Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
ЗАТ «Інститут інформаційних технологій»

ГОРБЕНКО Ю. І., ГОРБЕНКО І. Д.

ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС.

ТЕОРІЯ ТА ПРАКТИКА

МОНОГРАФІЯ

Харків
Видавництво «Форт»
2010

УДК 004.056.55
ББК 32.973-018.2
Г 67

Рекомендовано до видання Науково-методичною радою
Харківського національного університету радіоелектроніки
(Протокол № 6 від 25.06.2010)

Рекомендовано до друку Вченою радою
Харківського національного університету радіоелектроніки
(Протокол № 63 від 05.07.2010)

Рецензенти:
СКРИПНИК Л. В. – доктор технічних наук, професор, Заслужений діяч науки і техніки, Лауреат державної премії, начальник спеціальної кафедри Інституту державної служби спеціального зв'язку та захисту інформації НТТУ КПІ, виконуючий обов'язки Президента академії криптографії України;

СТАСЄВ Ю. В. – доктор технічних наук, професор, Заслужений діяч науки і техніки, заступник начальника Харківського університету Повітряних Сил ім. І. Кожедуба;

СОРОКА Л. С. – доктор технічних наук, професор, декан факультету комп'ютерних наук Харківського національного університету ім. В. Каразіна.

Горбенко Ю. І., Горбенко І. Д.

Г 67 Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. – Харків : Видавництво «Форт», 2010. – 608 с.

Горбенко Ю. І. (розділи 3–5, 7–10, додаток А, диск).
Горбенко І. Д. (розділи 1–2, 6, 11–13, додаток А, диск).

ISBN 978-966-8599-76-7

У монографії викладені стан, сутність та сучасні проблемні питання теорії та практики аналізу, синтезу та застосування електронного цифрового підпису в інформаційних та інформаційно-телекомунікаційних системах різноманітного призначення. У главах 1–5 розглядаються питання класифікації, вимоги та сутність криптографічних перетворень типу «Електронний цифровий підпис» та «Направлене шифрування», наводяться методики та результати порівняльного аналізу існуючих систем електронного цифрового підпису, даються відповідні рекомендації та пропозиції. У главах 6–9 наводяться результати класифікації, обґрунтування вимог і порівняльного аналізу механізмів і криптографічних протоколів на основі електронного цифрового підпису, а також розглядаються питання створення та характеристики інфраструктур відкритих ключів технологічно розвинених держав і національної системи електронного цифрового підпису. Глави 10–13 присвячені обґрунтуванню вимог до засобів криптографічних перетворень для ІВК, розробці принципів проектування та технологій виготовлення й застосування таких засобів, аналізу перспективних політик сертифікації ключів. Також розглядаються деякі проблемні питання розвитку ІВК і національної системи електронного цифрового підпису та можливі шляхи їх вирішення.

Для розробників і спеціалістів інфраструктур з відкритими ключами, систем, комплексів і засобів криптографічного захисту, підготовки аспірантів, магістрів і бакалаврів у галузі «Інформаційна безпека», користувачів сучасними інформаційно-телекомунікаційними системами, системами електронних документів та електронного документообігу.

УДК 004.056.55
ББК 32.973-018.2

ISBN 978-966-8599-76-7

ВСТУП

«По-справжньому безпечною можна вважати лише систему, що вимкнена, замурована в бетонний корпус, замкнена в приміщенні зі свинцевими стінами й охороняється збройною вартою, – але й у цьому випадку сумніви не залишають мене».

Юджин Х. Спаффорд

Безумовним і загальновизнаним є той факт, що сучасний етап розвитку нашої цивілізації значною мірою визначається станом розвитку та застосування інформаційних технологій у різних сферах нашого буття, дії та взаємодії в межах земної цивілізації. Основним призначенням і застосуванням інформаційних технологій є обробка інформації. Як правило, вона реалізується засобом створення та застосування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також автоматизованих систем управління. При цьому особливо важливу роль зазначені системи відіграють у таких сферах, як економіка, освіта, наука, державне управління, оборона, безпека життєдіяльності людини, інтеграція на міжнародному рівні тощо.

По суті, при функціонуванні вказаних систем через доступ до інформаційних ресурсів здійснюється обробка інформації систем.

*Під **обробкою інформації** в системі розуміють виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.* Таким чином, обробка інформації є широким поняттям; вона, по суті, у явному вигляді не включає тільки механізми архівування й архівного зберігання інформації.

Є різні підходи до визначення понять і термінів інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також самої інформації. Автори цієї монографії вважають за необхідне при викладенні матеріалу, що стосується інфраструктури відкритих ключів, використовувати поняття і терміни в такому значенні:

Інформаційна (автоматизована) система – система, у якій реалізується технологія обробки інформації за допомогою технічних і програмних засобів [1].

Телекомунікаційна система – 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 іншим способом [1].

Інформаційно-телекомунікаційна система – сукупність взаємопов'язаних інформаційних і телекомунікаційних систем, які в процесі обробки інформації діють як єдина система [1].

Інформація в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, інформаційних технологіях – сукупність даних, програм, повідомлень, команд сигналів тощо, які використовуються або передаються в них, незалежно від способу їх фізичного чи логічного представлення [1, 4]. Також керівна, науково-дослідна та науково-технічна, проектно-експлуатаційна й інша документація життєвого циклу вказаних систем і технологій.

Інформація – привселюдно оголошені чи опубліковані зведення про події та явища, що відбуваються в суспільстві, природному середовищі і т.д. (Закон України про інформацію) [4].

Необхідно також зазначити, що на нинішньому етапі розвитку широкого розповсюдження набуло використання специфічно поданої інформації – електронних документів і здійснення на їх основі електронного документообігу. При цьому під ***електронним документом*** розуміють інформацію, зафіксовану у вигляді електронних даних, включаючи обов'язкові реквізити документа [2, 3]. Уже перші впровадження підтверджують, що електронний документообіг є найбільш результативним підходом до суттєвого підвищення ефективності роботи органів державної влади та місцевого самоврядування. Надзвичайно важливим є впровадження електронного документообігу в час розбудови інформаційного суспільства, функціонування технологій електронного управління для забезпечення прозорості відносин «громадянин – держава», «підприємство – держава» та високої якості надання державних, комерційних і банківських послуг.

Вже достатньо великий досвід застосування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем і різноманітних технологій підтверджує, що в них користувачам і власникам інформації та ресурсів послуги із забезпечення безпеки інформації, що обробляється, повинні надаватись з необхідною якістю. Достатньо повно ці послуги визначені в [1–5, 48–50]. У подальшому під послугами криптографічної системи будемо розуміти послуги ***цілісності, автентичності (справжності), неспростовності (спостережливості), доступності, конфіденційності та надійності.***

Є декілька визначень указаних послуг з безпеки інформації. Як основні приймемо та будемо враховувати й використовувати такі [1–8, 48–50]:

Цілісність інформації – властивість інформації, яка полягає в тому, що вона не може бути змінена випадково або навмисне неавторизованими користувачами та (або) процесами.

Цілісність інформації – властивість захищеності інформації, яка полягає в тому, що інформація практично не може бути змінена випадково чи навмисне неавторизованими суб'єктами (порушниками) чи об'єктами (процесами); причому факт можливості порушення цілісності може бути визначений з наперед заданою ймовірністю.

Цілісність інформації – захист від несанкціонованої модифікації чи знищення інформації.

Автентифікація – заходи захисту, що призначені для встановлення достовірності передачі повідомлення чи відправника, або засобів верифікації санкціонування індивідуума для отримання конкретних категорій інформації.

Автентифікація – процедура чи процес встановлення достовірності твердження, що суб'єкт або об'єкт має заявлені (очікувані) властивості.

Як правило, автентифікація має дві складові – *ідентифікацію та верифікацію.*

Конфіденційність інформації – властивість захищеності інформації з наперед заданою якістю (імовірністю) від неавторизованого доступу до неї та спроб розкриття (отримання змісту) неавторизованими користувачами та (або) процесами.

Конфіденційність інформації – властивість захищеної інформації забезпечувати з наперед гарантованою стійкістю (імовірністю) захист від неавторизованого доступу до неї та спроб розкриття змісту неавторизованими суб'єктами чи об'єктами (порушниками).

Конфіденційність інформації – гарантія нерозголошування інформації для несанкціонованих об'єктів або процесів.

Доступність – властивість ресурсу системи (інформації, послуги, об'єкта інформаційної та (або) телекомунікаційної або ІТС, КСЗІ ІТ тощо), яка полягає в тому, що авторизований користувач і (або) процес, наділений відповідними повноваженнями, може використовувати ресурс згідно з правилами та з певною якістю, у тому числі за рахунок виконання криптографічних перетворень.

Доступність – властивість криптографічної системи, яка полягає в тому, що уповноважений суб'єкт (користувач) чи об'єкт (процес) може здійснювати криптографічний захист інформації згідно з правилами та наперед визначеною якістю (криптостійкістю, імітостійкістю тощо). Доступність криптографічної системи є складовою (як правило, основною в сенсі рівня гарантій) забезпечення доступності в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах тощо.

Неспростовність – властивість запобіганню можливості заперечення реальними суб'єктами (користувачами) та об'єктами (процесами) фактів повного або часткового взяття участі в інформаційному обміні або інформаційній взаємодії. Як правило, включає формування, надання та передавання доказів реального прийняття участі в інформаційному обміні чи інформаційній взаємодії і здебільшого ґрунтується на виконанні криптографічних перетворень з використанням особистих ключів.

Спостережливість – властивість ресурсу системи (комп'ютерної системи, об'єкта комп'ютерної системи, КСЗІ ІТ тощо), що дозволяє реєструвати (фіксувати) роботу та дії користувачів і процесів, використання ресурсу системи, однозначно встановлювати ідентифікатори (імена) причетних до певних подій користувачів та процесів, а також реагувати на ці події з метою мінімізації можливих втрат у системі, що здійснюється в тому числі за рахунок використання криптографічних перетворень.

Надійність – властивість незмінності певної поведінки та результатів.

Повний перелік термінів і визначень з відповідними посиланнями, що, на наш погляд, може бути застосований відносно ІВК, у тому числі електронний цифровий підпис.

Указані послуги повною мірою можуть бути надані засобом використання як основних асиметричних криптографічних перетворень типу «Електронний цифровий підпис», «Направлений шифр», а також криптографічних механізмів

розподілення таємниці та ключа, встановлення й підтвердження ключа тощо. Однією з фундаментальних системних проблем у цьому напрямку є генерування асиметричних пар ключів та відповідне їх зберігання й використання. Вирішення цієї проблеми ґрунтується на створенні, а також застосуванні на рівні держав, союзів, а то й на міжнародному рівні, інфраструктури відкритих ключів (ІВК). Також особливе місце в наданні зазначених послуг посідають криптографічні перетворення типу «Електронний цифровий підпис» [1–2, 6–10, 15–16, 27–29, 34–35, 40–47].

Електронний цифровий підпис – 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. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Під ***електронним підписом*** будемо розуміти дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Основним застосуванням ЕЦП є надання об'єктам і суб'єктам послуг електронного цифрового підпису для захисту інформації.

Під ***послугою електронного цифрового підпису*** розуміють надання користувачеві засобів електронного цифрового підпису, допомогу при генерації відкритих і особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування і поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги. Послуги електронного цифрового підпису надаються через використання засобів виконання електронного цифрового підпису. Основним суб'єктом використання електронного цифрового підпису є підписувач – особа, яка на законних підставах володіє особистим ключем і від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначений для генерації ключів, накладання та (або) перевірки електронного цифрового підпису. Вироблення електронного цифрового підпису здійснюється з використанням особистого ключа, перевіряння підписаної інформації за допомогою відкритого ключа. ***Особистий ключ*** – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу. ***Відкритий ключ*** – параметр криптографічного алгоритму електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Для надійного використання відкритого ключа виконується засвідчення його чинності – процедура формування сертифіката відкритого ключа. На національному рівні ***сертифікат відкритого ключа*** (далі сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі документа на папері та використовуватися для ідентифікації особи підписувача. ***Посилений сертифікат відкритого ключа*** (далі посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам Закону

«Про електронний цифровий підпис» від 22.05.03 № 825-IV, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Інфраструктури відкритого ключа, перш за все електронного цифрового підпису, мають достатньо значиму історію розроблення, створення та розвитку. Перші роботи в цьому напрямку стали актуальними після винаходу асиметричних криптографічних перетворень. Існує значне число асиметричних криптографічних систем [5–40]. Їх принциповою особливістю є те, що при виконанні криптографічних перетворень у них використовується одна або декілька асиметричних пар ключів.

Так, у RSA для ЕЦП та направленого шифрування використовуються різні випадкові асиметричні ключові пари $(E_к, D_к)$ особистого та відкритого ключів [7, 9, 10, 46]. Для криптографічних перетворень у полі $GF(p)$ кожна асиметрична ключова пара (x_A, Y_A) також породжується випадково, де x_A – особистий ключ, а Y_A – відкритий ключ [7, 9, 10, 40, 43, 46]. Для криптографічних перетворень у групі точок еліптичної кривої кожна асиметрична ключова пара (d_A, Q_A), де $1 \le d_A \le n$, є випадкове число – особистий ключ, а Q_A – точка на еліптичній кривій – відкритий ключ [7–10, 15–16, 27, 29–31, 34–35, 44–47]. Аналогічно й для інших асиметричних криптографічних перетворень, наприклад у групах точок гіпереліптичних кривих, зі спарюванням точок еліптичних кривих [11, 12, 53, 54] тощо.

У відповідності з концепцією асиметричних систем щодо застосування особистих ключів безумовно мають бути дотримані вимоги забезпечення їх конфіденційності, цілісності, справжності, доступності та неспростовності. Указані вимоги можуть бути забезпечені кожним із користувачів, оскільки особистий ключ доступний тільки його власнику, і він повинен і може зберігати його в таємниці. Необхідно зазначити, що не обов'язково E_k вибирати як особистий ключ, можна вибрати і D_k, але його після вибору треба використовувати із забезпеченням конфіденційності, цілісності, справжності та доступності, причому забезпечення конфіденційності з необхідним рівнем стійкості.

Значно складнішими є задачі захисту відкритих ключів, у нашому випадку це D_K, Y_A та Q_A. Це пояснюється тим, що відкриті ключі мають бути доступними всім користувачам, що виконують, наприклад, перевірку підписаних електронних документів, даних тощо. За таких умов необхідно забезпечити їх цілісність, справжність, доступність і неспростовність. Вирішення цієї задачі ґрунтується на використанні концепції сертифікатів відкритих ключів, причому для різних додатків – направленого шифрування, ЕЦП, криптографічного протоколу тощо.

Вирішення вказаних задач безпосередньо спочатку було пов'язано з рекомендаціями X.509 [13–14] Міжнародного союзу телекомунікації (ITU — International Telecommunication Union). Ці рекомендації є частиною рекомендацій серії X.500, що визначають стандарт служби каталогів. Каталог являє, по суті, сервер або розподілену систему серверів, що підтримують базу даних з інформацією про користувачів. Указана інформація містить відповідність імен користувачів та їхніх мережних адрес, а також інші атрибути користувачів.

Рекомендації X.509 визначають каркас схеми надання послуг автентифікації каталогом X.500 своїм користувачам. Каталог може служити сховищем сертифікатів відкритих ключів, що обговорювались. Причому кожен сертифікат містить

відкритий ключ користувача і підписується за допомогою особистого ключа надійного центру сертифікації. Також X.509 визначає альтернативні протоколи автентифікації, що будуються на використанні сертифікатів відкритих ключів. У подальшому рекомендації X.509 були прийнятими як міжнародний стандарт ISO/IEC 9594-8 | ITU-T Rec. Стандарт є важливим через те, що структура сертифікатів і протоколів автентифікації, обумовлених у X.509, використовується в багатьох випадках. Наприклад, формат сертифіката X.509 прийнятий у протоколах S/MIME, IP Sec, SET тощо.

Стандарт (рекомендації) X.509 був запропонований у 1988 році [51]. Його було переглянуто і виправлено деякі недоліки захисту інформації. Виправлені рекомендації були опубліковані в 1993 році. Проект третьої версії з'явився в 1995 році. Нині чинною, у тому числі в Україні, є версія ДСТУ ITU-T Rec. X.509 ISO/IEC 9594-8 «Основні положення сертифікації ключів та сертифікації атрибутів». Рекомендації цього стандарту (у подальшому рекомендації X.509) базуються на використанні методів криптографії з відкритим ключем і цифровими підписами. З 1 квітня 2008 року ISO/IEC 9594-8 | ITU-T Rec. X.509 прийнятий в Україні як національний стандарт і визначений як ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8 [14].

Але, як показала практика, стандарту X.509 було недостатньо, щоб створювати ІВК. З'явилася необхідність розробки та введення ряду Інтернет-рекомендацій RFC, основними з них є:

– RFC 2631 "Diffie-Hellman Key Agreement Method", June 1999;

– RFC 2785 Methods for Avoiding the «Small-Subgroup» Attacks on the Diffie-Hellman Key Agreement for S/MIME, March 2000;

– RFC 3279 "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002;

– RFC 3281 "An Internet Attribute Certificate Profile for Authorization", April 2002;

– RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002;

– RFC 3394 "Encryption Standard (AES) Key Wrap Algorithm", September 2002;

– RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004;

– RFC 4490 – Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001;

– Algorithms with Cryptographic Message Syntax (CMS), May 2006;

– RFC 5008 "Suite B in Secure/ Multipurpose Internet Mail Extensions (S/MIME)", September 2007;

– RFC 5480 "Elliptic Curve Cryptography Subject Public Key", March 2009;

– RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009.

Також на національному рівні було розроблено чи гармонізовано ряд міжнародних стандартів криптографічного захисту інформації, що дозволили побудувати систему ЕЦП в Україні. До них перш за все необхідно віднести:

– ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» [35];

– ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3. Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях» [21, 22];

– ДСТУ ISO/IEC 15946-3:2002 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів» [56];

– ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009) «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [38];

– ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції» [39] тощо.

Окрім того, знайшли застосування такі міждержавні стандарти, як:

– ГОСТ 34.310-95 (ДСТУ ГОСТ 34.310-2009) «Информационные технологии. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма» [40];

– ГОСТ 34.311-95 (ДСТУ ГОСТ 34.311-2009) «Информационная технология. Криптографическая защита информации. Функция хеширования» [41].

Але, незважаючи на відзначене, з'ясувалося, що названих стандартів недостатньо для реалізації системи ЕЦП в Україні, перш за все для забезпечення взаєморозуміння між різними розробниками та постачальниками. Необхідно було розробити, узгодити й затвердити ряд технічних специфікацій форматів представлення базових об'єктів, у першу чергу [57–60]:

– Технічні специфікації форматів представлення базових об'єктів. Формат підписаних даних;

– Технічні специфікації протоколів взаємодії. Протокол визначення статусу сертифікату;

– Технічні специфікації протоколів взаємодії. Протокол фіксування часу;

– Технічні специфікації форматів криптографічних повідомлень.

Тільки з прийняттям указаних специфікацій з'явилася можливість створювати уніфіковані центри сертифікації ключів. Але це дорого коштувало для розробників і власників центрів, особливо для тих, у кого засоби КЗІ реалізовані у вигляді апаратно-програмних або апаратних засобів.

Ця монографія складається з 13 глав та ряду додатків. Викладений тут матеріал отримано авторами за останні 12 років у процесі участі в проектуванні, експертизі, впровадженні й застосуванні інфраструктур відкритих ключів, включаючи системи ЕЦП в Україні. У монографії подано стан, сутність і сучасні проблемні питання теорії та практики аналізу, синтезу й застосування в цілому ІВК та системи ЕЦП в інформаційних та інформаційно-телекомунікаційних системах різноманітного призначення. У главах 1–5 розглядаються питання класифікації, вимоги та сутність криптографічних перетворень типу «Електронний цифровий підпис» та «Направлене шифрування», наведено методики та результати порівняльного аналізу існуючих систем електронного цифрового підпису, подано відповідні рекомендації та пропозиції. У главах 6–9 наводяться результати класифікації, обґрунтування вимог і порівняльного аналізу механізмів і криптографічних протоколів на основі електронного цифрового підпису, а також розглядаються питання створення та характеристики інфраструктур відкритих ключів

технологічно розвинених держав і національної системи електронного цифрового підпису. Глави 10–13 присвячені обґрунтуванню вимог до засобів криптографічних перетворень для ІВК, розробці принципів проектування і технологій виготовлення й застосування таких засобів, аналізу перспективних політик сертифікації ключів. Також розглядається ряд проблемних питань розвитку ІВК і національної системи електронного цифрового підпису та можливі шляхи їх вирішення. У додатку А ми вважаємо за необхідне навести сучасний математичний апарат перетворень у групі точок еліптичних кривих (базуючись здебільшого на [32]).

Монографія адресована в першу чергу розробникам систем ІВК, спеціалістам, що пов'язані з експлуатацією та застосуванням інфраструктур з відкритими ключами в інформаційних та інформаційно-телекомунікаційних системах, розробникам систем, комплексів і засобів криптографічного захисту, підготовки аспірантів, магістрів і бакалаврів у галузі «Інформаційна безпека», користувачів сучасними інформаційно-телекомунікаційними системами, системами електронних документів і електронного документообігу. Ми сподіваємося, що монографія послугує подальшому розвитку національної системи електронного цифрового підпису, її трансформації в ІВК, що є традиційною в технологічно розвинених державах, вирішенню завдань взаємодії на міжнародному та міждержавному рівнях.

Висловлюємо подяку ректору Харківського національного університету радіоелектроніки, члену-кореспонденту Національної академії наук України професору Бондаренко М.Ф за спонукання та підтримку в написанні монографії, генеральному директору ЗАТ «Інститут інформаційних технологій» Сінаюку С.Ю. за підтримку та фінансове забезпечення видання. Ряд результатів, наведених у монографії, на які є посилання, були отримані разом зі співробітниками кафедри й аспірантами, а також співробітниками ЗАТ «Інститут інформаційних технологій» під час спільної роботи.

Безумовно, велика подяка Ганні Миколаївні та Ользі Миколаївні Горбенко, які терпіли та підтримували нашу роботу над монографією останні два роки.

Дуже вдячні рецензентам монографії:

– доктору технічних наук, професору, Заслуженому діячу науки і техніки, Лауреату державної премії, начальнику спеціальної кафедри інституту державної служби спеціального зв'язку та захисту інформації НТТУ КПІ Скрипнику Леоніду Васильовичу;

– доктору технічних наук, професору, Заслуженому діячу науки і техніки, заступнику начальника Харківського університету Повітряних Сил ім. І. Кожедуба Стасєву Юрію Володимировичу;

– доктору технічних наук, професору, Заслуженому винахіднику України, декану факультету комп'ютерних наук Харківського національного університету ім. Каразіна Сороці Леоніду Степановичу.

Будемо вдячні всім за висловлені зауваження та побажання щодо матеріалу та результатів, наведених у монографії.