ЗМІСТ

ПЕРЕДМОВА

Завдання захисту інформації від несанкціонованого доступу вирішувалося в усі часи історії людства. Уже в стародавньому світі виділилося два основні напрями рішення цього завдання, що існують і до сьогоднішнього дня: криптографія й стеганографія. А особливо за сучасних умов повномасштабного вторгнення російського агресора на територію України ця тематика є надто затребуваною. Метою криптографії є приховання вмісту повідомлень за рахунок їх шифрування. *На відміну від цього, з огляду стеганографії приховується сам факт існування таємного повідомлення.*

Саме розвиток сучасних засобів інформаційних в останнє десятиліття в новий поштовх для розвитку комп'ютерної стеганографії. З'явилась значна кількість нових галузей застосування. При цьому, існують два основні напрями в комп'ютерній стеганографії: пов'язаний із цифровою обробкою сигналів і непов'язаний. Останній напрям має обмежене застосування у зв'язку з відносною легкістю розкриття й/або знищення прихованої інформації. Більшість поточних досліджень у множині стеганографії так чи інакше пов'язані із цифровою обробкою сигналів. Це дозволяє вважати про цифрову стеганографію. Саме цій науці і присвячений даний навчальний посібник.

Серед завдань навчальної дисципліни «Воєнна стеганографія: квантова симуляція та космічна гіперспетроскопія» важливим також є вивчення основ стеганографічного захисту інформації, методів та кіберобчислювальних алгоритмів стеганографічного перетворення, дослідження відповідних атак на стеганосистеми, а також вивчення методів протидії. Саме для вивчення відповідної теми навчальної дисципліни і призначений

новий навчальний посібник у повоєнній Україні, здатний системно висвітлювати методи та принципи побудови, а також кіберстійке застосування стеганографічних моделей (блоків, підсистем тощо) і протоколів. Вивчення відповідної теми має основоположне значення, оскільки стеганографічні системи та протоколи є, після криптографії, фундаментальною основою захисту інформації та кібербезпеки.

У даному посібнику наведені основні напрями стеганографії, математична модель та структурна схема стеганографічної системи, класифікація систем цифрової стеганографії та їх використання, методи стеганографічного захисту інформації, розглянуті атаки на стеганосистеми та протидія їм. За результатами вивчення відповідної теми навчальної дисципліни студенти повинні:

знати: основні методи, системи та засоби забезпечення стеганографічного захисту інформації, аналізу стійкості стеганосистем та безпечності стеганопротоколів; порядок та умови застосування ключових стеганосистем, а також методи та засоби управління ключовими даними; основні тенденції та напрями розвитку теорії та практики стеганосистем та стеганопротоколів, прогнозування їх можливостей та можливостей стеганоаналітиків (порушників); функціональні можливості та порядок застосування сучасних пакетів програмної реалізації стеганографічних перетворень та стеганографічних бібліотек; порядок оцінки якісних показників стеганосистем та стеганопротоколів;

вміти: розробляти вимоги та обирати для застосування стеганосистеми та стеганопротоколи, що мінімізують впливи порушників; вибирати та застосовувати критерії та показники оцінки стійкості стеганосистем та безпечності стеганопротоколів; обґрунтовувати вимоги до ключових систем та управління ключовими даними стеганосистем, здійснювати аналіз їх властивостей; проводити аналіз та синтез стеганопротоколів за критерієм безпечності, порівнювати їх з використанням умовних та безумовних критеріїв; застосовувати стандартні пакети при розв'язанні прикладних задач моделювання стеганосистем, ключових систем і стеганографічних протоколів.

Таким чином, у результаті вивчення відповідної теми навчальної дисципліни, для викладення якої і призначено даний навчальний посібник, студенти повинні засвоїти методи та принципи побудови, реалізації та застосування стеганографічних систем та протоколів, вміти застосовувати методи, алгоритми та засоби оцінки стеганостійкості та інших якісних показників стеганосистем та стеганографічних протоколів. При вивченні стеганографічних протоколів студенти повинні вміти обґрунтовувати вимоги, розв'язувати завдання аналізу та синтезу стеганографічних протоколів, складати програмні моделі та здійснювати моделювання стеганосистем, а також саме у воєнних практиках реалізовувати кіберобчислювальні алгоритми стеганографічного захисту інформації.

Від авторів

РОЗДІЛ 1.
СИСТЕМА АЛГОРИТМУ ПРІОРИТЕТНОСТІ ЯК ПРЕДМЕТ ВОЄННОЇ СТЕГАНОГРАФІЇ

1.1. Сутність воєнної стеганографії

Автори означеного посібнику є лаконічними та стислими щодо сутності воєнної стеганографії, оскільки сама назва говорить про себе («менше порожніх слів, а більше діла як конкретизації справи»). Адже, на наш погляд, це така утаємнюваність, при якому повідомлення закодовані таким чином, що не виглядає як повідомлення, оскільки відсутній очевидний факт його існування. Лише одному людському нейромозку довічно знати сам факт такого існування завдяки його феноменальній пам'яті, а саме: ніщо і ніколи в житті не стирається. А, навпаки, в екстремальних умовах життєвого світу феноменальна пам'ять з неймовірною швидкістю здатна відновлювати ту чи іншу інформацію (повідомлення, факт, подію, фрагмент, сюжет тощо).

1.2. Базова термінологія та її класифікаційний характер у воєнній стеганографії

Саме у повоєнній Україні варто окреслити, що різноманітні способи застосування кібератак у розвідувально-підривній діяльності іноземних спецслужб або під час ведення кібервійни країною-агресором безпосередньо цілеспрямовані на зупинку у роботі, втрату контролю або виведення з ладу інформаційних систем, які забезпечують першочергові потреби людини, суспільства і держави (води, тепла, світла, транспорту, банківських операцій, систем зв'язку тощо) задля породження хаосу, посилення суспільної напруги, дестабілізації країни в цілому. Через збільшення кількості випадків успішних кібератак, у більшості провідних країнах світу з метою зведення до єдиної системи важливих об'єктів й найуразливіших інформаційно-телекомунікаційних систем та мереж, втрата або

порушення сталого функціонування яких призведе до значних або навіть непоправних негативних наслідків для національної безпеки і оборони, введено термін «критична інфраструктура» [35, с. 214].

В повоєнній Україні, з огляду на останні події, кількість реалізованих кібератак, зокрема з боку російського ворога, значно збільшується і оцінка уразливості та потенційних наслідків припинення або руйнування об'єктів інфраструктури стає однією із основних функцій держави. Тому, в інтересах забезпечення національної безпеки виникає питання необхідності підвищення ефективності використання та захисту державних інформаційних ресурсів (ДІР), особливо інформації з обмеженим доступом, яка обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, втрата якої може завдати й інших (додаткових) тяжких наслідків. Так як в основу порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави з метою їх першочергового захисту від кібератак покладено принцип «негативний наслідок – критична інфраструктура», тому питання визначення ступеня тяжкості негативних наслідків й величини завданої шкоди та інших можливих витрат на обмеження доступу та захист інформації з обмеженим доступом від її витоку, до якого може призвести кібератака, є актуальним.

Адже аналіз праць вітчизняних науковців (Д. Бірюков Д, С. Кондратов, О. Суходоли, С. Гнатюк, О. Юдін) виявив наявність значної кількості проблем у сфері захисту критичної інфраструктури держави, починаючи з відсутності базових необхідних понять, наприклад «захист критичної інфраструктури» та «захист критичної інформаційної інфраструктури», нормативного-правового забезпечення даної сфери (закону, концепції, стратегії, доктрини тощо) і до необхідності формування державної системи забезпечення захисту критичної інфраструктури у цілому [35. с. 214]. Але, на наш погляд, всі ці наукові здобутки вище означених дослідників є дотичними до воєнної стеганографії, що свідчать про існуючий складний стан кіберпростору України. Все це вимагає віднесення захисту критичної інфраструктури до пріоритетних напрямів протидії загрозам національній безпеці з метою попередження можливої потенційної школи державі та усунення негативних наслідків від їх реалізації.

Важливим є аналіз потенційних негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему об'єкта критичної інфраструктури, яка обробляє інформацію з обмеженим доступом (ІзОД) (або ДІР) з метою подальшої уніфікації їх у єдиний класифікатор негативних наслідків кібератак при проведенні процедури оцінювання школи національній безпеці України у разі її витоку.

У цьому змісті основне базове поняття ***інформаційно-телекомунікаційної системи*** (ІТС) як сукупності інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле, наведено у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [37], який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТС. Цим законом [37] наведені й інші поняття, необхідні для проведення досліджень у даній сфері такі як:

– ***телекомунікаційна система*** (ТС) – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– ***інформаційна (автоматизована) система*** (ІС(АС)) – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– ***захист інформації в системі*** – діяльність, що спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– ***несанкціоновані дії щодо інформації в системі*** – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

– ***обробка інформації в системі*** – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– ***знищення інформації в системі*** – дії, внаслідок яких інформація в системі зникає;

– ***виток інформації*** – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– ***користувач інформації в системі*** (користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

– ***доступ до інформації в системі*** – отримання користувачем можливості обробляти інформацію в системі;

– ***порядок доступу до інформації в системі*** – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

– ***комплексна система захисту інформації*** (КСЗІ) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

– ***криптографічний захист інформації*** (КЗІ) – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування / відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– ***технічний захист інформації*** *(ТЗІ)* – вил захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушенні цілісності та режиму доступу до інформації;

– ***блокування інформації в системі*** – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

– ***порушення цілісності інформації в системі*** – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

– ***власник системи*** – фізична або юридичні особа, якій належить право власності на систему;

– ***володілець інформації*** – фізична або юридична особа, якій належать права на інформацію. [35, с. 214]

Також законодавчо визначено [37], що об'єктом захисту в ІТС є інформація, яка обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Наразі загальними вимогами та організаційними засадами забезпечення захисту інформації в інформаційних, телекомунікаційних та ІТС є «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [55], які містять поняття автентифікації та ідентифікації, і конкретизують інформацію, яка підлягає захисту в ІТС, а саме [55]: відкрита інформація, яка належить до ДІР, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (викрита інформація); конфіденційна інформація (у т. ч. персональні дані); службова інформація; інформація, яка становить державну або іншу передбачену законом таємницю (таємна інформація); інформація, вимога щодо захисту якої встановлена законом.

На виконання плану заходів щодо захисту ДІР затвердженого Розпорядженням КМУ №1135 від 05.11.2014 року та з метою підвищення рівня захисту інформаційних ресурсів, що обробляється в ІТС об'єктів критичної інфраструктури держави, визначено механізм, за яким відбуватиметься формування їх переліку. Зокрема, розроблено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» [54] (далі – Порядок), який затверджено Постановою КМУ від 09 жовтня 2020 р. №943 «Деякі питання об'єктів критичної інформаційної інфраструктури», за якою державні органи, органи центральної виконавчої влади, інші заінтересовані державні органи повинні сформувати та подати Державній службі спеціального зв'язку та захисту інформації (Держспецзв'язку) пропозиції для формування переліку ІТС об'єктів критичної інфраструктури держави [54]. У відповідності до цих пропозицій заінтересовані органи мають визначити негативні наслідки та вказати їх умовне позначення, до яких може призвести кібератака на ІТС із приведеного у порядку переліку із зазначенням виду інформації, яка обробляється. І якщо вказати, що в ІТС обробляється ІзОД, тоді виникає питання щодо необхідності врахування й інших тяжких наслідків, які визначаються при обмеженні доступу до такої інформації як державна таємниця [50], та зазначення їх у пропозиціях, до яких може призвести

кібератака на ІТС у разі її витоку. У Порядку [54] містяться такі поняття та визначення як:

– ***заінтересовані органи*** – державні органи, органи місцевого самоврядування, органи управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні яких є об'єкт критичної інфраструктури держави та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта);

– ***кібератака*** – несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи);

– ***критична інфраструктура*** – сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв);

– ***об'єкти критичної інфраструктури*** –підприємства та установи (незалежно від форми власності) таких галузей як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення) [35, с. 216].

Також, судячи зі змісту положень пп. 4, 5 Порядку [54], під ***критичною інформаційною інфраструктурою держави*** (КІІД) слід розуміти включені до переліку ІТС об'єктів критичної інфраструктури, що захищаються від кібератак у першу чергу (пріоритетно) власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки.

У додатку цього Порядку [54] приведені пропозиції до формування переліку ІТС об'єктів критичної інфраструктури держави (табл. 1.1), які після погодження з СБУ налаються заінтересованими