МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

В. Я. Пєвнєв, Т. В. Лавровська

ІНФОРМАЦІЙНА БЕЗПЕКА. ТЕРМІНИ І ВИЗНАЧЕННЯ

Довідник

Харків «ХАІ» 2016

УДК 004.056.3:34(477)(035)
ББК 32.973.018
П 23

Рецензенти: д-р техн. наук, проф. Г. А. Кучук,
д-р техн. наук, проф. О. А. Серков

Пєвнєв, В. Я.
П 23 Інформаційна безпека. Терміни і визначення [Текст] : довідник / В .Я. Пєвнєв, Т. В. Лавровська. – Х. : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харк. авіац. Ін-т», 2016. − 84 с.

Розглянуто питання, які пов'язані із забезпеченням інформаційної безпеки. Детально викладено існуючі значення інформаційної безпеки, науково обґрунтовано визначення, що відображає тимчасову залежність. Проаналізовано можливі загрози і методи протидії їм. Описано математичну модель інформаційної безпеки. Терміни і їхні визначення, подані у довіднику, відповідають нормативно-правовим документам.

Для викладачів, аспірантів, студентів, які вивчають дисципліни, пов'язані з інформаційною безпекою і захистом інформації.

Табл. 1. Бібліогр.: 53 назви

УДК 004.056.3:34(477)(035)
ББК 32.973.018

© В .Я. Пєвнєв, Т. В. Лавровська, 2016
© Національний аерокосмічний університет
ім. М. Є. Жуковського
«Харківський авіаційний інститут», 2016

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система

ЗАЗ - засоби активного захисту

ЗІ - захист інформації

ЗС - замкнута система

ІБ - інформаційна безпека

ІС - інформаційна система

КЗ - контрольована зона

КЗІ - криптографічний захист інформації

МЕН - морально-етичні норми

НСД - несанкціонований доступ

ОПД – об’єкти протидії

ОТЗС - основні технічні засоби і системи

ТЗЗІ - технічні засоби захисту інформації

ТЗІ - технічний захист інформації

ВСТУП

Розвиток інформаційних технологій наприкінці XX– початку XXI ст. привів до необхідності зростання окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. У сучасному світі інформація є найціннішим глобальним ресурсом.

Інформаційна складова на сучасному етапі розвитку суспільства являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, оброблення, формування, розповсюдження та використання інформації. З’явився новий термін – «інформаційно-комунікаційні технології». Ці технології включають як процеси, що забезпечують життєвий цикл інформації, так і технічні засоби, що підтримують ці процеси.

Інформаційна сфера є системоутворюючим фактором життя суспільства. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів і рівнем розвитку інформаційної інфраструктури. Усе частіше поняття "інформація" використовується як позначення спеціального товару, який можна придбати, продати, обміняти на щось інше. При цьому вартість інформації часто перевершує у сотні й тисячі разів вартість комп'ютерної системи, в якій вона знаходиться. Тому цілком природно виникає необхідність у захисті інформації від несанкціонованого доступу, умисної модифікації, крадіжки, знищення та інших злочинних дій. Разом із розвитком способів і методів перетворення і передачі інформації постійно розвиваються і методи забезпечення її безпеки.

Сучасний етап розвитку цієї проблеми характеризується переходом від традиційного її подання як питання захисту інформації до більш широкого розуміння - проблеми інформаційної безпеки (ІБ), що полягає у комплексному її вирішенні.

Забезпечення ІБ поступово виходить на перший план у проблематиці національної безпеки. Прийнята у 2009 році Доктрина інформаційної безпеки України [1] свідчить про те, що ІБ стає найважливішою складовою національної безпеки. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без

застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

Особливої актуальності ІБ набуває у зв'язку з використанням технічних засобів оброблення і передачі інформації, прогнозування й аналізу розвитку держави, суспільства і особистості. ІБ держави, насамперед, забезпечує її розвинена економіка, яка дозволяє створювати умови безпеки особистості, суспільства як від внутрішніх, так і зовнішніх загроз. А з цим з'являються необмежені можливості доступу правопорушників до інформаційних ресурсів користувачів з метою порушення цілісності інформації.

Аналізуючи існуючу літературу, можна дійти висновку, що для пересічного громадянина неможливо самостійно визначити терміни, які використовуються у галузі «інформаційна безпека». Оскільки не існує точних визначень, котрі б повною мірою розкривали зміст цих термінів, то в різних законодавчих документах вони різні.

Метою написання довідника є розроблення визначення ІБ, що відповідає вимогам наукової термінології, та створення тезаурусу в галузі ІБ.

У першому розділі аналізуються сучасні визначення поняття ІБ, обґрунтовується запропоноване визначення, яке відповідає вимогам наукової термінології.

У другому розділі розглянуто загрози ІБ, методи і засоби її забезпечення і запропоновано математичну модель ІБ.

У третьому розділі надано терміни, які відносяться до сфери ІБ, та їх визначення, що наведені у керівних документах. У тому випадку, коли один термін має різні тлумачення, запропоновано усі можливі варіанти.

У додатках наведено деякі нормативно-правові документи, які стосуються сфери ІБ, і список допоміжної літератури з інформаційної безпеки.

Розділ 1 ІНФОРМАЦІЙНА БЕЗПЕКА

1.1 Аналіз існуючих визначень терміна «інформаційна безпека»

За сучасних умов інформаційна складова набуває дедалі більшої значущості та стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Інформаційна безпека (ІБ) є невід'ємною складовою кожної зі сфер національної безпеки. Водночас ІБ є важливою самостійною сферою забезпечення національної безпеки.

Саме тому розвиток України, як суверенної, демократичної, правової та економічно стабільної держави, можливий тільки за умови забезпечення належного рівня її ІБ [1,2].

Згідно з [2] в інформаційній сфері України вирізняються ІБ особи, суспільства і держави.

ІБ особи - це [2]:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- недопущення несанкціонованого втручання у зміст, процеси оброблення, передачі та використання персональних даних;
- захищеність від негативного інформаційно-психологічного впливу.

ІБ суспільства - це [2]:

- збереження і примноження духовних, культурних і моральних цінностей українського народу;
- забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди;
- формування і розвиток демократичних інститутів громадянського суспільства.

ІБ держави - це [2]:

- недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав і міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного і науково-технологічного розвитку України;

– формування позитивного іміджу України;

– інтеграція України у світовий інформаційний простір.

Визначити термін ІБ складно, оскільки нормативно-правова база України не має закону про ІБ та однозначного тлумачення терміна ІБ у других законах. Існує велика кількість визначень, що пояснюють значення ІБ, але всі вони досить специфічні або характеризують цю область досить у вузькому діапазоні. Розглянемо визначення ІБ, яке надано в Законі [3].

Інформаційна безпека - це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Таке визначення має глибоке протиріччя, яке його дискредитує. Поставимо запитання: «Що таке несанкціоноване розповсюдження інформації?» Відповімо: «Це означає, що будь-яка інформація має отримати дозвіл на її поширення». Це також означає наявність органу, який дає цей дозвіл, тобто цензора, який обмежує доступність інформації. Зрозуміла наявність цього органу, коли йдеться про конфіденційну інформацію, але в цьому фрагменті визначення береться до уваги вся інформація, оскільки про конфіденційну інформацію йдеться нижче. Про це написано також і в Конституції України, ст.15 «… Цензура заборонена…»

У ст.24 Закону України «Про інформацію» наведено, що «забороняється цензура - будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання у будь-якій іншій формі тиражуванню або поширенню інформації». Тобто наведене визначення суперечить існуючому закону.

Розглянемо такий фрагмент: «***запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується***». Це свідчить про те, що повна, своєчасна і достовірна інформація не може завдати шкоди. Але подальшим висловом

«***негативний інформаційний вплив*** » виключається така можливість. Слід зазначити, що перший розглянутий фрагмент у цьому абзаці є ніщо інше, як порушення цілісності інформації, про яку йдеться у кінці визначення.

Абсолютно незрозуміло, які можуть бути «***негативні наслідки застосування інформаційних технологій***», якщо дотримується цілісність, конфіденційність і доступність інформації. Негативні наслідки можуть настати при використанні достовірної інформації, яка несе потенційну загрозу. При цьому інформація залишається відкритою і доступною. У цьому фрагменті відбувається підміна понять - ІБ замінюється на поняття «небезпечна інформація».

У роботі [4] ІБ описується як захищеність встановлених законом правил, за якими відбуваються інформаційні процесі в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави. Таке тлумачення ототожнює ІБ й ІБ держави, тобто звужує саме поняття ІБ.

У роботі [5] ІБ трактується, як стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від внутрішніх і зовнішніх інформаційних загроз. Це поняття є точною копією визначення ІБ, котре покладене в основу Доктрини інформаційної безпеки і законодавства у сфері забезпечення інформаційної безпеки Російської Федерації.

У роботі [6] дається таке тлумачення ІБ: стан, що забезпечує захищеність інформаційних ресурсів і каналів, а також доступ до джерел інформації. Таке поняття вельми близько до поняттям ІБ інформаційних систем.

У роботі [7] ІБ розуміється як захищеність інформації на будь-яких носіях від випадкових і навмисно несанкціонованих впливів природного чи штучного характеру, спрямованих на знищення, руйнування, видозміни тих чи інших даних, зміна ступеня доступності цінних відомостей. Це поняття ІБ вживається у досить вузькому розумінні та прирівнюється до безпеки інформації.

ІБ - це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [8].

Це визначення є найбільш оптимальним, оскільки воно об'єднує пасивну (стан захищеності) та активну (стан інформаційного розвитку) складові й передбачає поділ інформаційної безпеки на різновиди. Але у цьому визначенні є заміна поняття ІБ на безпечну інформацію. Автор у роботі [8] взяв за основу класифікацію інформаційної безпеки, яку наведено у [2], змінивши її значення з точки зору суспільства і психічного здоров’я особи.

1.2 Визначення інформаційної безпеки

Історично поняття ІБ з'явилося, як калька англійського терміна information security або information . Рівнозначний його переклад – «захист інформації». У роботі [9] термін information security перекладено як «безпека інформації», що означає стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. У професійному співтоваристві information перекладається як інформаційна надійність, тобто мають на увазі технічну складову.

Слід розглянути такі особливості ІБ, ґрунтуючись на яких, можна дати визначення цьому терміну. Коли говорять про ІБ, то розмова йдеться про якусь систему, наприклад про державу, корпорацію, телекомунікаційну мережу або про щось інше. Під системою розуміється об'єднання деякого розмаїття в єдине і чітко розчленоване ціле, елементи якого по відношенню до цілого та інших частин займають відповідні їм місця [10]. Кожна система має ряд властивостей і може перебувати у тому чи іншому стані.

Стан системи – це її характеристика на певний момент функціонування [11]. Поняття стану характеризує миттєву «фотографію», тимчасовий «зріз» системи. Стан системи у певний момент часу - це безліч її істотних властивостей у цей момент [12].

Поняття ІБ завжди має бути логічно прив'язаним до інформації, засобів її оброблення, зберігання, доставлення, впливу на об'єкт. У життєвому циклі інформація може бути піддана різного роду впливам, які спрямовані на порушення конфіденційності, цілісності та доступу до неї. Слід зазначити, що у багатьох нормативних документах як ІБ, так і ІБ держави, розглядаються у конкретний момент часу, наприклад говориться, що «Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України до конкретних умов певного історичного періоду» [2]. Тобто, ІБ має бути забезпеченою деякий час. Залежно від системи цей час може бути різноманітним.

На підставі викладеного пропонується таке визначення ІБ: ***інформаційна безпека - властивість системи у перебігу заданого часу протистояти несанкціонованому зняттю і модифікації інформації*** [13].

Під несанкціонованим зняттям розуміється отримання інформації, до якої у абонента немає доступу, тобто є порушення правил доступу. Під несанкціонованою модифікацією розуміється зміна інформації, яка призводить до порушення її цілісності. Слід зазначити, що цілісність у загальному випадку це не тільки отримана інформація у початковому вигляді, але і її повнота.

Розглянувши детально всі аспекти терміна «інформаційна безпека», логічно буде навести також і його складові. Оскільки інформаційна безпека являє собою комплекс заходів, то основним завданням його є забезпечення таких властивостей інформації :

- конфіденційність - можливість ознайомитись з інформацією (саме з даними або відомостями, що несуть смислове навантаження, а не з послідовністю біт їх подання) мають тільки ті особи, які на це уповноважені;
- цілісність - право ввести змінення в інформацію (знову мова йде про смислове вираження) мають тільки ті особи, хто на це уповноважені;
- доступність - можливість отримання авторизованого доступу до інформації з боку уповноважених осіб у відповідний санкціонований для роботи період часу.

Допоміжні фактори, які дають змогу конкретизувати ІБ:

- облік, тобто всі значущі дії особи, виконувані нею в рамках, контрольованих системою безпеки (навіть, якщо вони не виходять за рамки визначених для цієї особи правил), мають бути зафіксовані й проаналізовані;
- неспростовність – запобігання можливості заперечення реальними суб'єктами та об'єктами фактів повного або часткового взяття участі в інформаційному обміні або інформаційній взаємодії;
- спостережливість – можливість фіксувати роботу та дії користувачів і процесів, використання ресурсу системи, однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів, а також реагувати на ці події з метою мінімізації можливих втрат у системі;
- апелювання (характерно для організацій, в яких функціонує обмін електронними документами від юридичної, фінансової або іншої спрямованості), тобто особа, що направила інформацію іншій особі, не може відректися від факту направлення інформації, а особа, що отримала інформацію, не може відректися від факту її отримання [14].

Розділ 2 ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Загрози інформаційній безпеці

Аналіз і виявлення загроз ІБ є важливою складовою для забезпечення ІБ. Тому під загрозою, згідно з [15], розуміється витік, можливість блокування чи порушення цілісності інформації. Чіткіше формулювання загроз дається в роботі [16]. Вони визначаються як сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації.

Найчастіше загроза є наслідком наявності уразливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення, а також відсутність системи протидії різноманітним програмам, які завдають шкоду або порушують процес роботи обчислювальних засобів.

В наш час існує досить великий перелік загроз ІБ, що нараховує сотні пунктів. Найбільш характерні й найчастіше використовувані з них перелічені в роботі [17].

- За типом загроз:
  а) природні загрози;
  б) штучні загрози.

  До природних відносять такі загрози, які мають природний характер. Це можуть бути землетруси, цунамі, повінь, гроза і т.ін. До такого типу загроз можна віднести і пожежу, але за однією умови, що вона виникла не з вини людини.

  Штучні загрози виникають у результаті людської діяльності. До їхнього виникнення призводять, як цілеспрямовані протиправні дії, так і звичайна неуважність, порушення правил роботи з обладнанням, приладами, носіями інформації.
- За місцем розташування джерела загроз:
  а) зовнішня загроза;
  б) внутрішня загроза;
  в) внесена загроза.

  Під зовнішніми розуміють такі загрози, що виникають за межами периметра КЗ. До цього типу загроз можна віднести: можливість зняття інформації за допомогою електромагнітного випромінювача або перехоплення повідомлень під час їх передачі по лініях зв’язку (телефонних, повітряних, оптоволоконних).

  Внутрішні загрози виникають всередині периметра КЗ. Частіше за все це дефекти об’єктів і апаратури, порушення

правил і заходів безпеки, правил експлуатації, які можуть призвести до витоку, спотворення і модифікації або до знищення інформації.

Найнебезпечнішими є внесені загрози. Під такими загрозами слід розуміти завчасно внесені дефекти в обладнання, споруди, технічні системи і програмні продукти, які не були виявлені в процесі випробувань і експлуатації, неточності в експлуатаційній документації, а також вмонтовані у будівельні конструкції, приміщення або прикріплені до сувенірів або подарунків пристрої для зняття інформації.

- За впливом на інформацію:
  а) несанкціоноване зняття;
  б) спотворення (аж до знищення);
  в) відмова;
  г) нав'язування.

  Під несанкціонованим зняттям розуміють використання технічних та інших засобів отримання інформації. При цьому можливе як підключення до носіїв інформації, так і використання побічних факторів. До цього виду загроз можна віднести прослуховування телефонних ліній, прийом паразитних електромагнітних випромінювань, приховану фото- і відеозйомку.

  Під спотворенням необхідно розуміти дії, спрямовані на порушення цілісності інформації. Це єдина загроза, яка може виникнути незалежно від людини.

  Під відмовою слід розуміти заперечення достовірної інформації. Ця загроза може здійснюватись, як при наявності помилок в експлуатаційній документації, так і з причини наявності дефектів.

  Під нав'язуванням слід розуміти інформацію, прийняту до виконання, яка була отримана або від фіктивної особи, або відправлена від імені відомої особи, але сфальсифікована порушником. Іншими словами, така загроза передбачає прийняття помилкової інформації за істинну.

- За типом доступу до інформації:
  а) несанкціонований доступ;
  б) блокування доступу.

  Під несанкціонованим доступом (НСД) розуміється незаконне проникнення в закритий інформаційний простір. Згідно з роботою [15], НСД – це доступ до інформації, при якому порушуються порядок його здійснення і встановлені правові норми. Як приклад можна розглянути доступ до закритих баз

даних силових відомств або банківських структур осіб, які не мають прав на доступ до цих даних.

Під блокуванням розуміється такий стан системи, який не дозволяє здійснити законний доступ до всієї інформації, що циркулює в цій системі, або до будь-якої її частини. Таке блокування можна здійснити, наприклад, за допомогою хакерської атаки, коли на сервер за короткий час приходить така кількість запитів, які неможливо обслужити.

- За часом впливу на інформацію бувають такі загрози:
  а) миттєві;
  б) тривалі;
  в) відстрочені.

Як приклад миттєвої загрози можна показати дію електромагнітного імпульсу на елементи пам'яті.

Загрози тривалої дії дозволяють накопичувати або руйнувати інформацію за якийсь, досить тривалий, проміжок часу.

Відстроченою загрозою будемо називати такі загрози, які починають діяти або в заздалегідь призначений час, або після закінчення певного терміну. Як приклад можна показати загрозу знищення інформації при пожежі, якщо при будівництві був прокладений електричний провід меншого діаметра, ніж було заплановано під час проектування.

Слід зазначити, що найбільшою загрозою ІБ можуть бути співробітники, що мають доступ до комп'ютерних мереж, до інформації з обмеженим доступом, що володіють тими чи іншими виробничими технологіями.

2.2 Методи і засоби забезпечення інформаційної безпеки

Для забезпечення ІБ необхідно застосовувати нормативно-правові та морально-етичні норми (МЕН), технічні засоби захисту інформації (ТЗЗІ).

Правовий захист інформації як ресурс визнано на міжнародному, державному рівні й визначається міждержавними договорами, конвенціями, деклараціями і реалізується патентами, авторським правом і ліцензіями на їх захист. Також кожна самостійна держава повинна брати участь у розробленні нормативно-правових актів, що регламентують відносини в інформаційній сфері, та нормативно-методичних документів з питань забезпечення ІБ.

В нашій державі такими юридичними нормами виступають Конституція України, Закони України, Укази Президента та Постанови Кабінету Міністрів, а також Державні стандарти і накази Адміністрації Держспецзв'язку, які регулюють відносини стосовно ІБ.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства щодо захисту інформації, його складу та змісту, зіставлення його з усією системою законів і правових актів України. Вимоги ІБ повинні органічно включатися в усі рівні законодавства, в тому числі й у конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні закони, відомчі правові акти та інші [18].

Організаційний захист - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво перешкоджає неправомірному оволодінню конфіденційною інформацією і прояву внутрішніх і зовнішніх загроз.

Організаційний захист забезпечує:

- організацію охорони, режиму, роботу з кадрами, з документами;
- використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності.

Організаційні заходи відіграють важливу роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей значною мірою зумовлюються не технічними аспектами, а зловмисними діями, недбалістю і халатністю користувачів або персоналу захисту. Впливу цих аспектів практично неможливо уникнути за допомогою технічних засобів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних заходів, які зводили б до мінімуму можливість виникнення небезпеки для конфіденційної інформації.

До основних організаційних заходів можна віднести:

- організацію режиму і охорони. Їх мета: виключення можливості таємного проникнення на територію і у приміщення сторонніх осіб; забезпечення зручності контролю проходу і переміщення співробітників і відвідувачів; створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу; контроль і дотримання тимчасового режиму праці та перебування на території персоналу фірми, організація і підтримання надійного пропускного режиму та контролю співробітників і відвідувачів та інше;
- організацію роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення із співробітниками, їх вивчення, навчання їх правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та інше;
- організацію роботи з документами і документованою інформацією, включаючи організацію розроблення і використання

документів і носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;

- організацію використання технічних засобів збирання, оброблення, накопичення і зберігання конфіденційної інформації;
- організацію роботи з аналізу внутрішніх і зовнішніх загроз конфіденційній інформації та вироблення заходів щодо забезпечення її захисту;
- організацію роботи щодо проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

Завдання забезпечення інформаційної безпеки має вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні взаємодіяти і забезпечувати захист, як від зовнішніх, так і від внутрішніх загроз [18].

Засоби технічного захисту інформації – це технічні засоби, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування технічних засобів, у яких додатково до основного призначення передбачено функції захисту інформації, засоби, що призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв, які створюють загрозу для інформації, або контролю ефективності технічного захисту інформації [19].

ЗТЗІ, які присутні в наш час на ринку, умовно можна розділити на кілька груп:

- активні й пасивні технічні засоби, що забезпечують захист від витоку інформації у різних фізичних полях, що виникають при застосуванні засобів її оброблення;
- програмні та програмно-технічні засоби, що забезпечують розмежування доступу до інформації на різних рівнях, ідентифікацію та автентифікацію користувачів;
- програмні та програмно-технічні засоби, що забезпечують захист інформації та підтвердження її справжності при передачі по каналах зв'язку;
- програмно-апаратні засоби, що забезпечують цілісність програмного продукту і захист від несанкціонованого його копіювання;
- програмні засоби, що забезпечують захист від впливу програм-вірусів та інших шкідливих програм;
- фізико-хімічні засоби захисту, що забезпечують підтвердження достовірності документів, безпеку їх транспортування і захист від копіювання.

До пасивних засобів захисту відносяться:

- екранування приміщень об'єкта з малою КЗ, в яких розміщені ОТЗС;
- установка в колах електроживлення ОТЗС електричних протизавадних фільтрів.

До засобів активного захисту (ЗАЗ) відносяться:

- засоби просторового зашумлення;
- екранування приміщень, яке застосовується у випадках, коли контрольована зона від ОТЗС перевищує розміри контрольованої зони об'єкта.

Слід також розуміти, що не можна захиститися від усіх загроз ІБ хоча б тому, що неможливо передбачити дії зловмисників, не кажучи вже про всі помилки користувачів. Однак існує ряд загальних методів захисту, які дозволяють значно понизити вірогідність реалізації широкого спектру загроз та захистити підприємство від різного роду атак і помилок користувачів.

Вибір методів аналізу стану забезпечення ІБ залежить від конкретного рівня і сфери організації захисту. Залежно від різних рівнів загроз, ставиться завдання щодо різних рівнів захисту. Що стосується сфери ІБ у ІС, то у ній зазвичай виділяють такі рівні:

- фізичний;
- програмно-технічний;
- управлінський;
- технологічний;
- рівень користувача;
- сітьовий;
- процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, а також управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики ІБ спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На сітьовому рівні така політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт [20].

2.3 Математична модель інформаційної безпеки

Оскільки ІБ - це властивість системи у перебігу заданого часу протистояти несанкціонованому зняттю і модифікації інформації, то завданням математичної моделі ІБ є разом із відомими критеріями визначення ІБ, такими, як конфіденційність, цілісність, доступність, треба врахувати і час, протягом якого система є захищеною.

Математичну модель ІБ можна записати у вигляді [13]:

$$\sum_{i}^{n} f\left(C_i, I_i, A_i\right) \Rightarrow max \qquad (1)$$

при

$$f(C_i, I_i, A_i) > D_{зад_i},$$

де $f\left(C_i, I_i, A_i\right)$ - значення функції ІБ для ***i***-ї загрози;

n- кількість загроз;

C_i, I_i, A_i - ймовірність порушення цілісності, доступності та конфіденційності для ***i***-ї загрози;

$D_{зад_i}$ - заданий рівень ІБ ***i***-ї загрози.

З урахуванням визначення ІБ формулу (1) можна записати так:

$$\sum_{i}^{n} f(C(\Delta t)_i, I(\Delta\ t)_i, A(\Delta t)_i) \Rightarrow max \qquad (2)$$

при

$$\Delta\ t > t_{зад}$$

$$\Delta t = t_{зз} - t_{пз},$$

де $\Delta\ t$ - час,протягом якого реалізується ***i***-а загроза цілісності, доступності або конфіденційності ІБ;

$t_{зад}$ – час, протягом якого необхідно підтримувати заданий рівень ІБ;

$t_{пз}$, $t_{кз}$ - час початку і закінчення дії загрози відповідно.

Запропонований підхід дозволяє формалізувати роботи по проектуванню і експлуатації систем захисту інформації, за допомогою яких реалізуються вимоги до ІБ систем.

Список літератури до розділів 1,2

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр/page.

2. Указ Президента України «Про Доктрину інформаційної безпеки України» [Електронний ресурс] : чинний від 08.07.09 № 514/2009. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/514/2009.

3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електронний ресурс] : чинний від 09.01.07 № 537-V. – Режим доступу: http://zakon4.rada.gov.ua/rada/show/537-16.

4. Кормич, Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Б. А. Кормич. – Київ : Кондор, 2004. – 384 с.

5. Богуш, В. М. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдин. – Київ : МК-Прес, 2005. – 432 с.

6. Рогозин, Д. О. Война и мир в терминах и определениях : воен.-полит. слов. / Д. О. Рогозин. – М. : ПоРог, 2004. – 624 с.

7. Степанов, Е. А. Информационная безопасность и защита информации : учеб. пособие / Е. А. Степанов, И. К. Корнеев. – М. : ИНФРА-М, 2001. – 304 с.

8. Информационно-психологическая безопасность в эпоху глобализации : учеб. пособие / В. М. Петрик, В. В. Остроухов, А. А. Штоквиш и др.; под. ред. В. В. Остроухова. – Киев, 2008. – 544 с.

9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://library.detut.edu.ua/images/stories/zahyst_info/23.pdf.

10. Философский энциклопедический словарь / ред.-сост.: Е. Ф. Губский, Г. В. Кораблева, В. А. Лутченко. – М. : ИНФРА-М, 2000. – 576 с.

11. Лопатников, Л. И. Экономико-математический словарь. Словарь современной экономической науки / Л. И. Лопатников. – 5-е изд., перераб. и доп. – М. : Дело, 2003. – 520 с.

12. Состояние системы [Електронний ресурс]. – Режим доступу: http://e-educ.ru/tsisa11.html.

13. Певнев, В. Я. Математическая модель информационной безопасности / В. Я. Певнев, М. В. Цуранов // Системи обробки інформації: зб. наук. пр. / МО України, ХУПС. – Харків, 2010. – № 3 (84). – С. 62–64.

14. Конеев, И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 752 с.

15. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Чинний від 01.01.98. – Київ : Держстандарат України, 1997. – 16 с.

16. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 01.02.08. – М. : Стандартинформ, 2008. – 8 с.

17. Певнев, В. Я. Анализ угроз информационной безопасности замкнутых систем / В. Я. Певнев // Радіоелектронні і комп'ютерні системи. – 2010. – № 6 (47). – С. 84–85.

18. Ярочкин, В. И. Информационная безопасность : учеб. для вузов / В. И. Ярочкин. – 2-е изд. – М. : Акад. проект, 2004. – 544 с.

19. Технические средства защиты информации [Електронний ресурс]. – Режим доступу: http://www.itdom.info/Bezpeka/TS1.html.

20. Методи забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki

Розділ 3 ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

Для розроблення тезаурусу було відібрано всі чинні Закони, Укази Президента та Постанови Кабінету Міністрів, а також стандарти в області захисту інформації. Крім того, було розглянуто деякі накази Адміністрації Держспецзв'язку та діючи Накази Департаменту спеціальних телекомунікаційних систем і захисту інформації служби безпеки України.

Загалом було оброблено 33 нормативно-правових документи. Усі визначення розташовані в алфавітному порядку. Таблицю побудовано таким чином: у першому стовпчику дається назва терміна; у другому – визначення цього терміна; у третьому – номер документа, з якого взято визначення терміна. У четвертому стовпчику надані посилання на допоміжну літературу, список якої наведено у додатку Б.

Під час складання таблиці термінів (табл.3.1) виникли колізії, тобто випадки, коли один термін має різні тлумачення. Це пояснюється тим, що нормативно-правовий документ тлумачить визначення у такому аспекті, який потребує визначена галузь застосування. Наприклад, витік інформації - це:

- результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї [30];
- неконтрольоване поширення інформації, яке призводить до її несанкціонованого отримання [19];
- результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [31];
- результат дій, унаслідок яких інформація у інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [4].

Таблиця 3.1 - Терміни та їх визначення

Термін	Визначення терміна	Джерело	Література
Автентифікація	– процедура встановлення належності користувачеві інформації в системі поданого ним ідентифікатора	[22]	[13]
Автоматизована система (АС)	– система, що здійснює автоматизоване оброблення даних і до складу якої входять технічні засоби їх оброблення (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення	[1, 7]	[13]
Автор електронного документа	– фізична або юридична особа, яка створила електронний документ	[6]	[12]
Адреса мережі Інтернет	– визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв	[14]	[1]
Адресат	– фізична або юридична особа, якій адресується електронний документ	[6]	[12]
Акредитація	– процедура документального засвідчення компетентності центру сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів	[5]	
Активне приховування інформації	– це приховування інформації створенням таких фізичних полів і речовин, які утруднюють здобування інформації або спричиняють невизначеність її змісту	[2]	[18]
Аналітично-синтетичне оброблення науково-техніч-ної інформації	– це процес оброблення інформації шляхом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінювання, зіставлення і узагальнення	[12]	
База даних	– іменована сукупність даних, що відображає стан об'єктів та їхніх відношень у визначеній предметній області	[11]	[15]
База знань	– масив інформації у формі, придатній до логічного і смислового оброблення відповідними програмними засобами	[11]	[15]
База персональних даних	– іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотеки персональних даних	[9]	[15]
Безпека даних автоматизованої системи	– властивість організації доступу до даних, що забезпечує їх захист від несанкціонованого використання, навмисного чи ненавмисного спотворення або руйнування	[1]	[15]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Безпека урядового або спеціального зв'язку	– стан зв'язку (системи зв'язку), який забезпечується запобіганням можливому витоку інформації, що передається в системі зв'язку (порушення режимів роботи системи зв'язку)	[1]	
Безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ)	– електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднанні до одного комутаційного центру	[14]	[13]
Блокування інформації	– дії, внаслідок яких припиняється доступ до інформації	[1,7]	[15]
Блокування інформації в системі	– дії, внаслідок яких унеможливлюється доступ до інформації в системі	[8]	[15, 16]
Блокування сертифіката ключа	– тимчасове зупинення чинності сертифіката ключа	[5]	[30]
Верифікація	– експертні дослідження, які здійснюються з метою установлення відповідності об'єкта експертизи зразку-свідку	[16]	
Використання інформації	– це задоволення інформаційних потреб громадян, юридичних осіб і держави	[1]	[30]
Вироби	– комплекси, системи, засоби, окремі установки, агрегати, блоки, вузли, прилади, хімічні продукти, апаратура, обладнання, макети тощо, з чого можна отримати інформацію	[30]	
Витік інформації	– результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї; – неконтрольоване поширення інформації, яке призводить до її несанкціонованого отримання; – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї; – результат дій, унаслідок яких інформація в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах стає відомою або доступною фізичним та/або юридичним особам, що не мають права доступу до неї	[7] [2] [8]	[28]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Відкритий ключ	– параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису	[5]	[30]
Віднесення інформації до державної таємниці	– процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування і визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього	[4]	
Відомості, що охороняються	– секретна інформація стосовно ОПД, що становить державну таємницю	[18]	
Відповідний орган	– орган держави Сторони, який згідно з чинним законодавством відповідає за захист таємної інформації та матеріалів	[30]	
Взаємоз'єднання телекомунікаційних мереж	– встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією	[14]	[13]
Власник інформації	– фізична або юридична особа, якій належить право власності на інформацію	[8]	[30]
Власник системи	– фізична або юридична особа, якій належить право власності на систему	[8]	[30]
Володілець персональних даних	– фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на оброблення цих даних, яка затверджує мету оброблення персональних даних у цій базі даних, встановлює склад цих даних і процедури їх обробки, якщо інше не визначено законом	[9]	[15]
Впровадження комплексу (системи) ТЗІ	– стадія життєвого циклу комплексу (системи), яка пов'язана із реалізацією передбачених проектною документацією інженерно-технічних заходів, проведенням приймальних (атестаційних) випробувань, складанням акта прийняття комплексу (системи) в експлуатацію	[17]	[15, 16, 17]
Вторинний документ	– це документ, який є результатом аналітико–синтетичного та іншого перероблення одного або кількох документів	[1]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Втрата інформації	– дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі	[1,7]	[15]
Геоінформаційні системи	– сучасні комп'ютерні технології, що дають можливість поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (статистичні дані, списки, економічні показники тощо)	[11]	
Гриф секретності	– реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації; – реквізит носія секретної інформації, що засвідчує ступінь секретності цієї інформації, який проставляється на носії секретної інформації або вказується у супровідній документації до нього; – реквізити, що наносяться на носій інформації або що вказуються у супровідній документації до нього, які свідчать про ступінь секретності інформації, що міститься в носії	[4,31] [25] [27]	
Дані	– інформація, яка подана у формі, придатній для її оброблення електронними засобами; – інформація у формі, придатній для автоматизованого оброблення її засобами обчислювальної техніки	[6] [14]	[15]
Дезінформування	– спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації	[2]	[8]
Державна експертиза у сфері КЗІ	– діяльність, метою якої є підготовка обґрунтованих висновків і надання рекомендацій для прийняття рішення про використання (застосування) об'єктів експертизи та яка передбачає перевірку відповідності об'єктів експертизи вимогам нормативних документів і (або) нормативно-правових актів, оцінку рівня захисту інформації об'єктами експертизи або науково-технічного рівня об'єктів експертизи	[16]	[28]
Державна інформаційна політика	– це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації	[1]	[22]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Державна система урядового зв'язку	– система спеціального зв'язку, яка призначена для забезпечення управління державою у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайних ситуацій. Забезпечує додержання вимог законодавства з питань захисту інформації, яка містить державну таємницю	[3]	
Державна таємниця	– вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України	[1,4]	
Державний експерт з питань таємниць	– посадова особа, уповноважена здійснювати, відповідно до вимог Закону, віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування	[4]	
Державний реєстр баз персональних даних	– єдина державна інформаційна система збирання, накопичення та оброблення відомостей про зареєстровані бази персональних даних	[9]	
Державні інформаційні ресурси	– інформація, яка є власністю держави; необхідність захисту її визначено законодавством	[3]	
Довгостроковий ключовий елемент	– ключ, що визначає заповнення таблиць блока підстановки алгоритму криптографічного перетворення	[15]	
Довідково-інформаціний фонд	– це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб	[12]	
Довідково-пошуковий апарат	– це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел	[12]	
Договір	– договір, угода або контракт, що укладається між уповноваженими органами держав-Сторін, у рамках якого утворюється або передається секретна інформація	[25]	
Дозвіл	– документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб	[33]	
Документ	– матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі й просторі	[10]	[16]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Документи	– конструкторська, технічна та інша документація, текстові та графічні матеріали, виконані будь-яким способом: рукописним, друкарським, машинописним, магнітним, копіювальним, перфоративним, кіно- і фототехнічним, комп'ютерним, відео- і аудіозаписом тощо	[30]	[16]
Документообіг	– процес переміщення документів, що використовуються в службовій діяльності, який включає підготовку, оброблення, зберігання, надання інформації, необхідної для видання актів управління, здійснення управлінських процедур, оформлення службових документів, котрі юридично підтверджують певні факти, складання планів, кошторисів, довідок службового характеру, ведення обліково-статистичної роботи, архівів, діловодство (ведення канцелярських справ)	[1]	[16]
Домен	– частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен і централізовано адмініструється	[14]	[16]
Домен.UA	– домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет	[14]	[16]
Домен другого рівня	– частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у мережі	[14]	[16]
Допуск до державної таємниці	– оформлення права громадянина на доступ до секретної інформації	[4]	
Допуск до секретної інформації	– процедура оформлення права фізичних осіб на доступ до секретної інформації, уповноважених органів; – на проведення робіт із використанням такої інформації; – право громадянина на доступ до секретної інформації; – процедура оформлення права фізичних і юридичних осіб на ознайомлення з секретною інформацією	[25] [31] [27] [26]	
Дослідження ефективності комплексу (системи) ТЗІ	– визначення відповідності фактичного рівня ТЗІ, який забезпечується комплексом (системою), вимогам нормативних документів з ТЗІ	[17]	[19]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Дослідження об’єктів інформаційної діяльності, інформаційних систем щодо безпеки інформації	– вивчення і аналіз проектної, програмної документації, технологічних процесів, інформаційних потоків, умов функціонування об’єктів інформаційної діяльності, інформаційних систем із метою визначення загрози безпеці інформації щодо її витоку, блокування чи порушення цілісності	[1]	[1,28]
Доступ до державної таємниці	– надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та проведення діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та проведення діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень	[4]	
Доступ до інформації (ТЗІ)	– можливість одержання, оброблення інформації, її блокування та (чи) порушення цілісності	[2]	[19]
Доступ до інформації в системі	– отримання користувачем можливості обробляти інформацію в системі; – надання дозволу фізичній або юридичній особі на ознайомлення із секретною інформацією	[8] [25]	[19]
Доступ до секретної інформації	– санкціонований відповідною посадовою особою дозвіл на ознайомлення з секретною інформацією і проведення роботи з нею; – дозвіл фізичній або юридичній особі знайомитися з секретною інформацією	[31] [27]	
Доступність	– властивість інформації бути захищеною від несанкціонованого блокування	[35]	[20]
Експертиза в галузі КЗІ	– науково-технічна діяльність, метою якої є дослідження, аналіз, оцінка або перевірка рівня захисту інформації в засобах КЗІ	[20]	[30]
Експертний висновок	– документально оформлений результат експертизи, який надається Адміністрацією Державної служби спеціального зв'язку та захисту інформації України за проведеним аналізом результатів експертних досліджень; – відповідним чином документально оформлені результати експертизи	[16] [20]	
Експертні дослідження	– дослідження і аналіз конкретних властивостей об'єкта експертизи з метою перевірки його відповідності вимогам нормативних документів і (або) нормативно-правових актів, оцінки рівня захисту інформації цим об'єктом або його науково-технічного рівня	[16]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
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	[5]	[12]
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	[5]	[12]
Ефективність технічного захисту інформації	– ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам	[2]	[15, 16, 17]
Загроза для Інформації	– витік, можливість блокування чи порушення цілісності інформації	[2]	[1]
Закладний пристрій	– потай установлений технічний засіб, який створює загрозу для інформації	[2, 17]	[17]
Замовник	– юридична особа будь-якої форми власності, яка замовляє встановленим порядком ключі до засобів КЗІ, у тому числі засобів електронного цифрового підпису, у яких реалізується криптографічний алгоритм; – організація, що робить замовлення в рамках контракту; – організація, яка дає замовлення в рамках контракту	[15] [28] [31]	
Засвідчення чинності відкритого ключа	– процедура формування сертифіката відкритого ключа	[5]	[30]
Засекречування матеріальних носіїв інформації	– введення у встановленому законодавством порядку обмежень на поширення і доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації	[4]	[30]
Засіб електронного цифрового підпису	– програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису	[5]	[12]
Засіб крипто-графічного захис-ту інформації	– апаратний, програмний, апаратно-програмний або інший засіб, призначений для криптографічного захисту інформації	[20] [32]	[30]
Засіб технічного захисту інформації	– пристрій та(чи) програмний засіб, основним призначенням яких є захист інформації від загроз	[2]	[15, 16, 17]
Засоби захисту інформації	– технічні, програмні та інші засоби, які використовуються для захисту інформації, а також засоби контролю ефективності захисту інформації	[23]	[15, 16, 17]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Засоби інформатизації	– електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їхні окремі елементи, інформаційні мережі й мережі зв'язку, що використовуються для реалізації інформаційних технологій	[11]	[15]
Засоби технічного захисту інформації	– технічні засоби, основним функціональним призначенням яких є захист порушення цілісності та блокування технічних засобів, у яких додатково до основного призначення передбачено функції захисту інформації, засоби, що призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв, які створюють загрозу для інформації, або контролю ефективності технічного захисту інформації	[17]	[17, 18]
Захист інформації в системі	– діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі	[8]	[15, 17]
Зразок-свідок	– зразок об'єкта експертизи, який отримав позитивний експертний висновок і призначений для проведення верифікації інших зразків об'єкта експертизи на відповідність цьому зразку	[16]	
Звід відомостей, що становлять державну таємницю	– акт, у якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених законом сферах	[4]	
Згода суб'єкта персональних даних	– будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки	[9]	
Знеособлення персональних даних	– вилучення відомостей, які дають змогу ідентифікувати особу	[9]	
Знищення інформації в системі	– дії, внаслідок яких інформація в системі зникає	[8]	[5]
Зона безпеки інформації	– простір, за межами якого інформація убезпечена	[2]	[6]
Ідентифікація	– процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою	[21]	[14]
Інтернет	– всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором і базується на Інтернет-протоколі, визначеному міжнародними стандартами	[14]	[30]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Інформативний сигнал (ТЗІ)	– фізичне поле та (чи) хімічна речовина, що містять інформацію з обмеженим доступом	[2]	[16, 17]
Інформатизація	– сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки	[11]	
Інформаційна атака	– дія, спрямована на завдання супротивнику конкретного відчутного збитку в окремих галузях його діяльності	[1]	[8]
Інформаційна безпека	– стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається завдання шкоди внаслідок: неповноти, невчасності та недостовірності інформації, що використовується; негативного інформаційного впливу; негативних наслідків застосування інформаційних технологій; несанкціонованого поширення, використання й порушення цілісності, конфіденційності та доступності інформації	[1]	[1]
Інформаційна безпека телекомунікаційних мереж	– здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації	[14]	[31]
Інформаційна війна	– це цілеспрямовані інформаційні впливи, що здійснюються суб’єктами впливу на мішені (об’єкти впливу) з використанням інформаційної зброї для досягнення запланованої мети	[1]	[8]
Інформаційна зброя	– засіб проведення запланованих дій з інформацією або ж алгоритм цілеспрямованого впливу на інформаційну систему шляхом передання такій системі інформації (або здійснення з інформацією інших запланованих дій)	[1]	[8]
Інформаційна послуга	– дії суб'єктів щодо забезпечення споживачів інформаційними продуктами	[11]	[24]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Інформаційна (автоматизована) система	– організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; – автоматизована система, комп'ютерна мережа або система зв'язку	[8] [33]	[24]
Інформаційна система загального доступу	– сукупність телекомунікаційних мереж і засобів для накопичення, оброблення, зберігання та передавання даних	[14]	[24]
Інформаційна сфера (середовище)	– сфера діяльності суб’єктів, пов’язана із створенням, перетворенням і споживанням інформації	[1]	[24]
Інформаційна технологія	– цілеспрямована, організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування	[11]	[8]
Інформаційний потік	– інформація, яка переміщується у просторі й часі	[1]	[24]
Інформаційний продукт (продукція)	– документована інформація, яка підготовлена і призначена для задоволення потреб користувачів	[11]	[24]
Інформаційний простір	– це простір, у якому циркулюють інформаційні потоки, властивості яких задаються інформаційною інфраструктурою	[1]	[24]
Інформаційний ресурс	– сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)	[1,11]	[24]
Інформаційний ринок	– це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг	[12]	[8]
Інформаційний суверенітет держави	– здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави	[1,11]	
Інформаційні процеси	– процеси збирання, оброблення, накопичення, зберігання, актуалізації, пошуку й поширення інформації	[1]	[31]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Інформаційні ресурси науково-технічної інформації	– це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях	[12]	
Інформаційні ресурси спільного користування	– це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які ведуть науково-технічну діяльність і з власниками яких укладено договори про їх спільне використання	[12]	
Інформаційно-телекомунікаційна система	– сукупність інформаційних і телекомунікаційних систем, які у процесі оброблення інформації діють як єдине ціле	[8]	[31]
Інформація	– будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді; – документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі й навколишньому природному середовищі; – будь-яка інформація, у будь-якій формі, в тому числі письмовій, усній або візуальній; – відомості про об'єкти, процеси та явища; – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи іншим способом	[10] [1] [29] [2] [14]	[15]
Інформація в АС	– сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного подання	[7]	[15]
Інформація з обмеженим доступом	– інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами; – інформація, право доступу до якої обмежено відповідно до національних законодавств держав-Сторін	[2] [23]	[15]
Канал електрозв'язку	сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі	[14]	[30]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Категорія режиму секретності	– категорія, яка характеризує важливість і обсяги відомостей, що становлять державну таємницю, ці відомості зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях	[4]	
Ключові дані	– деякий набір значень змінних параметрів криптографічного перетворення, використання яких дає змогу досягти мети цього перетворення	[20]	
Ключові документи	– матеріальні об'єкти із зафіксованими відповідним чином ключовими даними для подальшого практичного застосування щодо криптографічного перетворення повідомлення	[20]	[30]
Кінцеве обладнання	– обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг	[14]	
Компетентний орган	– державний орган, відповідальний за координацію діяльності щодо реалізації угоди при здійсненні міждержавного співробітництва; – державний орган, відповідальний за виконання угоди при здійсненні міждержавного співробітництва або виконанні окремих контрактів, на які поширюється дія угоди; – уповноважений орган виконавчої влади, відповідальний за виконання угоди або окремих її статей	[24] [28] [30]	
Комплекс (система) ТЗІ	– сукупність заходів і засобів, призначених для реалізації ТЗІ на об'єкті інформаційної діяльності	[17]	[15]
Комплекс технічного захисту інформації	– сукупність заходів і засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті	[33]	[15, 16, 17]
Комплексна система захисту інформації	– взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації	[8]	[15, 16, 17]
Компрометація особистого ключа	– будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа	[5]	[30]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Комп'ютерний вірус	– програма, що розмножується та поширюється самочинно; комп'ютерний вірус може порушувати цілісність інформації, програмне забезпечення та (чи) режим роботи обчислювальної техніки	[2]	[31]
Контракт	– договір, угода або контракт, що укладаються між організаціями держав-Сторін, у рамках якого створюється або передається секретна інформація; – зовнішньоекономічний договір (угода, контракт), у рамках якого суб'єкти зовнішньоекономічної діяльності можуть здійснювати діяльність, пов'язану з секретною інформацією	[28] [30]	
Контрольно-інспекторська робота з питань ТЗІ	– діяльність, спрямована на визначення та вдосконалення стану ТЗІ в органах, відносно яких здійснюється ТЗІ	[18]	[15, 16, 17]
Конфіденційна інформація	– відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов	[1, 20]	[20, 21]
Конфіденційність	– властивість інформації бути захищеною від несанкціонованого ознайомлення	[33]	[22]
Користувач	– юридична або фізична особа, яка відповідно до національного законодавства уповноважена використовувати секретну інформацію	[25]	[1]
Користувач АС	– фізична або юридична особа, яка має право використання АС за угодою із розпорядником АС	[1,7]	[1]
Користувач інформації в системі	– фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі	[8]	[1]
Криптографічна система (криптосистема)	– сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається	[32]	[30]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Криптографічний захист інформації	– вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства	[4,8, 20,32]	[30]
Ліцензія	– документ, що засвідчує право суб'єкта господарювання на здійснення зазначеного в ньому виду діяльності у сфері телекомунікації протягом визначеного строку на конкретних територіях з виконанням ліцензійних умов	[14]	[1]
Ліцензування	– видача, переоформлення, продовження терміну дії, визнання недійсними, анулювання ліцензій, видача копій та дублікатів ліцензій, ведення ліцензійних справ і ліцензійних реєстрів, контроль за додержанням ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов	[14]	[1]
Локалізація програмних продуктів	– приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, стандартами, нормами і правилами, що діють в Україні	[11]	[31]
Матеріали	– будь-які документи, вироби, речовини або фізичні поля, на/в яких інформація міститься або може бути записана і які охоплюють все, незалежно від фізичної природи, включаючи нижчезазначене, але не обмежуючись ним: друковані матеріали, апаратне забезпечення, обладнання, машини, прилади, макети, фотографії, записи, репродукції, карти і листи, а також інші продукти, речовини або вироби, які можуть бути джерелом інформації; – будь-що, на чому інформація записана чи зберігається, та все, з чого інформацію може бути вилучено, незалежно від його фізичної форми або складу, включаючи, серед іншого, документи, друковані записи, обладнання, прилади, машини, механізми, макети, звукові записи, репродукції, карти, комп'ютерні програми, компіляції та електронні носії інформації	[29] [27]	[15]
Матеріали експертизи	– усі матеріали і документи щодо об'єкта експертизи, які отримані або створені під час її проведення	[16]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Матеріальні носії секретної інформації	– матеріальні об'єкти, у тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів; – документи, вироби, речовини або фізичні поля, в яких секретна інформація відображена у вигляді текстів, знаків, образів, сигналів, технічних рішень, процесів тощо	[4] [30]	[15]
Методика генерації ключів	– опис послідовності операцій (алгоритму), що виконуються у процесі генерації ключів	[15]	[30]
Методика розподілу ключів	– опис послідовності операцій (алгоритму), що виконуються у мережі захищеного інформаційного обміну з метою формування (отримання) необхідних ключів	[15]	[30]
Модель загроз для Інформації	– формалізований опис методів і засобів здійснення загроз для інформації	[2]	[25, 26]
Модель загроз для секретної інформації	– формалізований опис методів і засобів здійснення загроз для секретної інформації	[1]	
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	[5]	[12]
Науково-інформаційна діяльність	– це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні	[12]	
Науково-технічна інформація	– будь-які відомості та/або дані про вітчизняні й зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді	[12]	[15]
Національна система конфіденційного зв'язку	– сукупність спеціальних телекомунікаційних систем подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади і органів місцевого самоврядування, створюють належні умови для їх взаємодії у мирний час та у разі введення надзвичайного і воєнного стану	[13]	[31]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Нерезиденти	– юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням за межами України, які створені й діють відповідно до законодавства іноземної держави, у тому числі юридичні особи та інші суб'єкти підприємницької діяльності, створені за участю юридичних і фізичних осіб	[11]	
Несанкціонований доступ (до інформації) НСД	– доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу; – доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми	[7] [2]	
Несанкціоновані дії щодо інформації у системі	– дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства	[8]	[28]
Носій ключової інформації	– матеріальний носій інформації, що призначений для запису та збереження ключів	[15]	[29, 15]
Носій інформації (ТЗІ)	– матеріальний об'єкт, що містить інформацію з обмеженим доступом	[2]	[15]
Носії секретної інформації	– матеріальні об'єкти, у тому числі фізичні поля, на/в яких секретна інформація, що підлягає захисту, відображена у вигляді символів, образів, сигналів, технічних рішень і процесів	[24]	
Обладнання КЗІ	– технічні засоби, що взаємодіють із засобами КЗІ або керують ними і можуть впливати на їхні криптографічні якості	[20]	[30]
Об'єкт інформаційної діяльності	– Інженерно-технічна споруда (приміщення), де здійснюється діяльність, пов'язана з інформацією, що підлягає захисту	[3]	[15]
Об'єкт "особливої норми"	– місце постійного або тимчасового перебування посадової особи, щодо якої здійснюється державна охорона, призначене для здійснення нею діяльності, пов'язаної з інформацією, необхідність захисту якої визначено законодавством	[18]	[15]
Об'єкти	– приміщення, в яких таємна інформація та матеріали використовуються або зберігаються; – приміщення, в яких секретні матеріали та інформація військового характеру використовуються або зберігаються	[29] [27]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Об'єкти протидії (ОПД)	– озброєння, військова та спеціальна техніка, об'єкти оборонно-промислового комплексу, військові об'єкти та об'єкти, використання яких передбачено в ході проведення заходів з мобілізації, інші об'єкти, призначені для застосування в інтересах оборони і безпеки держави	[18]	
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	[6]	[12]
Оброблення інформації	– уся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних	[7]	[5, 6]
Оброблення 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	[8]	[9]
Оброблення персональних даних	– будь-яка дія або сукупність дій, здійснених повністю або частково в інформаційній (автоматизованій) системі та/або в картотеках персональних даних, які пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням відомостей про фізичну особу	[9]	[9]
Оброблення інформації	– вся сукупність операцій (збирання, уведення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передання даних	[1]	[9]
Обслуговування комплексу (системи) ТЗІ	– забезпечення функціонування комплексу (системи) після його впровадження згідно з експлуатаційною документацією	[17]	[28]
Одержання інформації	– це набуття, придбання, накопичення, відповідно до чинного законодавства України, документованої або публічно оголошуваної інформації громадянами, юридичними особами чи державою Основними галузями інформації є політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна	[1]	[13]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Окреме завдання	– комплекс проектів інформатизації, взаємопов'язаних і взаємопогоджених за термінами реалізації, складом виконавців і спрямованих на досягнення конкретних цілей		
Організація	– державний орган або юридична особа, що бере участь у міждержавному співробітництві й виконанні контрактів, на які поширюється дія Угоди; – міністерство, інший державний орган, юридична або фізична особа, що бере участь у міждержавному співробітництві або виконанні контрактів у рамках Угоди; – будь-яка юридична або фізична особа, що бере участь у міждержавному співробітництві або виконанні контрактів, на які поширюється дія Угоди; – міністерство, інший орган державної виконавчої влади, будь-яка юридична особа незалежно від форм власності, що здійснює співробітництво насамперед в оборонній та військовій сферах; – будь-який суб'єкт, незалежно від форми власності, що здійснює співробітництво у військовій сфері	[28] [31] [30] [29] [27]	[13]
Організація-відправник	– організація держави Сторони-джерела, яка передає секретну інформацію в рамках контракту	[30]	[13]
Особа, що має допуск	– особа, яка має офіційні повноваження на доступ до секретної інформації військового характеру, відповідно до положень національного законодавства Сторони	[27]	
Організація-одержувач	– організація держави Сторони-одержувача, яка отримує секретну інформацію в рамках контракту	[30]	[13]
Особистий ключ	– параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу	[5]	[12]
Охорона державної таємниці	– комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв	[4]	
Оцінка (оцінювання) захищеності Інформації в інформаційній, телекомунікаційній та інформаційно-телекомунікаційній системі	– заходи щодо виявлення в інформаційній, телекомунікаційній, інформаційно-телекомунікаційній системі технічних рішень, що створюють можливість здійснення дій з порушення цілісності, конфіденційності та доступності інформації, яка в ній циркулює	[19]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Оцінка стану захищеності державних інформаційних ресурсів у інформаційно-телекомунікаційних системах	– сукупність заходів, спрямованих на виявлення загроз державним інформаційним ресурсам від здійснення несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах	[19]	
Пасивне приховування інформації	– приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин	[2]	[28, 29]
Первинний документ	– це документ, що містить вихідну інформацію	[1]	
Передавання даних	– передавання інформації у вигляді даних з використанням телекомунікаційних мереж	[14]	[28, 29]
Передумови витоку (просочення) інформації технічними каналами	– наявність технічного каналу поширення інформації за відсутності підтвердженої відповідності впроваджених заходів вимогам і нормам з ТЗІ	[18]	[15, 16, 17]
Персонал АС	– фізичні особи, яких власник АС або уповноважена ним особа чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС	[1,7]	[7]
Персональні дані	– відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована	[9]	[15]
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	[5]	[12]
Підробка інформації	– навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС	[1, 7]	[28, 29]
Підрядник	– організація, яка отримує замовлення в рамках таємного контракту; – організація, що одержує замовлення в рамках контракту	[31] [28]	
Порушення в сфері ТЗІ	– невиконання вимог нормативно-правових актів і нормативних документів системи ТЗІ за категоріями, які визначають можливість реалізації загроз безпеці інформації	[18]	[28, 29]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Порушення вимог безпеки	– дія або бездіяльність, що суперечить національному законодавству щодо вимог безпеки, в результаті якої може виникнути ризик для секретної інформації або секретна інформація може бути розголошена	[25]	[28, 29]
Порушення роботи АС	– дії або обставини, які призводять до спотворення процесу обробки інформації	[1, 7]	[27]
Порушення цілісності інформації	– спотворення інформації, її руйнування або знищення	[2]	[1]
Порушення цілісності інформації в системі	– несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст	[8]	[1]
Порушник	– фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній	[1,7]	[27]
Порядок доступу до інформації в системі	– умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації	[8]	[28, 29]
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	[6]	
Посилений сертифікат відкритого ключа	– сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом	[5]	[12]
Послуга пропуску трафіка	– телекомунікаційна послуга щодо здійснення термінації та/або транзиту трафіка, що надається оператором телекомунікацій іншим операторам	[14]	[31]
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	[5]	[12]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Постачальник	– підприємство, установа, організація або підрозділ Державної служби спеціального зв'язку та захисту інформації України, які визначаються Держспецзв'язку для здійснення постачання ключових документів до засобів КЗІ	[15]	
Поширення інформації	– це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації	[1]	[10, 11]
Право власності на інформацію	– це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією	[1]	[10, 11]
Право на інформацію	– це можливість вільного одержання, використання та зберігання відомостей, необхідних для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій	[1]	[10, 11]
Приховування Інформації	– спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого одержання інформації	[2]	[15, 16, 17]
Провайдер телекомунікацій	– суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку	[14]	[31]
Проводовий (дротовий) електрозв'язок	– передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконно-оптичними жилами	[14]	[31]
Програмна закладка	– потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері	[2]	[28, 29]
Проект інформатизації	– комплекс взаємопов'язаних заходів, як правило, інвестиційного характеру, що узгоджені за часом, використанням певних матеріально-технічних, інформаційних, людських, фінансових та інших ресурсів і мають на меті створення заздалегідь визначених інформаційних і телекомунікаційних систем, засобів інформатизації та інформаційних ресурсів, які відповідають певним технічним умовам і показникам якості	[11]	
Пропуск трафіка	– проходження трафіка між елементами однієї або різних телекомунікаційних мереж	[14]	[13]
Пункт закінчення телекомунікаційної мережі	– місце стику (з'єднання) мережі телекомунікацій та кінцевого обладнання	[14]	[13]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Разовий (сеансовий) ключ	– ключ, який визначає порядок заповнення ключового запам'ятовувального пристрою засобу КЗІ, що реалізує алгоритм криптографічного перетворення	[15]	[30]
Реальна загроза витоку (просочення) інформації технічними каналами	– наявність технічного каналу поширення інформації за умов підтвердження відповідними інструментально-розрахунковими методами невідповідності впроваджених заходів вимогам і нормам з ТЗІ	[18]	[9]
Режим безпеки	– реалізована система правових норм, організаційних і організаційно-технічних заходів, яка створюється на підприємствах під час розроблення, дослідження, виробництва та експлуатації засобів КЗІ з метою обмеження доступу до конфіденційної інформації	[20]	[9]
Режим доступу до інформації	– це передбачений правовими нормами порядок одержання, використання, поширення й зберігання інформації	[1]	[9]
Режим секретності	– встановлений, згідно з вимогами Закону та інших виданих відповідно до нього нормативно-правових актів, єдиний порядок забезпечення охорони державної таємниці; – сукупність норм і правил, чинних у державах-учасницях угоди, а також сукупність заходів і дій щодо їх застосування, які носять обов'язковий характер, регулюють доступ до секретної інформації і спрямовані на виключення несанкціонованого доступу до неї	[4] [26]	
Резиденти	– юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням на території України, які здійснюють свою діяльність відповідно до законодавства України	[11]	
Рівень (технічного) захисту інформації	– сукупність вимог (у тому числі й тих, що нормуються), які визначаються режимом доступу до інформації та загрозами для неї	[2]	[15, 16, 17]
Розпорядник АС	– фізична або юридична особа, яка має право розпоряджання АС за угодою з її власником або за його дорученням	[7]	[13]
Розпорядник бази персональних даних	– фізична чи юридична особа, яка є власником бази персональних даних, або законом ій надано право обробляти ці дані	[9]	[13]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Розроблення комплексу (системи) ТЗІ	– стадія життєвого циклу комплексу (системи), яка пов'язана зі складанням технічного завдання, ескізним, технічним (ескізно-технічним), робочим проектуванням, розробленням експлуатаційної документації, програм і методик приймальних (атестаційних) випробувань	[17]	[15, 16, 17]
Розсекречування матеріальних носіїв секретної інформації	– зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації	[4]	
Роумінг національний	– телекомунікаційна послуга, яка забезпечує можливість абонентам одного оператора телекомунікацій, що надає послуги рухомого (мобільного) зв'язку на території України, отримувати телекомунікаційні послуги в телекомунікаційній мережі іншого оператора (операторів) у межах України	[14]	[13]
Рухомий (мобільний) зв'язок	– електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції	[14]	[13]
Самочинний (технічний) канал витоку	– ненавмисний канал витоку інформації; технічний канал витоку інформації, в якому носії інформації та (чи) середовище їх поширення формуються самочинно	[2]	[15, 16, 17]
Секретна інформація військового характеру	– будь-яка офіційна інформація та матеріали в оборонній сфері, передані у письмовій або у будь-якій іншій формі, що в інтересах національної безпеки потребують захисту від несанкціонованого оприлюднення згідно із національним законодавством Сторони-джерела, та засекречені відповідним чином компетентними посадовими особами	[27]	
Секретне замовлення	– контракт, виконання якого пов'язане з використанням або створенням секретної інформації	[26]	
Секретний контракт	– правові відносини між двома або більше договірними особами, які визначають взаємні невід'ємні права і обов'язки, та які пов'язані з секретною інформацією	[25]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Секретна інформація	- відомості, виражені у будь-якій формі, що мають бути захищеними, згідно з законодавством держав-Сторін, передані в порядку, встановленому кожною із Сторін і Угодою, а також створені в процесі співробітництва Сторін; – інформація в будь-якій формі (документи, вироби, речовини, фізичні поля і ті, на (в) яких інформація міститься або може бути записана), що засекречена відповідно до законодавства держав-Сторін, положень Угоди і підлягає захисту від несанкціонованого доступу і поширення; – інформація у будь-якій формі, яка в інтересах національної безпеки держав-Сторін, згідно з їх чинним законодавством, підлягає охороні від несанкціонованого доступу і засекречена відповідно, включаючи ту, що створена спільно організаціями Сторін у рамках співробітництва та засекречена на основі чинного законодавства держав-Сторін і спільно погоджених критеріїв; – інформація, відображена в будь-якій формі, що охороняється відповідно до вимог чинного законодавства та інших нормативно-правових актів держав Договірних Сторін і передана в порядку, встановленому кожною із Договірних Сторін і Угодою, несанкціоноване поширення якої може завдати шкоди безпеці та інтересам сторін угоди; – інформація та матеріали, незалежно від форми, природи та способу передачі, яким надано певний рівень секретності, а також які в інтересах національної безпеки та згідно з національним законодавством держав-Сторін, підлягають охороні від несанкціонованого доступу	[24] [28] [30] [26] [25]	
Сертифікат відкритого ключа	– документ, виданий Центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувача	[5]	[12]
Система Інформаційної безпеки	– сукупність нормативно-правових актів, органів, інститутів публічної влади та інститутів громадянського суспільства, технічних і криптографічних засобів, заходів і методів вирішення питань щодо забезпечення умов функціонування і розвитку інформаційної сфери	[1]	[10, 11]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Система криптографічного захисту інформації	– сукупність органів, підрозділів, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та(або) розповсюджують криптосистеми і засоби криптографічного захисту інформації	[32]	[30]
Система технічного захисту інформації	– це сукупність суб'єктів, об'єднаних цілями і завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база; – сукупність організаційних структур, нормативно-правових документів і матеріально-технічної бази	[22] [2]	[15, 16, 17]
Спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею	– експертиза, що проводиться з метою визначення у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених Законом, для провадження діяльності, пов'язаної з державною таємницею	[4]	
Спеціальна телекомунікаційна система	– телекомунікаційна система (мережа), призначена для обміну інформацією з обмеженим доступом	[13]	[13]
Спеціальна телекомунікаційна система (мережа) подвійного призначення	– спеціальна телекомунікаційна система (мережа), призначена для забезпечення телекомунікацій (електрозв'язку) в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам	[13]	[13]
Спеціальний вплив (ТЗІ)	– вплив на технічні засоби, що призводить до здійснення загрози для інформації	[2]	[15, 16, 17]
Спеціальний зв'язок	– передавання, випромінювання та/ або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень, які містять інформацію з обмеженим доступом, по радіо, проводових, оптичних або інших електроманітних системах з використанням засобів криптографічного та/або технічного захисту інформації з додержанням вимог законодавства щодо її захисту	[3]	[13]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Спеціальні вимоги	– вимоги до принципів побудови засобів КЗІ та технічної реалізації криптографічних алгоритмів у засобах КЗІ, вимоги до криптографічної якості, а також вимоги і норми щодо захисту від можливих каналів витоку небезпечних сигналів засобів КЗІ	[20]	
Спеціальні інформаційно-телекомунікаційні системи	– інформаційно-телекомунікаційні системи, призначені для оброблення інформації з обмеженим доступом, у яких ЗІ забезпечується, у тому числі з використанням засобів КЗІ	[20]	[13]
Сталість телекомунікаційної мережі	– властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників	[14]	[13]
Статистична інформація	– це офіційна документована державна інформація, яка дає кількісну характеристику масових явищ і процесів, що відбуваються в економічній, соціальній, культурній та інших сферах життя	[1]	[14]
Сторона-джерело	– організація держави, в якій засекречена інформація, що наділена повноваженнями здійснювати передачу такої інформації уповноваженим організаціям іншої держави; – Сторона, яка засекретила і передала таємну інформацію; – Сторона, яка передає таємну інформацію та матеріали; – Сторона, яка передає секретну інформацію іншій Стороні	[28] [30, 31] [29] [25]	[14]
Сторона-одержувач	– організація, що наділена повноваженнями одержувати інформацію, засекречену в державі Сторони-джерела; – Сторона, якій передається таємна інформація; – Сторона, якій передається секретна інформація	[28] [29, 31] [30, 25]	
Сторона, що приймає	– Сторона, на територію держави якої здійснюється візит	[25]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Ступінь секретності	– категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї й рівень її охорони державою; – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї і рівень її охорони державами-Сторонами, на підставі якої проставляється гриф секретності; – категорія, яка характеризує важливість секретної інформації, можливу шкоду внаслідок її розголошення, ступінь обмеження доступу до неї та рівень її охорони державою; – категорія, яка характеризує важливість секретної інформації, на підставі якої надається гриф секретності; – категорія, яка характеризує ступінь важливості секретної інформації військового характеру, можливу шкоду внаслідок її розголошення, ступінь обмеження доступу до неї та рівень її охорони державами-Сторонами	[4] [24] [30] [26] [27]	
Суб'єкт владних повноважень	– орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень	[10]	
Суб'єкт персональних даних	– фізична особа, стосовно якої відповідно до закону здійснюється оброблення її персональних даних	[9]	[13]
Суб'єкт електронного документообігу	– автор, підписувач, адресат і посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу	[6]	[14]
Суб’єкти інформаційної діяльності	– учасники інформаційних процесів, які виступають як творці, поширювачі й споживачі інформаційних ресурсів	[1]	[1]
Суб'єкти національної системи конфіденційного зв'язку	– органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи	[13]	[1]
Таємна Інформація	– інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю	[2]	

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Таємна інформація та матеріали	інформація та матеріали будь-якого виду, які в інтересах національної безпеки країни-джерела, згідно з її чинним законодавством, підлягають захисту від несанкціонованого доступу і засекречені відповідною організацією, включаючи інформацію та матеріали, створені спільно організаціями Сторін у рамках співробітництва і засекречені на основі чинного законодавства держав-Сторін і спільно погоджених критеріїв	[29]	
Таємний контракт	– контракт, у рамках якого повинна передаватися або створюватися таємна інформація	[31]	
Телекомунікації (електрозв'язок)	– передавання, випромінювання та/ або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах	[14]	[13]
Телекомунікаційна мережа	– комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням	[14]	[13]
Телекомунікаційна мережа загального користування	– телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів	[14]	[13]
Телекомунікаційна мережа доступу	– частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно	[14]	[13]
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	[8]	[13]
Телемережі	– телекомунікаційні мережі загального користування, що призначаються для передавання програм радіо і телебачення, а також інших телекомунікаційних і мультимедійних послуг і можуть інтегруватися з іншими телекомунікаційними мережами загального користування	[14]	[13]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Термінація трафіка	– встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіка між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання	[14]	[13]
Технічна розвідка	– несанкціоноване здобування інформації за допомогою технічних засобів та її аналіз	[2]	[15, 16, 17]
Технічний засіб оброблення інформації	– технічний засіб, призначений для приймання, накопичення, зберігання, пошуку, перетворення, від ображення та передавання інформації каналами зв'язку	[20]	[15, 16, 17]
Технічний захист інформації	– вид ЗІ, 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; – діяльність, спрямована на запобігання витоку інформації технічними каналами, несанкціонованому доступу до неї, порушенню її цілісності або блокуванню; – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка є державною та іншою, передбаченою законом таємницею, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави; – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації	[8] [23] [22] [33]	[15, 16, 17]
Технічний захист секретної інформації	– вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації	[4]	[15, 16, 17]
Технічний канал витоку інформації	– сукупність носія інформації, середовища його поширення та засобу технічної розвідки	[2]	[15, 16, 17]
Технічний канал поширення інформації	– сукупність джерела інформації та середовища її поширення	[18]	[15, 16, 17]

Продовження таблиці 3.1

Термін	Визначення терміна	Джерело	Література
Технічні засоби телекомунікацій	– обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж	[14]	[15, 16, 17]
Транзит трафіка	– встановлення, підтримка телекомунікаційною мережею оператора фізичного та/або логічного з'єднання, пропуск трафіка між двома іншими телекомунікаційними мережами	[14]	[13]
Транспортна телекомунікаційна мережа	– мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу	[14]	[13]
Трафік	– сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію	[14]	[13]
Уповноважений орган	– державний орган або юридична особа, що уповноважені Сторонами передавати, одержувати, зберігати, захищати, використовувати передану або створену в процесі співробітництва Сторін секретну інформацію	[24]	
Управління інформаційною безпекою	– процес прийняття раціональних управлінських рішень у галузі ІБ за допомогою математичних моделей та на основі використання системи наукових знань	[1]	[21, 22]
Управління ключовими даними	– дії, пов'язані з генерацією, розподіленням, доставлянням, уведенням у дію, зміненням, зберіганням, обліком і знищенням ключових даних, а також носіїв ключових даних	[20]	[12]
Управління системою інформаційної безпеки	– це одночасно система наукових знань, мистецтва та досвіду забезпечення ІБ, втілених у діяльності професійних управлінців для досягнення цілей системи інформаційної безпеки	[1]	[21, 22]
Урядовий зв'язок	– вид спеціального зв'язку, надання якого забезпечується державною системою урядового зв'язку	[3]	
Цілісність	– властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення	[33]	[20]
Штучний (технічний) канал витоку інформації	– навмисний канал витоку інформації	[2]	[15, 16, 17]

Список використаних документів до розділу 3

1. Галузевий стандарт вищої освіти України. ОПП підготовки бакалавра. Галузі знань 1701 “Інформаційна безпека” Напрям підготовки. 6.170101 “Безпека інформаційних і комунікаційних систем” – К. :МОНУ, 2009.- 67 с.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. – К. : Держстандарт України, 1997.- 21 с.

3. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV / [Електронний ресурс] - Режим доступу: http://zakon0.rada.gov.ua/ laws/show/3475-15.

4. Про державну таємницю : Закон України від 21.01.94 р. № 3855-XII // ВВР. – 1994. – № 16. – Ст. 93 [Електронний ресурс] – Режим доступу : http://zakon4.rada. gov.ua/laws/show/3855-12.

5. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV [Електронний ресурс] – Режим доступу :http://zakon0. rada.gov. ua/ laws/show/852-15.

6. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV [Електронний ресурс] – Режим доступу :http://zakon2. rada. gov.ua/laws/show/ 851-15.

7. Про захист інформації в автоматизованих системах: Закон України 05.07. від 94N 81/94-ВР // ВВР, 1994, N 31. - Ст.286 [Електронний ресурс] – Режим доступу :http://www.bezpeka.com/ ru/lib/lawua /art516.html

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс] – Режим доступу :http://zakon0.rada.gov.ua/laws/show/80/94-%D0%B2% D1%80

9. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI [Електронний ресурс] – Режим доступу :http://zakon2.rada.gov.ua/ aws/show /2297-17

10. Про інформацію: Закон України від 02.10.92 р. № 2657-XII : за станом на 09.08.13 р. // ВВР – 1992. – № 48. – Ст. 650 [Електронний ресурс] – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12

11. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР [Електронний ресурс] – Режим доступу :http://search .ligazakon.ua/l_doc2.nsf/link1/Z980075.html

12. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII[Електронний ресурс] – Режим доступу :http://search. ligazakon.ua/ l_doc2. nsf/link1/ T332200.html

13. Про Національну систему конфіденційного зв'язку: Закон України від 10.01.2002 № 2919-III [Електронний ресурс] – Режим доступу :http://zakon1.rada.gov.ua/laws/show/2919-14

14. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV [Електронний ресурс] – Режим доступу :http://zakon5.rada.gov.ua/ laws/show/1280-15/print

15. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації від 12.06.2007 № 114 – Режим доступу :http://zakon4.rada. gov.ua/lawsshow/z0729-07

16. "Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації". Держспецзв'язку України. Наказ від 23.06.2008 № 100 [Електронний ресурс] – Режим доступу :http://zakon4.rada.gov.ua /laws/ show/z0651-08

17. "Про затвердження Ліцензійних умов провадження господарської діяльності з розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг у галузі технічного захисту інформації" Держспецзв'язку. Наказ від 20.01.2009 N 5/9 [Електронний ресурс] – Режим доступу :http://www.dsszzi.gov.ua/ dstszi/control/uk/publish/ article? art_id=76667&cat_id=38835

18. "Про затвердження Положення про державний контроль за станом технічного захисту інформації". Держспецзв'язку. Наказ від 16.05.2007 N 87 – Режим доступу :http://zakon4.rada.gov.ua/laws/ show/z0785-07

19. "Порядок оцінки стану захищеності державних інформаційних ресурсів у інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах". Держспецзв'язку. Наказ від 04.07.2008 N 112 [Електронний ресурс] – Режим доступу :http://www.dsszzi.gov.ua /dstszi/ control/uk/publish/ article? art_id=72978&cat_id=38835

20. "Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації". Департамент спеціальних телекомунікаційних систем і захисту інформації

служби безпеки України. Наказ від 30.11.99 N 53 [Електронний ресурс] – Режим доступу :http://zakon.nau.ua/ doc/?uid=1037.644.2

21. Постанова Кабінету Міністрів 29.03.06 N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс] – Режим доступу :http://zakon2.rada.gov.ua/laws/show/373-2006-п

22. Постанова Кабінету Міністрів 8.10.1997 N 1126 «Про затвердження Концепції технічного захисту інформації в Україні» [Електронний ресурс] – Режим доступу :http://uazakon.com/ document/spart78/inx78402.htm

23. Угода між Кабінетом Міністрів України і Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації. Ратифіковано Законом N 1434-IV (1434-15) від 04.02.2004 [Електронний ресурс] – Режим доступу :http://ua-info.biz/legal/basefe/ua-cmetvr.htm

24. Угода між Кабінетом Міністрів України і Урядом Республіки Вірменія про взаємну охорону секретної інформації. Ратифіковано Законом України від 19.06.03 р. № 1007-IV // ВВР. – 2004. – № 2. – Ст. 10. [Електронний ресурс] – Режим доступу : http://zakon.nau.ua/ doc/?code=1007-15

25. Угода між Кабінетом Міністрів України і Урядом Естонської Республіки про взаємну охорону секретної інформації: Ратифіковано Законом України від 07.09.2005р. № 2827-IV// ВВР.- 2005.- N 51, Ст.543. [Електронний ресурс] – Режим доступу: http://zakon1.rada. gov.ua/laws/show/2827-15

26. Угода між Урядом України і Урядом Італійської Республіки про взаємну охорону секретної інформації. Ратифіковано Законом України від 10.01.02 р. № 2941-III // (ВВР). – 2002. – № 23. – Ст. 161. [Електронний ресурс] – Режим доступу :http://zakon4. rada.gov.ua/ laws/show/2941-iii

27. Угода між Кабінетом Міністрів України і Урядом Республіки Корея про захист секретної інформації військового характеру. Ратифіковано Законом N 2826-IV (2826-15) від 07.09.2005, ВВР, 2005, N 51, Ст.542 [Електронний ресурс] - Режим доступу: http://ua-info.biz/legal/basehe/ua-cmtbir.htm

28. Угода між Кабінетом Міністрів України і Урядом Російської Федерації про взаємну охорону секретної інформації. Ратифіковано

Законом України від 15.11.01 р. № 2799-III// Голос України від 11.12.2001№ 235 [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2799-14

29. Угода між Урядом України і Урядом Словацької Республіки про взаємний захист таємної інформації та матеріалів. Ратифіковано Законом України від 10.01.2002р. N 2938-III // ВВР.- 2002.- N 23, Ст.158 [Електронний ресурс] - Режим доступу: http://zakon4.rada.gov.ua/ laws/show/703-006

30. Угода між Кабінетом Міністрів України і Урядом Туркменістану про взаємну охорону секретної інформації. Ратифіковано Законом України від 10.01.2002р. № 2940-III// ВВР.- 2002.- N 23, Ст.160. [Електронний ресурс] - Режим доступу: http://zakon.nau.ua/doc/?code=2940-14

31. Угода між Кабінетом Міністрів України і Урядом Федеративної Республіки Німеччина про взаємний захист таємної інформації. Ратифіковано Законом України від 10.01.2002р. N 2937-III// ВВР.- 2002.- N 23, Ст.157.[Електронний ресурс] - Режим доступу: http://zakon0.rada.gov.ua/laws/show/276-008

32. Указ Президента України 22.05.98 № 505-98 "Про положення про порядок здійснення криптографічного захисту інформації" [Електронний ресурс] - Режим доступу: http://zakon3.rada.gov.ua /laws/show/505/98

33. Указ Президента України від 27.09.99 N 1229/99 “Про Положення про технічний захист інформації в Україні” [Електронний ресурс] - Режим доступу: http://zakon0.rada.gov.ua/laws/show/1229/99

ДОДАТОК А
ВИТЯГИ З ДЕЯКИХ ЗАКОНІВ УКРАЇНИ

З А К О Н У К Р А Ї Н И

Про інформацію

{ Із змінами, внесеними згідно із Законами 2015 р. включно }

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Розділ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

· документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

· захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

· інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

· суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття 2. Основні принципи інформаційних відносин

1. Основними принципами інформаційних відносин є:

· гарантованість права на інформацію;

· відкритість, доступність інформації, свобода обміну інформацією;

· достовірність і повнота інформації;

· свобода вираження поглядів і переконань;

· правомірність одержання, використання, поширення, зберігання та захисту інформації;

· захищеність особи від втручання в її особисте та сімейне життя.

Стаття 3. Державна інформаційна політика

1. Основними напрямами державної інформаційної політики є:

· забезпечення доступу кожного до інформації;

· забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

· створення умов для формування в Україні інформаційного суспільства;

· забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

· створення інформаційних систем і мереж інформації, розвиток електронного урядування;

· постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

· забезпечення інформаційної безпеки України;

· сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Стаття 4. Суб'єкти і об'єкт інформаційних відносин

1. Суб'єктами інформаційних відносин є:

· фізичні особи;

· юридичні особи;

· об'єднання громадян;

· суб'єкти владних повноважень.

2. Об'єктом інформаційних відносин є інформація.

Стаття 5. Право на інформацію

1. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Стаття 6. Гарантії права на інформацію

1. Право на інформацію забезпечується:

· створенням механізму реалізації права на інформацію;

· створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

· обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

· обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

· здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

· встановленням відповідальності за порушення законодавства про інформацію.

2. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 7. Охорона права на інформацію

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття 8. Мова інформації

1. Мова інформації визначається законом про мови, іншими актами законодавства в цій сфері, міжнародними договорами та угодами, згода на обов'язковість яких надана Верховною Радою України.

Стаття 9. Основні види інформаційної діяльності

1. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Розділ II

ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- інші види інформації.

Стаття 11. Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки,

економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Стаття 12. Інформація довідково-енциклопедичного характеру

1. Інформація довідково-енциклопедичного характеру – це систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

2. Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж і систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їхніми працівниками та автоматизованими інформаційно-телекомунікаційними системами.

3. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством і міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 13. Інформація про стан довкілля (екологічна інформація)

1. Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;
- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);
- стан здоров'я та безпеку людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
- інші відомості та/або дані.

2. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Стаття 14. Інформація про товар (роботу, послугу)

1. Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

2. Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

3. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 15. Науково-технічна інформація

1. Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття 16. Податкова інформація

1. Податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності та необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

2. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Стаття 17. Правова інформація

1. Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. Джерелами правової інформації є Конституція України, інші законодавчі та підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

3. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним і юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Стаття 18. Статистична інформація

1. Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ і процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

3. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

4. Правовий режим державної статистичної інформації визначається Законом України "Про державну статистику", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 19. Соціологічна інформація

1. Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

2. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 20. Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21. Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Розділ III

ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ

Стаття 22. Масова інформація та її засоби

1. Масова інформація - інформація, що поширюється з метою її доведення до необмеженого кола осіб.

2. Засоби масової інформації - засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації.

Стаття 23. Інформаційна продукція та інформаційна послуга

1. Інформаційна продукція - матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин. Інформаційною послугою є діяльність з надання інформаційної продукції споживачам з метою задоволення їхніх потреб.

2. Інформаційна продукція та інформаційні послуги є об'єктами цивільно-правових відносин, що регулюються цивільним законодавством України.

Стаття 24. Заборона цензури та заборона втручання в професійну діяльність журналістів і засобів масової інформації

1. Забороняється цензура - будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації.

Ця заборона не поширюється на випадки, коли попереднє узгодження інформації здійснюється на підставі закону, а також у разі накладення судом заборони на поширення інформації.

2. Забороняються втручання у професійну діяльність журналістів, контроль за змістом поширюваної інформації, зокрема з метою поширення чи непоширення певної інформації, замовчування суспільно необхідної інформації, накладення заборони на висвітлення окремих тем, показ окремих осіб або поширення інформації про них, заборони критикувати суб'єкти владних повноважень, крім випадків, встановлених законом, договором між засновником (власником) і трудовим колективом, редакційним статутом.

3. Умисне перешкоджання законній професійній діяльності журналістів та/або переслідування журналіста за виконання професійних

обов'язків, за критику тягне за собою відповідальність згідно із законами України.

Стаття 25. Гарантії діяльності засобів масової інформації та журналістів

1. Під час виконання професійних обов'язків журналіст має право здійснювати письмові, аудіо- та відеозаписи із застосуванням необхідних технічних засобів, за винятком випадків, передбачених законом.

2. Журналіст має право безперешкодно відвідувати приміщення суб'єктів владних повноважень, відкриті заходи, які ними проводяться, та бути особисто прийнятим у розумні строки їх посадовими і службовими особами, крім випадків, визначених законодавством.

3. Журналіст має право не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язано до цього рішенням суду на основі закону.

4. Після пред'явлення документа, що засвідчує його професійну належність, працівник засобу масової інформації має право збирати інформацію в районах стихійного лиха, катастроф, у місцях аварій, масових безпорядків, воєнних дій, крім випадків, передбачених законом.

5. Журналіст має право поширювати підготовлені ним матеріали (фонограми, відеозаписи, письмові тексти тощо) за власним підписом (авторством) або під умовним ім'ям (псевдонімом).

6. Журналіст засобу масової інформації має право відмовитися від авторства (підпису) на матеріал, якщо його зміст після редакційної правки (редагування) суперечить його переконанням.

7. Права та обов'язки журналіста, працівника засобу масової інформації, визначені цим Законом, поширюються на зарубіжних журналістів, працівників зарубіжних засобів масової інформації, які працюють в Україні.

Стаття 26. Акредитація журналістів, працівників засобів масової інформації

1. З метою створення сприятливих умов для здійснення журналістами, працівниками засобів масової інформації професійної діяльності суб'єкт владних повноважень може здійснювати їх акредитацію. Усі дії, пов'язані з акредитацією, мають ґрунтуватися на принципах відкритості, рівності, справедливості з метою забезпечення права громадськості на одержання інформації через засоби масової інформації. Відсутність акредитації не може бути підставою для відмови в допуску

журналіста, працівника засобу масової інформації на відкриті заходи, що проводить суб'єкт владних повноважень.

2. Акредитація журналіста, працівника засобу масової інформації здійснюється безоплатно на підставі його заяви або подання засобу масової інформації.

У заяві, поданій журналістом, працівником засобу масової інформації, зазначаються його прізвище, ім'я та по батькові, адреса, номер засобу зв'язку, адреса електронної пошти (за наявності). До заяви додаються копії документів, що посвідчують особу та засвідчують її професійну належність.

У поданні засобу масової інформації зазначаються його повне найменування, дата і номер реєстрації, адреса, адреса електронної пошти (за наявності), номер засобу зв'язку, прізвище, ім'я та по батькові журналіста, працівника засобу масової інформації, щодо якого вноситься подання. До подання додаються копії документів, що посвідчують особу.

В акредитації не може бути відмовлено в разі подання усіх документів, передбачених цією частиною.

Суб'єкт владних повноважень може встановлювати спрощений порядок акредитації.

3. Порядок акредитації, визначений суб'єктом владних повноважень, підлягає оприлюдненню.

4. Суб'єкти владних повноважень, що здійснили акредитацію журналістів, працівників засобів масової інформації, зобов'язані сприяти провадженню ними професійної діяльності; завчасно сповіщати їх про місце і час проведення сесій, засідань, нарад, брифінгів та інших публічних заходів; надавати їм інформацію, призначену для засобів масової інформації; а також сприяти створенню умов для здійснення запису і передачі інформації, проведення інтерв'ю, отримання коментарів посадових осіб.

5. У разі якщо захід проводиться відповідно до міжнародних або інших спеціальних протоколів, можуть встановлюватися особливі умови допуску журналістів. Такі особливі умови оприлюднюються на офіційному веб-сайті відповідного суб'єкта владних повноважень до проведення заходу.

6. Журналіст, працівник засобу масової інформації зобов'язаний дотримуватися встановлених суб'єктом владних повноважень правил внутрішнього трудового розпорядку, не перешкоджати діяльності його службових та посадових осіб.

7. Суб'єкти владних повноважень, що акредитували журналіста, працівника засобу масової інформації, приймають рішення про

припинення акредитації у разі:

· подання ним відповідної заяви;

· неодноразового грубого порушення ним обов'язків, визначених цією статтею;

· звернення засобу масової інформації, за поданням якого здійснена акредитація.

8. У рішенні про припинення акредитації зазначаються посадова особа чи службова особа (суб'єкт владних повноважень), яка прийняла відповідне рішення, дата прийняття рішення, підстава для прийняття рішення та порядок його оскарження. Письмове повідомлення про припинення акредитації видається або надсилається засобу масової інформації або журналістові, працівникові засобу масової інформації протягом п'яти робочих днів з дня прийняття відповідного рішення.

9. Рішення про припинення акредитації може бути оскаржено до суду в установленому порядку.

Розділ IV

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 27. Відповідальність за порушення законодавства про інформацію

1. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Стаття 28. Неприпустимість зловживання правом на інформацію

1. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Стаття 29. Поширення суспільно необхідної інформації

1. Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

2. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків;

свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Стаття 30. Звільнення від відповідальності

1. Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

2. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому засобі масової інформації з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

3. Суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною.

4. Додаткові підстави звільнення від відповідальності засобів масової інформації та журналістів встановлюються законами України "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про інформаційні агентства" та іншими.

Стаття 31. Відшкодування матеріальної та моральної шкоди

1. У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

2. Суб'єкти владних повноважень як позивачі у справах про захист честі, гідності та ділової репутації вправі вимагати в судовому порядку лише спростування недостовірної інформації про себе і не мають права вимагати відшкодування моральної (немайнової) шкоди. Це не позбавляє посадових і службових осіб права на захист честі, гідності та ділової репутації в суді.

ЗАКОН УКРАЇНИ

Про захист інформації в інформаційно-телекомунікаційних системах

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

· блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

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

· власник інформації - фізична або юридична особа, якій належить право власності на інформацію;

· власник системи - фізична або юридична особа, якій належить право власності на систему;

· 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, внаслідок яких інформація в системі зникає;

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

· інформаційно-телекомунікаційна система - сукупність інформаційних і телекомунікаційних систем, які у процесі оброблення 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;

· оброблення 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 оброблення 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.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для оброблення цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

· власники інформації;

· власники системи;

· користувачі;

· уповноважений орган у сфері захисту інформації в системах.

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі - розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 5. Відносини між власником інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для оброблення інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для оброблення інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови оброблення інформації в системі

Умови оброблення інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не

передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Обов'язки уповноваженого органу у сфері захисту інформації в системах виконує центральний орган виконавчої влади у сфері криптографічного та технічного захисту інформації.

Уповноважений орган у сфері захисту інформації в системах:

· розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

· визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

· організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

· здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Державні органи в межах своїх повноважень за погодженням з уповноваженим органом у сфері захисту інформації встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України і Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом".

Постанова Кабінету Міністрів України

Правила
забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

Загальна частина

1. Ці Правила визначають загальні вимоги і організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних і інформаційно-телекомунікаційних системах (далі - система).

2. Дія цих Правил не поширюється на захист інформації в системах урядового і спеціальних видів зв'язку.

3. У Правилах наведені нижче терміни вживаються у такому значенні:

- 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.

Інші терміни вживаються у значенні, наведеному в Законах України "Про Інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про телекомунікації", Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27.09.1999 р. N 1229.

4. Захисту в системі підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру і використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в мережі Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);

- інформація, що становить державну або іншу передбачену законом таємницю (далі - таємна інформація).

Вимоги до забезпечення захисту інформації в системі

5. Відкрита інформація під час оброблення в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

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

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

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з оброблення конфіденційної інформації або позбавлення його такого права.

8. Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються цими Правилами і законодавством у сфері охорони державної таємниці.

9. Забезпечення захисту в системі таємної інформації, що не становить державну таємницю, здійснюється згідно з вимогами до захисту конфіденційної інформації.

10. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її власником (розпорядником), якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

11. У системі здійснюється обов'язкова реєстрація:

· результатів ідентифікації та автентифікації користувачів;

· результатів виконання користувачем операцій з оброблення інформації;

· спроб несанкціонованих дій з інформацією;

· фактів надання та позбавлення користувачів права доступу до інформації та її оброблення;

· результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації і знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

12. Ідентифікація та автентифікація користувачів, надання і позбавлення їх права доступу до інформації та її оброблення, контроль за цілісністю засобів захисту в системі здійснюються автоматизованим способом.

13. 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 і криптографічного захисту інформації.

14. Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

15. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для оброблення інформації, запобігання несанкціонованій його модифікації і ліквідація наслідків такої модифікації. Контролюється також цілісність програмних і технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Організаційні засади забезпечення захисту інформації

16. 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 оброблення інформації, інших технічних засобів і комунікацій;

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

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

Захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято власником(розпорядником) інформації.

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби її оброблення, забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації.

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

18. Організація і проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації і контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі, коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

19. Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі. План захисту інформації в системі містить:

· завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології оброблення інформації;

· визначення моделі загроз для інформації в системі;

· основні вимоги щодо захисту інформації та правила доступу до неї в системі;

· перелік документів, згідно з якими здійснюється захист інформації в системі;

· перелік і строки виконання робіт службою захисту інформації.

20. Вимоги та порядок створення системи захисту встановлюються Департаментом спеціальних телекомунікаційних систем і захисту інформації СБУ (далі - департамент). Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.

21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю. У разі використання засобів захисту інформації, які не мають підтвердження відповідності на

момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.

22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється департаментом. Органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації для власних потреб, вправі за згодою департаменту організовувати проведення державної експертизи системи захисту на підприємствах, в установах та організаціях, які належать до сфери їх управління. Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з департаментом.

23. Виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення системи захисту. Для проведення інших видів робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

24. Контроль за забезпеченням захисту Інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку, визначеному департаментом.

25. У системі, яка складається з кількох інформаційних та (або) телекомунікаційних систем, ці Правила можуть застосовуватися до кожної складової частини окремо.

ДОДАТОК Б

Список допоміжної літератури з інформаційної безпеки

1. Галатенко, В. А. Основы информационной безопасности: учеб. пособие / В. А. Галатенко; под. ред. В. Б Бетелена. – М. ИНТУИТ.РУ «Интернет–университет Информационных Технологий», 2006. – 208 с.

2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов / А. А. Малюк. – М. : Горячая линия – Телеком, 2004. – 280 с.

3. Основы информационной безопасности / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия – Телеком, 2006. – 544 с.

4. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; под ред. В. Ф. Шаньгина. – М. : Радио и связь, 2001. – 376 с.

5. Конев, И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. — 752 с.

6. Степанов, Е. А. Информационная безопасность и защита информации: учеб. пособие / Е. А. Степанов, И. К. Корнеев. — М. : ИНФРА-М, 2001. — 304 с.

7. Ярочкин, В. И. Информационная безопасность: учеб. для студентов вузов / В. И. Ярочкин. — 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. — 544 с.

8. Ярочкин, В. И Корпоративная разведка / В. И. Ярочкин, Я. В. Бузанова. – 2-е изд. – М. : «Ось – 89», 2008. – 304 с.

9. Устинов, Г. Н. Основы информационной безопасности систем и сетей передачи данных: учеб. пособие / Г. Н. Устинов. – М. : Синтег, 2000. – 248 с.

10. Информационная безопасность офиса : науч.–практ. сб. / Выпуск первый «Технические средства защиты информации». – К. : ООО «ТИД» «ДС», 2003. – 216 с.

11. Барсуков, В. С. Современные технологии безопасности / В. С. Барсуков, В. В. Водолазкий. – М. : «Нолидж», 2000. – 496 с.

12. Горбенко, Ю. І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: моногр. / Ю. І. Горбенко, І. Д. Горбенко.– Х. : Форт, 2010. – 608 с.

13. Кузнецов, А. А. Безопасность информационных систем и технологий / В. И. Есенин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.

14. Большая энциклопедия промышленного шпионажа / Ю. Ф. Каторин, Е. В. Куренков, А. В. Лысов, А. Н. Остапенко. – СПб.: ООО «Изд. Полигон», 2000. – 896 с.

15. Технічний захист інформації на об'єктах інформаційної діяльності / М. М. Браіловський, С. М. Головань, В. В. Домарєв та ін. – К. : ДУІКТ, 2007. – 178 с.

16. Коженевський, С. Р. Термінологічний довідник з питань технічного захисту інформації / С. Р. Коженевський, Г. В. Кузнецов, Д. В. Чирков. – 4-е вид. – К. : ДУІКТ, 2007. – 365 с.

17. Ленков, С. В. Методы и средства защиты информации : в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко: – К.: Арий, 2008 – Т. 1: Несанкционированное получение информации.– 464 с.

18. Ленков, С. В. Методы и средства защиты информации : в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко: – К. : Арий, 2008. – Т. 2: Информационная безопасность.– 344 с.

19. Інтелектуальна власність у сфері захисту інформації / С. М. Головань, С. Р. Коженевський, О. І. Стельмаховська, В. О. Хорошко; за ред. В. О. Хорошка. – К. : ДУІКТ, 2009.– 177 с.

20. Політика інформаційної безпеки / О. Л. Голубенко, В. О. Хорошко, О. С. Петров та ін. – Луганськ: СНУ ім. В. Даля, 2009. – 296 с.

21. Кобозева, А. А. Анализ информационной безопасности / А. А. Кобозева, В. А. Хорошко. – К. : ГУИКТ, 2009. – 251 с.

22. Основи інформаційної безпеки: підручник / В. І. Андрєєв, В. О. Хорошко, В. С. Чередніченко, М. Є. Шелест. – К. : ДУІКТ, 2009. – 292 с.

23. Баранов, В. Л. Моделювання фізичних процесів в інформаційній безпеці / В. Л. Баранов, М. В. Капустян, Р. М. Костюченко. – К. : ДУІКТ, 2009. – 175 с.

24. Кобозева, А. А. Аналіз захищеності інформаційних систем: підручник/ А. А. Кобозева, І. О. Мачалін, В. О Хорошко. – К. : ДУІКТ, 2010. – 316 с.

25. Управління інформаційною безпекою: підручник: у 2 т. / Л. Ф. Єжова, І. О. Мачалін, Я. В. Невойт, В. О. Хорошко. – Севастополь: СНУЯЕтаП, 2010.

26. Павлов, І. М. Проектування комплексних систем захисту інформації / І. М. Павлов, В. О. Хорошко. – К. : ВІТІ, 2011. – 245 с.

27. Павлов, І. М. Проектування комплексних систем захисту інформації: підручник / І. М. Павлов, В. О. Хорошко. – К. : ДУІКТ, 2011. – 245 с.

28. Железняк, В. К. Защита информации от утечки по техническим каналам: учеб. пособ. / В. К. Железняк – СПб. : ГУАП, 2006. – 188 с.

29. Технические средства и методы защиты информации: учебник / А. П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : ООО «Машиностроение», 2009 – 508 с.

30. Скляр, Б. Цифровая связь. Технические основы и практическое применение / Б. Скляр. – 2-е изд., исправл. – Изд. дом «Вильямс», 2004. – 1104 с.

31. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – М. : ДМК Пресс, 2012. – 474 с.

Довідкове видання

Пєвнєв Володимир Яковлевич
Лавровська Таміла Валеріївна

ІНФОРМАЦІЙНА БЕЗПЕКА
ТЕРМІНИ І ВИЗНАЧЕННЯ

Редактор Є. О. Александрова

Зв. план, 2016
Підписано до видання

Ум. друк. арк 4,67. Обл.-вид. арк. 5,25. Електронний ресурс

Видавець і виготовлювач
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків-70, вул. Чкалова, 17
http:// www.khai.edu
Видавничий центр «ХАІ»
61070, Харків-70, вул. Чкалова, 17
izdat@khai.edu
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції сер. ДК № 391 від 30.03.2001