НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ

Кафедра інформаційної політики та електронного урядування

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ ТА ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник

Київ
2015

Національна академія державного управління
при президентові України

Кафедра інформаційної політики
та електронного урядування

КУКАРІН О.Б.

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ ТА ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник

Київ
2015

УДК 004.031:55(035)

Е 45

Рекомендовано Вченою радою Національної академії державного управління при Президентові України (протокол № 193/5-7 від 7 червня 2014 р.).

Автор:
О.Б. Кукарін, кандидат технічних наук, доцент, доцент кафедри інформаційної політики та електронного урядування Національної академії державного управління при Президентові України.

Рецензенти:
В.Д. Бакуменко, доктор наук з державного управління, професор, заслужений діяч науки і техніки України, проректор з наукової роботи Академії муніципального управління;
О.А. Загаєцька, кандидат технічних наук, головний спеціаліст Секретаріату Кабінету Міністрів України.

Загальна редакція:
Н.В. Грицяк - доктор наук з державного управління, професор, заслужений діяч науки і техніки України, завідувач кафедри інформаційної політики та електронного урядування Національної академії державного управління при Президентові України

Електронний документообіг та захист інформації: навч.
Е 45 посіб./ О.Б. Кукарін / За заг. ред. д.держ.упр., професора Н.В. Грицяк – К.: НАДУ, 2015. – 84 с.

У навчальному посібнику розкриваються основні теми навчальної дисципліни “Електронний документообіг та захист інформації”, зміст та основні принципи електронного документообігу. Викладено організаційні та інформаційно-технологічні аспекти запровадження та функціонування електронного документообігу та електронного цифрового підпису в системі державного управління. Особливу увагу приділено принципам та методам захисту інформації в умовах електронного урядування.

Навчальний посібник призначений для слухачів спеціальності “Електронне урядування” напряму підготовки “Державне управління”. Він буде корисним також для студентів інших вищих навчальних закладів, викладачів, працівників органів державної влади і органів місцевого самоврядування.

УДК 004.031:55(035)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС	автоматизована система
АСЕД	автоматизована система електронного документообігу
АЦСК	акредитований центр сертифікації ключів
ВК	відкритий ключ
ЕД	електронний документ
ЕДО	електронний документообіг
ЕП	електронна печатка
ЕЦП	електронний цифровий підпис
ІВК	інфраструктура відкритого ключа
ІР	інформаційний ресурс
ІС	інформаційна система
ІСЕД	інтегрована система електронного документообігу
ІТС	інформаційно-телекомунікаційна система
КЗЗІ	комплексні засоби захисту інформації
КЗІ	криптографічний захист інформації
КО	контролюючий орган
КСЗІ	комплексна система захисту інформації
НСД	несанкціонований доступ
НСКЗ	національна система конфіденційного зв’язку
ОК	особистий ключ
ОС	операційна система
ПБ	політика безпеки
ПЗ	програмне забезпечення
ПСВК	посилений сертифікат відкритого ключа
СВК	сертифікат відкритого ключа
СЕДО	система електронного документообігу
СЗІ	служба захисту інформації
СКД	система контролю доступу
СКУД	система контролю і управління доступом
ТЗІ	технічний захист інформації
ЦЗО	центральний засвідчувальний орган
ЦСК	центр сертифікації ключів

ВСТУП

Документообіг стає по справжньому електронним, коли в ньому зникають сканери, а з програмного забезпечення вилучається функція "ДРУК"

Управлінська діяльність органів державної влади та органів місцевого самоврядування здійснюється шляхом видання організаційно-розпорядчих документів. Документація використовується як спосіб і засіб реалізації функцій управління. При цьому в документах зосереджується інформація, яку необхідно надійно зберігати протягом певного часу.

Останнім часом суттєво ускладнилися функції управління та зросли обсяги завдань, які покладені на органи державної влади, змінюються вимоги до якості документів. Одночасно активно впроваджуються інформаційних технологій як засоби автоматизації процесів, що пов'язані з документованою інформацією. Крім того, в законодавстві з'явилися нові юридичні об'єкти – електронний документ та електронний цифровий підпис, розвиваються нові форми відносин, що базуються на електронному документообігу.

На порядок денний в Україні постало питання інтенсифікації впровадження і розвитку електронного урядування в усіх сферах життя суспільства, однією з важливих складових якого є електронний документообіг. Це дасть змогу отримати такі важливі якості державного управління, як оперативність обміну електронними документами, можливість їх дистанційного опрацювання, погодження і підписання, забезпечить накопичення і загальну доступність масивів документів, зробить цілком природнім створення і використання електронних архівів.

В посібнику систематизовано викладено основні засади створення та використання електронних документів. Розглянуті принципи організації та функціонування систем електронного документообігу, їх загальна класифікація, сучасний стан та тенденції розвитку. Розкриті основи технології застосування електронного цифрового підпису. Особливу увагу приділено проблемам комплексного захисту інформації в інформаційно-телекомунікаційних системах.

Всі аспекти розглядаються, переважно, з точки зору застосування відповідної нормативно-правової бази.

Посібник призначений для слухачів, які набувають кваліфікацію керівників організаційних систем електронного урядування і може бути корисним іншим фахівцям у сфері державного управління.

1. ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ ТА ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ

1.1. Поняття електронного документа та електронного документообігу

В основу інформаційно-аналітичного забезпечення роботи організації передусім покладено опрацювання документів, які підлягають створенню, фіксуванню та обліку в певній формі.

Документи використовуються в різних галузях знань, сферах людської діяльності й суспільного життя. Вони є об'єктом дослідження різних наукових дисциплін і тому поняття документ багатозначне і залежить від того, у якій галузі й для чого воно використовується.

Відповідно до ст. 1 Закону України "Про інформацію" [43] **документ** – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

В інших джерелах документ визначається як структурована одиниця інформації, призначена для сприйняття людиною і оформлена та зафіксована на матеріальному носієві в установленому порядку з дотриманням певної форми її подання та формуванням обов'язкових ознак:

функціональності – визначеності в межах існуючих суспільних відносин очікуваного впливу документа (в тому числі подальшого порядку дій) на його одержувачів після отримання та ознайомлення із вмістом;

санкціонованості – визначеності фізичної і/або юридичної особи, яка відповідає у певний час за існування документа;

реєстрованості – визначеності унікальної ідентифікації документа у множині документів.

Статтею 5 Закону України "Про електронні документи та електронний документообіг" [40] визначено, що **електронний документ** (ЕД) – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, склад та порядок розміщення яких визначається законодавством. При цьому ЕД може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму подання шляхом відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною. Обов'язковими реквізитами ЕД є дані, без яких він не може бути підставою для його обліку і не матиме юридичної сили.

Відповідно до ст. 6 зазначеного Закону України обов'язковим реквізитом ЕД є *електронний підпис*, який використовується для

ідентифікації автора та/або підписувача ЕД іншими суб'єктами електронного документообігу і дає змогу підтвердити його цілісність. Накладанням *електронного цифрового підпису* (ЕЦП) завершується створення ЕД. Однак необхідно зауважити, що лише ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки), а інші види електронного підпису такого статусу не мають.

Оригіналом ЕД відповідно до ст. 7 цього Закону вважається електронний примірник документа з обов'язковими реквізитами, в тому числі з ЕЦП автора. При цьому в разі надсилання ЕД кільком адресатам або його зберігання на кількох електронних носіях інформації, кожний з електронних примірників вважається оригіналом ЕД. Якщо автором створюються ідентичні за документарною інформацією та реквізитами ЕД та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу. Електронна копія ЕД засвідчується в порядку, встановленому законом. Копією документа на папері для ЕД є його візуальне подання на папері, яке засвідчене в порядку, встановленому законодавством.

Статус ЕД визначається його реквізитом, що набирає таких значень:

версія – примірник ЕД на стадії створення, який відрізняється від інших його примірників порціями вмісту;

оригінал – примірник ЕД, який першим набуває чинності, що зазначається в процесі реєстрації відповідним значенням спеціального реквізиту;

дублікат – примірник ЕД, який має юридичну силу оригіналу;

копія – примірник ЕД, який точно відтворює вміст його оригіналу, а також усі його реквізити чи їх частину;

витяг (з ЕД) – копія ЕД, яка відтворює частину всіх його структур і частину порцій вмісту.

Статтею 8 цього Закону визначено, що юридична сила ЕД не може бути заперечена виключно через те, що він має електронну форму, а також випадки, коли ЕД не може бути застосований як оригінал: свідоцтва про право на спадщину; документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів ЕД; в інших випадках, передбачених законом.

Життєвий цикл ЕД становлять чотири стадії: створення, поширення, виконання та використання, які реалізуються і забезпечуються як сукупність послідовних процесів за допомогою комп'ютерів та засобів зв'язку. При цьому виконання операцій із реалізації процесів відбувається автоматично або керується користувачами відповідних інформаційно-телекомунікаційних систем.

Технології створення ЕД дають змогу не тільки застосовувати їх нарівні із документами на папері, а й отримати якісно нові можливості їх

опрацювання. Головною з них є суттєве підвищення оперативності документообігу в діяльності суб'єктів, а також можливість укладання угод та інших правочинів з використанням інформаційних технологій через загальнодоступні телекомунікаційні канали, тобто дистанційно.

Термін "документаційне забезпечення управління" (діловодство) увійшов до наукового та практичного обігу приблизно з середини 1970-х рр. у зв'язку зі зміною його організаційно-технічної основи і методологічних підходів до вдосконалення завдяки активному впровадженню у сферу роботи з документами засобів обчислювальної техніки і появі нових інформаційно-телекомунікаційних технологій.

Діловодство розглядається як галузь діяльності, що забезпечує створення офіційних документів і організацію роботи з ними, а саме організацію руху документів з моменту їх створення або отримання до завершення виконання: відправку з організації і (чи) безпосередньо в архів.

У широкому розумінні документообіг можна визначити як інформаційну діяльність суб'єктів інформаційних відносин, що реалізується шляхом виконання певних дій над документами.

Під **системою документообігу** розуміється сукупність методів, засобів і персоналу, що підтримує документообіг у межах встановленого регламенту документообігу.

Система автоматизації документообігу (система електронного документообігу) – організаційно-технічна система, що забезпечує процес створення, управління доступом і поширення електронних документів у комп'ютерних мережах, а також контроль над потоками документів в організації.

Особливе значення має *регулювання (регламентування) документообігу*, яке пов'язане з електронними документами.

Регламент документообігу являє собою сукупність правил інформаційної діяльності суб'єктів інформаційних відносин, визначених законодавством, нормативними актами або угодами. Регламент документообігу визначає ролі та права суб'єктів щодо створення, володіння, користування та розпорядження документами, порядок оформлення і фіксації інформації на носієві інформації.

Як узагальнене поняття ***електронний документообіг*** (ЕДО) можна тлумачити як інформаційні технології, що реалізують життєвий цикл електронного документа. При цьому систему електронного документообігу (СЕДО) можна визначити як автоматизовану систему оброблення інформації, що реалізує ЕДО та спряжену з іншими системами документообігу.

Необхідність застосування електронних документів і використання можливостей, що надає електронний документообіг для різноманітних суспільних потреб, в Україні стала на порядку денному ще в другій

половині 90-х років минулого XX століття. До цього спонукав також і позитивний суспільний досвід розвинених країн у цій сфері. Але на той час не тільки в українському суспільстві в цілому, а й навіть в органах державної влади ще не було наявної матеріально-технічної бази та достатнього усвідомлення обсягу і складності тих завдань, які необхідно вирішити для досягнення зазначеної мети.

Зазначеними законами було визначено основні поняття та терміни у сфері електронного документообігу:

адресат – фізична або юридична особа, якій адресується електронний документ;

дані – інформація, яка подана у формі, придатній для її оброблення електронними засобами;

посередник – фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;

електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа;

обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

автор електронного документа – фізична або юридична особа, яка створила електронний документ;

електронний документообіг *(обіг електронних документів)* – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та в разі необхідності з підтвердженням факту одержання таких документів;

суб'єкти електронного документообігу – автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Слід виокремити такі *основні принципи та завдання електронного документообігу*:

– одноразова реєстрація документа, що дозволяє однозначно його ідентифікувати у будь-якій підсистемі;

– можливість паралельного виконання операцій, що дає змогу скоротити час руху документів і підвищити оперативність їх виконання;

– безперервність руху документа, що дозволяє ідентифікувати відповідального за його виконання (завдання) в кожен момент часу життєвого циклу документа (процесу);

– єдина (або погоджено розподілена) база документної інформації, унеможливлює дублювання документів;

– ефективно організована система пошуку документів, що забезпечує пошук документів, володіючи мінімальною інформацією про них;

– розвинена система звітності при різних статусах і атрибутах документів, що дає змогу контролювати їх рух по процесах документообігу і приймати управлінські рішення, ґрунтуючись на даних зі звітів.

1.2. Правові аспекти електронного документообігу в системі державного управління

Для запровадження електронного документообігу (ЕДО) перед органами влади, передусім, постало завдання зі створення нормативно-правової бази, що забезпечує його здійснення шляхом належної організації відповідних процесів та дотримання вимог до оформлення документів, уніфікації систем організаційно-розпорядчої документації, розроблення єдиної державної системи діловодства, єдиної державної системи документаційного забезпечення управління тощо. Це також мало стати основою для врегулювання відносин між суб'єктами в таких якісно нових сферах діяльності, як електронна комерція, електронна торгівля, подання електронної звітності, надання електронних (адміністративних) послуг через спеціалізовані інформаційні системи та загальнодоступні мережі, зокрема Інтернет.

З цією метою були прийняті два базових закони України: "Про електронний цифровий підпис" [41] та "Про електронні документи та електронний документообіг" [40]. При цьому слід зазначити, що положення першого з цих законів відповідають вимогам Директиви 1999/93/ЕС Європейського Парламенту та Ради Європи від 13 грудня 1999 року "Про систему електронних підписів, що застосовується в межах Співтовариства" [38]. З прийняттям зазначених законів за умови дотримання певних вимог електронний цифровий підпис було прирівняно за правовим статусом до власноручного підпису (печатки), встановлено основні організаційно-правові засади використання електронного документа та застосування ЕДО.

Законом України "Про електронні документи та електронний документообіг" [40] регулюються відносини, пов'язані з відправленням, передаванням та одержанням електронного документа. Зокрема, відправлення та передавання електронного документа здійснюються автором або посередником в електронній формі за допомогою засобів інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ. При цьому

електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про його одержання, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами ЕДО. Перевірка цілісності електронного документа проводиться шляхом перевірки справжності накладеного на нього електронного цифрового підпису.

На виконання зазначених законів Кабінет Міністрів України прийняв низку постанов, які конкретизували врегулювання відносин у цій сфері, зокрема:

– "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу" [48];

– "Про затвердження Порядку акредитації центру сертифікації ключів" [49];

– "Про затвердження Положення про центральний засвідчувальний орган" [50];

– "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" [51];

– "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади" [52];

– "Про затвердження Порядку обов'язкової передачі документованої інформації" [53].

Зазначені постанови поряд з іншим спрямовані на створення і розвиток в Україні ***інфраструктури відкритого ключа*** (англ. *PKI – Public Key Infrastructure*) для забезпечення використання електронного цифрового підпису, насамперед створення її суб'єктів – ***центрального засвідчувального органу*** та ***контролюючого органу***, а також ***засвідчувальних центрів***. Створення й забезпечення діяльності інших суб'єктів цієї інфраструктури – ***центрів сертифікації ключів***, у тому числі й ***акредитованих центрів сертифікації ключів***, здійснюється представниками бізнесу.

Затверджений Постановою Кабінету Міністрів України "Типовий порядок здійснення електронного документообігу в органах виконавчої влади" [52] встановлює загальні правила документування в органах влади управлінської діяльності в електронній формі і регламентує виконання дій з електронними документами з моменту їх створення або одержання до відправлення чи передачі до відповідного архіву. При цьому всі інші дії з електронними документами виконуються в органі влади згідно з вимогами до дій з документами на папері, передбаченими інструкцією з діловодства цього органу. Дія Типового порядку поширюється на всі електронні документи, що створюються або одержуються органом влади.

При цьому кожен державний орган влади, орган місцевого самоврядування, підприємство, установа або організація незалежно від форми власності конкретизує для своїх потреб загальні правила документування в електронній формі і регламентує виконання дій з електронними документами згідно з законодавством.

Орган влади здійснює ЕДО лише за умови використання надійних засобів електронного цифрового підпису (ЕЦП), що має бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації (КЗІ), одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів (ПСВК) у своїх працівників – підписувачів. При цьому ЕДО здійснюється органом влади через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування, а відправлення електронних документів через телекомунікаційні мережі загального користування здійснюється за рішенням керівника цього органу.

Згідно із законодавством система електронного документообігу (СЕДО) органу влади повинна відповідати вимогам нормативно-правових актів у сфері захисту інформації. Зокрема, це стосується положень Закону України "Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [42] та Постанови Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [54].

Створення архівів електронних документів, подання їх до архівних установ України та зберігання в цих установах здійснюється в порядку, визначеному законодавством. Зокрема, наказом Державного комітету архівів України було затверджено "Порядок зберігання електронних документів в архівних установах" [69].

Іншими рішеннями уряду, нормативно-правовими актами і нормативними документами центральних органів виконавчої влади було врегульовано ще низку юридичних, організаційних і технічних питань, але на сьогодні нагальні проблеми у цій сфері поки що вирішені не повністю.

Основою для врегулювання питань діловодства стала Постанова Кабінету Міністрів України "Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади" [45]. Примірна інструкція визначає порядок ведення загального діловодства, а її положення поширюються на всю службову документацію, в тому числі створювану за допомогою персональних комп'ютерів. Комп'ютерні (автоматизовані) технології обробки

документної інформації повинні відповідати вимогам державних стандартів, а також зазначеної інструкції.

Згідно з Примірною інструкцією відповідальність за організацію діловодства в установі несе керівник установи. Ведення діловодства відповідно до вимог державних стандартів, цієї Примірної інструкції та інструкцій з діловодства установ покладається на управління справами, загальні відділи, канцелярії або секретарів.

При цьому основним завданням діловодної служби є встановлення єдиного порядку документування і роботи з документами в установі на основі використання сучасної комп'ютерної техніки, автоматизованої технології роботи з документами та скорочення кількості документів.

Низка положень Примірної інструкції певною мірою вже закладала основу для впровадження в установах СЕДО. Зокрема, в них зазначалося, що механізація і автоматизація діловодних процесів є обов'язковою умовою раціональної організації діловодства в кожній установі, засобом підвищення продуктивності і здешевлення управлінської праці і повинні здійснюватися на основі впорядкованої системи документування управлінської діяльності, уніфікації та скорочення кількості форм використовуваних документів. Крім того, ці заходи вживаються на всіх етапах діловодного процесу: підготовки документів, їх копіювання, оперативного зберігання і транспортування, контролю за виконанням тощо, а засоби механізації і автоматизації діловодних процесів мають бути сумісними і передбачати можливість об'єднання в єдину систему.

У Примірній інструкції також зазначено, що комплекс технічних засобів повинен забезпечувати збирання і передачу інформації, її запис на машинні носії, введення інформації в персональний комп'ютер, виведення результатів, її обробку у формі машино- або відеограм, сумісність з іншими інформаційними системами, а також можливість об'єднання в єдину інтегровану систему. При цьому під час упровадження нових технологій роботи з документами необхідно враховувати:

– доцільність упровадження технічних засобів;

– можливість придбання технічних засобів у певні терміни;

– наявність придатних приміщень;

– необхідність залучення спеціалістів до обслуговування техніки тощо.

Відповідальність за ефективність використання механізованої і автоматизованої технології роботи з документами несе керівник установи.

Опрацювання документів в установі здійснюється за типовими схемами відповідно для вхідних, внутрішніх і вихідних документів. Зокрема, при опрацюванні вхідного документа виділяються такі етапи: отримання, попередній розгляд, реєстрація, доповідь керівництву, організація виконання – призначення виконавців та постановка завдань,

здійснення діловодного контролю за перебігом та наслідками виконання, закінчення справи (кінцеве оформлення) та направлення на зберігання.

Усі дії з електронним документом, якщо це не стосується специфіки їх створення або одержання до відправлення чи передачі до архіву, виконуються в установах згідно з вимогами до дій з документами на папері, передбаченими інструкціями з діловодства цих органів.

1.3 Електронний документообіг за умов електронного урядування

На сьогодні одним із пріоритетів України є розвиток інформаційного суспільства з його важливішою складовою – електронним урядуванням, впровадження якого сприятиме створенню умов для ефективного відкритого і прозорого державного управління.

Кабінет Міністрів України своїм розпорядженням [60] схвалив Концепцію розвитку електронного урядування в Україні. Згідно з Концепцією електронне урядування визначене як форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян.

В Концепції також зазначено, що незважаючи на стрімкий розвиток інформаційно-комунікаційних технологій та широке застосування їх у державному управлінні протягом останнього десятиліття, не розв'язаними залишаються такі проблеми:

– відсутність єдиних стандартів та регламентів функціонування системи ЕДО з використанням ЕЦП, а також ведення державних інформаційних ресурсів, адаптованих до міжнародних;

– обмеженість можливостей СЕДО органів державної влади та органів місцевого самоврядування;

– відсутність єдиних форматів та протоколів ЕЦП.

При цьому з урахуванням переваг технологій, що застосовуються в електронному урядуванні, завданнями із забезпечення його розвитку в Україні, зокрема, є:

– організація інформаційної взаємодії органів державної влади та органів місцевого самоврядування на базі ЕДО з використанням ЕЦП;

– забезпечення передачі і довгострокового зберігання електронних документів у державних архівах, музеях, бібліотеках, підтримки їх в актуалізованому стані та доступу до них.

Реалізація Концепції передбачена на певний період та складається з трьох основних етапів.

На першому етапі передбачається:

– розроблення необхідної нормативно-правової та нормативно-технічної бази, зокрема щодо надання адміністративних послуг в електронній формі, а також єдиних стандартів, протоколів і регламентів взаємодії суб'єктів електронного урядування, їх гармонізація з міжнародними стандартами;

– створення єдиної загальнодержавної СЕДО.

На другому етапі планується, зокрема, забезпечити передачу електронних документів у державні архіви, музеї, бібліотеки, їх довгострокове зберігання, підтримка в актуалізованому стані та надання доступу до них.

Таким чином, в Концепції чітко зазначається, що впровадження СЕДО є важливою складовою розвитку електронного урядування.

Слід відмітити, що з розвитком завдань та технологій електронного урядування ЕДО поширюється на всі сфери діяльності держави й забезпечує взаємодію між органами влади всіх рівнів та гілками (G2G), органами влади та бізнес-структурами (G2B), органами влади та громадянами (G2C). При цьому такі взаємодії виходять за межі обміну лише документами і виникає необхідність обміну даними (інформацією) у різних її формах та застосуваннях, що, безумовно, є більш складним в організаційному та науково-технічному сенсі.

Завдання зі створення єдиної загальнодержавної СЕДО в першому наближенні реалізуються шляхом запровадження *системи електронної взаємодії органів виконавчої влади* [61].

Система призначена для виконання таких функцій:

– формування єдиного інформаційного простору для обміну, обробки та зберігання організаційно-розпорядчих документів в електронному вигляді, що є передумовою подальшого створення центрального електронного архіву документів;

– прийом/передача організаційно-розпорядчих електронних документів Секретаріату Кабінету Міністрів та центральних органів виконавчої влади;

– організація погодження проектів нормативних актів між центральними органами виконавчої влади;

– контроль виконання доручень Секретаріату Кабінету Міністрів, погодження проектів нормативних документів Кабінету Міністрів України;

– посилення контролю за виконанням організаційно-розпорядчих документів;

– підвищення оперативності прийняття управлінських рішень;

– створення передумов для переходу на внутрішній електронний документообіг у відомстві з використанням виключно електронного документа.

Основні характеристики системи:

– Web-орієнтована архітектура. Робота із системою здійснюється за допомогою стандартного Web-браузера. Користувачі можуть працювати в системі в будь-який час і в будь-якому місці, для цього необхідний тільки комп'ютер, що підключений до мережі Інтернет;

– єдине сховище документів. Після розміщення на файловому сервері документ доступний адресатам та не потребує переміщення між ними, що дає змогу всім користувачам, яким адресований документ, спільно над ним працювати;

– інтеграція із СЕД за узгодженим форматом (наказ Міністерства освіти і науки, молоді та спорту України від 20 жовтня 2011 р. № 1207 [66]).

Одним з найважливіших завдань, яке необхідно вирішити при обміні даними (документами) між учасниками інформаційної взаємодії, є сумісність даних для різних систем. Це регламентується вимогами до форматів даних електронного документообігу в органах державної влади, затвердженими наказом Міністерства освіти і науки, молоді та спорту України № 1207 від 20 жовтня 2011 р. [66].

Цим наказом установлюються вимоги до електронного повідомлення, що застосовуються під час створення систем електронного документообігу органів державної влади та/або при забезпеченні їх взаємодії, які є обов'язковими при організації електронної взаємодії всіх органів влади.

Основний зміст вимог такий.

Програмне забезпечення, що реалізує необхідний формат, може бути окремим автономним рішенням або інтегроване у внутрішню систему електронного документообігу як його складова частина.

Електронне повідомлення є XML-документом із встановленою цими Вимогами структурою і складом елементів та їх атрибутів. Електронне повідомлення передається із системи електронного документообігу відправника в систему електронного документообігу одержувача у вигляді файла.

XML-документ – текстовий документ, сформований у повній відповідності зі стандартом XML. Він складається з прологу, одного кореневого елемента XML, коментарів, декларації типів даних і символів.

Електронне повідомлення – це XML-файл, у який відповідно до вимог вкладаються електронний документ та метадані. Воно в цілому та його складові частини можуть бути незалежно засвідчені електронними цифровими підписами та (або) зашифровані.

Відправник електронного повідомлення – система електронного документообігу (СЕД), ініціатор інформаційної взаємодії, яка формує і надсилає електронне повідомлення до іншої СЕД.

Одержувач електронного повідомлення – СЕД, яка під час інформаційної взаємодії отримує електронне повідомлення і забезпечує його обробку.

Основний документ може мати додаткові матеріали – документ або сукупність документів, інформація яких роз'яснює, уточнює окремі питання тощо.

Мова XML (Extensible Markup Language) – розширювана мова розмічання даних. Стандарт на структурований опис даних, орієнтований, зокрема, на обмін інформацією між незалежними учасниками, запропонований консорціумом World Wide Web.

Документ повинен мати обов'язкові реквізити – дані в електронному документі, без яких він не може бути підставою для обліку і не матиме юридичної сили.

Контрольні питання

1. Визначення електронного документа та його основних ознак.
2. Ознаки статусу електронного документа.
3. Життєвий цикл електронного документа.
4. Поняття електронного документообігу.
5. Основні терміни у сфері електронного документообігу.
6. Основні принципи та задачі електронного документообігу.
7. Мета базових законів, що регламентують електронний документообіг.
8. Особливості електронного документообігу в у мовах електронного урядування.
9. Сутність системи електронної взаємодії органів виконавчої влади.
10. Рішення стосовно уніфікації та стандартизації форматів електронних повідомлень.
11. Пріоритетні напрями впровадження систем електронного документообігу в сферу державного управління.
12. Державне регулювання у сфері електронного документообігу.

2. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

2.1. Поняття та визначення електронного цифрового підпису

Статтею 1 Закону України “Про електронний цифровий підпис” [41] визначено такі терміни:

електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

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;

засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

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 або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

акредитація – процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов’язану з обслуговуванням посилених сертифікатів ключів;

компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування сертифіката ключа – тимчасове зупинення чинності сертифіката ключа;

підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

послуги електронного цифрового підпису – надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється в порядку, визначеному законодавством.

Власноручний підпис та електронний цифровий підпис

Документ у традиційному розумінні цього поняття передбачає наявність носія інформації, за допомогою якого забезпечується сприймання інформації тільки органами чуттів людини (зір, слух тощо).

Підпис, який проставляється автором документа на папері (власноручний підпис), – це рукописне, та іноді графічно стилізоване ім'я або інший графічний знак, що ідентифікує автора (підписувача), і означає його згоду зі змістом документа. Перевірка справжності власноручного підпису здійснюється шляхом його візуального звірення з оригіналом, який зафіксований у встановленому порядку. За необхідності для офіційної перевірки підпису може бути здійснена відповідна експертиза.

На відміну від документа на папері, електронний документ (ЕД) дуже легко може бути підданий різним змінам. Тому, для гарантії забезпечення можливості здійснення контролю справжності підпису, накладеного на ЕД, необхідно застосовувати відповідний механізм, який дає змогу однозначно визначити, чи вносилися будь-які несанкціоновані автором зміни до вмісту ЕД після його підписання.

Накладання підпису на ЕД шляхом графічного відтворення власноручного підпису не може слугувати підтвердженням того, що документ санкціонований підписувачем, оскільки графічний образ може бути скопійований і проставлений під будь-яким текстом або іншим елементом ЕД, і тим самим підписувачу буде приписане незаконне авторство "документа.

Для ЕД повним аналогом власноручного підпису під документом на папері на сьогодні є електронний цифровий підпис (ЕЦП), застосування

якого реалізується за допомогою інформаційних технологій і здійснюється шляхом певних криптографічних перетворень над ЕД (набором електронних даних), на основі яких відтворюється вміст цього ЕД. За визначених законодавством умов ЕЦП прирівнюється до власноручного підпису і має однакову з ним юридичну силу.

Ключі електронного цифрового підпису

Технологія застосування ЕЦП базується на методах криптографії. З цієї сфери було привнесено термін "ключ", тобто набір двійкових даних фіксованої довжини. У практичній криптографії використовується пара пов'язаних між собою ключів – ключ для шифрування і, відповідно, для дешифрування. Зазначені дані слугують параметрами для відповідних алгоритмів криптографічних перетворень. У сфері застосування ЕЦП використовується аналогічна пара – особистий ключ (ОК) і відкритий ключ (ВК), перший з якої застосовується для накладання підпису, а другий – для його перевірки. Ця пара ключів створюється шляхом їх генерації за допомогою засобів ЕЦП на основі алгоритмів отримання випадкових чисел великої розрядності. При цьому до надійного засобу ЕЦП висувається, зокрема, вимога, з якою за його допомогою пара ключів може бути практично згенерована лише один раз, а їх захищеність має бути достатньо гарантованою – зокрема після перенесення ключів, згенерованих за допомогою цього засобу, на зовнішній носій інформації. Ці дані в такому засобі (наприклад персональний комп'ютер) будуть знищені, тобто стануть у подальшому недоступними. Крім того, технології використання надійного засобу ЕЦП повинні забезпечувати з достатньою гарантованістю, що ключі не можуть бути отримані похідними способами, а сам підпис є захищеним від підробки шляхом використання наявних інформаційних технологій.

Слід зазначити, що терміну "*особистий ключ*", тобто ключ, який повинен використовуватися особисто, із закриттям доступу до нього інших осіб, в англійській мові відповідає термін – "*private key*".

Важливість значення ОК у застосуванні ЕЦП підкреслюється у відповідних положеннях законодавства. Зокрема, відповідно до статті 7 Закону України "Про електронний цифровий підпис" [41], підписувач (власник ОК) зобов'язаний зберігати ключ у таємниці, а відповідно до статті 8 – зберігання ОК підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

У законодавстві немає вимоги до форми зберігання ВК, за допомогою якого перевіряється ЕЦП. Він може зберігатися, зокрема, на папері – у вигляді запису відповідного коду, а також на традиційних електронних носіях інформації – дискетах, дисках, флеш-картах, апаратних носіях тощо. На сьогодні на ринку присутні, апаратні носії ключової інформації, які призначені, зокрема, для збереження і

використання ВК та апаратної реалізації криптографічних перетворень, і які виготовляються у формі, що зовні виглядає як флеш-картка з USB-інтерфейсом. Апаратні носії ключової інформації забезпечують захищеність процесу виконання криптографічних перетворень, які здійснюються з використанням ОК, та унеможливлюють доступ до нього з боку апаратно-програмного середовища комп'ютера. За допомогою апаратного носія можуть генеруватися та зберігатися в ньому ОК та ВК підписувача. При цьому ОК підписувача зберігаються у внутрішній пам'яті апаратного носія, де забезпечується їх захист від несанкціонованого доступу.

Національний банк України своїм листом [72] рекомендував банкам України розглянути питання щодо зменшення ризиків під час використання інформаційних технологій та програмно-технічних комплексів банків, зокрема, шляхом використання ряду апаратних носіїв ключової інформації систем криптографічного захисту інформації і погодив використання цих апаратних носіїв у системі криптографічного захисту інформації Національного банку.

Захищеність електронного цифрового підпису

Захищеність ЕЦП від відтворення чи підробки базується на застосуванні у відповідних технологіях методів криптографії. Так, у разі застосування алгоритму, визначеного ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" [75], для формування та перевіряння електронного цифрового підпису з довжиною ключа у 264 біти тривалість часу, необхідного для його можливого "зламування" шляхом застосування найсучасніших методів криптоаналізу з допомогою комп'ютера із частотою процесора у 3 ГГЦ, експерти оцінюють величиною майже 1 тис. років. Тобто такий тривалий час і лежить в основі гарантії стійкості ЕЦП. Крім того, додатковою перешкодою для зловмисників, які можуть здійснити спробу "зламування" ОК, є те, що термін його використання обмежується (як правило, не більше року) і підписувач періодично замінює ОК (одночасно з ним і ВК). Підписувач також може замінювати ОК і достроково – за наявності підозри про його компрометацію, тобто виникнення ситуації, коли існує ймовірність того, що він став доступним іншій особі (особам).

Правовий статус електронного цифрового підпису

Відповідно до статті 1 Закону України "Про електронний цифровий підпис" [41] ЕЦП накладається на набір електронних даних, який додається до цього набору або логічно з ним поєднується. Відповідно до статті 6 Закону України "Про електронні документи та електронний документообіг" [40] електронний підпис є обов'язковим реквізитом ЕД,

який використовується для ідентифікації автора та/або підписувача ЕД іншими суб'єктами електронного документообігу. Слід зазначити, що використання ЕЦП дає змогу також підтвердити цілісність ЕД. При цьому необхідно підкреслити, що лише ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки), а інші види електронного підпису не мають такого статусу.

Відповідно до статті 5 Закону України "Про електронний цифровий підпис" [41] органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності повинні застосовувати лише ЕЦП, а для засвідчення чинності ВК використовують лише *посилений сертифікат відкритого ключа* (ПСВК). При цьому слід зазначити, що відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" [51] зазначені у ній установи ЕЦП не застосовують:

– для складання ЕД, які не можуть бути оригіналами у випадках, передбачених законодавством;

– для здійснення правочинів на суму, що перевищує 1 млн. грн.

Електронна печатка

У разі, коли згідно із законодавством необхідне засвідчення справжності підпису печаткою на документах та відповідності копій документів оригіналам, застосовується спеціально призначений для таких цілей ЕЦП, який називається ***електронною печаткою*** (ЕП). Хоча із суто технологічного погляду ЕЦП і ЕП цілком аналогічні, одночасна наявність цих об'єктів у законодавстві про ЕД зумовлена різними функціями, які повинні забезпечуватися за їх допомогою, і викликано, зокрема, існуванням двох різних типів суб'єктів, яких умовно можна назвати "директор" і "секретар". Представники першого типу суб'єктів підписують документ, а представники другого – скріплюють підпис печаткою.

Відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" [51] зазначені у її назві установи застосовують ЕП лише за наявності у них відповідної печатки, що використовується для документів на папері. При цьому у ПСВК, що використовується установою для ЕП, додатково зазначається спеціальне призначення ЕЦП та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці (так звана "мокра" печатка). Право проставляння ЕП

на ЕД надається лише тому працівнику установи, який проставляє відповідну “мокру” печатку на документах на папері.

Цілком очевидно, що за відсутності у законодавстві поряд з положеннями про ЕЦП також положень і про ЕП, говорити про повноцінне використання ЕД нарівні з документами на папері неможливо.

Застосування ЕЦП й ЕП зокрема дасть змогу використовувати ЕД під час проведення виборів різних рівнів. При цьому стане можливим більш оперативне отримання Центральною виборчою комісією протоколів виборчих комісій в електронній формі, які міститимуть поряд з ЕЦП також й ЕП. Такі протоколи за своїм юридичним статусом матимуть рівну силу з документами на папері, на які проставлені власноручні підписи, скріплені “мокрою” печаткою.

2.2. Використання електронного цифрового підпису

Згідно із законодавством ЕЦП накладається на ЕД, а більш загально – на набір електронних даних і додається до цього набору або логічно з ним поєднується. Таким набором може бути файл, який являє собою вміст ЕД, сформованого, наприклад за допомогою текстового процесора Microsoft Word чи редактора електронних таблиць Microsoft Excel, текстовий, графічний, аудіо- або відеофайл тощо.

Слід зазначити, що особистий ключ (ОК), відкритий ключ (ВК) й електронний цифровий підпис (електронна печатка) аналогічно з ЕД, як правило, формуються, подаються і зберігаються в інформаційній системі і на персональному комп’ютері в електронному вигляді як файли з двійковими даними.

Накладання ЕЦП (ЕП) на ЕД (набір електронних даних) здійснюється за допомогою ОК, який слугує параметром для криптографічного перетворення цих даних. Початковим етапом цього криптографічного перетворення даних, або гешування (рос. – *хеширование*, англ. – *hashing*), яке називають також геш-функцією (функцією згортки), є отримання геш-значення (геш-коду) ЕД. Іноді геш-код називають ще дайджестом (“відбитком”) повідомлення (англ. – *message digest*). При цьому геш-код має фіксовану довжину, є унікальним і однозначно представляє ЕД (набір електронних даних), які підписуються. Після цього за допомогою ОК підписувача, який також є кодом фіксованої довжини, здійснюється шифрування геш-коду ЕД і в результаті цього формується код фіксованої довжини, який, власне, і являє собою ЕЦП, накладений на ЕД. Цілком зрозуміло, що не існує оберненого до гешування перетворення, за допомогою якого з геш-коду ЕД (набору електронних даних) можна відтворити сам ЕД (рис. 1).

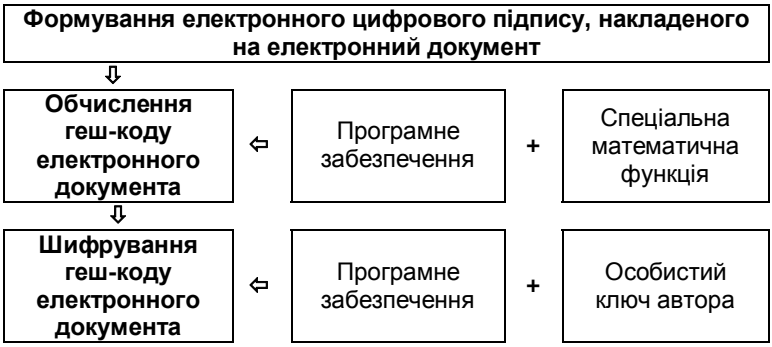

Рис. 1. ***Схема формування електронного цифрового підпису***

З урахуванням того, що ЕЦП являє собою код, тобто набір електронних даних у двійковій формі, "прочитати" безпосередньо з нього дані про особу підписувача неможливо. Для цього існує і використовується механізм, в основу якого покладено сертифікат відкритого ключа (СВК), що формується для кожного конкретного ВК одним з суб'єктів інфраструктури відкритого ключа (ІВК) – центром сертифікації ключів (ЦСК)/акредитованим центром сертифікації ключів (АЦСК), або засвідчувальним центром.

Слід відзначити, що власноручні підписи, проставлені підписувачем на два різних документи на папері, однакові між собою. Хоча, строго кажучи, точного графічного співпадіння вони не мають, але за необхідності графологічна експертиза може підтвердити, що вони проставлені однією й тією ж особою. Це, на перший погляд, може сприйматися як певний парадокс, але на відміну від ситуації з власноручним підписом, два ЕЦП, накладені підписувачем на два різних ЕД (із застосуванням одного й того ж ОК), відрізняються один від одного. Тобто два відповідних набори електронних даних (коди), отримані при цьому, є різними. Якщо ж припустити, що один і той же код виступатиме ЕЦП для різних ЕД, то, враховуючи, що такий "підпис" може бути вільно скопійований, точніше – отриманий інший його примірник, стане можливим і його подальше тиражування для будь-якої кількість інших "документів" без участі автора. Таким чином, авторові можна буде нав'язати ЕД, з яким він не згоден, але при цьому буде зобов'язаний нести за нього відповідальність. Це означатиме, що за такої ситуації застосування ЕДО з використанням ЕЦП втратить будь-який сенс.

Технології використання надійного засобу ЕЦП повинні забезпечувати з достатньою гарантованістю, що ОК підписувача не може бути відтворений з ЕД (набору електронних даних), його геш-коду та ЕЦП, накладеного на цей ЕД, або з сукупності таких наборів даних (для різних документів). Як уже зазначалося, тривалість часу, необхідного для

реалізації можливості відтворення ОК шляхом застосування найсучасніших методів криптоаналізу з допомогою сучасного комп'ютера оцінюється фахівцями величиною, близькою до 1000 років.

Перевірка справжності ЕЦП (ЕП), накладеного на ЕД (електронний набір даних), здійснюється за допомогою ВК.

Першим кроком цієї процедури є дешифрування коду ЕЦП за допомогою коду ВК, в результаті чого отримується первісний геш-код ЕД, тобто той геш-код, який був обчислений під час накладання ЕЦП на ЕД. Потім обчислюється геш-код ЕД, що перевіряється зараз, оскільки невідомо, чи збігається цей ЕД за вмістом із тим, ЕД, який підписувався.

Рис. 2. ***Схема перевірки справжності електронного цифрового підпису***

Після цього порівнюються ці два геш-коди і за позитивними результатами порівняння робиться висновок про справжність ЕЦП і цілісність ЕД (набору електронних даних), тобто про те, що після накладання ЕЦП на ЕД до нього не вносилося жодних змін.

Перевірка справжності ЕП, проставленої на ЕД, здійснюється за такою самою процедурою, що й перевірка ЕЦП (рис. 2).

Слід зазначити, що зміни, внесені до ЕД, точніше до відповідного набору електронних даних, можуть бути, зокрема, наслідком:

– умисної модифікації або знищення даних, здійснених певною особою;

– впливу шкідливої комп'ютерної програми, тобто ураження комп'ютерним вірусом;

– збою, тобто виходу зі штатного й переходу в позаштатний режим роботи інформаційної системи в цілому, або окремого комп'ютера, чи їх "зависання";

– дії технічних завад на електричні сигнали, за допомогою яких через телекомунікаційні канали передавалися ці дані.

Відповідно до статті 1 Закону України "Про електронний цифровий підпис" [41] ЕЦП дає змогу перевірити цілісність електронних даних, на які він накладений, та ідентифікувати особу підписувача. Оскільки ЕЦП являє собою код, то для отримання даних про особу підписувача використовується механізм сертифікату відкритого ключа (СВК). При цьому СВК (ПСВК) являє собою документ, виданий ЦСК (АЦСК, ЦЗО, засвідчу вальним центром). Відповідно до статті 1 зазначеного Закону цей документ засвідчує чинність і належність ВК підписувачу. При цьому СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. Склад СВК визначено у статті 6 цього Закону. Він містить, зокрема, основні дані (реквізити) підписувача – власника ОК, а також ВК, який є парним до цього ОК, що означає, що ці ключі були згенеровані разом.

Якщо після перевірки справжності ЕЦП, накладеного на ЕД, за допомогою ВК, який міститься у СВК, буде отриманий позитивний результат, то дані про підписувача у СВК якраз й ідентифікують цю особу. Таким чином і співставляється, власне, код (ЕЦП) з особою підписувача. При цьому, хоча два коди (ЕЦП), накладені за допомогою одного й того ж ОК підписувача на два різних ЕД, будуть різними, перевірка їх справжності здійснюється за допомогою одного й того ж ВК. За позитивного результату перевірки буде ідентифікована одна й та ж особа – підписувач, дані про якого зазначені в СВК. Слід зазначити, що відповідно до статті 5 Закону України "Про електронний цифровий підпис" [41] органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності ВК використовують лише ПСВК, які видаються АЦСК.

Відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" [51] справжність ЕЦП, накладеного на ЕД або інші електронні дані, та цілісність цього документа (електронних даних) перевіряється з дотриманням таких вимог:

– ЕЦП повинен бути підтверджений з використанням ПСВК за допомогою надійних засобів ЕЦП;

– під час перевірки повинен використовуватися ПСВК, чинний на момент накладення ЕЦП;

– ОК підписувача повинен відповідати ВК, зазначеному у ПСВК;

– на час перевірки повинен бути чинним ПСВК, сформований АЦСК та/або ПСВК відповідного засвідчувального центру.

Відмінності накладання електронного підпису на електронний документ від підписання документа на папері

Відповідно до статті 6 Закону України "Про електронні документи та електронний документообіг" [40] накладанням електронного підпису завершується створення ЕД. Це означає, зокрема, що на цей момент в ЕД повинні бути присутніми усі необхідні елементи, включаючи його номер і дату підписання. На цю обставину слід звернути увагу під час впровадження і використання ЕД і ЕДО із застосуванням ЕЦП. Практика традиційного документообігу свідчить, що дата і номер зазвичай вносяться до документа на папері вже після його підписання. Внесення дати і номера до ЕД, на який вже накладено ЕЦП, порушить цілісність цього ЕД (набору даних) і при перевірці справжності ЕЦП буде отриманий негативний результат.

Позначка часу

Постановою Кабінету Міністрів України "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу" [48] визначено умови та вимоги до процедури засвідчення і створені правові засади для надання ЦСК відповідних послуг ЕЦП (точніше – послуг у сфері використання ЕЦП). У цьому Порядку визначено такі терміни:

послуга фіксування часу – процедура засвідчення наявності ЕД (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу;

позначка часу – сукупність електронних даних, створена за допомогою технічних засобів та засвідчена ЕЦП центру сертифікації ключів, яка підтверджує наявність ЕД (електронних даних) на певний момент часу.

Затвердженням зазначеного Порядку врегульовано функціонування ЦСК – довірених суб'єктів в ІВК, які повинні цілодобово надавати послуги зі створення позначок часу і мати при цьому точне й надійне джерело часу. У процесі фіксування часу позначка часу (англ. – *Time Stamping*) додається або логічно поєднується з електронними даними таким чином, щоб була виключена можливість вносити до них зміни, а також зберігати позначки часу після надання послуги фіксування часу. Наявність позначки часу дає змогу перевірити достовірність часу наявності ЕД (електронних даних). При цьому можна використовувати

СВК, який на момент перевірки ЕЦП, накладеного на ЕД, вже анульований або відкликаний. В іншому випадку, актуальність підписаного ЕД обмежена терміном дії СВК.

Спільним наказом Держкомінформнауки та Держспецзв'язку затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису (протокол фіксування часу)" [70]. Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмно-технічних комплексів АЦСК. Правильність реалізації протоколу та наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

Технічні специфікації визначають процедуру формування позначки часу, зокрема дії, які при цьому виконують користувач та ЦСК.

Згідно з процедурою, користувач попередньо обчислює геш-код (геш-значення) ЕД (електронного набору даних). Слід зазначити, що обчислення цього коду є проміжним технологічним етапом при формуванні ЕЦП, що накладається на ЕД. Після цього користувач формує запит на формування позначки часу, який містить, у тому числі й обчислений геш-код, і передає його до ЦСК. В свою чергу, ЦСК перевіряє правильність формату запиту та виконує його обробку, формує позначку часу та відповідь, що містить цю позначку, чи відповідь з інформацією про відмову у формуванні позначки часу.

За результатом опрацювання цієї послуги ЦСК пересилає користувачеві відповідь, що містить позначку часу, засвідчену ЕЦП центру. Сформована позначка часу, тобто сукупність електронних даних, створена за допомогою технічних засобів, містить у тому числі й геш-код ЕД (електронного набору даних), для яких було сформовано позначку, час її формування та серійний номер.

Користувач після отримання відповіді, отриманої від ЦСК, перевіряє результат обробки свого запиту у відповіді центру. За позитивного результату обробки користувачем перевіряється відповідність імені суб'єкта, що підписав позначку часу, власне імені ЦСК, наявність у центру права формувати позначки часу, чинність СВК центру та справжність ЕЦП, накладеного на отриману від центра позначку. Після цього користувач порівнює попередньо обчислений ним геш-код ЕД та геш-код, записаний у позначці часу. За позитивним результатом порівняння позначка часу може бути додана до ЕД.

Перевірка позначки часу може бути виконана будь-яким суб'єктом (верифікатором) за допомогою СВК, що належить ЦСК, автономно, без взаємодії з цим центром. З цією метою верифікатор витягує позначку часу з ЕД, до якого вона була прикріплена, і отримує з неї ідентифікаційну інформацію про ЦСК. На її основі може бути отриманий СВК, що

належить ЦСК, який зберігається у ЦЗО (засвідчувальному центрі). За допомогою чинного (на момент формування позначки) СВК центру сертифікації ключів версифікатор перевіряє справжність ЕЦП, накладеного на позначку часу. Після цього, шляхом порівняння обчисленого геш-коду ЕД та геш-коду, що зберігається у позначці часу, можна вже перевірити відповідність позначки часу та ЕД, до якого вона була прикріплена.

Позначка часу на ЕД засвідчує точний час, на який цей документ вже існував і тому за її допомогою в подальшому можна буде розв'язувати конфлікти, пов'язані з використанням цього документа. Зокрема, за її допомогою можна забезпечити невідмовність автора ЕД від свого ЕЦП.

Наявність позначки часу, доданої до ЕД, дозволяє продовжувати термін дії накладеного на нього ЕЦП. Така позначка (штамп) засвідчує, наприклад, що ЕЦП був накладений на ЕД до того, як відповідний СВК був анульований (відкликаний). Таким чином, для перевірки справжності ЕЦП, накладеного на ЕД до моменту відкликання СВК, можна використовувати ВК, що міститься у вже анульованому або відкликаному сертифікаті. Ланцюжок позначок часу дозволяє створювати системи архівного зберігання ЕД, причому зі збереженням справжності ЕЦП, накладених на ці документи. В іншому випадку, справжність підписаного ЕД обмежена терміном дії СВК, який був чинним на момент накладання ЕЦП.

Слід підкреслити, що для отримання позначки часу користувач не повинен надсилати до ЦСК ні сам ЕД (електронний набір даних), ні накладений на нього ЕЦП. Тобто процедура формування позначки часу жодним чином не може порушити конфіденційність ЕД (електронного набору даних) і вона може бути використана, наприклад, як один з механізмів у підтвердженні авторства на літературний твір, аудіовізуальний твір у цифровому форматі, базу даних, комп'ютерну програму тощо.

2.3. Інфраструктура відкритого ключа

Сертифікат відкритого ключа

За умови корпоративного використання ЕЦП, тобто визначеним колом осіб, для забезпечення перевірки справжності підписів цих осіб їм достатньо обмінятися між собою ВК. Крім того, за такої ситуації питання ідентифікації особи підписувача не стоїть. Доступність і достовірність приналежності ВК може бути досягнута за допомогою певних правил, яких повинні дотримуватися зазначені особи в межах цієї корпорації.

Для забезпечення можливості перевірки справжності ЕЦП невизначеним колом осіб на практиці напрацьований механізм

використання СВК, що являє собою документ, виданий ЦСК, який засвідчує чинність і належність ВК підписувачу.

Відповідно до статті 6 Закону України "Про електронний цифровий підпис" [41] СВК містить такі обов'язкові дані:

– найменування та реквізити ЦСК (ЦЗО, засвідчувального центру);

– зазначення, що СВК виданий в Україні;

– унікальний реєстраційний номер СВК;

– основні дані (реквізити) підписувача – власника ОК;

– дату і час початку та закінчення строку чинності СВК;

– відкритий ключ;

– найменування криптографічного алгоритму, що використовується власником ОК;

– інформацію про обмеження використання ЕЦП.

При цьому ПСВК, крім обов'язкових даних, які містяться в СВК, повинен мати відповідну ознаку (що це є, власне, ПСВК).

Інші дані можуть вноситися у ПСВК на вимогу його власника.

Суб'єкти інфраструктури відкритого ключа підпису

Основу ІВК (англ. *PKI – Public Key Infrastructure*) складають суб'єкти, які є ЦСК, частина з яких має статус АЦСК. Головною функцією ЦСК є надання можливості необмеженому колу користувачів мати доступ до СВК підписувачів через загальнодоступні телекомунікаційні мережі, зокрема через Інтернет. Наявність СВК дає змогу перевірити справжність ЕЦП, накладеного підписувачем, та ідентифікувати його особу.

Ключовим елементом ІВК є ЦЗО, який визначається Кабінетом Міністрів України і веде Реєстр суб'єктів – засвідчувальних центрів та акредитованих центрів сертифікації ключів [73], які надають визначені Законом України "Про електронний цифровий підпис" [41] послуги, пов'язані з ЕЦП (послуги ЕЦП). Головною функцією ЦЗО в ІВК є засвідчення приналежності ВК відповідним ЦСК, які, в свою чергу, засвідчують приналежність ВК підписувачам. Умовно кажучи, довіра до ЦЗО поширюється на СВК, що належать ЦСК, а довіра до ЦСК – відповідно на СВК підписувачів. На сьогодні функції ЦЗО виконує Міністерство юстиції України.

В інституційному забезпеченні функціонування ІВК важливу роль відіграє Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Відповідно до статті 12 зазначеного Закону функції контролюючого органу (КО) здійснює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (на сьогодні – Адміністрація Держспецзв'язку). Для забезпечення здійснення своїх функцій Адміністрація Держспецзв'язку своїм наказом затвердила "Положення

про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису" [63], відповідно до якого КО перевіряє дотримання вимог цього Закону ЦЗО, засвідчувальними центрами та ЦСК.

Відповідно до статті 10 зазначеного Закону Кабінет Міністрів України за необхідності визначає засвідчувальний центр центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи ЦСК, які надають послуги ЕЦП цьому органу і підпорядкованим йому підприємствам, установам та організаціям. Засвідчувальний центр по відношенню до такої групи ЦСК має ті ж функції і повноваження, що й ЦЗО стосовно ЦСК. Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання таких функцій.

Згідно з частиною сьомою статті 5 зазначеного Закону порядок застосування ЕЦП в банківській діяльності визначається Національним банком України. Зокрема, Національний банк України прийняв постанову "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України" [55]. Для забезпечення формування складової ІВК для банківської системи України та створення умов для подальшого функціонування ЕЦП в банківській діяльності Кабінет Міністрів України відповідним розпорядженням [58] погодив створення Засвідчувального центру Національного банку України. Це, зокрема, надасть змогу досягти зменшення витрат банківської системи на послуги ЕЦП за рахунок використання централізованої інфраструктури відкритих ключів та прискорити більш широке застосування ЕЦП в банківській системі й сприяти подальшому розвитку сучасних ІТ у банківської діяльності.

Центр сертифікації ключів

За наявності ІВК будь-яка фізична або юридична особа, що виявила бажання застосовувати у своїй діяльності ЕЦП, може звернутися до ЦСК (АЦСК) або до його повноважного представника, який в ході процедури реєстрації здійснює ідентифікацію заявника і отриманих від нього даних, необхідних для формування СВК (ПСВК). При цьому ЦСК формує СВК підписувача у вигляді документа, завіреного своїм підписом. Обов'язковим елементом цього документа є ВК підписувача. Після того, як ЦСК сформував СВК, він надає його підписувачу, для якого цей СВК був сформований, а також забезпечує вільний доступ користувачів до цього документа через загальнодоступні телекомунікаційні канали у разі згоди на це підписувача.

Відповідно до статті 6 Закону України "Про електронний цифровий підпис" [41] ЦСК може бути юридична особа незалежно від форми

власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги ЕЦП та засвідчила свій ВК у ЦЗО або засвідчувальному центрі з дотриманням вимог статті 6 зазначеного Закону. Обслуговування фізичних та юридичних осіб здійснюється ЦСК на договірних засадах.

Відповідно до цього Закону послугами ЕЦП є:

– надання у користування засобів ЕЦП;

– допомога при генерації ВК та ОК;

– обслуговування СВК (формування, розповсюдження, скасування, зберігання, блокування та поновлення);

– надання інформації щодо чинних, скасованих і блокованих СВК;

– послуги фіксування часу;

– консультації та інші послуги.

Акредитований центр сертифікації ключів

Відповідно до статті 9 Закону України "Про електронний цифровий підпис" [41] ЦСК, акредитований в установленому порядку, є АЦСК. Процедура акредитації, яка здійснюється на добровільних засадах, документально засвідчує компетентність ЦСК здійснювати діяльність, пов'язану з обслуговуванням ПСВК. При цьому АЦСК має виконувати усі зобов'язання та вимоги, встановлені законодавством для ЦСК, та додатково зобов'язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП.

Відповідно до "Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" [51] установа, тобто будь-який суб'єкт, зазначений в цьому Порядку, отримує на договірних засадах послуги ЕЦП від АЦСК. При цьому установа може отримувати такі послуги лише від одного АЦСК, а використання підписувачами (працівниками установи) ОК, відповідні ВК яких засвідчені іншими АЦСК, забороняється.

На виконання постанови Кабінету Міністрів України "Про затвердження Порядку акредитації центру сертифікації ключів" [48] наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (його правонаступником є Адміністрація Держспецзв'язку) затверджено "Правила посиленої сертифікації" [65], які визначають організаційні, технічні і технологічні вимоги до АЦСК під час обслуговування ними ПСВК та забезпечення їх використання. Відповідно до зазначеного Порядку та з метою створення умов технологічної сумісності програмно-технічних комплексів АЦСК та засобів ЕЦП спільним наказом Держкомінформнауки та Держспецзв'язку [70] були затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису", що містять:

– формат підписаних даних;
– протокол фіксування часу;
– протокол визначення статусу ПСВК.

Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмно-технічних комплексів АЦСК. Правильність реалізації наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері КЗІ. Тип формату ЕЦП обирається залежно від вимог до зберігання підписаних даних.

Розповсюдження сертифікатів відкритих ключів

Згідно із законодавством СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. При цьому ПСВК є СВК, який відповідає вимогам Закону України "Про електронний цифровий підпис" [41], виданий АЦСК, засвідчувальним центром, ЦЗО. Відповідно до статті 8 цього Закону ЦСК зобов'язаний забезпечувати цілодобово доступ користувачів до СВК та відповідних електронних переліків СВК через загальнодоступні телекомунікаційні канали.

Користувачі у разі необхідності отримують СВК підписувача з бази даних сертифікатів ЦСК і при цьому перевіряється статус цього СВК (чинний, заблокований, скасований). Перевірка ЕЦП може здійснюватися за допомогою ВК, що міститься у СВК, лише у разі, коли на цей момент сертифікат є чинним (рис. 3).

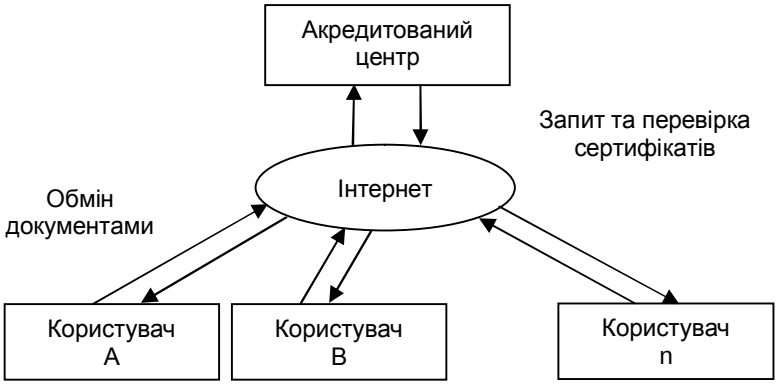

Рис. 3. ***Схема взаємодії користувачів електронного цифрового підпису***

Обов'язкова передача документованої інформації центрів сертифікації ключів

Сукупність СВК, які зберігаються АЦСК, відповідні реєстри, та інша документована інформація є головною інформаційною складовою ІВК. За її неповноти коло суб'єктів, що застосовують ЕЦП, буде обмеженим і може звестися лише до корпоративних груп, які самостійно будуть обмінюватися між собою ВК. Для забезпечення захисту прав суб'єктів, які використовують ЕЦП, та стабільного існування ІВК необхідно створити юридичні та організаційні умови, за яких гарантовано буде збережено зазначену інформацію.

Відповідно до статті 14 Закону України "Про електронний цифровий підпис" [41] ЦСК припиняє свою діяльність відповідно до законодавства. Про рішення щодо припинення своєї діяльності ЦСК повідомляє підписувачів за три місяці, якщо інші строки не визначено законодавством. При цьому АЦСК додатково повідомляє про рішення щодо припинення діяльності ЦЗО або відповідний засвідчувальний центр і протягом доби, визначеної як дата припинення його діяльності, відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку обов'язкової передачі документованої інформації" [53] передає ПСВК, відповідні реєстри ПСВК та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або ЦЗО.

Контрольні питання

1. Основні визначення електронного цифрового підпису.
2. Ключі електронного цифрового підпису.
3. Робота з особистим ключем.
4. Захищеність електронного цифрового підпису.
5. Використання електронної печатки.
6. Технології використання електронного цифрового підпису в системі електронного документообігу.
7. Підписання електронного документа електронним цифровим підписом.
8. Перевірка справжності електронного цифрового підпису.
9. Шифрування та дешифрування електронного документа.
10. Перевірка справжності електронного документа.
11. Організація створення та забезпечення функціонування центру сертифікації ключів.
12. Вимоги до засобів електронного цифрового підпису, що використовуються органами виконавчої влади.
13. Склад та функції елементів інфраструктури відкритого ключа.

3. СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

3.1. Організація електронного документообігу в органах державної влади

Затверджений постановою Кабінету Міністрів України "Типовий порядок здійснення електронного документообігу в органах виконавчої влади" [52] встановлює загальні правила документування в органах виконавчої влади управлінської діяльності в електронній формі і регламентує виконання дій з електронним документом (ЕД) з моменту їх створення або одержання до відправлення чи передачі до архіву органу виконавчої влади. При цьому усі інші дії з ЕД виконуються в органі виконавчої влади згідно з вимогами до дій з документами на папері, передбаченими інструкцією з діловодства цього органу. Дія Типового порядку поширюється на всі ЕД, що створюються або одержуються органом виконавчої влади.

Орган виконавчої влади здійснює електронний документообіг (ЕДО) лише за умови використання надійних засобів ЕЦП, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності ПСВК у своїх працівників – підписувачів. При цьому ЕДО здійснюється органом виконавчої влади через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування, а відправлення ЕД через телекомунікаційні мережі загального користування здійснюється за рішенням керівника цього органу.

Згідно із законодавством СЕДО органу виконавчої влади повинна відповідати вимогам нормативно-правових актів у сфері захисту інформації. Зокрема, це стосується положень Закону України "Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [42] та постанови Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [54].

Згідно з Правилами для забезпечення захисту інформації в ІС створюється комплексна система захисту інформації (КСЗІ), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Відповідальність за забезпечення захисту інформації в ІС, своєчасне розроблення необхідних для цього заходів та створення КСЗІ покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) ІС, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію ІС.

При цьому організація та проведення робіт із захисту інформації в ІС здійснюється службою захисту інформації (СЗІ), яка забезпечує визначення вимог до захисту інформації в ІС, проектування, розроблення і модернізацію КСЗІ, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Утворення СЗІ здійснюється згідно з рішенням керівника організації, що є власником (розпорядником) ІС. У разі коли обсяг робіт, пов'язаних із захистом інформації в ІС, є незначний, захист інформації може здійснюватися однією особою. Захист інформації на всіх етапах створення та експлуатації ІС здійснюється відповідно до розробленого СЗІ плану захисту інформації в ІС.

Суб'єкти СЕДО повинні зберігати ЕД на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях, а строк їх зберігання повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання ЕД протягом такого строку, суб'єкти ЕДО повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, ЕД повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері).

Створення архівів ЕД, подання ЕД до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

Слід зазначити, що на сьогодні в Україні СЕДО та системи архівного зберігання ЕД сприймаються як різні системи, хоча з функційної точки зору вони є надзвичайно близькими. Вірогідною тенденцією подальшого розвитку зазначених систем буде їх інтеграція.

На виконання постанови Кабінету Міністрів України "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади" [52] Державним комітетом архівів України було затверджено "Порядок зберігання електронних

документів в архівних установах" [69]. Цим Порядком встановлені загальні правила:

– оперативного зберігання ЕД, створених згідно із законодавством про ЕЦП, ЕД та ЕДО органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями незалежно від форм власності (установи);

– підготовки та передавання ЕД на тривале зберігання до архівного підрозділу установи;

– тривалого зберігання ЕД в архівному підрозділі установи.

При цьому вимоги до забезпечення захисту ЕД формуються для кожної автоматизованої системи окремо відповідно до вимог нормативно-правових актів у сфері захисту інформації.

Підготовка ЕД для передавання до архівного підрозділу установи у вигляді електронних справ включає:

– перевірку всіх електронних підписів;

– експертизу цінності ЕД;

– оформлення електронних справ;

– складання описів електронних справ;

– підготовку комплекту супровідної документації.

Порядок та строки передавання ЕД постійного зберігання до державної або іншої архівної установи, а також формати подання даних в електронній справі та комплект супровідної документації визначаються спеціально уповноваженим центральним органом виконавчої влади у сфері архівної справи і діловодства.

3.2 Нормативне забезпечення систем електронного документообігу

Реалізація ЕДО передбачає наявність автоматизованої системи оброблення інформації, спряженої з іншими системами документообігу.

На виконання постанови Кабінету Міністрів України "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади" [52] наказом Державного департаменту з питань зв'язку та інформатизації Мінтрансзв'язку затверджені "Технічні умови на систему електронного документообігу органу виконавчої влади" (ТУ У 30.0-33240054-001:2005) [68]. Ці Технічні умови поширюються на СЕДО, призначену для забезпечення обміну ЕД та повідомленнями з дотриманням вимог зазначеного Типового порядку.

Дотримання Технічних умов забезпечує можливість:

– уніфікації форматів обміну інформацією між органами виконавчої влади;

– інтеграції СЕДО в єдину загальнодержавну СЕДО органів виконавчої влади.

Загальний порядок створення і приймання СЕДО повинен відповідати вимогам ГОСТ 34.601-90 “Автоматизированные системы. Стадии создания” [76]. Приймання СЕДО здійснюється державною (міжвідомчою) комісією, до якої мають бути залученими представники розробника системи, органу виконавчої влади та уповноважених органів, що відповідають за впровадження ЕДО в органах виконавчої влади України, та затверджується актом приймання-здавання науково-технічної продукції.

Одним з етапів впровадження СЕДО є закупівля або створення відповідного програмного забезпечення (ПЗ). З метою врегулювання питань постачання, створення або технічної підтримки програмних продуктів (ПЗ) які закуповуються або створюються на замовлення державних органів, у тому числі під час виконання завдань (проектів) Національної програми інформатизації, зокрема зі створення СЕДО, Кабінет Міністрів України прийняв постанову “Про затвердження загальних вимог до програмних продуктів, які закуповуються або створюються на замовлення державних органів” [55].

Слід також зазначити, що питання створення СЕДО є актуальним для багатьох країн, у тому числі для членів Європейського Союзу. Зокрема, в межах програми IDA Європейської Комісії компанією Cornwell Management Consultants plc (раніше Cornwell Affiliates plc) розроблена Специфікація MoReq (Model Requirements) “Типові вимоги до автоматизованих систем електронного документообігу” [74]. Ця специфікація має універсальний характер й не містить в собі будь-якої національної специфіки. Вона визначає не те, як в конкретній організації повинні виконуватися процеси реєстрації, узгодження й виконання документів, а те, яким функціональним вимогам повинна відповідати автоматизована система, щоб підтримати будь-які регламенти роботи з документами.

Специфікація описує типові вимоги до управління ЕД (*Management of Electronic Record*) чи вимоги до ЕДО й фокусується в основному на функціональних вимогах до управління ЕД за допомогою автоматизованих систем електронного документообігу (АСЕД).

При розробленні специфікації передбачалося, що до числа користувачів АСЕД належать не лише адміністратори, діловоди та архівісти, але також і працівники загальноадміністративних й функціональних структурних підрозділів, які використовують АСЕД в повсякденній діяльності для створення ЕД й для доступ до них.

У специфікації також зазначається, що управління ЕД це складне завдання, яке вимагає широкого спектру функціональності й високого рівня впровадження. Очевидно, що АСЕД, яка відповідає цим вимогам, потребує спеціалізованого програмного забезпечення. Таке програмне забезпечення може являти собою спеціалізований пакет, декілька

інтегрованих пакетів, розробку на замовлення чи комбінацію зазначеного вище; в усіх випадках рішення має бути доповнене організаційними заходами й політиками (методиками) керування. Характер АСЕД буде варіюватися від установи до установи. У цій специфікації не робляться припущення про характер конкретної АСЕД. Користувачі цієї специфікації повинні самі визначити, яким чином повинні бути реалізовані функціональні вимоги, щоб відповідати їх потребам.

3.3 Системи електронного документообігу в органах державної влади

Першим кроком до впровадження СЕДО в органі виконавчої влади є, зокрема, забезпечення його працівників ключами ЕЦП. Тобто, зазначені органи мають укласти угоди про обслуговування ПСВК своїх працівників. Станом на 2010 рік відповідні угоди були укладені з двадцятьма органами державної влади: Міністерством аграрної політики та продовольства, Міністерством внутрішніх справ, Міністерством культури, Міністерством надзвичайних ситуацій, Міністерством освіти і науки, молоді та спорту, Міністерством охорони здоров'я, Міністерством соціальної політики, Міністерством фінансів, Державною митною службою, Державною податковою службою, Адміністрацією Державної прикордонної служби, Державною службою фінансового моніторингу, Національним агентством України з питань державної служби, Державною службою статистики, Державною інспекцією України з питань праці, Державною службою з питань інвалідів та ветеранів, Національним банком України, Фондом соціального страхування від нещасних випадків на виробництві та професійних захворювань, Фондом соціального страхування від тимчасової втрати працездатності, Єдиним державним реєстром юридичних та фізичних осіб-підприємців.

Процес впровадження СЕДО в органи виконавчої влади, за рідкими винятками, знаходиться лише на початковому етапі. Хоча в Національному агентстві України з питань державної служби така система вже активно використовується і цей досвід розповсюджується для інших органів.

Одним із прикладів галузевого впровадження ЕДО можна назвати комплекс, пов'язаний з перевезенням вантажів залізничним транспортом. Розпорядженням Кабінету Міністрів України [59] було затверджено План заходів, яким передбачено, зокрема:

– затвердження формату електронного перевізного документа;

– внесення змін до ряду нормативних документів;

– розроблення та впровадження технологій ЕДО в автоматизованих системах управління перевезеннями вантажів залізничним транспортом;

– створення спеціалізованого програмно-апаратного комплексу;

– забезпечення застосування електронних перевізних документів під час перевезення вантажів залізничним транспортом в межах України.

На виконання Плану заходів Міністерством інфраструктури України видано відповідний наказ [71], яким, зокрема, внесено зміни до ряду правил та інструкцій.

Другим прикладом можна назвати створення багатофункціональної комплексної системи "Електронна митниця". Концепцію її створення було схвалено відповідним розпорядженням Кабінету Міністрів України [57].

Серед шляхів реалізації Концепції визначено, зокрема:

– запровадження ЕЦП для посадових осіб митних органів;

– створення системи електронного документообігу та електронного декларування.

Одним з пріоритетних напрямів створення технологічної інфраструктури електронного урядування в Україні є об'єднання інформаційних систем, які існують в органах державної влади та органах місцевого самоврядування, а також систем, які будуть розроблятися в подальшому, в єдиний інформаційно-аналітичний комплекс, який має функціонувати в єдиному інформаційному і телекомунікаційному середовищі. Важливою складовою цього комплексу має стати інтегрована система електронного документообігу (ІСЕД).

Мета створення інтегрованої системи електронного документообігу:

– забезпечення руху ЕД (укази, постанови, закони, розпорядження, повідомлення, звіти, аналітичні довідки, тощо);

– скорочення терміну підготовки та прийняття рішень шляхом автоматизації процесів колективного створення та використання ЕД в органах державної влади.

Головні завдання, які вирішуються за допомогою Інтегрованої системи електронного документообігу:

– автоматизація обробки ЕД, пошук та відбір необхідної інформації, розсилка опрацьованих ЕД для подальшої обробки;

– обмін ЕД між вузлами ІСЕД, уніфікація технологічних процедур проходження, передачі та опрацювання ЕД, збирання, реєстрація, накопичення, обробка та аналіз інформації, що надходить до кожного з вузлів, забезпечення постійного зв'язку та обміну інформацією між вузлами;

– автоматизація управління процесами синхронізації робіт;

– автоматизація контролю виконання ЕД;

– автоматизація процесів реєстрації ЕД з використанням класифікаторів та довідників, забезпечення механізмів анотованого опису ЕД та збору резолюцій, доставка звітів про виконання доручень;

– автоматизація збирання даних про результати виконання технологічних процесів, формування довільних аналітичних довідок;

– розсилка, зберігання та використання вхідних, вихідних і внутрішніх ЕД за єдиною нумерацією з початку року;

– відправлення, приймання та опрацювання електронної пошти;

– оперативний пошук інформації про вхідні, вихідні та внутрішні ЕД;

– наскрізний контроль обміну інформацією;

– ведення системи класифікаторів та довідників;

– постійне оновлення та адміністрування головної бази даних;

– забезпечення надійного зберігання всіх версій ЕД та інших інформаційних об'єктів;

– організація служб копіювання-відновлення та захисту інформації;

– формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання;

– визначення та призначення рівнів доступу до інформації, повноважень та прав користувачів;

– удосконалення методів підтримки прийняття рішень з питань ЕДО.

Інтегровану систему електронного документообігу складають комплекси:

– "Підготовки документів комп'ютерними засобами";

– "Реєстрації та введення електронних документів в оперативний електронний архів";

– "Ведення електронного архіву, підтримка паперового архіву та організація доступу до його інформації";

– "Контролю виконавчої діяльності";

– "Проектування маршрутів руху документів";

– "Обміну даними";

– "Підтримки формування аналітично-статистичної звітності та оперативного аналізу";

– "Ведення нормативно-довідкової інформації";

– "Адміністрування";

– "Уніфіковане клієнтське місце".

На рівні центральних органів виконавчої влади та органів місцевого самоврядування залежно від стану інформатизації та структури органу використовуються засоби (інформаційні системи) ЕДО, які в основному можна розподілити на такі (табл. 1).

Таблиця 1.

Класифікація систем електронного документообігу

Клас системи	Функції (особливості)	Зберігання документів
“Електронне діловодство”	Забезпечення роботи з електронними версіями документів і *реквізитами реєстраційно-контрольних форм* відповідно до прийнятих в Україні правил і стандартів діловодства	Робоча станція виконавця
“Документообіг”	Забезпечення чітко регламентованого і формально контрольованого руху документів усередині і поза організацією на основі інформаційно-телекомунікаційних технологій, часткова підтримка процесів роботи над документами	Робоча станція виконавця, файл-сервер
“Системи електронного управління документами”	Забезпечення повного циклу: створення, перетворення, забезпечення безпеки, управління доступом і поширення великих обсягів документів у корпоративних комп’ютерних мережах, забезпечення контролю над потоками документів в установі, знищення тощо	Спеціальні сховища (центральні або розподілені файл-сервери) або в ієрархії файлової системи
“Корпоративні системи електронного управління документами”	Забезпечення спільної роботи над документами і їх публікації, доступної практично всім користувачам, інтеграція з офісними пакетами, наявність інформаційних порталів та зв’язку через мережі Internet, Intranet та Extranet	Спеціальні сховища (центральні або розподілені файл-сервери) або в ієрархії файлової системи

Основними властивостями корпоративних системи електронного управління ЕД є:

– можливість управління життєвим циклом ЕД – від авторської розробки до остаточної редакції, затвердження, поширення і архівації;

– забезпечення розподіленого редагування ЕД, що дає змогу співробітникам, які працюють у різних територіально віддалених підрозділах, спільно використовувати ЕД на локальних серверах, зберігаючи при цьому цілісність ЕД в масштабі всього органу (підрозділу) з розподіленою структурою;

– повний набір засобів управління ЕД – оформлення, отримання (виписування), контролю версій, повнотекстового пошуку в масштабах всього керованого інформаційного вмісту системи, контрольних журналів, можливості роботи з шаблонами, надання повідомлень про зміни ЕД та ін.;

– можливість редагування/затвердження ЕД;

– багаторівневий контроль версій ЕД з організацією їх створення і збереження чернеток;

– захист даних за допомогою сертифікованих засобів шифрування промислового рівня, засобів повномасштабної ідентифікації користувачів;

– підтримка різноманітних типів файлів подання ЕД, включаючи текстові, графічні зображень, електронні таблиці, аудіо- та відеодані, Web-документи тощо.

Під управлінням ЕДО в загальному випадку розуміють організацію руху ЕД між підрозділами установи, окремими користувачами чи їх групами. При цьому під рухом ЕД розуміється не їх фізичне переміщення, а власне передача прав на їх застосування (доступ), що супроводжується відповідним повідомленням про це конкретних користувачів, а також контролем за виконанням ЕД.

Очікувані результати від впровадження інтегрованої системи електронного документообігу:

– більш ефективне управління ЕДО за рахунок автоматичного контролю виконання, прозорості діяльності установи на всіх рівнях;

– підтримка ефективного накопичення, управління й доступу до інформації і знань;

– забезпечення кадрової гнучкості за рахунок більшої формалізації діяльності кожного співробітника і можливості збереження всієї історії його діяльності;

– усунення дублювання і багаторазового перетворення інформації;

– чітка авторизація доступу до інформації з обмеженим доступом, за рахунок чого підвищується персональна відповідальність співробітників за виконані дії строго в рамках наданих повноважень;

– протоколювання діяльності установи в цілому (внутрішні службові розслідування, аналіз діяльності підрозділів, виявлення “гарячих точок“ у діяльності тощо);

– оптимізація управлінських процесів, автоматизація їх виконання і контролю;

– виключення або максимально можливе скорочення обігу паперових документів;

– заощадження ресурсів за рахунок скорочення витрат на управління потоками ЕД в організації;

– виключення необхідності чи істотне спрощення і здешевлення збереження паперових документів за рахунок наявності оперативного електронного архіву.

Підсистема інтегрованого ЕДО документообігу повинна забезпечити вдосконалення процесу обробки ЕД та виконання функцій:

– підтримки об'єктної моделі ЕД, у тому числі побудови взаємозв'язків між об'єктами;

– контролю та управління процесами створення ЕД, надання користувачу можливості виконувати всі необхідні операції над ЕД, у тому числі їх динамічного компонування, а також забезпечення пошуку, збереження, перегляду і друку ЕД;

– забезпечення прозорого доступу через архів ЕД до архівів інших даних чи робочих баз даних з можливістю здійснення операцій над цими даними;

– доступу до ЕД, що знаходяться в електронному сховищі, маршрутизації виконання всього набору дій над ЕД із застосувань;

– розробки спеціалізованих застосувань для інтеграції з іншими ІС, зокрема з поштовою системою.

Стосовно сучасних СЕДО слід зазначити, що вони повинні відповідати низці вимог.

З точки зору функціональності СЕДО мають забезпечувати:

– можливість виконання документів і доручень;

– моніторинг та контроль виконання документів і доручень;

– виконання процедур погодження проектів та затвердження ЕД відповідно до маршруту та правил їх проходження;

– можливість формування необхідного маршруту та відповідних правил проходження для нових типів ЕД.

З точки зору комплексності СЕДО повинні містити у своєму складі підсистеми:

– адміністрування;

– забезпечення захищеного сховища ЕД та облікових записів;

– навігації та пошуку;

– сканування та візуалізації;

– планування та контролю виконання доручень

– забезпечення редактора форм та звітів.

Щодо зручності використання СЕДО повинні забезпечити:

– інтуїтивно зрозумілий Web-інтерфейс;

– можливість налаштування кожного окремого робочого місця;

– прості та зручні інструменти взаємодії під час колективної роботи з ЕД;

– можливість оперативного доступу до необхідної інформації та баз ЕД;

– можливість віддаленого, а також мобільного доступу користувачів до системи;

– підтримку звичного середовища роботи з ЕД (наприклад з пакетом MS Office).

Режим технічної підтримки забезпечує:

– відсутність жорсткої прив'язки до постачальника системи;

– можливість масштабування системи та коригування довідників адміністратором системи;

– можливість зміни системного та базового програмного забезпечення без впливу на роботу системи;

– мінімальну прив'язку програмного забезпечення до апаратного;

– повне відновлення інформації при відновленні працездатності системи після збоїв у роботі.

Контрольні питання

1. Основні засади електронного документообігу в органах державної влади та органах місцевого самоврядування.
2. Регулювання функціонування систем електронного документообігу.
3. Нормативне забезпечення систем електронного документообігу.
4. Етапи впровадження систем електронного документообігу.
5. Характеристики систем електронного документообігу, що використовуються в органах державної влади України.
6. Приклади систем електронного документообігу в органах державної влади.
7. Інтегровані системи електронного документообігу – мета та завдання створення.
8. Основні комплекси, що складають інтегровані системи електронного документообігу.
9. Класифікація систем електронного документообігу.
10. Властивості корпоративних систем управління документами.
11. Вимоги до сучасних систем електронного документообігу.

4. ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ УРЯДУВАННІ

4.1. Складові інформаційної безпеки органів державної влади

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуку шляхів її вирішення.

Базовою характеристикою інформаційної безпеки слід вважати імовірність підвищеного ризику реалізації загрози або небезпеки для діяльності органів виконавчої влади в цілому і для кожного її структурного елементу зокрема. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Сукупність внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи органів виконавчої влади.

Напрями забезпечення інформаційної безпеки у внутрішньо системному функціонуванні органів виконавчої влади характеризує сама їх компетенція, котра пов'язана із виконанням покладених на них державою функцій і завдань. До характеристик, що дають змогу описати дану систему можна віднести такі:

– доступність – можливість за прийнятний час отримати необхідну інформаційну послугу будь-яким суб'єктом виконавчої влади;

– цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни;

– конфіденційність – захист від несанкціонованого ознайомлення.

Сутність і зміст інформаційної безпеки проявляються по-особливому на кожному з рівнів системи органів влади, зокрема на:

– стратегічному (загальнодержавному);

– тактичному (органів влади, установ тощо);

– оперативному (структурних підрозділів органів державної влади, місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації).

Таким чином, можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення. У зв'язку з цим слід виділити такі її рівні:

– законодавчий та нормативно-правовий – закони, нормативно-правові акти, тощо;

– адміністративний – дії загального характеру, що вживаються

органами виконавчої влади;

– процедурний – конкретні процедури забезпечення інформаційної безпеки;

– програмно-технічний – конкретні технічні заходи забезпечення інформаційної безпеки.

Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як:

– розроблення теоретичних основ забезпечення безпеки інформації;

– створення системи органів та структур, відповідальних за безпеку інформації;

– вирішення та автоматизація проблем керування захистом інформації;

– створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації;

– налагодження виробництва засобів програмно-технічного захисту інформації; організація підготовки відповідних фахівців та ін.

Серед основних принципів державної політики у сфері забезпечення інформаційної безпеки можна зазначити:

– держава формує програму інформаційної безпеки, що поєднує зусилля державних організацій і комерційних структур у створенні єдиної системи інформаційної безпеки;

– держава здійснює контроль за створенням і використанням засобів захисту інформації за допомогою їхньої обов'язкової сертифікації і ліцензування діяльності в області захисту інформації;

– обмеження доступу до інформації є виключення з загального принципу відкритості інформації і здійснюється тільки на основі законодавства;

– відповідальність за зберігання, засекречення і розсекречення інформації персоніфікується;

– доступ до інформації, а також обмеження доступу, здійснюються з обліком обумовлених законом прав власності на цю інформацію;

– держава формує нормативно-правову базу, що регламентує права, обов'язки і відповідальність усіх суб'єктів, що діють в інформаційній сфері;

– юридичні і фізичні особи, що збирають, нагромаджують і обробляють персональні дані і конфіденційну інформацію, несуть відповідальність перед законом за їх зберігання і використання;

– держава проводить протекціоністську політику, що підтримує діяльність вітчизняних виробників засобів інформатизації і захисту інформації, і здійснює заходи для захисту внутрішнього ринку від проникнення на нього неякісних засобів інформатизації й інформаційних продуктів;

– держава прагне до відмовлення від закордонних інформаційних

технологій для інформатизації органів державної влади і управління по мірі створення конкурентоздатних вітчизняних інформаційних технологій і засобів інформатизації [4].

Відповідно до вищеназваних принципів і положень забезпечення інформаційної безпеки держави необхідно вирішити наступні ключові проблеми:

– розвиток науково-практичних основ інформаційної безпеки, що відповідають сучасній геополітичній ситуації та умовам політичного і соціально-економічного розвитку держави;

– формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, у тому числі розробка регламенту інформаційного обміну для органів державної влади, підприємств, нормативного закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки; розробка механізмів реалізації прав громадян на інформацію;

– формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни;

– розробка сучасних методів і технічних засобів, що забезпечують комплексне рішення задач захисту інформації;

– розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікація;

– комплексне дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією [32].

Базовим елементом інформаційного середовища органів державної влади є інформаційна інфраструктура, що являє собою єдність наступних компонент, тобто системи сервісного обслуговування елементів інфраструктури [25]:

– виробництва інформаційних продуктів;

– доставки їх до споживача;

– виробництва засобів виробництва інформаційних продуктів та їх доставки;

– виробництва інформаційних технологій;

– накопичення і збереження інформаційного продукту або інформаційного ресурсу.

4.2. Комплексний захист інформації як компонент інформаційного забезпечення органів виконавчої влади

Згідно з Законом України “Про захист інформації в інформаційно-телекомунікаційних системах” [42], основна термінологія систем захисту інформації використовує наступні поняття:

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

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

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

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

• знищення інформації в системі – дії, унаслідок яких інформація в системі зникає;

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

• інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

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

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

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

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

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

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

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

• 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 в інший спосіб;

- технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [42].

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмно-технічне забезпечення, яке призначене для обробки цієї інформації.

Суб'єктами відносин, що пов'язані із захистом інформації в інформаційних системах органів влади, є:

- власники інформації;
- власники системи;
- користувачі;
- спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

Для забезпечення захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – система) повинні обов'язково виконуватися наступні процедури:

- автентифікація – процедура встановлення належності користувачеві інформації в системі (далі – користувач) пред'явленого ним ідентифікатора;
- ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних визначається законодавством [54]. Для забезпечення захисту інформації в системі

створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;
- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;
- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації [42].

Комплексність підходу до захисту інформації є рішення в рамках єдиної концепції двох або більшої кількості різнопланових завдань. Сучасна система захисту інформації повинна включати структурну, функціональну і часову комплексність. Структурна комплексність припускає забезпечення необхідного рівня захисту у всіх елементах системи обробки інформації.

Функціональна комплексність означає, що методи захисту повинні бути направлені на всі виконувані функції системи обробки інформації. Часова комплексність припускає безперервність здійснення заходів щодо захисту інформації як в процесі безпосередньої її обробки, так і на всіх етапах життєвого циклу об'єкту обробки інформації [4].

Склад комплексної системи захисту визначається на основі вивчення усіх інформаційних процесів та потоків системи телекомунікацій і, як наслідок, розробці такої моделі загроз, щоб забезпечити мінімізацію втрат. На основі моделі загроз має бути розроблена та запроваджена концепція та політика інформаційної безпеки органів державної влади та створена комплексна система захисту інформації, які мають забезпечувати такі функції:

- конфіденційність інформації – властивість інформації, коли неавторизовані особи, які не мають доступу до інформації, не можуть розкрити зміст цієї інформації;
- цілісність інформації – властивість інформації, яка полягає в тому, що вона не може бути змінена навмисно або випадково користувачем чи процесом. А також властивість, яка полягає в тому, що жодний з її компонентів не може бути усунений, модифікований або доданий з порушенням політики безпеки;
- доступність – властивість ресурсу системи (інформації), яка полягає в тому, що авторизований користувач може отримати доступ до

ресурсу тільки із заданим змістом та якістю;

• спостережливість – властивість ресурсу інформаційної технології, що дозволяє реєструвати всі дії користувачів, здійснювати доступ поіменно, відповідно до ідентифікаторів та повноважень, а також реагувати на ці дії з метою мінімізації можливих втрат в системі, що здійснюється також за рахунок застосування криптографічного захисту інформації (КЗІ).

До складу КЗЗІ входять заходи і засоби, які реалізують способи, методи, механізми захисту інформації від:

• витоків технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань, акустоелектричних і інших каналів;

• несанкціонованих дій і несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування помилковій інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів і т.п.;

• спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної інформаційної системи склад, структура і вимоги до КЗЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи (АС) і умовами її експлуатації.

Однією з вимог забезпечення захисту інформації в АС є те, що обробка конфіденційної інформації повинна здійснюватись з використанням захищеної технології, яка містить програмно-технічні засоби захисту і організаційні заходи, які забезпечують виконання загальних вимог з захисту інформації. Загальні вимоги передбачають:

• наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці; у разі потреби можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів і іншими класифікаційними ознаками;

• наявність відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації (служба захисту в АС, СЗІ);

• створення КСЗІ, яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, направлених на забезпечення захисту інформації під час функціонування АС;

• розробку плану захисту інформації в АС;

• наявність атестату відповідності КСЗІ в АС нормативним документам із захисту інформації;

• можливість визначення засобами КСЗІ декількох ієрархічних

рівнів повноважень користувачів і декількох класифікаційних рівнів інформації;

- обов'язковість реєстрації в АС всіх користувачів і їх дій щодо конфіденційної інформації;
- можливість надання користувачам тільки за умови службової необхідності санкціонованого і контрольованого доступу до конфіденційної інформації, яка обробляється в АС;
- заборона несанкціонованій і неконтрольованій модифікації конфіденційної інформації в АС;
- здійснення за допомогою СЗІ обліку вихідних даних, отриманих під час рішення функціональної задачі, у формі віддрукованих документів, які містять конфіденційну інформацію, відповідно до керівних документів;
- заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації, в електронному вигляді;
- забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації, в електронному вигляді;
- можливість здійснення однозначної ідентифікації і аутентифікації кожного зареєстрованого користувача;
- забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

Приведені вимоги є базовими і застосовуються при захисті інформації від несанкціонованого доступу (НСД) у всіх типах АС [34].

Отже, зважаючи на викладене вище, доступ до інформації у суб'єктивному розумінні – це гарантована державою можливість фізичних, юридичних осіб і державних органів вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законних інтересів інших громадян, прав та інтересів юридичних осіб [2].

Провівши оцінку необхідності захисту інформації від НСД, можна судити про складність КСЗІ, оцінити вірогідність погроз, що проявляються, на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів. Спираючись на вимоги із захисту інформації від НСД [34], можна привести основні принципи захисних заходів від НСД в АС.

Принцип перший – обґрунтованість доступу. Даний принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню "форму допуску" для отримання інформації потрібного ним рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. У сфері автоматизованої обробки інформації як користувачі можуть виступати активні програми і процеси, а також носії інформації різного ступеня складності. Тоді система доступу припускає

визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій.

Принцип другий – достатня глибина контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип третій – розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

Принцип четвертий – чистота повторно використовуваних ресурсів. Даний принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип п'ятий – персональна відповідальність. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, а також за випадкові або умисні дії, які можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її спотворенню або знищенню, або виключенню можливості доступу до такої інформації законних користувачів.

Принцип шостий – цілісності засобів захисту. Даний принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі [35].

При розгляді питань безпеки інформації в АС завжди говорять про наявність деяких "бажаних" станів системи. Ці бажані стани (які бувають звичайно представлені в термінах моделі самої АС) описують "захищеність" системи. Поняття "захищеності" принципово не відрізняється від інших властивостей технічної системи, наприклад "надійної роботи". Особливістю поняття "захищеність" є його тісний зв'язок з поняттям "загроза" (те, що може бути причиною виведення системи із захищеного стану).

Отже, виділяються три компоненти, що пов'язані з порушенням безпеки системи:

- "загроза" – зовнішнє відносно системи джерело порушення властивості «захищеність»;

• “об’єкт атаки” – частина системи, на яку діє загроза;

• “канал дії” – середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об’єднує всі ці компоненти, є політика безпеки – якісний (або якісно-кількісний) вираз властивостей захищеності в термінах, що представляють систему. Опис політики безпеки повинен включати або враховувати властивості загрози, об'єкта атаки та каналу дії.

За означенням [8, 33], під політикою безпеки інформації розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін “політика безпеки” може бути застосований до організації, автоматизованої системи, операційної системи (ОС), послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз, і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки органу виконавчої влади і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної автоматизованої системи політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама автоматизована система може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій автоматизованій системі буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси автоматизованої системи, що потребують захисту, зокрема установлювати категорії оброблюваної в ній інформації. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Класифікація методів та засобів забезпечення безпеки інформації показані в табл. 2.

Методи мають такий зміст:

• перешкоди – фізичної перешкоди доступу зловмиснику до інформації, що захищається.

• керування доступом – захист інформації шляхом регулювання використання всіх ресурсів комп’ютерної інформаційної системи.

• маскування – захисту інформації шляхом її криптографічного закриття.

• регламентація – захист інформації, що створює такі умови автоматизованої обробки, зберігання й передачі інформації, що захищається, за яких можливості несанкціонованого доступу до неї зводилися б до мінімуму.

• примушення – захист, за якого користувачі й персонал системи змушено дотримувати правил обробки, передачі й використання інформації, що захищається, під загрозою матеріальної, адміністративної або карної відповідальності.

• спонукання – захист, який спонукує користувача й персонал системи не порушувати встановлений порядок за рахунок дотримання моральних і етичних норм, які склалися.

Таблиця 2.

Класифікація методів та засобів забезпечення безпеки інформації

Методи

Перешкоди	Керування доступом	Маскування	Регламентація	Примус	Спонукання

Засоби

Формальні			Неформальні		
Технічні		Програмні	Організаційні	Нормативні	Морально-етичні
Фізичні	Апаратні				

Розглянуті методи забезпечення безпеки реалізуються на практиці шляхом застосування різних засобів захисту, таких, як технічні, програмні, організаційні, законодавчі й морально-етичні. До основних засобів захисту, які використовуються для створення механізму забезпечення безпеки, належать такі.

Технічні засоби реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Уся сукупність технічних засобів поділяється на апаратні й фізичні.

Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Організаційні засоби – це організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення та експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їх життєвого циклу.

Морально-етичні засоби реалізуються у вигляді різних норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи.

Законодавчі засоби захисту визначаються нормативно-правовими актами, якими регламентуються норми та правила користування, обробки й передачі інформації обмеженого доступу. За порушення цих правил встановлюються відповідальність.

Захист інформації в системі обробки інформації повинен ґрунтуватися на наступних основних принципах:

1) системності;
2) комплексності;
3) безперервності захисту;
4) розумної достатності;
5) гнучкості керування й застосування;
6) відкритості алгоритмів і механізмів захисту;
7) простоти застосування захисних заходів і засобів.

Системний підхід до захисту комп'ютерних систем припускає необхідність обліку всіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння й вирішення проблеми забезпечення безпеки. При створенні системи захисту необхідно враховувати всі слабкі, найбільш уразливі місця системи обробки інформації, а також характер, можливі об'єкти й напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи й несанкціонованого доступу до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення й несанкціонованого доступу до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки [9].

4.3. Характеристика загроз інформаційній безпеці системи органів виконавчої влади

Загрози інформаційній безпеці, з одного боку, є організаційним компонентом функціонування системи органів виконавчої влади, а з іншого – індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчать про неефективність функціонування даної системи, і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв. Найнебезпечнішими на даному етапі розвитку українського суспільства є інформаційні війни [10].

На сьогодні саме інформаційні війни становлять одну з найбільших небезпек нормальному функціонуванню системи органів виконавчої влади. Це і зумовлює детальний розгляд нами питань щодо визначення поняття та встановлення суттєвих ознак інформаційної війни.

Інформаційна війна виникає з нових підходів до застосування інформації, визначення її ролі та місця. Можна виділити два визначення поняття інформаційної війни: гуманітарна і технічна.

Вважається, що у гуманітарному сенсі інформаційна війна являє собою активні методи трансформації інформаційного простору, що знаходять відображення у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на структури породження інформації – процеси міркувань. Водночас технічне трактування даного поняття полягає у тому, що за допомогою спеціальних програм руйнується обладнання, програмне забезпечення тощо. Що стосується іншого розуміння поняття інформаційної війни, себто технічного, то тут обов'язковою умовою є те, що ведення інформаційної війни є результатом узгодженої діяльності по використанню інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності. При цьому інформаційна війна включає такі дії:

- здійснення впливу на інфраструктуру систем життєзабезпечення – телекомунікації, транспортні мережі, електростанції тощо;
- хакінг – злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні: не фізичне знищення противника та ліквідація його збройних сил, а широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури та підкорення населення країни, що зазнала атаки, волі країни-переможця [26].

На Заході інформаційну війну визначають як "нефізичну атаку на інформацію, інформаційні процеси та інформаційну інфраструктуру", причому ціллю інформаційної війни є вплив на систему знань та уявлень зовнішнього супротивника. Під знанням тут розуміється об'єктивна інформація, загальна для всіх, а під уявленнями – інформація, що носить суб'єктивний характер. Основним інструментом ведення інформаційної війни є інформаційна зброя.

До "інформаційної зброї" ми будемо відносити, по-перше, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів. По-друге, це безперечно, інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на думку суспільства та на функціонування органів виконавчої влади.

Таким чином, інформаційна зброя – це пристрої та засоби, що призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів).

Виходячи зі змісту дослідження, об'єктами впливу інформаційної зброї можуть бути: інформаційно-аналітичні та інформаційно-технічні системи, які включають канали та засоби зв'язку органів виконавчої влади, інформаційні ресурси, державні засоби масової інформації, а також психологічний стан конкретного співробітника органу.

Інформаційна війна може бути спрямована проти трьох елементів [29]: комп'ютер, програмне забезпечення, людина.

Найбільш широко загрози інформаційним ресурсам системи органів виконавчої влади можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто знаходження джерела актуалізації певних подій у загрозі, характеризується таким елементом, як вразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, самі загрози за своєю суттю відповідно до теорії множин є невичерпними, отже вони не можуть бути описані у повному обсязі.

Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання [10, 30], можна виділити такі види загроз інформаційній безпеці:

– розкриття інформаційних ресурсів;

– порушення цілісності інформаційних ресурсів;

– збій у роботі обладнання.

Розглянемо більш детально кожний з цих видів.

Загроза розкриття інформаційних ресурсів полягає у тому, що дані, інформація та знання стають відомі необмеженій кількості осіб. У дослідженні стосовно системи органів виконавчої влади під загрозою розкриття будемо розуміти такий стан, коли отримано несанкціонований доступ до інформаційних ресурсів Секретаріату Кабінету Міністрів України, центральних та місцевих органів виконавчої влади, причому нас цікавлять як відкриті ресурси, такі і ресурси з обмеженим доступом. Ці ресурси мають передаватися один одному і зберігатися у єдиній інформаційній системі.

Загроза порушення цілісності інформаційних ресурсів полягає в зумисному антропогенному впливі (модифікація, видалення тощо) даних, які зберігаються в інформаційній системі органів виконавчої влади, а також передаються від даної інформаційної системи до інших. Система органів виконавчої влади складається з трьох рівнів, і якщо на рівні Секретаріату Кабінету Міністрів України і центральних органів управління така єдність є організованою, то зв'язки місцевих державних адміністрацій і Секретаріату Кабінету Міністрів України, а також органів

центральної виконавчої влади залишаються неналагодженими на відповідному рівні.

Загроза збою в роботі самого обладнання може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи. Насправді блокування може бути постійним, коли ресурс, що запитується, не може бути отриманим, або виникають затримки в його отриманні, що є достатнім для того, щоб він став некорисним.

Згідно з викладеним, розглядаються наступні загрози, що виникають відносно інформаційної безпеки системи органів виконавчої влади.

Найбільш частими і небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Іноді такі помилки є загрозами (невірно введені дані, помилки в програмі, котрі викликають колапс системи), іноді вони створюють ситуації, якими можуть скористатися зловмисники. Як свідчать фахівці, понад 65% шкоди, що завдається інформаційним ресурсам, – наслідки ненавмисних помилок [37]. Пожежі і землетруси, тобто загрози природного характеру, трапляються набагато рідше. Саме тому, враховуючи низьку імовірність реалізації загроз природного та техногенного характеру, пропонується максимально автоматизувати інформаційні системи органів виконавчої влади, а також ввести чіткий контроль за правильністю дій, що вчиняються.

Наступними, за розміром шкоди, можна виділити підлоги. У більшості випадків суб’єктами вчинення даних дій є штатні працівники структурних підрозділів органів виконавчої влади, які добре обізнані з роботою інформаційної системи, а також заходів безпеки [37]. У цьому аспекті дуже небезпечними є співробітники, які незадоволені або не поділяють цінностей тієї організації, де працюють. Як правило, діями ображених співробітників керує намагання нанести шкоду організації, в якій вони працювали і яка, на їхню думку, їх образила. Така образа може знайти відображення у вчиненні таких дій:

– пошкодження обладнання;
– вбудовування логічної бомби, яка з часом руйнує програми і дані;
– введення невірних даних;
– знищення даних;
– зміна даних;
– модифікація даних;
– надання доступу до даних із обмеженим доступом тощо.

Також серед загроз безпеці інформаційних систем чимало аналітичних служб визнають, що проблема інсайду – небезпечних дій в інформаційних системах власних працівників, як навмисних, так і пов'язаних з недбалістю та низкою кваліфікацією (рис. 4), стала головним трендом останніх років у багатьох організаціях і продовжує тільки загострюватися.

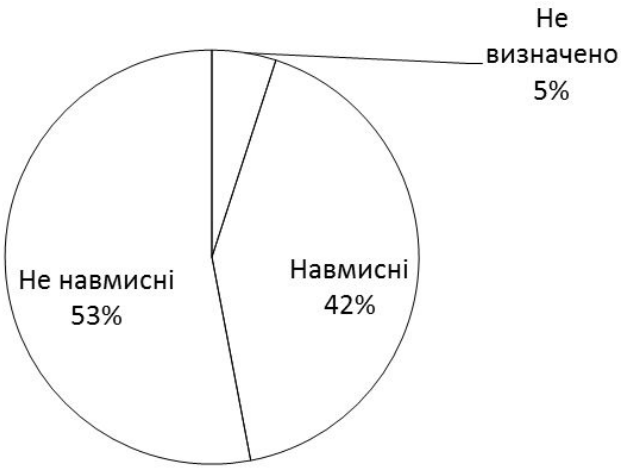

Рис. 4. ***Відношення кількості навмисних та ненавмисних витоків конфіденційної інформації***

Такі людські якості як користь, ненависть (помста, злість), страх, некомпетентність у міру зростання цінності даних, накопичених в організації, змушують працівників красти й "зливати" конфіденційні відомості, несанкціоновано модифікувати й знищувати інформацію, блокувати доступ до неї, запускати в мережу троянів і хробаків, виконувати інші дії, що інколи мають катастрофічні наслідки [77].

Невдоволені своїм становищем співробітники здатні дуже ефективно нашкодити інтересам органів, в яких вони працюють. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування з особами, що мають доступ до важливої інформації.

Ці загрози вельми актуальні для системи державної влади, до якої кіберзлочинці мають підвищений інтерес. Так, за даними Міністерства внутрішніх справ України щодо статистики різного роду мотивів при здійсненні комп'ютерних злочинів поряд із корисливими політичні мотиви посідають досить відчутне місце (рис. 5) [77].

Рис. 5. ***Статистика мотивів при здійсненні комп'ютерних злочинів***

Через чисельність видів загроз була зроблена спроба виокремити загрози інформаційній безпеці системи органів виконавчої влади [19].

Відомий аналітичний центр InfoWatch щорічно підбиває підсумки й представляє глобальні дослідження інцидентів внутрішньої інформаційної безпеки. За 2010 р. було проаналізовано всі витоки конфіденційної інформації, що згадувалися в ЗМІ у всіх країнах світу й в усіх галузях. За цими даними серед усіх інцидентів частка державних установ серед різних типів організацій, що зазнали втрат, сягнула вже майже 16% (рис. 6) [77]. При цьому:

1. За об'єктами, що підлягають розкраданню: апаратні засоби (блоки, вузли і готові вироби), якими оснащуються комп'ютери та мережі, носії програмного забезпечення й інформації, тверді копії із роздрукованою інформацією.

2. За способами здійснення розкрадань інформаційних джерел та носіїв: з робочих місць користувачів, в момент транспортування, з місць збереження.

3. За джерелами помилок у програмному забезпеченні (ПЗ):

логічні помилки розробників програмного забезпечення; непередбачені ситуації, що виникають при модернізації, заміні чи додаванні нових апаратних засобів, встановленні нових додатків, виході на нові режими роботи ПЗ, появі раніше незафіксованих нештатних ситуацій; віруси, якими інфіковані програми; спеціальні програмні компоненти, які передбачені розробниками ПЗ для різного роду цілей.

Рис. 6. ***Відношення кількості навмисних та ненавмисних витоків конфіденційної інформації в залежності від типу джерела***

Віруси самі по собі становлять також небезпеку і можуть проявлятися у видачі повідомлень на екран монітора; затиранні інформації на дисках; переміщенні фалів до інших папок; уповільненні роботи комп'ютера; зборі інформації про роботу організації тощо.

4. Залежно від мети здійснення атаки на інформаційні системи: встановлення доступу до інформації з обмеженим доступом; викрадення ключів, паролів, ідентифікаторів, списку користувачів; ініціалізація контрольованого алгоритму роботи комп'ютерної системи; доведення до непридатного стану частини або всієї системи органів державного управління.

5. За джерелами виникнення:

– природного походження – включають в себе небезпечні природні явища;

– техногенного походження – транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів виконавчої влади тощо;

– антропогенного походження – вчинення людиною різноманітних дій по руйнуванню інформаційних систем, ресурсів, програмного забезпечення системи органів виконавчої влади тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими, чи ненавмисними, діями людини (наприклад, помилковий запуск програми, ненавмисне інсталювання закладок тощо); навмисні (інспіровані), що стали результатом навмисних дій людей (наприклад: навмисне

інсталювання програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо).

6. За ступенем гіпотетичної шкоди:

– загроза – явні чи потенційні дії, що ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для органів виконавчої влади, життєзабезпечення її системостворюючих елементів;

– небезпека – безпосередня дестабілізація функціонування системи державного управління.

7. За ймовірністю реалізації:

– вірогідні – загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може бути оголошення атаки інформаційним ресурсам органів виконавчої влади, яке передує самій атаці;

– неможливі – загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай носять більше декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають характер залякування;

– випадкові – загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

8. За значенням:

– допустимі – такі загрози, що не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

– недопустимі – такі загрози, що: 1) можуть у разі їх реалізації призвести до колапсу та системної дестабілізації системи; 2) можуть призвести до змін, несумісних із подальшим існуванням системи національної безпеки.

9. За структурою впливу:

– системні – загрози, що впливають одразу на усі складові системи органів виконавчої влади. Цей вплив має відбуватись одночасно в декількох найбільш уразливих і важливих місцях. Для органу державного управління це може бути дискредитація працівників органів виконавчої влади через телебачення, радіо, друковані засоби масової інформації, Інтернет;

– структурні – загрози, що впливають на окремі ланки системи. Дані загрози є також небезпечними, водночас вони стосуються структури окремих органів державної влади або їх компонентів;

– елементні – загрози, що впливають на окремі елементи структури

системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або відсутності їх моніторингу;

10. За характером реалізації:

– реальні – активізація алгоритмів дестабілізації є неминучою та не обмеженою часовим інтервалом і просторовою дією;

– потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу виконавчої влади;

– здійснені – такі, що втілені у життя;

– уявні – псевдоактивізація алгоритмів дестабілізації або ж активізація таких алгоритмів, які за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

11. За відношенням до наявних загроз:

– об'єктивні – такі, що підтверджуються сукупністю обставин і фактів, які об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі, через те що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. На жаль, український законодавець у Законі України «Про основи національної безпеки України» не визначив пріоритетність захисту від інформаційних загроз, відвівши їм найменшу увагу;

– суб'єктивні – така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин та чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці.

12. За об'єктами впливу:

– Секретаріат Кабінету Міністрів України;

– центральні органи виконавчої влади;

– місцеві органи виконавчої влади.

Звичайно, що дана класифікація не претендує на універсалізм, втім ми намагалися, зважаючи на власну специфіку, продемонструвати багатоманітність і неоднаковість, багатошаровість і певну нескінченість загроз та небезпек інформаційній безпеці органів виконавчої влади.

4.4. Технічний захист інформації

В загальному комплексі заходів щодо забезпечення національної безпеки держави важливе місце займають заходи, пов'язані із безпосереднім захистом інформації від загроз, реалізація яких може нанести особі, суспільству, державі політичні, економічні, фінансові та інші збитки [67]. Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

1. Здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку

Незважаючи на позитивні зміни в міжнародній обстановки навколо України, діяльність технічних розвідок іноземних держав із здобування інформації продовжується. Проти України безперервно ведеться розвідка багатофункціональними космічними, повітряними, наземними, морськими системами та комплексами технічної розвідки. Провідні країни світу продовжують модернізувати свої розвідувальні служби, вдосконалюють технічну розвідку, нарощують її можливості.

Наявні можливості технічних розвідок практично вже сьогодні дають змогу забезпечити безперервне спостереження за всією територією України, і у подальшому, засоби технічної розвідки, зокрема космічної компоненти, будуть мати виключно високі характеристики, які дозволять забезпечити постійне стеження за всією територією держави в реальному масштабі часу.

2. Несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування систем обробки інформації

За умови недостатньої номенклатури засобів обробки інформації та програмного забезпечення вітчизняної розробки в інформаційно-телекомунікаційних системах широко використовуються продукти іноземного виробництва, які здебільшого не мають об'єктивних оцінок механізмів захисту, а також створюють передумови впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило широке розгортання інформаційно-телекомунікаційних систем, різке збільшення обсягів інформації, яка обробляється, зберігається в цих системах, значне збільшення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів тощо.

При цьому, за відсутності конкурентоспроможних вітчизняних зразків, перевага надається інформаційним технологіям та технічним засобам обробки інформації іноземного виробництва, які здебільшого не забезпечують захист інформації, а також створюють передумови неконтрольованого використання спеціальних програмних та апаратних засобів ("закладних пристроїв").

У світі зберігається тенденція поширення масштабів комп'ютерної злочинності, розповсюдження комп'ютерних вірусів, насамперед, з використанням Інтернет, істотно зростає небезпека наслідків неправомірних дій, технічних і технологічних помилок та збоїв при застосуванні інформаційно-телекомунікаційних систем, що є особливо

актуально в умовах широкого входження вітчизняних інформаційно-телекомунікаційних систем до глобальних.

Окремими державами реалізується "концепція інформаційного протиборства", яка полягає в реалізації заходів щодо спеціального впливу на інформаційну інфраструктуру з метою ураження (знищення) інформаційних ресурсів та руйнування системи управління в сферах оборони, економіки, безпеки, фінансів тощо.

3. Виток інформації з обмеженим доступом технічними каналами внаслідок виникнення побічних електромагнітних випромінювань і наведень, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об'єкту інформаційної діяльності

В процесі здійснення інформаційної діяльності для зберігання, обробки та передавання інформації, в тому числі й інформації з обмеженим доступом, широко використовуються технічні засоби різного призначення (засоби обчислювальної техніки, оргтехніка, засоби зв'язку, автоматизовані системи тощо). На об'єктах інформаційної діяльності здійснюється обговорення службових питань за різними напрямками діяльності установи, в ході яких може озвучуватися інформація з обмеженим доступом.

Проте, окремі фізичні процеси, що відбуваються в технічних засобах та під час обговорення інформації, та інші фактори створюють об'єктивні передумови для появи технічних каналів витоку інформації, що зумовлює необхідність реалізації заходів зі створення комплексів (систем) технічного захисту інформації, спрямованих на запобігання витоку інформації цими каналами.

Активний розвиток міжнародного співробітництва з закордонними державами в політичній, військовій, економічній та інших сферах призводить до широкого відкриття в державі іноземних дипломатичних установ та представництв, іноземних комерційних установ, розташування яких в безпосередній близькості від державних органів та установ створює передумови для здобування технічними засобами розвідки інформації з обмеженим доступом, яка циркулює на об'єктах інформаційної діяльності, що є особливо актуальним внаслідок широкого використання незахищених імпортних технічних засобів обробки інформації.

Всі ці фактори значно підвищують уразливість інформації і, як наслідок, визначають необхідність здійснення відповідних заходів з боку держави. При цьому вагомість негативних наслідків реалізації загроз інформації, насамперед, з обмеженим доступом, для національної безпеки обумовлюють загальнодержавну важливість заходів попередження таких загроз, а також зумовлюють необхідність переходу від фрагментарного відомчого підходу до формування і реалізації заходів з забезпечення технічного захисту інформації до систематичного та комплексного

підходу, залучення необхідного кадрового потенціалу, акумулювання необхідних ресурсів для вирішення проблеми захисту інформації.

Для протидії зазначеним загрозам в державі створена, функціонує та розвивається система технічного захисту інформації, яка є сукупністю організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази.

Відповідно до Концепції технічного захисту інформації в Україні технічний захист інформації визначено як складову частину забезпечення національної безпеки України.

Метою державної політики у сфері технічного захисту інформації є створення правових, організаційних, економічних засад функціонування системи технічного захисту інформації.

Побудова і організаційна структура системи технічного захисту інформації в Україні

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється у напрямах нормативно-правового і організаційного забезпечення, науково-технічної та виробничої діяльності. Важливість для безпеки держави галузі ТЗІ, її наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади, академій наук.

Ошибка! Объект не может быть создан из кодов полей редактирования.

Відповідно до цього, визначено основні принципи і концептуальні засади організації забезпечення ТЗІ в Україні. До таких належать:

– додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

– єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;

– комплексність, повнота та безперервність заходів ТЗІ;

– гармонізованість нормативно-правових актів та нормативних документів щодо ТЗІ з відповідними міжнародними договорами України та міжнародними стандартами;

– обов`язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади, інших державних органах та органах місцевого самоврядування, у допоміжних органах і службах Президента України, Національній

академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях;

– виконання на власний розсуд суб`єктами інформаційних відносин вимог щодо технічного захисту інформації, що є їхньою власністю, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних організацій;

– покладання відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

– ієрархічність побудови організаційної структури системи ТЗІ, суб'єкти якої належать до сфери управління або підпорядковані відповідній державній організації, та її керівництво діяльністю цих суб`єктів у межах повноважень, наданих нормативно-правовими актами;

– методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

– фінансова забезпеченість системи ТЗІ за рахунок державного бюджету, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Організаційна структура системи ТЗІ має ієрархічну деревовидну будову з підлеглістю і підзвітністю знизу-доверху по вертикалі та незалежністю суб'єктів одного рівня ієрархії.

Функції уповноваженого державного органу у сфері ТЗІ виконує Держспецзв'язку.

На відомчому рівні заходи із забезпечення ТЗІ здійснюються безпосередньо суб'єктами системи ТЗІ – міністерствами й іншими органами державної влади та підпорядкованими їм підприємствами, установами та організаціями, а відповідальність за організацію і стан захисту інформації покладається на їх керівників. Вони мають створювати або визначати підрозділи для оцінювання стану загроз інформації, розроблення та реалізації планів заходів щодо її захисту, координації діяльності інших суб'єктів у сфері підпорядкування, здійснення розрахунків та обґрунтувань потрібних для цього коштів.

На сьогодні нормативно-правовими актами повністю визначена правова основа функціонування всіх елементів організаційної структури системи ТЗІ, завдання і функції суб'єктів ТЗІ, їх права і обов'язки, порядок їх взаємодії і здійснення ними діяльності, а також порядок функціонування таких основних елементів як системи ліцензування і оцінювання продукції, підготовки і перепідготовки кадрів.

Одним з важливих напрямів діяльності в галузі ТЗІ є організація протидії технічним розвідкам. Організація протидії, своєчасне розроблення та впровадження необхідних заходів покладається на

керівника органу державної влади, органу місцевого самоврядування, органу управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України (далі орган), підприємства, установи, організації (далі організація). Проведення заходів протидії покладається на створений або визначений наказом керівника органу (організації) штатний чи позаштатний підрозділ ТЗІ або призначену особу.

Протидія технічним розвідкам (ПДТР) є невід'ємною складовою частиною систем охорони державної таємниці та захисту інформації з обмеженим доступом, яка є власністю держави (ІОДД) і здійснюється шляхом впровадження заходів щодо запобігання порушенню конфіденційності ІОДД засобами технічної розвідки. Сукупність впроваджуваних організаційних й інженерно-технічних заходів, програмних і технічних засобів, які використовуються для забезпечення протидії, є складовою частиною комплексу ТЗІ, спрямованого на приховування ІОДД та дезінформування технічних розвідок.

Держспецзв'язку здійснює організацію та координацію робіт з протидії, надання суб'єктам системи ТЗІ консультативної допомоги щодо застосування нормативних документів, забезпечення виявлення і прогнозування загроз для ІОДД, формування та супроводження моделей технічних розвідок, визначення напрямів робіт, розроблення нормативних документів системи ТЗІ, контроль за виконанням вимог нормативно-правових актів з питань протидії.

Слід зазначити, що сучасна система ПДТР була збудована на підґрунті, закладеному ще при СРСР. На час здобуття Україною самостійності в державі існувала система протидії іноземним технічним розвідкам (ПДІТР), організаційна структура якої базувалася на штатних підрозділах ПДІТР органів і організацій.

З проголошенням Україною незалежності система ПДІТР була трансформована в систему ТЗІ, а в більшості державних органів і організацій, діяльність яких пов'язана з ІОДД, на базі підрозділів ПДІТР були створені підрозділи ТЗІ, на які було покладено вирішення питань протидії і діяльність яких повинна узгоджуватися з діяльністю режимно-секретних органів. Одночасно розпочався процес розроблення вітчизняних нормативних документів з питань ТЗІ та створення засобів захисту інформації та захищених технічних засобів. Накопичений досвід з протидії не було втрачено – нормативні документи системи ПДІТР були ретельно переглянуті і деяким з них було надано чинності (в основному це стосується норм і методик).

Таким чином, на сьогодні організаційна структура ПД ТР є складовою частиною інфраструктури ТЗІ, а її діяльність повністю з нею узгоджується.

Ліцензування діяльності у галузі технічного захисту інформації

Одним з суттєвих важелів регулювання діяльності у сфері ТЗІ є процедура ліцензування діяльності суб'єктів господарської діяльності. Механізм ліцензування діяльності у сфері ТЗІ провадиться в Україні з 1995 року. Метою провадження ліцензування є формування в Україні контрольованого ринку послуг з ТЗІ, виконання вимог нормативних документів з питань захисту інформації, розповсюдження систем та засобів технічного захисту інформації, що відповідають законодавству України, а також виключення:

– передумов до можливості застосування засобів ТЗІ в протизаконних та злочинних діях, внаслідок їх неконтрольованого обігу в країні;

– можливості компрометації інформації з обмеженим доступом через надання некваліфікованих послуг та використання неякісних засобів ТЗІ, що може призвести до реальних загроз безпеці особистості, суспільству та державі;

– розповсюдження засобів ТЗІ, що не відповідають вимогам нормативних документів чи засобів низької якості, зокрема засобів іноземного виробництва, що може призвести до знищення вітчизняної галузі розробки та виробництва надійних, конкурентоспроможних засобів ТЗІ.

Таким чином, крім безпосередньо регулятивних і контрольних функцій ліцензування діяльності спрямоване також на розвиток матеріально-технічної бази системи ТЗІ.

Всього в галузі ТЗІ підлягає ліцензуванню 7 видів робіт, а саме:

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля, надання консультативних послуг;

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали, надання консультативних послуг;

– розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу, надання консультативних послуг;

– виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності, надання консультативних послуг;

– виробництво засобів забезпечення технічного захисту інформації, носіями якої є акустичні поля;

– виробництво засобів забезпечення технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є хімічні речовини, надання консультативних послуг.

На цей час за ліцензіями у сфері ТЗІ активно проводять діяльність понад 230 суб'єктів господарювання, які географічно охоплюють всі регіони України.

У зв'язку з тим, що органи державної влади та органи місцевого самоврядування не є суб'єктами господарювання і не можуть отримувати ліцензії, для них визначено порядок одержання дозволів на проведення робіт з технічного захисту інформації для власних потреб. Держспецзв'язку надає органам державної влади та органам місцевого самоврядування такі дозволи і здійснює контроль за проведенням ними визначених видів робіт. На цей час дозволи на проведення робіт з ТЗІ для власних потреб одержали 13 органів державної влади.

Система оцінювання продукції у сфері ТЗІ включає дві процедури – сертифікацію засобів ТЗІ та державну експертизу.

Сертифікація засобів технічного захисту інформації

Об'єктом сертифікації в галузі ТЗІ є окремі засоби ТЗІ, які можуть вироблятися як серійно, так і одиничні зразки, у тому числі сертифікації можуть підлягати і засоби імпортного виробництва. Процедура призначена надавати споживачу засобів ТЗІ гарантії відповідності цих засобів нормативним документам. Така гарантія може бути надана після проведення певних організаційно-технічних заходів. Результатом сертифікаційних робіт є спеціальний документ встановленого зразка – сертифікат відповідності.

Створення системи сертифікації засобів ТЗІ в Україні було розпочато ще в середині 90-х років і складність полягала в тому, що раніше ні в СРСР, ні в Україні не проводилася сертифікація засобів ТЗІ, до того ж на той час бракувало необхідної для досягнення цієї мети нормативно-правової та матеріально-технічної бази.

Порядок та вимоги щодо проведення сертифікації засобів ТЗІ визначаються Порядком проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення, який є обов'язковим як для акредитованих у системі органів з сертифікації засобів ТЗІ та випробувальних лабораторій, так і для підприємств, установ й організацій, у тому числі іноземних, які виготовляють і (або) постачають засоби ТЗІ у державні і недержавні установи, де циркулює інформація, що підлягає захисту у відповідності до законодавства.

На цей час в нашій державі сертифікація засобів ТЗІ проводиться акредитованими в Українській державній системі сертифікації продукції (УкрСЕПРО) органами та випробувальними лабораторіями. Зараз функціонують 2 органи із сертифікації та 2 випробувальні лабораторії.

За період функціонування системи сертифікації видано 94 сертифікати відповідності на 93 види засобів ТЗІ.

Державна експертиза у сфері технічного захисту інформації

Введення процедури експертного оцінювання комплексних систем захисту інформації в ІТС, технічних і програмно-апаратних засобів захисту інформації обумовлено логічною складністю сучасних програмно-апаратних комплексів, а також суттєвим впливом на безпеку інформації конкретних умов експлуатації ІТС, іншими словами такі об'єкти не повторюють один одного і кожний з них має тільки йому притаманні особливості. У випадках оцінки програмно-апаратних засобів закордонного виробництва, як правило, відсутня необхідна для проведення їх сертифікації технічна документація, практично неможливою є оцінка умов виробництва, організація взаємодії органів сертифікації з закордонними виробниками засобів захисту.

Правову основу цієї процедури складає Закон України "Про наукову та науково-технічну експертизу". Методологічною основою є експертиза технічних рішень і організаційних заходів, які базуються як на узагальненні висновків окремих експертів, так і на результатах інструментальних вимірювань і випробувань комплексу програмно-апаратних і технічних засобів захисту інформації.

Порядок проведення державної експертизи в сфері ТЗІ, основні функції й права суб'єктів експертизи визначено Положенням про державну експертизу в сфері технічного захисту інформації.

У відповідності з законодавством у ньому визначені суб'єкти експертизи (Замовник, Організатор експертизи, Експерт), основні функції ДСТСЗІ СБ України та суб'єктів експертизи, порядок їх взаємодії, порядок документального оформлення результатів експертизи та видачі Експертного висновку (для окремих засобів захисту інформації) і Атестату відповідності на комплексні системи захисту інформації в ІТС.

Наявність позитивного рішення щодо засобу є підставою для його включення до Переліку засобів технічного захисту інформації загального призначення, які дозволені до використання з метою ТЗІ, а наявність атестату відповідності - підставою для одержання дозволу на обробку в ІТС інформації, що підлягає захисту.

Система державної експертизи функціонує з початку 2000 року і за цей час стала одним з найбільш вагомих чинників реалізації державної політики у галузі, а її результати – розвитку матеріально-технічної бази

системи ТЗІ та наповнення ринку ефективними конкурентоспроможними програмно-апаратними засобами захисту інформації.

На сьогодні зареєстровано 44 організації, яким надано повноваження проводити експертні випробування, а до Реєстру експертів внесено близько 265 висококваліфікованих спеціалістів у галузі ТЗІ.

Загалом проведено експертизу і видано 98 експертних висновків на окремі засоби захисту інформації та 467 атестатів відповідності на КСЗІ в ІТС.

Науково-технічна діяльність у галузі технічного захисту інформації

Науково-технічна діяльність у галузі ТЗІ здійснюється шляхом формування, супроводження та контролю за виконанням комплексних та цільових програм, метою яких є розвиток та удосконалення трьох складових системи ТЗІ.

Науково-технічна діяльність у галузі ТЗІ започаткована у 1994 році, коли вперше в Україні було розроблено Науково-технічну програму "Розвиток системи технічного захисту інформації України" та Програму робіт з організації стандартизації та сертифікації в галузі технічного захисту інформації на 1995-1998 рр. Програми передбачали проведення науково-дослідних та дослідно-конструкторських робіт в рамках державного оборонного замовлення. Переліки запланованих науково-дослідних та конструкторських робіт та потрібні обсяги їх фінансування визначалися окремо на кожний рік.

Всього в рамках обох зазначених Програм проведено 87 науково-дослідних та дослідно-конструкторських робіт з питань технічного захисту інформації загальною вартістю 2143,65 тис. грн. За їх результатами розроблено 44 проекти нормативних документів системи ТЗІ, створено 11 макетних та дослідних зразків засобів забезпечення ТЗІ та випробувального обладнання.

На поточний час наукові та прикладні дослідження здійснюються згідно з Державною програмою розвитку криптографічного та технічного захисту інформації на період до 2008 року, затвердженою постановою Кабінету Міністрів України від 24.12.2002 р. № 1941-22.

Реалізація завдань Програми забезпечить подальший розвиток та удосконалення технічного захисту інформації в Україні, поетапний перехід до використання в України вітчизняних технологій та засобів забезпечення технічного захисту інформації, сприятиме подальшому розвитку існуючого науково-технічного та промислового потенціалу держави.

Контрольні питання

1. Основні принципи та задачі захисту інформації в електронному урядуванні.
2. Державна політика у сфері забезпечення інформаційної безпеки в умовах впровадження електронного урядування в Україні.
3. Основна термінологія систем захисту інформації.
4. Обов'язкові процедури, що виконуються для забезпечення захисту інформації з обмеженим доступом.
5. Функції комплексних систем захисту інформації.
6. Основні принципи захисних заходів від несанкціонованого доступу в автоматизованих системах.
7. Компоненти, що пов'язані з порушенням безпеки інформаційної системи.
8. Класифікація та зміст методів і засобів забезпечення безпеки інформації.
9. Основні дії інформаційної війни.
10. Види загроз інформаційній безпеці.
11. Особливості необхідності технічного захисту інформації.
12. Найбільш впливові загрози інформації.
13. Основні принципи і концептуальні засади організації забезпечення технічного захисту інформації в Україні.
14. Ліцензування та сертифікація засобів технічного захисту інформації.

ГЛОСАРІЙ

ДОКУМЕНТ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

ЕЛЕКТРОННИЙ ДОКУМЕНТ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи його обов'язкові реквізити, склад та порядок розміщення яких визначається законодавством.

ЕЛЕКТРОННИЙ ПІДПИС – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

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

ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ (е-ресурси) – це систематизовані дані, інформація та знання, що мають цінність у певній предметній області і можуть бути використані людиною в своїй діяльності для досягнення певної мети.

ІНФОРМАЦІЙНА ЗАГРОЗА – це сукупність умов і чинників, що створюють потенційну або реально існуючу небезпеку порушення конфіденційності, доступності і (чи) цілісності інформації.

ІНФОРМАЦІЙНА СИСТЕМА (англ. – *Information System*) – організаційно-технічна система, яка впорядковує сукупність елементів (людей, документів, даних, інформації тощо) та інформаційних технологій, що реалізують інформаційні процеси, підтримують управлінську діяльність та прийняття рішень.

ПРОГРАМНЕ ЗАСТОСУВАННЯ (англ. Application**) –** програма, призначена для виконання певних завдань користувача і розрахована на безпосередню з ним взаємодію.

СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ (*система автоматизації документообігу*) – організаційно-технічна система, що забезпечує процес створення, управління доступом і поширення електронних документів в комп'ютерних мережах, а також що забезпечує контроль над потоками документів в організації.

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 в інший спосіб.

Список рекомендованої літератури

1. Вехов В. Б. Компьютерные преступления: Способы совершения, методики расследования – М.: Право и Закон, 2010.– 181 с.
2. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навч. посібник. – К.: Юстініан, 2006. – 176 с.
3. Гречко А.В. Основи електронного документообігу: Навч. посібник / Київський національний торговельно-економічний ун-т. – К., 2006. – 156 с.
4. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту: [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua.
5. Дрешпак В. М. Інформаційно-аналітичне забезпечення органів місцевої влади : навч. посіб. / В. М. Дрешпак, Т. М. Брус, О. В. Тинкован та ін. ; за заг. ред. В. М. Дрешпака ; Нац. акад. держ. упр. при Президентові України, Дніпропетр. регіон. ін-т держ. упр. - Дніпропетровськ : ДРІДУ НАДУ, 2007. – 159 с.
6. Дурняк Б. В. Семантичний захист інформації в системах документообігу. Інформаційні технології [Текст] : монографія / Б. В. Дурняк, В. І. Сабат. - Л. : Вид-во Укр. акад. друкарства, 2010. – 160 с.
7. Іванова Т.В., Піддубна Л.П. Діловодство в органах державного управління та місцевого самоврядування: підруч. – К.: – 2007. –290 с.
8. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К.. ДСТСЗІ СБ України, 1999 – 16 с.
9. Зибін С.В. Захист інформації від несанкціонованого доступу в системах обробки інформації // Інформаційна безпека. – 2011. – №1.
10. Зіма І.І. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) / І.І. Зіма, І.М. Ніколаєв.– К.: Наука і оборона. – 1998. – № 1. – С. 56-58.
11. Клименко І. В. Електронний документообіг у державному управлінні [Текст] : навч. посіб. / Клименко І. В., Линьов К. О., Горбенко І. Д., Онопрієнко В. В. ; Нац. акад. держ. упр. при Президентові України. – К. ; Х. : ФОРТ, 2009. – 232 с.
12. Клименко І.В., Линьов К.О. Система електронного документообігу в державному управлінні: Навч.-метод. посіб. – К.: Вид-во НАДУ, 2006. – 32 с.
13. Круковський М. Ю. Рішення електронного документообігу. – К.: "Азимут-Україна". 2006. – 112 с.
14. Кузьменко Б. В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки: навч. посібник. – К.: НАУ, 2008. – 164 с.

15. Кукарін О.Б., Логвинов В.Г., Мазуркевич М.В., Марчук О.В. Ресурс інформаційний. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 545-547.

16. Кукарін О.Б., Марчук О.В. Інфраструктура електронного урядування технологічна. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 235-236.

17. Кукарін О.Б., Марчук О.В. Система інформаційна. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011, Т.1. Теорія державного управління. – с. 518-520.

18. Кукарін О.Б., Марчук О.В. Технології інформаційні. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 615-616.

19. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України / В.А. Ліпкан– К.: Текст, 2009. – 600 с.

20. Марчук О. В Захист інформації. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 170-172.

21. Марчук О. В. Документ електронний. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 142-144.

22. Марчук О. В. Документообіг електронний. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 144-146.

23. Марчук О. В. Підпис електронний цифровий. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 447-449.

24. Матвієнко О.В. Основи організації електронного документообігу [Текст] : навч. посіб. для студ. вищ. навч. закл. / О. В. Матвієнко, М. Н. Цивін. – К. : Центр учбової л-ри, 2008. – 111 с.

25. Нестеренко О.В. Засади забезпечення необхідного рівня інформаційної безпеки державної влади: [Електронний ресурс] – Режим доступу:
http://www.nbuv.gov.ua/portal/soc_gum/nac_bez/2009_4/pdf/nesterenko.pdf.

26. Почепцов Г. Г. Информационные войны / Г.Г. Почепцов, С.Л. Удовик (отв. ред.). – М.: Рефл-бук, 2000. – 576 с.

27. Почепцов Г. Г., Чукут С. А. Інформаційна політика. – К.: Вид-во "Знання", 2008. – 665 с.

28. Раздорожный А. А. Документирование управленческой деятельности: Уч. пособ. – М.: ИНФРА-М, 2007. – 304 с.

29. Ракитов А.И. Философия компьютерной революции / А.И. Ракитов. – М.: Политиздат, 1991. – 287 с.

30. Рибак М.І. До питання про інформаційні війни / М.І. Рибак, А.В. Атрохов. – К.: Наука і оборона. – 2003. – № 2 – С. 65-68.

31. Соколов В. С. Документационное обеспечение управления: Учебник. – 2-е изд. – М.: ФОРУМ: ИНФРА-М, 2007. – 176 с.

32. Степко О. М. Аналіз головних складових безпеки держави: [Електронний ресурс] – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Nvimvnau/2011_1/83-92.pdf.

33. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТСЗІ СБ України, 1999. - 26 с.

34. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие / Хорев А.А. – М.: Гостехкомиссия России, 1998. – 320 с.

35. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. – М. : МО РФ, 1998. – 224 с.

36. Хорев А.А. Способы и средства зашиты информации. – М.: МО РФ, 2006. – 316 с.

37. Ярочкин В.И. Информационная безопасность: Учеб. для студ. вузов, обуч. по гуманит. и соц.-экон. спец. – М.: Фонд «Мир», 2009. – 640 с.

38. Директива 1999/93/ЕС Європейського Парламенту та Ради від 13 грудня 1999 року "Про систему електронних підписів, що застосовується в межах Співтовариства" (DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Офіційний журнал L 013, 19/01/2000 p. 0012 – 0020. Переклад здійснено Центром перекладів актів Європейського права при міністерстві юстиції України): [Електронний ресурс] – Режим доступу: http://uazakon.com/document/spart50/inx50337.htm.

39. Про державну таємницю : Закон України від 21 січня 1994 № 3855-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

40. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-IV: [Електронний ресурс] – Режим доступу: http:// www.rada.gov.ua

41. Про електронний цифровий підпис : Закон України від 22 травня 2003 р. № 852-IV: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

42. Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

43. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

44. Про національну систему конфіденційного зв'язку України від 10 січня 2002 № 2919-III : Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

45. Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади : Постанова Кабінету Міністрів України від 17 жовтня 1997 р. № 1153: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

46. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : Постанова Кабінету Міністрів України від 4 лютого 1998 р. № 121: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

47. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади : Постанова Кабінету Міністрів України від 10.09.2003 р. № 1433: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

48. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова Кабінету Міністрів України від 26 травня 2004 р. № 680: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

49. Про затвердження Порядку акредитації центру сертифікації ключів : Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

50. Про затвердження Положення про центральний засвідчувальний орган : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

51. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1452: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

52. Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1453: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

53. Про затвердження Порядку обов'язкової передачі документованої інформації : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1454: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

54. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

55. Про затвердження загальних вимог до програмних продуктів, які закуповуються або створюються на замовлення державних органів : Постанова Кабінету Міністрів України від 12 серпня 2009 р. № 869: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

56. Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України : Постанова Національного банку України від 17 червня 2010 р. № 284: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

57. Про схвалення Концепції створення багатофункціональної комплексної системи: "Електронна митниця" : Розпорядження Кабінету Міністрів України від 17 вересня 2008 р. № 1236: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

58. Про погодження створення Засвідчувального центру Національного банку України : Розпорядження Кабінету Міністрів України від 6 травня 2009 р. № 483: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

59. Про затвердження плану заходів із запровадження електронного документообігу, пов'язаного з перевезенням вантажів залізничним транспортом : Розпорядження Кабінету Міністрів України від 16 грудня 2009 р. № 1557: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

60. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

61. Питання впровадження системи електронної взаємодії органів виконавчої влади : Розпорядження Кабінету Міністрів України від 28 грудня 2011 р. № 1363: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

62. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 р. № 141: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

63. Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від

24 липня 2007 р. № 143: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

64. Технічні специфікації форматів криптографічних повідомлень. Захищені дані : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 травня 2010 р. № 112: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

65. Про затвердження Правил посиленої сертифікації : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 р. № 3: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

66. Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення : Наказ Міністерства освіти і науки, молоді та спорту України від 20.10.2011 № 1207: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

67. Біла книга Держспецзв'язку – розділ 7. Технічний захист інформації: [Електронний ресурс] – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941.

68. Про затвердження Технічних умов на систему електронного документообігу органу виконавчої влади : Наказ Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України від 7 червня 2005 р. № 70 (ТУ У 30.0-33240054-001:2005).

69. Про затвердження Порядку зберігання електронних документів в архівних установах : Наказ Державного комітету архівів України від 25 квітня 2005 р. № 49: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

70. Про затвердження Технічних специфікацій форматів представлення базових об'єктів національної системи електронного цифрового підпису : Наказ Державного комітету України з питань науки, інновацій та інформатизації та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 13 серпня 2010 р. № 8/229: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

71. Про внесення змін до деяких нормативно-правових актів : Наказ Міністерства інфраструктури України від 8 червня 2011 р. № 138 (зареєстровано в Міністерстві юстиції України 24 червня 2011 р. за № 763/19501): [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

72. Про використання апаратних носіїв ключової інформації систем криптографічного захисту інформації : Лист Національного банку України від 10 грудня 2010 р. № 24-112/2550-22346: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

73. Реєстр суб'єктів – засвідчувальних центрів та акредитованих центрів сертифікації ключів: [Електронний ресурс] – Режим доступу: http://www.czo.gov.ua/index.php?page=reestr.

74. Специфікація MoReq "Типові вимоги до автоматизованих систем електронного документообігу": [Електронний ресурс] – Режим доступу: http://www.cornwell.co.uk/moreq.html.

75. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".

76. ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания".

77. Глобальное исследование утечек информации за 2010 год [Електронний ресурс] – Режим доступу: http://www.infowatch.ru/analytics.

Навчальне видання

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ ТА ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник

Укладач
Кукарін Олександр Борисович

Загальна редакція

Грицяк Наталя Вітіславна