Інформаційні технології

Ржавська Анастасія Ігорівна

студентка

Навчально-наукового інституту інформаційних технологій

Науковий керівник:

Редич Олександр Володимирович

кандидат економічних наук,

доцент кафедри інтелектуальних управляючих та обчислювальних систем

Навчально-науковий інститут інформаційних технологій

ОГЛЯД СИСТЕМ ПІДТРИМКИ ПРОЦЕСІВ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ
OVERVIEW OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION SUPPORT SYSTEMS

Анотація. *У статті висвітлено напрями розвитку та вдосконалення спеціального зв'язку. Проведено аналіз державної політики у сфері спеціального зв'язку та захисту інформації. Обґрунтовано захищеність секретної та службової інформації від несанкціонованого доступу.*

Ключові слова: *Спеціальний зв'язок; безпека; захист інформації; державна політика; протидія загрозам; система підтримки процесів.*

Summary. *The article highlights the areas of development and improvement of special communication. The analysis of the state policy in the field of special communication and information protection is carried out. The protection of classified and official information from unauthorized access is substantiated.*

Key words: *Special connection; security; information protection; public policy; countering threats; process support system.*

Постановка проблеми. Безумовним та загальновизнаним є той факт, що рівень розвитку держави та суспільства значною мірою залежить та визначається рівнем їх інформатизації. У зв'язку з цим в Україні як і у більшості країн світу широко та інтенсивно в усі сфери життєдіяльності людини, суспільства та держави впроваджуються новітні інформаційні системи, телекомунікаційні системи, інформаційно-телекомунікаційні системи, інформаційні технології та системи інформаційних технологій, інформаційно-аналітичні системи та автоматизовані системи управління. Особливу важливу роль інформаційно-телекомунікаційні та інформаційно-аналітичні системи відіграють в таких сферах як державне управління, економіка, освіта, наука, оборона, безпека життєдіяльності особи тощо. При функціонуванні вказаних систем здійснюється обробка інформації. Зокрема актуальним питанням є система підтримки процесів спеціального зв'язку та захисту інформації.

Аналіз останніх досліджень. Найголовнішим надбанням у галузі захисту інформації стали праці вчених, які вивчали питання розвитку системи захисту інформації, періодизації захисту інформації и визначали стан такого захисту в певний період часу або принаймні стан складових досліджуваної системи. Це, зокрема праці А.М. Гуза [1], Б.А. Кормича [2], В. Шапети [3], В.І. Гурковського [4] й деяких інших. У зв'язку з таким станом розроблення питання, яке підлягає аналізу, найбільш цікавим залишається визначеність і розвинутись складових частин системи захисту інформації на сучасному етапі її існування.

Мета статті. Визначити та провести огляд систем підтримки процесів спеціального зв'язку та захисту інформації. Обґрунтувати захищеність інформації з обмеженим доступом.

Виклад основного матеріалу. Під обробкою інформації в системі розуміється виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення,

реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. При цьому обмін інформацією здійснюється з використанням інформаційно-телекомунікаційних систем як внутрішнього так і загального користування, в тому числі при підключенні до міжнародних інформаційно-телекомунікаційних систем через глобальну світову інформаційну інфраструктуру. На практиці поряд з інформаційними та телекомунікаційними системами широке застосування знаходять інформаційно-телекомунікаційні системи.

Спеціальний зв'язок - зв'язок, що забезпечує передачу секретної та/або службової інформації шляхом застосування відповідних організаційних та технічних заходів [5].

Система спеціального зв'язку - сукупність обладнання, засобів, комплексів та систем обробки, передачі, технічного та криптографічного захисту інформації, що організаційно, технічно та функціонально поєднані в єдине ціле, призначена для забезпечення користувачів спеціальним зв'язком [5].

Інформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (рис. 1).

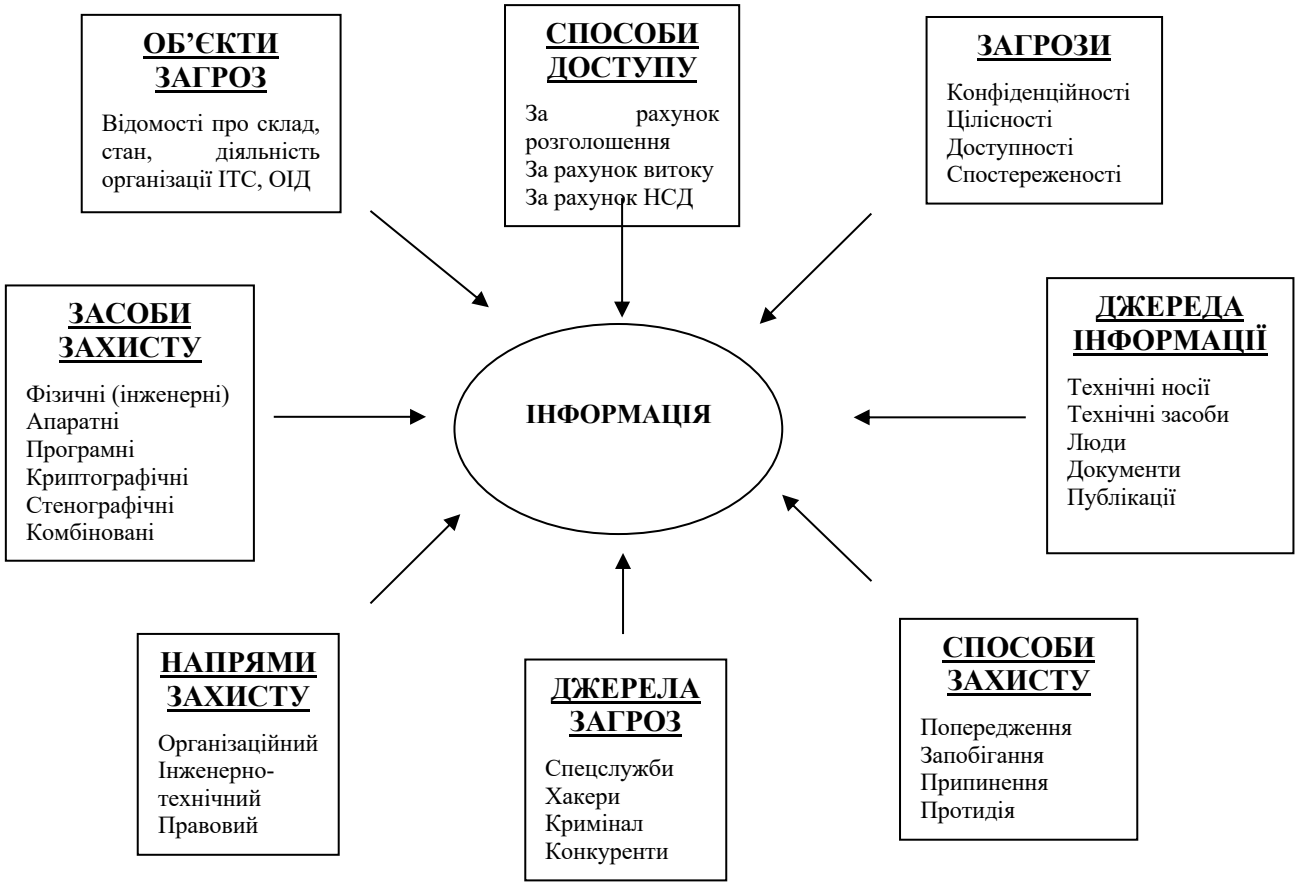


Рис. 1. Концептуальна модель безпеки інформації

Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України, є центральним органом виконавчої влади із спеціальним статусом, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України, центральним органом виконавчої влади в галузі зв'язку (крім прав та обов'язків, пов'язаних із реалізацією функцій у сфері надання послуг поштового зв'язку загального користування), спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації, головним органом у системі центральних органів виконавчої влади з формування та забезпечення

реалізації державної політики у сферах організації спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Для протидії загрозам безпеки інформації в державі створена, функціонує та розвивається система спеціального зв'язку та захисту інформації, яка складається з сукупності трьох основних компонентів: організаційної інфраструктури, нормативно-правової та нормативно-технічної бази та матеріально-технічної бази, поєднаних взаємозабезпеченням та взаємообумовленням, а також цілями і завданнями захисту інформації.

Цільовою функцією спеціального зв'язку та захисту інформації є забезпечення безпеки (конфіденційності, цілісності, доступності) інформації, як складової національної безпеки України.

Метою державної політики у сфері спеціального зв'язку та захисту інформації є створення правових, організаційних, економічних засад функціонування системи технічного захисту інформації для унеможливлення реалізації загроз для інформації.

Державна політика у сфері спеціального зв'язку та захисту інформації визначається пріоритетністю національних інтересів та здійснюється за напрямами нормативно-правового, організаційного та технічного забезпечення, регуляторної і науково-технічної діяльності, науково-методичного управління підготовкою кадрів. Важливість для безпеки держави сфери спеціального зв'язку та захисту інформації, її наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших органів влади.

З метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування спеціального зв'язку.

Порядок розроблення, виготовлення, розповсюдження, експлуатації, збереження, використання, випробування, сертифікації та допуску до експлуатації засобів спеціального зв'язку та захисту інформації, контролю за додержанням вимог безпеки при проведенні цих робіт визначається відповідними положеннями.

Діяльність, пов'язану з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів захисту інформації, а також з наданням послуг із захисту інформації, можуть здійснювати суб'єкти підприємницької діяльності, зареєстровані в порядку, встановленому законодавством.

У разі порушення вимог щодо порядку здійснення захисту інформації суб'єкти підприємницької діяльності, установи, організації посадові особи та громадяни несуть відповідальність згідно із законодавством України.

Організаційно-технічні принципи, порядок здійснення заходів з технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з захисту інформації, порядок атестації та експертизи визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами [6].

Всеохоплююче проникнення інформаційно-комунікаційних технологій в життєдіяльність особи, суспільства, держави; цифровізація сфери безпеки та оборони; атаки, пов'язані з використанням існуючих та розробкою нових вразливостей, на державні інформаційні ресурси та іншу чутливу інформацію особи, суспільства, держави, а також стрімкий розвиток та впровадження сучасних технологій штучного інтелекту, нейронних мереж, квантових та хмарних обчислень тощо, потребують удосконалення систем криптографічного захисту інформації та зумовлюють необхідність проведення модернізації спеціальних інформаційно-комунікаційних систем, їх мереж і комплексів, розроблення і впровадження

технологій і методів криптографічного захисту інформації, застосування яких забезпечить захищений інформаційний обмін між органами державного управління.

Міжнародна та вітчизняна практика спеціального зв'язку свідчить про посилення захисних характеристик засобів захисту інформації; постійно проводиться вдосконалення спроможностей уповноважених безпекових органів, дослідницьких організацій, відбувається обмін інформацією для найскорішого реагування на інциденти безпеки інформації та інформаційно-комунікаційних систем, підготовки кадрів та постійного підвищення їх кваліфікації.

Розпочата в Україні раніше робота з модернізації спеціального зв'язку, яка особливо активізувалась з моменту збройної агресії Російської Федерації проти нашої держави, дозволила вирішити низку першочергових найважливіших завдань із забезпечення захисту інформації від сучасних викликів та загроз.

Разом з тим, для забезпечення сталого розвитку спеціального зв'язку існує необхідність нарощування її виробничого потенціалу; удосконалення діючих та створення нових механізмів та інституцій для функціонування нової системи безпеки інформації, розвитку її нормативно-правового регулювання, технічного, технологічного та наукового забезпечення.

Крім того, сучасні загрози спеціального зв'язку актуалізуються через дію таких чинників, зокрема, як:

- світові тенденції з розвиту сучасних та потужних засобів електронної техніки призводять до вдосконалення методів аналізу, за допомогою яких підвищується ефективність здобування та аналізу розвідувальних даних;
- стрімкий розвиток та впровадження сучасних технологій обробки та обміну інформації, зокрема, застосування суперкомп'ютерних систем, «хмарних» технологій, технологій квантових обчислень

зумовлюють необхідність розроблення і впровадження відповідних технологій, методів та засобів спеціального зв'язку;

- не повнота обґрунтування, вибору та гармонізації міжнародних стандартів в Україні, аналізу їх безпечності;
- апаратура СРСР технічно і морально застаріла, а постійне продовження термінів її експлуатації сповільнює перехід державних органів та органів військового управління на сучасні вітчизняні засоби спеціального зв'язку.

Висновок. Таким чином, існують певні невідповідності системи спеціального зв'язку вимогам, які забезпечать виконання завдань в умовах сучасних загроз державним інформаційним ресурсам.

Слід зазначити, що для розвитку та вдосконалення спеціального зв'язку може бути застосований програмно-цільовий метод, що дозволить створити умови для ефективного використання державних фінансових ресурсів, виробничого та науково-технічного потенціалу України.

Огляд системи підтримки процесів спеціального зв'язку та захисту інформації здійснюється на основі аналізу показників складових систем спеціального зв'язку та захисту інформації у відповідності до визначених критеріїв.

Література

1. Гуз А.М. Історія захисту інформації в Україні та в провідних країнах світу : навчальний посібник. – Київ : КНТ, 2007. – 260 с.
2. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навчальний посібник / Б. А. Кормич. – К. : Кондор, 2008. – 382 с.
3. Шепет О.В. Адміністративно-правові засади технічного захисту інформації : монографія. – Київ : ФОП О.С. Ліпкан, 2012. – 296 с.
4. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис.

канд. наук з держ. упр.: 25.00.02 / Національна академія держ. управління при Президентові України. - К., 2004. URL: http://www.disslib.org/orhanizatsiyno-pravovi-pytannja-vzayemodiyi-orhaniv-derzhavnoyi-vlady-u-sferi.html (Дата звернення 26.10. 2021).

5. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (Дата звернення 26.10. 2021).
6. Про положення про технічний захист інформації в Україні : Указ Президента України №1229 від 27.09.2021. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (Дата звернення 26.10. 2021).