УДК 681.3.06:519.248.681

Мельник С. В., канд. техн. наук. Тел. +380 (44) 241 11 21. E-mail: msvcontakt@gmail.com
(Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України)

КОНЦЕПТУАЛЬНІ ОСНОВИ ОРГАНІЗАЦІЇ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Mel'nyk S. V. The conceptual basis for the organization of cryptographic protection. With the system approach examines the main principles of cryptographic protection as management features modern sector activities at national level, which aims to create the necessary conditions to ensure a sufficient level of cryptographic protection of information resources of man, society and the state, to ensure compatibility and reliability (cryptographic stability) cryptographic information protection on the Internet and so on.

As the basic processes of the National system of cryptographic information protection considered certain activities related to the development, manufacturing, sales, implementation and use of cryptographic information protection and provision of cryptographic protection. As the National System of cryptographic protection is considered an organizational system that includes the following structural elements: special authorized central executive authority (creates and implements national policies), organizations and individuals, in relation to which provides the cryptographic information protection; organizations and businesses which carry out activities with cryptographic protection. The effectiveness of the National system of cryptographic information protection considered in the light of the major factors of national and international policy in this area, and taking them into account in the national and international legal framework.

Keywords: cryptography, information protection, information resources, cryptographic stability, National system of cryptographic information protection

Мельник С. В. Концептуальні основи організації криптографічного захисту інформації. В роботі розглядаються основні принципи організації криптографічного захисту інформації як функції управління сучасною галуззю діяльності на державному рівні. Аналізуються необхідні умови для забезпечення достатнього рівня криптографічного захисту інформаційних ресурсів людини, суспільства та держави, а також забезпечення сумісності та достатнього рівня стійкості засобів і систем криптографічного захисту інформації в мережі Інтернет.

***Ключові слова*:** криптографія, захист інформації, інформаційні ресурси, криптографічна стійкість, Національна система криптографічного захисту інформації

Мельник С. В. Концептуальные основы организации криптографической защиты информации. В работе рассматриваются основные принципы организации криптографической защиты информации как функции управления современной отраслью деятельности на государственном уровне. Анализируются необходимые условия для обеспечения достаточного уровня криптографической защиты информационных ресурсов человека, общества и государства, а также обеспечения совместимости и достаточного уровня стойкости средств и систем криптографической защиты информации в сети Интернет.

Ключевые слова: криптография, защита информации, информационные ресурсы, криптографическая стойкость, Национальная система криптографической защиты информации

1. Вступ та постановка задачі

Розвиток криптографії як мистецтва, галузі знань та науки, а також криптографічного захисту інформації (КЗІ) як сучасної галузі діяльності, є світовою історією інформаційного протиборства в рамках нескінченних конфліктів військового, політичного, економічного та іншого характеру (навіть побутового рівня). В сучасних умовах розвитку інформаційного суспільства коло завдань, які вирішуються методами криптографії не зменшується, а навпаки, значно розширюється, оскільки стрімко зростає потреба у захисті інформації на рівнях людини, суспільства, держави та міжнародної спільноти.

За останні 30-40 років у світі відбулося немало подій, що пов'язані з появою та масовим поширенням комп'ютерної техніки, мережевих та інформаційних технологій, насамперед, Інтернет. При цьому на стан розвитку і поширення сучасних інформаційно-телекомунікаційних технологій безпосередньо вплинули події, пов'язані з появою:

– стандартів криптографічних алгоритмів, що обумовило доступність "сильної" криптографії для простих громадян і підприємств, а також суттєво вплинуло на розвиток так-званою "відкритої" (або "громадської") криптографії, що обумовило доступність широкому загалу фахівців теоретичних знань щодо побудови і оцінювання криптографічних методів;

– методів нової асиметричної криптографії (або криптографії з відкритим ключем), які дозволили вирішувати нові завдання, які було неможливо виконати методами класичної симетричної криптографії, а саме – автентичність і неможливість відмови від авторства на інформацію.

І це фактично призвело до появи окремої галуззі діяльності з широким спектром адміністративних і технічних питань, що стосуються розроблення, виробництва, реалізації, застосування методів, засобів і систем КЗІ.

Безумовно, процеси впровадження інформаційно-телекомунікаційних технологій не лише вплинули на розвиток методів, засобів, систем та заходів КЗІ, а призвели також до появи галузі технічного захисту інформації (ТЗІ). Крім того, стала актуальною концепція комплексного підходу до захисту інформації та почала формуватись загальна теорія захисту інформації, що охоплює:

– об'єкти, суб'єкти, загрози та їх реалізації, види та відповідні методи захисту інформації;

– концепцію комплексного підходу до захисту інформації (включаючи технологічну, правову та організаційну складову) через призму взаємодії базових методів технічного і криптографічного захисту інформації, спеціального діловодства і режиму, інженерно-технічного захисту об'єктів інформаційної діяльності, а також методів забезпечення надійності персоналу;

– характеристики та показники ефективності методів, засобів та заходів захисту інформації;

– формалізації та оцінки систем захисту інформації та систем управління захистом інформації (управління інформаційною безпекою).

Тому питання криптографічного захисту інформації доцільно розглядати лише в контексті комплексного захисту з позицій системного підходу до організації КЗІ як функції управління сучасною галуззю діяльності, побудови та ефективного функціонування Національної системи КЗІ зокрема.

2. Аналіз літературних даних

Тематика криптології (криптографії та криптоаналізу), як галузі знань та науки, розглянута багатьма іноземними та вітчизняними фахівцями [1-3] та стосується, насамперед, методів симетричної і асиметричної криптографії, їх подолання відповідно.

Тематика комплексного захисту інформації, системного підходу до захисту інформації, моделювання та оцінювання ефективності систем захисту інформації висвітлена в багатьох роботах, насамперед, роботах [4-9]. Більшість з них стосується особливостей захисту інформації в інформаційно-телекомунікаційних системах від несанкціонованого доступу, побудови комплексних систем захисту інформації та систем управління інформаційною безпекою.

В свою чергу, питання організації захисту інформації з обмеженим доступом розглядалися вітчизняними вченими [10-13] через призму нормативно-правових актів України, що визначають необхідність захисту інформації, порядок захисту та відповідальність за його порушення.

На основі аналізу літературних джерел, доцільно зазначити, що малодослідженими є методологічні основи криптографічного захисту інформації як системи принципів та способів організації продуктивної практичної діяльності – організації криптографічного захисту інформації.

3. Мета і задачі дослідження

Мета роботи полягає в обґрунтуванні основних чинників, що впливають на формування і реалізацію національної політики у галузі криптографічного захисту інформації, оцінку ефективності Національної системи КЗІ на сучасному етапі розвитку глобального інформаційного суспільства.

Для досягнення поставленої мети вирішувалися наступні завдання:

– дослідження історичних аспектів розвитку криптографії і криптографічного захисту інформації;

– визначення основних складових національної і міжнародної політики у галузі криптографічного захисту інформації, обґрунтування основних засад нормативно-правового регулювання у галузі криптографічного захисту інформації.

4. Історичні аспекти розвитку криптографії і криптографічного захисту інформації

У перекладі з грецької мови слово *криптографія* (*cryptography*) – це тайнопис. Значення цього терміну визначає основне, найбільш відоме із історії, призначення криптографії – це захист інформації від несанкціонованого ознайомлення з її змістом (тобто загрози витоку або порушення конфіденційності інформації). *Сучасна криптографія* – це знання про математичні методи захисту інформації від загроз її витоку та нав'язування фальшивої інформації, а також унеможливлення відмови від авторства на інформацію (тобто від загроз порушення конфіденційності, цілісності та авторства інформації).

Тобто методи сучасної криптографії використовуються для захисту інформації з обмеженим доступом (ІзОД) та відкритої інформації.

Звісно методами криптографії неможливо забезпечити доступність інформації в сучасних інформаційно-телекомунікаційних системах (ІТС, оскільки математичні методи безпорадні з точки зору захисту від загроз несанкціонованого знищення або блокування інформації. Однак математичний метод забезпечення цілісності і авторства інформації (криптографічний алгоритм електронного цифрового підпису) є єдино можливим методом автентифікації в умовах коли сторони інформаційного обміну не довіряють один одному. Крім того, математичному методу забезпечення конфіденційності (шифруванню) немає альтернативи, коли мова йде про захист інформації в каналах зв'язку та базах (носіях) даних.

Основним параметром оцінювання ефективності сучасних систем КЗІ (оскільки використовуються не методи та засоби, а системи КЗІ) є поняття рівня криптографічної стійкості. Де *система КЗІ* – це організаційно-технічна структура, що включає в себе засоби КЗІ (технічну реалізацію методів криптографії), персонал та організацію (порядок) діяльності із захисту інформації (управління ключами та експлуатацію засобів КЗІ). В свою чергу, *рівень криптографічної стійкості* – це інтегральний показник безпеки, який включає оцінки рівня:

– практичної стійкості криптографічних алгоритмів і протоколів до методів дешифрування і нав'язування інформації (*математичних перетворень криптосистем*);

– надійності технічної реалізації засобів КЗІ, з точки зору можливостей витоку інформації про відкриті тексти та ключі в наслідок неполадок технічних засобів (*інженерно-криптографічних характеристик засобів КЗІ*);

– технологій технічного захисту інформації в засобах КЗІ від загроз несанкціонованого доступу до інформації про відкриті тексти та ключі, а також витоку цієї інформації каналами побічних електромагнітних випромінювань та наведень (*технічного захисту інженерних рішень засобів КЗІ*);

– організаційно-технічних заходів безпеки систем КЗІ, що стосуються питань виготовлення, розповсюдження, зберігання, використання і знищення ключів, експлуатації

засобів КЗІ, включаючи питання пропускного та внутрішньооб'єктового режиму заходів КЗІ (*організаційно-технічної структури системи КЗІ*);

– організаційних заходів допуску осіб до експлуатації засобів КЗІ та контрольних функцій щодо їх виконання (*виконавчої дисципліни та благонадійності особового складу*).

Таким чином, під час оцінювання рівня криптографічної стійкості систем КЗІ окрім математематичних методів крипто аналізу враховуються додаткові загрози – це: технічні канали доступу до відкритого тексту та ключів або їх витоку; можливості несанкціонованої випадкової/навмисної модифікації засобів КЗІ; можливі помилки або навмисні дії користувачів засобів КЗІ. Відповідно, достатній рівень стійкості криптографічного захисту інформації (відповідно до моделі загроз та моделі потенційного криптоаналітика) може бути забезпеченим лише за умови використання комплексного підходу до захисту, що передбачає використання також методів технічного захисту інформації, організаційно-технічних та організаційних заходів безпеки.

Додатковими чинниками, що впливають на рівень стійкості криптографічного захисту інформації є механізм правового захисту інформації (відповідальність за несанкціоноване подолання КЗІ) та механізм страхування інформаційних ризиків (ризиків витоку та нав'язування інформації). І саме ці чинники, у певній мірі, дозволяють зменшити вимоги до вищезазначених характеристик систем КЗІ.

Далі доцільно зазначити, що історія криптології та криптографічного захисту інформації дозволяє нам глибше усвідомити важливість цієї галузі знань та діяльності на сучасному етапі розвитку інформаційних відносин, їх роль та місце в сучасних завданнях захисту інформації на рівнях людини, суспільства, держави. Наприклад, через призму питання цінності інформації як у давньому, так і сучасному світі, а також через призму того, як знання і талант однієї людини або невеликого колективу криптоаналітиків (математиків, інженерів, фахівців оперативної та оперативно-технічної справи) впливали на хід історії та залишили свій слід у військових справах, політиці, науці, економіці та багатьох інших сферах людського життя.

Історія криптології налічує тисячі років та фактично починає свій відлік із часів появи писемності в Єгипті, Індії, Китаї та інших давніх цивілізаціях. На протязі близько 4000 років розвиток криптології був дуже повільним, відбувався у кожній країні (цивілізації) окремо та стосувався обмеженого кола осіб. В одних місцях вона з'являлася і зникала разом із цивілізацією, що її породила, а в інших, перші методи криптографії стали пам'ятниками літератури та зумовили подальший світовий розвиток цієї галузі знань.

Як відомо, криптографія з давніх часів і до 70-80 років минулого століття не була публічною, а відносилась виключно до компетенції спеціальних служб (в сучасній термінології), що забезпечували безпеку систем військового та дипломатичного зв'язку, або здійснювали розвідувальну та контррозвідувальну діяльність. На сьогодні криптографія, як галузь знань, та криптографічний захист інформації, як окрема галузь діяльності, стосується не лише питань шифрувальної справи, а й новітніх технологій електронного Урядування, електронної торгівлі, автоматизованого управління, звітування та контролю тощо. Тобто, в світі відбулося становлення так званої «громадської криптографії», обумовлене об'єктивною необхідністю використання її методів широким загалом організацій та пересічних громадян, що не мають ніякого відношення до спеціальних служб.

Основними чинниками, що впливали та впливають на розвиток криптографії та КЗІ є:

– багатовікова і постійно зростаюча потреба у захисті інформації;

– розвиток фундаментальної та прикладної математики, відповідно, розвиток теоретичної і практичної криптології;

– багатовіковий процес вдосконалення технологічної бази обміну інформацією – запису на каменях, глиняних табличках (Месопотамія), папірусі (Єгипет), бересті (Русь), шовковій

тканині (Китай), пергаменті (Єгипет, Греція, Рим), дерев'яних дощечках (Греція, Рим), папері (Китай) і нарешті сучасних електронних технологіях зберігання та передачі інформації.

При цьому, слід зазначити, що у більшій мірі, етапи розвитку криптології пов'язані з історією *технічного розвитку людства*, що визначала технічні можливості по реалізації досягнень у теоретичній і практичній криптології на певний період часу. Наприклад, можна розглянути:

– *епоху ручних шифрів* (з III-го тисячоліття до н.е. до XIX ст.), що об'єктивно характеризується розвитком найбільш простих математичних перетворень, фактично, різновидів та комбінацій шифрів простої та пропорційної заміни, перестановки, лінійних шифрів багатозначної (колонної) заміни;

– *період роторних (механічних та електромеханічних) шифраторів* (перша половина XX ст.), в який за рахунок, насамперед, можливостей тодішньої механіки в технічній реалізації лінійних та нелінійних шифрів багатозначної заміни, отримали активний розвиток методи побудови та аналізу цих шифрів;

– *період апаратури автоматичного засекречування* (*електронних шифраторів*) тимчасової та гарантованої стійкості (30-80 роки XX ст.) – період технічної реалізації, насамперед, лінійних та нелінійних шифрів багатозначної заміни з використанням перших можливостей аналогової та цифрової електроніки та систем зв'язку з комутацією каналів, що характеризується активним розвитком методів побудови та аналізу потокових алгоритмів шифрування;

– напевне, все ж таки *епоху комп'ютерних технологій* (почалася з 70-х років XX ст.), яка характеризується, фактично, необмеженими можливостями в технічній реалізації будь-яких криптографічних перетворень симетричної та асиметричної криптографії, що призвело до активного розвитку сучасних алгоритмів шифрування, ключових та безключових функцій гешування, алгоритмів електронного цифрового підпису, а також криптографічних протоколів різного призначення.

Етапи розвитку криптографії доцільно також розглянути і з точки зору розвитку *теоретичних знань із криптології*, оскільки на цих етапах є суттєва різниця в ефективності її методів як з точки зору стійкості криптографічних перетворень, так і з точки зору завдань захисту інформації, що могли бути вирішені цими методами. Так, наприклад, можна розглянути:

– *епоху криптографіїї як ремесла та мистецтва, або донаукової криптографії* (співпадає з епохою ручних шифрів та періодом роторних шифраторів), коли методи шифрування, як правило, не забезпечували гарантований рівень стійкості, бо не мали теоретичного підґрунтя для оцінювання;

– *період наукової класичної або симетричної криптографії* (співпадає з періодом апаратури автоматичного засекречування), коли були чітко визначені критерії теоретичної та практичної стійкості методів шифрування, активно розвивалися методи побудови та аналізу зазначених криптографічних перетворень;

– напевне, все ж таки *епоха нової асиметричної криптографії* (співпадає з епохою комп'ютерних технологій), коли з'явилися абсолютно нові функціональні можливості, не притаманні класичній криптографії, що стосуються забезпечення цілісності та автентичності інформації в умовах, коли всі учасники інформаційного обміну не довіряють один одному.

5. Національна та міжнародна політика у галузі криптографічного захисту інформації

В зв'язку з тим з'явилась потреба у врегулюванні порядку здійснення (застосування) криптографічного захисту інформації на національному та міжнародному рівнях, а саме:

– визначенні вимог до рівня криптографічного захисту різних видів інформації з обмеженим доступом та відкритої інформації (порядку розроблення, виробництва, реалізації, застосування засобів і систем КЗІ);

– визначенні правових обмежень на застосування засобів і систем КЗІ;

– стандартизації методів, засобів і систем КЗІ;

– визначення вимог до системи ЕЦП (архітектури відкритих ключів);

– державній регуляторній політиці щодо господарської діяльності у галузі КЗІ.

В сучасних умовах, національна політика у галузі КЗІ формується під достатньо вагомим впливом суспільних організацій та правозахисних груп. І цей вплив стосується питань забезпечення прав і свобод людини в глобальному інформаційному просторі, насамперед, забезпечення конфіденційності в мережі Інтернет шляхом використання засобів КЗІ.

Іншим чинником впливу є проблеми правоохоронної діяльності, що пов'язані із законним доступом до зашифрованих даних громадян в рамках заходів розслідування та розкриття правопорушень, насамперед, під час проведення комп'ютерно-технічної експертизи.

Ще одним, найбільш вагомим чинником впливу, є завдання забезпечення достатнього рівня захисту різних видів інформації з обмеженим доступом та відкритої інформації, що безпосередньо стосується питань забезпечення захисту інформації людини, суспільства, держави.

І це питання національної безпеки.

Таким чином, національна політика у галузі КЗІ повинна бути спрямована на досягнення компромісу при вирішенні наступних завдань.

1. Створення необхідних умов для забезпечення достатнього рівня КЗІ державних структур, організацій і підприємств усіх форм власності, а також громадян.

2. Зменшити ризики використання стійких засобів шифрування в противоправній діяльності, у тому числі і терористичного характеру.

Основні інтереси міжнародного товариства у галузі КЗІ полягають у створенні умов для розгортання глобальних Інтернет технологій з використанням засобів КЗІ (насамперед, систем електронної комерції) шляхом:

– забезпечення доступу пересічних громадян та бізнесу до «сильної» криптографії та довіри до рівня їх практичної стійкості (насамперед, засобів автентифікації);

– сумісності методів та засобів КЗІ різних виробників;

– сумісності законодавства різних країн щодо забезпечення юридичної сили електронних документів при використанні засобів ЕЦП.

Організація по міжнародному співробітництву та розвитку (ОЕСР) у 1996 році запропонувала наступні рекомендації для формування національної політики у галузі КЗІ:

1. Методи КЗІ повинні користуватися довірою, щоб такою ж довірою користувалися інформаційно-телекомунікаційні системи.

2. Користувачі методів КЗІ повинні мати право обирати будь-який метод, що не забороняється законом.

3. Розвиток засобів КЗІ повинен визначатися потребами приватних осіб, комерційних організацій і державних структур.

4. Стандарти методів та засобів КЗІ повинні розроблятися і підтримуватися як на національному, так і міжнародному рівнях.

5. Основні права людини на недоторканність приватного життя повинні бути недоторканими в національній політиці у галузі КЗІ.

6. Національна політика у галузі КЗІ може передбачати законний доступ до зашифрованих даних або ключів.

Національна політика у галузі КЗІ реалізується нормативно-правовою базою, яка складається із стандартизації, адміністративно-правового регулювання господарської діяльності у галузі КЗІ, нормативно-правового забезпечення системи ЕЦП.

Стандартизація у галузі КЗІ (як на національному, так і міжнародному рівні) забезпечує:

– доступ пересічних громадян, бізнесу та державних установ до "сильної" криптографії та довіру до рівня їх практичної стійкості, відповідно, необхідні умови для забезпечення достатнього рівня КЗІ для відкритої інформації та всіх видів ІзОД (окрім державної таємниці);

– сумісність методів та засобів КЗІ різних виробників.

Адміністративно-правове регулювання господарської діяльності у галузі КЗІ створює систему довіри між суб'єктами господарської діяльності, споживачами засобів і послуг КЗІ, а також державою – гарантом забезпечення достатнього рівня захисту національних інформаційних ресурсів.

Як правило, адміністративно-правове регулювання включає в себе порядок *ліцензування*, *експертизи*, *розроблення*, *впровадження*, *експлуатації* засобів і систем КЗІ.

Крім того, визначаються також додаткові норми до створення, впровадження та експлуатації *системи ЕЦП* (*архітектури відкритих ключів, РКІ*).

Ліцензування – це процедура підтвердження спроможності суб'єкта господарської діяльності виконувати заявлені види робіт шляхом перевірки державою кваліфікаційних, організаційних, технологічних та інших необхідних характеристик.

Експертиза – це процедури державного підтвердження якості виконання заявлених видів робіт суб'єктом господарської діяльності, що включає в себе перевірку математичних, технічних і організаційно-технічних характеристик засобів і систем КЗІ.

Порядок розроблення, впровадження, експлуатації засобів і систем КЗІ визначає додаткові норми до організаційно-технічних заходів безпеки і порядку технічного захисту інформації у засобах і системах КЗІ в залежності від їх призначення і виду інформації, яка потребує захисту.

Основною метою побудови систем ЕЦП є реалізація механізму *забезпечення правового статусу електронного підпису* як аналога підпису фізичної і юридичної особи, що дозволяє будувати системи електронного документообігу з юридичною відповідальністю сторін.

При цьому питання правового статусу електронного підпису може бути вирішене як на загальнодержавному рівні з використанням національної системи ЕЦП, так і в рамках договірних відносин між суб'єктами електронного документообігу.

7. Висновки

Основними проблемними питаннями нормативно-правового регулювання діяльності у галузі КЗІ є створення умов для:

– забезпечення достатнього рівня КЗІ державних структур, організацій і підприємств усіх форм власності, а також пересічних громадян;

– зменшення ризиків використання стійких засобів шифрування в противоправній діяльності;

– сумісності засобів і криптосистем в мережі Інтернет;

– забезпечення правового статусу ЕЦП на національному та міжнародному рівнях.

З точки зору комплексного підходу до захисту інформації, доцільно звернути увагу на формалізацію вимог до рівня криптографічного захисту різних видів інформації з обмеженим доступом, гармонізації цих вимог із законодавством, яке визначає відповідальність за розголошення (порушення цілісності та авторства) цих видів інформації, оскільки захист інформації повинен бути збалансованим з точки зору можливих дій потенційного

супротивника (людський фактор, ТЗІ, КЗІ). Додатково, доцільно формалізувати вимоги до засобів КЗІ, які призначені для захисту інформації з обмеженим доступом (наприклад, як у FIPS 140-3).

Основними напрямами нормативно-правового регулювання діяльності у галузі КЗІ є формування вимог до рівня і порядку криптографічного захисту різних видів ІзОД, визначення змісту та порядку ліцензування, розроблення, виробництва, експертизи, впровадження і експлуатації засобів і систем у галузі КЗІ, створення і функціонування систем ЕЦП. Ефективність цих процедур визначається функціоналом державних адміністративних послуг, що надаються.

Література

1. Eurocrypt Conference is an international conference on all aspects of cryptology [Електронний ресурс] // – Режим доступу : http://www.iacr.org/meetings/eurocrypto/.

2. Crypto conference is an international conference on all aspects of cryptology [Електронний ресурс] // Santa Barbara, USA. – Режим доступу : http://www.iacr.org/meetings/crypto/.

3. Asiacrypt conference is an international conference on all aspects of cryptology [Електронний ресурс] // – Режим доступу : http://www.iacr.org/meetings/asiacrypt/.

4. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – Москва ; Санкт-Петербург; Киев : ДиаСофт, 2004 . – 992 с.

5. Архипов О. Є. Оцінювання ефективності системи охорони державної таємниці : моногр. / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – Київ : Нац. акад. служби безпеки України. Ін-т захисту інформації з обмеж. доступом, 2007.

6. Бурячок В. Л. Політика інформаційної безпеки : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; за заг. ред. докт. техн. наук, проф. В. О. Хорошка. – Київ : ПВП «Задруга», 2014. – 222 с.

7. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – Київ : МК-Прес, 2005. – 432 с.

8. Бойченко О. В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О. В. Бойченко, Я. І. Торошанко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №4(20). – С. 15-19.

9. Толюпа С. В. Пути обеспечения безопасности электронных хранилищ / С. В. Толюпа, Я. И. Торошанко, А. Ю. Мороко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2012. – №3(23). – С. 17-22.

10. Стоцький О. Б. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. для студ. вищ. навч. закл. / О. Б. Стоцький, О. І. Тимошенко, А. М. Гуз, В. В. Макаренко, А. І. Марущак, С. О. Князєв, В. Ю. Артемов ; ред.: В. С. Сідак; Національна акад. СБ України, Інститут захисту інформації з обмеж. доступом, Європ. ун-т. – Київ, 2006. – 232 с.

11. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навч. посіб. / А. М. Гуз. – Київ : КНТ, 2007. – 255 с.

12. Гуз А. М. Організація захисту інформації з обмеженим доступом : Підручник / А. М. Гуз, О. Д. Довгань, А. І. Марущак та ін.; за заг. ред. Є. Д. Скулиша. – Київ : Наук.-вид. відділ НА СБ України, 2011. – 378 с.

13. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення : підручник / О. К. Юдін. – Київ : НАУ, 2011. – 640 с.

Дата надходження в редакцію: 07.08.2015 р. Рецензент: д.т.н., проф. О. О. Скопа