Міністерство освіти і науки 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 України як навчальний посібник для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Безпека інформаційних і комунікаційних систем». Лист № 1/11-10311 від 09.11.2010 р.

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.

Л83 Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.

ISBN 978-966-641-514-4

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 978-966-641-514-4

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.

1.3 ВАЖЛИВІСТЬ І СКЛАДНІСТЬ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні вона не розглядалася – національному, галузевому, корпоративному або персональному.

Для ілюстрації цього положення наведемо кілька прикладів.

- Американський ракетний крейсер «Йорктаун» був змушений повернутися в порт через численні проблеми з програмним забезпеченням, що функціонувало на платформі Windows NT. Таким виявився побічний ефект програми ВМФ США з максимально широкого використання комерційного програмного забезпечення з метою зниження вартості військової техніки.

- Міністерство оборони Великобританії у 2009 р. 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.

- В зв'язку з кризовою ситуацією в економіці у 2008 р. компанія Microsoft наполегливо рекомендує компаніям та організаціям використовувати шифрування важливих даних та закривати доступ до внутрішньої мережі для звільнених або таких, що будуть звільнені, співробітників.

- Британський спеціаліст з інформаційних технологій Максвелл Парсонс отримав 2,5 року ув'язнення за злам банкоматів за допомогою MP3-плеєра і спеціального програмного забезпечення. Таким чином він отримував конфіденційну інформацію про банківські рахунки клієнтів для клонування кредитних карток.

- Американські військові оголосили про створення Командного центру кіберпростору ВВС США (U.S. Air Force Cyberspace Command) для захисту країни від онлайнових загроз з Інтернету.

- Невідомі «жартівники» скористалися принципами роботи онлайнової енциклопедії Wikipedia для розповсюдження шкідливого програмного забезпечення – нової модифікації вірусу Blaster.

- 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.

У листопаді 2006 року виник скандал з викраденням трьох ноутбуків з персональними даними 15 тис. британських поліцейських у лондонському Скотланд Ярді. Викрадачів так і не знайшли.

При аналізуванні проблематики, пов'язаної з інформаційною безпекою, необхідно зважати на специфіку даного аспекту безпеки, яка полягає в тому, що ІБ є складовою частиною інформаційних технологій, – галузі, що розвивається безпрецедентно високими темпами.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ. Слід виходити з того, що необхідно конструювати надійні системи ІБ із залученням ненадійних компонентів (програм). У принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу ІС.

У березні 1999 року був опублікований черговий, четвертий, річний звіт «Комп'ютерна злочинність і безпека-1999: проблеми і тенденції» (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). У звіті наголошувалося на різкому зростанні кількості звернень у правоохоронні органи з приводу комп'ютерних злочинів (32 % опитаних); 30 % респондентів повідомили про те, що їх інформаційні системи були зламані зовнішніми зловмисниками; атак через Internet зазнали 57 % опитаних; у 55 % випадків наголошувалося про порушення з боку власних співробітників. Примітно, що на питання «чи були зламані ваші Web-сервери і системи електронної комерції за останні 12 місяців?» 33 % респондентів відповіли «не знаю».

У аналогічному звіті, опублікованому у квітні 2002 року, цифри змінилися, але тенденція залишилася такою ж: 90 % респондентів (переважно з великих компаній і урядових структур) повідомили, що за останні 12 місяців в їх організаціях мали місце порушення інформаційної безпеки; 80 % респондентів констатували фінансові втрати від цих порушень; 44 % (223 респонденти) змогли та/або захотіли оцінити втрати кількісно (загальна сума склала більше 455 млн. доларів). Найбільшого збитку завдали крадіжки і фальсифікації (більше 170 і 115 млн. доларів, відповідно).

У звіті, опублікованому у січні 2010 року, змінилися і цифри, і тенденції: 64,3 % респондентів повідомили, що їх системи були заражені шкідливим програмним забезпеченням; 29,2 % зазнали атак на відмову в обслуго-

вуванні; 17,3 % констатували перехоплення паролів; 13,5 % зафіксували спотворення веб-сайтів. Більшість опитаних незадоволені системами захисту, оскільки вони не забезпечують комплексної безпеки. Велике занепокоєнні викликає відсутність належної підготовки та обізнаності в області безпеки кінцевих користувачів. 43,4 % опитаних респондентів зізналися, що на навчання користувачів витрачається менше 1 % бюджетної забезпеченості. В той час як 25 % респондентів заявили, що більше 60 відсотків фінансових втрат викликані випадковими порушеннями з боку інсайдерів, а 16 % заявили, що більше 81 % всіх втрат компанії зазнали через випадкові порушення.

Збільшення кількості атак – це не найбільша неприємність. Гірше те, що постійно виявляються нові вразливі місця в програмному забезпеченні і, як наслідок, з'являються нові види атак.

У таких умовах системи ІБ повинні мати можливість протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває частки секунди, а інколи пошук вразливих місць розтягується на години і підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ – доступності, цілісності і конфіденційності.

1.4 ОБ'ЄКТНО-ОРІЄНТОВАНИЙ ПІДХІД ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У наш час ІБ є відносно замкнутою дисципліною, розвиток якої не завжди синхронізований із змінами в інших галузях інформаційних технологій. Зокрема, в ІБ поки не знайшли віддзеркалення основні положення об'єктно-орієнтованого підходу, що став основою для побудови сучасних інформаційних систем.

Спроби створення великих систем ще в 60-х роках минулого століття розкрили численні проблеми програмування, головною з яких є складність створюваних і супроводжуваних систем. Результатами досліджень у галузі технології програмування стали спочатку структуроване програмування, потім об'єктно-орієнтований підхід. Об'єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем.

Складність має двояку природу. По-перше, складні не тільки апаратно-програмні системи, які необхідно захищати, але і самі засоби безпеки.

По-друге, швидко зростає складність сім'ї нормативних документів, таких, наприклад, як профілі захисту на основі «Загальних критеріїв», мова про які попереду. Ця складність менш очевидна, але нею також не можна нехтувати.

Будь-який розумний метод боротьби зі складністю опирається на принцип «Divide et impera» – «розділяй і володарюй». У даному контексті цей принцип означає, що складна система інформаційної безпеки на верхньому рівні повинна складатися з невеликої кількості відносно незалежних компонентів. Потім декомпозиції підлягають виділені на першому етапі компоненти, і так далі – до заданого рівня деталізації. Результатом є система у вигляді ієрархії з декількома рівнями абстракції.

Об'єкти реального світу мають, як правило, декілька відносно незалежних характеристик. Поняття рівня деталізації важливе не тільки для візуалізації об'єктів, але й для систематичного розгляду складних систем, поданих в ієрархічному вигляді. Саме по собі воно дуже просте: якщо черговий рівень ієрархії розглядається з рівнем деталізації $n > 0$, то наступний – з рівнем (n-1). Об'єкт з рівнем деталізації 0 вважається атомарним.

Поняття рівня деталізації дозволяє розглядати ієрархії потенційно нескінченні заввишки, варіювати деталізацію як об'єктів у цілому, так і їх граней. При застосуванні об'єктно-орієнтованого підходу до питань ІБ можна виділити такі три грані: це доступність, цілісність і конфіденційність. Їх можна розглядати відносно незалежно, і вважається, що якщо всі вони забезпечені, то забезпечена і ІБ у цілому.

Введемо також такі поняття (рис.1.1):

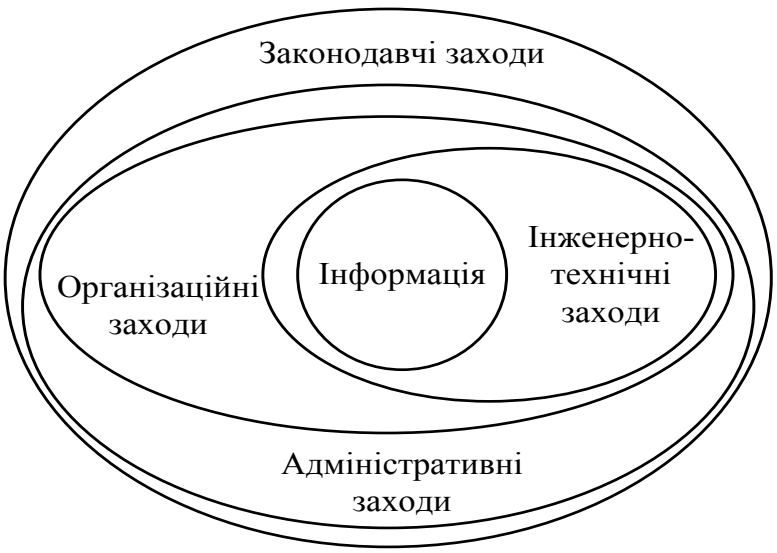

Рисунок 1.1 – Заходи забезпечення інформаційної безпеки

- **законодавчі заходи** забезпечення інформаційної безпеки;
- **адміністративні заходи** (накази та інші дії керівництва організацій, пов'язаних з інформаційними системами, що захищаються);
- **організаційні (процедурні) заходи** (заходи безпеки, орієнтовані на людей);
- **інженерно-технічні заходи.**

Далі кожна з виділених граней буде розглядатися детальніше. Тут же відзначимо, що їх можна розглядати і як результат варіювання рівня деталізації. Тому в подальшому буде вживатися поняття «рівень».

Закони і нормативні акти орієнтовані на всіх суб'єктів інформаційних відносин незалежно від їх організаційної належності (це можуть бути як юридичні, так і фізичні особи) в межах країни, адміністративні заходи – на всіх суб'єктів у межах організації, процедурні – на окремих людей (або невеликі категорії суб'єктів), інженерно-технічні – на устаткування і програмне забезпечення.

Нехай інтереси суб'єктів інформаційних відносин концентруються навколо ІС певної організації, яка має у своєму розпорядженні два територіально рознесені виробничі майданчики, на кожному з яких є сервери, що обслуговують своїх і зовнішніх користувачів. Один з майданчиків обладнаний зовнішнім підключенням (тобто має вихід в Internet).

Нульовому рівню деталізації відповідає інформаційна система в цілому. Вже тут необхідно врахувати закони, застосовні до організацій, що мають в своєму розпорядженні інформаційні системи. Можливо, якунебудь інформацію не можна зберігати і обробляти на комп'ютерах, якщо ІС не була атестована на відповідність певним вимогам.

На адміністративному рівні можуть декларуватися цілі, заради яких створювалася ІС, загальні правила закупівель, впровадження нових компонентів, експлуатації тощо. На процедурному рівні потрібно визначити вимоги до фізичної безпеки ІС і шляхи їх виконання, правила протипожежної безпеки тощо. На інженерно-технічному рівні можуть бути визначені переважні апаратно-програмні платформи тощо.

На першому рівні деталізації (рис. 1.2) або визначаються сервіси і користувачі, або здійснюється поділ на клієнтську і серверну частину.

На цьому рівні потрібно сформулювати вимоги до сервісів (до їх наявності, до доступності, цілісності і конфіденційності інформаційних послуг, що надаються), викласти способи виконання цих вимог, визначити за-

гальні правила поведінки користувачів, необхідний рівень їх попередньої підготовки, методи контролю їх поведінки, порядок заохочення і покарання тощо. Можуть бути сформульовані вимоги щодо серверних і клієнтських платформ.

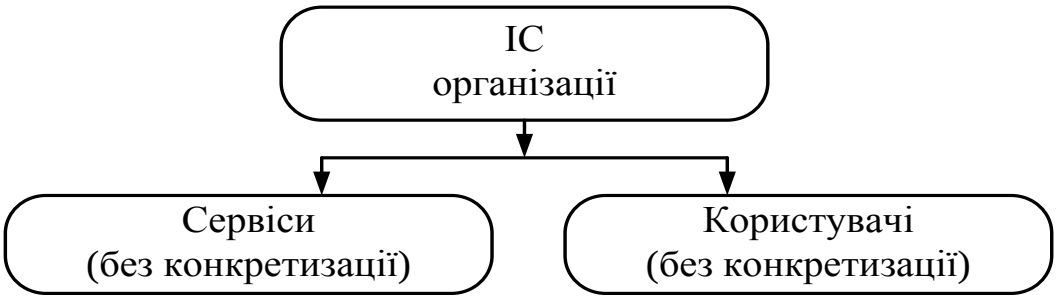

Рисунок 1.2 – ІС при розгляді з рівнем деталізації 1

На другому рівні деталізації (рис.1.3) ще не описується внутрішня структура ІС організації і деталі Internet.

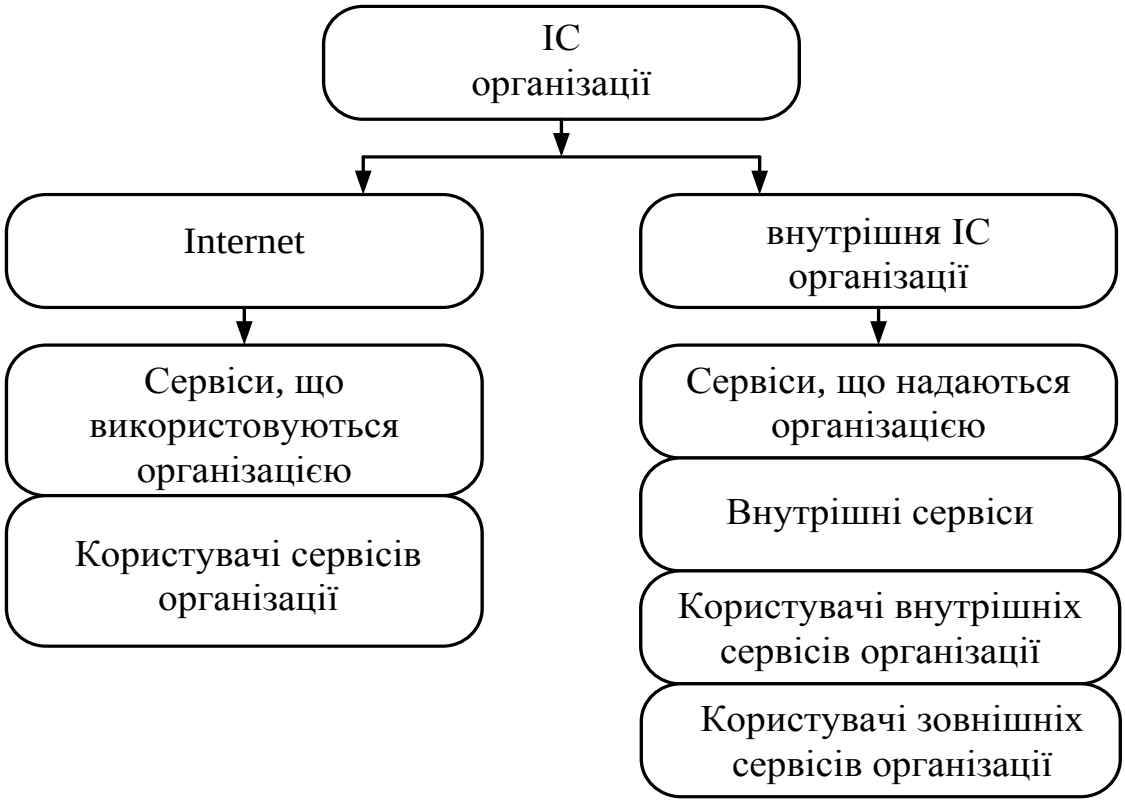

Рисунок 1.3 – ІС при розгляді з рівнем деталізації 2

Констатується тільки існування зв’язку між цими мережами, наявність в них користувачів, а також внутрішніх та зовнішніх сервісів без опису їхнього змісту.

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.

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 22.08.2013 р.
Формат 29,7 × 42 ¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. 14,4.
Наклад 300 (1-й запуск 1-100) прим. Зам № 2013-025.

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.