DOI: http://www.doi.org/10.21272/legalhorizons.2018.i11.p26

# РОЗВИТОК ЗАХИСТУ ІНФОРМАЦІЇ У СВІТІ – ІСТОРИЧНИЙ АСПЕКТ

***Риженко Олег Сергійович,***
*Аспірант кафедри Адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету*

У статті проведений аналіз способів, методів та засобів захисту інформації у світі у різні часи та епохи існування людства. Дослідження вказаного питання має актуальний характер з метою створення повного, об'єктивного та всебічного уявлення про захист інформації у різні часові періоди існування людства. В умовах сьогодення питання захисту інформації є досить актуальними для звичайних користувачів мобільних телефонів, комп'ютерів, працівників бізнесу, юридичних осіб приватного чи публічного права, державних службовців та працівників правоохоронних органів. Питаннями захисту інформації людство переймалося з давніх часів, як це робить і до цього часу.

Історія криптографії налічує кілька тисяч років. Перші надійні способи передачі інформації з'являлися завдяки військовим конфліктам. Становлення розгалуженого державного апарату в арабському світі сприяло поширенню криптографії серед державних діячів, а також появі перших наукових праць по криптоаналізу. З розвитком дипломатичних відносин, розвиваються і нові способи захисту інформації. Світові війни XX століття стверджують в черговий раз необхідність шифрування інформації. Розвиток електронних, а потім і комп'ютерних технологій революційно змінює принципи будування систем захисту інформації. Бурхливий технічний прогрес кінця XX століття сприяє широкій інформатизації суспільства. Інформація стала досить цінною, що обумовлює подальші пошуки більш досконалих систем захисту інформації не тільки державної, а й пересічних громадян.

Проведено аналіз відомих історичних способів захисту інформації у світі від передачі інформації примітивними захищеними способами, які не потребували великих зусиль для їх розшифрування, ієрогліфами, зміненими, спеціально вигаданими шрифтами до захисту інформації за допомогою шифрування ймовірностей, квантової криптографії та ін. Розвиток квантової фізики розкриває потенційні горизонти розвитку криптографії. Розширюються сфери застосування криптографії.

Ключові слова: інформація, захист інформації, криптографія, криптоаналіз, історія захисту інформації, шифрування, розшифрування, шифр, історія криптографії.

**Ryzhenko O.S., Development of information security in the world - a historical aspect.** The article analyzes methods, methods and means of protecting information in the world at different times and periods of human existence. The study of this issue is relevant in order to create a complete, objective and comprehensive view of the protection of information in different time periods of human existence. In today's context, the issue of information security is very relevant for ordinary users of mobile phones, computers, business people, private or public law entities, civil servants and law enforcement officers. With the protection of information, mankind has been concerned with ancient times, as it does to this time.

The history of cryptography is several thousand years old. The first reliable means of transmitting information came from military conflicts. The formation of a ramified state apparatus in the Arab world contributed to the spread of cryptography among statesmen, as well as the emergence of the first scientific papers on cryptanalysis. With the development of diplomatic relations, new ways of protecting

information are developing. World wars of the twentieth century claim once again the need for encryption of information. The development of electronic, and then computer technology revolutionizes the principles of building information security systems. The rapid technological progress of the late twentieth century contributes to the wide informatization of society. Information has become rather valuable, which results in further search for more perfect information security systems not only for state but also for ordinary citizens.

The analysis of known historical methods of protecting information in the world from the transmission of information by primitive, protected methods that did not require much effort to decrypt them, hieroglyphs, modified, specially fictitious fonts to protect information through probability encryption, quantum cryptography, and others. The development of quantum physics reveals the potential horizons of the development of cryptography. The scope of application of cryptography is expanding.

Key words: information, information protection, cryptography, cryptanalysis, history of information security, encryption, decryption, cipher, history of cryptography.

В умовах сьогодення перед кожним постає актуальним питання захисту інформації, будь це звичайний користувач мобільного телефону, комп'ютеру, працівник бізнесу, юридичної особи приватного чи публічного права, державний службовець чи працівник правоохоронних органів. Особи установлюючи пароль на телефон, комп'ютер, надаючи документу гриф «Для службового користування» або секретності бажають захистити інформацію – персональні дані, комерційна таємниця, державна таємниця. Захищена інформація стає відомою лише обмеженому колу осіб.

Кожного дня практично всі люди зустрічаються з різними видами та способами захисту інформації, але більшість із них навіть не здогадується з чого все починалось.

На сьогоднішній день найдавнішим свідченням захисту інформації є ієрогліфи Стародавнього Єгипту виявлені на руїнах стародавніх міст, стінах пірамід та стародавніх папірусах, вік яких датується періодом з 2667 по

2648 р.р. до н.е. [1],[2]. За допомогою ієрогліфів стародавні єгиптяни здійснювали документування інформації про життя фараона, його роль у суспільстві, збудовані храми для поклоніння Богам та життя пересічних жителів Стародавнього Єгипту. До цього часу не розроблено єдиного трактування ієрогліфів. Вчені-єгиптологи у XX столітті намагалися класифікувати ієрогліфи, так наприклад серед європейських дослідників спроби прочитати ієрогліфічні тексти робили Беканус у 16 столітті та Атанасіус Кірхер у 17 столітті, однак вони не здобули успіху. Відкриття розетського каменю наполеонівськими військами, дало можливість справжнього прориву. Над написаним на ньому текстом працювали Сільвестр де Сасі, Йоган Давид Акерблад та Томас Янг. Врешті Жан-Франсуа Шампольйон у 1820-их роках зумів добитися повного розшифрування. [3]

Єдиної класифікації давньоєгипетських ієрогліфів до цього часу залишається відкритою. Одним із перших здійснив спробу каталогізувати єгипетські ієрогліфи у 1920 році англійський єгиптолог і філолог

Уолліс Баджоднім в «Словнику єгипетських ієрогліфів» [4]. Ним класифікація здійснена на зовнішніх ознаках цих знаків. У 1927 році, також ґрунтуючись на поділі ієрогліфів за зовнішньою ознакою, систематизував інший англійський єгиптолог і лінгвіст - А. Х. Гардінер, у своїй «Єгипетської граматиці» [5], який поділив їх на групи, що позначаються латинськими літерами, а всередині груп їм присвоєні номери. Класифікатор з «Єгипетської граматики» А.Х. Гардінера став загальноприйнятим, а ієрогліфи які відкривалися додавалися до запропонованих ним груп з присвоєнням додаткових літерних значень вже після цифр. Але всі ці спроби щодо розшифрування ієрогліфів Стародавнього Єгипту не можна вважати вдалими оскільки вченими-археологами виявляються все нові і нові ієрогліфи, достовірне значення яких знають лише ті, яких немає в світі живих уже не одне тисячоліття.

Одними із відомих прикладів шифрування є атбаш - простий шифр підстановки для івриту, заснованим на пересуванні алфавіту на всю довжину. Прикладом використання вказаного шифру є в Біблії, де під ім'ям Шешах зашифровано ім'я царя Вавилона (Єр. 25:26) [6]. Мету вказаного шифрування до цього часу не відомо.

До спроб захисту інформації вдавали і в Стародавній Спарті за допомогою так званого скитала – спосіб шифрування з допомогою шкіряної смужки або смужки паперу та предмета циліндричної форми. Стрічка намотувалась по спіралі на циліндричний предмет, а текст наносився по довжині циліндра, якщо рядок

заповнювався, то повідомлення продовжували писати на наступному рядку до тих пір поки не закінчувався текст, або обсяг циліндра. Після нанесення тексту циліндр виймався, а смужка з текстом передавалася адресату. З метою прочитання тексту адресат повинен був використати циліндр того ж діаметру, що при написанні.

Перевагою зазначеного шифру є простота і відсутність помилок. У той же час, він може бути легко розшифрований. Спосіб дешифрування запропонував Едгар Аллан По в роботі «A Few Words on Secret Writing» [7], за допомогою використання конусу, що має змінний діаметр і переміщенням пергаменту з повідомленням по його довжині до тих пір, поки текст не почне читатися - таким чином розшифрується ключ - діаметр скиталу.

Також, ще один спосіб захисту інформації вигадав у IV столітті до н.е. Еней Тактик – полководець Стародавньої Греції, політичний діяч та автор трактатів. Про життя Тактика на даний час відомості практично відсутні, але він залишається і залишатиметься відомим завдяки своїм працям такими, як: «Про витримання облоги», «Про військове мистецтво», «Військова доктрина», «Засоби поставити ворогу перешкоди», «Збір коштів», «Запобіжні заходи проти зненацьких атак», «Військові красномовства», «Правила застереження, заохочення і мотивація команди, загальної тактики» [8].

Тактик запропонував захищати інформацію за допомогою диска з отворами та ниткою. Даний диск має отвори по зовнішньому діаметру, їх кількість відповідає кількості букв в алфавіті, в центрі прикріплена котушка з ниткою. З метою шифрування інформації нитка протягувалася в отвори відповідних букв. Щоб розшифрувати повідомлення, отримувачу, необхідно було витягувати нитку по черзі з кожного твору, отриманий текст мав дзеркальне відображення, його необхідно було читати з кінця. [9].

Єнеєм Тактиком запропоновано ще один спосіб захисту інформації – книжний шифр. Суть вказаного способу полягає в передачі інформації за допомогою ледь помітних позначок в тексті зроблених поруч з буквами. Для книжкового шифру використовується будь-який фрагмент тексту. Сам шифр складається з точного зазначення номеру рядка і номера букви в рядку. За допомогою даного шифру одна і та ж буква могла отримувати кілька позначень, що збільшувало надійність шифру. [10].

Ще одним прикладом є квадрат Полібія, його ще називають шаховою дошкою Полібія. Зазначений спосіб захисту інформації являє собою заміну кожної літери нижчестоящою буквою в квадраті, або парою координатних чисел. Відомо, що даним способом шифрування інформації користувався Цезар для листування з генералами. Вказаний спосіб, як і атбаш, шифр зсуву теж є шифром підстановки, в якому кожен символ замінюється іншим символом того ж алфавіту, що знаходяться на деякій відстані від замінюваного символу. Неписемність противника, на час використання квадрату Полібія, була запорукою його успішності [11: 28].

Араби перші відкрили і описали метод криптоаналізу, тому арабська цивілізація мала великий вплив на розвиток криптографії (докладний переклад з грецької – приховано писати). [12]. Ісламська держава, яка перебувала в стані стрімкого розвитку, потребувала добре налагодженої системи державного управління. Тогочасні державні управлінці покладалися на налагоджену систему обміну повідомленнями, безпеку якої забезпечували шифруванням. На початку розвитку державності чиновники користувалися шифро-алфавітом на зразок способів захисту інформації перелічених вище. Однак внесок арабів складається не тільки в широкому використанні шифро-алфавіту, але і в створенні криптоаналізу (дешифрування повідомлення без знання ключа). Високі досягнення в криптології пояснюються високим рівнем розвитку в області математики і лінгвістики. Далеко не останнім фактором розвитку криптології в арабському світі стала релігія [11: 20]. Ісламські релігієзнавці, які активно досліджували Хадиси (релігійні письмена про слова і дії пророка Мухаммада) на предмет часто вживаних слів. Головним відкриттям стало те, що деякі літери в арабській мові зустрічаються частіше інших. Це відкриття привело до прориву в криптографії. Пізніше арабський вчений Аль-Кінді вперше описав криптосистему на основі частотного аналізу в праці «Рукопис по дешифруванню криптографічних повідомлень».

В Європі криптографія почала використовуватись в епоху Відродження. До цього часу способами захисту інформації були: написання тексту в зворотному порядку, по вертикалі, голосні букви замінялися крапками, використовували іноземні алфавіти, кожна буква відкритого тексту замінялася наступною. На той час криптографія відносилась до чорної магії.

Одним із яскравих прикладів захисту інформації епохи Відродження є Манускрипт Войнича, датований першою половиною XV століття та написаний невідомим автором та невідомою мовою. До цього часу вказаний Манускрипт не розшифрований.

З появою в Європі, в XVI столітті, перших дипломатів виникла необхідність захисту інформації. Шифри стали застосовуватися не лише представниками влади, церкви, але і вченими для захисту своїх наукових відкриттів. «Стегано-графія розвивалася як метод шифрування, придатний для політики і військової справи. Недарма ж вона зароджується разом з початком конфліктів між національними державами, а її розквіт припадає на період великих абсолютистських монархій» [13]. Починаючи приблизно з 1400 до 1850 років в шифрувальній практиці домінували системи, які були наполовину кодом і наполовину шифром [14].

В книзі Чикко Сімонет, датованої XIV століттям, описано принцип лозунгово шифру. У XV столітті вийшла робота Габріеля де Лавінда «Трактат про шифри», в якій описано спосіб захисту інформації – шифр пропорційної заміни. Даний спосіб забезпечує заміну букв декількома символами, пропорційно частотності букв в початковому тексті [15].

У 1466 році з'являється «Трактат про шифри» Леона Альберті. В ньому розглядається напівалфавітний шифр власної розробки, реалізований у вигляді шифрувального диска, де для захисту інформації використовувалося два окремих алфавіту. Альберті вперше засновував свої дослідження на принципі комбінаторики [16].

Проривом у розвитку захисту інформації є публікація у 1518 році в Німеччині книги «Поліграфія», автором якої є Йоганнеса Трітемія. У книзі описано кілька способів захисту інформації, один з яких стає основою для розвитку ідеї напівалфавітной заміни. Послідовником Трітемії є Джовані Белазо.

Д. Белазо, випустивши в 1533 році книгу «Шифр сеньйора Белазо», запропонував до використання пароль – слово або група слів, що записуються над відкритим текстом, а кожен символ паролю означав номер замінної букви. Даний спосіб отримав назву «шифр Віженера» на ім'я свого засновника [17]. Посол XVI століття Блейс де Віжінера, в написав книгу «Трактат про шифри», в якій запропонував використовувати для шифрування 26 алфавітів, а порядок використання шифру визначався знанням паролю. Схожий принцип був в подальшому застосований Томасом Джефферсоном.

Першим професійним криптоаналітиків був Антуан Россиньоло, що служив при Людовіку XIV. Саме Россиньоло першим сформулював концепцію «тимчасової стійкості шифрів». Россиньоло винайшов шифр, який назвав «великим» і стійкість якого була безсумнівна, аж до кінця XIX століття, поки Етьєн Базері не зламати його [16]. Найважливішим нововведенням в криптографії стало винайдення роторних шифрувальних систем, які дуже спрощували використання напівалфавітних шифрів. Першопрохідцем був Томас Джефферсон, який створив в 1790 році дисковий шифр. Його пристрій дозволив автоматизувати процес шифрування [18].

Винахід телеграфу суттєво вплинув на способи здійснення захисту інформації. Більшість колишніх способів захисту інформації стали несумісними з принципами роботи телеграфу. У 1854 році британськими військами почали використовувати шифр Плейфера, в снові якого лежить шифр біграмм – пар символів замість одиночних символів. Шифр Плейфера залишався актуальним до початку Другої світової війни [19].

Поштовхом до розвитку нових способів захисту інформації стала Перша світова війна.

З 20-х років XX століття стала активно використовуватися «Енігма» шифрувальна машина роторного типу, розроблена Едвардом Хеберном і згодом вдосконалена Артуром Кирхом. Найбільшого поширення набула в Німеччині під час Другої світової війни. Алан Тьюринг вніс великий вклад в дешифрування перехоплених повідомлень і в створення електронно-механічної машини Bombe [20]. Робота Клода Шеннона «Теорія зв'язку в секретних системах», випущена в 1949 році є ще однією перехідною точкою, коли утвердилися нові теоретичні принципи захисту інформації. Криптографія проголошується математичної наукою. До кінця 1960 років з'являються перші більш досконалі блочні шифри, які змінювали роторні системи.

Бурхливий розвиток отримує комп'ютерна криптографія в 1970-х роках, що пояснюється серйозним збільшенням обчислювальних потужностей, які дозволяли вже до того моменту створювати повноцінні криптосистеми. Комп'ютерні криптосистеми в рази перевищували свої механічні аналоги. Крім того, з 1970-х криптографія стає повноцінною цивільної галуззю [15]. У 1978 р виникає стандарт шифрування – DES, поява якого сприяла розвитку нових кріптоаналітичних алгоритмів [21].

Уітфілд Діффі і Мартін Хеллман у 1976 році видають роботу «Нові напрямки в криптографії», в якій описують спосіб шифрування з відкритим ключем. Першою криптосистемою з відкритим ключем вважається алгоритм RSA, назва якого є акронімом імен творців – Rivest, Shamir, Adleman [22].

З цього часу інтерес до криптографії проявляють незалежні дослідники, оборонна промисловість і представники бізнесу. Зі збільшенням наукових розробок в галузі криптографії збільшується і активність влади. В США АНБ (Агентство національної безпеки)

намагалося всіляко засекретити будь-які розробки і досягнення в цій галузі не тільки державних організацій, а й незалежних дослідників. Широкого розголосу набув законопроект, який вимагав від розробників шифрувальних пристроїв включати в свої продукти так званий backdoor – чорний хід, - який дозволяв би спецслужбам отримувати доступ до інформації, що передається. Надалі, в 1993 році, АНБ вживало заходів щодо просування проекту Clipper Chip, який давав би можливість третій стороні отримувати доступ до закритого ключа [20].

У 80-90-і роки минулого століття з'являються нові види захисту інформації: шифрування ймовірностей, квантова криптографія та ін. Розвиток квантової фізики проявляє потенційні горизонти розвитку криптографії. Розширюються сфери застосування криптографії.

З моменту винаходу Інтернету і його подальшого поширення, а також перетворення його в головне засіб обміну інформацією між людьми криптографія стала актуальною для всіх верств населення, це підтверджується викриттям Едварда Сноудена. Він став говорити про необхідність підвищення криптографічної грамотності. Актуальність криптографії в наш час пояснюється тим, що доступ до Інтернету та інших мереж обміну інформацією є у переважної більшості людей в розвинених країнах, проте далеко не вся інформація, якою обмінюються люди, є захищеною. Нагадаємо, що за останній час широке поширення набули покупки онлайн, соціальні мережі, послуги державних порталів, на яких зосереджена найважливіша особиста інформація громадян. Крім того, що інформація стала більш різноманітною і більш конфіденційною, збільшилася і загальна кількість інформації.

У 2013 року системний аналітик і співробітник АНБ Едвард Сноуден передав пресі ряд документів, які підтверджують, що АНБ здійснює перехоплення електронних повідомлень, телефонних дзвінків (в тому числі керівників держав), відстеження пересування власників мобільних телефонів, потоків SMS, спостереження за співробітниками іноземних дипломатичних місій. Крім того стало відомо, що АНБ здійснювало співпрацю з найбільшими телекомунікаційними компаніями і найбільшими інтернет-провайдерами США, а також має можливості для здійснення несанкціонованого доступу до особистої інформації власників смартфонів на популярних платформах.

Отже, історія криптографії налічує кілька тисяч років. Перші надійні способи передачі інформації з'являлися завдяки військовим конфліктам. Становлення розгалуженого державного апарату в арабському світі сприяло поширенню криптографії серед державних діячів, а також появі перших наукових праць по криптоаналізу. З розвитком дипломатичних відносин, розвиваються і нові способи захисту інформації. Світові війни XX століття стверджують в черговий раз необхідність шифрування. Розвиток електронних, а потім і комп'ютерних технологій революційно змінює принципи будування систем захисту інформації. Бурхливий технічний прогрес кінця XX століття сприяє широкій інформатизації суспільства. Інформація стала досить цінною, що обумовлює подальші пошуки більш досконалих систем захисту інформації не тільки державної, а і пересічних громадян.

Можливо, Всесвіт є однією із систем захисту інформації, яка людством залишається не розгаданою. Навколо нас є дуже багато інформації, яка на даний час не відома, оскільки людство ще її не розшифрувало.

Історичний аспект виникнення та розвитку захисту інформації у світі проаналізовано з урахуванням відомих історичних та сучасних фактів. З розвитком новітніх технологій робитимуться відкриття в галузі захисту інформації, можливо і в розрізі історичного аспекту, що у свою чергу приведе і до перегляду історії виникнення та захисту інформації.

**Література:**

1. Slackman, Michael. In the Shadow of a Long Past, Patiently Awaiting the Future, The New York Times (17 November 2008);

2. Mark Lehner (2008). The Complete Pyramids: Solving the Ancient Mysteries. p. 34.. — Thames & Hudson, 2008-03-25. — ISBN 978-0-500-28547-3;

3.https://ru.wikipedia.org/wiki Египетское_ироглифическое_письмо;

4. Budge W. An Egyptian Hieroglyphic Dictionary, With an Index of English Words, King List and Geographical List with Index, List of Hieroglyphic Characters, Coptic and Semitic Alphabets, etc. — John Murry, 1920. — Vol. I—II.;

5. Gardiner A. H. Egyptian Grammar. Being an Introduction to the Study of Hieroglyphs. — 1927.;

6.ttps://allbible.info/bible/sinodal/jer/25/ (Єр. 25:26);

7. http://users.telenet.be/d.rijmenants/secret_writing.pdf - Edgar Allan Po.

A Few Words on Secret Writing. — C. first two paragrafe;

8. В.Ф. Беляев. «Эней Тактик — первый военный теоретик античности» http://www.xlegio.ru/sources/aeneas-tacticus/1st-military-theorist-of-antiquity.html

9. Германн Дильс «Телеграфия». (Перевод: М.Е. Сергеенко,

П.П. Забаринский);

10. Эней Тактик. О перенесении осады 31, 2—3.(Перевод: В.Ф. Беляев) http://xlegio.ru/sources/aeneas-tacticus/de-obsidione-toleranda.html;

11. Сингх С. Книга кодов: тайная история кодов и их взлома // Пер. с англ. А. Галыгина. М.: АСТ: Астрель, 2007. – 447 с.;

12. «Словник іншомовних слів» https://www.jnsm.com.ua/cgi-bin/m/s.pl?Article=10589&action=show;

13. . Эко У. Поиски совершенного языка в европейской культуре // Пер. сител. А. Миролюбовой (Серия «Становление Европы»). М.: Алексан- дрия, 2007. – 430 с.;

14. Кан Д. Взломщики кодов // Пер. А. Ключевский. М.: Центрполиграф,

2000. – 480 с.;

15. Носов В.А. Краткий исторический очерк развития криптографии // Московский университет и развитие криптографии в России. Материалы конференции МГУ 17-18 октября 2002 г. М.: МЦНМО, 2003. – С. 17-25.;

16. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. М.: ДМК Пресс, 2012. – 256 с.;

17. Dooley, John F. A Brief History of Cryptology and Cryptographic Algorithms. New York: Springer, 2013. – 99 p.;

18. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 3-е изд., стереотип. М.: ФЛИНТА, 2011. – 244 с.;

19. Бабаш А.В., Шанкин Г.П. Средневековая криптография. URL: http://cccp.narod.ru/work/book/kgb/babash_02.html.;

20. . Жельников В. Криптография от папируса до компьютера. М.: ABF,

1996. – 336 с.;

21. Скляров Д.В. Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. – 288 с.;

22. Баричев С.Г., Серов Р.Е. Основы современной криптографии. М.: Горячая линия – Телеком, 2011. – 175 с.