечення інформаційної безпеки, державні органи.*

Вступ

Постановка проблеми. Аналіз літератури. Проблеми забезпечення інформаційної безпеки у воєнній сфері, з огляду на появу нових та зростання рівня існуючих ризиків і загроз в інформаційному просторі України, набувають великої значущості і потребують відповідного наукового підгрунтя для їх вирішення. Одним з напрямів розв'язання цих проблем є постійне удосконалення науково-методичного забезпечення інформаційної безпеки, а саме визначення спрямованості загроз та оцінка їх рівня, виявлення об'єктів інформаційного впливу та вибір дієвих методів забезпечення інформаційної безпеки.

Існує низка публікацій, що присвячені проблемам інформаційної безпеки в інформаційних системах і мережах передачі й обробки інформації. Завдання створення, організації й дослідження процесів функціонування, удосконалювання й розвитку систем забезпечення безпеки інформації тою чи іншою мірою знайшли відбиття в працях ряду вітчизняних і закордонних учених [1 – 4].

Однак дотепер повною мірою не вивчені й залишаються дискусійними методологічні, методичні й практичні аспекти дослідження проблем визначення ефективних методів безпеки складних інформаційних систем. Сучасні науково-практичні напрацювання в Україні, а так само ряд провідних міжнародних стандартів містять норми й вимоги, спрямовані в основному на захист від несанкціонованого доступу. При цьому вони часто не забезпечують базового рівня безпеки, тому що дозволяють моделювати лише частину загроз. При цьому в даний момент не існує загальноприйнятих стандартів або підходів, що дозволяють забезпечити підвищений або високий рівень захисту. Так само до негативного боку застосування сучасних стандартів варто віднести шаблонність пропонованого захисту й відсутність варіантності [5].

Метою статті є аналіз методів забезпечення безпеки інформаційної інфраструктури держави та побудова концептуальної моделі безпеки інформаційної інфраструктури держави.

Основний матеріал

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування [6 – 8].

Важливими методами аналізу стану інформаційної безпеки є *методи опису та класифікації.* Для здійснення ефективного захисту інформаційного середовища України слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

Розповсюдженими методами аналізу стану інформаційної безпеки є методи дослідження причинних зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи щодо їх нейтралізації та протидії їм. У числі даних методів причинних зв'язків можна назвати такі: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану інформаційної безпеки залежить від конкретного рівня і сфери організації захисту та протидії. У залежності від загрози

уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів протидії. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів.

На *фізичному рівні* здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, а також управлінських технологій. На *програмно-технічному* рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності. На *управлінському рівні* здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку системи інформаційної безпеки держави. На *технологічному рівні* здійснюється реалізації стратегії інформаційної безпеки держави шляхом застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні *користувача* реалізація стратегії інформаційної безпеки держави спрямована на зменшення рефлексивного впливу на державне інформаційне середовище. На рівні інформаційно-телекомунікаційних мереж ця політика реалізується у форматі координації дій суб'єктів системи інформаційної безпеки (СІБ), які пов'язані між собою однією метою. На *процедурному* рівні вживаються заходи, що реалізуються суб'єктами. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування відновлювальних робіт.

Можна виокремити декілька типів методів забезпечення інформаційної безпеки:

– *однорівневі методи* будуються на підставі одного принципу управління інформаційною безпекою;

– *багаторівневі методи* будуються на основі декількох принципів управління інформаційною безпекою, кожен з яких слугує вирішенню окремого завдання. При цьому часткові технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

– *комплексні методи* – багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

– інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням [8].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать:

прийняття рішення з визначення типу та змісту інформаційної загрози і складу суб'єктів, які ведуть протидію;

ухвалення загальної стратегії і алгоритму дій адекватного сприйняття загрози;

виділення необхідних ресурсів, достатніх для реалізації протидії інформаційним загрозам і збереження сталого розвитку інформаційних ресурсів держави;

трансформації результатів оцінки ризиків у відповідну стратегію інформаційної безпеки.

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану професійної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні носія інформації, структурного підрозділу і державного органу в цілому заважає розповсюджена думка про те, що захист інформації і криптографія одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі. Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передавання, тобто забезпечення її цілісності.

Таким чином, конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації державних органів. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що співробітник буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї.

Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності, конфіденційності та цілісності інформації.

Можна перераховувати інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. З іншого боку, не слід плекати надію на створення абсолютної системи інформаційної безпеки, оскільки, як зазначалося вище, інформаційні загрози та небезпеки є атрибутивними компонентами системи інформаційної безпеки, отже їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і

водночас, слугують імпульсом до вдосконалення. Отже, важливим методом забезпечення інформаційної безпеки є *метод розвитку.*

Основним методом аналізу інформаційних ризиків *є кількісний та якісний аналіз, факторний аналіз* та інші. Мета якісної оцінки ризиків – ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну протидію їм.

Важливим методом забезпечення інформаційної безпеки є також *метод критичних сценаріїв.* У зазначених сценаріях аналізуються ситуації, коли противник паралізує роботу органу управління і відповідно знижує здатність підрозділів виконувати завдання за призначенням.

Також можна зазначити на *метод моделювання,* за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно провадяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної кампанії. Серед методів забезпечення інформаційної безпеки важливе значення має *метод дихотомії.* Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку зниження вразливостей об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів із забезпечення інформаційної безпеки органу управління.

Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об'єкту безпеки. Метою захисту є переконання противника у недоцільності здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на створення умов, за яких здійснення небезпечних дій щодо об'єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у противника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від противника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації.

Методи впливу на інформаційну інфраструктуру можуть поділятися на *інформаційні та неінформаційні.* Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації, і таким чином, на попередження завдання шкоди предметам суспільних відносин, що захищаються.

У цілому ж слід зазначити, що обрання цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки [9]. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державного управління, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності [10 – 11].

На підставі викладеного можна визначити концептуальну модель безпеки інформаційної інфраструктури держави (рис. 1).

Висновки

Таким чином, забезпечення безпеки інформаційної інфраструктури держави є проблемою високої складності та потребує комплексного підходу. Тому для ефективного функціонування СІБ України сукупність зазначених організаційно-технологічних та організаційно-правових заходів слід поєднати в систему управління інформаційною безпекою.

Відповідно до теоретичних розробок спеціалістів у галузі інформаційної безпеки, основними напрямами забезпечення інформаційної безпеки є правовий, організаційний, інженерно-технічний. Застосування всіх цих напрямів є необхідним для формування комплексної СІБ держави.

Список літератури

1. Киселев В.Д. Современные проблемы защиты в системах ее передачи и обработки / В.Д. Киселев, О.В. Есиков, А.С. Кислицын. – М.: Солид, 2000. – 200 с.

2. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – М. : ДМК, 2002. – 134 с.

3. Гарбарчук В. Кибернетический подход к проектированию систем защиты информации; Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т / В. Гарбарчук, З. Зинович, А. Свиц. – К., Луцк, Люблин, 2003. – 658 с.

4. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества / Н.А. Маслова // Штучний інтелект. – Донецьк: ІШІ, 2007. – № 1. – С. 51-57.

5. Косогов О.М. Модель динаміки зміни рівня інформаційної безпеки системи / О.М. Косогов // Зб. наук. праць. – К.: ЦВСД НУО імені Івана Черняховського, 2015. – № 2 (54). – С. 76-79.

6. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Пєвцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – 2011. – Вип. 2 (92). – С. 57-59.

7. Власюк О.С. Можливості застосування аналітичного планування для обґрунтування та підготовки рішень на вищих рівнях управління. НІСД. – Вип. 47, серія наукові доповіді, 1996. – 71 с.

8. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: моногр. / А.І. Семенченко. – К.: Вид-во НАДУ, 2008. – 428 с.

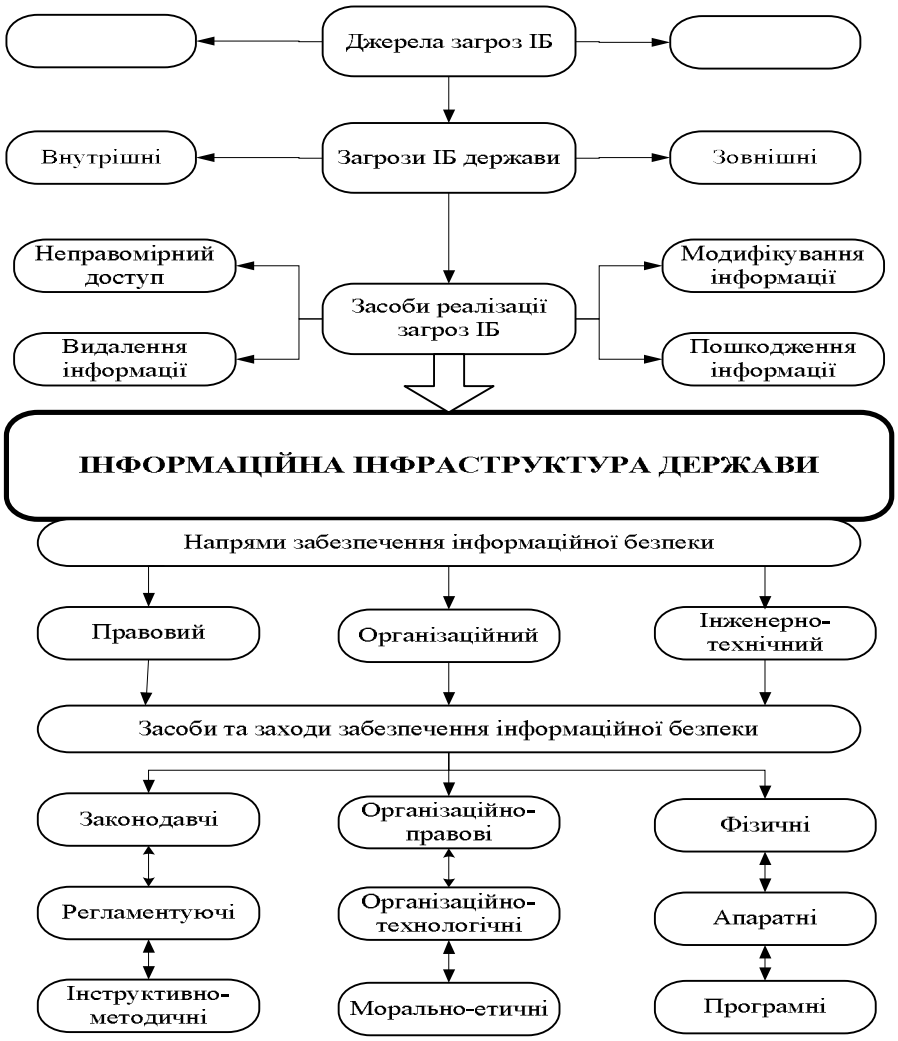

Рис. 1. Концептуальна модель безпеки інформаційної інфраструктури держав

9. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О.М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2014. – Вип. 3 (40). – С. 127-129.

10. Асанович В.Я. Информационная безопасность: анализ и прогноз информационного воздействия / В.Я. Асанович, Г.Г. Маньшин. – Мн.: Амалфея, 2006. – 204 с.

11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи / Б.А. Кормич. – К.: Кондор, 2003. – 384 с.

Надійшла до редколегії 8.02.2016

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

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

А.Н. Косогов

На основе анализа методов обеспечения безопасности информационной инфраструктуры государства определены основные направления обеспечения информационной безопасности. Указано, что выбор целей и методов противодействия конкретным угрозам информационной безопасности представляет собой важную проблему и составную часть деятельности по реализации основных направлений государственной политики информационной безопасности. В пределах решения данная проблема предложены возможные формы деятельности органов государственного управления. Определена концептуальная модель безопасности информационной инфраструктуры государства.

Ключевые слова: *информационная безопасность, информационная инфраструктура, методы обеспечения информационной безопасности, государственные органы.*

METHODS OF THE PROVISION TO SECURITY OF THE STATE'S INFORMATION INFRASTRUCTURE

O.M. Kosogov

On base of the analysis of the methods of the provision to security of the state's information infrastructure are determined main trends of the provision to information safety. It is specified that choice integer and methods of the reluctance concrete threat to information safety presents itself massive problem and component part to activity on realization of the main trends state politicians to information safety. Within decision given problem are offered possible forms to activity organ state management. It is determined conceptual model to security of the state's information infrastructure.

Keywords: *information security, information infrastructure, methods of the provision to information safety, state organs.*