3. Крылов И. Ф. Криминалистика: Учебник / И. Ф. Крылов, А. И. Бастрыкин. −М. : Дело, 2007. – 934 с.

4. Шеремет А. П. Криміналістика : навч. посібник для студ. вищих навч. закл. / А.П. Шеремет. − Чернівці : Наші книги, 2008. − 440 с.

References:

1. Egorov, H. H. and Ishchenko, E. P. *Criminalistics [Kriminalistika]*. Vladivostok : TGEU publishing house. 2010. Print.

2. Krylov, V. and Lopashenko, N. *Modern criminalistics. Legal informatics and cybernetics [Sovremennaia kriminalistika. Pravovaia informatika i kibernetika]*. Moscow : LexEst. 2007.

3. Krylov, I. F. and Bastrykin, A. I. *Criminalistics [Kriminalistika]*. Moscow : Business. 2007. Print.

4. Sheremet, A. P. *Criminalistics [Kriminalistika]*. Chernivci : Nashi kny`gy`. 2008. Print.

DOI: 10.5281/zenodo.3233440
УДК 351.74:341.9

Шведун В. О., д.держ.упр., проф., ННВЦ НУЦЗУ, м. Харків,
Надьон О. В., к.ю.н., ННВЦ НУЦЗУ, м. Харків

Shvedun V., Dr. Of Scciences in Public Administration, Full Professor, Head of the Management Department, Educational, Scientific and Production Center, National University of Civil Protection of Ukraine, Kharkiv,
Nadyon O., PhD in Law sciences, Lecturer of the Management Department, Educational, Scientific and Production Center, National University of Civil Protection of Ukraine, Kharkiv

ДЕРЖАВНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ОСОБЛИВОСТІ ФОРМУВАННЯ ТА ВПРОВАДЖЕННЯ

THE STATE SYSTEM OF CYBER SECURITY ENSURING: THE FEATURES OF FORMATION AND INTRODUCTION

У статті здійснено дослідження особливостей формування та впровадження державної системи забезпечення кібербезпеки. Зокрема, визначено функції державного забезпечення кібербезпеки; виокремлено напрями функціонування державної системи моніторингу кіберпростору; виділено складові комплексної державної системи захисту інформації.

Ключові слова: *державна система; кібербезпека; кіберпростір; захист інформації; підсистема захисту.*

The research of features of formation and introduction of the state system of cyber security ensuring is conducted in the article. In particular, the functions of the state cyber security ensuring are defined; the directions of functioning of the state system of a cyberspace monitoring are allocated; the components of a complex state system of information security are defined.

Keywords: *state system; cyber security; cyberspace; information security; protection subsystem.*

Постановка проблеми. У сучасних умовах державні структури усіх рівнів гостро потребують дієвих стратегій та ефективних інструментів забезпечення кібербезпеки, оскільки саме кібербезпека є центральною складовою національної безпеки.

Визначення відповідного механізму (переважно, суспільно-державного партнерства) дозволяє приватним і державним зацікавленим сторонам обговорювати і затверджувати політики, пов'язані з проблемою кібербезпеки. Вищенаведене підкреслює актуальність обраної теми дослідження.

Аналіз останніх досліджень і публікацій. Питання забезпечення кібербезпеки досліджувалися багатьма вченими, зокрема, С. О. Бажиним [1], Є. О. Роговським [2], В. В. Скориком [3] та ін. Однак державне регулювання у сфері забезпечення кібербезпеки все ще залишається таким, що потребує вдосконалення.

Постановка завдання. Метою роботи є дослідження особливостей формування та впровадження державної системи забезпечення кібербезпеки. Досягнення поставленої мети вимагає вирішення відповідних завдань: 1) визначення функцій державного забезпечення кібербезпеки; 2) виокремити напрями функціонування державної системи моніторингу кіберпростору; 3) виділити складові комплексної державної системи захисту інформації.

Виклад основного матеріалу. Планування і визначення необхідних політик і регулюючих механізмів, чітке позначення ролей, прав і відповідальності для приватного і державного сектора в межах державного забезпечення кібербезпеки передбачає впровадження таких заходів:

- нова законодавча база для боротьби з кіберзлочинністю;
- обов'язкове інформування про інциденти безпеки;
- базові заходи забезпечення безпеки;
- нові норми матеріально-технічного забезпечення;
- підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв і механізмів захисту для ключових інформаційних інфраструктур (наприклад, національний план дій за особливих обставин, порядок поведінки в кіберпросторі, ситуаційна обізнаність);
- визначення ключових інформаційних інфраструктур, зокрема, осно-

вних активів, сервісів і взаємозалежностей;

- розробка системного та інтегрованого підходу до державного управління ризиками (наприклад, довірений обмін інформацією та державні реєстри ризиків);

- обґрунтування необхідності розробки та впровадження нової програми освіти, що акцентує увагу на навчанні ІТ-фахівців і професіоналів в сфері кібербезпеки;

- забезпечення міжнародного співробітництва у сфері кібербезпеки як з країнами-членами Євросоюзу, так і з країнами, що не входять до Євросоюзу (наприклад, прийняття міжнародних угод) [2; 3].

У деяких державних стратегіях кіберзлочинності приділяється особлива увага визначенню цілей і способів розвитку державних можливостей і необхідної законодавчої бази для вступу до міжнародної боротьби з кіберзлочинністю.

Крім того, необхідно визначити інтегровані організаційні структури, в обов'язки яких входить розробка, впровадження та тестування засобів підвищення готовності, планів відновлення після збоїв і механізмів захисту інформації. Також можлива інтеграція існуючих структур, наприклад, національних чи урядових груп реагування на надзвичайні ситуації.

У цілому, проведення комплексного дослідження і розробка програм розвитку, спрямованих на вирішення проблем забезпечення кібербезпеки та відмовостійкості як існуючих, так і майбутніх систем і сервісів (наприклад, інтелектуальних пристроїв дозволить суттєво підвищити рівень захищеності державних і службових таємниць, що, у свою чергу, дозволить зміцнити національну безпеку держави.

Державна система моніторингу кіберпростору повинна являти собою сукупність спеціалізованих апаратно-програмних засобів, призначених для:

- оцінки обстановки в кіберпросторі;

- систематичного збору і обробки інформації про можливі загрози кібербезпеки;

- комплекс засобів для прогнозування можливих варіантів і технологій реалізації кібератак і потенційно небезпечних об'єктів, здатних здійснювати кібератаки;

- виявлення ознак і фактів кібератак на інформаційні об'єкти і надання інформації про можливий вплив кібератак на інформаційну інфраструктуру [1; 4].

При цьому необхідно відмітити, що ведення розвідки в кіберпросторі вимагає цифрового проникнення в мережі і комп'ютери потенційного противника і передбачає використання абсолютно нових джерел, форм і способів збору даних й інформації, а також розробку нових розвідувальних засобів і технологій, тактичних і технічних прийомів. На систему моніторингу і розвідки кіберпростору повинна покладатися функція забезпечення формування та ведення бази даних щодо розкритих різних видів і джерел кі-

берзагроз (кібератак), що передбачає створення і ведення каталогу потенційних загроз кібербезпеки і ознак кібервпливів на інформаційні ресурси, а також визначення номенклатури потенційних загроз кібербезпеки,створення і ведення банку критеріїв виявлення кібератак на інформаційні системи.

Комплексна державна система захисту інформації повинна містити сучасні системи захисту інформації та засобів контролю їх ефективності. До складу системи повинні входити:

- система попередження і виявлення комп'ютерних атак;
- підсистема програмно-апаратних засобів захисту від несанкціонованого доступу;
- підсистема криптографічного захисту інформації та шифрування;
- підсистема контролю стану і функціональної стійкості (рис. 1) [1; 3].

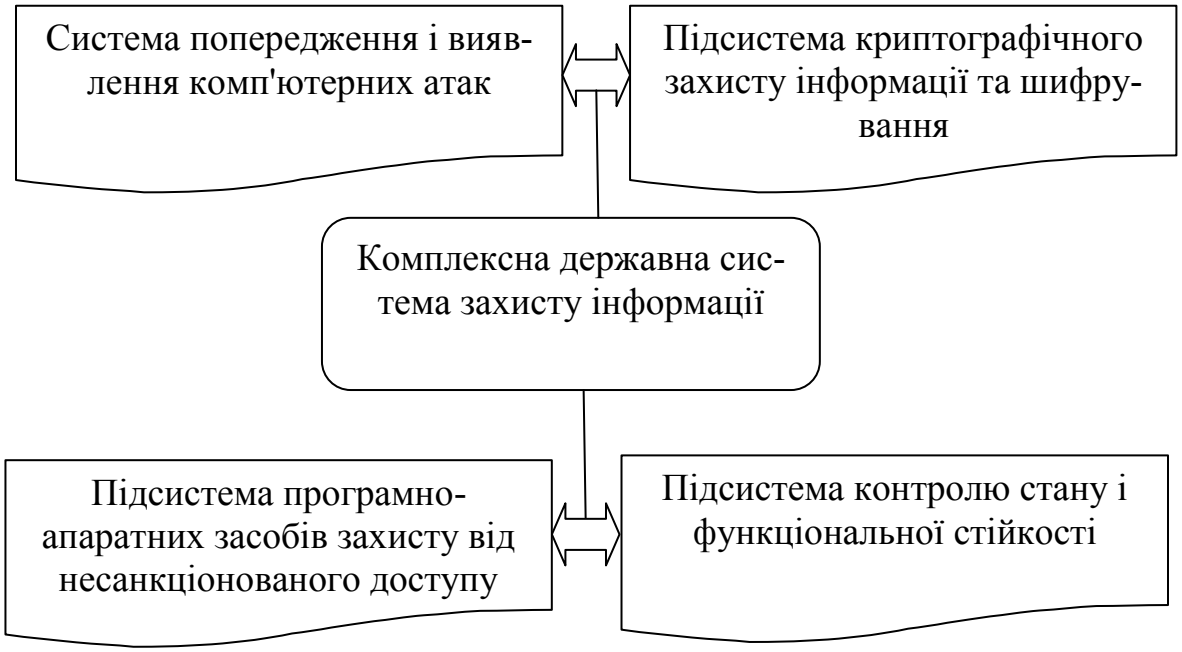

Рис. 1. Комплексна державна система захисту інформації

Зокрема, підсистема програмно-апаратних засобів захисту від несанкціонованого доступу повинна містити наступні компоненти:

- системи і засоби захисту (ідентифікації й аутентифікації користувачів);
- засоби розмежування доступу, а також антивірусного захисту, захищені системи управління базами даних;
- засоби міжмережевого екранування;
- засоби формування та перевірки електронних підписів;
- апаратно-програмні засоби доступу до віртуальних систем;
- засоби посилення аутентифікації на основі біометричних сканерів, і радіоміток;
- засоби захисту інформації від витоку (односпрямовані шлюзи) і засоби запобігання витоку інформації;

- засоби контролю захищеності (сканер захищеності);

- програмно-апаратні засоби захисту інформації технології «тонкий клієнт»;

- засоби захисту від спаму тощо [1; 2].

Необхідно також безумовне застосування технічних засобів охорони даних, що обробляють критично важливу інформацію і комплексів засобів захисту даних. Що стосується підсистеми криптографічного захисту інформації і шифрування, то вона являє собою сукупність апаратних, програмних і апаратно-програмних засобів, а також систем і комплексів, призначених для захисту інформації, що циркулює в технічних засобах, в процесах її обробки, зберігання і передачі по каналах зв'язку, включаючи шифрувальну техніку, і забезпечуючи криптографічне перетворення інформації і управління процесом розподілу ключів. При цьому засоби криптографії та шифрування повинні захищати не тільки інформацію всередині мережі і каналах зв'язку, а також і внутрішні інформаційні ресурси технічних засобів (внутрішні та зовнішні носії інформації) і є ключовим бар’єром захисту в державній системі забезпечення кібербезпеки.

Висновки. У цілому, у роботі було досягнено її основну мету, зокрема, було отримано такі результати.

1. Визначено функції державного забезпечення кібербезпеки. Показано, що переважно воно повинно бути орієнтоване на визначення ключових інформаційних інфраструктур, зокрема, основних активів, сервісів і взаємозалежностей, а також на розробку системного та інтегрованого підходу до державного управління ризиками.

2. Виокремлено напрями функціонування державної системи моніторингу кіберпростору. Наголошено, що ключовими з них повинні бути систематичний збір і обробка інформації про можливі загрози кібербезпеки, а також розробка комплексу засобів для прогнозування можливих варіантів і технологій реалізації кібератак і потенційно небезпечних об'єктів, здатних здійснювати кібератаки.

3. Виділено складові комплексної державної системи захисту інформації: система попередження і виявлення комп'ютерних атак; підсистема програмно-апаратних засобів захисту від несанкціонованого доступу; підсистема криптографічного захисту інформації та шифрування; підсистема контролю стану і функціональної стійкості.

Список використаних джерел:

1. Бажин С. А. Дезоптимизация управляющих решений в автоматизированных системах как способ информационного терроризма / С. А. Бажин // Вопросы защиты информации. − 2008. − № 4. − С. 24−28

2. Роговский Е. А. Кибербезопасность и кибертерроризм / Е. А. Роговский // США. Канада. Экономика, политика, культура. – 2003. − N 8. − С. 23−41.

3. Сельцовский П. А. Разновидности и формы терроризма в современных условиях / П. А. Сельцовский // Социально-гуманитарные знания. – 2003. − № 4. −

С. 301−307.

4. Скорик В. В. Международная информационная безопасность: проблемы и перспективы / В. В. Скорик // Электросвязь. − 2008. − № 8. − С. 2−4.

References:

1. Bazhin, S. A. "Dezoptimization of the operating decisions in the automated systems as a way of information terrorism. [Dezoptimizatsiya upravlyayushchikh resheniy v avtomatizirovannykh sistemakh kak sposob informatsionnogo terrorizma]" *Questions of information security* 4 (2008): 24−28. Print.

2. Rogovsky, E. A. "Cyber security and cyberterrorism." *USA. Canada. Economy, policy, culture* 8 (2003): 23−41. Print.

3. Seltsovsky, P.A. "Versions and forms of terrorism in modern conditions." *Social and humanitarian knowledge* 4 (2003): 301−307. Print.

4. Skorik, V. V. "International information security: problems and prospects." *Telecommunication* 8 (2008): 2−4. Print.