

УДК 004.056.5:342

Орловський Д.І.¹, Куцак С.В.²

¹студ. гр. РТ-818 НУ «Запорізька політехніка»

²старш. викл. НУ «Запорізька політехніка»

СТАН НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Серед методів захисту інформації від несанкціонованого доступу стеганографія виділяється своєю особливістю, забезпечуючи конфіденційність не шляхом приховування змісту повідомлення, а через збереження в таємниці самого факту його існування.

Базові поняття стеганографії були погоджені в 1996 році на 1-й Міжнародній конференції з приховування інформації – Information Workshop on Information Hiding'96. Проте імплементація напрацювань науковців, що передбачає підготовку відповідних нормативно-правових актів (НПА) і нормативних документів з технічного захисту інформації (НД ТЗІ), відбувається повільно і через це не дає можливості забезпечити належне правове, понятійне та технологічне взаємоузгодження у використанні методів стеганографічного захисту інформації.

В даній роботі проводиться аналіз вітчизняного нормативно-правового забезпечення стеганографічного захисту інформації та (з урахуванням положень Доктрини інформаційної безпеки України і Стратегії національної безпеки України) Сполучених Штатів Америки (США) як стратегічного партнера і Російської Федерації (РФ) як джерела довгострокових системних загроз національній безпеці України.

Дослідження показало, що у вітчизняних НПА відсутні будь-які норми-дефініції щодо стеганографії. Єдина згадка про стеганографію є лише в НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» як синоніму «принципу забезпечення конфіденційності шляхом організації прихованого каналу передачі всередині іншого відкритого каналу».

Не менш «обмеженою» (але більш предметною) щодо стеганографії є нормативно-правова база РФ, де це поняття зустрічається у декількох методичних документах з інформаційної безпеки та детально розглядається в наказі Федеральної податкової служби «Про забезпечення безпеки персональних даних при їх обробці в автоматизованих інформаційних системах податкових органів», де стеганографічному захисту відведений окремий розділ: «Загальна характеристика нетрадиційних інформаційних каналів» [1]. У цьому наказі стеганографія визначається як «мистецтво приховувати інформацію серед іншої інформації», а методи комп'ютерної стеганографії - це методи, що «призначені для приховування факту передачі повідомлення шляхом вбудовування прихованої інформації в зовнішньо нешкідливі дані (текстові, графічні, аудіо- або відеофайли). Також у цьому документі наводяться пояснення щодо можливих каналів реалізації стеганографічних методів у інформаційних системах передачі даних.

В США питаннями стеганографічного захисту займаються декілька державних інституцій. Так, Федеральним Бюро Розслідувань ще у 2004 році опублікувало статтю «Огляд стеганографії для експерта з комп'ютерної криміналістики» [2], в якій детально розглянуті базові поняття стеганографії. Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) дає визначення стеганографії як «мистецтва та науки спілкування таким чином, що прихованим є сам факт існування спілкування» [3] та «вбудовування даних у інші дані з метою їх приховування» [4].

В інструкціях Комітету із систем національної безпеки Міністерства оборони США (Committee on National Security Systems (CNSS) Instruction) стеганографія визначена як «мистецтво, наука та практика спілкування таким чином, щоб приховати існування спілкування». Крім цього, термін «стеганографія» широко використовується галузевих статтях Міністерства юстиції США, де питання стеганографії вивчається в контексті нової можливої кіберзагрози [5].

Таким чином, порівняльний аналіз понятійної бази стеганографії в різних країнах показав, що США мають найбільш повну та інформативну термінологію в галузі стеганографії. В РФ та Україні практично відсутнє нормативно-правове регулювання методів та засобів стеганографії.

На нашу думку, відсутність належного вітчизняного нормативного-правового забезпечення в сфері стеганографічного захисту інформації,

можливо, є недопрацюванням суб'єктів нормотворення або ж таке забезпечення існує, але з грифом обмеженого доступу (грифом секретності), і не може бути досліджено в рамках відкритих літературних джерел.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Приказ Федеральной налоговой службы от 21 декабря 2011 г. N ММВ-7-4/959@ [Електронний ресурс]. – Режим доступу: <https://www.garant.ru/products/ipo/prime/doc/70012476/>
2. Kessler G.C. An Overview of Steganography for the Computer Forensics Examiner [Електронний ресурс]. – Режим доступу: <https://bit.ly/3rA9F0W>
3. NIST Special Publication 800-101. Revision 1 [Електронний ресурс]. – Режим доступу: <https://bit.ly/2PDobI2>
4. NIST Special Publication 800-86 [Електронний ресурс]. – Режим доступу: <https://bit.ly/3rzlgxn>
5. Wingate J.E. Digital Steganography: Threat or Hype? [Електронний ресурс]. – Режим доступу: <https://bit.ly/3cu83S6>