УДК 681.3.06

О.С.Глущак
А.В.Дудатьєв

ІНЖЕНЕРНО – ТЕХНІЧНИЙ ЗАХИСТ ПІДПРИЄМСТВА

Вінницький національний технічний університет;

Анотація
Детальний огляд існуючих методів інженерно-технічного захисту та його складових.
Ключові слова: інженерно, технічний, захист, безпека, підприємство.
Abstract
Detailed review of existing methods of engineering protection and its components.
Keywords: *engineering, technical, protection,* security, company.

Вступ

Перед сучасним підприємством гостро стоять проблеми забезпечення інформаційної безпеки. Це пов'язано з розвитком інформатизації підприємства, з постійно зростаючою вартістю інформації, з одного боку, і активністю інформаційно-аналітичних структур і різного роду порушників, з іншого. Інформація обмеженого доступу використовується компаніями-конкурентами, шахраями, терористами у своїх корисливих цілях, завдаючи збитки підприємству – власникові цієї інформації.

Проблеми й завдання компаній сьогодні стали порівнянні із проблемами й завданнями цілих держав. Як і держави, вони співробітничають і воюють. Але війни тут називаються інформаційними: хто має інформацію, володіє якщо не світом, то фінансовими потоками. Як не дивно, але й сьогодні не всі керівники усвідомлюють нагальну потребу організації на їхньому підприємстві системи захисту комерційної таємниці. Серед тих, хто таку необхідність все-таки розуміє, чимало не знають, що слід робити, аби зберегти ті чи інші відомості в таємниці, з вигодою реалізувати їх, не зазнати збитків від їхнього витоку або втрати.

Метою даного дослідження є опис інженерного-технічного захисту його завдань і засобів.

Результати дослідження

Інженерно-технічний захист (ІТЗ) - це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації [1]. Яскравим прикладом інженерно-технічного захисту є побудова різноманітних конструкцій, а також застосування різноманітного устаткування.

Основні положення концепції інженерно-технічного захисту інформації визначають її принципи, які конкретизуються в методах, способах і засобах інженерно-технічного захисту інформації. Якщо ціль відповідає на запитання, що потрібно досягти в результаті інженерно-технічного захисту інформації, а завдання - що треба зробити для цього, то принципи дають загальне подання про підходи до рішення поставлених завдань. Принципи можна розділити на принципи інженерно-технічного захисту інформації як процесу й принципи побудови системи інженерно-технічного захисту інформації [1].

Інженерно-технічний захист інформації на об'єкті досягається виконанням комплексу організаційно-технічних і технічних заходів із застосуванням (за необхідності) засобів захисту інформації від витоку інформації чи несанкціонованого доступу до неї по технічним каналах з порушенням її цілісності, процесів її обробки, передачі й зберігання, порушення її доступності та працездатності технічних засобів носіїв інформації тощо [2].

Обов'язковість захисту інженерно-технічними заходами інформації, яка становить передбачену законом таємницю, конфіденційної інформації, що є власністю держави чи інших установ, відкритої інформації, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації,

важливої для особи та суспільства, якщо ця інформація циркулює в різноманітних установах, органах державної влади та органах місцевого самоврядування, у військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях, тощо обумовлена нормативно-правовим забезпеченням України [2].

Різноманіття класифікаційних характеристик дозволяє розглядати інженерно-технічні засоби по об'єктах впливу, характеру заходів, способам реалізації, масштабом охоплення, класу засобів зловмисників, яким чиниться протидія з боку служби безпеки [3].

Засоби інженерного захисту поєднують конструкції, що утрудняють рух зловмисника й поширення стихійної сили до джерела інформації, і включають огородження території, будинків і приміщень, шафи, сейфи й сховища, а також засобу системи контролю й керування доступом людей і транспорту в контрольовані зони.

До засобів технічного захисту інформації відносяться:

- технічні засоби, основне функціональне призначення яких - захист інформації від загроз витоку, порушення цілісності та блокування;
- технічні засоби, у яких додатково до основного призначення передбачено функції захисту інформації;
- засоби, що призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв, які створюють загрозу для інформації, або контролю ефективності технічного захисту інформації [3].

Висновки

Практичне застосування інженерно-технічного захисту, як елемента комплексної системи захисту інформації, приведе до зменшення ризику несанкціонованого доступу до інформаційних ресурсів підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Організація інженерно-технічного захисту [Електронний ресурс]. – Режим доступу: URL http://bukvar.su/informatika_programmirovanie/page,2,169899-Organizaciya-inzhenerno-tehnicheskoiy-zashity-informacii.html – Назва з екрану
2. Інженерно-технічний захист інформації та її класифікація [Електронний ресурс]. – Режим доступу: URL http://um.co.ua/9/9-2/9-26963.html – Назва з екрану
3. Захист інформації та інформаційного продукту [Електронний ресурс]. – Режим доступу: URL http://referat-ok.com.ua/informatika/zahist-informaciji-ta-informaciinogo-produktu – Назва з екрану

Глущак Олександр Сергійович — студент групи 1БС-15мс факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: gluschak.dezmen@gmail.com

Науковий керівник:
Дудатьєв Андрій Вініамінович —канд. техн. наук, доцент кафедри захисту інформації м. Вінниця

Gluschak Olexandr S. — student group 1BS-15ms faculty of Information Technology and Computer Engineering, Vinnytsia a National Technical University, Vinnytsia, e-mail: gluschak.dezmen@gmail.com

Supervisor:
Dudatyev Andriy V.— candidate. Sc. Associate Professor, Department of Information security,c. Vinnitsa