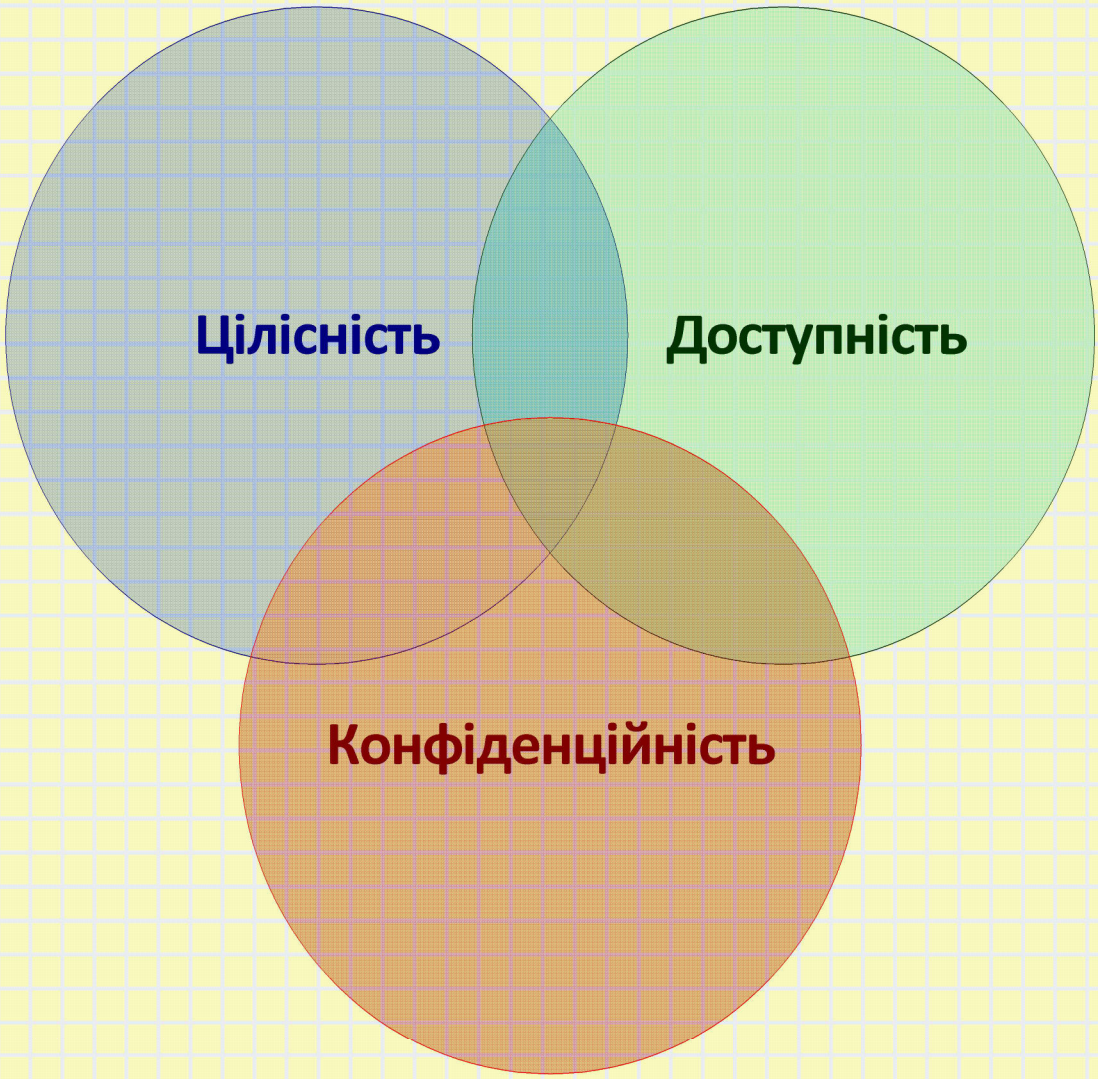
Серія Безпека інформаційних і комунікаційних систем

Лужецький В. А.
Кожухівський А. Д.
Войтович О. П.



ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет

В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Вінниця
ВНТУ
2013

УДК 681.3.6
ББК [32.97.я73]
Л83

Рекомендовано Міністерством освіти і науки, молоді та спорту України як навчальний посібник для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Безпека інформаційних і комунікаційних систем». Лист № 1/11-10311 від 09.11.10.

Рецензенти:
О. Є. Архипов, доктор технічних наук, професор
О. Г. Корченко, доктор технічних наук, професор
М. І. Мазурков, доктор технічних наук, професор

Лужецький, В. А.
Л 83 Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.
ISBN

У посібнику розглядаються основні поняття інформаційної безпеки і компоненти системи захисту інформації. Описуються заходи та засоби законодавчого, адміністративного, організаційного та інженерно-технічного рівнів забезпечення інформаційної безпеки організацій та установ. Окрему увагу приділено програмно-технічному захисту інформаційних систем.

Для студентів напрямків «Інформаційна безпека» всіх спеціальностей денної та заочної форм навчання.

УДК 681.3.6
ББК [32.97.я73]

ISBN

ЗМІСТ

ВСТУП

Сучасний світ розвивається у напрямку все більшої інформатизації як окремих галузей народного господарства, так і суспільства взагалі. Вже не можна собі уявити світ без інформаційних технологій, персональних комп'ютерів, глобальних комп'ютерних мереж та мобільного зв'язку, хоча ще 20 років тому це здавалось чимось фантастичним або дуже дорогим.

Особливо гостро постає проблема забезпечення інформаційної безпеки в зв'язку із стрімким впровадженням комп'ютерної техніки в такі сфери, як біржова та банківська справа, страхування, медицина тощо. Необхідність вирішення проблем захисту інформації також зумовлена різким зростанням комп'ютерної злочинності, результат діяльності якої призводить до значних матеріальних втрат, незалежно від того чи це вірусна атака, чи шахрайство в електронній комерції.

Інформаційна безпека досить молода галузь, яка знаходиться на перетині інформаційних технологій та захисту інформації. Лише комплексний підхід дозволить забезпечити інформаційну безпеку на належному рівні. Це однаково стосується захисту інформації, що зберігається й обробляється як в окремому комп'ютері, так і в корпоративній мережі.

Кожний комерційний об'єкт повинен будувати свою систему захисту інформації на концептуальній основі, виходячи із призначення об'єкта, його розмірів, умов розміщення, характеру діяльності тощо. При розробці концепції захисту необхідно виходити з детального аналізу напрямків діяльності підприємницької структури й комплексних вимог захисту. Особливо, якщо структури застосовують у своїй діяльності засоби інформатики.

Основними напрямками забезпечення інформаційної безпеки бізнесу є:

- захист інформації про стан і рух матеріальних активів;
- захист інформації про стан нематеріальних активів і їх носіїв;
- захист засобів зберігання, оброблення й передавання інформації.

З огляду на різноманіття потенційних загроз інформації в системі обробки даних, складність структури й функцій, а також участь людини в технологічному процесі обробки інформації цілі захисту інформації можуть бути досягнуті тільки шляхом створення системи захисту інформації на основі комплексного підходу.

Дуже важливо правильно підійти до вирішення питань інформаційної безпеки, щоб не викидати «на вітер» гроші й, найважливіше, інформацію,

яку було потрібно захистити. Існує таке поняття як відношення ціна/якість, тобто людина (організація) повинна розуміти, інформацію якої вартості якою ціною вона збирається захищати.

У посібнику розглядаються основні поняття інформаційної безпеки і компоненти системи захисту інформації. Значну увагу приділено заходам та засобам законодавчого, адміністративного, організаційного інженерно-технічного та програмно-технічного рівнів.

Наводяться відомості про українське та зарубіжне законодавство, основні стандарти щодо інформаційної безпеки.

Для адміністративного рівня розглядаються правила побудови політики та програми безпеки. Для процедурного рівня описуються заходи, що стосуються роботи з персоналом та організації служби безпеки підприємства чи установи. Для інженерно-технічного рівня описуються заходи та засоби фізичного, апаратного, програмного, криптографічного та стеганографічного видів захисту інформації та інформаційних ресурсів. Окрему увагу приділено програмно-технічному захисту інформаційних систем.

Наприкінці кожного розділу наведено контрольні питання, які призначені для перевірки студентами рівня засвоєння матеріалу в процесі самостійної роботи.

Також в кінці кожного розділу запропоновані теми практичних занять, які призначені для закріплення теоретичних знань та застосування їх для розв’язання задач інформаційної безпеки на підприємстві.

У посібнику викладено методично опрацьований матеріал ряду літературних джерел, перелік яких наведено в кінці посібника. Методику викладення матеріалу апробовано під час читання лекцій і проведення практичних занять.

Автори висловлюють особливу подяку рецензентам: доктору технічних наук, професору Архипову О. Є., доктору технічних наук, професору Корченко О. Г. та доктору технічних наук, професору Мазуркову М. І. за корисні зауваження, що сприяли покращенню матеріалу посібника.

1 ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям **«інформація»**. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям.

Інформація – нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього подання.

У галузі інформаційних систем рекомендується таке означення інформації.

Інформація – це відомості, які є об'єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп'ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому має певні споживчі якості, а також має і своїх власників або виробників.

1. Інформація, яку ви маєте, не та, яку ви б хотіли отримати.
2. Інформація, яку б ви хотіли отримати, не та, яка вам насправді потрібна.
3. Інформація, яка вам насправді потрібна, вам не доступна.
4. Інформація, яка в принципі вам доступна, коштує більше, ніж ви можете за неї заплатити

Чотири закони теорії інформації

Таємна інформація – це майже завжди джерело великого статку або результат публічного скандалу

Оскар Уайльд

Найбільшого успіху досягає той, хто має в своєму розпорядженні більше інформації

Бенджамін Дізраелі

Відповідно до різноманітності поняття інформації, словосполучення «інформаційна безпека» в різних контекстах може мати різний сенс. Так, у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» наводиться таке поняття інформаційної безпеки.

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

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону України «Про інформацію», що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації та інформаційних систем;
- суб'єктів – учасників інформаційних процесів;
- правовідносин виробників – споживачів інформаційної продукції;
- власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

У даному посібнику увагу буде зосереджено на процесах зберігання, оброблення і передавання інформації. Тому термін «інформаційна безпека» використовуватиметься у вузькому сенсі.

> ***Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури.***

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій.

Тут необхідно зауважити, що трактування проблем, пов'язаних з ІБ, для різних категорій суб'єктів може істотно різнитися. Для ілюстрації досить зіставити режимні державні організації і навчальні заклади. У першому випадку «хай краще все зламається, ніж ворог дізнається хоч один секретний біт», у другому – «немає у нас жодних секретів, аби все працювало». Отже, інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це поняття принципово ширше.

Фахівцем з інформаційної безпеки, як і знавцем футболу, вважає себе кожен другий користувач (не рахуючи кожного першого).

"Закони Мерфі для інформаційної безпеки" О. В. Лукацький

Суб'єкт інформаційних відносин може постраждати (зазнати збитків та/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій власне захист від несанкціонованого доступу до інформації стоїть за важливістю зовсім не на першому місці.

Повертаючись до питань термінології, відзначимо, що термін **«комп'ютерна безпека»** (як еквівалент або замінник ІБ) є дуже вузьким. Комп'ютери – тільки одна із складових ІС, і хоч наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно з визначенням ІБ, вона залежить не тільки від ІС, але й від інфраструктури, що її підтримує, тобто системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання ІС своїх функцій.

У визначенні ІБ перед іменником «втрати» знаходиться прикметник «неприйнятний». Очевидно, застрахуватися від усіх видів втрат неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує очікуваних втрат. Отже, з чимось треба миритися і захищатися тільки від того, з чим змиритися ніяк не можна. Іноді такими неприпустимими витратами є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальний (грошовий) вираз, а метою захисту інформації стає зменшення розмірів втрат до припустимих значень.

1.2 ОСНОВНІ ЗАДАЧІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека – це багатогранна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

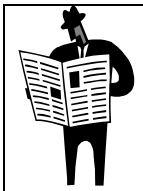
Основними задачами інформаційної безпеки є:

- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, поданої у вигляді електронного документа;
- забезпечення невідстежуваності дій користувача.

Доступність – це властивість інформаційного об'єкта щодо одержання його користувачем за прийнятний час.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, виділимо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних і авіаквитків, банківські послуги тощо).



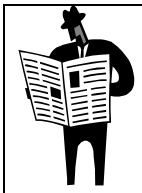
Хвилинна зупинка Лондонської фондової біржі через внутрішні несправності інформаційної системи призвела до багатомільйонних втрат.

cnews.ru

Цілісність – це властивість інформаційного об'єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання.

Розрізняють цілісність *статичну* (тобто незмінність інформаційних об'єктів) і *динамічну* (стосується коректного виконання складних дій (тра-

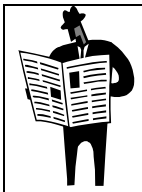
нзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізуванні потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.



Міністерство оборони Великобританії веде розслідування з приводу порушення безпеки. Газета The Times пише, що всі повідомлення електронної пошти з ряду баз британських військово-повітряних сил потрапляють на російський сервер.

Inopressa.ru

Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація є «керівництвом до дії». Рецептура ліків, зміст медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може призвести до небажаних наслідків. Неприємно і спотворення офіційної інформації, чи то тексту закону, чи сторінки Web-сервера урядової організації.



У 2011 році невідомі зловмисники зламали сайт Верховної ради України і розмістили на головній сторінці непристойні фотографії. Зловмисників так і не знайшли.

tcn.ua

Конфіденційність – це властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов’язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

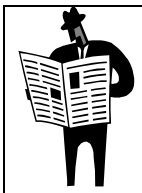
Вірогідність інформації – це її властивість, яка полягає у строгій належності об’єкту, що є її джерелом, або тому об’єкту, від якого ця інформація прийнята.

Юридична значимість – це властивість інформації, поданої у вигляді електронного документа, мати юридичну силу.

З цією метою суб'єкти, що мають потребу в підтвердженні юридичної значимості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують її здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Невідстежуваність – це здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з'явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть умови для тотального стеження за користувачами ІС.



Наприкінці 2007 року більш ніж 13 тис. користувачів соціальної мережі Facebook заявили про своє незадоволення новою рекламною моделлю цієї мережі. Їх занепокоїв той факт, що завдяки цільовій рекламі інформація про їхні покупки стала відомою їхнім друзям.

http://telnews.ru

Існує кілька шляхів вирішення проблеми неможливості стеження:

- заборона за допомогою законодавчих актів будь-якого тотального стеження за користувачами інформаційних систем;
- застосування криптографічних методів для підтримки неможливості слідкування.

Інформаційна безпека в рамках забезпечення роботоздатності ІС **повинна забезпечувати захист від:**

- порушення функціонування ІС шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;
- несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;
- руйнування вбудованих та зовнішніх засобів захисту;

- неправомірних дій користувачів і обслуговуючого персоналу мережі.

Пріоритети серед перерахованих задач інформаційної безпеки визначаються індивідуально для кожної конкретної ІС і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

З погляду державних структур захисні заходи в першу чергу покликані забезпечити *конфіденційність, цілісність* і *доступність* інформації.

Комерційним структурам, ймовірно, найважливішими є *цілісність* і *доступність* даних і послуг. На відміну від державних, комерційні організації більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, але й якістю.

Для розв'язання задач забезпечення безпеки в інформаційних системах необхідно:

- захистити інформацію під час її зберігання, оброблення і передавання мережею;
- підтвердити дійсність об'єктів даних і користувачів;
- знайти і попередити порушення цілісності об'єктів даних;
- захистити технічні пристрої і приміщення;
- захистити конфіденційну інформацію від витоку вбудованими електродними пристроями знімання інформації;
- захистити програмні засоби від приєднання програмних закладок і вірусів;
- захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема, до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі;
- організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

Конкретна реалізація загальних принципів забезпечення інформаційної безпеки може полягати в організаційних або технічних заходах.

АФОРИЗМИ І ПОСТУЛАТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дальше покладеш – ближче візьмеш.

* * *

Береженого Бог береже.

* * *

Спочатку подумай, потім говори.

* * *

Не знаючи броду, не лізь у воду.

* * *

Сім раз відмір, один раз відріж.

* * *

Діло майстра боїться.

* * *

Віднайди всьому початок, і ти багато зрозумієш. (*К. Прутков*)

* * *

Мудрий той, хто вміє мовчати.

* * *

Слово – срібло, мовчання – золото.

* * *

Що в тверезого на умі, то в п'яного на язиці.

* * *

Язик мій – ворог мій.

* * *

Їж суп з грибами і тримай язик за зубами.

* * *

Слово – не горобець, вилетить – не впіймаєш.

* * *

Хто слідкує за своїм язиком, віками не буде ним обкрадений.

* * *

На кожну отруту є протиотрута.

* * *

Нічого не виникає із нічого.

* * *

Ніщо не зникає просто так.

* * *

В глибині всяких грудей є своя змія. (*К. Прутков*)

* * *

Півень прокидається рано, але злодій – раніше. (*К. Прутков*)

* * *

Голота на вигадки хитра.

* * *

Зі світу – по нитці, голому – сорочка.

* * *

Курка по зернинці харчується.

* * *

Хто шукає, той завжди знайде.

* * *

Крапля камінь точить не силою, а частим падінням.

* * *

Бійся допитливості. Допитливість – це дослідження чужих справ.

* * *

Ворог діє іноді через злих людей: через гордих, через розпусних, використовуючи при цьому різні звaблювання.

* * *

Безпечних технічних засобів немає.

* * *

Джерелами утворення технічних каналів витоку інформації є фізичні перетворювачі.

* * *

Будь-який електронний елемент за певних умов може стати джерелом утворення каналу витоку інформації.

* * *

Будь-який канал витоку інформації може бути виявлений і локалізований.

* * *

Канал витоку інформації легше локалізувати, ніж виявити.

* * *

Якщо не впевнений в безпеці, вважай, що небезпека існує реально.

* * *

Безкоштовної безпеки не буває.

* * *

Безпеки не буває забагато.

* * *

Безпека повинна бути тільки комплексною.

* * *

Комплексна безпека може бути забезпечена тільки системною безпекою.

* * *

Жодна система безпеки не забезпечує необхідного рівня без належної підготовки керівництва, працівників та клієнтів.

* * *

У безпеці повинен бути зацікавлений кожен.

СПИСОК ЛІТЕРАТУРИ

Основна

1. Анин Б. Защита компьютерной информации / Анин Б. – СПб. : БХВ-Санкт-Петербург, 2000. – 384 с.
2. Бабак В. П. Інформаційна безпека та сучасні мережеві технології / В. П. Бабак, О. Г. Корченко. – К. : «МК-Пресс», 2003. – 248 с.
3. Бармен С. Разработка правил информационной безопасности / Бармен С. ; пер. с англ. – М. : «Вильямс», 2002. – 208 с.
4. Вертузаєв М. С. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посібник / Вертузаєв М. С., Юрченко О. М., Лаптева С. Г. – К. : Вид-во Європ. ун-ту, 2001. – 321 с.
5. Галатенко В. А. Основы информационной безопасности [Електронний ресурс] / Галатенко В. А. // Институт інформаційних технологій – Режим доступу до курсу : http://www.intuit.ru/department/security/secbasics/
6. Голубєв В. О. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посібник / Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. ; за заг. ред. доктора юридичних наук, професора Р. А. Калюжного. – Запоріжжя : ГУ «ЗІДМУ», 2002. – 292 с.
7. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.
8. Домарев В. В. Безопасность информационных технологий. Методология создания ситем защиты / Домарев В. В. – К. : ООО «ТИД «ДС», 2001. – 688 с.
9. Защита информации в телекомуникационных системах / Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г. – К. : «МК-Пресс», 2005. – 288 с.
10. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. – М. : КУДИЦ-ОБРАЗ, 2001. – 346 с.
11. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 752 с.
12. Лужецький В. А. Інформаційна безпека : навчальний посібник / Лужецький В. А., Войтович О. П., Дудатьєв А. В. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с.

13. Лужецький В. А. Захист персональних даних : навчальний посібник / Лужецький В. А., Войтович О. П., Дудатьєв А. В. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 487 с.
14. Лукацкий А. В. Обнаружение атак / Лукацкий А. В. – СПб. : БХВ-Петербург, 2001. – 224 с.
15. Малюк А. А. Информационная безопасность : концептуальные и методологические основы защиты информации : учеб. пособие для вузов / Малюк А. А. – М. : Горячая линия – Телеком, 2004. – 280 с.
16. Медведев Н. Г. Аспекты информационной безопасности виртуальных частных сетей : учебное пособие / Н. Г. Медведев, Д. В. Москалюк. – К. : Изд-во Европ. ун-та, 2002. – 95 с.
17. Основы информационной безопасности : [учебное пособие для вузов] / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия-Телеком, 2006. – 544 с.
18. Основи комп'ютерної стеганографії : [навчальний посібник] / В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. – Вінниця : ВНТУ, 2003. – 143 с.
19. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / Петров А. А. – М. : ДМК, 2000. – 448 с.
20. Романец Ю. В. Защита информации в компьютерных системах и сетях / Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. ; под ред. В. Ф. Шаньгина. – М. : Радио и связь, 2001. – 376 с.
21. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.
22. Смит Р. Э. Аутентификация: от паролей до открытых ключем / Смит Р. Э. – М. : «Вильямс», 2002. – 432 с.
23. Столингс В. Криптография и защита сетей: принципы и практика / Столингс В. ; пер. с англ. – М. : «Вильямс», 2001. – 672 с.
24. Чмора А. Л. Современная прикладная криптографія / Чмора А. Л. – М. : Гелиус АРВ, 2001. – 244 с.
25. Ярочкин В. И. Информационная безопасность : учебное пособие / Ярочкин В. И. – М. : Междунар. отношения, 2000. – 400 с.

Додаткова

1. Закон України «Про інформацію» : за станом на 1 січня 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : за станом на 1 січня 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0
3. Закон України «Про науково-технічну інформацію» : за станом на 1 січня 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/3322-12
4. Закон України «Про державну таємницю» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12
5. Закон України «Про ліцензування певних видів господарської діяльності» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/1775-14.
6. Закон України «Про стандартизацію» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/2408-14.
7. Закон України «Про авторське право і суміжні права» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/3792-12 .
8. Закон України «Про електронні документи та електронний документообіг» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon1.rada.gov.ua/laws/show/851-15 .
9. Закон України «Про електронний підпис» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/852-15 .
10. Закон України «Про охорону прав на промислові зразки» : за станом на 24 лютого 2011 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon1.rada.gov.ua/laws/show/3688-12 .
11. Захист інформації. Технічний захист інформації. Порядок проведення робіт : ДСТУ 3396.1-96. – [Чинний від 1997-08-01] - К. : Державний

комітет стандартизації метрології та сертифікації України, 1997 – 32 с. – (Основоположні стандарти).

12. Захист інформації. Технічний захист інформації. Основні поняття. : ДСТУ 3396.0-96. – [Чинний від 1997-08-01], – К.: Держстандарт України, 1996. – 8 с.
13. Захист інформації. Технічний захист інформації. Терміни та визначення. : ДСТУ 3396.0-96. – [Чинний від 1997-08-01], – К.: Держстандарт України, 1996. – 16 с.
14. Аграновский А. В. Компьютерная стеганография : Теория и практика / А. В. Аграновский, А. Н. Пузыренко – М. : МК-Пресс, 2006. – 283 с.
15. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Шнайер Б. – СПб. : Питер, 2003. – 368 с.

Глосарій

Автентифікація Аутентификация Authentication	процедура підтвердження того, що пред'явлене ім'я відповідає даному суб'єктові (підтвердження дійсності суб'єкта)	179, 96, 100, 103, 121, 158, 165, 176, 181
Апаратні засоби захисту інформації Аппаратные средства защиты информации Hardware protection	різноманітні за принципом дії, будовою і можливостями технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації	154
Асиметричне шифрування Асимметричное шифрование Asymmetric encryption	передбачає використання двох ключів. Один з них, несекретний (він може публікуватися разом з іншими відкритими відомостями про користувача), застосовується для зашифрування, інший (секретний, відомий тільки одержувачу) – для розшифрування	163, 167
Атака Атака Attack	спроба реалізації загрози	38
Аудит Аудит Audit	аналіз накопиченої інформації, що здійснюється оперативно, у реальному часі або періодично	188, 65, 94, 103, 138, 176
Безпечна система Безопасная система Safe system	система, в якій за допомогою відповідних засобів здійснюється керування доступом до інформації в такий спосіб, що тільки належним чином авторизовані особи або процеси, що діють від їх імені, отримують право читати, записувати, створювати і видаляти інформацію	93
Виток Утечка Leakage	безконтрольний вихід конфіденційної інформації за межі організації чи кола осіб, яким вона була довірена; результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї	54, 13, 28, 30, 53, 55, 90
Вікно небезпеки Окно опасности Danger window	проміжок часу від моменту, коли з'являється можливість використати слабке місце, і до моменту, коли пропуск ліквідується	40
Вірогідність Достоверность	властивість інформації, яка полягає у строгій належності об'єкту, що є її	12

Authenticity	джерелом, або тому об'єкту, від якого ця інформація прийнята	
Віруси Вирусы Viruses	коди, що мають здатність до розповсюдження (можливо, із змінами) шляхом впровадження в інші програми	49, 14
Державна таємниця Государственная тайна State Secret	(секретна інформація) – вид таємної інформації, що охоплює відносини у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою	30
Дешифрування Дешифрование code-breaking	(розкриття шифру) процес одержання інформації із шифротексту без знання застосованого ключа	161
Довільне (дискреційне) управління доступом Избирательное (Дискреционное) управление доступом Discretionary access control	метод розмежування доступу до об'єктів, заснований на обліку особи суб'єкта або групи, до якої суб'єкт входить	95, 100,186
Довірена обчислювальна база Доверенная вычислительная база Trusted Computing Base	сукупність захисних механізмів ІС (включаючи апаратне і програмне забезпечення), що відповідають за проведення в життя політики безпеки	94
Довірена система Доверенная система Trusted System	система, що використовує достатні апаратні і програмні засоби для забезпечення одночасного оброблення інформації різного ступеня секретності групою користувачів без порушення права доступу	93
Доступність Доступность Accessibility	властивість інформаційного об'єкта щодо одержання його користувачем за прийнятний час	11, 18, 44, 50, 106, 182, 196
Екран (Міжмережевий екран) Экран (Межсетевой екран, брандмауэр) Firewall	засіб розмежування доступу клієнтів однієї мережі до серверів іншої мережі	192
Загроза Угроза Threat	потенційна можливість певним чином порушити інформаційну безпеку	38, 27, 102, 219

Захист інформації Защита информации Information Protection	комплекс заходів, спрямованих на забезпечення інформаційної безпеки; діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі	21, 22, 28
Зашифрування Зашифрование Encoding	процес перетворення інформації, при якому її зміст стає незрозумілим для суб'єктів, що не мають відповідних повноважень	161, 164
Зловмисник Злоумышленник Intruder	той, хто робить спробу реалізації загрози	38, 52
Ідентифікація Идентификация Identification	процедура однозначного розпізнавання унікального імені суб'єкта інформаційної системи	181, 96, 103, 119, 176
Інженерно-технічний рівень Инженерно-технический уровень Engineering level	сукупність спеціальних органів, технічних засобів і заходів щодо їхнього використання в інтересах захисту конфіденційної інформації	144
Інформаційна система (ІС) Информационная система (ИС) Information system (IS)	організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів	9
Інформаційна безпека (ІБ) Информационная безопасность Information Security	1) стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації; 2) стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури	9, 10, 11, 13, 106
Інформація Информация Information	1) нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього подання; 2) це відомості, які є об'єктом зберігання, передавання і оброблення	8, 29, 55, 84, 85

Канал витоку інформації Канал утечки информации Leakage channel	шлях від джерела конфіденційної інформації до зловмисника, за допомогою якого останній може одержати доступ до відомостей, що охороняються	54, 59
Комерційна таємниця Коммерческая тайна Commercials secret	відомості, що не є державною таємницею, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій чи фірм, розголошення, виток і несанкціонований доступ до яких може завдати шкоди їх інтересам	35, 30, 81
Конфіденційність Конфиденциальность Confidentiality	властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація	12, 46, 161
Криптоаналіз Криптоанализ Cryptanalysis	наука (і практика її застосування) про методи і способи розкриття шифрів	162
Криптографічний протокол Криптографический протокол Cryptographic protocol	протокол, у якому учасники для досягнення певної мети використовують криптографічні перетворення інформації	166
Криптографія Криптография Cryptography	наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів	160, 161, 162
Криптологія Криптология Cryptology	наука, що складається із двох галузей: криптографії і криптоаналізу	162
Ліцензія Лицензия Licence	дозвіл, що видається державою на проведення деяких видів господарської діяльності, зокрема зовнішньоторговельних операцій і надання права використовувати захищені патентами винаходи, технології, методики	81, 71
Логічне управління доступом Логическое управление доступом Logical access control	механізм доступу багатьох користувачів до інформації та інформаційних ресурсів системи, що забезпечує конфіденційність і цілісність об'єктів і, до певної міри, їх доступність шляхом заборони доступу неавторизованим користувачам	185
Мобільні агенти Мобильные агенты Mobile agents	програми, які завантажуються на інші комп'ютери і там виконуються	51
Невідстежуваність Неотслеживаемость Nontraceability	здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів	13

Несанкціонований доступ Несанкционированный доступ Unauthorized access	протиправне навмисне оволодіння конфіденційною інформацією суб'єктом, який не має права доступу до секретів, що охороняються	54, 53
Організаційний рівень Организационный уровень Organizational level	це регламентація виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає чи істотно утруднює неправомірне оволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз	125
Персональні дані Персональные данные Personal data	інформація (зафіксована на будь-якому матеріальному носієві) про конкретну людину, яка ототожнена або може бути ототожнена з нею	36
Підозріла активність Подозрительная активность Suspicious Activity	поведінка користувача або компонента інформаційної системи, що є зловмисною відповідно до певної політики безпеки або нетиповою згідно з прийнятими критеріями	189
Політика безпеки Политика безопасности Security policy	1) набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію; 2) це сукупність документованих рішень, що приймаються керівництвом організації і спрямовані на захист інформації та асоційованих з нею ресурсів	94, 95, 109
Порушник Нарушитель Illegal intruder	той, хто робить спробу реалізації загрози	38, 62, 64
Правопорушник Правонарушитель Misfeasor	легальний користувач, що намагається одержати доступ до даних, програм чи ресурсів, не маючи на це прав доступу, або користувач, що має у своєму розпорядженні відповідні права доступу, однак використовує їх у зловмисних цілях	64
Примусове (мандатне) управління доступом Принудительное (мандатное) управление доступом Mandatory access control	метод розмежування доступу до об'єктів, заснований на зіставленні міток безпеки суб'єкта і об'єкта	95, 187
Принцип мінімізації привілеїв Принцип минимизации привилегий Principle of minimizing privileges	полягає у виділенні користувачам тільки тих прав доступу, які необхідні їм для виконання службових обов'язків	126, 179

Принцип розділення обов'язків Принцип распределения обязательств Principle of commitments	зобов'язує так розподіляти ролі і відповідальність, щоб одна людина не могла порушити критично важливий для організації процес	126, 179
Програмні засоби захисту даних Программные средства защиты информации Software protection environment	складові програмного забезпечення, що реалізують функції захисту даних самостійно або в комплексі з іншими засобами захисту	157
Програмно-технічні заходи Программно-технические меры Software/hardware means	заходи, спрямовані на контроль комп'ютерної суті устаткування, програм та даних	175
Протоколювання Протоколирование Logging	процес збирання і накопичення інформації про події, що відбуваються в інформаційній системі	187, 94, 176, 189
Ризик Риск Risk	з кількісної точки зору рівень ризику є функцією вірогідності реалізації певної загрози, що використовує деякі вразливі місця, а також величини можливого збитку	118, 105, 120, 121
Рівень гарантованості Уровень гарантированности Assuredness level	міра довіри, яка може бути надана архітектурі і реалізації ІС	94
Розголошення Разглашение Disclosure	навмисні чи необережні дії з конфіденційними відомостями, що призвели до ознайомлення з ними осіб, не допущених до них	53, 67
Розшифрування Расшифрование Decrypt	це процес відновлення інформації із шифротексту	161, 163
Рольове управління доступом Ролевое управление доступом Role access control	суть його полягає в тому, що вводиться поняття ролі, яка пов'язує користувачів і їх привілеї. Для кожного користувача одночасно можуть бути активними декілька ролей, кожна з яких дає йому певні права	187
Сигнатура атаки Сигнатура атаки Attack signature	сукупність умов, при виконанні яких атака вважається такою, що має місце та викликає певне реагування	189
Симетричне шифрування Симметричное шифрование Symmetric Encryption	передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних	163

Система безпеки Система безопасности Security System	організована сукупність спеціальних установ, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз	25
Система захисту інформації (СЗІ) Система защиты информации System of information protection	організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз	21, 22, 23, 131
Стеганографія Стеганография Steganography	спрямована на приховання самої присутності конфіденційної інформації	160, 169
Страхування Страхование Insurance	відносини по захисту майнових інтересів фізичних і юридичних осіб при настанні визначених подій (страхових випадків) за рахунок грошових фондів, що формуються зі страхових внесків, які сплачуються ними	82
Троянські програми Троянские программы Trojan programs	легальні програми, які мають незадокументовані функції, направлені, зазвичай, на перехоплення даних	49, 52
Тунелювання Тунелирование Tunneling	сервіс безпеки, суть якого полягає в тому, щоб «упакувати» передану порцію даних разом із службовими полями в новий «конверт»	199, 176
Фізичні засоби захисту Физические средства защиты Physical means for protection	різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників	145
Хробаки Черви Worms	коди, здатні самостійно, тобто без упровадження в інші програми, викликати розповсюдження своїх копій в ІС і їх виконання (для активізації вірусу потрібен запуск зараженої програми)	49
Цілісність Целостность Integrity	властивість інформаційного об'єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання	11, 45, 100, 106, 166
Юридична значимість Юридическая значимость Legal significance	властивість інформації, поданої у вигляді електронного документа, мати юридичну силу	12

Додаток А

Список підприємств для виконання практичних завдань

1. Агентство нерухомості.
2. Банківське відділення.
3. Конструкторське бюро.
4. Підприємство з виробництва зброї.
5. Букмекерська контора.
6. Провайдер Інтернет-послуг.
7. Секретне підприємство.
8. Науково-дослідний інститут.
9. Підприємство з розробки програмного забезпечення.
10. Підприємство з обробки алмазів.
11. Комп’ютерна мережа банківського відділення.
12. Рекламна агенція.
13. Підприємство з виробництва коштовностей.
14. Віддалений доступ до даних.
15. База даних працівників підприємства.
16. Агентство нерухомості.
17. Підприємство із забезпечення інформаційної безпеки.
18. Телефонна компанія.
19. Компанія із надання послуг Інтернет.
20. Проектний інститут.
21. Інтернет-магазин із продажу книжок.
22. Мережа автозаправних станцій, з’єднаних через Інтернет.
23. Типографія.
24. Туристична агенція.
25. Завод із виготовлення мінеральних добрив.
26. Приватна лікарня.
27. Статистичне управління.
28. Обленерго.
29. Інтернет-портал з дистанційної освіти.
30. Фармакологічна компанія.

Додаток Б

ДСТУ 3396.0-96
ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ
Захист інформації. Технічний захист інформації. Основні положення

1 Галузь використання

Цей стандарт установлює об'єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян - суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

2 Нормативні посилання

У цьому стандарті наведено посилання на такі документи:

- ДСТУ 1.0-93 Державна система стандартизації України. Основні положення;
- ДСТУ 1.2-93 Державна система стандартизації України. Порядок розроблення державних стандартів;
- ДСТУ 1.3-93 Державна система стандартизації України. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов;
- ДСТУ 1.4-93 Державна система стандартизації України. Стандарт підприємства. Основні положення;
- ДСТУ 1.5-93 Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення і змісту стандартів;
- ДБН А.1.1-1-93 Система стандартизації та нормування в будівництві. Основні положення;
- ДБН А.1.1-2-93 Система стандартизації та нормування в будівництві. Порядок розробки, вимоги до побудови, викладу та оформлення нормативних документів.

3 Загальні положення

3.1 Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі - інформація з обмеженим доступом, ІзОД).

3.2 Об'єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ.

3.3 Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення (далі - інформаційна діяльність).

3.4 Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцеве і проміжне обладнання, інженерні комунікації і споруди, відгороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші середовища, грунт, рослинність тощо.

3.5 Витік або порушення цілісності ІзОД (спотворення, модифікація, руйнування, знищення) можуть бути результатом реалізації загроз безпеці інформації (далі - загроза).

3.6 Метою ТЗІ є запобігання витоку або порушенню цілісності ІзОД.

3.7 Мета ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ. Технічний захист інформації здійснюється поетапно:

1 етап - визначення й аналіз загроз;

2 етап - розроблення системи захисту інформації;

3 етап - реалізація плану захисту інформації;

4 етап - контроль функціювання та керування системою захисту інформації.

4 Побудова системи захисту інформації

4.1 Визначення й аналіз загроз

4.1.1 На першому етапі необхідно здійснити аналіз об'єктів ТЗІ, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

4.1.2 Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

4.1.3 Загрози можуть здійснюватися:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкційованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

4.1.4 Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

4.2 Розроблення системи захисту інформації

4.2.1 На другому етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об'єкта ТЗІ.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

4.2.2 Для технічного захисту інформації слід застосовувати спосіб приховування або спосіб технічної дезінформації.

4.2.3 Заходи захисту інформації повинні:

- бути відповідними загрозам;
- бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;
- забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

4.2.4 Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог ТЗІ.

4.2.5 Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

4.2.6 Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами системи ТЗІ.

4.3 Реалізація плану захисту інформації

4.3.1 На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

4.3.2 Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі - засоби ТЗІ) та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далі - засоби забезпечення ТЗІ).

4.3.3 Засоби ТЗІ можуть функціювати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

4.3.4 Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

4.3.5 Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право

проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.

4.4 Контроль функціювання та керування системою захисту інформації

4.4.1 На четвертому етапі слід провести аналіз функціювання системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати засадничі дані для керування системою захисту інформації.

4.4.2 Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації.

За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

4.4.3 У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації.

4.4.4 Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами.

5 Нормативні документи системи ТЗІ

5.1 Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ.

5.2 Нормативні документи повинні забезпечувати:

- проведення єдиної технічної політики;
- створення і розвиток єдиної термінологічної системи;
- функціювання багаторівневих систем захисту інформації на основі взаємнопогоджених положень, правил, методик, вимог та норм;
- функціювання систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації;
- розвиток сфери послуг у галузі ТЗІ;
- установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури;
- організацію проектування будівельних робіт у частині забезпечення ТЗІ;
- підготовку та перепідготовку кадрів у системі ТЗІ.

5.3 Нормативні документи системи ТЗІ поділяються на:

- нормативні документи із стандартизації у галузі ТЗІ;
- державні стандарти та прирівняні до них нормативні документи;
- нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України;
- нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом;
- нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

5.4 Порядок проведення робіт із стандартизації та нормування в галузі ТЗІ встановлюється ДСТУ 1.0, ДБН А.1.1-1, документами системи ТЗІ.

5.5 Порядок розроблення, оформлення, узгодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів установлюється ДСТУ 1.2, ДСТУ 1.3, ДСТУ 1.4, ДСТУ 1.5, ДБН А.1.1-2, документами системи ТЗІ.

Навчальне видання

Володимир Андрійович Лужецький
Андрій Дмитрович Кожухівський
Олеся Петрівна Войтович

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Редактор Т. Старічек
Оригінал-макет підготовлено О. Войтович

Підписано до друку
Формат 29,7 × 42 ¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк.
Наклад прим. Зам №

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к.114.
Тел. (0432) 59-85-32.
Свідоцтво суб'єкта видавничої справи
Серія ДК №3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті
в комп'ютерному інформаційно-видавничому центрі.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к.114.
Тел. (0432) 59-87-38.
Свідоцтво суб'єкта видавничої справи
Серія ДК №3516 від 01.07.2009 р.