УДК 351:342.57
DOI https://doi.org/10.32838/2663-6468/2019.3/31

Торічний В.О.
Національний університет цивільного захисту України

ОСОБЛИВОСТІ ДЕРЖАВНОГО УПРАВЛІННЯ РЕГІОНАЛЬНИМИ СИСТЕМАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті досліджено особливості державного управління регіональними системами інформаційної безпеки. Зокрема, визначено основні напрями діяльності держави щодо забезпечення інформаційної безпеки регіону. Окреслено проблеми побудови регіональних систем інформаційної безпеки. Виокремлено методи державного управління регіональними системами інформаційної безпеки.

Ключові слова: *державне управління, регіональна система інформаційної безпеки, методи державного управління, напрями діяльності держави.*

Постановка проблеми. Ефективність функціонування регіональних соціально-економічних комплексів і систем управління безпосередньо залежить від стану інформаційної безпеки регіону, під якою зазвичай розуміється стан захищеності інформаційного середовища суспільства, що забезпечує його формування та розвиток в інтересах громадян, організацій і держави загалом.

Аналіз останніх досліджень і публікацій. Інформаційна безпека як об'єкт державного управління систематично підлягає різнохарактерним дослідженням й опрацюванню з боку вчених і практиків України й інших країн. Зокрема, такі вчені, як: А.І. Марущак [1], В.М. Фурашев [2], Л.С. Харченко [3], Ю.С. Шемшученко [4] присвятили свої праці зазначеній проблематиці.

Однак регіональні системи інформаційної безпеки все ще потребують більш детальних досліджень, оскільки суттєво залежать як від особливостей функціонування загальнодержавної системи інформаційної безпеки, так і від зміни внутрішньорегіональних умов.

Постановка завдання. Метою роботи є дослідження особливостей державного управління регіональними системами інформаційної безпеки.

Досягнення поставленої мети передбачає вирішення таких завдань:

– визначити основні напрями діяльності держави щодо забезпечення інформаційної безпеки регіону;

– окреслити проблеми побудови регіональних систем інформаційної безпеки;

– виокремити методи державного управління регіональними системами інформаційної безпеки.

Виклад основного матеріалу дослідження. Слід відзначити, що до основних напрямів діяльності держави щодо забезпечення інформаційної безпеки регіону належать:

– формування, нарощування та раціональне управління державними і муніципальними інформаційними ресурсами;

– виявлення загроз інформаційній безпеці та їх джерел;

– забезпечення інформаційних прав особистості, суспільства, органів державної влади та місцевого самоврядування, їх захист від негативних інформаційних впливів (організація інформаційного обміну з зовнішнім середовищем, що не завдає шкоди безпеці суб'єктам регіону і суб'єктам зовнішнього середовища стосовно регіону);

– захист інформації, віднесеної в законному порядку до категорії обмеженого доступу (що складає державну чи службову таємницю), від загроз її витоку до недружніх суб'єктів, в т. ч. внаслідок незаконного ведення технічної розвідки і несанкціонованого доступу до інформації;

– захист інформації (незалежно від категорії доступу до неї та форми подання) від загроз небажаних несанкціонованих і ненавмисних дій [1; 3].

Першою з проблем, що виникають у побудові регіональних систем інформаційної безпеки, є встановлення правильного (оптимального) співвідношення командних і координаційних методів державного управління.

Неможливість реалізації виключно командного методу державного управління регіональними системами інформаційної безпеки пов'язана з тим, що інформація обмеженого доступу використовується і обробляється в загальному випадку цілим рядом організацій, установ і підприємств різної відомчої належності та різних форм власності, розташованих на території регіону. Такими організаціями

можуть бути місцеві органи виконавчої влади, органи місцевого самоврядування, військові частини, підприємства оборонних галузей промисловості, науково-дослідні інститути тощо. Тому реалізація комплексу заходів, які зачіпають кілька власників або користувачів інформації, не може бути здійснена виключно командними методами. Необхідність спільних дій згаданих суб'єктів інформаційної безпеки і є потребою у використанні єдиного підходу до організації, планування та реалізації інформаційної безпеки. Надзвичайно важливим у цьому плані видається забезпечення єдиної методології оцінки можливостей реалізації загроз і засобів протидії їм, а також з урахуванням впливу цих засобів захисту інформації на функціонування регіонального інформаційного простору.

Тому першим із завдань вдосконалення підсистеми державного управління регіональними системами інформаційної безпеки є створення такої системи державного управління, яка забезпечувала б раціональне поєднання командних і координаційних методів. Для вирішення цього завдання в регіоні повинен ефективно функціонувати координуючий орган за участю всіх зацікавлених осіб, яким делегуються певні повноваження [2; 4].

Друга проблема полягає в тому, що у процесі забезпечення інформаційної безпеки можливо супутнє виникнення загроз безпеці інформації, не передбачених у проектуванні і створенні системи захисту. Фактично це означає зменшення розмірів контрольованої зони об'єкта захисту і, тим самим, можливість утворення нового, каналу витоку інформації, якого раніше не було. Тому система державного управління інформаційною безпекою повинна бути готова до функціонування у двох режимах, які можна умовно назвати «повсякденним» і «оперативним».

Зокрема, у повсякденному режимі (за своєю суттю це сталий стан системи захисту і об'єкта захисту за незмінних загроз безпеці інформації) управління здійснюється на основі довгострокових, заздалегідь розроблених і апробованих планів, програм, інструкцій із застосуванням оптимально (раціонально) підібраних технічних засобів і організаційних заходів щодо захисту інформації [1; 4].

В оперативному режимі державне управління інформаційною безпекою повинно бути орієнтоване на швидке виявлення можливих загроз безпеці інформації, їх оцінку і вироблення рекомендацій щодо запобігання або нейтралізації таких загроз.

Тому другим завданням вдосконалення підсистеми державного управління регіональними системами інформаційної безпеки є забезпечення її адаптації до зовнішніх умов.

Суть третьої проблеми державного управління регіональними системами інформаційної безпеки полягає в тому, що в силу різнорідності і різної належності сил і засобів захисту, які утворюють у сукупності регіональну систему інформаційної безпеки, необхідне здійснення контролю стану системи й оцінка її реальних можливостей щодо поведінки в умовах як постійно існуючих, так і нових загроз безпеці інформації [2; 3].

В іншому разі навіть елементарний вихід із ладу конкретного одиничного засобу захисту інформації (або проведення регламентних робіт) може спричинити витік інформації з непередбачуваними наслідками. Тому ще одним завданням вдосконалення підсистеми державного управління регіональними системами інформаційної безпеки є безперервне відстеження стану елементів системи захисту й обґрунтування пропозицій щодо вжиття заходів, що виключають негативні наслідки зміни цього стану. Вирішення цього завдання вимагає проведення моніторингу стану регіональних систем інформаційної безпеки за обраними параметрами, визначення переліку яких є самостійним і складним завданням.

Як регіональна система інформаційної безпеки є невід'ємною частиною державної системи інформаційної безпеки, так і її система управління повинна узгоджуватися з системою управління державною системою інформаційної безпеки [1; 2].

Так, на першому етапі створення регіональних систем інформаційної безпеки і розгортання державної системи інформаційної безпеки таке узгодження може бути проведено за схемою «узгодження входів-виходів», а надалі – і на базі єдиного математичного забезпечення.

Підсумовуючи сказане вище, можна зробити висновок про можливість застосування таких методів державного управління регіональними системами інформаційної безпеки:

– директивне управління органами регіональних систем інформаційної безпеки з використанням організаційно-розпорядчих актів органів виконавчої влади, спрямованих на виконання прийнятих рішень в області інформаційної безпеки;

– регламентація відносин у сфері інформаційної безпеки на рівні регіону і використанням системи необхідних і достатніх правил і норм, реалізованої у вигляді системи правових і нормативних документів у сфері інформаційної безпеки;

– регулювання відносин у сфері інформаційної безпеки з використанням методів переконання, заснованих на обґрунтуванні та демонстрації переваг методичних рекомендацій із питань інформаційної безпеки, що виходять від органів виконавчої влади;

– управління розвитком регіональних систем інформаційної безпеки на основі обґрунтування пріоритетних напрямків, розробки і реалізації цільових державних програм розвитку регіональних систем інформаційної безпеки [2; 3].

Висновки. Проведене дослідження дозволило зробити такі висновки.

1. Визначено основні напрями діяльності держави щодо забезпечення інформаційної безпеки регіону: формування, нарощування та раціональне управління державними і муніципальними інформаційними ресурсами; виявлення загроз інформаційній безпеці та їх джерел; забезпечення інформаційних прав особистості, суспільства, органів державної влади та місцевого самоврядування; захист інформації, віднесеної в законному порядку до категорії обмеженого доступу; захист інформації від загроз небажаних несанкціонованих і ненавмисних дій.

2. Окреслено проблеми побудови регіональних систем інформаційної безпеки. Зазначено, що першою проблемою у цьому контексті є встановлення правильного (оптимального) співвідношення командних і координаційних методів державного управління. Друга проблема полягає в тому, що в процесі забезпечення інформаційної безпеки можливо супутнє виникнення загроз безпеці інформації, не передбачених при проектуванні і створенні системи захисту. Третя проблема передбачає необхідне здійснення контролю стану системи й оцінку її реальних можливостей щодо поведінки в умовах як постійно існуючих, так і нових загроз безпеці інформації.

3. Виокремлено методи державного управління регіональними системами інформаційної безпеки: директивне управління органами регіональних систем інформаційної безпеки; регламентація відносин у сферіінформаційної безпеки на рівні регіону; регулювання відносин у сфері інформаційної безпеки з використанням методів переконання; управління розвитком регіональних систем інформаційної безпеки на основі обґрунтування пріоритетних напрямків, розробки і реалізації цільових державних програм розвитку регіональних систем інформаційної безпеки.

Загалом завдання вдосконалення державного управління регіональними системами інформаційної безпеки зумовлені тим, що кожен із перелічених вище методів управління повинен ґрунтуватися на об'єктивній, повній і своєчасній інформації про процеси, які відбуваються в регіональних системах інформаційної безпеки, а також на прийнятті всебічно обґрунтованих рішень, що спираються на цю інформацію.

Список літератури:

1. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92–95.

2. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. *Інформація і право : науковий журнал*. 2012. № 1 (4). С. 46– 56.

3. Харченко Л.С. Інформаційна безпека України : глосарій. Київ : Текст, 2004. 136 с.

4. Шемшученко Ю.С. Правове забезпечення інформаційної діяльності в Україні. Київ : ТОВ «Видавництво «Юридична думка», 2011. 384 с.

ОСОБЕННОСТИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ СИСТЕМАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье исследованы особенности государственного управления региональными системами информационной безопасности. В частности, определены основные направления деятельности государства по обеспечению информационной безопасности региона. Обозначены проблемы построения региональных систем информационной безопасности. Выделены методы государственного управления региональными системами информационной безопасности.

Ключевые слова: *государственное управление, региональная система информационной безопасности, методы государственного управления, направления деятельности государства.*

THE FEATURES OF PUBLIC ADMINISTRATION OF REGIONAL INFORMATION SECURITY SYSTEMS

The features of public administration of regional information security systems are investigated in the article. In particular, the main activities of the state concerning ensuring of information security of the region are determined. The problems of creation of regional information security systems are designated. The methods of public administration of regional information security systems are allocated.

Key words: *public administration, regional information security system, public administration methods, state activities.*