УДК 378:004.056.55

Загацька Н. О.
Житомирський державний університет імені Івана Франка, Житомир, Україна

ОСНОВИ ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНОГО АПАРАТУ КРИПТОЛОГІЇ

DOI:10.14308/ite000478

Становлення криптології як науки зумовило необхідність формування власного понятійного апарату цієї дисципліни з притаманною йому специфікою. Проблема полягає у відсутності до теперішнього часу загальноприйнятого тлумачення понять та термінів, вивчення яких є основою для успішного засвоєння студентами навчального матеріалу дисципліни.

Одним із основних завданнями, що мають бути вирішені у процесі навчання цієї дисципліни, є забезпечення ґрунтовного вивчення студентами теоретичних основ, що в подальшому сприятиме формуванню професійних компететностей, необхідних для розуміння загальних принципів побудови криптографічних систем.

Статтю присвячено дослідженню понятійно-термінологічного апарату криптології. Проведено порівняльний аналіз понять цієї науки на основі вітчизняних та зарубіжних фахових джерел, тлумачних і спеціалізованих словників, нормативно-правових та законодавчих актів України у галузі криптографічного захисту даних. У статі описуються фундаментальні та похідні терміни з огляду на їх структурно-логічні зв'язки. Запропоновано класифікацію криптосистем: за особливостями ключа, за видом та за технологію шифрування. Робиться спроба уточнення єдиної термінології науки, що сприятиме підвищенню рівня оволодіння нею майбутніми фахівцями з інформатики.

Ключові слова: *криптологія, криптографічний алгоритм, шифрування, ключ, електронний цифровий підпис, хеш-функція, імітовставка.*

Постановка проблеми. Однією з найважливіших умов успішного функціонування будь-якої інформаційної системи є захист її даних від несанкціонованого доступу. На сьогоднішній день випускник вищого навчального закладу, зокрема фахівець з інформатики, має володіти не лише фундаментальними знаннями, уміннями та навичками з інформаційно-комунікаційних технологій, а й мати також спеціальну підготовку в галузі захисту інформаційних ресурсів відповідно до сучасних вимог ринку праці. Підготовка студентів здійснюється згідно з навчальними планами, що включають перелік нормативних курсів, серед яких все більшого значення набуває «криптологія – дисципліна, яка вивчає методи побудови та аналізу систем захисту інформаційних ресурсів, основаних на математичних перетвореннях даних з використанням секретних параметрів [1, с. 4]». У процесі навчання цієї дисципліни передбачається ознайомлення студентів зі спеціальною термінологією, яка є доволі складною і неоднозначною. Це зумовлено тим, що з давніх часів і протягом багатьох століть криптологія знаходилася переважно в руках державних, військових та дипломатичних служб. Тому коло людей, які вивчали та застосовували цю науку, було дуже вузьким, а самі методи перетворення даних трималися в секреті. Основними чинниками, що вплинули на розвиток і відкритість криптології стали поява персональних комп'ютерів та удосконалення технологічної бази обміну інформаційними ресурсами. Становлення криптології як науки зумовило необхідність формування власного понятійного апарату цієї дисципліни з притаманною йому специфікою. Проблема полягає у відсутності до теперішнього часу загальноприйнятих тлумачень понять та термінів, вивчення яких є основою для успішного засвоєння студентами навчального матеріалу дисципліни.

Аналіз останніх досліджень і публікацій. Вивченням загальних питань захисту даних, у тому числі за допомогою криптографічних методів займалися І. І. Маракова, А. А. Пєтров, А. І. Рибак, Ю. С. Ямпольський та інші. Вагомий внесок у напрямку висвітлення основних теоретичних понять, завдань і проблем класичної та сучасної криптології зробили М. В. Адаменко [2], А. П. Алферов [3], В. М. Богуш [1], О. В. Вербіцький [4], А. Ю. Зубов [3], А. В. Бабаш, С. Г. Барічєв [5], С. А. Доріченко [6], Н. А. Молдовян [7], А. А. Молдовян [7], А. С. Кузьмін [3], Р. Є. Сєров [5], А. В. Черемушкін [3], Г. П. Шанкін, В. В. Ященко [6] та багато інших.

Основні поняття прикладної криптології розглядали такі науковці як А. В. Аграновский [8], І. Д. Горбенко [9], Т. О. Гріненко, В. К. Задірака, І. М. Коваленко, О. Г. Корченко, Й. У. Мастяниця, О. В. Потій та інші. Розробці термінологічно-навчальних довідників та словників у галузі криптографічного захисту інформаційних ресурсів присвячені дослідження В. М. Богуша [10], В. Г. Кривуци [10], А. М. Кудіна [10], Б. А. Погорєлова [11], В. Н. Сачкова [11] та інших.

Варто зазначити, що значним підґрунтям для наукових досліджень вище вказаних науковців були праці видатних зарубіжних вчених Вітфілда Діффі (Whitfield Diffie), Ральфа Меркла (Ralph Merkle), Рональда Рівеста (Ronald Rivest), Арто Саломаа (Arto Salomaa) [12], Вільяма Фрідмана (William Friedman), Мартіна Хелмана (Martin Hellman), Клода Шенона (Claude Shannon), Брюса Шнайєра (Bruce Schneier) [13].

Аналіз наукових джерел показав, що існують термінологічні суперечності в інтерпретації понять різними авторами. Постійне *розширення предмета досліджень і кола дослідників призводить до появи нових понять та* термінів, які у різних джерелах можуть мати протилежні значення. Також це зумовлено тим, що переважна більшість понять перекладені з іноземної літератури і не мають загальноприйнятих вітчизняних тлумачень.

Метою статті є уточнення понять та термінів для формування однозначної та єдиної термінологічної бази криптології, що є важливою складовою в системі наукових досліджень і в організації навчального процесу підготовки випускників вищого навчального закладу, які спеціалізуються в галузі інформатики.

Виклад основного матеріалу. Переважна більшість науковців притримуються думки, що криптологія – це наука, яка поділяється на два взаємозалежні напрями: криптографію та криптоаналіз. Фундамент криптології як науки у 1949 р. заклала робота американського вченого Клода Шеннона «Теорія зв'язку в секретних системах», у якій фактично вперше було представлено математичну модель шифрів.

У Великому тлумачному словнику сучасної української мови під криптографією розуміється спосіб письма спеціальними умовними знаками – шифром; шифроване письмо, тайнопис [14, с. 587]. Проте, тайнопис дещо ширше поняття, що крім шифрування допускає стеганографічні способи збереження таємниці, тобто такі, при яких повідомлення не перетворюється, а приховується сам факт його передачі чи існування. Відомий американський науковець та криптограф Брюс Шнайєр називає криптографію мистецтвом і наукою забезпечення секретності повідомлень [13, с. 17]. Однак зберігати дані в секреті можна й шляхом заборони або обмеження доступу до них. Більш точне визначення криптографії міститься у словнику термінів з інформаційної безпеки Національного інституту стандартів і технологій США: криптографія – наука про принципи, засоби та методи перетворення даних з метою приховування їх змісту, запобігання несанкціонованого використання або підробки [15, с. 56]. У довіднику з прикладної криптографії говориться, що криптографія є наукою, що вивчає математичні методи, пов'язані з такими функціями захисту даних, як конфіденційність, цілісність та автентичність [16, с. 4]. Проте ці функції часто забезпечуються розмежуванням повноважень користувачів та введенням відповідних блокувань. Український науковець Горбенко І. Д. дає вичерпне визначення: «*криптографія – напрям у криптології, що вивчає основні закономірності, протиріччя, методи, системи та засоби забезпечення конфіденційності, цілісності, дійсності, доступності та*

спостережливості інформації та ресурсів тощо, ґрунтуючись на криптографічних перетвореннях [9, с. 11]».

Запропоновані визначення містять декілька понять, що потребують додаткових пояснень. А саме, забезпечення *конфіденційності* полягає у вирішенні проблеми захисту інформаційних ресурсів від несанкціонованого ознайомлення з їх змістом [10, с. 306]. Залежно від контексту замість терміна «конфіденційні» дані можуть виступати терміни «секретні», «приватні», «обмеженого доступу». *Цілісність* інформаційних ресурсів полягає у гарантуванні неможливості їх несанкціонованої зміни (модифікації) [10, с. 721]. *Дійсність* (*достовірність*) визначається ймовірністю відсутності помилок, властивістю інформаційних ресурсів бути правильно сприйнятими [10, с. 146]. *Доступність* ресурсу полягає у можливості його використання за вимогою користувача, який має відповідні повноваження [10, с. 150]. Під *спостережливістю* мається на увазі властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати їх ідентифікатори в системі з метою запобігання порушення політики безпеки та забезпечення відповідальності за певні дії [10, с. 638].

Кожне *криптографічне перетворення* однозначно визначається ключем (секретним параметром) та описується криптографічним алгоритмом [3, с.58]. Сукупність криптографічних алгоритмів, що використовуються для шифрування називають *шифром* [17, с.14]. Низка вчених, зокрема Брюс Шнайєр, ототожнюють поняття криптографічний алгоритм та шифр, розуміючи під цими поняттями математичну функцію, що використовується для шифрування [13, с.18]. Проте, на нашу думку, *криптографічний алгоритм* є ширшим поняттям, що являє собою набір математичних правил та процедур, який окрім шифрування описує ще й такі види перетворень, як формування та перевірка електронного цифрового підпису, обчислення хеш-значень, спеціальних криптографічних контрольних сум, створення імітовставки тощо.

Звичайно, історично основним завданням криптографії являється *шифрування даних*, що складається з процесів зашифрування або розшифрування [17, с. 9]. Також, у вузькому значенні, термін «шифрування» використовується як синонім до терміну «зашифрування». *Зашифрування даних* – процес перетворення відкритого тексту до виду, незрозумілого несанкціонованому користувачеві [10, с. 222]. *Відкритий текст* являє собою вихідне повідомлення, що підлягає зашифруванню [13, с. 17]. У сучасній комп'ютерній криптографії це повідомлення найчастіше являє собою двійкові дані. Зауважимо, що за визначеннями, поданими у деяких джерелах, під відкритим текстом розуміються дані з доступним семантичним змістом [17, с. 9]. Однак, це не завжди так, наприклад, при багаторазовому шифруванні, попередньо зашифрований текст може бути відкритим по відношенню до наступного кроку алгоритму шифрування. Результатом зашифрування відкритого тексту є *шифротекст* [13, с. 17], що також називають *криптотекстом* або *криптограмою*. При чому, шифротекст за розмірами не завжди може співпадати з відкритим.

Як зазначалося вище, шифрування відбувається за правилами шифру (алгоритму шифрування) та з використанням криптографічного ключа або просто ключа, що зазвичай являє собою деяку послідовність символів. Російський вчений Доріченко С. А. під ключем розуміє змінний елемент шифру, що застосовується для шифрування конкретного повідомлення [6, с.18]. Найчастіше в науковій літературі зустрічається наступне визначення: *ключ – конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму* [10, с. 270; 17, с. 9; 7, с. 10; 5, с. 10]. На нашу думку, для уточнення варто додати, що ключ – це *секретний* змінний елемент або *секретний* стан параметрів шифру, оскільки секретність є найважливішою вимогою, що забезпечує неможливість відновлення відкритого тексту по шифротексту. В криптографії існує загальноприйняте правило, яке сформулював голандський вчений Огюст Керкхоф (Auguste Kerckhoffs): стійкість зашифрованого повідомлення забезпечується в першу чергу ключем. Тобто передбачається ймовірність того,

що сам алгоритм шифрування, шифротекст або якась його частина є відомими зловмиснику та доступні для вивчення.

Зауважимо, що варто відрізняти поняття ключ і пароль. Пароль як і ключ є секретною послідовністю символів деякого алфавіту, однак використовується не для шифрування, а для аутентифікації суб'єктів [10, с. 426].

Вважається, що зашифроване повідомлення передається від відправника до отримувача по незахищеним каналам зв'язку, в той час, коли ключ має передаватися цілком надійним способом. Учасники обміну повідомленнями можуть завчасно домовитися про використовувані алгоритми шифрування, ключі тощо, наприклад при особистій зустрічі. Знаючи шифр та ключ, отримувач виконує зворотний процес перетворення шифротексту у відкритий текст, що називається *розшифруванням* або *дешифруванням* [5, с. 9]. Обидва ці терміни з точки зору української мови являються синонімами [14, с. 291]. Проте, в роботах з криптології останніх десятиліть часто ці слова розрізняють. При чому, під «розшифруванням» найчастіше розуміють процес перетворення шифротексту у відкритий текст за допомогою ключа, а під «дешифруванням» – процес перетворення шифротексту у відкритий текст без знання [3, 7, 8]. Такі понятійні розбіжності можуть мати негативний вплив на ефективність вивчення студентами подальших тем курсу «Криптологія». Тому ми пропонуємо терміни «розшифрування» та «дешифрування» вважати рівнозначними та у подальшому розуміти під ними процес обернений до шифрування, тобто перетворення шифрованого повідомлення до початкової інформації (відкритого тексту) за допомогою певних правил шифру та відомого ключа.

Також вживання в криптології термінів «код» та «кодування» як синонімів до «шифру» та «шифрування» відповідно, на нашу думку, є помилковим. Код – це усталене правило для заміни одиниць інформації (букв, слів, цілих фраз) певними символами. Наприклад, ASCII код згідно з яким символ кодується двійковою послідовністю. Коди, які вивчає математична теорія кодування, застосовуються з метою дещо протилежною до криптографічної. Повідомлення шифрується для того, щоб воно стало незрозумілим, а кодується для того, щоб бути зрозумілим навіть після часткового спотворення через природні перешкоди у каналі зв'язку. Ці два терміни варто чітко розмежовувати тому, що на практиці одна й та ж інформація може підлягати обом діям – у типовій ситуації текст закодовують у двійкову послідовність, а потім її шифрують, а отриманий криптотекст перед відправленням кодують за допомогою коду, який дозволить виправити помилки після передачі. Справа в тому, що за останні десятиліття сформувалася теорія кодування – великий науковий напрям, який розробляє і вивчає методи захисту інформації від випадкових спотворень в каналах зв'язку [4, с. 16]. В даний час, терміни кодування і шифрування застосовуються для позначення самостійних наукових напрямів і вживати їх як синоніми неприпустимо.

Центральним поняттям у криптографії є поняття криптографічної системи або криптосистеми. Ряд дослідників розглядають криптосистему аналогічно до поняття шифру, як сукупність алгоритмів, що використовуються для зашифрування та розшифрування [7, с. 14; 5, с. 9; 8, с. 13; 4, с. 12]. Проте, проаналізувавши праці вчених Брюса Шнайєра, Арто Саломаа та інших, можна зробити висновок, що сам по собі опис криптографічних алгоритмів не є криптосистемою. Лише доповнена усіма можливими відкритими текстами, шифротекстами і ключами, система може назватися криптографічною [13, с. 18; 12, с. 12]. Отже, *криптосистема – це система криптографічного перетворення даних, що містить у собі п'ять компонентів: множину відкритих текстів, множину шифротекстів, множину ключів, сімейство зашифровуючих та розшифровуючих перетворень* [10, с. 312]. Фахівець, який займається розробкою криптосистем називається *криптографом* [10, с. 311].

У процесі навчання криптології студент повинен не лише знати суть кожного поняття, вміти чітко його формулювати, а також встановлювати його зв'язок з іншими поняттями. Наприклад, відношення між описаними вище термінами можна представити у вигляді схеми обміну секретними повідомленнями (рис. 1).

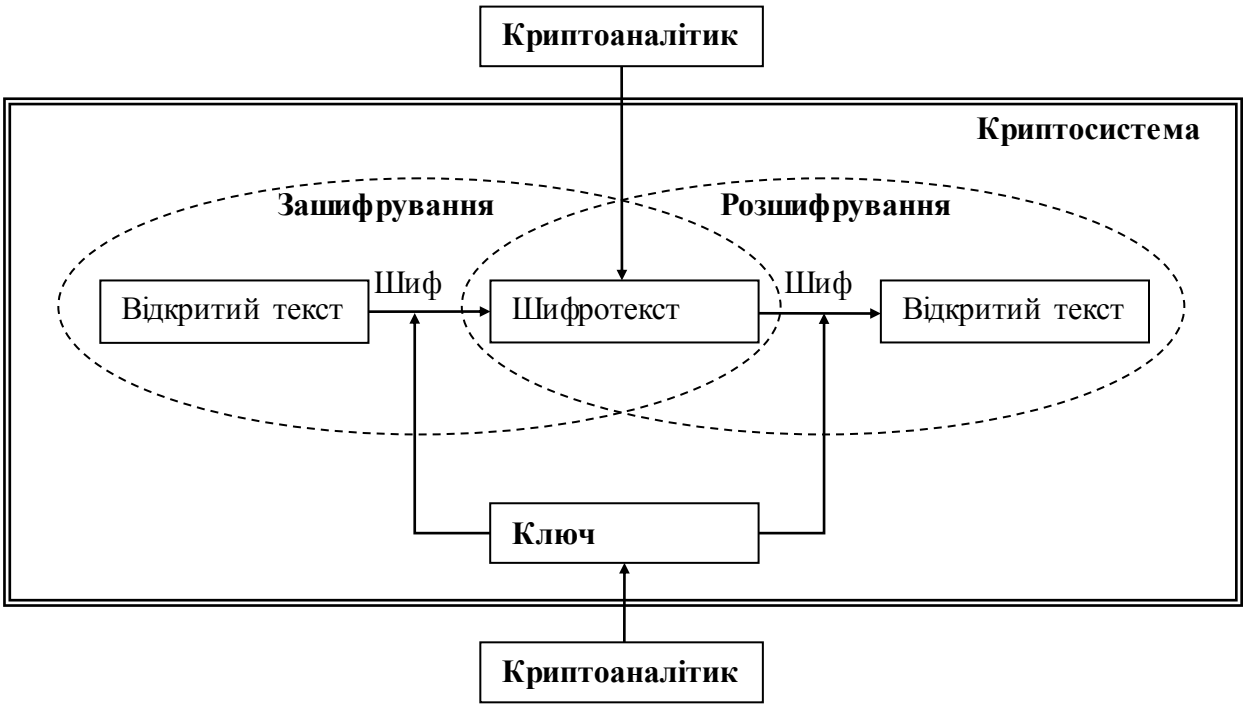

Рис. 1. Схема обміну секретними повідомленнями

Невід'ємною складовою понятійно-термінологічного апарату і разом з тим одним з фундаментальних понять криптології є криптостійкість. Згідно з визначанням, запропонованим у словнику криптографічних термінів Погорєлова Б. А., *криптостійкість – це властивість криптосистеми протидіяти атакам супротивника, спрямованим на отримання секретного ключа або відкритого повідомлення* [11, с. 69]. На думку Доріченко С. А стійкість криптосистеми визначається її здатністю протидіяти усім можливим атакам [6, с. 20]. Під *атакою на криптосистему* розуміється спроба порушення безпеки конкретної реалізації криптосистеми [11, с. 19]. Вдалу криптоатаку називають *зламом* [5, с. 12]. Криптостійкість часто вимірюється кількістю операцій, необхідних для перебору всіх можливих ключів, або інтервалом часу, необхідного для зламу. Вона оцінюється у процесі проведення криптографічного аналізу, який виконується, з одного боку, розроблювачами й законними користувачами криптосистеми з метою отримання оцінки її стійкості, а з іншого боку – супротивником з метою підготовки й реалізації атаки на криптосистему.

Термін «криптоаналіз» був запропонований американським криптографом Вільямом Фрідманом у 1920 році. Брюс Шнайєр під криптоаналізом розуміє мистецтвом і науку зламу шифротексту [13, с. 17]. Проте, якими методами відбувається злам не уточнюється. У словнику термінів з інформаційної безпеки Національного інституту стандартів і технологій США говориться, що криптоаналіз – це наука про математичні методи порушення безпеки криптографічних систем [15, с. 52]. Найбільш повне трактування дає Горбенко І. Д., який зазначає, що «*криптоаналіз є напрямом у криптології, що вивчає основні закономірності, протиріччя, методи та засоби аналізу криптографічних систем, ґрунтуючись на їх вхідних та вихідних даних, у тому числі можливо на частині ключових даних, що здійснюється з метою визначення спеціальних (ключових) даних і значущої інформації, які можуть бути використані для порушення конфіденційності, цілісності, справжності, доступності, неспростовності (спостережливості) інформації та ресурсів тощо* [9, с. 11]» .

Фахівець, який займається розробкою методів криптоаналізу називається *криптоаналітиком* [10, с. 311]. Синонімами є терміни зловмисник, порушник, супротивник. Основна діяльність криптоаналітика спрямована на перетворення шифротексту у відкритий текст без знання ключа або отримання самого секретного ключа (рис. 1).

Дослідники вважають, що не існує єдиної криптосистеми, яка б підходила для усіх випадків. Вибір способу шифрування залежить: по-перше, від особливостей інформаційних ресурсів, їх цінності та можливостей власників по захисту даних; по-друге, від обсягів і необхідної швидкості передачі шифрованого повідомлення; по-третє, від проміжку часу необхідного для збереження даних в таємниці. Також варто враховувати і можливості супротивника, від якого захищається дана інформація. Криптоаналіз еволюціонує разом із розвитком криптографії: на зміну класичним криптосистемам приходять нові більш досконалі.

Велике значення у підготовці майбутніх фахівців з інформатики має питання класифікації криптосистем, що є підґрунтям для подальшого вивчення більш складних розділів науки. Криптографічні системи класифікуються за різними ознаками (рис.2). За особливостями ключа розрізняють симетричні та асиметричні криптосистеми. У *симетричних* криптосистемах для зашифрування та розшифрування використовується один і той самий ключ [5, с. 15]. Тому їх ще називають *одноключовими* або *із закритим ключем*. Основними перевагами цих криптосистем є висока швидкість роботи, достатня вивченість, простота реалізації. Значним недолікам є необхідність реалізації абсолютно захищеного каналу зв'язку для передачі даних, що породжує проблему обміну та зберігання ключів. Оскільки компрометація ключа несе в собі загрозу безпеці всієї криптосистеми. Крім того, при використанні криптосистем із закритим ключем виникає проблема підтвердження істинності даних. Одним із найефективніших способів подолання цих недоліків стало винайдення у 1976 р. американськими математиками Вітфілдом Діффі, Мартіном Хелманом, а також Ральфом Мерклом, *асиметричних криптосистем*, у яких використовуються два ключі – відкритий (публічний) і закритий (секретний), які математично пов'язані один з одним. Повідомлення зашифровується за допомогою відкритого ключа, що доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу [5, с.62]. Асиметричні криптосистеми ще називають *двоключові* або *із відкритим ключем*. Криптостійкість таких систем ґрунтується на односторонніх функціях, що легко обчислюються в прямому напрямку й утворюють математичну проблему надзвичайної обчислювальної складності при способі розв'язку оберненої задачі. Проте, криптосистем з відкритим ключем мають відносно малу швидкість роботи. Тому широкого застосування сьогодні набуває *гібридна криптосистема* – це криптосистема, в якій розподіл ключів здійснюється за допомогою двоключових криптоалгоритмів, а процес шифрування інформації – за допомогою одноключових [7, с.9]. Гібридні криптосистеми поєднують в собі зручність розподілу секретних ключів та високу швидкість шифрування.

В свою чергу, залежно від виду криптографічного перетворення криптосистеми можуть містити шифри перестановки та підстановки. Останні називають ще шифрами заміни. *Шифр підстановки* (*заміни*) – це шифр, у якому кожен символ відкритого тексту у шифротексті замінюється іншим символом [13, с. 23]. Брюс Шнайєр виділяє чотири типи шифрів підстановки: проста підстановка, або моноалфавітна – це шифр, де кожен символ відкритого тексту замінюється відповідним символом шифротексту [13, с. 23], при чому, конкретній літері відкритого повідомлення відповідає єдина, завжди одна і та сама літера шифротексту; однозвучний шифр підстановки схожий на простий шифр підстановки за винятком того, що один символ відкритого тексту символ відкритого тексту замінюється на один з декількох можливих символів шифротексту [13, с. 23]; поліграмний шифр підстановки – це шифр, який блоки символів шифрує по групах, наприклад, біграма – це група з двох символів, триграма – з трьох символів і т.д. [13, с. 23]; поліалфавітна підстановка складається з декількох простих шифрів підстановки [13, с. 23], тобто одна і та сама літера відкритого тексту може бути замінена кожен раз по різному (відбувається циклічне застосування декількох моноалфавітних шифрів).

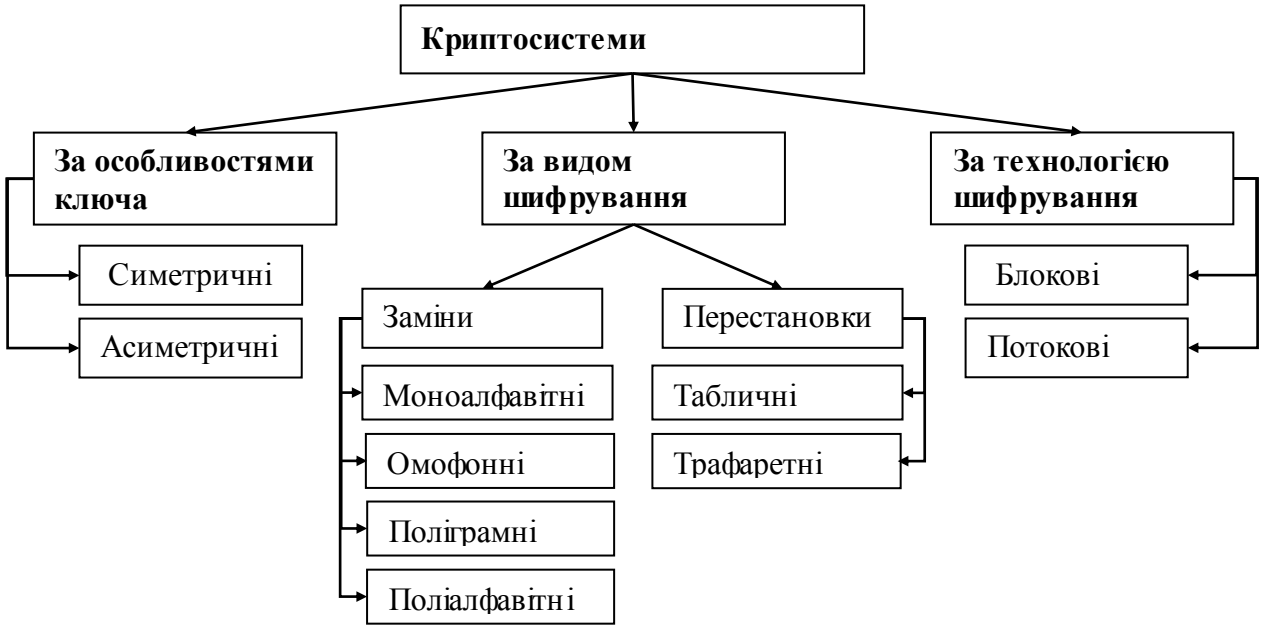

Рис. 2. Класифікація криптосистем

Шифром перестановки називається шифр, у якому символи повідомлення переставляються місцями безпосередньо у відкритому тексті за певним правилом, що залежить від ключа [8, с. 21]. Не зважаючи на різноманіття шифрів даного виду, в криптографічній літературі не запропоновано їх чіткої класифікації. Найчастіше перестановка виконується за допомогою таблиці, комірки якої спочатку заповнюють відкритим текстом в деякому порядку, а потім шифротекст зчитують відповідно до заздалегідь визначеного алгоритму [2, с. 209]. В історичному плані також цікавим є трафаретний шифр, у якому для шифрування використовувався трафарет з прорізаними комірками. Приклавши трафарет до аркушу паперу, в прорізаних комірках записували повідомлення, а решту аркуша заповнювали довільними символами [2, с. 222]. Зазначимо, що навіть дуже складні сучасні криптосистеми в якості типових компонентів використовують прості шифри заміни та перестановки, або їх поєднання.

За технологією шифрування розрізняють блокові та потокові криптосистеми. *Блокові шифри* здійснюють шифрування блоків фіксованої довжини, що складаються з послідовності символів відкритого тексту [3, с. 59]. *Потокові шифри* здійснюють шифрування окремих символів відкритого тексту [3, с. 59].

З часом задачі криптології значно розширилися та вийшли за межі шифрування повідомлень. На сьогоднішній день вони також включають розробку систем електронного цифрового підпису, імітозахисту, протоколів автентифікації та ідентифікації користувачів тощо. Коротко розглянемо деякі з них. Для захисту від підробки, перевірки цілісності даних та достовірності джерела повідомлення використовують *електронний цифровий підпис (ЕЦП)* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача [18].

Як правило, до процесу накладання цифрового підпису повідомлення підлягає хешуванню. *Хешуванням* називається процес обчислення значення хеш-функції [7, с. 13]. *Хеш-функція* являє собою функцію, математичну або іншу, що отримує на вхід рядок змінної довжини і перетворює його в рядок фіксованої, зазвичай меншої, довжини [5, с. 37].

У випадку, коли учасники не довіряють один одному, то для обміну повідомленнями використовується схема електронного цифрового підпису. Якщо ж учасники інформаційного обміну довіряють один одному і захищаються від несанкціонованої модифікації та нав'язування фальшивого повідомлення, то процес передачі даних будується на основі

імітозахисту, у ході якого обчислюється код достовірності повідомлення (MAC-код) або іміговставка, що по суті являє собою хеш-функцію з додаванням секретного ключа. Отже, *імітовставка* – блок даних фіксованої довжини, що одержується із відкритого тексту і ключа, однозначно відповідний даному відкритому тексту [10, с. 236].

Висновки. Понятійно-термінологічний апарат криптології уточнюється і вдосконалюється в процесі розвитку двох тісно пов'язаних між собою наукових напрямів: криптографії та криптоаналізу. Одним із основних завдань, що мають бути вирішені у процесі навчання цієї дисципліни, є забезпечення ґрунтовного вивчення студентами теоретичних основ, що в подальшому сприятиме формуванню професійних компетентностей, необхідних для розуміння загальних принципів побудови криптографічних систем. Однією з особливостей науки про захист даних є використання термінів з англомовних джерел, які можуть мати не завжди коректний переклад і викликати суперечності. Наголосимо, що у процесі навчання криптології варто чіткого розмежовувати такі фундаментальні поняття як «шифр», «криптографічний алгоритм» та «криптосистема». В той самий час, не бажано надавати протилежні тлумачення таким тотожним термінам, як «розшифрування» та «дешифрування». Однак, зауважимо, що понятійно-термінологічний апарат криптології не є остаточно сформованим та продовжує поповнюватися з огляду на постійний розвиток цієї науки та розширення кола її завдань, у чому і полягатиме подальше дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В. М. Криптографічні застосування елементарної теорії чисел/ В. М. Богуш, В. А. Мухачов // Навчальний посібник – К.: ДУІКТ, 2006. – 126 с.
2. Адаменко М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко – М.: ДМК Пресс, 2012. – 256 с.
3. Основы криптографии: [учебное пособие. 2-е изд., исп. и доп.] / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М: Гелиос АРВ, 2002. – 480 с.
4. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький – Л.: ВНТЛ, 1998. – 247 с.
5. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, Р. Е Серов – М.: Горячая линия – Телеком, 2002. – с. 152.
6. Дориченко С. А. 25 этюдов о шифрах: Популярно о современной криптографии / С. А. Дориченко, В. В. Ященко. – М.: Теис, 1994. –72 с.
7. Молдовян Н. А. Введение в криптосистемы с открытым ключом./ Н. А. Молдовян, А. А. Молдовян. – С.-Пб.: БХВ Петербург, 2005. – 288 с.
8. Аграновский А. В. Практическая криптография: алгоритмы и их програмирование / Аграновский А. В., Р. А. Хади. – М.: СОЛОН-Пресс, 2009. –256 с.
9. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / Горбенко І. Д., Горбенко Ю. І.; Харк. нац. ун-т радіоелектрон., Приват. АТ «Ін-т інформ. Технологій». – Х.: Форт, 2012. – 868 с.
10. Богуш В. М. Інформаційна безпека: Термінологічний навчальний довідник/ В. Г. Кривуца, А. М. Кудін // За ред. Кривуци В.Г. – К.: ООО «Д.В.К.» 2004. – 508 с.
11. Погорелов Б. А. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. – М.: МЦНМО, 2006. – 94 с.
12. Саломаа А. Криптография с открытым ключом. / Арто Саломаа – М.: Мир, 1995. – 318 с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М.: Триумф, 2002. – 816 с.
14. Великий тлумачний словник сучасної української мови (з дод. і доп.) / Уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2005. – 1728 с.
15. Glossary of Key Information Security Terms [Електронний ресурс] / Editor Richard Kissel. Режим доступу: – http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, 25.03.2014.
16. Handbook of Applied Cryptography [Електронний ресурс] / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Режим доступу: – http://cacr.uwaterloo.ca/hac/about/chap1.pdf, 25.03.2014.
17. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. – Офіц. вид. – К.: ДСТСЗІ СБ України, 1999. – 30 с.

(Нормативний документ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України).
18. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/852-15, 25.03.2014.

Стаття надійшла до редакції 24.03.14

Zagatska N.
Zhytomyr Ivan Franko State University, Zhytomyr, Ukraine

THE FOUNDATIONS OF CONCEPTUAL AND TERMINOLOGICAL APPARATUS OF CRYPTOLOGY

Formation of cryptology as a science has necessitated the formation need of its own conceptual apparatus of the discipline with its inherent characteristics. The problem is the lack of up to date generally accepted interpretation of concepts and terms which studying is the basis for successful mastering the discipline's educational material by the students.

One of the main tasks to be solved in the studying process of this discipline is to provide a careful examination of the theoretical foundations by students that will facilitate the formation of professional competencies necessary to understand the general principles of cryptographic systems.

The article studies the conceptual and terminological cryptology apparatus. The comparative analysis of the science's concept on the basis of national and foreign professional sources, explanatory and specialized dictionaries, legal and legislative acts of Ukraine in the field of cryptographic data protection has been hold. The article describes the fundamental and derivative terms due to their structural and logical connections. The classification of cryptosystems is proposed: key features, type and encrypting technology. An attempt to clarify the common terminology of the science is made that will contribute the future specialists in computer science to master it.

Keywords: cryptology, cryptographic algorithm, ciphering, key, digital signature, hash function, message authentication code.

Загацкая Н. А.
Житомирский государственный университета имени Ивана Франка, Житомир, Украина

ОСНОВЫ ПОНЯТИЙНО-ТЕРМИНОЛОГИЧЕСКОГО АППАРАТА КРИПТОЛОГИИ

Становление криптологии как науки обусловило необходимость формирования собственного понятийного аппарата этой дисциплины с присущей ему спецификой. Проблема заключается в отсутствии до настоящего времени общепринятых толкований, понятий и терминов, изучение которых является основой для успешного усвоения студентами учебного материала дисциплины.

Одной из основных задач, которые должны быть решены в процессе обучения этой дисциплине, является обеспечение тщательного изучения студентами теоретических основ, что в дальнейшем будет способствовать формированию профессиональных компететностей, необходимых для понимания общих принципов построения криптографических систем.

Статья посвящена исследованию понятийно-терминологического аппарата криптологии. Проведен сравнительный анализ понятий этой науки на основе отечественных и зарубежных профессиональных источников, толковых и специализированных словарей, нормативно-правых и законодательных актов Украины в области криптографической защиты данных. В статье описываются фундаментальные и производные термины учитывая их структурно-логические связи. Предложена классификация криптосистем: по

особенностям ключа, по виду и по технологии шифрования. Делается попытка уточнения единой терминологии науки, что будет способствовать повышению уровня овладения ею будущими специалистами по информатике.

Ключевые слова: криптология, криптографический алгоритм, шифрование, ключ, электронная цифровая подпись, хэш-функция, имитовставка.