УДК 681.12

А. О. Артоуз[1]
І. С. Колесник[2]

КОМП'ЮТЕРИЗОВАНА СИСТЕМА МОНІТОРИНГУ ЗАХИЩЕНОСТІ ОБ'ЄКТУ

Вінницький національний технічний університет

Анотація
Проаналізовано актуальність дослідження. Наведено основні методи та засоби забезпечення захисту інформації.
Ключові слова: система захисту атак, інтенсивність атак, бар'єр захисту.

Abstract
The relevance of the study is analyzed. The main methods and means of ensuring information protection are presented.
Keywords: attack protection system, attack intensity, protection barrier.

Вступ

В епоху глобалізації процесів життєдіяльності сучасного суспільства, коли інформаційні канали стали невід'ємною системоутворюючою частиною діяльності людства, усе більшої актуальності набуває завдання передачі величезних інформаційних потоків та забезпечення конфіденційності передаваної інформації, а також розмежування прав доступу до неї. [1].

Результати дослідження

Війна з росією значно змінила життя кожного, будь яка наявність загроз інформації є небезпечною. Кожна держава відстоює свій інформаційний суверенітет, основою якого є національні інформаційні ресурси. Тому Конституція України визначає захист суверенітету і територіальної цілісності, забезпечення інформаційної безпеки найважливішою функцією держави, справою всього українського народу. У свою чергу, Закон України «Про інформацію», виділяє основні елементи забезпечення інформаційного суверенітету України [2], захист яких диктує, що в першу чергу необхідно протидіяти: порушенню права власності України на свої інформаційні ресурси; спробам завадити створенню та функціонуванню національних систем інформації; несанкціонованій зміні, тобто порушенню режиму доступу інших держав до інформаційних ресурсів України; порушенню принципу рівноправного співробітництва з іншими державами.

До основних засобів захисту інформації можна віднести:

- фізичні засоби;
- апаратні засоби;
- програмні засоби;
- апаратно-програмні засоби;
- криптографічні;
-організаційні методи.

Викладене свідчить про те, що проблема надання інформації безпеки держави об'єктів критичних інфраструктур є актуальним завданням.

Визначення основних завдань ІТ-безпеки показує, що пріоритетом є створення ефективного механізму

координація зусиль органів влади та підрозділів організацій, які повинні забезпечувати безпеку

інформації відповідних установ [3].
Крім того, необхідно здійснити ряд важливих державних заходів, регіональний та галузевий рівні організації, регулювання та права та науково-методичне забезпечення.
Як показує досвід розвинених країн, вивчення механізмів захисту інформації включає на перших кроках етап ідентифікації (визначення) елементів, які слід вважати критичною інфраструктурою. Проте важливий напрямок захисту інформації на об'єктах критичної інфраструктури є впровадження належного управлінського впливу.[4]
Враховуючи вищевикладене, можна сказати, що основні завдання в забезпечення безпеки інформації в має бути:

- нормативно-правове регулювання у сфері забезпечення безпеки інформації;
- визначення загроз безпеки інформації і виявлення уразливостей в програмному і апаратному забезпеченні;
- оцінка реальної захищеності об’єктів критичних інфраструктур держави;
- розробка вимог по забезпеченню безпеки інформації;
- розробка та реалізація заходів по забезпеченню безпеки інформації;
- здійснення контролю і нагляду в галузі забезпечення безпеки інформації;
- інформаційне, матеріально-технічне і науково-методичне забезпечення безпеки інформації;
- підготовка та перепідготовка фахівців в області забезпечення безпеки інформації.

Висновки

Таким чином, створення комплексної системи захисту дозволяє забезпечити ефективний захист інформації та ресурсів з її обробки від можливих загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. . Леоненко Г.П., Юдин А.Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. -2013. — Вип. 1(3). — С. 44.
2. Конституція України. Прийнята Верховною Ра-дою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – № 30 – С. 141.
3. Закон України «Про національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України, 1998. – № 27 – 28. – С. 181
4. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв’язання». — К.: НАДУ, 2014. — С. 92-95.

Артоуз Анастасія Олександрівна – студентка групи 1КІ-19б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: artouznastia13@gmail.com.
Науковий керівник: ***Колесник Ірина Сергіївна*** –доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: iskolesnyk@gmail.com.

Artouz Anastasia Oleksandrivna - student of group 1KI-19b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: artouznastia13@gmail.com.
Scientific adviser: Kolesnyk Iryna Serhiivna - Associate Professor of Computer Science, Vinnytsia National Technical University, Vinnytsia, e-mail: iskolesnyk@gmail.com.